Secret and Urgent

THE STORY OF CODES AND CIPHERS

by

FLETCHER PRATT

THE BOBBS-MERRILL COMPANY

INDIANAPOLIS *Publishers* NEW YORK

Copyright, 1939, by Fletcher Pratt

PRINTED IN THE UNITED STATES OF AMERICA
BY THE HADDON CRAFTSMEN, INC.

CONTENTS

PREFATORY NOTE

MY WARMEST thanks and the dedication of this book to Major D. D. Millikin, O.R.C., who has made one of the finest collections in existence of works dealing with ciphers, and who has been most generous in allowing me to consult them, beside helping to locate other sources. Thanks are also due to Dr. E. H. Sutherland for permission to quote from his THE PROFESSIONAL THIEF and to Mr. Waldemar Kaempffert, for permission to use his material with regard to Dr. Hans Gross.

A good bibliography on the subject of ciphers and codes can be found in Major Millikin's article on the subject in the ENCYCLOPEDIA AMERICANA. The only work now in print in English touching on the subject is THE MILITARY CIPHER OF COMMANDANT BAZERIES by Rosario Candela. (Cardanus Press, New York, 1938.) The American Cryptogram Association has announced for publication a textbook on cryptography, ELEMENTARY CRYPTANALYSIS (The American Photographic Publishing Company, Boston).

INTRODUCTORY

I

ARCHAEOLOGISTS believe written languages began as series of pictures representing actions. In the case of all but the Aztec hieroglyphics, and to a lesser degree, the Egyptian, these pictures speedily lost their direct significance, and today all written language is cipher. Its symbols have no intrinsic meaning; they convey an idea only when interpreted according to a system whose secret is shared by the writer and reader. We are apt to lose sight of this today because most people learn to read early in life; but it is only necessary to remember the Middle Ages, when a man who could read was about as rare as a telegrapher is now. When the average citizen received a letter, he had to take it around to someone and have it interpreted, and he would now if he were given a missive written in the dots and dashes which are the special cipher of telegraphy.

One could conceivably learn to speak a language—say Japanese or Arabic—without learning how the symbols in which it is normally written could be translated into sound, though if the same words were expressed in the familiar Latin letters the difficulty would disappear. The art of ciphering or cryptography may be defined by saying it is the process of expressing words that convey an idea to everyone in symbols that convey an idea only to the few persons who share the secret.

It is an extremely old art, which seems to come into being almost spontaneously when—and wherever—a large proportion of the population learns to read. In Egypt, Babylon and medieval Europe, where reading and writing were largely monopolies of a priestly class, there is little or no record of ciphers. The ordinary written language was secret enough. The first certain appearance of the art is among the comparatively well-educated Greeks, who seem to have invented one of the two great classes

of ciphers—the *transposition cipher*, in which the letters of the original message are thrown into some meaningless order, and can be returned to their original arrangement by anyone in possession of the key.

The relatively well-educated ruling class of the late Roman Republic seem to have invented the other great system, the *substitution cipher*, in which each letter of the original message is replaced by some other letter, symbol or figure. During the dark ages ciphers vanish; when they reappear it is among the Italian city states, where learning is beginning to bloom under the dawn-sun of the coming Renaissance, and as that movement spreads across Europe, it takes the device of ciphered messages with it.

The rise of the general literacy curve in Europe and subsequently in America has been paralleled by a similar rise in the number of persons who know something of ciphers. We are a highly literate nation today; and there are regular cipher departments in four magazines and a good many newspapers, while the many members of an association of intelligentsia spend much of the new leisure trying to puzzle one another with ciphered messages which the recipient is obligated to work out without the aid of the key.

In other words, the thing has become a game, following the course of development normal to such other necessities of primitive life as hunting, camping and fighting with swords. But the progress of invention has made the sword a sport only by turning the serious business of warfare over to the machine; and this is true also in cryptography. The interests of military and diplomatic secrecy can now be served only by elaborate mechanical devices, such as codes, radio that emits "jumbled facsimile" and ciphering machines. The cipherer who uses nothing but his brain, a writing instrument and a clean piece of paper stands about as much chance against them as a good fencer does against a machine gun.

The inclusion of codes in the list of mechanical devices will be noted. Essentially a code is just that, and it always makes cryptographers indignant to hear the terms "code" and "cipher"

used synonymously. Anyone who knows the key of a cipher can read it without any apparatus but pencil and paper; but even when the key of a code is known, mechanical equipment is required to interpret the message—a code-book, or code dictionary. The ABC and Bentley's commercial telegraphic codes are good examples, their dictionaries being volumes that compare favorably as to poundage with Webster's.

There is also an important difference of central structure between a code and a cipher. In a cipher, every letter of the original message (the *clear*, it is called by cryptographers) is represented by a letter, figure or symbol of the enciphered message. In a code, a code-word (four, five or seven letters long) stands for a phrase, a sentence or even the whole message of the clear.

Ciphers are thus systematic and can be used to express any thought the sender is capable of putting into words; codes are wholly arbitrary, and can express nothing but the limited number of phrases that can be put into a code dictionary. Every navy in the world uses codes to the exclusion of ciphers. Their arbitrary character presents enormous difficulties to the solver, and the partial solution of the code does not entail the fall of the rest, while the number of things ships can be ordered to do is somewhat limited, and does not demand a great vocabulary.

Most armies, on the other hand, use ciphers. Except for units with large staffs and semi-permanent locations, such as division headquarters, they simply cannot carry code dictionaries around, and if they did would always run the obvious danger of losing them by capture. It is worth noting that naval code-books are bound in lead and, when a warship is in danger of being sunk or captured, it is the officers' first duty to throw these books overboard.

Diplomacy hesitates between codes and ciphers, generally favoring the latter because of their greater flexibility and the fact they can be used to express delicate shades of meaning. Codes are popular in secret-service work and espionage because they can express more in less space. Long messages are always dangerous to spies, and they really prefer something, like invisible ink, which will give the impression that no message at all

has been sent. Criminals (it is an amusing comment on the first two institutions that diplomacy, war and crime are the great sources of secret writing) nearly always use ciphers.

It will be the business of this book to trace, as far as possible, the story of the development of secret writing. Unfortunately that story will be episodic and mainly the tale of successful decipherments. At points where we would most like to have a clear narrative of development we shall find nothing but a vague general outline illuminated by flashes of incident. This is inherent in the nature of such a subject; for we shall not much outrage the probabilities by supposing that the most interesting successes of secret writing have remained secret.

There are certain gaps in the main line of the tale which strengthen this supposition and make it impossible to generalize about cryptography on any but a hypothetical basis. Logically, one would expect the Byzantine Empire to have accomplished something special in ciphers. The later Greeks were a particularly subtle and ingenious race with a strong taste for intrigue, and they had Roman experience to go on. (The early Greek ciphers seem to have disappeared without leaving any traces but a note or two in the works of writers attracted by the curious.) Byzantium was a state in which enough people knew how to read so that it must have been decidedly dangerous to send, in clear text, written messages that anyone wished to keep secret. Yet no literature of the period mentions ciphers, nor have any been preserved.

What makes this all the stranger is that while a general line of development can be traced through the Middle Ages with the suggestion that the Roman method of ciphering was first lost, then rediscovered, bit by bit, the line has such enormous gaps that it may not really exist at all. In one of the earliest manuals on cryptography in existence (di Lavinde's from the fifteenth century) the use of an enciphered code is recommended: an extremely modern and complex development, which has not been surpassed today. It argues decades and perhaps centuries of effort to defeat decipherers who have become extremely acute at their business. We have not the slightest clue as to how and where

that skill was acquired. It may have been at Rome; it may have been at Constantinople; or it may have been at Venice and Genoa. If it was a Venetian-Genoese discovery there is a possibility, rather faint, that ciphers were originally developed in that Near East from which the two great commercial cities drew so much else.

In short, when we begin to investigate the history of ciphers, we are digging in a graveyard whose limits we do not know and where there are headstones only for the failures. Decipherments that have changed the course of history (and they are not a few) are often recorded. The triumphs of encipherment, of messages that got through without being read by interceptors are never mentioned—if for no other reason, because people who have used a cipher successfully wish to keep it secret and use it again.

It is probably for this reason as much as because cryptographers are naturally proud of their own performance that the statement is often made that there is no such thing as an insoluble cipher. Strictly speaking it is not true. Roger Bacon in the early Middle Ages wrote a whole manuscript in a cipher that has thus far defied analysis. It is extremely probable that an insoluble cipher could be produced by mathematical means today.

This is true, however, only if the production of an insoluble cipher and the recording of some relatively short message in it were the only end in view. All ciphers in actual use break down on repetitions, not merely repetitions which can be avoided by careful phrasing in a single message but the necessity of repeating the same words or sentences in several messages. The redundancies of action defeat the best efforts of those who would send secret communications.

Nor is the phrasing always careful, even in a single message. Wherever ciphers are most frequently used, they must be written in a hurry, usually by men without much special training, and always without special apparatus. The effort to break them down, to read the messages they contain, will always be made by experts with ample training, a wealth of time at their disposal and whatever special apparatus they need. No systematic method of defeating this analysis has ever been found or is likely to be.

Moreover, another factor enters here. The only method of delaying expert analysis is by complicating the enciphering process; and complication is fatal. An officer of the British Black Chamber estimates that one-third of all the cipher messages which passed through that department during the World War were garbled; that is, mistakes had been made in the enciphering process. The more complex and safer the cipher, the greater the likelihood of these errors; and in some of the better ciphers they are progressive, so that a single error renders all the rest of the message gibberish, even to the man with the key.

The utmost any modern cipher can hope to accomplish is to force the decipherer to employ his last resources, particularly his resources of time; to delay decipherment until the information obtained by the process is no longer of value. That the information obtained by decipherments will always be of some value is the reason why navies use codes.

But this is already trespassing on matters that should be reserved for the text of this volume.

II

A few definitions of special terms will help to make that text clearer.

A *cipher* is a method of writing a message so that it cannot be read by anyone ignorant of the method.

A *cryptogram* is a message written in cipher.

The *clear* is the communication which it is desired to make.

The *message* is that communication after it has been written in cipher.

A *substitution cipher* is one in which letters of the clear are replaced by letters, figures or symbols.

A *simple-substitution cipher* is one in which one letter of the clear is represented by one, and always the same, letter, figure or symbol of the cipher. Example: if the clear be "Come here" and each letter be represented by the one following it in the alphabet, the resulting message will read DPNF IFSF.

A *simple-substitution cipher with suppression of frequencies*

is one in which each of the very common letters (such as E) is represented by several figures or symbols. Example: the same clear as above, "Come here," with each letter still represented by the one following it in the alphabet. But it has been concerted that in addition to F, the figures 2 and 3 will also represent *E.* The message now reads DPNF I2S3.

A *double-substitution cipher* is one in which letters of the clear are represented in the cipher by letters which vary according to a system, the basis of which is a *key-word.* To be more fully explained and illustrated in the text. See Chapter Six.

A *two-step cipher,* not at all the same thing as the last, is one in which the message, usually obtained by enciphering by simple or double substitution, is now enciphered for a second time. The second substitution is usually made according to a table, of which both sender and receiver have copies. This table may (for instance) make the second substitution on the basis of two or more letters at a time. Example: the same "Come here," enciphered as DPNF IFSF. The cipherer refers to his table; suppose it indicates as the value for DP, 416; 317 as that for NF; 96 for IF and 138 for SF. The message would then be 416 317 96 138. In two-step ciphers one of the steps is usually substitution, the other transposition.

A *transposition cipher* is one in which the letters remain the same as in the clear, but are shuffled according to a prearranged pattern. Example: the same clear as above, written in two lines:

C m h r
o e e e

which is read off line by line, the message sent being CMHR OEEE.

A *combination cipher* is a two-step cipher in which the steps are transposition and substitution. Example: "Come here," enciphered by substitution to DPNF IFSF, which is now written:

D n i s
p f f f

and the message taken off as DNIS PFFF.

A *grill cipher* is one in which a grill or mask with holes in it is

placed over the paper on which the message is to be written. The message, in clear, is then written through the holes; the grill removed and the spaces between the words or letters filled up with others to give the whole the appearance of an innocent letter containing no cipher message.

A *syllable cipher* is one in which substitution or transposition is made on the basis of syllable or pairs or triplets of letters instead of single letters. This is very rare.

Nulls are letters or words having no connection with the clear, introduced to confuse a decipherer.

Stops are punctuation marks, usually sentence endings, for which special characters are provided, sometimes placed after each word.

To *encipher* a message is to put it in cipher. To *decipher* it is to reduce it to clear. To *break* a cipher or code is to discover the system by which it was composed. It is perfectly possible for a cryptographer to read the content of a ciphered message without being able to discover the system on which it was written. Another message in the same cipher forces him to repeat the work of decipherment.

Frequency tables are the most important tools of the cryptographer. They are tables showing the relative frequencies of letters, pairs of letters, triplets (trigrams), syllables or words in normal text.

Chapter I

SERMONS IN STONES

I

The Japanese language uses three systems of writing, quite unlike one another, to express the same verbal sounds. In Turkey recently Mustafa Kemal Atatürk ordered that the language be changed over from the old Arabic script, with its system of curves and dots, to the more flexible and printable Latin characters. The whole nation had to relearn its letters, or, in other words, had to learn a new system of cipher, and it is quite possible that within a few more generations the Arabic Turkish will be unreadable to all but a few antiquarians.

What is happening to the most complicated of the three Japanese forms, and to Arabic Turkish, happened long ago to many other languages; that is, the key to the written cipher was lost. The result is that the problems of archaeology are those of cryptography, and occasionally the problem proves insoluble. For a couple of centuries explorers in Asia Minor have been copying from the rocks of that ancient land certain inscriptions which were undoubtedly carved by a race known in the Bible as the Hittites and to the Egyptians as the Khita, but knowledge of the language in which they were written and the system on which it is constructed is so utterly lacking that the inscriptions have never been interpreted. The urns and tombs of that mysterious Etruscan race which preceded the Romans in central Italy have also furnished inscriptions that have thus far defied analysis.

Our knowledge of the language and hence of the civilization and history of ancient Persia might be as tenuous as that of the Hittites and Etruscans but for the greatest single task of decipherment ever performed, a job that took the entire lifetimes

of a number of brilliant men. Their starting point was the Persian inscriptions, a considerable number of which had already been copied from the rocks of that land when the work began. Nobody knew the purpose of these inscriptions; scientists were so uncertain of their date that estimates varied across a sweep of twelve centuries, and of the language in which they were written it was known only that it was no longer spoken.

Carsten Niebuhr, a Danish archaeologist of the eighteenth century, was the first person to make any impression on what had been the impenetrable mystery of the Persian inscriptions. All the inscriptions were written in the cuneiform characters of Babylon, but the groupings of the little wedge-shaped units which made up these characters were very different. Long examination convinced Niebuhr that there were three main classes, which he unromantically designated as inscriptions of types I, II and III.

This classification stood up throughout the inscriptions—that is, no grouping of wedges in a type I inscription was ever found in an inscription of type II or III, and vice versa.

Since the type I inscriptions were much the most numerous, Niebuhr concentrated on them in the effort to find the key of the cipher. Type I exhibited a special characteristic not found in the other two: the points of the wedges with which the characters were written were always directed to the right or downward. Niebuhr therefore suggested that the language in which these inscriptions were written should read from left to right, like modern European tongues, and not in the opposite direction, like all the Oriental languages then known. He then proceeded to compile tables of the characters and their relative frequency. There were forty-two different characters; he therefore assumed that the unknown tongue was written with an alphabet of forty-two letters, and, having spent forty years in making discoveries which have been described in three paragraphs, died.

Niebuhr's pupil, Tychsen, took up the work where his preceptor left off, using as a basis the tables the older man had compiled. Tychsen noted that one of the forty-two letters, an isolated single wedge pointing diagonally downward, accounted for over

twenty-five per cent of the total number of characters. He had compiled tables showing the frequency of letter occurrence in modern languages in the hope of getting some help from analogy, and had found that the highest frequence of any letter in any modern language was the seventeen per cent for E in French. The idea that any one letter in a forty-two-letter alphabet could constitute twenty-five per cent of the whole language struck him as irrational. However, all the characters in all the inscriptions were strung together without gaps. If this slanting wedge were a conventional sign indicating the gap between the end of one word and the beginning of the next, twenty-five per cent would be just about right. Tychsen therefore accepted the hypothesis that this was the case, and passed on to another step.

This step was based on his assumption that the type I inscriptions belonged to the age of the Parthian kingdom in Persia, contemporary with the Roman Empire. There had been several kings of Parthia named Arsaces, and one of them was known, from Roman accounts, to be particularly fond of building monuments and leaving his name around on them where people could see it. Tychsen therefore guessed that a certain word, which had the right number of characters and was very frequently repeated in the inscriptions, was the name of Arsaces. If this were true, the first character in the word would be pronounced as *A* and so on; and by putting an *A* wherever else this character occurred in the inscriptions, one would eventually find other names partially cleared, be able to fill up the gaps, and so eventually to solve the whole alphabet. He tried it on this system; it gave him nothing but gibberish and, still getting gibberish, Tychsen died, worn out and discouraged.

His failure discouraged further inquiry for a number of years, or until one of those persistent and remorselessly logical German investigators took the matter up. He was Georg Friedrich Grotefend, a professor at the University of Göttingen. Looking over Tychsen's work, he was struck by the fact that the Dane had gone at the task in so reasonable a manner that only a fundamental error in his presumptions could account for his utter failure.

Further examination convinced Grotefend that this error lay

in dating the inscriptions. It was certain that all three types of inscriptions came from the same period, for there were in existence clay tablets on which all three types were present—that is, tablets on which the wedges had been impressed while they were still soft and then baked in. The wedges in the inscriptions of types II and III pointed to the left; therefore they must represent different languages from type I. But if one assumed that type I came from the Parthian period, there was no way of accounting for the other two languages, for in Parthian times only a single language had been spoken in Persia. The Parthians, a semi-barbarous people, would certainly not have bothered to translate their important announcements into foreign tongues for the benefit of casual travelers.

In fact, the long history of Persia held only one era when three languages had been current in the country—the era of the Persian Empire, when Median, Persian and Babylonian were on an almost equal footing. Grotefend therefore assumed that this was the correct date of the ancient inscriptions, and that type I was ancient Persian, the tongue of the ruling race, since it came first wherever the three were associated.

Tychsen's identification of the diagonal stroke as a word division struck him as acceptable. He accepted it and passed to the consideration of some of the inscriptions in detail. In two of the longer texts he found a word occurring again and again, but in two different forms, a shorter form and one which reproduced it with the addition of a couple of letters. In the pair of texts Grotefend was examining the word appeared in both forms together, the shorter form being followed by the longer. The tables of word frequencies compiled by Tychsen showed that the shorter form appeared in all the inscriptions more frequently than any other word.

Now in most departments of human thought it is not permissible to make a hypothesis and then find facts to prop it up; but in cryptography this is frequently the only method that will work. Grotefend did what every cipherer does when confronted with a cipher which gives no starting point. He guessed at the "probable word"; and the word he guessed as so frequently

recurring was *king*. The shorter form would be, then, simply *king*, the longer, the genitive form *of kings*, and the doubled word, *king of kings*.

This was not entirely a shot in the dark; in good cipher practice no probable word should be pure guess. Both the language and the culture of the medieval Persian, or Sassanid Empire, were well known to scientific men. It had been a period of conscious archaism and imitation of the ancient kingdom as far as the latter was understood. The title assumed by the Sassanid rulers had been "king of kings"; and the title given to the ancient Persian emperors in Greek histories would, with a little straining, bear translation into the same phrase. This was the license Grotefend had for choosing his probable word.

He now had to prove it correct. In cipher practice this step consists in substituting the letters obtained from guessing the probable word wherever else the same letters occur in the message being solved; the step Tychsen had taken with the name *Arsaces*. If the substituted letters make sense, when occurring in different combinations in other places in the message, then the probable word is right. But this is precisely the step Grotefend could not take; for ancient Persian was a lost language, there was no way of telling whether the letters made sense or not in other combinations.

Therefore, he was compelled to erect still taller towers of hypothesis in the air, hoping that he would someday be able to shove foundations underneath. In medieval Persian inscriptions the first word is always the name of a king, followed by the title "king of kings." The "king of kings" phrase in two long inscriptions with which Grotefend was working occurred in the right places (as shown by the word-division marks) to justify the idea that the ancient Persians had begun their inscriptions in the same way as the medieval. Grotefend guessed, therefore, that the first words in these two long inscriptions were the names of kings. If he could discover what kings were represented, he would be a long way toward solving the whole business, for the names of the Persian kings were known.

The first word, which he had taken for the name of a king, in

inscription A also occurred in inscription B (of the pair he was studying) not first this time, but lower down and with a small word dependent from it, the termination of which was the same as the termination of the long form of the word Grotefend had accepted as *king*. By his hypothesis this long form was the genitive *of kings*; therefore this new word must be a genitive also—*of* something. Most likely *son of*, thought the professor, given the connection with the names.

In short Grotefend had now arrived at the provisional identification of the beginning of the two inscriptions as:

A) X——, king of kings, son of Y——, king of kings —
B) Z——, king of kings, son of X——, king of kings —

This meant that the inscriptions had been set up by a father and son, both Persian emperors, and that the father's father had also been a Persian emperor. The succession order of the emperors was well known from Greek histories. There was only one instance of father, son and grandson following one another to the throne, and the three in question were Hystaspes, Darius and Xerxes.

Assuming always that his identifications were accurate, Grotefend now had something that would give him a clue to alphabetical identifications and pronunciations of the letters in these names. "Hystaspes," "Darius" and "Xerxes" were Graecized forms; he had to throw the three names back into old Persian, taking his cue as to what the old Persian form would be from medieval Persian and Hebrew texts. "Darius" thus appeared as "Darheush" and "Xerxes" as "Khshayarshtra." When these forms were applied to the texts in question the number of letters came out exactly right. It was the first crumb of proof he had obtained after a long Barmecide banquet on pure theory; and with this crumb of proof Grotefend's work came to an end for, like Niebuhr and Tychsen before him, he had now spent a lifetime on the Persian inscriptions.

He had, however, taken the essential step. The three names he had thus provisionally read gave to later workers ten or fifteen letters of the old Persian alphabet with their pronunciations.

Those later workers applied the letters thus obtained to the remaining inscriptions of type I and discovered other recognizable names, which in turn yielded still further dividends of letters. Within twenty-five years of Grotefend's passing the archaeologists were able to read old Persian phonetically; within another five years they were able to translate it with the aid of medieval Persian. Today anyone who wishes to take the trouble can decipher a Persian inscription as easily as a German and sometimes more so.

II

Scientific history is filled with the strangest repetitions, as though new ideas float into the world on some invisible medium and are caught through senses attuned by study in many places at once. The planet Uranus was discovered twice within a month; the periodic law which forms the basis of modern chemistry was propounded separately by two men who had never heard of each other and were working along different lines. Similarly, at about the time that Georg Friedrich Grotefend was painfully spelling out the names of forgotten kings of kings, another archaeological cryptographer was using the same methods to work out the other great puzzle of antiquity—the Egyptian hieroglyphics.

He was Jean François Champollion, an infant prodigy, whose father had been an archaeologist before him and had talked shop over the dinner table so entertainingly that at the age of fifteen the boy was already publishing a learned essay on "The Giants of the Bible" which won the applause of the bewigged professors at the French Institute.

Champollion's problem in dealing with hieroglyphic was radically different from the one Grotefend of Göttingen had faced. The latter had before him various combinations of markings which were altogether meaningless except as the letters of an unknown language. Champollion was trying to read verbal sense into long strings of pictures which were considered by many very good scientists to have no more than a mystic religious sense, like the work of certain savage races which draw a picture of a

deer when they feel hungry, expecting the gods to send them the real article in exchange for the pictured image.

Again, Niebuhr had identified forty-two different alphabetic signs, or letters, in ancient Persian; but the scientists who had already held hieroglyphic under investigation for centuries had discovered over a hundred and sixty signs—far too many to constitute any alphabet, beside which they were unmistakably conventionalized pictures. Moreover Grotefend had plunged into a new field, where all thought was independent thought; Champollion entered a domain already strewn with the wreckage of hypotheses, where it would be fatally easy to accept the errors along with the logic of some previous failure.

Particularly since the discovery of the famous Rosetta Stone. That celebrated chunk of crockery had been found by the scientists who accompanied Napoleon's expedition to Egypt, and was surrendered to the English with the remains of that expedition. It bore an inscription in Greek, together with two other inscriptions, one in hieroglyphic and one in a third form known as Egyptian Demotic, then as unreadable as hieroglyphic. No great intelligence was required to make the supposition that all three inscriptions said essentially the same thing; but some of the best brains in Europe had spent years trying to resolve the hieroglyphic into an intelligible language, and even with the aid of the Greek texts it had proved impossible. The general conclusion was that the problem was insoluble.

For everything seemed to indicate that if the hieroglyphic were a language at all (and not a series of mystical pictures) it was that extremely rare thing, a purely syllabic tongue. For example, in the place where the word *king* appeared in the Greek text, the hieroglyphic had a picture of an extraordinarily tall man with a sword in his hand. This was a logical symbol for *king*; a whole word in one picture-letter. And if this were true, many of the other symbols stood for entire words or syllables; there would be no clue from the interrelation of letters as to how the language had been pronounced, and it would be forever unreadable.

There was also another difficulty. The British scientists who first handled the Rosetta Stone had taken the obvious step of

making parallel lists of Greek words and the hieroglyphics that supposedly represented them. To their dismay they discovered that Greek words which appeared more than once in the inscription were represented on these different appearances by wholly unrelated sets of hieroglyphics, and that the same hieroglyphics were sometimes used to represent different words of the Greek text. Even the names, through which Grotefend was even then breaking ancient Persian, were of no help in this case. The only personal name in the Greek text was that of King Ptolemy V; in the hieroglyphic it was represented by four symbols—too few to spell it out with letters, too many to spell it in syllables. There seemed no conclusion but that the hieroglyphics were purely symbolical; and they had been generally abandoned as such when Jean François Champollion, the boy wonder, entered the lists.

His first step was to count the total number of symbols in the Greek and hieroglyphic texts, a method which is now a commonplace of decipherment, but which Champollion seems to have been first to take in this science. The count revealed that there was something radically wrong with all previous efforts to solve hieroglyphic; for there were three times as many Egyptian as Greek letters. If the hieroglyphics were, then, either symbols for syllables or for ideas expressed as directly as the cave man's deer, the Egyptian inscription must be more than three times as long as the Greek. But the very basis of any deduction must be that the inscriptions say the same thing; and the nature of the Greek text (a hymn of praise to Ptolemy V by a corporation of priests) made it seem unreasonable that there could be any great difference. If the inscriptions were identical, then the hieroglyphics must, after all, be letter-symbols. There were too many of them for any other theory.

On the other hand an alphabet of 160 letters remained inadmissible. But since other scientists had allowed themselves to be hung up on the horns of this dilemma, Champollion neglected it and plunged ahead on the alphabetic theory, attacking the names as Grotefend had in Persian. The name of Ptolemy was neatly enclosed in an outline, preceded by the symbol the English inves-

tigators had taken to represent the word for *king*. Now "Ptolemy" is a Greek word; Champollion made the reasonable deduction that in Egyptian it would have to be spelled phonetically. If the four symbols that stood for the name on the Rosetta Stone were letters, some letters in the name must have been omitted—which? The vowels, Champollion answered himself, remembering that Hebrew, which had a considerable Egyptian heritage, also omitted the vowels. The four symbols of the name were the letters pronounced *P*, *T*, *L* and *M*.

At this point the investigator turned to some older hieroglyphic inscriptions to check his conclusions. He had at hand a couple whose origin in the reigns of Kings Rameses and Thutmoes were proved by portraits and other evidence. The symbol he had adopted as *M* appeared in both names, and the *T* twice, in the proper places, in the second name. Thus it checked and, checking, gave him values for *R* and *S*; and with six letters to work on the scientist-cryptographer began to work through all the Egyptian inscriptions containing known names, obtaining new letter values at every step.

Very rapidly as scientific processes go—that is, in a matter of a few years—he accumulated enough data from names to provide the correct symbols for every possible consonant sound. There remained many letters of the impossibly extended alphabet for which he had no values; letters which never appeared as part of a name. Of these Champollion formed a separate list.

Returning to the Rosetta Stone inscriptions, he noted that one of these unidentified symbols appeared before every noun in the hieroglyphic text, and a few of them appeared before verbs. Now one such symbol was the picture of a tall man that had preceded King Ptolemy's name. Later, where a temple was mentioned the word was preceded by a conventionalized picture of a building, and when the sun-god Ra's name appeared there was a conventionalized solar disc. Champollion therefore reasoned that such characters were "determinatives"—special signs placed in the text by the Egyptian writers to indicate the character of the object they were talking about.

He died at the age of thirty-four without having worked out

all the alphabet, and without having accounted for the remainder of the enormous surplus of letters, for even with the determinatives taken out, most of the words were far too long. It remained for later investigators to show that the Egyptians, in writing words, were never satisfied by expressing a sound in a single letter, but must repeat the same sound in three of four other ways to make certain the reader got the idea. It is as though one were to write the word "seen" as S-C-SC-EE-IE-EA-N. In a cryptological sense hieroglyphic was thus a substitution cipher with suppression of frequencies and the introduction of a prodigious number of nulls; and Champollion's great merit as a decipherer was that he held to the main issue without allowing these things to throw him off the track.

Chapter II

THE ELEMENT OF DOUBT

I

The cryptographer, however, must balance more delicately than an aerialist between not being distracted by collateral issues and failing to recognize root objections. He may hold so tightly to a main line of theory that he fails to see the facts have been fatally strained; and apparently this is what happened in the case of another famous decipherment.

In 1912 a New York bibliophile and dealer in old documents named Wilfrid Voynich bought in Italy a chest full of ancient manuscripts. Most of them were the material of his ordinary business and as such were catalogued for sale, but one had special interest for him. It was a volume of about eight by six inches, written on vellum in a fine clerkly hand, with its pages ornamented by some extremely curious drawings, the whole being bound in with a later but still very old dedication sheet which declared the volume to be the work of Roger Bacon, the famous medieval philosopher.

Dr. Voynich had handled Bacon manuscripts before. If the handwriting were any indication this was from the same pen as the others, and the materials used established it as being indubitably from the thirteenth century, when Bacon had lived. A long course of investigation which stretched across Europe from Italy to England, via Prague and Vienna, established with practical certainty that the manuscript was the work of the famous friar.

The particularly interesting thing about the manuscript was the language. It was not in clerk's Latin, in which Bacon had written all his other known works, nor in any of the other six languages with which he was known to be familiar. It was not

in any language whatever; it was in cipher. The characters in which it was written were not those of any alphabet ever seen, but a set of arbitrary signs, apparently belonging to the alphabet of a substitution system.

As soon as he had established the work as being genuinely from Roger Bacon's pen, therefore, Dr. Voynich submitted it to several cryptographers. The discovery of a substitution cipher from the thirteenth century, employing an arbitrary alphabet, excited them greatly for, although ancient historians had mentioned the alphabet of Julius Caesar, no ciphered text of a date earlier than 1500 had ever before been found, and all the known early cipher texts were simple substitutions using either figures or the normal Latin alphabet. When the signs in the Bacon manuscript were copied off and classified, their appearance and number were found to be consistent throughout, both internally and with the idea that the manuscript had been composed in a simple single-alphabet substitution cipher.

But to the dismay of the cryptographers, their utmost resources proved unequal to the task of extracting a sensible message in any language from the text. This was astonishing in view of the fact that some of the same cryptographers had already performed such feats as reading messages which had first been translated into Chinese and then thrown into a complex cipher—and this without any previous knowledge of Chinese. Nevertheless there the fact was. The cipher experts reported they could go no farther without a great deal of time and expense and that, even then, they would not answer for the results.

Dr. Voynich therefore turned to scientists in other fields. The drawings that accompanied the text were partly of plants, roots, seeds and the process of germination; partly of astrological symbols; partly of stars, among which Aldebaran and the group Hyades were readily recognizable. It seemed logical to believe that the captions which appeared under these drawings were descriptions of the objects, and the manuscript was accordingly submitted to several botanists and astronomers, as well as to experts in ancient languages for attack along the lines used by Grotefend and Champollion. None of them was able to make

the slightest impression on it; and that simple statement may be qualified by mentioning that they put several years of effort into the task.

At this point it occurred to Dr. Voynich that Roger Bacon had also been an expert in the interpretation of the mystic symbolical Jewish Kabbala, and that the manuscript might require interpretation in the light of cabalistic lore. He therefore turned it over to Dr. William E. Newbold, of the University of Pennsylvania, one of the greatest students of medieval philosophy and science. Over the other investigators who had looked into the work Newbold possessed this advantage—that he was familiar with medieval methods of thought and turns of expression.

He knew, for example, that a good medieval thinker who wrote a manuscript in any kind of cipher would be almost certain to include in the manuscript itself a key for reading it; but the key would be couched in symbolic language and its interpretation would be loose and difficult. He began his work by a search for that key.

The last page of the manuscript held a single sentence, and this was the only sentence in the whole manuscript written with ordinary Latin characters instead of the peculiar and unreadable letters of the body of the text. "Michiton oladabas multos te fec cerc portas," read the sentence. No process of anagramming or regarding this sentence as a simple substitution cipher would make sense of it; but if one supposed the presence of a large number of nulls, and supplied a preposition where a corner had been torn from the page, the sentence jelled out as *A mihi dabas multos portas*, which is clerk Latin (with an error in agreement between adjective and noun) meaning "Thou wast giving me many gates."

In his *Epistle on the Nullity of Magic* Bacon had described seven systems of secret writing. One of them consisted in the inclusion of a large number of nulls in an ordinary text. Furthermore, in cabalistic lore the key to a secret, particularly a written secret, is always called a "gate." It seemed perfectly reasonable therefore, to believe that Bacon meant to convey in this sentence that the manuscript had been written in a secret method with

several keys; that is, that it was a cipher of more than one step, perhaps of several.

From this point Professor Newbold turned to the text itself. Under even an ordinary reading glass it was apparent that the wide ink-lines of the letters which composed it were carefully built up of a system of small dots, sweeps and shadings. When these were enlarged it was apparent that a regular system was perceptible in them. Dr. Newbold found twenty-two different signs, or combinations of dots and shadings, in various arrangements. Among these twenty-two he recognized the fifteen signs that composed an ancient Greek system of shorthand.

This system of shorthand was known to Bacon; he had written a Greek grammar with which the scientific world had been familiar for some time in which he described it, at the same time remarking that the Greeks had employed other systems of shorthand. The other seven signs of Dr. Newbold's twenty-two were unfamiliar, but all were of the same general character as the fifteen shorthand signs, and careful compilation from the entire text of the manuscript showed they were probably Roger Bacon's own invention, to fill out the Greek shorthand, which was not well calculated to express all sounds.

The Greek shorthand was a known quantity and so were its gaps; it was not, therefore, especially difficult to discover the significance of the seven additional signs, and thus to translate the entire text into letters. It made gibberish; and when every known method of solving these accumulations of letters as a simple or double substitution cipher was tried on them, the result was still gibberish.

But the key had not said merely "gates" or "two gates" which would indicate a two-step cipher; it had been specific about "many gates." Dr. Newbold interpreted this to mean that whether or not he had been on the right track thus far, he had certainly not gone far enough. In other words there were two and possibly more steps in the cipher still ahead of him. He turned back to Bacon's *Epistle on the Nullity of Magic* and examined the ciphering systems proposed there.

He never told what process of reasoning he employed at this stage, but by some process he became convinced that the next

two steps in the decipherment were those of unraveling an extremely curious system of two-step simple substitutions. The first step in this process was that of doubling each letter recovered from the shorthand and writing the result in linked pairs, as though one should write the phrase "Come here" as CO, OM, ME, EH, HE, ER, RE. For each of these pairs of letters another pair was now substituted according to a regular system; and for this second pair a single letter, again according to a regular system.

The result was still gibberish. But no more than the great archaeological cryptographers would Dr. Newbold give in. He noted that the final step in these various solutions yielded a Latin alphabet; that is, one without k, w, j or y, and a count on the letters showed that the frequencies were just what they should be for Latin. Now a count of the letters in a transposition cipher has exactly the same characteristic; the count is correct, but the letters do not appear in the right order. It therefore seemed to Dr. Newbold highly probable that he had reached the last of the many gates and he attacked the letters that had resulted from his last step as though they were the elements of a regular transposition cipher.

He was still unable to find any orderly system on which they could be arranged to make sense. On the other hand, the professor knew that anagramming of names, mottoes and even of entire inscriptions was a very common practice in the Middle Ages. It occurred to him that anagramming might be successful in this instance also, and that the drawings scattered through the text were more likely than not intended to furnish a clue to such an anagramming process.

Dr. Newbold therefore attacked the illustrated pages; and now at last he began to get sense, and without going too far afield for the letters of his anagrammed text. Mostly the letters to be rearranged occurred in pairs next to one another in the Latin-letter text, either in direct or reversed order. Only relatively infrequently did he have to go as far distant as twelve letters away to find one that would fill out a word, only once in a great while was the letter he needed thirty or forty letters away.

The matter he found in the text when thus developed was sufficiently startling to set the whole scientific world by the ears. It showed that Roger Bacon in the thirteenth century must have discovered and used the microscope which was not reinvented until 1677. The botanical and biological drawings in the text were described as representations of the seminiferous tubes, the microscopic cells with nuclei and even the spermatozoa—details with which modern science has come abreast only recently. But that was not all; among the astronomical drawings was a representation and a description of a spiral nebula, and another of a coronary eclipse—things which had not been rediscovered till the nineteenth century, and then with the aid of powerful telescopes, and which are invisible without telescopes. Bacon must, therefore, have invented the telescope as well as the microscope; and this would place him as the most gigantic intellect the world has ever seen.

Professor Newbold now began to look about for a check on his conclusions. Bacon had written a treatise on alchemy, most of which read like nonsense; and the Professor found it difficult to believe that a man of his intellectual powers could have believed in alchemy or written nonsense unless it were deliberate. He therefore tried his anagramming process on the text of the alchemy book. From it he soon extracted the following note:

> February 26, 1273. King Edward ordered the clergy to undertake a systematic inquisition into crime. They began it, but owing to the antagonism of the nobility, soon desisted. At Oxford the knights besieged the friars; long speeches were exchanged: Bacon exploded gunpowder to scare the assailants with the belief that hell was opening and the devils coming out.

Research in old English records showed that such an inquisition had been ordered in 1273, and that afterward there had been a state trial on rebellious nobles who had attacked the brethren at Oxford. Dr. Newbold waited no longer; in a paper read before the American Philosophical Society in 1921, he described his decipherment and its results.

II

He was instantly and violently attacked. In the first place he was attacked by research chemists, who pointed out that the vellum surface on which the Roger Bacon manuscript had been written was rough, and the ink used in writing the famous document exceedingly thick, almost the consistency of printer's ink. Examination of very old printed records on vellum under the microscope showed the ink breaking up into spots and shadings in almost the same fashion as in the Roger Bacon document.

There was an answer to this objection; no other manuscripts written with the same type of ink had ever been found. The oldest printed documents, with comparable ink, were nowhere near as aged as the Roger Bacon manuscript, the cracking of the ink had not gone so far in them, and the method of application had not been the same in the beginning. Moreover the manuscript was obviously a cipher of some sort, and Dr. Newbold had identified only twenty-two characters; an entirely accidental arrangement of dots and shadings would almost certainly have produced more. The criticism was important only in introducing one more element of doubt to those presently brought forward by cryptographers.

The first of these cryptographic doubts was concerned with the two steps of Dr. Newbold's decipherment which dealt with pairs of letters. To understand the objection it is necessary to reverse the process he used and encipher a short text by the biliteral method. A frame is constructed on some such lines as these:

	A	B	C	D	E
F	A	B	C	D	E
G	F	G	H	IJ	K
H	L	M	N	O	P
I	Q	R	S	T	U
J	V	W	X	Y	Z

The clear is now enciphered by substituting for each letter the

pair of letters which describe its position in the frame. N = HC or CH, for example. If the words "Come here" are thus enciphered the result is:

FC–HD–HB–FE–GC–FE–IB–FE

This is the first step in the double biliteral cipher which Dr. Newbold had described Roger Bacon as taking; and the next step is to substitute for these pairs of letters in the message, other pairs of letters, according to a definite system, which result in the completely enciphered message consisting of interlocking paired letters on the system (mentioned above) CO, OM, ME, EH, HE, ER, RE.

But it can readily be seen that the first pairs of letters enciphered by means of this frame do not interlock; and if the first set will not interlock, neither will the second, nor can they be made to interlock by any process whatever. The Newbold decipherment depends wholly on this interlocking feature, for unless the pairs of letters interlock at the second stage of this encipherment, they cannot be reduced from pairs of complementary letters to single letters for insertion into the shorthand; for shorthand, it will be recalled, was the last step of the encipherment, the first of the decipherment.

Dr. Newbold had an answer here also. Roger Bacon, he said, had not necessarily enciphered his text by the use of such a frame. In fact it was altogether likely that he had done nothing of the sort. What process he had used it was now impossible to say; the decipherment by interlocking pairs of letters was simply a method of approximating the result reached by Bacon along another route. But a second element of doubt had now been introduced.

The anagramming process which came at the end of the decipherment was attacked most heavily of all. The first quality of any good cipher is that it must convey its message with absolute certainty; that it should have two possible interpretations is absolutely inadmissible. Conversely, the first requirement of a decipherment is that it must be the only possible answer. But this is precisely what the Newbold anagramming process was not;

for given the random assortment of letters that resulted from the last step but one of Dr. Newbold's process, it was perfectly possible to construct another text than the one he found. Indeed, the English astronomer Proctor demonstrated that with a text as long as the one resulting from the early stages of the Newbold decipherment, the chances were several millions to one that it could be anagrammed into any clear the decipherer consciously or unconsciously desired to find, thanks to the frequencies of letters in the language. Indeed, one of the United States Army cryptographers, by applying exactly the same anagramming process to the dedication of Shakespeare's First Folio, has been able to read into it a startling prophecy, beginning "Heil Hitler! Roosevelt is C.I.O. He is using the F.B.I. to turn the country Red."

The objection was fatal, and the thing that rendered it fatal was the drawings on which the decipherment was based. Not one of the biological pictures was a clear and certain representation of the life-processes described in Dr. Newbold's decipherment of the accompanying text. They were cabalistic, symbolical, vague and capable of various interpretations. In one notable instance Dr. Newbold's interpretation was almost certainly wrong. He had deciphered the caption under a drawing of a great spirally-toothed circle to mean that it was a representation of the great spiral nebula in Andromeda. Now the spiral nebula in Andromeda lies edge on to the earthly observer; even quite a powerful telescope shows it as an uncertain egg-shaped mass. It was only years after its examination with the best telescopes, and then with the aid of elaborate electrical apparatus, that its spiral character was detected, and no one claimed that Bacon had invented electrical measuring devices or anything that would approximate their results.

Finally, on the general process it was extremely unlikely that Bacon would have used a cipher with so many steps; there is no instance of even a two-step cipher being used for many centuries after his time, and a one-step simple substitution cipher would have adequately baffled any man in his century.

Nor did the decipherment stand up very well in the long run. Neither Dr. Newbold nor anyone else using his system was able to get a sensible reading from the pages of the mysterious manuscript which had no drawings, and to this day it lies there waiting for a cryptographer who can eliminate the element of doubt.

Chapter III

JARGON

I

Lysander of Sparta, commander of the city state's armies in the north, sat in his house at Sestos. At the moment he was the most powerful man in the Greek world. A year had not gone by since he crushed forever the power of the Athenian Empire in the great sea-fight at Aegospotami, captured that proud imperial city, and sailed on to the Hellespont, where Greece met Persia, to put the world in order.

Yet victory had brought problems as well as power. It was the nature of Greeks to be jealous; in overthrowing the parties that had held for Athens among the cities of the north his proceedings had necessarily been highhanded, and of late there had reached him from the home city nothing but an ominous silence. His position was the more difficult because precisely at this moment he had arrived at a parting of the ways of policy, a point where instruction as to the intent and position of the Spartan government was most needed.

Pharnabazus, the Persian satrap who held the Asia Minor shores, had supported him and Sparta in their war with Athens. Outwardly, the Persian was friendly still; but Lysander had reason to believe that Persia looked with as much disfavor on a Greece united under Spartan hegemony as on a Greece united under Athens. The riots among the cities had seemed spontaneous, but there were not wanting signs that Persia had interfered.

The question before Lysander was what course to take—what course the home government wished him to take. Action against Persia might precipitate a major Persian war for which Sparta was unprepared. Doing nothing might allow the anti-Spartan,

pro-Athenian movement among the cities to gather such momentum it could not be halted. It was altogether possible that the home government was already planning on that great war with Persia which Lysander had discussed with them before leaving the city. If he went back to Sparta now, he might just miss the troops and ships coming north for the great adventure. This would be equal to desertion.

As he meditated, a slave was brought in. The man said he was from Sparta, one of four, with messages from the government. Where the other three were he did not know; probably killed or taken somewhere along the route. He himself had been carried off to prison till those who held him were satisfied that he had no message beyond the innocuous one on his tablets, commanding Lysander to observe some religious festival.

The general nodded, and asked the man for his belt, a narrow one of soft leather, written round with one of those meaningless jumbles of letters which the priests of certain mysteries prepare for travelers as invocations to the patron god of journeys, Hermes. The slave handed it over and was dismissed. When he had gone Lysander detached from his own belt the baton which always hung there, an article which those who did not know the Spartan system understood as merely the emblem of his office. The baton was pierced at the end farthest from the handle; through this hole Lysander inserted the end of the slave's belt and wound the strip of leather spirally around the staff, close-packing it so that no wood was left bare between one circuit and the next.

As he did so the dissociated letters, which had been merely gibberish while the belt lay in a straight line, were brought into a new relation to one another. Words and sentences leaped from loop to loop; Pharnabazus had played false to the general and to Sparta. Lysander's friend Thorax had been murdered; his messages to the home city evidently had been intercepted, and there was a bribery complaint against him before the government. Since Lysander had not responded to their request for a reply to these charges (which he had never received) he would be presently judged guilty in absence and condemned.

Within the night a fast galley bore Lysander of Sparta south,

homeward through the Aegean; the first recorded use of cipher had saved a general and an empire, and set in motion the chain of circumstances that led unbroken to the triumph of West over East under Alexander the Great.

II

Suetonius, the Walter Winchell of ancient Rome, says that Julius Caesar kept his fingers on the political pulse of the home city by writing to his friends from Gaul in a cipher that was prepared by shifting each letter of the original clear four places down the alphabet. *Habes opinionis meae testimonium,* which he wrote to Cicero, would thus come out as MDEHV RSNQN-RQNV PHDH XHVXNPRQNZP, allowing for the fact that the Roman alphabet lacked J, K, W and Y.

Given that the science of solving ciphers had not yet been invented this simple system was enough to protect his correspondence from unauthorized eyes. However, we have the best of reasons for believing that Julius Caesar's ciphers were neither used very long nor for the conveyance of very important information. Cicero was one of the people in the secret; and Cicero changed political sides, which meant that the great conqueror's secret was a secret no longer. Moreover, a good many of Caesar's letters in clear have been preserved. We know from them and from other sources that his usual method of secrecy was to say nothing in writing, but to appoint someone he trusted to carry a message orally.

The only thing he really contributed to the history of secret writing was the use of his name. A cipher composed by displacing the letters of the alphabet two, three or more steps down the line is still known as a "Julius Caesar cipher" in spite of the fact that there is good evidence this type of communication was in use before he was born.

III

The ciphers of Sparta and Rome left no recognizable direct descendents. Roger Bacon's, whatever one may think of the New-

bold decipherment, was an isolated effort; and the interpretation of the records of the rocks took place at a time when cryptography was already highly developed. A certain Abbot Trithemius who wrote an early book on ciphers in Holland, says that Charlemagne used ciphers to communicate with his agents, but the tale stands on about the same basis as the confident medieval assertions that Virgil was a necromancer who could fly through the night on broomsticks. We know as a matter of historical fact that Charlemagne himself never learned to read or write any language till he reached maturity, and that most of the great officers of his court remained illiterate to the end. Any kind of writing would have been cipher enough in such an age.

And if Charlemagne did use ciphers, it was another case of an isolated effort. The genuine sources of modern cryptography can be traced, vaguely and with some difficulty, to two widely separated medieval springs—clerkly authorship and thieves' slang. The first may reasonably be looked upon as the beginning of ciphers and the latter of codes, but the two blend and divide like a slow stream passing many islands, and it is not until relatively modern times that they become sharply distinguished.

It is a little difficult to realize today that during the Middle Ages literature was an extra-hazardous occupation. The Church exercised both a monopoly and a close censorship of it and used that censorship in a manner that seemed to contemporaries highly capricious. When a writer set down his thoughts, he knew for a certainty that sooner or later they would come to the attention of the Church authorities, but not what the result would be. Thus Roger Bacon's writings were discovered to be highly heretical; he was put into prison. But the works of his pupil, Thomas Aquinas, were found not only good doctrine but extremely valuable, and he was canonized.

Under the circumstances most medieval writers tried to conceal authorship by some device that would enable them to throw off the mask if the Church approved their work, but keep it up if she did not. One of these devices was that of anagramming the author's name; Rabelais thus appeared as Messer Alcofribas, just as Monsieur Arouet junior (l.j.) was later to become famous under his anagram of Voltaire. The Newbold decipherment has

at least the justification that anagramming was common practice at the time the Bacon manuscript was written.

A more common device and one more important in the history of ciphers was that of suppressing the vowels in signatures and doubtful passages. There were two methods of doing this. One was to replace the vowels with dots on a regular system, *I* being represented by a single dot, *A* by two, *E* by three and *O* by four. (*U*, then written as *V*, was let alone.) Thus "Richard, Roi d'Angleterre" would become R.ch..rd, r..... d'..ngl...t...rr... The other system was to replace the five vowels, in their order, with B, F, K, P and X, making of "Archepiscopus Arnulfus" BRCHFPKSCPPXS BRNXLFXS. The second scheme violated one of the cardinal principles of cryptography by making it difficult to tell a letter of the clear from an enciphered letter; and both were so simple and so well known that they could hardly have deceived anyone, even in the Middle Ages. But as the objective seems to have been not so much complete deception as something to furnish a lawyer's talking point in case the matter came before an ecclesiastical court, these simple devices seem to have served their purpose.

At this point there occurs in the history of cryptography one of those gaps which can be crossed only on the slack wire of hypothesis. The earliest known writing concerned with ciphers is a book by one Sicco Simonetta, who was connected with the chancellery of the Sforza Dukes of Milan between 1375 and 1383. It is called the *Liber zifrorum*; its nature is that of a manual for the diplomatic agents of the duchy. In it Simonetta recommends the use of simple substitution ciphers with suppression of frequencies and the insertion of an occasional code sign. This argues that the Italian courts had already learned the method of solving straight simple substitution ciphers, and requires a brief digression to describe that method.

IV

Simple substitution is the ABC and arithmetic of cryptography, and a complete understanding of it and of the method of

breaking it is essential to any knowledge of the art. Explanations of the method, surrounded by very good stories, are given both in Poe's *Gold Bug* and Conan Doyle's *Adventure of the Dancing Men,* but as ninety per cent of all cipher messages are in some form of simple substitution it is worth giving another here.

Perhaps the simplest form of all is that which assigns a number to each letter of the alphabet in order of occurrence—A = 1, B = 2, C = 3, and so on; or reverses the process, making Z = 1, Y = 2, X = 3. Along with it goes the alphabet of Julius Caesar, which replaces each letter by the one that follows it, two, three or more places down the alphabet. Both are still occasionally met with—usually among school children or pairs of secretive and romantic lovers. Most simple substitution ciphers go beyond this to introduce some slight complication, such as writing the message in conventional signs instead of letters, or using a key-word, something in which no letter is repeated, the key-word being written down, with the rest of the alphabet following and the clear alphabet below:

N E W Y O R K A B C D F G H I J K M P Q S T U V X Z
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

In enciphering, the letters of the top line are substituted for those of the lower line. Example: *All cats are grey at night* becomes NFF WNQP NMO KMOX NQ HBKAQ, or, making the message up into five-letter groups and adding nulls at the end to fill out the last group, as is frequently done:

NFFWN QPNMO KMOXN QIIBKA QVCDZ

Suppose now that the cryptographer is faced with a message of unknown content. (The groups are numbered for convenience in referring to them.)

1	2	3	4	5	6	7
SZPQP	ERJKQ	PCRKJ	VZXPU	PJSZP	GKRSC	GCSPT
8	9	10	11	12	13	14
QIQXL	SKNQC	LZPQR	ZKTFM	ZPRES	CSPFK	JNKUP
15	16	17	18	19	20	
QCREG	LFPRT	HRSES	TSEKJ	IELZP	Q	

The first step in decipherment is to count the frequency with which each letter appears and to draw up a table of the result. In the present case it is:

P - 13	J - 5	N - 2
S - 10	L - 4	M - 1
Q - 8	T - 4	H - 1
K - 8	F - 3	V - 1
R - 8	G - 3	
Z - 7	I - 2	
C - 6	U - 2	
E - 6	X - 2	

The first observation to be made from this table is that the message cannot be in a transposition cipher. There are not enough vowels and though in a short message frequencies do not always correspond to those given by the tables, P, Q and X come altogether too often.

Therefore the cipher is substitution; and if substitution, then simple substitution, since double substitution (for reasons that will be given later) would very likely have more than twenty letters represented, and would show no such violent variations in frequency as the drop from 13 P's to a single M, H, and V.

Having cleared the track by identifying the cipher according to type, the cryptographer now turns to his table of letter frequencies. (Table I) Here he finds that E is the most frequent letter in English with T next. It seems likely, therefore that P is *E* and S is *T*. In a message as short as this the order of the first two may be reversed; but it will be noted that the P's are scattered fairly evenly through the message while the S's tend to bunch, which would indicate the correctness of the P = *E* solution. Consonants group themselves; vowels invariably scatter. The message is accordingly rewritten with the provisional values P = *E* and S = *T* in the proper places below:

1	2	3	4	5	6	7
SZPQP	ERJKQ	PCRKJ	VZXPU	PJSZP	GKRSC	GCSPT
t.e.e	.....	e....	...e.	e.t.e	...t.	..te.

8	9	10	11	12	13	14
QIQXL	SKNQC	LZPQR	ZKTFM	ZPRES	CSPFK	JNKUP
. . . . .	t	. . e . .	. . . . .	. e . . t	. t e . .	. . . . e

15	16	17	18	19	20
QCREG	LFPRT	HRSES	TSEKJ	IELZP	Q
. . . . .	. . e . .	. . t . t	. t . . .	. . . . e	.

This seems very reasonable; it contains no impossible linguistic combinations and the spacing of the *T's* and *E's* appears what it should be in normal text. Following T and E the next letters in the alphabet in order of frequency are A, O, N, R, I and S. In the message under consideration this corresponds very well with the high frequencies of the letters K, Q, R, Z, C, and E; but both in message and in frequency table these six letters are so closely grouped that it would be very difficult to tell which was which without extensive experiment along trial and error lines.

The cryptographer therefore takes a short cut by consulting the table of trigrams, or three-letter groups. (Table XII) These show that *the* is overwhelmingly the most frequent three-letter combination in the language; and further, that it is very rare to find any letter but H standing between T and E. In the present message the combination *T*-blank-*E* occurs twice, in groups 1 and 5. In both cases the blank is represented by the same letter of the cipher (Z), and on frequency Z can well represent *H*.

But if Z = *H*, then Q is probably *R* or *S*; for with the insertion of the *H* group 1 reads *THE*-blank-*E*, which is a strong possibility for *THERE* or *THESE*. Q, which fills the blank could be, on frequency, either *R* or *S*. However in group 10 the combination ZPQ occurs and the ZP has been solved as *HE*; and the same combination is repeated in groups 19-20. Reference to the trigram table shows that HER is one of the most common in the language, while HES is relatively rare. The balance of the probabilities thus favors the hypothesis that:

$$Q = R$$

and it is accordingly filled in that way.

In groups 17-18 occurs the combination SESTSE. This has been partially solved to read *T*-blank-*T*-blank-*T*-blank, which, with the repeated E's, constitutes a pattern word. The cryptographer therefore looks at his table of pattern-words (Table XI) and discovers that this pattern usually means TITUTI or TETATE. Since P = *E* in this cipher, the pattern must represent the first of these two combinations, which yields the values:

$$E = I;\ T = U$$

both of which check very well by the frequency table for the message. These values are now filled in, and it becomes evident that the cipher is near complete solution.

1	2	3	4	5	6	7
SZPQP	ERJKQ	PCRKJ	VZXPU	PJSZP	GKRSC	GCSPT
there	i...r	e....	.h.e.	e.the	...t.	..teu

8	9	10	11	12	13	14
QIQXL	SKNQC	LZPQR	ZXTFM	ZPRES	CSPFK	JNKUP
r.r..	t..r.	.her.	h.u..	he.it	.te..	....e

15	16	17	18	19	20
QCREG	LFPRT	HRSES	TSEKJ	IELZP	Q
r..i.	..e.u	..tit	uti..	.i.he	r

Of the little group of letters that showed high frequencies in the message there now remain unsolved R, C, K and J; of high-frequency letters for which no values in the message have been found there remain A, O, N and S. Two of these drop into place with the acceptance of the *TITUTI* combination, which can hardly end in anything but *ON*, yielding the equations:

$$K = O;\ J = N$$

If this be correct, groups 1-2 now read *THERE I-NOR*, or, dividing it into words along the obvious lines, *THERE I- NO R*, which makes it apparent that:

$$R = S$$

This leaves only one letter in the high-frequency group (*A*) to be accounted for and only one letter of high frequency in the

message (C); and unless there be some strong reason to the contrary the cryptographer can assume that:

$$C = A$$

Once more filling in, with the obvious word divisions indicated, the following result is obtained:

```
 1       2       3       4       5       6
SZPQP/ER/JK/Q  PCRKJ/  VZXPU  PJ/SZP/  GKRS/C
there/i s/no/r  eason/  .h.e.  en/the/  .ost/a

 7       8       9       10      11      12      13
GCSPT Q/IQXL SKNQC LZPQR ZKTFM/ ZPRES CSP/FK
.ateu r/.r.. to.ra .hers hou../hesit ate/.o

 14      15      16      17      18      19      20
JNKUP Q/C/REG LFP/RT HRSES TSEKJ/ IELZP Q
n.o.e r/a/si. ..e/su .stit ution/.i.he r
```

It is apparent how nearly this finishes the task. Obviously nothing will do at the end of group 11 but the letters *L* and *D*, to complete the word *should*, which gives the equations:

$$F = L;\ M = D$$

Similarly replacing the G of the message in group 6 with *M* yields a satisfactory result, and the U's in groups 4 and 14 work out nicely as *V's*. *LON*-blank in groups 13-14 now becomes clear as *LONG*, and H = *B* is required in group 17. The remainder can now be filled in:

$$V = W;\ X = Y;\ L = P;\ I = C.$$

The message is solved and the cryptographer now draws up his table of equivalents:

```
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
C H I M P . N Z E . . F G J K L . Q R S T U V . X .
```

The key-word was evidently "chimpanzee" with the final E dropped off (repetitions are not permissible) and it is now possible to fill in the whole table and wait for the appearance of the next message written with the same key.

V

This is the basic method in all decipherments of substitution ciphers. Admittedly the example shows the process at its shortest and simplest. In normal English text the alphabetic frequency tables are unreliable until two hundred or more letters have been reached in one message or two or three written with the same key. Still with the backing of the bigram and trigram tables any cryptographer can dismember any simple substitution cipher in a few minutes and with a minimum of trials. The fact was evidently widely known when Sicco Simonetta wrote that first book on ciphers, for he included alphabetic frequency tables in it.

At the same time the earliest codes were also being found wanting. In the sense that they are mentioned earlier, they antedate ciphers; and, like ciphers, appear to have grown out of the then new custom of keeping at foreign courts resident ambassadors who found it necessary to send reports home and ask for instructions. Venice and the Papal Curia were the first powers to use resident ambassadors; and, though the latter may well have used means of secret communication before the republic of the lagoons, the oldest reference to any code system is in an instruction to the Venetian ambassador at the Court of Austria. In his dispatches it is ordered to refer to the Doge as "V," the King of Hungary as "P" and the Pope as "Q."

The context alone would apparently betray the secrets of such messages if they were intercepted, an observation with which the Venetians evidently agreed; for only twelve years after this first crude code, another Venetian instruction orders the city's diplomats to refer to important personages by periphrasis—that is, to speak of Austria as the "Sun," since the sun rises in the east; the east = Ost = Österreich; and to replace all the verbs in their dispatches with meaningless words according to a regular system outlined in a little code dictionary they were given when setting out on a mission.

Then comes another of those gaps in cipher history, followed

by the appearance of the *Trattati in Cifra* of G. di Lavinde in 1480. It is quite a remarkable book, showing cryptography already in a state of considerable development, for he recommends a method of decipherment by attacking the vowels, which is still classic for the Latin languages, and a method of defeating this decipherment, by first throwing messages into a kind of jargon-code, and then enciphering them by simple substitution with suppression of frequencies. Perhaps more remarkable still, di Lavinde's official position was that of special secretary for secret communications before the Pope. Ciphers had already become so important a business at the Curia as to require the attention of a full-time expert.

Within the next hundred years every major court and minor principality of Italy, Spain and France was using ciphers, and all the great systems of encipherment but one had been invented. Decipherment does not seem quite to have kept pace; indeed it was nearly four hundred years before the classic method of deciphering double substitutions was discovered. Now in cryptography as in other fields of human activity necessity is so much the mother of invention that it is difficult to believe that if the complex systems of cipher had been widely used, means of breaking them down would not have become as widely known as the ciphers themselves. As a matter of fact, practically all the ciphers of which samples have been preserved to us from periods before the Napoleonic era belong to relatively simple types. It is difficult to avoid the conclusion that the more elaborate systems, though they were developed early, remained buried for some time in the theoretical manuals of the men who invented them.

This theory is considerably strengthened by the fact that we know northern Europe, where the greatest development in deciphering processes subsequently took place, did not take readily to ciphers in the early days of resident ambassadors. There were two or three striking historical incidents which painted the unreliability of the existing systems of cipher across the continent (they will be described later); and the North had long since developed its own device for private communication. Under the

pressure of the rising art of diplomacy this device began to develop into a regular system. Its basis was a code which is not a code—jargon, cant, euphuism, the erection into a regular method of expression of that system which had formed part of the means of communication used by the Venetian agents in the fourteenth century.

VI

Partly this method is inherent in the Teutonic languages themselves, which drop the precision of the Latin tongues for a tendency toward double meanings and involved images. One of the earliest written works in any northern language, the Prose Edda, is a handy manual of involved periphrastic metaphors for the use of poets.

"What shall we call the air?" says one passage. "The air may be called the ravens' causeway; or the bearer of storms; or the woof of the winds."

If figures of speech are constantly used, if they be sufficiently farfetched and involved, or if they have reference to something known only to a few persons, this sort of thing can be developed into a code which can be either written or spoken. It is difficult to state positive facts when dealing with so indefinite a subject, but it would seem that the inspiration for the use of this type of code for diplomatic purposes comes ultimately from the very root of the language growing through medieval thieves' slang, which was already highly developed in the fourteenth century.

"These Babes of Grace," says an early Elizabethan instruction for the training of young thieves, "should be taught by a master well verst in the cant language or slang patter, in which they should by all means excel."

A good deal could be and has been written about these peculiar crooks' codes, about which it is enough to remark here that they seem to have reached their greatest development in the early part of the nineteenth century. This was the period when a pair of initiates could carry on a whole conversation without an eavesdropper catching any more of it than the prepositions. Both

Victor Hugo (*Les Misérables*) and Eugène Sue (*Les Mystères de Paris*) give some interesting examples, most of them already out of date when they were distilled into the books; and the famous Vidocq, who was on both sides of the law at different times, quotes a long song by means of which young members of the profession were taught its special language, not very good as a song but intended more as a school exercise:

J'ai fait par comblance
Gironde languepé,
Soiffant picton sans lance,
Pivois non maquillé,
Tirants, passe à la rousse,
Attaches de gratousse,
Cambriot galuché.*

The very facts that such a mnemonic rhyme should be necessary and that Vidocq, who was then a member of the police, could record it, marks the decline of thieves' argot as a language or code, peculiar to the profession.

The fact is that the argot had obeyed the natural tendency all codes have, that of spreading to cover more and more of the possible exigencies of conversation, and in this process it had become so complicated and difficult as to fall of its own weight. The men for whom it was produced simply could not or would not spend the time and effort necessary to learn it. The early nineteenth century was also the period when police science enjoyed its great and rapid development, with most detective forces coming into being. It was instantly evident to such officers as M. Henry in France and Sir Richard Mayne in England that a man who could hang about criminals' haunts as one of themselves could learn their argot, and through it learn anything else he wished to know about their operations. Smart detectives

* I acquired, moreover,
A pretty mistress
Dreaming of wine without water,
And unadulterated booze,
Stockings, fine shoes,
A lace-covered waist,
A feathered hat.

therefore made a business of learning argot, and the moment this happened it began to decline.

VII

A criminals' code of sorts, common to the whole underworld, still exists, but it has become largely a matter of inflection and innuendo, with the inclusion of a few special identifying terms. The professional thief in E. H. Sutherland's *Professional Thief* tells the following story:

> "The language of the underworld is both an evidence of the isolation of the underworld and also a means of identification. A professional thief can tell in two minutes' conversation with a stranger whether he is acquainted with the criminal underworld and in two minutes more what particular rackets he knows intimately. If a thief were in the can and another person were brought in, the first might ask, 'Where were you nailed?' The second might say, 'In the shed.' It is possible that an amateur might know that 'nailed' meant arrested but no amateur would use the word 'shed' for railroad station.
>
> "I was eating supper in a cafeteria with an occasional thief who was a student in law school. Two coppers were sitting at another table near by. The occasional thief had selected our table and had not recognized them as coppers. They were not in uniform. My friend said loud enough so the coppers could hear, 'Did you hear what Jerry Myers got?' I knew alright Jerry got four years, but I was not going to let the coppers know we were talking about anyone who had received a bit, and I had to hush the youngster up. I could not say 'Nix!' as a thief might have said if the coppers had not been able to hear, for this in itself would have informed the coppers that we were worth watching. So I said, 'I understand the doctor said he got tonsillitis.' A professional thief would have sensed danger at once and would have carried on along that line, but my friend started in again, 'No, I mean—' but I kicked him under the table and butted in again with some more about tonsillitis. The police were watching us carefully and I could not

office my partner by moving my eyes toward them. I had to get up and go to the counter for something more to eat. When I returned I picked up his book on Conveyances and looked at it and then asked, 'Have you seen the new book on abnormal psychology by Dr. Oglesby?' The policemen immediately got up and reached for their hats. I nudged my partner to look at them as they got up and you could see that each had a revolver in a holster. My partner now understood why I had interrupted him and he asked, 'Why didn't you tell me they were here?' I had told him a half-dozen times in language any professional thief would have understood."

VIII

It is impossible to say when and in what manner thieves' slang got itself into a gold-laced coat and began to present diplomatic credentials. We sight only a few details through the fogs, just enough to be fairly sure that while ciphers were developing in Italy the diplomatic jargon-codes were coming into being at the opposite end of Europe. Margaret, the queen who united Scandinavia for a brief period under one head, writes to her ministers in language none but they and she can understand; almost two hundred years later Queen Elizabeth's ambassador to Ivan the Terrible sends home a dispatch couched in strange terms.

There is also the record of a complete jargon-code from 1622, just before Cardinal Richelieu came into power in France. Louis XIII's ambassador to Rome takes with him a code-book written on two large sheets of paper. The Pope is to be referred to as "the rose," and Rome is "the garden"; Cardinal de Savoye is "the laurel," Cardinal Aldobrandini "the jasmine," Germany "the stable," Spain "the manger."

The use of such a code was apparently the product of dissatisfaction with the ciphers that had just preceded it as the common vehicle of diplomatic use, and it was left to the ambassador's ingenuity to combine these various botanical references into sentences that would slip through the mind of an interceptor without making an impression. The Louis XIII code,

however, suffers to an exaggerated degree from the common defect of all codes—that of limiting the writer's power of expression. It is difficult to conceive, for instance, by what verbal trickery such a statement as "the jasmine is now acting in the interest of the manger" could be so altered that it would not appear to have a secret meaning; and once the fact of such a code's existence was discovered, its secret was as good as gone. The context of even a single message would be enough to give the whole thing away.

Yet the basic idea was too good to be abandoned without thorough trial—a code that would convey secret information right under the nose of an interceptor by means of a perfectly harmless text. All through the eighteenth century the jargon-code is tried again and again, by governments and private individuals and at times it becomes a perfect mania. Frederick the Great invited Voltaire to leave France and come to his court in such an allegorical code, and after he got there sent him the famous "code invitation" which is still a puzzle for schoolboy students of French:

$$\frac{\text{P}}{\text{Ce soir}} \quad \text{à} \quad \frac{\text{Ci}}{\text{Sans}}$$

To which the reply was:

J a*

Bonnie Prince Charlie and the Scotch Jacobites sent one another information in an allegorical code, and when the latter toasted the King at dinner they passed their wineglasses over the water carafe to signify "The King over the water." The great Duke of Marlborough and his hatchet-faced wife used such a code.

About the middle of the century the French state papers furnish another example of such a code in diplomatic use, an ambassador to Russia taking with him a small code dictionary much more elaborate than the one of a hundred years before. In it individuals are referred to under the names of furs; nations, in-

*See notes at back.

trigues and movements of armies are described in terms of the trade. The code lists the English ambassador as "fox," the Austrian as "wolf," and refers to English troops as "moleskins."

The system was possible because the French ambassador carried a perfectly genuine fur merchant in his suite. When he wished to send a secret dispatch, he would first write an ordinary dispatch in ordinary language, deliberately getting as much wrong as possible, and send it through the regular channels, being quite sure it would be intercepted and read. Meanwhile the fur-merchant secretary would send to another fur merchant in Paris something like the following:

> "Wolf is all the fashion at St. Petersburg now. I hear that Herr Emmerich of Berlin has sent through an order for thirty thousand moleskins, although his financial condition is not good and one wonders where he will find the money to pay for them."

The Paris fur merchant would take this innocent commercial message around to the French chancellery, where it would be interpreted to mean that Russia and Austria were drawing toward an alliance, and that there was a rumor the King of Prussia had asked for the services of 30,000 British soldiers, but was having some difficulty in obtaining them, not having much to offer in return.

In spite of the fact that it was difficult to convey precise and specific information in a code of this type, it was a useful instrument, concealing the fact that there was any secret to be unraveled. The allegorical code was still very much in use at the time of the World War, especially in espionage work, and none of the nations could find a much more effective answer to it than by censoring telegrams. One day, when a British squadron steamed out to sea, a telegraph censor in Edinburgh found among the messages going over the commercial cables an order for several thousand safety-razor blades, addressed to a firm in Stockholm. He happened to have been in the safety-razor business and was slightly surprised by the size of the order, which did not seem justified by what he knew of current commercial conditions.

A check-back was instituted, and he discovered that in the past six months the same agent had ordered from Sweden more safety-razor blades than all England had used in the last three years! Within an hour the safety-razor agent was facing a military court which wanted explanations and wanted them in a hurry.

On another occasion a censor in the south of England found in his hands a telegram from a man suspected of being a spy, but against whom there was no proof, and addressed to somewhere in Holland. "Father is dead," the message said simply. The censor considered it briefly, changed the text to "Father is deceased" and let it go through. Next morning the reply was placed on his desk:

"Is father dead or deceased?"

There is really no method of breaking such codes but that of common sense; and the main difficulty lies in detecting their existence. As early as 1916 the Allies became certain that information was leaking through to Germany by this method and a check-up, performed by sending out bits of false information in suspected quarters and watching for the result, showed this was perfectly true. To counter the work of the spies the practice was adopted of holding up all private telegrams of whatever nature for forty-eight hours on the eve of important military movements.

There was also a good deal of talk about using the Personal columns of the daily newspapers for code communications, but it is highly doubtful whether this was ever done. Obviously only the most generalized information could be sent through the limited wordage of a newspaper classified ad; and it is equally obvious that to use the method consistently would be an invitation to the counter-espionage workers, not to mention the fact that papers published in London or Paris could not possibly reach Germany through neutral countries in less than three or four days.

The general public remained convinced that most Personal ads were in code, however, and bombarded the government departments in both France and England with warnings—which gave rise to some ludicrous incidents, such as the occasion when an amateur cryptographer came rushing into the headquarters of

the British deciphering department and demanded to see the chief.

"I've got it!" he cried, when he finally secured admission, and brandished a copy of a morning paper, pointing to a Personal:

> ETHEL—Sorry I cannot meet you under the limes at five o'clock.—Sally.

"There have been three of these Ethel-Sally messages in a week, and they make up a system of code," declared the amateur. "I've finally solved it. Here's the answer."

He held out a slip of paper on which was written:

> To all Channel U-boats. Transports will leave Southampton tonight at eight o'clock.

The officer read through the decipherment without displaying any signs of perturbation.

"That's very interesting," he said.

"I know it is. That's just what I've been writing letters to your department about—letters to which they have paid not the slightest attention. These messages were put in by German spies!"

The cipher expert permitted himself to smile. "Oh, I think not," he replied. "It just happens that I inserted those Ethel-Sally messages in the paper myself to see what you amateurs would make of them."

IX

On the other hand there is a story, several times repeated by Italian sources, unverified and possibly not true, but which, if true, represents one of the greatest coups ever put over by means of an invisible code. When the last great Austrian advance rolled down to the Piave in the autumn of 1917 it embraced a town a mile or so back from the left bank of that stream where there was a big inn with a courtyard, in the center of which stood a well. This well the Italians wired for sound, concealing a microphone under the curbing and carrying wires down through the water and underground to a point where they could be led across

to the side of the river in their possession. The inn they left intact; it was an obvious spot for an Austrian headquarters, and sure enough a divisional staff established itself there.

Unfortunately the conversations picked up by the microphone were not rich in information. But the device worked beautifully as far as audibility went, and the Italians turned it to use by sending through the Austrian lines one of their best spies, a girl named Rosita, who was a clever singer and an accomplished guitarist. She established herself in the town with the inn and well, and every night came to the courtyard to entertain the Austrian divisional staff with improvised ditties, into which were woven amusing little comments on each division and regiment that arrived in line, with personal chatter about its officers.

Naturally, these songs also formed a convenient code by means of which she was telling her countrymen through the microphone, the name, location and characteristics of every Austrian unit facing them. In a cryptographic sense the thing is possible but very difficult; Rosita would have had to be extraordinarily clever to get that much information into her songs without arousing suspicion. But it is certain that the Italians were particularly well informed as to the enemy order of battle before they launched their troops in the great offensive of Vittorio Veneto that broke Austria and drove her out of the war.

Chapter IV

INVENTION AND DEATH

I

The same Abbot Trithemius, who attributes a cipher to Charlemagne without much evidence to support the claim, attributes to himself without much more the invention of a system of encipherment which has become classic under his name and which has had a numerous and curious progeny. Its basis is simple substitution, but instead of substituting letters, figures or signs for the letters of the clear, it replaces them with words or phrases, allowing a wide choice for each letter so that the result will make sense and conceal the existence of a cipher.

Part of his substitution table, for example, reads:

A	B	C	D
I salute thee	beautiful	lovely	we hasten
Mary	Pallas	Isis	Astarte
filled	glorified	devoted	enthroned
of grace	of enticement	of wisdom	of charm
the Lord	a god	desire	happiness
with thee	at thy breast	in thy arms	in thy heart
you are blest	you are admired	you are the shield	adored
of women	of the unhappy	of all wise men	of lovers
fruit	work	delicacy	treasure
is blest	is eternal	is admirable	is adorable
holy	eloquent	gorgeous	powerful

—and so on, twenty choices for each letter, and any word or phrase under the letter in the table standing for it in the resulting message. The word *bad* may thus be enciphered by "Beautiful Mary, we hasten—" or "Pallas is blest of lovers—" or "You are admired of women, Astarte," while *cac-* could be rendered "Lovely Mary, you are the shield—" or in divers other ways.

The advantages of the Trithemius system are that with the

exercise of some care the existence of any ciphered message at all can be concealed; the clear may be in one language, the message in another; and a considerable amount of material must accumulate before the letter-frequency tables will begin to operate, thanks to the numerous equivalents offered for each letter.

These characteristics have made it a great favorite with theorists and an occasional fiction writer who do not have to cope with the serious practical difficulties that it makes every message ten or fifteen times as long as the clear and that the users must carry around a cipher table as extensive as a small code-book. It is fairly safe to say that no Trithemius cipher has ever been used where the transmission of secret information in a hurry was a consideration; and time is nearly always a consideration, for there are better ways of getting information through than cipher where the business can wait.

II

But if Trithemius' system is not itself of value, it has a certain historical importance as being one of the few identifiable steps in the development of the method which spread through every diplomatic office of Europe during the sixteenth century. Simonetta and di Lavinde, on that century's threshold, had already noted how much more frequently the vowels occurred than any other letters. It is true only of the Latin languages, but the two early cryptographers were dealing with no others; in their systems of decipherment they made them the point of attack, and in their systems of encipherment proposed beating the decipherers by furnishing several equivalents for each vowel. This meant in turn the use of either figures or arbitrary signs, since there were not enough letters to go around.

Trithemius followed them, offering a long list of equivalents not for the vowels alone, but for every letter of the clear, and in addition demonstrated that it was not necessary to use an alphabet at all for encipherment. From his date the history of ciphers suddenly dives into a dark passage, where all Latin

Europe is ciphering furiously away for a hundred years, while the north fumbles with the beginnings of the jargon-code. The next flash of light shows us a Europe in which Queen Elizabeth has recently died; on her throne sits the bubbling, padded "learned fool" James I, and across the Channel Henri IV of Navarre is King of France and surrounded by enemies.

The enemies were all of one house. Spain was on his southern border, and, though the imperceptible decay of her greatness had already set in, Spain was still the greatest military power of Europe, holding in addition to her home territories and the vast sources of wealth in the Americas, the Italian kingdom of Naples and duchy of Milan. Her king was Philip III, a Hapsburg, closely allied by friendship and family with the Austrian Hapsburgs who ruled Alsace, Luxembourg and Franche Comté in addition to the Belgian Netherlands. They hemmed France in on a frontier running from Calais through Amiens to Verdun, closer to Paris than the Germans were in 1914. All his life Henri had struggled to beat off this House of Hapsburg; had barely kept it from breaking up France and swallowing it piece by piece. As the century turned he could detect beneath his feet the groundswell of the onrushing Thirty Years' War—the great offensive in which Hapsburg would presently try to break the North German Protestants as both a religious and a political force before turning against France once more.

Henri had managed to knit the nations that held the Protestant religion and those that were Catholic, yet dreaded the menace of Hapsburg, into an alliance. James of England had hesitatingly promised support; the Scandinavian kings had joined enthusiastically (though no one, not even themselves, knew they held in reserve one of the greatest soldiers of history); the kingdom of Savoy had joined, and Portugal; the Venetian Republic would help. In Germany, French agents had succeeded in forming the Evangelical Union, a league of Protestant princes; in his own country Henri had built up a fine new army and his great minister, Sully, had filled a war chest with pieces of gold. In 1609 the hour seemed ripe to strike; for in that year the Duke

of Cleves-Jülich died, leaving a succession disputed between two anti-Hapsburg claimants.

Yet his territories were too important for the overmastering house to neglect; they included the cities of Cologne and Münster and formed the best, the only convenient road between Belgium and the Hapsburg hereditary lands on the Danube. Regardless of the claims of the heritors the Austrian Emperor threw an army into Cleves-Jülich and announced that he had taken the duchy over. Up to this time Henri had delayed open hostilities because he had been unable to bring one important personage into line—the Elector of Brandenburg, the greatest Protestant lord in Germany. He was one of the claimants to Cleves-Jülich; when he heard the Hapsburgs had stolen the duchy, he sent in his adhesion to the great alliance, and word went out to all its members that the hour for a reckoning with Hapsburg had come.

The cipher in which that word went forth has been preserved. It was devised by some unknown expert at Henri's court and it is a simple substitution with suppression of frequencies and inserted code signs on the following plan:

Clear	A	B	C	D	E	F	G	H	I	L
Cipher equivalents	31	26	27	28	32	29	3	33	12	14
	34	35	36	37	38	39	30	41	42	43
	37		59	60	61	62	40	64	65	66
	80				81				82	

Clear	M	N	O	P	R	S	T	U	X	Y	Z
Cipher	44	15	16	17	9	20	21	22	23	24	25
equivalents	67	18	46	47	19	50	51	52	76	54	55
	85	45	69	70	49	73	74	75		77	78
		68	83	72	84			86			87

I was used instead of J, C instead of K or Q, U instead of V. Most of the unassigned numbers stood for common words, 10 being *le*, 39 standing for *mon*. But when the numbers were written with a bar over them, they stood for names, as $\overline{49}$, The Elector of Brandenburg, and the single numbers, 2, 4, 5, 6, 7, 8, not used in the system, were applied as nulls, always at the ends of words.

III

Of course Hapsburg agents had copies of some of these messages almost as soon as they went out. Now there is a good method for breaking ciphers of this type, known as the vowel method. Suppose one of these messages, written in a cipher of the same type, but with a different key, were the following (with an English clear behind it for convenience' sake):

a 36–49–33– 2–13	b 4– 5–29–32–14	c 13–54–20–53–40
d 22– 3–69–50–25	e 48–23–65–31–28	f 43–44–52–59–16
g 39–77–10–27– 4	h 81–39–56– 8–17	i 38–69–61–18–14
j 17–47–38–68–47	k 72–62–84–82–66	l 34– 9–11–13–40
m 30–74–31–59–58	n 53–49–64– 2–68	o 75–79–50–29–69
p 77–48–76–18–72	q 32– 9–81–65–14	r 5–20– 4–89–17
s 22–43–38–52–28	t 66–57–25–46–44	u 37–40–22–61–62
v 84– 3–53–13–49	w 50–67–32–21– 7	x 5–10–27–69–79
y 31–65–34–14–59	z 82– 8–53–43–66	aa 85–52–74–29–22
bb 47–77–48–25–81	cc 69–49–17–64–44	dd 46– 2–82– 4–84
ee 40–18–32–52–49	ff 50–29–38–84–61	gg 44–32–59–35–75
hh 77–10–27– 4–29	ii 20–56–52–74–68	jj 28–62–40–84–79
kk 2–15–59–47–65	ll 55–77–58–89– 9	mm 18–32–52–85–13

nn	oo	pp
4–43– 5–84–40	16–39–59–46–10	77–48–75–56–69
qq —	rr	ss
61–38–14–17–63	34–25–27–46–69	74–26– 4–17–41
tt	uu	vv
44–40–10–76–62	81– 8–67–59–31	32–66–82–89–17
— ww	xx	yy
63– 5–84–33–29	2–57–27–77–14	49– 9–47–50–15
zz	ab —	ac
4–34–25–53–79	65–54–69–17–38	52–18–32–84–70
ad	ae	
13–38–48–75–40	52–89	

The preliminary examination which should take place even before a count on the characters is made marks the barred numbers as special word-signs, probably titles. They do not fall in the right places to be stops, with one each in groups i and j, which would make too short a sentence, and a long gap between the barred number in group s and that in qq, which would give too long a sentence. Moreover each of these barred numbers is preceded by 17, which marks that character also as a word-sign, with a strong probability in favor of *the*.

Having gathered so much from the preliminary observation, the cryptographer now takes that inevitable first step of making a count of the characters. The result:

1 – 0	16 – 2	31 – 4	46 – 4	61 – 4	76 – 2
2 – 5	17 – 8	32 – 8	47 – 4	62 – 4	77 – 7
3 – 2	18 – 5	33 – 2	48 – 5	63 – –	78 – –
4 – 8	19 – –	34 – 4	49 – 6	64 – 2	79 – 4
5 – 5	20 – 3	35 – 1	50 – 5	65 – 5	80 – –
6 – –	21 – 1	36 – 1	51 – –	66 – 4	81 – 4
7 – 1	22 – 3	37 – 1	52 – 8	67 – 2	82 – 4
8 – 3	23 – 1	38 – 5	53 – 5	68 – 3	83 – –
9 – 4	24 – –	39 – 3	54 – 2	69 – 8	84 – 8
10 – 5	25 – 5	40 – 8	55 – 1	70 – 1	85 – 2
11 – 1	26 – 1	41 – 1	56 – 3	71 – –	86 – –
12 – –	27 – 5	42 – –	57 – 2	72 – 2	87 – –
13 – 6	28 – 3	43 – 4	58 – 2	73 – –	88 – –
14 – 6	29 – 6	44 – 5	59 – 7	74 – 4	89 – 4
15 – 2	30 – 1	45 – –	60 – –	75 – 4	90 – –

271 characters all told, plus the 6 barred characters already eliminated from the count. None shows a frequency higher than 8. Obviously the application of the ordinary frequency tables for letters will yield nothing since the frequencies have been suppressed by using several representations for each letter.

The next step in the solution then, is the discovery of what characters represent the same letter. This can be accomplished by comparing sequences of characters that show similarities. In this connection two remarkable groups at once strike the eye—the sequences located in groups f—h and gg—ii. Line them up:

f g h
59-16/39-77-10-27-4/81-39-56

gg hh ii
59-35-75/77-10-27-4-29/20-56

Each group comprises ten characters, and in this group of ten characters there are no less than six exact correspondences. So many similarities can hardly result from anything but the encipherment of identical words or phrases. Therefore:

$$16 = 35;\ 39 = 75;\ 29 = 81;\ 20 = 39$$

Or making things equal to the same thing equal to each other:

$$20 = 39 = 75$$

In groups i and pp-qq there is another shorter set of similarities:

i
69-61-18-14

pp qq
69/61-38-14

which similarly yields:

$$18 = 38$$

and groups mm and ac, though the deduction is more tenuous here and contains the possibility of error, as the correspondences are not quite so complete:

mm
18-32-52-85-13

ac ad
18-32-84-70/13

$$52 = 84;\ 70 = 85$$

When the numbers which equal each other are paired together, or substituted for each other, the two long sequences which were the original point of attack appear as:

$$59\text{–}\frac{16}{35}\text{–}\frac{20}{75}\text{–}39\text{–}77\text{–}10\text{–}27\text{–}4\text{–}\frac{29}{81}\text{–}\frac{20}{75}\text{–}39\text{–}56$$

and when this is done there is another long sequence, of exactly the same number of characters, showing striking points of similarity, *viz*:

$$\begin{matrix} \text{nn} & & \text{oo} & & & & \text{pp} \\ 40/16\text{–}39\text{–}59\text{–}46\text{–}10/77\text{–}48\text{–}75\text{–}56 \end{matrix}$$

The correspondence is not as exact as before, but the whole science of cryptography is one of hypothesis, and we may attempt the hypothesis that:

$$40 = 59;\ 59 = 77;\ 10 = 27;\ 27 = 46;\ 4 = 77$$

or again combining:

$$4 = 40 = 59 = 77;\ 10 = 27 = 46;\ 29 = 48 = 81$$

On glancing back at the character-count for the message it appears that the 4–40–59–77 combination furnishes all told 30 characters out of the 271. The table of letter frequencies for English shows that E occurs 131.05 times in 1000 letters, which would be about 33 for the 271 in the message. No other letter approaches this frequency, and in a message of 271 characters the percentages among the more frequent letters work out fairly accurate, so this combination must represent the *E* of the message.

But efforts at discovering other correspondences break down into doubtful identifications, and the remaining sets of co-equivalent characters give only:

equations	total appearances in message	possibilities by frequency table
20–39–75	10	*S, H, D, L, F*
29–48–81	15	*N, I, S, H, D*
10–27–46	14	*I, S, H, D, L*

The combinations 16–35, 52–84 and 70–85 are probably incom-

pletely identified, and the others (in view of the four values for *E*) possibly incomplete. In other words, the straight frequency method has become, in this case, one of many trials and errors. The vowel method of solution therefore seems indicated.

A new frequency count is accordingly taken on the message, showing the total appearances of each character that either precedes or follows *E* at any time, and the number of times it associates with that letter. Characters, themselves rare, that only meet *E* once are omitted as possible accidentals:

Character	Total appearances	Preceding *E*	Following *E*
5	5	–	1
10–27–46	14	4	4
13	6	3	–
14	6	1	1
15	2	2	–
16–35	3	–	3
18 = 38	10	–	1
20–39–75	10	4	–
22	3	–	2
31	4	1	1
29–48–81	15	–	5
32	8	1	–
43	4	–	1
44	5	1	–
47	4	1	1
53	5	2	–
52–84	16	5	3
58	2	–	2
69	8	1	–

This table permits a good many deductions, the first feature to strike the eye being the behavior of the groupment 10 = 27 = 46. It shows a fairly high frequency; it associates very readily with *E*, both preceding and following that letter on a number of occasions, and in the message it is very frequent as a doubled letter.

The table of bigram frequencies shows that no vowel would behave like this. O, the only vowel which occurs as a doubled letter, does not combine readily with E, neither preceding nor

following it very often. Of the consonants H frequently precedes E but seldom follows, and H does not double at all; M frequently precedes E and doubles readily, but seldom follows E; N both precedes and follows E with high frequency, but seldom occurs as a doubled letter, and the same is true for both R and S. L and T meet all three conditions, and we may therefore adopt the hypothesis that $10 = 27 = 46 = L$ or T, with an outside possibility for R or S.

The behavior of the 16–35 combination is equally arresting. It shows a very low frequency, only 3 times in the message, and every time following E. Only one letter in the alphabet combines very low frequency with such an affection for E, and that one is X. Therefore, $16 = 35 = X$.

The high-frequency combination $29 = 48 = 81$ occurs often after E in the message but never before it. This would fit N or D by the data from the frequency table, with the possibilities in favor of the former; while the $20 = 39 = 75$ group might well be H on the strength of its frequency and the way it precedes E. But there is an element of doubt here. Most of the HE combinations in the language come about as the result of the word THE and the sign 17 had already been identified as standing for this word. $20 = 39 = 75$ might therefore be a medium-frequency letter that often precedes E, say M or V.

Meanwhile the high-frequency combination $18 = 38$ (10 appearances for only two characters) is almost certainly a vowel, for only once in the message does it occur with E. O or A would meet these requirements. Similarly $52 = 84$ can be either S or N (same reasoning as above—frequent association with E, but more often preceding than following), and 44, which five times occurs before $52 = 84$, must be a vowel, with I or O probabilities since E is already located. With these provisional identifications made it is time to repeat the message with the possible solutions:

a	b	c
36–49–33– 2–13	4– 5–29–32–14	13–54–20–53–40
. . . . .	E . D . .	. . M . E
	N	V
		H

d

22– 3–69–50–2 5
. . . . .

e

48–23–65–31–28
N . . . .
D

f

43–44–52–59–16
. I S E X
O N

g

39–77–10–27– 4
M E L L E
V T T
H

h

81–39–56– 8–17
N M . . the
D H
V

i

38–69–61–18–14
? . . A .
O

j

17–47–38–68–47
the ? A . .
O

k

72–62–84–82–66
. . S . .
N

l

34– 9–11–13–40
. . . . E

m

30–74–31–59–58
. . . E .

n

53–49–64– 2–68
. . . . .

o

75–79–50–29–69
H . . N .
M D
V

p

77–48–76–18–72
E N . A .
D O

q

32– 9–81–65–14
. . N . .
D

r

5–20– 4–89–17
. H E . the
M
V

s

22–43–38–52–28
? . A S .
O N

t

66–57–25–46–44
. . . L O
T I

u

37–40–22–61–62
. E . . .

v

84– 3–53–13–49
S . . . .
N

w

50–67–32–21– 7
. . . . .

x

5–10–27–69–79
. L L . .
T T

y

31–65–34–14–59
. . . . E

z

82– 8–53–43–66
. . . . .

aa

85–52–74–29–22
. S . N .
N D

bb

47–77–48–25–81
. E N . N
D D

cc

69–49–17–64–44
. . the . O
I

dd

46– 2–82– 4–84
L . . E S
T N

cc
40–18–32–52–49
E A . S .
O N

ff
50–29–38–84–61
. N A S .
D O N

gg
44–32–59–35–75
O . E X H
I M
V

hh
77–10–27– 4–29
E L L E N
T T D

ii
20–56–52–74–68
M . S . .
V N
H

jj
28–62–40–84–79
. . E S .
N

kk
2–15–59–47–65
. . E . .

ll
55–77–58–89– 9
. E . . .

mm
18–32–52–85–13
A . S . .
O N

nn
4–43– 5–84–40
E . . S E
N

oo
16–39–59–46–10
X H E L L
M T T
V

pp
77–48–75–56–69
E N H . .
D M
V

qq —
61–38–14–17–63
. A . the ?
O

rr
34–25–27–46–69
. . L L .
T T

ss
74–26– 4–17–41
. . E the .

tt
44–40–10–76–62
O E L . .
I T .

uu
81– 8–67–59–31
N . . E .
D

vv
32–66–82–89–17
. . . . . the

— ww
63– 5–84–33–29
? . S . N
N D

xx
2–57–27–77–14
. . L E .
T

yy
49– 9–47–50–15
. . . . .

zz
4–34–25–53–79
E . . . .

ab —
65–54–69–17–38
. . . the ?

ac
52–18–32–84–70
S A . S .
N O N

ad
13–38–48–75–40
. A N H E
O D M
V

ae
52–89
S .
N

This compilation permits a considerable amount of deduction:

1) The attribution of *H* or *M* to the 20–39–75 group is wrong. It will not fit in the long group (f–h) which was the original point of attack. That word, as it appears when we get the values laid out, can only be *excellence* or *excellency,* and the 20–39–75 group thus represents *C*. This confirms the 10–27–46 group as *L* and the 29–48–81 group as *N*.

2) *Excellency* is much more probable than *excellence,* being a common title, not unlikely to be three times repeated in such a message. Moreover, there are already four values for *E*; if the word were *excellence* it would add a fifth, 56, which is not very probable in a cipher containing less than ninety characters all told. Therefore, 56 = *Y*.

3) But if 29–48–81 = *N*, then 52–84 = *S*, the only other possible letter to represent this combination. If 52–84 were *N* as well as 29–48–81, this would give five characters for that letter—again too many in a ninety-character cipher.

4) 5 is a vowel; it precedes double *L* in group x and stands between a name and *S* in group ww; and if 5 is a vowel, then *I* is overwhelmingly the most likely vowel. In group r occurs the sequence 5–*CE*; the table of trigrams shows the chances are three to two that this is *ICE* rather than any other combination. *IS* would fit better after the name in group ww also (making, for instance *The King is* –). Therefore 5 = *I*.

5) 43 is a consonant. It comes between a name and the $\frac{A}{OS}$ in group s. But if a consonant, almost certainly *H*, to make the word in that group *HAS*. Therefore it is highly probable 43 = *H*; 18 = 38 = *A*.

6) 64 is a consonant. It comes between *the* and $\frac{O}{I}L$ in group cc. As to what consonant it may be there is no clue at present.

7) 32 is a consonant. It follows a vowel at the end of the word preceding *excellency* in group gg. Now 43 has been provisionally identified as *H* (deduction 5); this identification makes the combination in group f, preceding the word *excellency* there, into *his* and identifies 44 as *I* instead of *O*. It seems logical that the phrase

61–*I*–32 (ff–gg) of which we have now discovered 32 as a consonant, is also the word *his*. As a result:

$$5 = 44 = I;\ 43 = 61 = H;\ 32 = 52 = 84 = S.$$

and the table of letter frequencies confirms this.

8) 41 is a consonant. In groups ss–tt it falls between *the* and *IEL*. No present clue as to which consonant.

There is now a considerable accumulation of new values, and fairish certainties in place of several hypotheses. The newly-won letters are again substituted in the message, and as a result it becomes possible to make more deductions.

1a) 89 is a null or a stop, probably the latter. It occurs at the very end of the message, following the group *ANCES*, which is a logical word termination, to which no letter could readily be added. It also occurs in group r, following another word termination and preceding a title, which is itself the likely beginning of a sentence.

2a) 14 is *T*. The trigram table shows that the chances are 29 to 20 in favor of this letter following the *NS* of group b; and in group i there is the peculiar combination, *Name* 69–*HA*–14 *the*. The word can hardly be anything but *that*. Therefore $14 = 69 = T$.

3a) 8 is a null. No letter will fit in group h, where it stands between *excellency* and *the*.

4a) 65 is *O*. In order to fill in the obvious word *notice* in groups q–r, where just before the close of a sentence stands *N*–65–*TICE*.

5a) 55 is a low-frequency consonant. It stands between *O* and *E* on the only occasion it appears in group 11.

6a) 13 is *R* and $70 = 85$, already paired, are *U*; both are required to fill in the word *assurances* in groups ac–ad, and *assure* in groups mm–nn.

7a) 49 and 50 are both *O*; in order to make *as soon as* of the combination in groups ee–ff, which lacks only these two letters, clearing up the triple equation $49 = 50 = 65 = O$.

When these substitutions are added to those that have gone before, the whole cipher begins to fall apart. $2 = A$, $54 = 70 = 85 = U$, $14 = 53 = 69 = T$, $22 = D$ are apparent to make the

phrase *are instructed* in groups a–d. $26 = 56 = Y$ and $33 = 54 = 70 = 85 = U$ are similarly necessary for the first word of the message, *you*. 3, which fills the gap between *instructed* and *to* in group d is evidently a null; and the missing letters needed for the phrase *ten days notice* in groups o–r, give $53 = 76 = D$ and $36 = 56 = 72 = Y$, which in turn permits the identification of 9 as another null.

The combination in groups y–bb reads now as *TE–82–TH–66–US–74–ND–47–EN*; clearly *ten thousand men*, and gives the further equations $29–48–81–82 = N$, $49–50–65–66 = O$, $47 = M$, and $74 = A$. 68–R is needed to make the word *army* in group j. The rest now easily fall in place:

$$23 = F \quad 31 = 68 = R \quad 28 = 47 = 64 = M \quad 25 = 62 = I$$
$$7 = 34 = W \quad 58 = D \quad 61 = 79 = H \quad 57 = B$$
$$11 = 30 = 67 = P \quad 37 = Z \quad 15 = 55 = V \quad 26 = K$$
$$21 = \textit{and}^*$$

IV

The process of solution by this method is represented here in perhaps its most difficult form, with an English clear and a relatively short message which contains few of the inadvertent repetitions so often made in practice. In a Latin language it would be fairly easy to pick out the other four vowels as soon as the count on the letters preceding and following *E* had been taken; and the usual diplomatic dispatch would be five or six times as long as this.

It was then, perfectly possible and not too difficult for his opponents to break the cipher which Henri IV used to convey his most secret instructions. The only question is—did the Hapsburg agents or their allies know how to use this method? For a long time there was no answer to this question but supposition, and, though the subsequent chain of events made it clear that Austria-Spain knew what Henri was up to, proof was lacking of the means in which the information had been obtained.

But in the twentieth century a member of the Finnish Acad-

* Full translation of this message in notes.

emy of Sciences was investigating the diplomatic position of the Papal Curia with regard to the election of King Sigismund of Poland in 1587. Among the Vatican papers bearing on the subject, he discovered a long dispatch in cipher. He solved it by a modern method far simpler than that given above, and discovered it was of exactly the same type as the Henri IV cipher. It was vastly more complicated, with a long list of special word signs and a rule that all the numbers were to be written together without breaks, which made it easy for a would-be solver to confuse one-figure and two-figure signs.

This was of course twenty-two years before Henri's cipher, but knowing how to use such an instrument does not necessarily imply that the Roman cipher experts knew also how to break it. However, among the Sigismund papers the Finnish scientist discovered a work sheet on which some sixteenth-century cryptographer had evidently been working out the solution of another cipher of the same time, using the vowel method given above. It was not the Henri IV cipher; but it was one resembling it as closely as that in the example given here, and, if Rome could break Henri's cipher, so could Austria-Spain, the great support of Rome and the Catholic cause.

The Hapsburg chancelleries, then, could and did read the king's cipher; could and did learn of the attack on them and when it was to be launched. They had good reason to fear it, for Henri of Navarre then passed for the first captain of Europe. As things were seen from Spain there was only one sure means of crippling this attack before it started, and that was to eliminate Henri, the key piece among the chessmen arrayed against them. Assassination was a normal part of Spanish political strategy, the thing they would think of first. A plot was formed for the removal of the dangerous king; the Duc d'Épernon, Henri's favorite, was brought into it, a dozen determined and skillful bravoes were sent to Paris. D'Épernon arranged that he and they should be alone with the king to do the business.

The ironic part of the story is that the arrangements proved unnecessary. As Henri rode through Paris on the morning of May 14, 1610 in a coach like a four-poster bed, an ordinary maniac

named Ravaillac, who had nothing to do with the plot jumped down from a horse block and struck the king dead with a single blow of his dagger.

V

The act of the mad assassin threw a veil over the intentions of the sane men who intended to be assassins, leaving it for contemporaries obscure whether treachery or cryptography had been responsible for the betrayal of Henri's war plans, or, indeed, whether they had been fathomed at all. It was quite a different and much more sensational plot that focused attention on the ciphers of the age and demonstrated their fatal unreliability.

During the reign of King Edward VI in England a young man named Francis Walsingham, son of a prominent London lawyer, was pursuing his studies at Oxford. He made himself prominent by his decided views in favor of the reformed religion and, when Queen Mary the Catholic came to the throne, found it expedient to make the grand tour and to complete his education in Italy. He had money enough to move in good circles, cleverness enough to conceal his political and religious views, and he found Italy fascinating. *Nihil humanum alienum* was the motto of the age; and among the subjects not alien to young Walsingham's inquiring mind was that of secret communication. He certainly brought back to England when he came a copy of an early manual on cryptography by one Alberti, as well as the Cardan grill which produced the first transposition cipher since the Spartans; for he is discovered using both.

Queen Elizabeth was on the throne at his return. He entered politics, was returned for Parliament, and there instantly attracted the notice both of Elizabeth and of her great secretary Cecil—not as a parliamentarian but as a secret agent of quite unusual powers. In 1567, only two years after he reached London his name is attached to a report on the foreign agents in the city, and a very good, clear and accurate report it is. Two years more, and the Royal Treasury is granting him certain monies to be used in setting up a watch on these foreign agents.

Walsingham's official position became that of a secretary of state, which entitled him to sit in the most secret councils of the government. He did much to enliven their proceedings, for in Spain-dominated Italy he had acquired a hearty dislike for the Dons and a conviction that England would sooner or later have to try conclusions with them. It was at one of these cabinet sessions that he appeared with the startling news of Ridolphi's plot to assassinate the Queen, and offered proofs that Philip II of Spain had known all about the plan, and had, indeed, sponsored it.

He wanted war with Spain at once, and made himself such a nuisance on the subject that Elizabeth, who was then playing friendly, sent him out of the kingdom. Officially, his post was that of ambassador to France; unofficially he was to do whatever he could to sustain the anti-Spanish party there. Whatever plans he had for this part of the mission blew up in his face at the massacre of St. Bartholomew, and Walsingham was called home to take charge of a new department of secret police.

It was exactly the right spot for him; unfortunately we know but little of the details of his activities, for one of Walsingham's first principles was not to keep archives. There are, however, certain sidelights; at one time he had fifty-three spies on the Continent, an enormous number for those days. A letter from King Philip's governor of the Netherlands complains that the news he sends home, even in secret cipher, is known in London before it reaches Madrid.

Walsingham's house in London contained an elaborate cipher department, in addition to an excellent department of forgeries and an academy in which spies and secret agents received a thorough course of training. One of them, not unknown to later fame, was Christopher Marlowe.

Among the young men who took the course in this remarkable institution of learning was one Gilbert Gifford. He came of an old Catholic family and had originally been trained as a Jesuit, but apparently lacked the moral fiber for the Church. Being caught in some shady deal or other he was laid by the heels, and while in prison wrote to Walsingham, offering to turn spy on

other Jesuits if suitably rewarded. Walsingham interviewed him personally, estimated him as one of those adventurous youths with a taste and talent for intrigue and no particular scruples, and decided to use him. After a course in the secret academy he was sent to his home, which was in a country house near that occupied by Mary Queen of Scots.

That celebrated lady was then enjoying, or failing to enjoy, her semi-captivity in England. It must be noted that she was the heir apparent to the throne of England, and according to the views of her co-religionists the rightful queen. If Elizabeth were dead there would be no one to contest her claim, and Walsingham had good reason to believe she was not above clearing the path.

It was not long before Mary, or some of her suite, learned of the existence of young Gifford, who had come back professing strong Catholic and anti-Elizabethan views. He seemed an ideal instrument; a safe person by his background, and one with no court connections, who could journey unobtrusively about the country. Within a month the Queen of Scots was using him as a messenger for carrying her secret correspondence with the people of the party who wished to place her on the throne.

Gifford was copying this correspondence as fast as he got his hands on it, and, expertly trained by Walsingham's professional forgers, replacing the seals so cleverly no one could tell they had ever been broken.

As luck would have it, two of Mary's supporters on the outside, John Ballard and Anthony Babington, chose this time to hatch a plot. Shortly before the Gifford letter line was opened they had traveled through the country, securing assurances in writing from various personages that in the event of a "vacancy of the throne" they would call out whoever they could in arms and support Mary's cause. The next thing was to get Mary's co-operation and to arrange an accommodation between her and the Spanish monarchy, which would, it was supposed, be willing to send a fleet and an army to help the cause.

Ballard, who had been in Rome for some time, and had presumably been initiated into the methods of the Papal ciphering department, succeeded in getting through to Mary the key of a

cipher, providing Babington with a duplicate. Babington handled the correspondence with the Queen of Scots; her letters, written in cipher, were to be forwarded to him, he would decipher them and send them to their destinations. It was done; but Gifford was passing copies of the correspondence to Walsingham, and Walsingham had his own experts working on the ciphers.

The first message to fall into his hands was one from Babington to Mary. Subjected to the usual sweating process in Walsingham's private Black Chamber, it proved to be a simple substitution cipher with suppression of frequencies and inserted code words, along the same lines as the Henri IV cipher. The message explained the detail of an ingenious plot for the assassination of Elizabeth, Cecil and Walsingham himself. Six young men of Elizabeth's own household were in the scheme (Babington assured Queen Mary); they would take care of the actual work of assassination, and could hardly fail. He gave their names; but he gave them in code-numbers, and the context was no clue to their identities.

The letter closed with a statement of what remained to be done. Babington already had the approval of the Spanish court, but would have to arrange things with the governor of the Netherlands, who under the Spanish system was a good deal of an independent satrap. The detail of rescuing her from her jailers would have to be attended to, and there were several questions of detail that remained to be settled, on which Babington consulted his mistress.

That letter alone was enough to condemn everybody mentioned in it, but Walsingham had had enough dealings with Elizabeth to know that no one document could stir her to action. She was naturally a temporizer, naturally a person who thought people would behave themselves if they knew they were watched. It appears that he kept knowledge of the first letter even from the Queen, guarded her more carefully, and instructed Gifford to keep on bringing copies of the correspondence.

He got what he wanted. After two or three exchanges of letters Mary definitely approved of the plot to murder Elizabeth and suggested improvements of detail in Babington's plan for carry-

ing it out. She herself could be rescued from confinement by setting fire to the stables of the place where she was being kept and making an attack under cover of the confusion, or by overpowering her guard when they were taking her for a ride.

Meanwhile Walsingham was letting the correspondence accumulate, in the hope of getting the names of the six young men. He could afford this step; the correspondence itself showed that Spanish co-operation from the Netherlands was an essential element of the scheme, and Babington was remarking that he would have to go there in person to get it. At Walsingham's suggestion there was a mix-up in the department handling passports; the plotter's journey was delayed.

He could hardly, however, have been prepared for what happened next. Babington, imagining that nothing whatever was known about his scheme, boldly came to Walsingham's own house to ask him to unravel the departmental red tape and clear his passports for a journey to the Low Countries, which he must make "for business reasons." The Secretary for Secret Service was not at home; while Babington was explaining his case to one of the assistants, a note was brought in to the latter. Babington contrived to get a glimpse of it; it was from Walsingham himself and said that a good man should be set to shadow Babington night and day.

The plotter instantly perceived that the fat was in the fire; while his host was out of the room he left without so much as waiting for his hat and cloak. Walsingham had the news before night, instantly clapped an embargo on every ship in port and started a huge man-hunt, and this step achieved what decipherment had not been able to, for the six young men of Elizabeth's suite fled for their lives. They were all caught, and, within a month, Mary Queen of Scots was on trial for her life.

At that trial, the damning evidence was furnished by the ciphered letters and the keys of some sixty ciphers found in the Scotch Queen's possession, almost the entire equipment of the Papal ciphering department of the date. Mary's partisans always claimed that the letters were forgeries cooked up by Walsingham for the purpose of getting rid of her.

It is faintly possible, though not very probable, for the one thing certain is that the incident marked the end of the simple substitution cipher with suppression of frequencies and inserted code signs. The demonstration of the ineffectiveness of this means of secret communication was now complete, and Europe turned away from it to the jargon-code; and it is difficult to believe that anything less than the death of a queen could have brought such a change.

Chapter V

BACON OR SHAKESPEARE?

I

Francis Bacon, Lord Verulam, opens his great *Advancement of Learning* by saying, "It is my intention to make the circuit of knowledge, noticing what parts lie waste and uncultivated . . . with a view to engage the energies of private and public persons in their improvement." Among the fields he visited on that circuit was cryptography, and there he made the logical observation that if one human mind could plot out the sinuosities of a system of cipher writing another could follow the path backward, knowing that there was such a path. The only truly secret system of writing, he concluded, is one that conceals the existence of a secret. He offered a tentative method of accomplishing this result by the use of two fonts of type in printing a text, any text, which should contain a secret message.

Let one font be called the *a* font and the other the *b* font. Let us assign to each letter of the alphabet a series of values made up of *a* and *b* in different combinations, as follows:

A - aaaaa	B - aaaab	C - aaaba	D - aaabb	E - aabaa
F - aabab	G - aabba	H - aabbb	I-J - abaaa	K - abaab
L - ababa	M - ababb	N - abbaa	O - abbab	P - abbba
Q - abbbb	R - baaaa	S - baaab	T - baaba	U - V - baabb
W - babaa	X - babab	Y - babba	Z - babbb	

Every time a letter of the *a* font is used, no matter what the letter is, *a* will be indicated to a person who knows the secret of the cipher; and similarly, whenever a letter of the *b* font is used, he will read *b* of the cipher alphabet. Suppose that font *a* is a roman, font *b* an Italic font; Come here would be read by someone familiar with the Bacon biliteral cipher as *abababab*. Suppose, now with this arrangement of an *a* roman font and a *b* italic font,

the clear to be conveyed is "Francis Bacon's work." Using the text of the opening lines of *King Richard III* one induces a printer to set the play in type thus, partly in roman and partly in italic:

> Now *is* the winter of *our* discon*t*ent
> Made glorio*u*s summer b*y* th*i*s sun *o*f York;
> And *all* the *cloud*s that lower'd upon our house

The ordinary citizen will take this for a rather bad job of typesetting; the initiate will divide the letters up in groups of five, count off his *a* and *b* alphabets and read the secret message.

The fundamental principle of this system, which is the arrangement of two different symbols in various combinations to compose an alphabet, was known long before Bacon's day. It is, indeed, older than civilization. Polybius tells of the armies of ancient Greece using it to communicate with one another at night, with a torch swung in one direction for the *a* sign, in the other for the *b*. The Indians have used the same basic idea to make smoke signals to one another across the mountains of the West, and today the longs and shorts of telegraphy and blinker signaling are basically *a* and *b* signs, while wigwag is the system of Polybius.

Cryptographically it is simple substitution; a cipherer without previous knowledge of the system could read any message in it in half an hour. Bacon's merit as a cryptographer was the discovery that it could be made to underlie a surface text which would conceal the fact that there was anything to conceal, producing in effect a two-step cipher, of which the first step was so obvious that one would never look for a second. It is a device which has not lost its validity even today, and was even more valid in Bacon's period, before the invention of the linotype machine. In fact, there are considerable numbers of persons who believe that the supposition set forth above with regard to the authorship of *King Richard III* is less a hypothesis than a plain statement of fact. Their efforts to prove the point have given rise to some of the most remarkable chapters in the history of secret writing.

Baconism, the theory that Lord Verulam wrote the Shake-

spearean plays, is a wine of comparatively recent vintage. The earliest suggestion that this might be the case was made in Horace Walpole's *Historic Doubts*, a series of essays in which the author also demonstrates that Julius Caesar never existed. After Walpole the matter rested on a basis of elaborate foolery until 1848 when an English writer named Joseph G. Hart took the matter seriously enough to write a book in favor of Bacon's claims to Shakespearean authorship and who with an American woman, Delia Bacon, who had the same idea, immediately founded a whole school. The evidence adduced by Hart and his followers was purely internal and literary, based on the phraseology of the plays, the knowledge displayed in them, etc. In the 1870's one of these followers wrote a magazine article declaring that the legal knowledge in the plays was such that only a lawyer could have written them.

This article fell on the attention of one Ignatius T. T. Donnelly, a Minnesota politician with an extremely active mind, but possessing also that haste to form judgments and that lack of critical sense in testing them, which are often the result of self-education conducted by immense and unsystematic reading. At the time the Baconian article reached him he was already the author of a work demonstrating that both Egyptians and Aztecs must have been the descendants of a race inhabiting the lost Atlantis, and of another in which he tried to prove that the earth had been formed by the agglomeration of a large number of comets. The argument as to the legal knowledge displayed in the plays struck him as conclusive, but he was not impressed by the other evidences of Baconian authorship.

He had, however, read Bacon's *Advancement of Learning* and remembered something having been said about cipher in that work; and he supposed that Sir Francis, as lord chancellor of England would certainly have a good knowledge of cryptography. It struck Donnelly, therefore, as reasonable that if the Chancellor had written the Shakespearean plays he would have left within them some traces of his authorship, presumably in cipher. Donnelly set out to find such evidence, beginning by checking the

relatively rare occurrences of the word "bacon" within the plays themselves.

The scene in *Merry Wives of Windsor* where the boy William repeats his Latin lesson (Act IV, Scene ii) contains this word. Donnelly was impressed by its appearance in this particular place for two reasons—contemporary evidence clearly showed that this scene had not been in the original acting version of the drama, and the boy's name was *William*. Donnelly therefore reasoned that the scene was an interpolation into the printed version, placed there by the true author to carry a secret message, and that the message was concerned with the interrelation of Bacon and William (Shakespeare). The same scene also contains several repetitions of the word "play" and much mention of numbers; therefore the cipher concerned the plays and was built up of numbers.

Donnelly counted off the number of words in the scene in question, reckoned the number of words from the beginning to the appearance of each of the key-words and the number between each. No simple numerical relation among these sets of figures appeared, but by a complex system of factoring he managed to bring them into association.

Certain now that he was on the verge of the most sensational discovery in literary history the politician-author hunted out a copy of the famous First Folio of Shakespeare's complete plays, published in 1623. He discovered that the numbering of the pages in this volume was very irregular, some page numbers being repeated, some omitted, some pages not numbered at all. What more reasonable (since the cipher appeared to be mathematical) than to suppose this curious pagination was the result of design rather than accident and that it had something to do with the Bacon-William-play-number cipher? Adopting this as a hypothesis Donnelly began counting and factoring all through the volume, noting down every relation in numbers he established among words that might be part of the enciphered text.

He began to find repetitions of certain of these mathematical relations, and in two years of labor gradually worked out a complete system of decipherment. It turned on five "basic

numbers"—505, 506, 513, 516, 523—which were used in counting from one word of the cipher to the next. But these basic numbers had to be modified by one or more of a series of facts. The number of the page was one of these factors; so were the number of words from the top of the page to its first subdivision (as determined by the number of the page subtracted from the total number of words on the page); the number of words in the second subdivision; the number of words from the twenty-seventh word on the page to the bottom of the page—and many others. In each case the factor-number had first to be chosen from among several factor-numbers, then added to, subtracted from or divided into the basic number according to a system which itself fluctuated, and the word at the end of the resulting count taken as the word of the cipher. But this often yielded gibberish which could only be made to come out right sometimes by counting hyphenated words as one word, sometimes as two; sometimes including, sometimes eliminating, words enclosed in brackets.

Following these rules, Donnelly, as he had hoped and expected, extracted from the plays a text describing how Bacon had written them, but suppressed his authorship in view of the fact that he had political ambitions and certain of the dramas, particularly *King Richard II*, were interpreted by the court as highly treasonable. The text of the decipherment and a description of the method were embodied in a book called *The Great Cryptogram* and published by the author.

Unfortunately for the Baconians Donnelly was no cryptographer and his volume was instantly greeted with shouts of derision from those who were. They pointed out that his rules for solution were practically all variables, and that his solution in fact consisted of finding whatever words he wished to make up part of his "decipherment" and then finding some combination of basic numbers and factor-numbers that would yield the desired result. Given so many variables it is possible to extract almost any message from a wordage as large as Shakespeare's; and even more remarkable coincidences of numbers and text can be discovered elsewhere. The anti-Donnelly camp, for example, demonstrates that Shakespeare wrote the Forty-sixth Psalm in a much

easier fashion than he proved Bacon wrote Shakespeare. The Psalm is numbered forty-six; the forty-sixth word from the beginning is *shake*, the forty-sixth word from the end is *spear*: Q.E.D.

It is not recorded that the Hon. Donnelly was much disturbed by the explosion of his theory. At the time he was busy stumping Minnesota for the Populist ticket.

II

But a number of other Baconians were disturbed at having their hopes raised and then dashed in this fashion. One of them was a Dr. Owen, a retired professor who lived in Wisconsin. He fully agreed with Donnelly that Bacon had written the Shakespearean works and that he must have concealed the traces of his authorship in a word cipher in the works themselves. He disagreed with the Minnesotan only on the method of decipherment. Owen considered this hasty and spurious and set out to find a better and more consistent mathematical relation among the frequent recurrences in the plays of such words as *shake, spear, peer, bacon, pork, lard, William, Francis, Francisco,* since such words formed the obvious points of attack.

In due time he published a decipherment of his own, like Donnelly's except that he avoided the Minnesotan's difficulty with the critics by saying nothing at all about his method of work. This saved Dr. Owen from criticism, but only by plunging him into neglect; for without proof of method his *Sir Francis Bacon's Cipher Story* was merely another wild tale. Moreover, before it appeared, Owen's secretary had removed all interest from his book by publishing one of her own.

Her name was Mrs. Elizabeth Wells Gallup, a woman whose tremendous appetite for detail work was apparently the reason why the doctor had had her do most of the difficult and tedious word-counting that was necessary for his interpretation. But she also had some sense of logic and it seemed to her profoundly unreasonable to suppose that Bacon would have described a relatively secure and simple method of committing a secret text

to record in his *Advancement of Learning* and then have trusted his most important communication, his legacy to all future ages, to a complex verbal-mathematical cipher, whose correct interpretation could be made forever impossible by a printer who chose to drop out a word or a pair of brackets.

If there were any cipher in Shakespeare, she reasoned, it would be a Bacon biliteral cipher. She set herself to search for evidence of such a cipher in the famous First Folio of 1623 where it could be found if it were ever to be discovered at all. Two fonts of type had certainly been used in printing that volume, an italic and a roman, but there were long passages in the roman type without the interspersion of a single italic letter, and equally long passages in solid italic; nor were there any cases where italic and roman mingled in the rhythm necessary to establish a biliteral cipher. It was, therefore, inadmissible that these were the two styles of type Bacon had used.

The italic type had, however, been used throughout the volume much more frequently than modern printing practice likes and in a manner often highly irrational, words that required no special emphasis being in this type. Closer examination of the book with the aid of a magnifying glass convinced Mrs. Gallup that she could distinguish two distinct fonts of italic; and the periodicity with which one and then the other had been used were exactly what a biliteral cipher would demand.

Mrs. Gallup set to work on this basis, independently of her employer. The differences between the two fonts of type were often minute and she encountered considerable difficulty, but counting the italic letters alone she did extract from the First Folio a definite statement, or better, a series of statements, in a straight Bacon biliteral cipher.

The word "series" expresses the case, for according to Mrs. Gallup, the statements were by no means consecutive. The ciphered message in *Titus Andronicus*, which should have been a part of the thrilling narrative which broke off in the middle with the close of *Cymbeline*, the preceding play, turned out to be some stanzas in rhymed heroic couplet. The message in *King Henry IV* referred in the most unmistakable manner to Bacon's

connection with *The Jew of Malta* which had appeared over the signature of Christopher Marlowe, and in several other portions of the deciphered text there were references to various Elizabethan authors.

Mrs. Gallup soon had enough material of this kind to suggest to her that the works of these other authors might also contain ciphers. She obtained access to several of these in printings of about the same date as the First Folio Shakespeare. They were in the same curious combination of roman and italic types, with the italic in two fonts. By successive decipherments and arrangements she worked out an extraordinary series of statements which she published in a book entitled *The Biliteral Cipher of Francis Bacon.*

Briefly they summed up to this amazing story: In her youth Queen Elizabeth had been secretly married to the Earl of Leicester. The child later known as Francis Bacon was one and the earliest product of this marriage. Since he could not be avowed, he had been placed with Nicholas Bacon for upbringing. Later another child was born, to be known as the Earl of Essex. For obvious political reasons Bacon had never dared claim the inheritance that was his by right; the flighty Essex had made the attempt for himself, late in the old Queen's life, and ended on the scaffold, prosecuted by his own elder brother (Bacon) at the order of Elizabeth, an act ordered to convince Bacon that he had better claim nothing for himself. Bacon had written not only the works attributed to Shakespeare, but also those bearing the names of Burton, Ben Jonson, Peele, Greene, Marlowe and Spenser, as well as unrevealed translations of the *Iliad* and *Odyssey*, which latter were so tainted with treason that they had to be concealed in cipher in the other works. The putative authors of all this Elizabethan literature were real persons of small importance whom Bacon had hired to lend their names to the fraud.

On historical grounds the tale is highly improbable, and it is difficult to believe that Bacon wrote the works of seven of the most productive authors in human history in addition to those that are undoubtedly his, but these things in themselves do not destroy the value of the decipherment, since there is always the

answer that while Bacon told this story he might have been stretching the facts. However, study of Mrs. Gallup's work by cryptographers raised serious doubts as to her process. It is well known that type was very costly in Elizabethan times and once acquired by a printer was used and used to the destruction point, so that books were frequently printed from much muddled fonts, in which some of the letters were badly battered. They were also printed on much rougher paper than is used for the same purpose today; and the combination of these factors often brought it about that two letters from the same font showed striking variations. After Mrs. Gallup had published her book other observers tried to check her results; but they found it so difficult to distinguish between the *a* and *b* fonts of italic she had discovered that some of them declared it was frankly impossible.

One of them, an English Baconian named Mallock, who experienced no qualms about accepting her story of Bacon's life and ancestry, nevertheless wished the process cleared up to convince the doubters. He sent Mrs. Gallup a facsimile of Macbeth's letter to Lady Macbeth (Act I, Scene iii) which is entirely in italic in the First Folio, asking her to indicate under each letter whether it belonged to the *a* or *b* font, after which he proposed to have the whole passage thrown up to several magnifications to reveal the differences between the types in a manner beyond question.

Her reply was long delayed. In the meanwhile other investigators had been busy. It was pointed out that in the deciphered text, supposedly by Bacon, the pronoun *its* had been constantly used, although during Bacon's lifetime the word nowhere else appears, even when reference is made to inanimate objects. Where we should write "Gold keeps its color" an Elizabethan would always use "Gold keeps *his* color." In other words, Mrs. Gallup's decipherment of Bacon, though in many respects archaic, used words that had not come in till after the noble author's death. Nor was this the worst attack on her decipherment. The deciphered translation of the *Iliad* varied widely from Homer's version, but, in many respects and in several long passages almost

entire, it was a duplicate of Alexander Pope's translation, made nearly a century after Bacon's death.

It was after these findings had been published that Mrs. Gallup's reply to Mallock appeared. She admitted that "inspiration" was necessary to distinguish between the *a* and *b* faces of type used in the cipher, and that only by inspiration could one tell which letter belonged to each font in the Macbeth letter.

III

The Donnelly, Owen and Gallup failures only served to excite the now thoroughly aroused Baconians in their efforts to find a cipher in the plays. The next attempt was made by William Stone Booth, who published a book called *Some Acrostic Signatures of Francis Bacon* in which he discovered, running all through the plays and poems, an elaborate series of acrostics carrying the name of the Chancellor.

This theory had the advantage of good literary precedent, for the use of acrostic signatures was not even new in Elizabethan times. Some of the most delicate of Villon's ballads are acrostic; that is, when one reads the initial letter of each line downward, the name François Villon, or Villon, without the François, leaps to the eye. More recently Edgar Allan Poe had published his "Enigma" sonnet, in which the name of Sarah Anna Lewis can be discovered by reading the first letter of the first line, the second of the second, the third of the third and so to the end. His valentine poem to Frances Sargent Osgood is a more elaborate construction on the same plan; and the Harvard baccalaureate hymn of 1926 was a famous and scandalous acrostic whose hidden properties the university authorities did not discover till it had been sung in their chapel and published in the Boston press.

In cryptography acrostics are difficult—it takes more literary skill than most cipherers possess to construct a text which reads well yet contains an acrostic meaning—but not impossible. They fall into the same classification as the grille or Cardan cipher, invented as long ago as the sixteenth century by an Italian mathematician named Girolamo Cardan, who brought into the then

nascent science an entirely new principle. Cardan was evidently familiar with the frequency tables existing in his day and the manner in which they were used to break down all types of substitution ciphers. He did not believe that a substitution cipher could be devised that would be safe against this method of attack and, like Bacon, conceived that the only really safe cipher would be one that concealed the fact of its own existence.

To accomplish this result he proposed to bury the enciphered message in some text dealing with an innocuous subject—the same idea as that which underlies the Bacon biliteral. But Cardan perceived what Bacon did not—that the objection to any such system was the length of the covering text, for cases would and do arise when time and space are lacking for a long covering text. Cardan reconciled the conflicting requirements by the use of a device called a *grille* or *cardan* which would either permit the use of a long covering text, or, in an emergency, allow the message to be sent in a short form without covering text but with the order of the letters so disturbed that the message could not be read without the key.

Both sender and receiver are supplied with copies of this grille, which is a mask divided into a certain number of cells (usually 36) and provided with a central pivot. Nine of these cells are punched out and numbered. The sender writes his clear through the holes of the grille onto the paper that will be transmitted, the letters following the order of the numbers. Suppose the grille were arranged as follows, with the numbers representing the holes:

	9		1		3
8				2	
7			4		
		6	5		

Suppose the message to be sent were "Come here." The operator lays his grille over the paper and writes:

c m

e o

r e

e h

then fills up the vacant spaces with innocent letters to make the message as sent:

The c a m p,

e v e r y o n e

knows, will

never theless

be held on

the fifteenth.

This illustrates both the strength and the weakness of the system. It effectively conceals the clear, which can be read instantly by the recipient, who has only to place his own copy of the grille over the enciphered text and read off the letters in order. But it results in highly suspicious bunchings and spacings of letters, in themselves enough to let an interceptor know that this is not the innocent text it seems to be, and in addition it often makes for a highly abnormal covering text, due to the difficulty of accounting for all the letters of the clear.

Suppose that one wishes to avoid these troubles, or that the clear is so long that the resulting message, written through many replacings of the grille, would be too long for the method of transmission available, or that the text must be transmitted telegraphically or by signal, which would destroy the spacing and render a covering text impossible. Cardan then asked his operator to write the first nine letters through the holes of the grille; rotate the device on its central pivot through a quarter turn, write the next nine letters; rotate a second time for the third nine, and a third time for the fourth nine. The grille is so designed that no two of these letters will fall into the same space. Suppose the clear to be transmitted is "Please send us a reliable agent to help us." The grille is placed, the first nine letters written in order:

```
  N   P   E
E       L

S     A
    E S
```

Now the grille is rotated, and the next nine letters written, again using the 1 hole first:

```
  N L P I E
E       L A
  E
S R A A   D
    E S U
          S
```

After the next rotation, the message reads:

```
  N L P I E
E   G E L A
  E A     N
S R A A   D
  L E S U T
E   B   T S
```

and the final message:

E N L P I E
E H G E L A
O E A L P N
S R A A U D
X L E S U T
E X B S T S

with X's to fill out the final square and put the whole in convenient shape for transmission in even six-letter groups.

The result can be transmitted by many means, while attack by the normal method for substitution will fail. There has been no substitution, the frequencies are perfectly normal with the exception of the two X's, and other nulls could be used instead of these.

Cardan's grille was the earliest appearance of the transposition system of cipher in the modern world. It has not produced so numerous a progeny as the various systems of substitution, nor has it been quite so popular, chiefly because it affords less variety of method, that is, less opportunity for the introduction of those complications which delay decipherment. But it is a good alternative, and particularly where the communication is a long one, can be very difficult for a decipherer.

Of course the grille itself has long ceased to be popular; it violates one of the fundamental rules of cryptographic practice by demanding the use of special apparatus, which special apparatus itself forms a key to any ciphered message made with its use. Modern ciphering practice contemplates two methods of transposition in the main. In one, the letters of the clear are written in a regular pattern arrangement, let us say in the downward diagonals of five-letter squares, with the last square filled out with nulls. Example, with the message "Please send us a reliable agent to help us":

U S A L P
L S E S E
L I A N E
G E A R D
N E A B E

B P W T T
G C U E O
M H D S L
P N I E A
S R O L F

The message is then written down in normal groups:

USALP LSESE LIANE GEARD NEABE BPHTT GCUEO
MHDSL PNIEA SROLF

In the other method the message is written down under a key-word, the resulting columns being numbered according to the order of the key-word letters in the alphabet, and the message transcribed by reading down the columns in the order of their numbering:

W	a	s	h	i	n	g	t	o	n
10	1	8	3	4	5	2	9	7	6
P	L	E	A	S	E	S	E	N	D
U	S	A	R	E	L	I	A	B	L
E	A	G	E	N	T	T	O	H	E
L	P	U	S						

which would be transcribed for sending as:

LSAPS ITARE SSENE LTDLE NBHEA GUEAO PUEL

IV

The latter case is perhaps the better for illustrating the method of solution, which is based on fitting up bigrams and trigrams with the aid of the frequency tables. Example:

1 2 3 4 5 6
EHUOD TSTCM TIOWO AARLW OTNEE IDNMG

7 8 9 10 11 12
OLTOO WYTAE HWEOE ENMTN SKILT LAILT

13 14 15 16
AWBIY THAET LSIUT C

The compilation of a frequency table for the message (always the decipherer's first necessary step) shows that in all probability

this is a transposition cipher, since the five most frequent letters are T, E, O, A, L. A kind of anagramming process is therefore begun by bringing together two letters of the message to form some common bigram, at the same time bringing together the letters that precede and follow those of the chosen bigram to form subsidiary bigrams. If the subsidiary bigrams thus made up do not affront the probabilities of the language it is likely that portions of two or more columns of the clear have been brought into association.

Bigrams involving the high-frequency vowels are practically useless as a base of operations. They require so many trials that the process is unreasonably prolonged. Because of the high frequency of T, the TH combination, although the most frequent bigram in the language, is open to the same objection. The best working combination is a bigram made up of letters themselves relatively infrequent, but which together form a bigram of high frequency, the ideal combination being QU.

But the message before us contains no Q. The next most frequent bigrams made up of low-frequency letters are WH, PL and CK. The message is without P's; one of the two C's is at the very end and thus affords little opportunity to test subsidiary bigrams. If the other C (group 2) be brought into association with the only K, at the same time the two letters preceding and following each are placed in association to form subsidiary bigrams the result is:

S N
T S
C K
M I
T L

This is most unsatisfactory when the result is checked by the bigram table (Table VII). Only the *TS* combination shows so much as an average frequency, and three others are almost nonexistent. It is therefore fairly evident that the C and K of this message do not belong together.

There are in the message, however, three W's and five H's, out of which it seems probable that at least one set belongs together

in the clear. The question is, which set? The method of arriving at a decision is to compile a table bringing into association each W with each H successively, at the same time following the procedure adopted with the C and K—that is assembling the two letters preceding each and the three letters following. The first W is in group 3, the first H in group 1; assembling them in this fashion, we have:

I
O E
W H
O U
A O
A D

or, compiling the whole table statistically, and writing beside each of the subsidiary bigrams thus formed its frequency index-figure as given in Table VII, with the total frequency indices for each set of combinations shown at the bottom of the column:

H, group 1 with

W, group 3	W, group 4	W, 8	W, 9	W, 13
I –	R –	O –	E –	T –
O E – 3	L E – 39	O E – 3	H E –132	A E – 0
W H – –	W H – –	W H – –	W H – –	W H – –
O U – 40	O U – 40	Y U – 0	E U – 3	B U – 7
A O – 1	T O – 41	T O – 41	O O – 12	I O – 31
A D – 21	N D – 61	A D – 21	E D – 46	Y D – 1
65	181	65	193	39

H, group 9 with

W, 3	W, 4	W, 8	W, 9	W, 13
I A – 16	R A – 26	O A – 2		T A – 29
O E – 3	L E – 39	O E – 3	Cannot	A E – 0
W H – –	W H – –	W H – –	be	W H – –
O W – 8	O W – 8	Y W – 0	combined	B W – 0
A E – 0	T E – 46	T E – 46		I E – 14
A O – 1	N O – 11	A O – 1		Y O – 4
28	130	52		47

H, group 14 with

W, 3		W, 4		W, 8		W, 9		W, 13	
I Y –	0	R Y –	11	O Y –	3	E Y –	7	T Y –	8
O T –	13	L T –	7	O T –	13	H T –	7	A T –	68
W H –	–	W H –	–	W H –	–	W H –	–	W H –	–
O A –	2	O A –	2	Y A –	3	E A –	31	B A –	10
A E –	0	T E –	46	T E –	46	O E –	3	I E –	14
A T –	68	N T –	37	A T –	68	E T –	14	Y T –	0
	83		103		133		62		100

The process yields a mathematical compilation of the probabilities as to which combinations are correct. The superiority of the combination W, 9–H, 1 is marked in this respect, but the result carries with it a warning to caution. A grouping which owes its superiority to a single combination of very high frequency (HE in this case) is less likely to represent the correct solution than one in which the subsidiary bigrams strike a generally high level, such as the W, 4–H, 1 or the W, 4–H, 9 combinations here.

In some cases of this kind it is altogether possible that more than one of the combinations might represent a *WH* of the clear, but in this case the three strong possibilities are mutually exclusive. Therefore, with the other combinations eliminated the decipherer seeks to arrive at a decision among the three by taking in longer sections of the message and again totaling bigram frequencies:

W, 9 H, 1		W, 4 H, 1		W, 4 H, 9	
E –		R –		R A –	26
H E –	132	L E –	39	L E –	39
W H –	–	W H –	–	W H –	–
E U –	3	O U –	40	O W –	8
O O –	12	T O –	41	T E –	46
E D –	46	N D –	61	N O –	11
E T –	14	E T –	14	E E –	14
N S –	24	E S –	52	E E –	14
M T –	0	I T –	38	I N –	86
T C –	2	D C –	0	D M –	2
	233		285		246

This longer table is very informative. The probabilities now strongly favor W, 4–II, 1 as the correct combination; not only is its total higher than either of the others, but the bigrams show high frequencies all down the line in fairly even distribution. It also appears from the table that the columns in which the clear was written were eight letters long; for when one goes beyond the eighth letter in each of the three combinations the subsidiary bigrams become rare or impossible. But the message contains seventy-six letters all told. If some of the columns contain eight letters, there must also be some that contain nine. Leaving this feature aside for the moment, it may be considered as established that two columns have been correctly resurrected from the cryptogram:

Groups 4–6	Groups 1–2
L	E
W	H
O	U
T	O
N	D
E	T
E	S
I	T

The next step would normally be a search for other eight-letter groups which would fit conveniently on the right end of the columns already cleared, a step which can be performed with the aid of the trigram table (Table XII). In this case the use of the tables can be short-circuited; for group 8 consists of the combination WYTAE, which will supply both the clear *Y* which the *OU* combination in the two columns solved seems to demand and the *A* which will fit so exactly on ND. Taking out the eight-letter section which begins in group 7 and includes this section the result is:

O L E
W W H
Y O U
T T O
A N D
E E T
H E S
W I T

The WWH combination is questionable; there seems a strong possibility that it includes the final letters of some other grouping. The best procedure in such a case is to drop out the *W* together with the *O* that precedes it, pending further investigations and solutions.

It is now possible to try for a combination to fit on the other side of the columns. A good method for accomplishing this result is to build up a formula for the eight-letter group to be added. *LE*, the first pair of letters in the solved columns, requires to be followed either by A,E or a consonant (see Table XII), and *WH*, the second pair, by a vowel. *YOU* is a word complete; unless it be followed by an R any letter at all will fit. *TTO, AND, SET* and *HES* furnish no good clues, but *WIT* imperatively demands an H. The desired group, therefore, will consist of the following sequence—Consonant or A–vowel–?–?–?–?–?–H.

There is only one H left in the message, that in group 14, and the accompanying letters exactly meet the conditions set forth in the formula. Taking the eight-letter group of which it is the terminal the result is:

. L E T
. W H A
Y O U W
T T O B
A N D I
E E T Y
H E S T
W I T H

To extend this another formula is compiled for the next group desired. Anything at all will do after *LET*; *WHA* takes a T, *YOU W*, a vowel (since there are no examples remaining of H,

the only other good possibility); *–T TO B* a vowel, probably E; *AND I* a consonant, with the remainder doubtful. The combination in group 3 most nearly matches this formula and gives as a result:

. L E T M
. W H A T
Y O U W I
T T O B O
A N D I W
E E T Y O
H E S T A
W I T H A

Although the vowel following *B* is not E but *O* the result is so generally satisfactory as to deserve acceptance.

At this point it is perhaps worth while repeating the message, with blank spaces for the letters already taken out:

1	2	3	4	5	6	7	8
.....	...C.	.....	..R..	.....	.DNMG	OLTOO	W....

9	10	11	12	13	14	15	16
..EOE	ENMTM	SKILT	LAIL.	.....	..AET	LSIUT	C

The isolation of the C in group 2 and of the R in group 4 are obvious. They apparently belong at the bases of the columns to which they form the terminations—EHUODTST and MTIOWOAA respectively. When they are placed in that position, each of the other columns must be extended to match, and a new line appears at the base of the now nearly solved cryptogram—*EDCAR*.

The formula for the next column following is now evidently—Vowel–?–L or T–consonant–vowel–U–consonant–?–?. Only the last group in the message will fit; when it is placed, there are only three groups left in the message and it is easy to find room for them, giving the final result:

. L E T M E K N O.
W W H A T T I M E
Y O U W I L L G E
T T O B O S T O N
A N D I W I L L M
E E T Y O U A T T
H E S T A T I O N
W I T H A C L O S
E D C A R . . . .

V

This is the basic method in transposition ciphers, and probably the only one an amateur cryptographer could use with success, but it would strike a professional as rather slow and cumbrous; and there is a shorter method for ciphers which have been written by the more usual method of repeated squares in which the letters are arranged according to a given pattern, or the columns shuffled. The professional confronted with a message whose letter-count indicated transposition, would begin the decipherment by counting the total number of letters.

Suppose there are 96, a not unlikely number. He factors this figure to its least divisors: $96 = 2 \times 2 \times 2 \times 2 \times 2 \times 3$. This would allow for one square of 8×12 letters (possible); one of 4×24 (unlikely); one of 6×16 (unlikely); two of 8×6 (probable); three of 8×4 (unlikely)—and various other combinations of varying degrees of probability. The two squares of 8×6 or 6×8 being the most likely, he would now rewrite the message in this arrangement and take a count of the vowels in each resulting line and column. If the count comes out fairly even, that is, if it develops that no lines or columns show vowel proportions greatly higher or lower than the others, it is a fair indication that he has arrived at the correct arrangement.

Each column (or line) of letters is now written on a slip of paper. The slips are laid next to one another in various arrangements until words leap to the eye out of one of these combinations. If the letters fail to fall into words under such treatment, the decipherer may be fairly certain that he has not arrived at the correct arrangement of squares and can try another. He must

necessarily always bear in mind that the letters may be written down the diagonals or around a spiral. But these complications all yield with relative ease under the method of factoring to ascertain the square or squares used and the comparison of the resulting lines.

VI

The method of breaking a grille cipher in which all the letters are part of the clear, that is, one without covering text, is basically the same as that described first—i.e., the method of matching up bigrams, though the process is somewhat longer. When a covering text has been used, common sense is the best guide; the unusual bunchings of letters and the phraseology forced by the necessity of fitting certain letters into the message indicates the presence of such a cipher, and it thereupon becomes a question of reconstructing the grille which, placed over the message, will give a reading that makes sense.

William Stone Booth adopted the common-sense method in his attempt to discover Baconian signatures in Shakespeare. He found, for example, three lines in Scene iii, Act IV of *Love's Labour's Lost* which read:

> But with the motion of all elements,
> Courses as swift as thought in every power,
> And gives to every power a double power.

which to him yielded:

B . . . .
C O . . .
A N . . .

and this he read as BACON.

This is possible provided a grille, or a grille system had been used in beginning these particular lines with these letters, and the spaces of the grille had been numbered to bring the letters into the proper order. However, Booth failed to demonstrate any consistency in the placing of the letters which made up the name *BACON*. In some cases one letter began it, in some another; the order was hardly ever twice the same. His process thus became not one of ciphering but of anagramming, and it was susceptible

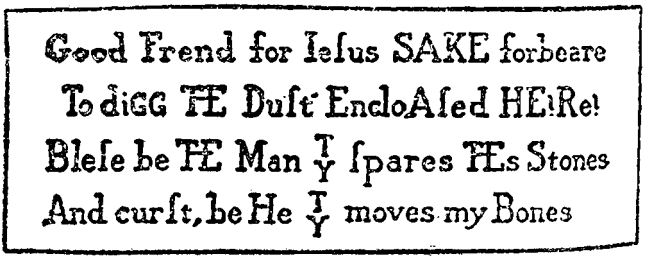
of more than one result. If the quotation from *Love's Labour's Lost* be prolonged only two lines farther, one finds:

> Above their functions and their offices.
> It adds a precious seeing to the eye:

Under the same process used by Booth for discovering *BACON* in the first three lines, the word *BAIT* can be found here. "Bacon bait" is the result; and the interpretation that Shakespeare was a fish poacher, conveying to others of his kidney in this secret manner instructions for the best method of taking fish from protected streams.

Booth's proofs therefore followed the others into limbo, but his failure did not in the least serve to close the floodgates of speculation about the existence of a cipher in the 1623 folio. The next effort came from Colonel George Fabyan of the American Army. Like Mrs. Gallup, he was impressed by the typographical irregularities of the 1623 folio and by the fact that Bacon had described a system of cipher which would produce just such a result on the printed page. Unlike her and also unlike the others, Fabyan was an able cryptographer. His point of departure, however, was not the famous folio, but the Shakespeare gravestone at Stratford.

The text on that piece of rock is now carved in even capital letters, but it is well known that the present cutting is one made in 1831 when the original stone had so decayed as to be hardly legible. Facsimiles of the older carving, presumably placed on the stone at the time of Shakespeare's death, are in existence. They show it to have been made up partly of capitals, partly of lower-case letters, partly of three letters combined into one to make up the word *the*.



Fabyan believed he could detect in this carving not merely the use of two alphabets, but of three. This is a development of the Bacon biliteral system into a triliteral, as described for the first time in print by a German writer named Frederici in 1685. The date was long after Bacon's death, but this did not form a fatal objection to Fabyan's theory, for there are many occasions in cryptographic history when a cipher has been in common use for many years before any description of it reached print. Frederici himself declared he was not the inventor of the triliteral cipher and that it was known for some time before him. It seemed reasonable to believe that if Bacon wished to leave a really secret message he might have left the description of the biliteral cipher as a clue, then put any message he wished to convey into the more complicated system growing out of it.

Unlike Mrs. Gallup in another respect Colonel Fabyan did not fear to put his proofs on public exhibition. He interpreted the gravestone thus:

Goo dFr end for Ies usS AKE for bea re aba bba aab aac aca cbc cab abb aac bc-	text divided into 3 alphabets.
F R B A C O N H A Z	Interpreted by the Frederici system

T odi GGT -ED ust Enc loA sed HER e
c aac bba acc bbc cbc cab acb aca c-
A R D S O N E C

Bl ese beT -EM Tsp are sT- EsS ton es
ca aba abb bba cca cab aac caa bbc bc-
I P H R I N A M S W

A ndc urs tbe HeY Tmo ves myB one s
c cca bab abb cca cab bac caa bba
I T H I N W M R

and read it off *Fr. Bacon hazards one ciph'r in a ms. within WMR.*

Following up the clues thus obtained, Fabyan found in the introduction of the famous First Folio a biliteral message reading, "If I sometimes place rule and directions in other ciphers you

must seeke for the others soone to aide in reading. Fr. of VE." This find was followed by others, some in the First Folio, some in a Ben Jonson text of 1616 (the date of the carving of the Shakespeare gravestone), and all pointing to the confirmation of Mrs. Gallup's remarkable theory not only of Bacon's true ancestry but his authorship of the plays as well. The difference between Fabyan and Mrs. Gallup was that the former made few positive statements, beyond that of the cipher in the gravestone, and that his labors at the War Department kept him from developing the theory as fully as earlier laborers in the vineyard.

But although it is offered by an experienced cryptographer the Fabyan decipherment is open to some serious objections. It pivots on the gravestone decipherment; and the gravestone decipherment is weak, for photography was unknown before 1831, the date of the re-carving. The three existing facsimiles taken off before that date differ among themselves as to certain details—not very gravely it is true, but enough to make it doubtful whether one of the dash H's (that in the second line) could legitimately be assigned to the *a* alphabet, while the other (in the third line) is interpreted as part of the *b* alphabet. Moreover, Fabyan's interpretation of the first word of the third line as *Blese* appears to involve a misunderstanding. Most other observers agree that there was a little mark between the S and the final E, which should be read as a T, making the word *Bleste*. If this is done, whether the T be counted as part of the *a*, *b* or *c* alphabet, all the rest of the decipherment from this point on is gibberish.

More serious still is the general criticism of all the Shakespearean decipherments to date. Bacon's description of his biliteral system clearly demands the use of two altogether different forms of type, while all the decipherments thus far offered depend upon the detection of minor variations, often perceptible only with a magnifying glass, in two fonts of type which are essentially the same. In addition the Elizabethan custom of using battered type makes any consistent biliteral decipherment practically impossible.

This may be illustrated. Suppose we have a text reading:

There is a *tide* in the affaires of *men*
Which taken *at* the . . .

When one attempts to decipher this according to the Bacon biliteral system there is no difficulty about bringing out the word *ALL* at the start. But the interpretation of what follows hinges on the letter A in "affaires." If this letter belongs to the *a* font, the letter of the clear following *ALL* is *I*; but if it belongs to the *b* font the letter is *N*.

The letter is so banged about as to make the proper interpretation uncertain. The decipherer therefore drops it and presses on to seek elucidation. Immediately he encounters the E of "affaires," a word not usually spelled with an E, even in Elizabethan times. This E, therefore, may be an interpolation, not part of the cipher at all; and like the A it is so knocked about that if it is part of the cipher it is impossible to say whether it should be counted as part of the *a* or the *b* alphabet.

If the E is not counted there are two possibilities in the short portion of the message before us, according to our reading of the A in "affaires":

ALL IS LEFT
ALL N. LEFT

If that battered E be counted as part of the *a* alphabet, there are again two choices of interpretation:

ALL NUCC-
ALL FOUR (IV) LEFT

While if it be counted as belonging to the *b* alphabet, there are two more:

ALL N. ACC-
ALL I ACC-

These varying interpretations increase in geometrical progression with the appearance of every bad letter, and the bad types in the 1623 folio average two or three to the line. It therefore seems in the highest degree unlikely that a coherent and provable

message will ever be extracted from the 1623 folio through the use of the biliteral cipher. The other techniques either devolve into anagramming, like Booth's, or into insanity, like Donnelly's. This is not to deny that Bacon wrote the plays; it is merely to say that there is no unquestionable cryptographic evidence that he did.

VII

The Bacon biliteral is not one of the great systems of cipher; it breaks down too readily when its existence becomes known. But with the systems derived from it, it will always be dangerous as a trap, or secondary cipher, concealing a meaning two steps down, as in the case of the Truth and Freedom movement.

During the 1860's and 1870's Russia was ruled by Alexander II, the "Tsar Liberator," a reasonably enlightened autocrat who freed the serfs in his backward country and pushed it gently in the direction of a more liberal social and political organization. Progress was too slow for the young intellectual radicals, many of whom had formed a colony in Switzerland where, along with their western educations, they had imbibed the heady doctrines of Karl Marx, and of Bakunin the Anarchist thinker who believed in the overthrow of all government as a first step in the desirable extinction of the human race.

These young intellectuals disseminated a great deal of propaganda in their home country and became such a nuisance to the government that all Russian citizens were ordered home from Switzerland on pain of losing their passports. Most of the radicals came, but they brought their doctrines with them and immediately set about the formation of the Truth and Freedom society, whose purpose was the overthrow of the Tsarist government in favor of a completely socialized state.

Naturally, their difficulties with the police now became acute. A good many were shipped to Siberia, a good many more thrown into prison, but their movement remained an insignificant affair of garrets until 1878. In that year a war between Russia and

Turkey ended, and, as usual under the Tsars, that end brought with it a terrific scandal about official corruption and mismanagement. The scandal might have been borne, for Russia had been gloriously victorious in the field; but at the peace conference the Russian diplomats were badly outmaneuvered and lost everything the armies had gained. The bourgeois and intellectual classes were at the moment riding the crest of an immense wave of pan-Slavism, and the treaty disgusted them with the government. They fell willing victims to the Truth and Freedom propaganda; and simultaneously the executive committee of that group, partly in despair at the slowness of results from the straight propaganda campaign, partly anxious to make the most of the moment of unrest, determined it was "desirable to diminish the number of reactionary individuals and to exterminate as many of them as possible."*

This was the beginning of the movement known as the Nihilist terror; and so unpopular was the government that when a Nihilist girl named Vera Zassulich shot down Chief of Police Trepoff at St. Petersburg, the jury acquitted her amid scenes of wild rejoicing. The event seems to have opened the eyes of the government, which met the challenge by liberalizing constitutional concessions on the one hand and increasing police vigilance on the other. The concessions were enough to satisfy the middle classes, and the evidence produced by the police of the intent of the Terrorists horrified them. By the winter of 1878-79 it was evident that the Nihilists were losing out.

Their remedy was to intensify the Terror so that the middle classes would be driven back into their arms, and there ensued something like a state of war, with all the apparatus of spies and secrecy, and the Terrorists still losing ground. There remained only one step that would create the state of national terror and repression they wished and they took that step. At an executive meeting of the Truth and Freedom group a solemn sentence of death was passed on the liberal and intelligent Tsar, Alexander II. Within six months a young man stepped up to him as he took

* See notes at rear.

his daily unaccompanied walk in the street and fired a pistol point blank. He missed. A train in which the Tsar was supposed to be traveling was blown up with the death of twenty persons and a section of the Winter Palace was dynamited with the death of thirty more.

Alexander II had not even been scratched in any of these attempts; and the efforts had the opposite effect from what the Terrorists intended. He called a committee to prepare the rough draft of a liberal written constitution and summoned to the Ministry of the Interior a brilliant officer, General Loris Melikoff, who abolished the old political police and set up a new organization whose key method was that of working by espionage from within the revolutionary organization. The Nihilists were now threatened with extinction; they would have to work fast.

Melikoff's spies managed to put into his hands two important revolutionaries, Goldenberg and Mikhailoff. Under examination Goldenberg cracked; the Truth and Freedom group was desperate, he said, but they had recently secured the adhesion of an able engineer named Kibaltchich, and Kibaltchich had invented a new form of contact bomb, which was to be used in a big coup of which he was ignorant. Goldenberg also furnished the names and addresses of two or three other figures in the Truth and Freedom group and said he believed Mikhailoff was connected with the publication of one of the two propaganda "newspapers"—leaflets which the Nihilists issued at sporadic intervals, full of information about Terrorist activities which the censorship kept out of the regular press.

The discoveries of the secret presses on which these leaflets were printed had long been a desire near to the heart of the police; now they handled Mikhailoff with extreme care. One of the warders guarding him let slip a phrase or two which made it clear to Mikhailoff that he sympathized with the Truth and Freedom movement. From another the imprisoned man secured pen and paper on the pretext of writing a letter—which, incidentally, he did write, and which proved to be perfectly innocuous. Three or four days later Mikhailoff engaged the sympathetic warder in

conversation—could he be persuaded to carry a message to the comrades on the outside? The warder allowed himself to be persuaded; Mikhailoff handed him a bulky document and before night it was on General Melikoff's desk.

It was in cipher, but one of Melikoff's first steps on coming to the Ministry of the Interior had been to send members of his police force to study in the great cryptographic laboratory of the German government, and it did not take the trained men there long to discover that the cipher was a double transposition of an intricate type, based on the repetition of a series of numbers. The clear was first written down, with lines and columns numbered:

	1	2	3	4	5	6	7
1	W	O	R	K	E	R	S
2	O	F	T	H	E	W	O
3	R	L	D	U	N	I	T
4	E	Y	O	U	H	A	V
5	E	N	O	T	H	I	N
6	G	T	O	L	O	S	E
7	B	U	T	Y	O	U	R

The columns were then shuffled according to a numerical formula, as in the ordinary transposition cipher, let us say 4371652:

	4	3	7	1	6	5	2
1	K	R	S	W	R	E	O
2	H	T	O	O	W	E	F
3	U	D	T	R	I	N	L
4	U	O	V	E	A	H	Y
5	T	O	N	E	I	H	N
6	L	O	E	G	S	O	T
7	Y	T	R	B	U	O	U

and the lines now shuffled according to the same formula:

	4	3	7	1	6	5	2
4	U	O	V	E	A	H	Y
3	U	D	T	R	I	N	L
7	Y	T	R	B	U	O	U
1	K	R	S	W	R	E	O
6	L	O	E	G	S	O	T
5	T	O	N	E	I	H	N
2	H	T	O	O	W	E	F

then the message written down in five-letter groups as it appeared:

UOVEA HYUDT RINLY TRBUO UKRSW REOLO
EGSOT TONEI HNHTO OWEFX

The procedure is one that makes considerable difficulty for the cryptographer, rendering it difficult to bring bigrams together. But it has a great weakness in the fact that the same formula is used for both transpositions, and when a large amount of material has been written in such a cipher it breaks down fairly easily, due to the fact that a periodicity in one portion of the cipher being once established, the same periodicity has only to be accepted for the other portions. In this case there was a great deal of material and Melikoff's men made short work of the decipherment. They found the manuscript to be a long harangue on the woes of the working classes in the usual Nihilist style, evidently intended for publication, since instructions as to typography were appended. As had been arranged, it was allowed to go through in order to lead the way to the secret press, and two or three others like it were permitted to follow.

The secret press was duly discovered and several important arrests made. By checking on every name written on any scrap of paper connected with the arrested persons and by turning the lodgings of these persons into police traps, Melikoff's men made a neat roundup, including several men who were evidently high in the Truth and Freedom movement. But there was an ominous note; one of these leaders turned out to be a man high in the police department itself, and among the papers of another was discovered a document revealing that a plan for the murder of the Tsar was near fruition.

In desperation the police arranged for the release and shadowing of Mikhailoff. He escaped, but not before leading them to a member of the central Nihilist executive committee, one Jeliabov, and to a place called the Kobyzev cheese factory, which turned out to be a Nihilist headquarters. At the cheese factory the police made the further and terrifying discovery that the revolutionists had mined a whole street along which the Tsar was accustomed

to drive twice a week, with the intention of blowing it, him and all the houses into the air. Jeliabov, questioned by Melikoff himself, cheerfully avowed his participation in the movement and in the plot to kill the Tsar, shouting out his defiance with the statement that it was now too late to do anything about it—the mine from the Kobyzev cheese factory was not the only preparation the Nihilists had made.

Loris Melikoff now knew too much; if he told of the mined streets he would infallibly be immediately dismissed for having allowed such a thing to happen. The most he could do was to implore the Tsar not to leave the palace till "certain investigations" had been completed. But the Tsar was both brave and obstinate; without more definite reasons for apprehension he insisted on making his usual trip through the streets next morning to review the Imperial Guard. As he drove down the street on his way thither there was a violent explosion just behind his sledge; two men of his Cossack guard were killed and several wounded. Alexander dismounted and came back to the wounded men. As he bent over one there was another flash of motion and in a still more violent explosion the Tsar Liberator was blown to bits.

The arrests of men high in the Nihilist movement were pushed with redoubled energy, and only a day or two after the assassination Melikoff's men had captured Kibaltchich, the chemical engineer who produced the bombs, with the woman who had directed the bombing and several of the bomb-throwers. Six persons were tried, condemned and executed for their parts in the plot; and it is said that between trial and execution they were mercilessly third-degreed. Something of the kind must have happened; it was only in that interval between trial and execution that the facts came out.

In their very first drive the police had caught the key-man of the whole combination—Mikhailoff, the only person in the whole Truth and Freedom group who knew all the others, and who could assign them to their parts in the plot on the Tsar's life. The Nihilists had been in something like a panic when they heard he was arrested; it looked as though the whole scheme would have to be begun over again, and they had not time to

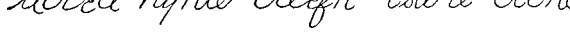
begin it over. But Mikhailoff had succeeded in smuggling through to them from prison a full set of instructions, and for nearly six months, while he was behind the bars, had directed things as smoothly as though he had been at liberty.

How had he done it? Right under the noses of the police, by means of a second cipher concealed in the enciphered texts he had sent through for publication in the propaganda sheets. He had used a variation of the Bacon biliteral,* in which the key is formed by a square of letters with numbers along the top and sides:

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	IJ	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

In writing this cipher the numbers describing a letter's position in the square are substituted for it. 14 thus represents D, and the sequence 13–34–32–15–23–15–42–15 stands for "come here."

In writing his text, already enciphered by the double transposition system noted above, Mikhailoff had indicated these numbers by breaks between the letters. Thus if the first letters of the covering message were UOVEA HYHTO, etc., and the concealed message "come here," the covering message would be written U OVE AHY HTOO WEF KR, etc. But the Nihilist leader had been cleverer than to leave such obvious breaks. He had written the covering text in neat five-letter groups, only making certain that when he wished the count to end on a given letter he lifted his pen between that and the next, and when he wished it to continue he ran the letters together. If the last letter of a five-letter group terminated on a downstroke, the group termination was also the end of a count; if on an upstroke the count was continued into the next group until a break was reached. The result would look something like this:



* See notes at rear.

In prison, waiting for execution, Kibaltchich the engineer drew plans for an airplane. Those who saw them declared later that it was so practical it would have anticipated Langley, Lilienthal and the Wrights by many years. But the police could not afford to take any more chances on concealed ciphers. They burned the plans and the instructions that accompanied them.

Chapter VI

SATELLITES OF THE ROYAL SUN

I

In the reign of King Henri III of France, whose vagaries furnished Dumas with three of his best books, there flourished at Paris a certain Blaise de Vigenère. He received the normal education of a noble of his period, did various odd jobs in the diplomatic service, found a post as secretary to the Duc de Nevers and, after that magnifico's death, went back to school, an act which was considered highly eccentric, since M. de Vigenère was then thirty-nine and the age was one when gentlemen needed to know only how to fence, dance and tell lies.

One of de Vigenère's contemporaries describes him as "delightful, grasping, intelligent and vicious." The combination is a peculiar one, but it helps explain his enthusiasm for re-education; someone seems to have told him that the study of the Kabbala would give him both the secret of the philosopher's stone and that of the kind of magic which enables a person to make others do his will. Both Greek and old Hebrew were certainly in his curriculum; and after spending four years on them and allied subjects de Vigenère was recalled to court and sent to Rome on a diplomatic mission.

While in that city he undoubtedly met and talked with some of the experts in the cryptographic department of the Papal Curia. The shop talk of the trade at the period he was in the city would have been about the remarkable new book by a doctor and mathematician from Naples, J. B. Porta, in which frequency tables more accurate than any before published were printed, and which proposed a novel method of writing a cipher which should be safe from attack by means of frequency tables. Porta's was a system of substitution, but one in which a given letter of the

clear might be enciphered with any one of eleven different letters, and in which a single letter of the cryptogram might represent any one of eleven different letters of the clear. Obviously this threw the frequency tables, as they were used for simple substitution, entirely out of joint. Opinion at Rome, however, seems to have been that the Porta system was like so many other theoretically insoluble ciphers—perfect as to design, but in operation impractical. It demanded that both sender and receiver resort to the highly dangerous expedient of carrying key-tables around with them, and under it errors of encipherment were easy to make. Though his book earned for Porta the title of "father of modern cryptography" it does not appear that his system was ever much used anywhere.

One of the reasons why it never reached general acceptance was the presence of Blaise de Vigenère in Rome at this particular date. After that gentleman had returned to Paris he distilled his studies of ciphers and those of cabalistic lore into one extraordinary volume under the title *A Treatise on Secret Writing*. As literature it was bad, and as philosophy unimportant, but it contained a description of the method of double substitution known as the "Vigenère tableau" which was the first great cryptographic invention since Julius Caesar, and the method which was ultimately to drive almost all others from the field.

It was in fact a development and refinement of Porta's system, but where Porta required a special key-table Vigenère asked only that the operator write down an arrangement of letters which he could carry in his head:

No special apparatus of any kind was necessary.

The tableau is used in connection with a key-word. The clear is written down with the key-word written over it, letter matching with letter, and the key-word being repeated as many times as necessary. In enciphering with the tableau the cryptographer now makes use of pairs of letters, one letter from the key-word with the letter of the clear that appears with it. He runs along the alphabet at the top of the tableau till he comes to the first letter of the key-word; then drops down this column till he finds the line which begins with the first letter of the clear, and writes

THE VIGENÈRE TABLEAU

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
B	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a
C	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b
D	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c
E	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d
F	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e
G	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f
H	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g
I	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h
J	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i
K	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j
L	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k
M	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l
N	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m
O	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n
P	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
Q	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p
R	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q
S	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r
T	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s
U	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t
V	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u
W	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v
X	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w
Y	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x
Z	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y

as the first letter of his message that letter which stands at the junction of the line and column thus selected. The process is repeated with each letter of clear and key-word in turn. Illustration, with the key-word "turnips," and the clear "Come here":

T u r n i p s/t
C o m e/h e r e
V I D R P T J X

The three E's of the clear, which were represented by the same letter each time in the simple-substitution system, and by a letter and two figures in the suppression-of-frequencies method (with the certainty that this letter and these figures would be many times repeated in a long message), are now enciphered by means of three totally different letters.

Reading the message, when one knows the key-word, is as simple as the process of encipherment. The recipient reconstructs the tableau; runs down the column headed by the first letter of the key-word till he encounters the first letter of the message. The letter at the left of that line is the first of the deciphered clear.

The cipher can be, and nowadays usually is, written on the reverse system of setting the key-word down beneath the clear instead of above it, and finding the column in which the first letter of the clear appears, then the line of the first letter of the key-word. The practical difference is nil.

Vigenère called his system that of "the indecipherable cipher"; and for many years it remained exactly that.

II

But the effect of his great invention on his own period and country was exactly nothing. The book in which he published it was so muddied by cabalistic lore and obscure references that it received little more attention than the bad poetry from the same pen. The cipher appears to have been given a brief trial by experts in the French diplomatic service during the next reign (that of Henri IV), but the elaborate suppression-of-frequencies systems, with their inserted code signs, were in full possession of the field, growing daily more complicated; and, as has often happened since, the experts distrusted the simplicity and ease of operation of the new scheme.

But in Germany, the home of philosophical hair-splitting, the cabalistic vagueness of Vigenère's book was not so much a defect as an invitation. The *Treatise on Secret Writing* seems to have found there an enthusiastic if limited public, the more so since the Germans then and ever since have claimed the famous tableau as an invention of the Abbot Trithemius. Such a tableau was undoubtedly published in Trithemius' book, but he calls it a "transposition tableau" and does not use it on the Vigenère system; and it was not until the Frenchman's work fell into the hands of a certain Graf Gronsfeld that the next development took place. Gronsfeld came a few decades after Vigenère; he found the

system very attractive, as other students of the matter were to find it attractive during the great cryptographic revival in the nineteenth century. But by the standards then current it was slow in operation and offered wide opportunity for operators' errors.

Gronsfeld therefore conceived that the Vigenère system might be combined with the old one attributed to Julius Caesar with the result of remedying the defects of both. Instead of a key-word, he suggested a set of key-numbers, in a series not too long for easy memory. These numbers would be written down over the clear, repeated as often as necessary, in the same manner as Vigenère's key-word. Each letter of the clear was then represented in the written message by that letter which appeared the number of places farther along in the alphabet called for by the key-number over it. Example:

1 4 0 3/1 4 0 3
C o m e/h e r e
D S M H I I R H

Two of the *E*'s are now represented by H; but on the other hand both *H* and *E* are represented by I, and the frequency tables are quite as effectively nullified as by the use of the full Vigenère tableau, while the system is easy for an inexperienced person to handle and particularly rapid. In fact, it may be described as a streamlined Vigenère; the result here is exactly what would have been obtained by enciphering with the Vigenère tableau and the key-word "bead."

These virtues gave the Gronsfeld system immediate and lasting popularity, particularly among the Protestant states of North Germany, where the influence of the complex suppression of frequency ciphers flowing from the Papal Curia had been less felt than in the Latin countries. In fact, until the development of the Gronsfeld system there seems to have been relatively little use of ciphers in Central Europe, except as they were brought in from the South and West. The babel of languages that came into that country during the Thirty Years' War also delayed the art; for a brief time the use of unknown tongues as cipher seems to have risen to the dimensions of a regular system.

Parenthetically, it is worth remarking that this device has occasionally been tried since. During the great Sepoy Mutiny, British officers made a regular practice of writing messages to one another in straight English, but with Greek characters, and, during the Boer War, where few of their opponents had any but the most elementary education Latin was found thoroughly adequate as a cipher.

The Gronsfeld cipher, then, became and long remained popular in Central Europe, particularly as a "field" cipher—that is, one that could be used by an army during a campaign. Frederick the Great used it to convey messages across the disturbed German principalities to his lieutenant, Ferdinand of Brunswick, on the French frontier. Yet it does not seem ever to have been much used for those diplomatic purposes which most severely test any system of secret writing. For it has a fatal defect; the defect that being based on key-figures and not letters, it really uses only the top ten rows of the Vigenère tableau and is open to being broken down by the simple process of repeated alphabets, which makes it a process that will delay rather than defeat cryptography.

III

Suppose the intercepted message be:

ROFGS GVFTD WVBTA IHOZ

and either from previous experience or acquired information the interceptor knows that he is dealing with a Gronsfeld type cipher. He writes the message down, with the letters of the alphabet repeated backward up the list under each to (at the utmost) the tenth, though a smaller number will usually be sufficient:

R	O	F	G	S	G	V	F	T	D	W	V	B	T	A	I	H	O	Z
Q	N	E	F	R	F	U	E	S	C	V	U	A	S	Z	H	G	N	Y
P	M	D	E	Q	E	T	D	R	B	U	T	Z	R	Y	G	F	M	X
O	L	C	D	P	D	S	C	Q	A	T	S	Y	Q	X	F	E	L	W
N	K	B	C	O	C	R	B	P	Z	S	R	X	P	W	E	D	K	V
M	J	A	B	N	B	Q	A	O	Y	R	Q	W	O	V	D	C	J	U
L	I	Z	A	M	A	P	Z	N	X	Q	P	V	N	U	C	B	I	T
K	H	Y	Z	L	Z	O	Y	M	W	P	O	U	M	T	B	A	H	S

Beginning at the first column and working on through the others, a letter is selected from each of the first three. The result is a word-beginning trigram.

In the present instance (as in nearly all in practice) the number of possible trigrams is quite restricted. The list of possible trigrams with their relative frequencies by the trigram table (Table XII) is now set down:

LID – 2	LOD – 1	MOD – 8	OLD – 22
ONE – 78	PLE – 37	PIC – 11	PID – 4
RIC – 53	RID – 3	ROD – 5	

Zero frequencies in the table are omitted. Of the trigrams here a number show frequencies so low that they can be neglected until the possibilities of the more likely combinations have been canvassed—that is, OLD, ONE, PLE and RIC.

Counting from the list of letters placed under those of the message it is possible to discover what the key-number must have been to produce each of these combinations. The result:

OLD – 332 *ONE* – 311 *PLE* – 231 *RIC* – 063

By one of those short cuts, the result of experience, which are constantly being made in the practical business of solving ciphers, it is possible to set *OLD* and *ONE* aside as unlikely to have formed part of the clear. Both show repeated numbers at or near the beginning of the formula, a procedure which is extremely dangerous in any cryptogram. Either may, of course, represent the correct formula, but it is unlikely, and as with the low-frequency trigrams, it is more convenient to set them aside till the others have failed to yield results.

The cryptographer now applies the number formulas 231 and 063 to each succeeding trigram of the message, noting the results. If either of these sequences of numbers is part of the formula by which the clear was enciphered, the message will now yield, periodically, new trigrams of high probability. When this periodicity is established it will give both the answer as to which sequence of numbers formed part of the original formula and the total

length of that formula (by the distance between periods). The result, in tabular form:

Applied to Columns:	Results from Applying Formula 231	063	Comment on Resulting Trigrams
4–5–6 (GSG)	EPF	GMD	Both trigrams impossible, particularly in association with first three letters.
5–6–7 (SGV)	QDU	SAS	231 trigram impossible; 063 trigram does not combine well with *RIC* for first three letters.
6–7–8 (GVF)	ESE	GPC	231 trigram highly probable; 063 impossible.
7–8–9 (VFT)	TCS	VZQ	Both trigrams impossible.
8–9–10 (FTD)	DQC	FNA	Both trigrams impossible.
9–10–11 (TDW)	RAV	TXT	231 probable; 063 trigram impossible.
10–11–12 (DWV)	BTU	DQS	231 possible but dubious; 063 trigram impossible.
11–12–13 (WVB)	USA	WPY	231 trigram probable; 063 trigram impossible.

The process can be carried on to the end of the message, but it has already gone far enough to demonstrate that the 063 formula must be incorrect except in the improbable event of its forming part of a key-formula more than twelve numbers long. On the other hand the 231 formula shows good probabilities at several points. Will they show periodicity? Set down the sets of three letters in the message which show good probabilities when the 231 formula is applied:

1 – 2 – 3
6 – 7 – 8
9 – 10 – 11
10 – 11 – 12 ?
11 – 12 – 13

The last three are mutually exclusive; but if a key-formula five numbers long has been used it will fit exactly with the supposition that the 1–2–3, 6–7–8 and 11–12–13 trigrams have now been correctly deciphered. If the 231 formula be now applied at

the next spot called for by such a series (16–17–18, message letters HHO), the result is the high-frequency trigram *GEN*.

With the solved portions of the message above and the unsolved columns below, the message now reads:

PLE	*ESE*	*USA*	*GEN*
G S	T D	T A	Z
F R	S C	S Z	Y
E Q	R B	R Y	X
D P	Q A	Q X	W
C O	P Z	P W	V
B N	O Y	O V	U
A M	N X	N U	T
Z L	M X	M T	S

It is now only necessary to resort to the same process as at the beginning of the solution; that of selecting a letter from each of the first two columns that will fit, deriving the formula through the letters selected, and then applying it to the other columns. The remainder of the formula works out rapidly as 60; the complete formula works out as 23160, and the message is solved with rather less material to work on than one would need for a simple substitution cipher.

Naturally, this process is not applicable to a message written with the full Vigenère tableau; there would be twenty-six letters, the whole alphabet, in each column, and the possibilities would be only limited by those of the language.

IV

With the death of King Henri IV the exterior policy of France became an interior policy. The Huguenots of the South and West, who had secured considerable privileges under Henri's Edict of Nantes, became restive under a king who was a minor in the hands of a regency unfriendly to them. It was an age when religious struggles were being transmuted into political; and the Huguenot movement quickly acquired political overtones as a drive in favor of the court party supporting the queen mother against the nobles around the young king. The latter party dis-

covered in the privileges granted by the Edict of Nantes an obstacle to that strong and centralized monarchy toward which they were working. Treating the Huguenot movement as altogether political, they marched an army into the South and broke through the interlocked privileges of the famous edict.

This was before 1618, when the Thirty Years' War broke out in Germany. The house of Austria-Spain was victorious in the first exchanges of that great struggle, and its power increased so alarmingly that Richelieu, who had now come to the fore in France, began to link up with the German Protestants, though his policy in his own country was strongly Catholic. French armies moved through the passes into Italy; but before they clashed with the Empire, they had to be recalled. The Huguenots were up in armed revolt, probably with Spanish support, certainly with Austrian approval.

There followed a confused, profitless and desperate struggle of small sieges, ambush and treachery, without battles or great events. The great nobles, already feeling the hand of the rising monarchy, fought, fled and betrayed on both sides, shifting with the tide of victory. At the height of the struggle the Prince of Condé laid siege for the crown to the rebellious stronghold of Réalmont. The place made a stout defense; the season was autumn, and if Réalmont held till spring Condé's army would be decimated by disease. The royal cause could not afford that, for Condé commanded the best and almost the last strong force in the field.

It was just at the moment when he was considering whether to raise the siege that a man was caught trying to sneak through the lines. He was recognized by someone as of the opposite party, and a search revealed in his possession a long poem, so bad that it was evidently something more important than it seemed. Various officers of Condé's army tried to unriddle its secret without the slightest success; but one of them, we shall never know who, remembered that there lived not too far away a country gentleman named Antoine Rossignol. He was a bookish man, then in his thirty-sixth year, whose studies in mathematics had led him to make a hobby of ciphers, and who had formed a library of the

leading Italian books on the subject, since there were then few others in any language.

Rossignol was summoned; he sat down with the message (which from the fact that it was in verse, the only thing we know about it, would seem to have been a Cardan grille cryptogram or one of that type) and, before the day, he furnished a rendition into clear. It was a message from the commander of Réalmont to the Huguenots of Montauban saying the town was well provisioned in everything but munitions of war, but must soon surrender if a relieving expedition did not soon appear with these essential supplies. Condé had a trumpet blown, and under a flag of truce returned the message and its clear to Réalmont. Next morning the place surrendered at discretion, and there had been brought onto the stage of history one of the greatest cryptographers who ever lived.

He came to Richelieu's attention a year later, when the great Huguenot stronghold of La Rochelle was under siege. Messages were intercepted which no one could decipher, and Condé, now with the Cardinal's army, remembered M. Rossignol. The latter broke down the La Rochelle ciphers with ease; when Richelieu returned to Paris, he took the cryptographer with him and placed him in charge of a new academy for all matters dealing with secret correspondence. From that day forward the French cryptographic department was, almost without interruption, the best in the world.

On his deathbed Louis XIII, Richelieu's king, recommended Rossignol to his queen as the man above all others in the kingdom who must be preserved, encouraged and pushed forward. Mazarin took the great cryptographer under his protection during the early years of Louis XIV, and after Mazarin left the scene Rossignol remained under the direct supervision of the king, living to the great age of eighty-three, and until the last day of his life working daily in the department he had founded.

Rossignol's great achievements were mainly in decipherment, of which we know no details, but the fact is that he made them in a fashion so marvelous to his contemporaries that the device with which a lock is opened when the key has been lost is still

called in French a *rossignol*. From what we know of the ciphers of the time it is probable that most of these decipherments were effected on Cardan grille and suppression-of-frequency ciphers, with perhaps an occasional Porta, Gronsfeld or (since some of the diplomatic business was with England) simple transposition. In his later years Rossignol evidently became convinced that none of these systems would meet the exacting requirements of diplomatic communications. They would do, and his department made them do, for the field use of minor army units where the main requirement is that the cipher shall be capable of rapid writing and reading by relatively inexperienced men. The doctrine he established—that a field cipher is acceptable if it delays decipherment of an order until the order can be executed—is still one of the basic principles of cryptography.

But even more than at present there was a demand for diplomatic ciphers, in which the first consideration is not simplicity or speed but security; and with which the use of any amount of special apparatus is permissible. Now the safest cipher yet devised in Rossignol's time was the Vigenère. The great cryptographer undoubtedly knew of it, and as evidently considered that, thanks to its regularity, it was not safe enough for diplomatic purposes. But the suppression-of-frequencies ciphers of the reign of Henri IV were only partly systematic; and the least systematic features in them, the inserted code-words, were just the features that made the greatest difficulty in decipherment.

When he was commissioned to prepare a new system of cipher for the use of French diplomats and the upper reaches of the military command, Rossignol therefore overleaped the intervening years of the Porta, Gronsfeld, Vigenère and Cardan grille, and based himself on the unsystematic cipher of Henri IV. The result was something between a cipher and a code, which was known as the Great Cipher of Louis XIV. For over two centuries it remained the only known example of a wholly indecipherable cipher, for the key became lost and every effort by cryptographers to break down the remaining examples of messages written with it ended in failure.

V

During the year 1674 the inhabitants of the fortress town of Pignerol in the French part of Italy, near Turin, observed that there was a new tenant in the castle where prisoners of the more important sort were kept. He was a tall man of erect and soldierly bearing; like the other inmates he took his exercise on the battlements of the castle under guard. The battlements were too tall for anyone to be able to see what he looked like, even if anyone had cared, which they did not.

Evidently this prisoner was a person of some importance; M. de Saint-Mars, the governor of Pignerol, served him in person. Some years later Saint-Mars was promoted to the governorship of the larger prison at the Isles Ste.-Marguerite. When he left Pignerol this prisoner, together with two or three others, went with him, under heavy guard. As the governor's train passed through Pignerol, its inhabitants noted that the prisoner of 1674, or someone who much resembled him, had his face and head entirely covered with a black mask. At the Isles Ste.-Marguerite he was installed in a cell, where a guard named De Formanoir served him.

In 1696 M. de Saint-Mars was transferred again, this time to the greatest prison of France, the Bastille, in Paris. Those who noted his arrival, and they were not many, were subsequently persuaded to remember that in the center of the armed party which formed the governor's guard of honor was a man, manacled, and with his features entirely concealed beneath a black mask.

In 1715 M. Constantine de Renneville, who had been imprisoned in the Bastille, and who had liked neither the place nor the company he found there, wrote an angry book about his experiences. In the course of the arguments by which he sought to describe the barbarity of the treatment in the prison, he remarked that he had seen and talked to a man who had been a prisoner for thirty-one years, and who, during that time, had been forced to wear a mask that covered his face and head except for the mouth.

Nobody was particularly excited about this at the time, since

it was not unusual for the government to conceal the identity and place of captivity of its prisoners as a preventive against efforts to escape. There had even been masked prisoners before, notably the son of a prominent munitions contractor, who had been caught in a series of prodigious embezzlements and forgeries. The appearance of de Renneville's book did, however, move de Formanoir, the warder of the Isles Ste.-Marguerite, to tell somebody who wrote it down, that he had served the masked prisoner; that he was a man with good features and dark hair, just turning to gray; that the prisoner went always masked when there was any likelihood he might be seen by outsiders; that his linen was of the finest quality; that he was always treated with the utmost respect by the governor; and that no one had ever told him who the man was.

There the matter rested for nearly fifty years, or until the great Voltaire, in one of his attacks on the French monarchy, retold the story. In his version the mask became one of riveted iron (no one but de Renneville mentions an iron mask during the prisoner's own time, and de Renneville's testimony is suspect). The prisoner was followed during his exercises on the battlements by at least two guards; and once, when the mysterious man scratched a name and message on a silver plate and threw it from the window of the prison at Isles Ste.-Marguerite, the illiterate peasant who found the missive was spirited away to a distant province and never heard from again. Yet this imprisoned person (said Voltaire) was evidently someone of the greatest importance, for Saint-Mars had served him humbly, and when the great Louvois, first minister of France, called on the prisoner in the Bastille he had addressed the man as "Monseigneur" and remained standing and uncovered before him till the man gave him permission to sit. Voltaire concluded with the suggestion that the prisoner might have been the Comte de Vermandois, son of Louis XIV by his first mistress, Louise de la Vallière, and that the horrible crime for which he had been sentenced to a lifetime of anonymous imprisonment was that of having once raised his hand to slap the Dauphin of France.

That was the beginning of the mystery of the man in the iron mask. In Voltaire's own time records were brought forward to prove that the Comte de Vermandois had certainly not been in prison in 1680, and had certainly died of cholera in 1683, while the man in the mask had been as certainly buried from the Bastille in 1704. Then came the French Revolution; the Bastille was destroyed with all its records, and the thing turned into one of the great mysteries of history. For the French monarchy's reply to Voltaire's story had been negative and what everyone wanted to know was: if the man in the iron mask had not been the Comte de Vermandois, who was he?

Enough midnight oil was burned over the problem during the nineteenth century to float a battleship, and enough paper spent on printed solutions to carpet a path to the moon. Every solution sooner or later ran into hopelessly unassimilable facts. Alexandre Dumas' gained perhaps the widest circulation and excited the greatest interest. The Man in the Iron Mask (he said) must have been a prince of France, either a twin brother of Louis XIV or an illegitimate son of Anne of Austria, Louis XIII's queen. Various other prominent persons of the period, about whose death there was or was supposed to be some mystery, were suggested. He could have been Mattioli, a minister of the Duke of Mantua; he could have been a prince of Savoy who had violated an agreement to open the passes into Italy for the French Army. Always theories, bolstered with appeals to historical facts, always encountering other facts which were fatal to the theories.

This was the status of the question in the early 1890's, when Commandant Gendron of the French Army undertook a military study of the campaigns of Marshal Catinat, one of the greatest of the officers who had served Louis XIV. In exploring the Marshal's correspondence, Gendron found a number of dispatches either wholly or partly in cipher and, as these appeared to be the most crucial in the whole collection, set out to solve them. The cipher was composed of groups of numbers and had every appearance of being an ordinary suppression-of-frequencies cryptogram; but despite an almost embarrassing amount of ma-

terial, it altogether failed to yield to any method of solution Gendron knew of or could devise.

Cryptography was at this time a highly advanced science in the French Army. Several of Commandant Gendron's brother officers also tried to solve the messages, and, when they failed, the matter became important enough to turn over to Commandant Bazeries of the Army Cryptographical Department, who was then recognized as one of the world's greatest experts. Bazeries was at first as contemptuous of the simple groups of numbers as Gendron had been; but his interest rose as he found the cipher failed utterly to yield to the ordinary simple methods of solution, and he now set to work on the problem from the foundation.

He began by counting the number of different figures. There were 587. This argued at the very outset that he was faced with something very unusual in the line of ciphers. Since the cipher was expressed in numbers it could not be either a double substitution or a transposition, though the possibility that a transposition or double substitution might have been superimposed on some other type to make a two-step cipher had to be kept in mind. On the other hand it was most unlikely that a suppression-of-frequencies cipher would employ such an outrageous number of signs; it would be unbearably slow and clumsy in operation. Moreover, some of the numbers were so often repeated that, if it had been a suppression-of-frequencies cipher, it must long since have yielded to the methods for that type, which he had already applied. No more could it be a code; for if 587 characters were too many for a suppression-of-frequencies cipher, they were far too few to yield the large vocabulary demanded either by the simplest word or sentence code. In fact, Bazeries reached the conclusion that the French language could not be expressed in 587 signs with many repetitions, unless these signs stood for syllables.

He must, therefore, be dealing with the Great Cipher of Louis XIV, Rossignol's masterpiece. Its character was evidently that of a semi-code, a cipher in which numbers were assigned to all

the possible syllabic combinations in a pattern painstakingly irregular.

The obvious steps in solution were to compile syllabic frequency tables for the language and to compare them with the frequencies of the numbers in the enciphered dispatches. It would not even do to search for more materials in the archives of the period, since Rossignol would certainly have used more than one key-table in enciphering dispatches with various generals and diplomats. Therefore, Bazeries confined himself to the Catinat papers. In the messages among these papers Bazeries found a total of 11,125 signs, among which the highest frequencies were:

22	with	187	appearances
124	"	185	"
42	"	184	"
341	"	145	"
125	"	127	"
24	"	124	"
145	"	122	"

His syllabic frequency table showed that the most common syllables in French were EN, ON, LES, DES; but the frequencies shown in the messages were so close together that it would be (Bazeries realized) extremely dangerous to assume that they represented these syllables in the order given without some clear indication as to which syllable was to be matched with which sign.

However, he had also prepared tables showing the cases in which certain sequences of numbers were repeated in the Catinat dispatches either wholly or in part. One sequence of four numbers was five times repeated with only one change in the series:

124 – 22 – 146 – 46
124 – 22 – 125 – 46
124 – 22 – 125 – 46
124 – 22 – 146 – 46
124 – 22 – 125 – 46

It will be noted that the two numbers showing the highest frequencies in all the messages stand at the head of each of these

sequences. Of the syllables showing extremely high frequencies in the languages there were only three pairs that could be thus assembled—*LES EN-*, *EN LES*, *DES EN*. But the five repetitions evidently represented a word or phrase of frequent occurrence. This practically ruled out the second of the three pairs, for *EN LES* already consists of two words, and the cryptographer could think of no third word, which added to these two, would yield so many repetitions.

On the other hand both *LES EN-* and *DES EN-* were promising. In either case the word beginning with *EN* could well be "ennemi" (enemy), a word extremely likely to occur in dispatches from the minister of war to a general in the field. If the complete phrase were "the enemy," then the matter was decided in favor of *LES* rather than *DES* as the value for 124; for Des owes much of its high frequency in the language to its occurrence as a part of other words, while Les nearly always stands alone. Bazeries adopted this hypothesis, and had the following equations:

$$124 = LES;\ 22 = EN;\ 125 = 146 = NE;\ 46 = MI$$

But "ennemi" when preceded by "les" takes a plural ending in French. Therefore the number next following 46 in each of the five repetitions must represent *S*, a letter which even in a syllabic cipher would have to have a separate sign for exactly the purpose of forming plurals. Bazeries went back to his dispatches; at the end of the five repetitions of his *LES ENNEMI-* stood in each case a different number—120, 345, 460, 574, 584. This did not constitute a defect in his theory; Rossignol would certainly have used several values for anything so frequently repeated as the plural ending.

Now Bazeries proceeded to insert the values he had obtained throughout the Catinat messages. In one place he found a message beginning:

52	124	22	63	46	284
.	*LES*	*EN*	.	*MI*	.

It needed no great wit to recognize 63 as another value for *NE*

and 284 as another for *S*. As the phrase stood at the beginning of a message the unknown 52 must represent *QUE* or *SI* (in either case, "if"). Farther on there was another message beginning:

52	124	22	88	374	46	284
QUE	*LES*	*EN*	.	.	*MI*	*S*

Obviously, here was a case where the second syllable of the word "ennemis" had been broken up into two letters, with a number for each, a variation introduced into an otherwise straight syllabic cipher.

In this manner, step by step, Commandant Bazeries gradually broke down the Great Cipher of Louis XIV, Rossignol's monument. In the course of the decipherment he encountered this dispatch:

Versailles

To M. the Lieutenant-General de Catinat, Commander-in-Chief of the Army of Piedmont:

I have received the letters which you were good enough to send me on the first of the month.

I suppose it is unnecessary to tell you with what displeasure His Majesty receives the news of how flatly General Bulonde disobeyed his and your orders when he took it upon himself to raise the siege of Coni. His Majesty knows better than any other person the consequences of this act, and he is also aware of how deeply our failure to take the place will prejudice our cause, a failure which must be repaired during the winter.

His Majesty desires that you immediately arrest General Bulonde and cause him to be conducted to the fortress of Pignerol, where he will be locked in a cell under guard at night, and permitted to walk on the battlements during the day with a 330 309.

As the Governor of the fortress of Pignerol is under the orders of your military department, you will kindly give directions to him for the execution of His Majesty's desires.

I remain, sir, your most humble and obedient servant.

Louvois, Minister of War.

The numbers 330 and 309 appeared just once each in the whole series of dispatches; that is, in this particular place. Bazeries

verified the fact that General Bulonde's conduct in raising the siege of Coni had in fact been disobedient and very cowardly; verified the fact that after the date of the letter General Bulonde never again commanded in the armies of France; and published to the world his considered finding that 330 represented the infrequent single-syllable word *MASQUE*, 309 a period or stop; and that therefore, General Bulonde had been the Man in the Iron Mask.

VI

Ten years later an English investigator, seeking to prove that the Man in the Iron Mask had been James de la Cloche, illegitimate son of Charles II of England, prepared his ground by clearing other theories from his path. He demonstrated that General Bulonde had been alive, at liberty and writing letters to his friends, at least two years after the death of the mysterious prisoner of Pignerol and the Bastille.

VII

The age of the cryptographic giants under Louis XIV also produced its pygmies, of whom the most tragic and ridiculous was the Chevalier de Rohan, a member of one of the greatest houses of France. He was an officer in the Army during the Dutch wars, and it seems he boasted among his friends about his ability to read secret messages without the key. While he was in charge of a detachment guarding the fortified town of Quilleboeuf on the frontier the Dutch espionage service reached him with an offer for the betrayal of the town. De Rohan was desperate for money; he agreed to sell out, conducting negotiations as to the details through his aide, La Truaumont.

Unfortunately for the treacherous de Rohan, the French counter-espionage agents were as active as their enemies. One night as the commander waited for the arrival of his aide the outer dark was shot with flame; he heard La Truaumont cry, and the next moment was himself under arrest. As he lay in the military

detention quarters friends managed to convey to him the information that there was nothing against him but what his aide might say; if the latter kept his mouth shut de Rohan had only to deny and deny. Then he was taken to Paris and the Bastille, and the next communication he had with the world came in a package of shirts on the sleeve of one of which he found a line of writing:

mg dulhxcclgu ghj yxuj lm ct ulgc alj

It meant nothing, nor could the emergency bring to his brain the knowledge of cryptography that had never existed there in spite of his boasts. Actually he had only to count the frequencies of this brief message. He would have discovered at once that c, g and l were the most frequent letters, and that of these three only g could be *E*, standing as it did at the end of the two-letter word beginning the message.

But if g were *E*, then m must be *L* to make the word *LE*, the most common in French. And if m = *L*, then l must be *I* to make *IL* ("he") out of lm; and equally h must be *S;* and j, *T* to satisfy the requirements of the three-letter word ghj—*EST*, one of the commonest trigrams in French and the only trigram which is a word beginning with a vowel.

mg	dulhxcclgu	ghj	yxuj	lm	ct	ulgc	alj
LE	*..IS...IE.*	*EST*	*...T*	*IL*	..	*.IE.*	*.IT*

He would have known that in the French language there are only two words of four letters terminating in *T*—mort (dead) and fort (strong). Either way:

mg	dulhxcclgu	ghj	yxuj	lm	ct	ulgc	alj
LE	*.RISO..IER*	*EST*	*MORT* / *FORT*	*IL*	..	*RIE.*	*.IT*

RIE– now obviously ends with *N*, giving the equation, c = *N*, with *.RISONNIER,* for the second word, and *N*. for the sixth, which would have left only two gaps easily filled in, to make the complete message:

LE PRISONNIER EST $\frac{MORT}{FORT}$*: IL N'A RIEN DIT*

"The prisoner is dead (or, strong); he has said nothing." And whether La Truaumont was in one state or the other, de Rohan's problem would have been simple; he had only to deny.

But he could not read the simple message, and when called before the court he confessed everything and threw himself upon its non-existent mercy, with the result that he lost the head that was not equal to solving a simple cipher.

Chapter VII

KINGS, THIEVES AND DIARISTS

I

English ciphering, like English efforts in the other two arts that partake of mathematics—music and chess-play—is more remarkable for oddities than for logical development or for the amount of talent displayed. Walsingham had the best cryptographic department in Europe, but he died even before his queen, and the Stuarts who followed her broke diplomatic contact with the Continent to such an extent that the old reasons for secret communication systems no longer operated with the same force.

It was not until the Civil War between Charles I and his commons that the art was needed again; and, though by this time the great Rossignol was bringing it to a new level of perfection in France, and Germany was learning the Gronsfeld system, the knowledge of and taste for cryptography seemed almost completely to have passed from English memory.

One cryptographic story and one only, has come down from that Civil War: the story of Sir John Trevanion, locked up in Colchester Castle for participating on the Cavalier side of that quarrel. He was awaiting a trial that would almost certainly lead to execution, for it was the time when Parliament was making examples of the "malignants," and the heads of Sir Charles Lucas and Sir George Lisle had only lately rolled from the block. His warder brought Trevanion a letter which had been carefully examined before being allowed to pass:

> Worthie Sir John:—Hope, that is the beste comfort of the afflicted, cannot much, I fear me, help you now. That I would saye to you, is this only: if ever I may be able to requite that I do owe you, stand not upon asking me. 'Tis not much I can do: but what I can do, bee you

verie sure I wille. I knowe that, if dethe comes, if ordinary men fear it, it frights not you, accounting it for a high honour, to have such a rewarde of your loyalty. Pray yet that you may be spared this soe bitter, cup. I fear not that you will grudge any sufferings; onlie if bie submission you can turn them away, 'tis the part of a wise man. Tell me, as if you can, to do for you any thinge that you wolde have done. The general goes back on Wednesday. Restinge your servant to command.

R. T.

Sir John read it, spent a day in meditation, and in the evening asked to be conducted to the chapel that he might make his devotions. The chapel had one door only and narrow windows high in the walls. His jailers were willing to leave him alone there, kneeling before the altar, but when he did not reappear after a considerable delay, they stepped in to see what he was doing.

No prisoner, nor any sign that one had ever been there. For the letter of consolation was in a prearranged cipher. It was on the Cardan grille principle, very well handled; but if there had been any experienced cryptographers among the Roundhead jailers they would certainly have found something curious about the phraseology, and something more curious still about the placing of those commas, particularly that between "bitter" and "cup." In time they might have arrived at reading every third letter after a punctuation mark, to discover, as Sir John had, that "Panel at east end of chapel slides."

II

John Wilkins, that remarkable scientific-minded Bishop of Chester, who demonstrated on the basis of pure logic that the moon must be a world and the earth a planet, and who turned out plans for the construction of a submarine boat, also was the author of a short manual on cryptography which shows pretty clearly the state of the art in England in his time—the seventeenth century. He describes two or three simple methods of transposition, a suppression-of-frequencies cipher of the less complicated

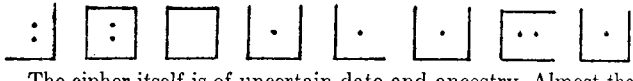
type, the Bacon biliteral system, and a method of double substitution which is that of Porta with some alterations. (He evidently did not know of Vigenère's book.) But he reserves his warmest admiration for the method of conventional signs, which he is the first writer on cryptography to mention.

The classic example of this type of cipher is that known as the "pig-pen" from the diagram on which it is based, or the "Rosicrucian cipher" from the fact that it is not infrequently encountered in books dealing with that esoteric system of thought.

The basis of this cipher is a nine-cell diagram, in which an alphabet is disposed:

ABC	DEF	GHI
JKL	MNO	PQR
STU	VWX	YZ

For each letter of the clear there is written the section of the diagram surrounding it. It will be observed that no two of these sections are alike. If the letter be the second of the three that appears within the section, the descriptive line encloses a dot; if it be the third, the line encloses two dots, and if the first the line is set down without dots. "Come here" is thus written:



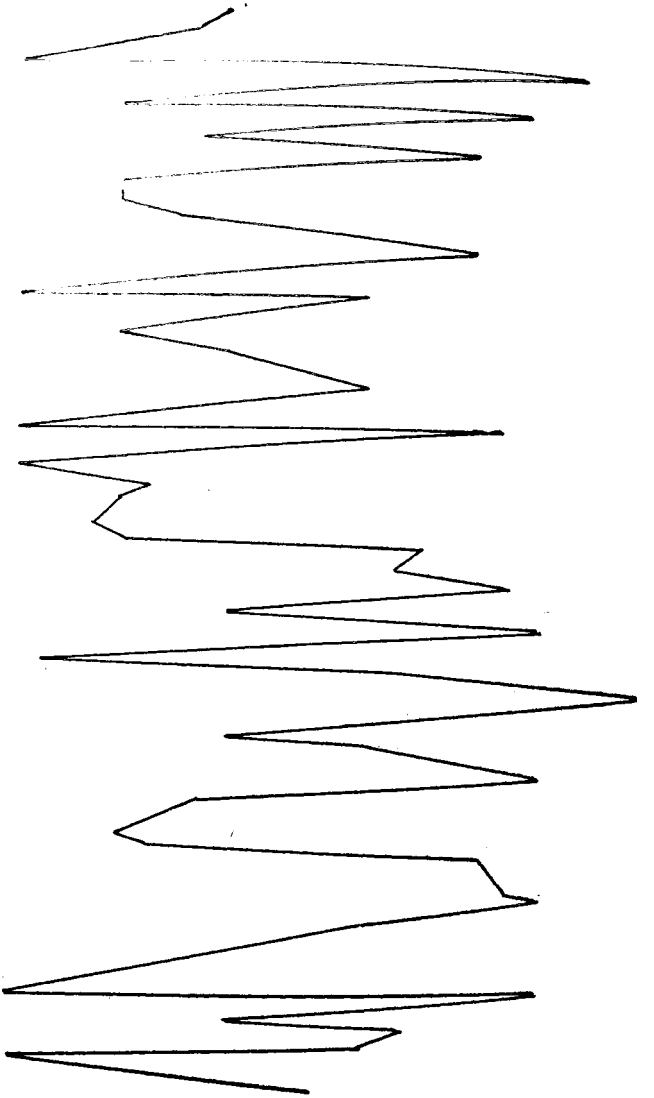
The cipher itself is of uncertain date and ancestry. Almost the only things we know about it is that it must be very old—one of the earliest stones in Trinity Churchyard, New York City, bears the inscription "Remember death" in this cipher—and that it has become very common. It was used during the American

Civil War by northern prisoners in southern prisons to communicate with friends on the outside; it is used in the "mysteries" of certain negro secret societies; and today there is hardly a schoolboy in any country who has not enjoyed the thrill of secret messages written with the pig-pen or one of its numerous variants.

Cardinal Wolsey used a conventional design cipher in corresponding with the Continental courts, interspersing the signs with passages of clear, and among the scholiasts of the Middle Ages a whole system of over thirteen hundred conventional signs was widely known. They were called the "Tyronian signs" after the personal secretary-slave of Julius Caesar, who is supposed to have invented the earliest examples of the system and used them as a form of shorthand.

The cipher of the dancing men which was used so very effectively in the Sherlock Holmes story of that name is another of the same general type, and its seems that Conan Doyle derived it from actual experience. The secret society of the Carbonari, in the days of Italy's revolt against Austrian-Spanish rule during the nineteenth century, communicated with each other by just such lines of little dancing men as Doyle used, though whether the idea was original with them remains uncertain.

Another conventional design cipher, with a background equally obscure is the zigzag, which is written by ruling a sheet of paper in vertical columns, with a letter at the head of each column. A dot is made for each letter of the message in the proper column, reading from top to bottom of the sheet. The letters at the head of the columns are then cut off, the ruling erased and the message of dots sent along to the recipient, who, knowing the width of the columns and the arrangement of the letters at the top, reconstitutes the diagram and reads what it has to say. In its most familiar form this cipher is written in a zigzag line, running from dot to dot down the page, each point or angle denoting a letter. This type of zigzag is a great favorite still with criminals, who, for some reason, appear to consider it particularly mysterious. An example:



Sometimes a zigzag appears as a series of triangles or other geometrical figures connecting the dots; and it has been reported that a German woman spy in France used the zigzag to stitch messages in samples of sewing which were transmitted across the Swiss border into Germany. The tale is more than doubtful; in World War times no espionage service with any vestige of common sense would have allowed its agents to use so obvious and easy a system.

For the conventional design cipher, no matter in what form it appears, is, like the Bacon biliteral, essentially a method of simple substitution. The sole difficulty in breaking it down consists in the identification of the characters as characters. Even when a zigzag has been used in which the order of the letters at the heads of the columns is disturbed it is a relatively simple matter for a decipherer to draw a series of vertical lines through the points, assign a number to each line, then set the numbers down in the order in which they occur, and solve the resulting number-message as a simple substitution of the common type. If this treatment fails on the zigzag given above the reader can look back to the notes and find the answer.

The cipher which is written by substituting musical notes for letters is another type of conventional design device; so much a favorite when it is necessary to refer to a cipher in fiction that it is worth mentioning. Very effective use of it was made in the movie *Dishonored*, with Marlene Dietrich as the beauteous lady spy who rolled out a few magnificent chords on the piano (she had memorized the air), then turned and wrote down the positions of the enemy units on the front, having recorded the words in a musical cipher. It is hardly likely to happen in fact, although Philip Thicknesse, an English writer, did produce a musical cipher that would work after a fashion. The difficulty is that a text, once enciphered, does not, and cannot except by the wildest feats of the imagination, be carpentered into a playable tune. As soon as a text in such a cipher falls on the attention of someone with musical knowledge, it is evident there is something wrong. Thicknesse achieved his result by allowing only the half-notes to count and filling up the rest with other types of notes to make the half-

notes into a kind of music, but this is nearly as bad, requiring that the cipher be made several times as long as the clear.

III

Yet the diagram cipher, sometimes becoming something like a pictured code, has always been and still remains the great favorite of criminals and the classes that just hover along the edges of criminality—tramps, gypsies, pitchmen, vagabonds of all kinds. Their diagrams, scrawled with chalk or pencil, sometimes even with burned sticks, on walls, fences, gates, even inside prisons, occasionally convey messages in the universal pig-pen cipher, more often turn out to be a special picture code of the underworld.

Tramp scrawlings now familiar in the United States, such as the zigzag line that signifies "This place has a mean dog," have been traced by Hans Gross, the famous German professor of criminology, all the way back to the fifteenth-century Central European bands of *Mordbrenner*. These *Mordbrenner* were loose associations, whose members wandered across the countryside, robbing lonely places, murdering everybody in them, and then burning the house to hide the traces of the other crimes. After each coup they would scatter; the members of the group would assemble with others only when they found chalked in some place one of the code-signs they used to indicate the place and date of another crime.

In time, like the jargon of the spoken criminal codes, these pictured signs became more and more elaborate, and there is now not a little literature of tramp signs. A circle with a diagonal line through it means, or once meant, "This is a good place to rob," a crudely drawn cat "Women only in this place," a crudely drawn hammer "You'll have to work for anything you get." All may be said to be much less common in the United States than they once were before the automobile became widely used to change this along with every other aspect of vagrant life, but in Europe the tradition is still strong.

Several years ago Hans Gross himself, then a junior magis-

trate, but already deeply interested in criminal communications, happened to stop in an Austrian village, near the frontier of Hungary. He noticed this crude drawing chalked on the wall of a chapel:

After examining it, he went to the local police post and told them that two or more vagabonds would be found loitering somewhere near the chapel on Christmas Day, then only a week away, and they were to be apprehended at once, as they would prove to be criminals contemplating a serious burglary.

The police set a watch as he asked and the magistrate's prediction was verified when they captured three men who were subsequently recognized as highwaymen with long police records. It was only after they had been taken that Gross consented to explain. He said:

> It is all written on the wall of the chapel. The first drawing is the crude sketch of a parrot, made in a single line. The fact that it has been made in this way means that it is the signature of a criminal, and the sketch itself indicates that he is known as "The Parrot." The drawing of a church means just that, and the key beside it signifies that the church is to be "unlocked" or robbed. The drawing below is a crude representation of an infant in swaddling clothes. I assumed that this meant Christmas Day; and the three stones are a symbol taken from a popular farmer's almanac and standing for St. Stephen,

who was stoned to death. St. Stephen's Day is December 26; therefore the meaning of the whole thing is, "The Parrot is going to burglarize a church on December 26. He wants someone to help him. Anyone who is willing meet him near here on Christmas Day, when the arrangements will be made."

And in fact the arrested men confessed that Dr. Gross had been right in every particular.

IV

Hans Gross was as much a brilliant exception in his day as Bishop Wilkins in his. The police of Europe have made little organized effort to follow up the suggestions of the former for the study of criminal scrawlings, and the diagram ciphers described by the latter do not seem to have attracted anyone in the Bishop's own time or for many years after. The next cipher to have left its traces on English history was that used by Charles II, while in exile in the Netherlands during the Commonwealth, to correspond with his partisans in England.

For a good many years this cipher was taken as an indication that English cryptographers had gone far in their art. It was an elaborate syllabic cipher, in which 70 was *ab*, 71, *ad*, 72, *ac*, and so on, while very common words had special code numbers, 407, 408, 468 and 469 all being *the king*. But we know that Charles's relations with the French court were intimate; we know that the great Rossignol was then in charge of ciphers at that court, and in view of the character of the Charles II cipher it seems a fair inference that it was one that was prepared for him at the instance of Louis XIV.

At all events the English ciphers that followed show no traces of so skillful a device as representing syllables with disordered numbers. And the next cipher in English history comes close on the heels of Charles II. The date is February of 1685, just after the death of that king. He left no legitimate children and the throne passed by order of succession to his brother James, Duke of York, hated and feared by much of England as a Papist,

respected by the rest as the legitimate sovereign. In Holland was the Duke of Monmouth, another James, bastard son of King Charles, who had been mixed up in a plot to keep his uncle from the throne, but who was merely exiled for his participation.

Monmouth was a Protestant, and it was thought by a good many persons, including himself, that he could prove his birth legitimate enough to make a try for the crown. With him in Holland was the greatest noble of Scotland, the Duke of Argyle, exiled for his part in a recent Covenanter rising. The two got their heads together, and agreed that with a few arms and ships from the Dutch they could lift the weight of a crown, Argyle to land in his own north of Scotland, Monmouth in England. But in such a game they would need hair-trigger timing, with everything ready for them when they touched shore, for the British Navy would be loyal to James, who had once been its admiral, and not so bad a one, and the Army, unless confronted by overwhelming force, would probably follow him as well.

Therefore the revolutionaries laid their scheme in deepest secrecy, arranging for ships and arms at the third remove from themselves, and so cleverly that no word of their coming leaked through. But when Argyle sent messages to his friends in Scotland, he entrusted them to a man who proved a blunderer. The fellow was laid by the heels and his papers sent down to London.

They were in cipher—a useless jumble of words. In the town a good many men knew they had come and memoirs of the day bear testimony of the feeling of tension in the city where it was being whispered that some great event was in the wind, its secret locked in those unreadable dispatches. But those dispatches were a jumble of words, not a jumble of letters; and someone in the government noticed that if he read the first word of each letter in the packet, then skipped 254 words, read two more, jumped to the 512th, he got a coherent sentence.

The cipher was, then, a word transposition. Within hardly any time at all from this discovery, the method was worked out complete. Argyle had set his message down in columns of 256 words, writing the first word in the first column, then the last in the same column, the first and last of the second column, first and

last of the third, first and last of all the columns, then back to the second and the last but one of each. The messages once straightened out were found to contain special code words for all names —Brand being Scotland, Birch for England—but these were easy, all but one, the word "Browne." Even that broke down when one of the letters was found to contain a sentence—"How can Browne employ so much money and so many horse better than for their own interest?" "Browne" was, of course, the Presbyterian congregation.

Once deciphered, the letters told that Argyle meant to land on the west coast of Scotland in early May, Monmouth following him in six days to a landing on the west coast of England, a device to set at fault the British ships watching the east. King James sent navy ships north; the militia was called out; Argyle's vassals forced to give hostages for their good conduct; all suspected persons in the district where the Duke might land thrown into prison. Argyle avoided the fleets and made his landing, but he could rouse only some two thousand miserable gillies. When he marched inland it was straight into a sack whose walls were royalist soldiers, while away behind him navy ships worked into the bay of the landing and burned his, cutting off escape. The Duke was taken without a battle; and away in the south, Monmouth, though he met more popular support, never stood a chance. Both men went under the axe, and, had King James used his victory better, he might have sat till his dying day on the throne his cryptographer preserved to him.*

V

In 1818 the diary of John Evelyn, a gentleman of the court of Charles II, after having lain in manuscript for many years, was published with great success. The applause with which it was received gave to the Hon. and Rev. George Neville, head of Magdalene College, Cambridge, the idea that a diary which had long lain in manuscript in his institution might be published with advantage. The diary in question was that of one Samuel Pepys,

*See notes at rear of volume.

a former commissioner of the Admiralty, of about the same period as Evelyn. There was only one difficulty about publishing the Pepys diary which occupied six volumes; it was written in a hand almost microscopically small and in what appeared to be some type of conventional design cipher which no one who had yet looked at it could interpret.

The Hon. and Rev. Neville took the matter up with Lord Braybrooke, hereditary visitor of the college. Lord Braybrooke agreed that the project was a worthy one, and after a little casting about, the two gentlemen discovered an amateur cryptographer among the undergraduates of the college itself, and agreed to turn the task over to him. He was a divinity student, one of those men who spends his life struggling against the anonymity of the name John Smith, and he seems to have been an even better cryptographer than his patrons imagined, perhaps one of the truly great decipherers.

His examination of the Pepys manuscript speedily convinced him that it was not written in a diagram system. The signs of which it was composed were not set down sharply and with decision; they were often vague, seemed to have been written in haste. It often took some care to determine which of two different signs was intended. This is not permissible in cryptography, where one of the first requirements is that no meaning but the one the encipherer wishes to convey shall be obtained. On this was piled another impossibility; no system of lines ruled across the page in any direction would bring the points, angles and curves into definite relation.

Therefore, Smith reasoned, the manuscript was not in cipher at all. But what was it? Apparently shorthand, though the signs in the diary bore no resemblance to any system of shorthand he knew. He therefore dug back into the history of shorthand and into that of Magdalene College, Cambridge, and among the documents of the early years of Charles II's reign discovered a poem by a fellow of the college celebrating in elegant but undistinguished lines the virtues of Mr. Shelton's new system of "Tachygraphy" which had just been approved by the university authorities.

There was a manual of this system in the university library, and Smith got it out to compare with the Pepys manuscript. There was certainly a resemblance, and whole passages yielded neatly when translated by Shelton shorthand, but Smith's difficulties were only beginning. The Shelton was one of the types of shorthand known as ABC shorthands, in which there is a sign not for every sound, but for every letter. In Shelton's system the lines and curves were reserved for consonants; vowels were indicated by dots, the position of the dot determining which vowel was meant. But either in a hurry or to make the diary more secure Pepys had almost always omitted his vowel dots. This brought it about that such sets of words as "pauper," "paper" and "pepper"; "left," "lift" and "loft"; "minister," "ministry" and "monastery" were written exactly alike, and thanks to the smallness of the N sign, the last might even be "mister," "master" or "mastery."

A still worse feature was the large number of arbitrary signs. Shelton's system contained a number of these, such as using the figure 4 for "heart," 5 for "because" and 6 for "us"; but as the solution of the diary progressed, it became more and more clear that this by no means satisfied Pepys, who had introduced a considerable number of arbitraries of his own invention, which could be solved only by the context.

And when all these difficulties were met and overcome, Smith encountered the fact that the diary, which had been running along very well for a distance, would suddenly turn into the most complete gibberish. Examination of the context drove Smith to the conclusion that these passages were with regard to matters which Pepys considered dangerous either to his political or domestic peace and that he must have enciphered them before putting them into shorthand. It was therefore necessary to transcribe these passages from shorthand to letters and then solve them as a cipher, no easy task, given Pepys' constant vagueness with regard to vowels. And still some of the solved passages continued to be gibberish. It was not for some time that Smith discovered that the tortuous mind of the naval secretary, not content with putting these passages in cipher and shorthand, had

first put some of them into foreign languages, spelled phonetically, then enciphered and finally written the result in shorthand.

John Smith worked over that manuscript for three years, twelve or fourteen hours a day. It was probably worth the labor, for Pepys' diary turned out to be one of the finest books ever written, though Lord Braybrooke appears to have considered portions of it too indecent for publication and they were withheld until the seventh edition, many years later. It is not recorded that John Smith had any particular objections to this; but he must have felt rather odd when, during one of his official visits to Magdalene some time after the Pepys' cipher had been so painfully worked out, Lord Braybrooke dragged forth another manuscript by Pepys. It was a history of the wanderings of King Charles II, fairly written out in longhand; and filed with it was a copy of the same thing in Pepys' shorthand, encipherments, special signs, foreign words and all the rest, constituting a complete key to the diary on which so much work had been spent.

Chapter VIII

FAILURE

I

The death of the illustrious Rossignol plunges us forthwith into the longest and one of the most puzzling gaps in the history of cryptography. It is true that by the time of Louis XIV the Papacy was already losing its importance as a factor in international diplomacy. In France and England the age of the jargon-codes was just dawning, and Central Europe had not yet taken up secret writing. Yet it remains inexplicably curious that, after developing energetically ever since the Renaissance, the art should not alone come to a sudden halt, but also recoil upon its own childhood. Even the great French cryptographic laboratory supplies not a single prominent name to the history of ciphers between the last years of Louis XIV and the last years of Napoleon, and the literature of the subject suddenly died out. For a hundred years from Rossignol's death the official records contain few ciphered dispatches, and those that are discoverable are written in bastard versions of the Rossignol system, so debased as to be no more difficult than the Henri IV ciphers which Rossignol took as his point of departure.

No doubt this was partly due to the fact that with the age of Louis XIV there had already begun the modern process of the retirement of the heads of government alike from the battlefield and the council table. The generals and diplomats of the eighteenth century were commonly given preliminary instructions and "full powers," then sent forth, as much on their own devices as though they had been pitched into the middle of the Antarctic continent. Events on the fronts where they made contact with one another moved too fast for them to keep contact with home

by any existing means of communication. The same slowness of communications cut to the vanishing point the type of espionage which depends upon resident spies who send secret messages home.

The disturbances of the American Revolution, with their entail of doubtful loyalties and unsafe communications in the colonies, did give rise to some ciphering, but cryptographically speaking, it was of a distinctly inferior order. Arthur Lee and James Madison seem to have been the only true enthusiasts. The latter used a variation on the Vigenère tableau which was, in effect, a kind of feeble Gronsfeld cipher. "The key," he writes to Edmund Randolph, with whom he is conducting this secret correspondence, "will be the name of a certain black servant boy who used to wait on Mr. James Madison." That name appears to have been "Cupid"; it was written at the head of five columns of letters with an alphabet in succession beneath each letter and a set of numbers paralleling the lines:

1	C	U	P	I	D
2	D	V	Q	J	E
3	E	W	R	K	F
4	F	X	S	L	G
5	G	Y	T	M	H
6	H	Z	U	N	I
7	I	A	V	O	J
8	J	B	W	P	K
9	K	C	X	Q	L
10	L	D	Y	R	M
11	M	E	Z	S	N

—and so on until the twenty-sixth letter in each column had been reached. The letters of the key were then repeated over those of the message, as many times as necessary, as in a Vigenère:

C U P I D C U P
C O M E H E R E

The encipherer now ran down the first column until he reached the first letter of the clear, and substituted for it the number at the left of the line represented; then down the U or second column till he found *O*, substituting for it the number at the left

of that line; then down the column P till he reached *M*, and so on, making the result for the clear given:

1 – 21 – 24 – 23 – 5 – 3 – 24 – 16

The result makes a cipher of fair quality, though not a very resistant one. (The fact that only twenty-six numbers are represented at once suggests their translation into letters, after which it does not take long to solve by any one of several methods, as in Chapter Nine.) In the use to which it was put practical difficulties developed instantly. Madison made so many mistakes in writing messages with it that Randolph found them utterly incomprehensible, finally being reduced to asking him to repeat them in plain English. Not even modern research has been able to make out what the future president meant to say in all cases.

Arthur Lee, who rather fancied himself in the role of intriguing secret diplomat, proposed as early as June 3, 1776 that the Committee of Secret Correspondence among the colonists make use of what he called a "cypher," but what today would be known as a book code. The proposal has no particular interest from the standpoint of general history. Congress does not seem to have been much impressed, and though in 1777–1779 Lee did carry on a considerable correspondence in such a code with the aid of Entick's *New Spelling Dictionary,* it was only with his brothers, William and Richard Henry Lee. But the idea has importance in the special history of cipher as the first public appearance of a device which is still regarded as the only unsolvable code by ninety per cent of the persons who have a smattering of cryptography.

The book code is operated by having each party to the correspondence in possession of a particular edition of a dictionary. Theoretically, any book will do; but as it is necessary to find the exact word it is desired to communicate, a dictionary is the only type of volume that contains all the necessary words in such an arrangement that they can be found without unbearably long research. The sender transmits a series of reference numbers, giving the page and line on which will be found the word he

wishes the receiver to read. The receiver looks up these numbers in his own copy of the same dictionary and reads off the message.

The system is not nearly so safe as it looks; the messages in the Lee papers were read in modern times without any particular difficulty, although no copy of the edition of Entick's dictionary he had used survived. During the World War American Army cryptographers broke down a dictionary code being used by the Germans for wireless messages to their agents in South America, although they had taken the precaution of concealing the actual reference numbers by alternately adding six to them and subtracting four from them. The curiosity is to discover that the system was already well known at the time of the American Revolution, for Arthur Lee certainly did not invent the device.

It is still more curious to find that neither the British nor the French armies in America were aware of even so simplified a form of the Vigenère system as the one Madison so misused. A few British dispatches in cipher survive, notably some in connection with Benedict Arnold's treason; they were written in a simple form of word transposition. French ciphers of the war invariably turn out to be simple substitution with suppression of vowel frequencies.

The art of cryptography reached a still lower ebb during the French Revolution. The royalists who had fled abroad plotted constantly and with the greatest energy for the restoration of their king, and a trip to the guillotine was the price of having their secret correspondence disclosed. But even under these impulsions they could think of no better cryptographic device than simple substitution of the simplest type—the Julius Caesar cipher.

II

The failure to find a good and workable cipher probably cost many unimportant men their heads, and it certainly brought death to one great figure—Charles Pichegru, general-in-chief of the French Army of the Rhine, who faced the Austrians along that river from Mannheim to the Swiss frontier.

He was probably the ablest officer then in the service of the French Republic, and his troops were devoted to him, but he was ambitious as Lucifer, dissatisfied with the rapidity of his own promotion, and a moderate republican, disgusted with the shabby electoral trick by which the violent elements had cemented their power under the new constitution of 1795. His armies were superior to those opposing him, but the campaign went badly. Two divisions were cut off and severely punished in losing battles, Mannheim fortress was lost, and to climax matters Pichegru signed a six months' armistice. At Paris they were still unsuspicious of his loyalty but a government can do only one thing when a campaign fails so badly, and the French Directory did that thing—recalled Pichegru and replaced him with General Moreau.

The truce was not yet in effect when Moreau reached the front, and though there was no time for large operations he demonstrated his activity by a series of cavalry raids beyond the Rhine. In one of them he caught the baggage train of General Klinger of the Austrian staff. In that baggage train was a wagonload of papers, and among those papers a packet in cipher. Some of the ciphered documents bore the signatures of members of the Aulic Council, the great Austrian war council, some, the name of the Prince of Condé, who was in charge of a small army of French emigrés, and some no signatures at all.

It struck Moreau that it would be worth while to know more about a three-cornered correspondence which, though carried on among allies and through friendly country, was so secret it had to be enciphered. It took a month to read those dispatches, although they were nothing but simple substitution and there was abundant material—the demonstration of how far cryptography had descended from the days of Rossignol.

But they were worth reading, all referring to something mysteriously called in them, "the affair of General Pichegru" or "the Pichegru matter." What this matter was it was not too hard to guess, but there was no definite reference to treason, and the French government, all unsure of popular support, did not dare bring the favorite general to trial without better evidence. They

warned him that he was in "preventive arrest" and told him not to leave Paris.

To Pichegru this was a guarantee that they did not dare to go to extremities with him. He plunged deeper than ever into royalist plottings, a mistake. Napoleon Bonaparte, then general of the Army of Italy, captured Venice soon after, and it was reported to him that a certain Comte d'Antraigues was leaving the city, disguised as a member of the Russian legation. D'Antraigues was a French royalist, known to be the center of their intrigues in Italy. Bonaparte had him stopped at Trieste and seized his papers. Among them was a series of ciphered letters, and when they proved to be the usual simple substitution with suppression of vowel frequencies which the royalists used, they were promptly read. There was a letter there from Pichegru; he agreed that as soon as he was placed in command of an army again, he would lead it to Paris, overthrow the republic in favor of the king, and in return would accept the offered reward of a marshal's baton, a million francs in cash and the governorship of Alsace.

Pichegru died in prison—a suicide, said some; strangled by orders of the government, said others. The point is unimportant—what he really died of was bad cryptography.

III

It would seem that Napoleon took to heart this or some other lesson on the value of secret communications. During the early part of his career there is no trace that he used ciphers; most of his orders, in any case, were written in the burning hurry of battle and called for such instant execution that even when they fell into the enemy's hands the emergency on which they bore had passed before any use could be made of them.

Later, in the imperial period, Napoleon apparently secured the services of some cryptographer who had been in the old French Royal Laboratory established by Richelieu and Rossignol. Toward the close of Napoleon's campaigns he was using, like Louis XIV, a "Lesser Cipher" for communication with minor officials and

officers and a "Great Cipher" into whose secrets only the marshals were admitted.

As with the Louis XIV ciphers both were composed of numbers to which values were assigned arbitrarily, but there the resemblance ended. The Rossignol Great Cipher had been fully syllabic, with signs for letters used only rarely, and it had comprised 587 numbers; moreover, it was handled by masters, with the messages written in it carefully composed to avoid repetitions. In the Napoleonic Great Cipher there were less than 200 signs; its basis was the assignment of numbers to letters, with the addition of other numbers for names, and in a few cases for words commonly used in military dispatches—"regiment," "infantry." Its value was still further reduced by the manner of its employment; Napoleon communicated the key to no one but the marshals, men not remarkable for subtlety of intellect, and they made a sad botch of the matter.

"Of course," said the Emperor Alexander of Russia, trying to console Marshal Macdonald for the French defeats when the two met after the war, "we were greatly helped by always knowing your Emperor's intentions from his own dispatches. In the last campaigns the country was much against you and we captured a number of them."

"I suppose it is hardly surprising that you were able to read them," replied Macdonald a trifle sadly. "Someone certainly betrayed the key to you."

The Russian was astonished. "Not at all. I give you my word of honor that nothing of the kind happened. We simply deciphered them."

In one instance it was a misunderstood rather than an intercepted dispatch that ruined Napoleon's chances. The event fell on the second day of the Battle of Leipzig, the "Battle of the Nations." The French had been half-victorious the first day; they were half-defeated that morning when Napoleon, realizing his position was untenable, planned a retreat. It was to take place that night; Marshal Augereau was ordered up from the rear with an army corps to build bridges across the river at the army's back and to cover the retirement.

The order is still extant; it went in duplicate, one copy fully enciphered, one enciphered only as to names of places and the word "enemy." (If the Allies had intercepted that second dispatch they could certainly have broken Napoleon's Great Cipher within the night, provided they had not already done so.) Augereau received the dispatch and replied with another, also in the Great Cipher. His men had marched long and late on the previous night, he said; he would come, but could not arrive as soon as the Emperor expected. Emergency measures would be needed to hold the lines till his arrival.

The dispatch reached Napolean's headquarters, but, like Madison's letters to Edmund Randolph, hopelessly garbled. No one could read it. Augereau did not arrive, and neither did any explanation of his non-appearance, while the army did nothing in hourly expectation of his coming. If Napoleon himself had been conscious of the failure he might have taken measures; but that marvelous engine of body and mind which had carried the Emperor through so many campaigns was wearing out. He had fallen asleep and there was no one who dared wake him or take the responsibility of giving orders without his approval. The Allies broke the French lines, the single bridge behind the army was insufficient. What had been a check turned into a wild rout; the French organization was broken, they lost twenty thousand prisoners and never recovered.

Nor was Augereau the only marshal whose clumsy cryptography led to a fall. Before that last campaign to Leipzig and Montmartre began, Joachim Murat, marshal of the Empire and king of Naples, had contemplated joining the Austrian side in the war. He sent secret overtures to Vienna; Austria was slow in replying, and when peremptory orders came from Bonaparte, the Marshal-King made up his mind the Austrians were not going to answer at all, and set out to join the French in Bohemia, hoping that after all they would win. Just beyond Rome, riding north with his suite, he met a messenger from Vienna with dispatches for him. They were in cipher, probably not much better as cipher than the simple substitutions the Austrians had used in 1795 when the Klinger dispatches were captured. But neither Murat himself

nor any one in his suite could read or break them down. He assumed they must represent a refusal of his offers and sent them away behind him to Naples for decipherment, while he rode on, down the long road that led to Leipzig, surrender and a firing squad in front of a wall. Actually, they had been a full acceptance of his alliance, with immunity and the extension of his kingdom.

Chapter IX

THE REVIVAL

I

No single and simple explanation will account for the revival of crytography that became apparent about the middle of the nineteenth century. Doubtless the general rise in the European literacy curve during the years following the French Revolution had something to do with it, though the connection would be somewhat difficult to trace. M. Chappe's "lightning telegraph" had a great deal to do with it—the ancestor of the semaphore signal system, a series of tall posts with movable arms, set up along the roads radiating from Paris to the frontiers of France in Napoleon's day. Each post was visible from those on either side; the arms were placed at varying angles to communicate the letters of a message, and when, on its first trial, the device carried the news of a battle from Strassbourg to Paris twelve hours before the fastest courier, it was made official by the French government. The conquering French carried it into Central Europe, and in England, meanwhile, a naval officer perfected the method of conveying information rapidly across long distances by hoists of colored flags. Before the century reached its halfway mark the greatest invention of all had come—the electric telegraph of S. F. B. Morse.

The influence of these inventions on cryptography was twofold. They made it possible for a home office to direct minutely the steps of a military, diplomatic or commercial maneuver being carried on at a distance. At the same time they threw these communications open to the public, for anyone could, in a few hours, acquire the knowledge necessary to read the messages waved across the skies or transmitted through the wires. Ciphers thus became almost obligatory in communications of great public

moment, and at the same time the political ferments of the 1830's and 1840's vastly increased the amount of secret and dangerous private communication.

Yet the great revival in cryptography appears to have stemmed rather from literary than practical sources. In 1819 Rees's *Encyclopedia* came out with an article on ciphers that has ever since been a classic among members of the profession. It described several methods of simple substitution, commenting in thoroughly modern style on how little security they offered; shorthand ciphers; several methods of conventional sign and diagram ciphers; the Bacon biliteral; and variants on the Porta and Vigenère. It is interesting nowadays to note that for the solution of the two latter it suggests no better method than that of attacking the initial letters of lines and words. The writer rather naïvely assumes that the word-groupings in the enciphered message will be the same as those in the clear, instead of the whole being divided into five-letter groups.

Two years after Rees's *Encyclopedia* there was a conspiracy in France to return the Bourbons to the throne from which they had been ousted by a revolution in favor of the rival House of Orléans. Its failure was due in no small part to the interception of correspondence between the Legitimist Duchesse de Berry and her co-plotters in Paris, and the decipherment of this correspondence by Berryer, the orator. The ciphers were nothing but simple substitution, even the precaution of suppressing vowel frequencies having been omitted. A year later the police picked up more ciphered correspondence relating to a conspiracy, this time in favor of that Prince Louis Napoleon who, after a life of wild adventure, was to become Napoleon III. Whether the letters were deciphered or betrayed does not appear. Certainly they threw no great obstacles in the path of a cryptographer, being in an allegorical code which sought to conceal political information under scandalous gossipy letters about persons supposedly the inhabitants of some small town. M. Antoine, in this code, stood for Queen Hortense; England was Mme. Lirson; the Army, Mlle. Amélie; the police, M. Pamberg; and the code was really handled with considerable skill.

The former of these two decipherments had important results; it attracted the attention of Edgar Allan Poe. Given his natural taste for the obscure and mysterious his reaction was foreordained, and it occurred without much delay. He read every book and reference on cryptography he could secure, and in 1840 published an article in a Philadelphia weekly, boldly declaring that there was no such thing as an unsolvable cipher, and still more boldly offering to solve any cipher message sent to him.

He took care to specify that the messages should be simple substitution, that they should be in English and that the word divisions of the clear should be preserved. In reply he received about a hundred messages of varying length, several accompanied by offers to bet that he could not solve them, and a great many stepping beyond the boundaries of his conditions in one direction or another. A few were in foreign languages, some did not preserve word or even sentence divisions, and some, as Poe himself describes it, "used several alphabets," which probably means the employment of some form of the Vigenère tableau. He solved all but one; that one he demonstrated to be a gibberish combination of letters sent in in the hope he would try to read a meaning into it.

In a general article on cryptography (*Graham's Magazine* 1840) Poe gives one of the typical messages he received as the result of his challenge:

> Ofoiioiiaso ortsiii sov eodisoioe afduiostifoi ft iftvi si tri oistoiv oiniafetsorit ifeov rsri afotiiiiv ridiiot irio rivvio eovit atrotfetsoria aioriti iitri tf oitovin tri aetifei ioreitit sov usttoi oioittstifo dfti afdooitior trso ifeov tri dfit otftfeov softriedi ft oistoiv oriofiforiti suitteii viireiiitifoi ft tri iarfoisiti iiti trir uet otiiiotiv uitfti rid io tri eoviieeiiiv rfasueostr ft tri dftrit tfoeei

He remarks that this was an extremely difficult cryptogram, requiring considerable time and the exercise of his utmost powers in decipherment, though without giving any information on the method he used. It seems fairly obvious that the repeated TRI combinations would suggest themselves at once as *THE*, the SOV combination as *AND* (on account of the presence of V, a char-

acter occurring elsewhere either as a terminal or a doublet in almost every instance); and that the four times repeated I in the second line would indicate that certain letters of the cryptogram represented more than one letter of the clear.

Poe also gives the solution:

> Nonsensical phrases and unmeaning combinations of words, as the learned lexicographer would have confessed himself, when hidden under cryptographic ciphers, serve to perplex the curious enquirer and baffle penetration more completely than would the most profound apothegms of learned philosophers. Abstruse disquisitions of the scholiasts, were they but presented before him in the undisguised vocabulary of the mother tongue—

—with a cipherer's error in the word *PERPLEX*. A key-phrase was the basis of the substitution—"Suaviter in modo, fortiter in re":

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
S U A V I T E R I N M O D O F O R T I T E R I N R E

This explains the difficulties Poe encountered during the decipherment; I stands for three letters of extremely high frequency (*E, I, S*) and one of the second rank (*W*). T stands for two high-frequency letters and one less frequent; R for four letters and O for three, not to mention the fact that the clear text is overloaded with unusual words. A reader in full possession of the key would have had almost as much difficulty in making out the meaning as Poe did.

The device of using a key-phrase in which several letters are repeated and therefore stand for more than one letter of the clear had some justification in Poe's day. It was then quite common practice and exactly the method used in the Legitimist cipher cracked by Orator Berryer. The plan of throwing decipherers off the track by the use of rare and ornate words is typical of amateurs. It lies at the basis of a type of cipher which has recently become very popular in the United States under the name of "crypts," and which are eagerly pursued through newspapers and magazines by puzzle fans. The usual procedure is to ar-

range a message that will defeat the frequency tables by giving E a low frequency, and making the ordinarily less frequent letters, such as W, F, M, come out at the top of the count for the cryptogram in question. It leads to some queer wordings. Typical crypt:

ABAACDB ABEBFGHICGEA AJCKLDM AHBDL
AHNOFGAINOP AGDQLCEF ABDGAACB*

—with the key:

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
G I R P B K F S C T U D H E N V W O A L Q X J Y M Z

Poe has an important niche in the history of cryptography although he brought little or nothing new to the art but his taste for it and a natural skill in decipherment. He made it briefly popular in Philadelphia in the 1840's, but what was a great deal more important he attracted literary interest to the subject, particularly in France, where his works were received so much more enthusiastically than in his own country. *The Gold Bug* had numerous imitators there. Jules Verne three times introduced cryptograms and their solution as important elements of his stories, and Balzac found the mania for ciphers in fiction so widespread that he was moved to put a cryptogram three pages long into *La Physiologie du Mariage*. It must have amused the last writer greatly to discover that for years after there was hardly a writer on ciphers in any country who did not attempt to solve the *Physiologie du Mariage* cryptogram and fail in the attempt. Commandant Bazeries, the same who broke the Great Cipher of Louis XIV, finally spoiled the sport with an analytical essay demonstrating that the message was an elaborate fake, almost as carefully composed as a genuine cipher, and arranged to have a number of almost-clues.

II

While the early telegraphs were clicking their teeth or fluttering their wings, while Poe and his readers were concocting artificial

* See notes at rear of volume for translation if you cannot work it out.

mysteries, literary interest in cryptography was taking another direction in Germany. Under the impulse of a flood of memoirs from the officers who had followed or fought Napoleon, that country was in the midst of an outburst of interest in military history. It was natural that among the students of the science of war there should be some to fix their attention on a matter so profoundly affecting the success of military operations as secret communications. But in an age when the rest of the world was fumbling with simple substitutions and allegorical codes, it is surprising that the interest should suddenly be concentrated on decipherment, which up to this time had been the stepchild of the art.

That it did so is primarily due to a single man, a German named Kasiski, about whom nothing is known but that he was a major on the Prussian staff. In 1863 he published the first comprehensive book on cryptography in more than a century. It is remarkable also in another respect: its outstanding feature was the statement of a method for deciphering the only hitherto impregnable system—the Vigenère tableau.

Now known as the Kasiski method for double substitutions, that method is the fundamental of all modern cryptography. It is based on the fact that in all languages certain bigrams, trigrams and even sets of four or five letters are frequently repeated, and the parallel fact that it is almost impossible to write a message of any length without repeating words. When a message is enciphered in Vigenère it therefore frequently happens that the repeated bigrams, trigrams or words of the clear, fall under the same letters of the key-word, resulting in repeated combinations in the cryptogram. Illustration:

Key-word	R A G S R	A G S	R A G S R	A G S R A G S R A G	
Clear	T H E R E/	A R E/	T H R E E/	M E T H O D S/	F O R/
Message Group	K H K J V/	A X W K H/	X W V M K/	L Y O J K/	W O X
	1	2	3	4	5
Key-word	S R A G S	R A G S R A G S R A G S R A G S R A			
Clear	T H E S E/	D O U B L E/	S U B S T I T U T I O N/		

Message	LY/E Y W U O/A T C E Y/M S S Z A/K U Z A F/N
Group	6 7 8 9

Key-word	G S R A G S R A G S R A G
Clear	D E C I P H E R M E N T S

Message	J W T I/V Z V R S/W E T Y
Group	10 11 12

The *TH* of *THERE* and the *TH* of *THREE* have both fallen under RA of the key-word, and the result in each case is KH in the message (beginning group 1—end of group 2.) *RE* in *ARE* and the same pair of letters in *THREE* have similarly been enciphered with GS of the key-word, producing XW (group 2, group 3). *TH* of *METHODS* coincides in the same way with *TH* of *THESE* (groups 4–5); and the *TI's* of *SUBSTITUTION* both come out as ZA (groups 8–9); and the *ES* of *THESE,* like the *ES* at the end of *DOUBLE* and the beginning of *SUBSTITUTION* both result in EY.

Obviously, if a repeated bigram in the message represents a case in which repeated bigrams of the clear have coincided with repeated bigrams of the key-word, the key-word must have occurred twice or more times to produce such a result. The number of letters between the repeated bigrams is, therefore, a multiple of the number of letters in the key-word.

This fact is the basis of the Kasiski method. The repeated bigrams in the message are listed and the number of letters between each set counted:

KH - KH - 8
XW - XW - 4
LY - LY - 8
ZA - ZA - 4
EY - EY - 8

The figures thus obtained are factored, and since some of them may represent more than one repetition of the key-word, the greatest common divisor is the length of the key-word itself. When the length of the key has been ascertained, so has the number of columns used in the Vigenère tableau to encipher—that is,

the number of alphabets. From this information a solution of the cipher can be worked out.

Example, with a message of unknown content:

1	2	3	4	5	6
WOFIP	DIBEU	KOXGV	QODXR	AWYRZ	CDYWZ
7	8	9	10	11	12
IWYRK	DODXR	RYXSI	IVPVF	BVKQV	AODWV
13	14	15	16	17	18
KSXFR	GFKKV	QSQME	HODWZ	MHRMI	IMISL
19	20	21	22	23	24
LWVPS	TGETF	DFDIU	DBISL	GZOJK	QMKFR
25	26	27	28	29	30
IHKPZ	DBYJT	POCWV	JFCVV	DFQEE	XNOEK
31	32	33	34	35	36
AWDXC	TVKQV	ATYVE	TKKXK	PQUEE	SBKOV
37	38	39			
AWKMJ	DBDSI	XUQLK			

The experienced cryptographer would know at a glance that he had a double substitution before him here. The possibility of transposition is eliminated by the enormous number of very low-frequency consonants (J, K, Q, Z) and the relative shortage of high-frequency vowels. Against simple substitution stands the fact that every letter is represented at least once, and every letter but one at least three times. This means that J, Q, X and Z, which among them would normally furnish only 1 letter to a clear 195 letters long, have here furnished not less than 12, even allowing that these four represent the lowest frequencies in the message.

Moreover no letter in this message furnishes as much as ten per cent of the total. In normal text E alone furnishes thirteen per cent and T slightly over ten per cent more, and if simple substitution had been used, the percentages would be reproduced, although assigned to different letters. Also, in the message before us eight letters furnish approximately five per cent each of the total while three other letters furnish percentages above this

figure. In normal text only nine letters furnish five per cent or more of the total text. (For all these figures, Table I.)

These characteristics, discovered as the result of the preliminary observation and letter-count which is the first step in any process of cryptanalysis, indicate a double substitution cipher. The next step is to discover the repeated bigrams (which mark the cipher as one of the Vigenère type) and count the distances between them, factoring the resulting counts and setting the result down in a table. Cases where more than two letters are repeated are also included.

Combination	Found in groups:	Distance between first letters of combinations	Factors of distance
KO	3 & 36	167	167
VQ	3/4 & 14/15	55	5×11
ODXR	4 & 8	20	$2 \times 2 \times 5$
OD	4 & 12	40	$2 \times 2 \times 2 \times 5$
	8 & 12	20	$2 \times 2 \times 5$
	4 & 16	60	$2 \times 2 \times 3 \times 5$
	8 & 16	40	$2 \times 2 \times 2 \times 5$
	12 & 16	20	$2 \times 2 \times 5$
DX	4 & 31	135	$3 \times 3 \times 3 \times 5$
	8 & 31	115	5×23
WYR	5 & 7	10	2×5
AW	5 & 31	130	$2 \times 5 \times 13$
	5 & 37	160	$2 \times 2 \times 2 \times 2 \times 2 \times 5$
	31 & 37	30	$2 \times 3 \times 5$
II	9/10 & 17/18	40	$2 \times 2 \times 2 \times 5$
SI	9 & 38	145	5×29
VP	10 & 19	46	2×23
VK	11 & 12/13	9	3×3
KQ	11 & 23/24	62	2×31
VKQVA	11/12 & 32/33	105	$3 \times 5 \times 7$
VA	11/12 & 36/37	125	$5 \times 5 \times 5$
DW	12 & 16	20	$2 \times 2 \times 5$
VK	11 & 12/13	8	$2 \times 2 \times 2$
	12/13 & 32	97	97
WV	12 & 27	75	$3 \times 5 \times 5$
	12 & 19	33	3×11

Combination	Found in groups:	Distance between first letters of combinations	Factors of distance
WV	19 & 27	42	$2 \times 3 \times 7$
FR	13 & 24	55	5×11
KK	14 & 34	99	$3 \times 3 \times 11$
QM	15 & 24	43	43
MI	17 & 18	3	3
ISL	18 & 22	20	$2 \times 2 \times 5$
ET	20 & 33/34	67	67
FD	21 & 20/21	2	2
DB	22 & 26	20	$2 \times 2 \times 5$
	22 & 38	80	$2 \times 2 \times 2 \times 2 \times 5$
	26 & 38	60	$2 \times 2 \times 3 \times 5$
EE	29 & 35	30	$2 \times 3 \times 5$
AW	31 & 37	30	$2 \times 3 \times 5$

Although this list seems very extensive it is not longer than that usually encountered in Vigenère decipherments.

There is no common divisor for all the numerical distances between repeated combinations, but some, such as the KO which heads the list, are obviously due to accidents, since it is extremely unlikely that a key-phrase 167 letters long has been used, and if it had the other repeats would hardly occur. Among the rest 2 x 2 and 2 x 3 are fairly frequent, but 5 is clearly the dominating factor. Moreover it is the only one that enters into the distances between the repeats of the four-letter group ODXR, the five-letter combination VKQVA and the three-letter sequences WYR and ISL. The possibility of such longer combinations being repeated by accident is extremely small. Hence it may be assumed that the key-word was five letters long.

In accordance with this finding the message is rewritten in five columns:

W O F I P
D I B E U
K O X G V
Q O D X R
A W Y R Z
C D Y W Z

I W Y R K
D O D X R
R Y X S I
I V P V F
B V K Q V
A O D W V
K S X F R
G F K K V
Q S Q M E
H O D W Z
M H R M I
I M I S L
L W V P S
T G E T F
D F D I U
D B I S L
G Z O J K
Q M K F R
I H K P Z
D B Y J T
P O C W V
J F C V V
D F Q E E
X N O E K
A W D X C
T V K Q V
A T Y V E
T K K X K
P Q U E E
S B K O V
A W K M J
D B D S I
X U Q L K

In each column there have now been assembled the letters enciphered with the same key-letter; that is, with the same column of the Vigenère tableau. To put it otherwise, each column by itself now consists of a simple substitution cipher, and can be solved as such with the aid of the letter-frequency tables.

This is the pure Kasiski method, seen at its most effective when there is a considerable amount of material in a single message, or when there are several messages. In cases like that presented by the cipher before us, it is attended by certain

inconveniences. The columns are only thirty-nine letters long; the alphabetic frequency table (Table I) is not accurate for so small a number of letters and, since the letters in each individual column do not run consecutively, the bigram, trigram and pattern-word tables cannot be applied.

When separate counts are taken on each of the five columns here, the highest frequencies are:

Columns:	1	2	3	4	5
	D – 7	O – 7	K – 8	E – 4	V – 8
	A – 5	W – 5	D – 7	S – 4	K – 5
	I – 4	B – 4	Y – 5	W – 4	E – 4
		F – 4		X – 4	R – 4
					Z – 4

Now if it be accepted that the highest frequency in each column represents *E* of the clear, and the next highest frequency *T* of the clear, group 31 (AWDXC) deciphers as *TTTT?* and the combination in groups 7-8 (K/DODX) deciphers as *TEEEE*. This is not merely improbable; it is impossible. It is possible, of course, to work the thing out by trying in turn each of the high-frequency letters of the alphabet for the letters that show the highest frequencies in the columns, but there is a short cut, introduced into the Kasiski method toward the close of the nineteenth century by the French cryptographer Kerckhoffs, which greatly speeds up the process.

Kasiski concentrated on the solution of the cryptogram; Kerckhoffs was of the French school which regards the recovery of the key-word as the most important step. When the message has been separated into columns each of which has been enciphered by means of the same key-letter and the count taken on each column separately, he begins to make deductions. Under his method the cryptographer considers column 1 separately. If D, the highest-frequency letter in that column, represents *E* of the clear, the Z-column of the Vigenère tableau was used for enciphering the column. If Z was the key-letter for this column, A (which shows the second highest frequency in the column) represents *B*, and I (third highest frequency) represents *J*. (See Vigenère tableau, page 120.) It is in the last degree improbable that two letters of

such low general frequency as B and J should show such high frequencies in this column and message. The hypothesis that D = E and Z is the key-letter in Column 1 is, therefore, unsatisfactory.

The other probabilities can be tabulated, supposing that D represents in turn each of the other letters of generally high frequency:

If D =	Then key-letter was	And, therefore (with comment)
T	K	A = *Q*; I = *Y* Impossible; too many *Q's*
A	D	A = *X*; I = *F* Impossible; too many of both *X* and *F*
O	P	A = *L*; I = *T* Satisfactory; both subsidiary equations give high-frequency letters
N	Q	A = *K*; I = *S* Impossible; too many *K's*
R	M	A = *O*; I = *W* Possible; rather a lot of *W's*
I	V	A = *F*; I = *N* Doubtful; *F* frequency too high
S	L	A = *P*; I = *X* Impossible
H	W	A = *E*; I = *M* Possible, though *M* seems pretty strong

There are, then, three fairly good possibilities for the first letter of the key-word—P, M, and W. The process is now extended to the second column and another tabulation made along the same lines:

If O =	Then key-letter was	And, therefore
E	K	W = *M*; B = *R*; F = *V* Doubtful; too many of both *M* and *V*
T	V	W = *B*; B = *G*; F = *K* Impossible; all subsidiaries rare letters

If O =	Then key-letter was	And, therefore
A	O	W = *I*; B = *N*; F = *R* Satisfactory
N	B	W = *V*; B = *A*; F = *E* Very doubtful
R	X	W = *Z*; B = *E*; F = *I* Impossible
I	G	W = *Q*; B = *V*; F = *Z*
S	W	W = *A*; B = *F*; F = *J* Possible; good many *J's*

This leaves two possibilities for the second letter of the key-word; namely, O and W.

Continuing to the third column:

If K =	Then key-letter was	And, therefore
E	G	D = *X*; Y = *S* Impossible
T	R	D = *M*; Y = *H* Possible but very doubtful; no vowels among high frequencies
A	K	D = *T*; Y = *O* Satisfactory
O	W	D = *H*; Y = *C* Possible
N	X	D = *G*; Y = *B* Impossible
R	T	D = *K*; Y = *F* Impossible
I	C	D = *B*; Y = *W* Impossible
S	S	D = *L*; Y = *G* Doubtful

Again two possibilities, K and W, with one dubiety, S. Another table for the fourth column:

If E =	Then key-letter was	And, therefore
E	A	S = *S*; W = *W*; X = *X* Impossible
T	L	S = *H*; W = *L*; X = *M* Doubtful; no vowels among high frequencies

If E =	Then key-letter was	And, therefore
A	E	S = *O*; W = *S*; X = *T* Probable
O	Q	S = *C*; W = *G*; X = *H* Doubtful
N	R	S = *B*; W = *F*; X = *G* Impossible
R	N	S = *F*; W = *J*; X = *K* Impossible
I	W	S = *W*; W = *A*; X = *B* Impossible
S	M	S = *G*; W = *K*; X = *L* Impossible

There is only one high probability for this column; E is almost unquestionably the key-letter. Fifth column:

If V =	Then key-letter was	And, therefore
E	R	K – *T*; E – *N*; R – *A*; Z – *I* Fits the frequency table so well that it is unnecessary to look further

The unified result of this compilation is, then, that the key-word consists of:

1	2	3	4	5
P				
M	O	K	E	R
W	W	W		

Obviously POKER is the only word that can be made out of these elements. (If the process has been carried this far and the selected key-word does not prove out, the compilations on possible key-letters can be carried farther, and if this fails another possible length tried for the key-word.) In the present case it does not fail; the application of the key-word to the message causes it to read off smoothly.*

* A full translation will be found in the notes at the end of the volume if you are too lazy to work it out.

III

Like many other systems in the history of cryptography Kasiski's was a reduction to reasoned processes of thought of a method already in use, but fitfully, depending upon the inspiration of the individual. Its importance lies in the fact that he completed the task of Edgar Allan Poe. He finished the demonstration that there was not in existence in his time any cipher both practically useful and practically unbreakable. Between them the German officer and the American author changed the main stream of cryptography. The early cipherers were more interested in concealing their own messages than in solving those of others; in the age just dawning the center of gravity was shifted to decipherment. Since Louis XIV, or better, since Rossignol, only two new basic methods of writing secret messages have been discovered; but every variation on a method has brought forth a whole school of new systems of decipherment.

The transition, like many others in connection with the military art, can be observed taking place during the American Civil War. At the outbreak of that conflict Governor Dennison of Ohio asked a telegraphic expert of his acquaintance, Anson Stager, to prepare a safe cipher for his own communications with the governors of Illinois and Indiana. Stager did his job in a highly satisfactory manner. When the Ohio troops moved into West Virginia for the campaign there under General McClellan, the latter officer asked Dennison for the loan of his cipher expert. There was a conference at a hotel in Cincinnati, with McClellan, Stager and Alan Pinkerton, the detective, present. The three together cooked up a cipher system which spread throughout the West, and was ultimately taken by the general to Washington when he went there as commander of the Army of the Potomac.

It was a word-transposition of the same general type as that used for preparing the Duke of Argyle's rising in Scotland, two hundred years before. A thoroughly typical message in it read:

To George C. Maynard, Washington:

Regulars ordered of my to public out suspending received 1862 spoiled thirty I dispatch command of continue of best otherwise worst Arabia my command discharge duty of my last for Lincoln September period your from sense shall duties the until Seward ability to the I a removal evening Adam herald tribune.

PHILIP BRUNER.

The address and signature were, of course, covers. The first word—REGULARS—was a code-word, indicating that the clear had been written in five columns of nine words each (the remainder of the 51 words being nulls), and giving the order in which the groups of words were to be written down. The capitalized words were code names, according to a simple one-page list. The receiving office in Washington would accordingly write it down in this pattern, nulls italicized:

tribune	Lincoln	*spoiled*		
herald	September	thirty	1862	*for*
Adam	period	I	received	last
evening	your	dispatch	suspending	my
removal	from	command.	Out	of
a	sense	of	public	duty
I	shall	continue	to	discharge
the	duties	of	my	command
to	the	best	of	my
ability	until	otherwise	ordered.	Arabia
	Seward			*worst*

Consulting his code-sheet the receiving operator would now discover that LINCOLN was a code-word for Louisville, Ky.; ADAM a code-word for General Henry W. Halleck, then chief of staff of the Union armies; and ARABIA a code-word for the name of General Don Carlos Buell, then commanding the Army of the Tennessee, at grips with the enemy in central Kentucky.

The message has obviously been written by reading the clear up the fourth column, down the third, up the fifth, down the second and up the first, then attaching the code-word REGULARS to indicate the route followed through the maze of words.

The Confederacy had an efficient espionage organization and an excellent cavalry service, particularly strong in raiding leaders

such as Forrest, Morgan and Wheeler. Both spies and horsemen tapped telegraph lines far behind the Union armies and repeatedly captured stations where Union cipher messages were on file. In spite of the abundance of material thus obtained and the relative simplicity of the cipher, they utterly failed to break down a single message—a fact which would be incredible if the Confederate government itself had not vouched for it by periodically publishing in the newspapers the latest batches of captured telegrams, with requests to anyone who could make anything of them to come forward.

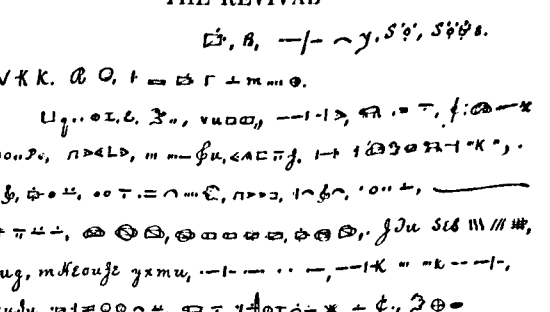
Twice rebel raiders captured Union cipher operators with copies of the latest ciphers and code-words in their possession, but even this did not mend matters. Anson Stager simply got out a new set of keys, slightly changing the route-patterns and extending the list of code-words. The result was always more than the Confederates could handle.

IV

Yet the Unionists, who themselves used the very weak word-transposition cipher, excelled in breaking down Confederate secret communications; and the Confederates, who could make nothing of the simple Union ciphers, themselves used an intricate combination of conventional-design cipher in their secret-service work, and a Vigenère for military messages.

In December, 1863, Postmaster Wakeman of New York City was handed a letter that had been placed in the mails, addressed to A. Keith of Halifax, Nova Scotia, an address which had already been indicated to him as a possible cover for rebel agents working in the North. When he opened it he found it was in a conventional-design cipher.

He could make nothing of it. Neither could the War Department stenographers in Washington, to whom it was immediately submitted, and it was finally turned over to three of the operators handling cipher telegrams for the Army—Turner, Bates and Chandler. They perceived at once that the ordinary methods used in breaking simple-substitution ciphers would not do here.



There were at least five complete sets of characters in the letter, so interspersed that there was insufficient material to set up a reliable frequency table for any one set.

However the letter presented three great cryptographic weaknesses. The line at the top was obviously a date-line, of which the last four figures evidently stood for the current year, 1863. As the two figures preceding "1863" were the same as the first two of that number, they were evidently 18; and as the month was December *DEC* could be deduced, and *N.Y.* was the correct translation of the two characters preceding *DEC*. This made another weakness clear: the encipherer had kindly divided the words of his message off with commas, and, as he had used only

one of his five or more alphabets in each word, the possibility of finding pattern-words offered an excellent line of attack.

The third weakness was the phrase *REACHES YOU* in clear; and this was the one that proved fatal. For *REACHES YOU* was preceded in the letter by two words, of which the first was a semi-pattern-word of the arrangement 123452. It was easy for Turner, Bates and Chandler to presume the words *BEFORE THIS*. The presumption gave them nine letters with a strong degree of plausibility, and the nine letters were in a variation on the Rosicrucian cipher.

When a diagram for this form of the Rosicrucian (which includes an X as well as the pig-pen, with two letters in each cell), was constructed and the nine letters inserted, the arrangement of the rest became clear, and all the portions of the letter written with this alphabet were solved. There resulted several complete phrases, notably one about the middle of the letter, which read *OTHER TWO STEAMERS AS PER*—with a nine-letter semi-pattern-word following: 123425667, in one of the other alphabets. *PROGRAMME* was obvious, proved correct, and gave the key to a second alphabet. At the beginning of the message the operators now found a six-letter word, then a two-letter word followed by *HERE*; they could with reason suppose "somebody *IS HERE*" and had another lead.

Working in this manner in less than an afternoon the three cipher men unlocked the whole letter:

New York, Dec. 18, 1863.

Hon J. P. Benjamin:

Willis is here. The two steamers will leave here about Christmas. Lamar and Bowers left here via Bermuda two weeks ago. 12,000 rifled muskets came duly to hand and were shipped to Halifax as instructed. We will be able to seize the other two steamers as per programme. Trowbridge has followed the President's orders. We will have Briggs under arrest before this reaches you; cost $2,000. We want some money; how shall we draw? Bills are forwarded to Slidell and rec'ts rec'd. Write as before.

J. H. C.

Here was a nice little nest of espionage and intrigue for the enemy in the middle of New York City. There was an investiga-

tion which confirmed the decipherment by discovering that a man named Cammack had in fact purchased 12,000 muskets and shipped them to a destination unknown. Unfortunately, there was not much that could be done about it, since the letter itself said that two of the men in the web had left the country, "Willis" could not be located, and it was considered more desirable to keep Cammack in operation than to arrest him.

Mr. Cammack obliged with another letter less than a week later and it was deciphered before midnight. "Say to Memminger," it said, "that Hilton will have the machine all finished and dies all cut ready for shipping by the first of January. The engraving of the plates is superb." Memminger was the Confederate Secretary of the Treasury; the letter made it clear that plates and machinery for printing rebel money were being made in New York. It was not hard to find Hilton, the engraver, and on the last day of the year the United States marshal swooped down on his place, arresting everyone connected with it and seizing several million dollars' worth of Confederate money and bonds, with the plates from which more would have been printed.

In the later years of the war it became particularly easy to tell counterfeit from genuine Confederate paper money. Lacking both a set of plates from England, captured by the blockade, and the New York set, taken through the skill of the Union decipherers, the rebel treasury had to engrave its own plates. The work was so wretchedly done that the counterfeit product looked enough better to mark it as fake.

V

It was on the front where the fighting armies clashed, however, that the Union cryptographers scored their most spectacular success. In the autumn of 1864 the war hung at a crisis. The North was on the edge of victory—Sheridan had won a battle in the Shenandoah Valley, Atlanta was in Sherman's hands. But Grant had been stopped before Petersburg, and Union operations in the Southwest beyond the Mississippi were not prospering. General Canby commanded there for the Federals; his problem was what Kirby Smith's rebels meant to do. They

might carry the war north into Missouri, march away west, head south toward New Orleans or attempt to regain a foothold on the river which they had lost the previous year.

The rebels moved lighter and faster than Canby could; unless he riddled out their intentions in advance, he would have to guard every point at once. As he repeatedly telegraphed to Washington this would take more troops—many more. They could come only from Grant or Sherman, and against that loomed the prospect that the deduction would so hamstring these main armies no victory could be looked for that fall—and, if not that fall, never, for it was the election year, and the Democrats were campaigning on the platform that Lincoln could not end the war.

It was at this junction that there were transmitted to Union headquarters in New Orleans three documents. One was a telegram, partly cipher, partly clear, that had been taken from a tapped Confederate wire:

September 30

To Genl. E. K. Smith:

What are you doing to execute the instructions sent you to HCDLLVW XMWQIG KM GOEI DMWI JN VAS DGUGUHDMITD. If success will be more certain you can substitute EJTFKMPG OPGEEVT KQFARLF TAG HEEPZZU BBWYPHDN OMOMNQQG. By which you may effect O TPQGEXYK above that part HJ OPG KWMCT patrolled by the ZMGRIK GGIUL CW EWBNDLXL.

JEFFN. DAVIS

The second was another such telegram, an old one, which the cipherers had never before seen, but which the accompanying note said had been intercepted during General Grant's Vicksburg campaign two years before.

Vicksburg, Dec. 26, 1862

Gen. J. E. Johnston, Jackson:

I prefer OAAVVR, it has reference to XHVKJ QCHFF IBPZE LREQP ZWNYK to prevent PNUZE YXSWS TPJW at that point. ROEEL PSGHV ELVTZ FIUTL ILASL TLHIF NOIGT SMMLF GCCAJ D.

J. C. PEMBERTON

With the third document was a note saying it evidently was the original clear of the second, to which it corresponded in date, phraseology and number of letters. It had been found among the captured Confederate papers at the fall of Vicksburg, but General Grant, who never had much use for secret communications, had simply done nothing about it at the time.

> I prefer Canton. It has reference to fortifications at Yazoo City to prevent passage of river at that point. Force landed about three thousand, above mouth of river.

The army officers had been unable to make anything of the Kirby Smith telegram. Would the New Orleans headquarters staff make an effort to decipher it? General Canby thought that the Pemberton message with its clear might aid in the decipherment of the other, which appeared to be of the same general type. It was essential to have the information contained in the latter if possible. Hurry.

Captain W. R. Plum, in charge of the Cryptographic Department at New Orleans, knew of the Vigenère tableau, and it did not take him long to discover that the Pemberton message of 1862 had been written by means of that device. With clear and message before him he worked out the key—MANCHESTER BLUFF.

But MANCHESTER BLUFF was not the key to the Kirby Smith message whose translation was so urgently desired. Kasiski's book had been published the year before, but at the time he remained an unknown even in his own country and Captain Plum had never heard of him or his method. The message therefore had to be worked out by some other means. Was there anything to give a clue to its meaning? There was: the Confederate cipherer's slovenly habits of putting part of his message in clear and dividing the rest into words.

The sentence at the end of the message had a peculiarly suggestive structure—*BY WHICH YOU MAY EFFECT* * ******** *ABOVE THAT PART* ** *** ***** *PATROLLED BY THE* ****** ***** ** ********. The only patrols in that part of the world and of the war were the naval gunboat patrols on the river.

On the river—two letters, three and five; and the words in the unknown message between *PART* and *PATROLLED* were two, three and five letters, respectively. Plum tried *OF THE RIVER* (It would be OF not On in the phraseology of the message) to extract a key. He got –TE VICTORY C–, a perfectly sensible key, which could not possibly have been achieved by any fortuitous process, but evidently not the whole key. What about the other gaps? The longer, at the end of the message, offered several possibilities, but the shorter, a one letter word followed by another of eight letters, he could conceive of as nothing but *A CROSSING*. Again he tried the process of extracting the key; which in the Vigenère tableau is just the reverse of enciphering the message. The result was –ORY COMPLE–, or, fitting with that portion of the key he had already extracted, COMPLETE VICTORY. And now his victory was complete; Kirby Smith was being ordered to stay close to the Mississippi and even to move troops to the east bank, Canby's campaign was planned for him, and no reinforcements need be sent.*

Why had the Confederates committed the absurd error of practically giving away their cipher by including passages in clear and indicating the word divisions? General Pemberton's cipherer in the Vicksburg campaign had done much better, breaking the letters into neat five-letter groups that gave no clue to the identity of the words. Captain Plum did not find out till after the war. Then, in some discussion of old campaigns, he learned that it had come about as the result of an accident in Grant's Vicksburg operation of 1863. The Union general thrust swiftly between the forces of Pemberton and Joe Johnston, defeated the former, drove him in on Vicksburg and laid siege to the place. Johnston telegraphed feverishly for reinforcements; one of those telegrams went to Kirby Smith, in the same Vigenère cipher, with MANCHESTER BLUFF for a key, that Pemberton had used. Unfortunately the cipherer made errors; and the telegraphers made more, such as confusing R (– —) with S (– – –), I (– –) with a pair of E's (–). The message arrived hopelessly illegible. Kirby Smith spent twelve vain hours trying to read

* Full translation of the message in notes at end of volume.

it and finally had to send his chief of staff, Major Cunningham, riding round the flank of the Federal armies to find out what the garbled order had been.

It took too much time. When Cunningham reached General Johnston and learned what the order had been, Grant's hurrying regiments had already filed between. It was too late by this time for the order to be executed, or to have done any good if it had been executed. After that dismal failure instructions went down from Confederate general headquarters that messages were henceforth to preserve their original word divisions so they might not be hopelessly embroiled in transmission.

It was too bad that this safety system succeeded only in making the ciphers utterly unsafe.

Chapter X

CODE

I

It took the Franco-Prussian War to reveal publicly that the European powers had for some time been quietly concentrating on decipherment to the neglect of their own secret communications. The Germans entered that conflict still using Gronsfeld ciphers and with the concept that the fundamental weakness of the system could be offset by frequent changes of key, an idea which signally failed to work out. Napoleon III's officers were seldom in doubt as to the meaning of any message they intercepted, but they did not intercept many, and those they did get were of little value to them. The German armies operated in mass, with the high command close to the front; the French intercepts had only local importance, and meanwhile they were being fatally hurt by the loss of their own ciphers.

For France went into the war with one of those suppression-of-frequency ciphers containing numerous arbitrary code-words that had been used ever since Rossignol. The value of such ciphers is always a matter of degree, a question of how carefully they are put together, and how astutely used. The degree of Napoleon III's cipher seems to have been even lower than that of the first Bonaparte; it had only a few alternatives for the most frequent letters and practically none for syllables. In addition, it had originally been prepared for diplomatic rather than military use. As early as the first skirmishes along the frontiers Marshal Bazaine was telegraphing Paris that "the cipher for the transmission of dispatches is very inconvenient and contains none of the technical terms used in war."

That telegram excited the government offices enough to get them to work on a new cipher, but as usual with government

offices under the third Napoleon, they were too vague and slow. While the letters and numerals of the new cipher were still being arranged Marshal MacMahon clashed with the gray armies of von Moltke in the west and was beaten at Wörth. The Germans came streaming through the gap between his forces and those of Bazaine. The latter, driven north from the contact, tried to break through; was beaten at Vionville, beaten again at Gravelotte, and driven back into the fortress of Metz with nearly half the French armed forces.

The Germans laid siege to him there; southward, MacMahon and Napoleon drew in reinforcements and came up to break the circle of the siege. Now the question in all such cases is this: whether the relievers can concert time and place of attack with the besieged, so that both together will fall in mass on some point on the necessarily thin encircling lines around the latter. Fortunately for the French, Metz is set on and in the midst of high hills; the season was summer, whose bright days allowed easy heliograph communication across the summits. Unfortunately for them Bazaine still had only the old diplomatic cipher with "none of the technical terms used in war."

It had to be employed, since there was no other. Such perfect pattern-words as *ennemi, bataillon, artillerie,* had to be spelled out in simple substitution. Not half a dozen messages had been passed before the Germans had solved the whole thing. They concentrated opposite the spot of MacMahon's drive; Bazaine's sortie was broken, MacMahon dreadfully defeated and driven away northwest to the hills of Sedan, where French Army and French Emperor were forced to surrender together.

II

A few years before, the United States had experienced difficulties with another semi-code, though under circumstances by no means so serious. When government under the Constitution had been set up, back in 1789, an elaborate cipher of the Rossignol type was prepared for official diplomatic use, probably with the assistance of French experts, though there is no record

of who made the cipher. It contained nearly 1600 numbers, with representations for every possible English syllable, numerous values for each letter, and a considerable number of word-signs. It was in fact, almost a full code, as the term is understood today.

In the early years of the American Republic this code seems to have given good service. The number of ministers to foreign countries was small enough so it could be kept a secret from all but a few, and these few men of sufficient intelligence to handle with some skill the cumbersome processes of encipherment and decipherment. The close of the Napoleonic Wars brought about a change. Diplomatic questions were no longer so urgent as during the wars. During the more leisurely negotiations of a period of general peace it was possible to send out ambassadors who had received full instructions by hand. Since ships were no longer being held up and dispatches seized by the navies of the warring powers, the ordinary diplomatic mails carried in perfect safety all the messages it was necessary to communicate by correspondence. Thus it came about that from 1815 on, the American diplomatic cipher fell into disuse.

Even the Civil War, which restored haste and secrecy to diplomatic contacts, particularly those with England, failed to restore the big cipher to its old position. Persons high in the councils of the Lincoln Cabinet, such as Thurlow Weed, were continually making the trip to Europe as bearers of instructions, and dispatches were normally made safe by sending them on ships of the wartime navy.

But in 1866 came another in the series of inventions which have had so much to do with the revival of secret writing. The first transatlantic cable was laid. As soon as the long wire was in position the president of the cable company called on Secretary of State Seward. The company, said the magnate, was extremely anxious to get business. There were many persons anxious to transmit messages across the ocean, who were debarred from the new device by simple unfamiliarity. If the State Department would use the cable for its urgent official messages the patronage of the government would greatly help the company, and the company was so sensible of the benefit that reductions to "a very

reasonable figure" could be made from the ten-dollar-a-word price the public was being charged.

The moment was most opportune. Mr. Seward had just then some messages he wished to transmit to Europe with particular speed. In 1864 French fleets and troops had established the Australian Maximilian as Emperor of Mexico. The United States had been occupied with the Civil War at the time and made no protest, but the war was over now, and the Cabinet felt it was time to reassert the Monroe Doctrine. General Phil Sheridan was accordingly ordered to the Texas border with 50,000 veterans; and the news Mr. Seward wished to transmit to Europe in a hurry was that Sheridan and his 50,000 were only a raindrop in the storm that was coming unless the French troops evacuated the American continent.

It was not the type of message that can be sent in clear, for word of it leaking out would be almost certain to bring on strained relations and a war. Mr. Seward therefore sought a peculiarly safe and swift means of communication, and someone thought of the American diplomatic cipher, copies of which were on file in the major embassies in Europe. It had been used so little in recent years as to be as safe as any cipher could be. Seward accordingly put the message to Paris into the cipher and sent it along—about 1100 groups of three, four and five-figure characters.

It reached Paris, Sheridan reached the border and the French decided that it would be easier to clear out of Mexico than to fight a transatlantic war against a navy and army that were then the best in the world. Then the cable company's bill reached Seward. It was for $23,000.

He summoned the president of the cable company and demanded indignantly whether the latter considered this a very reasonable price for the transmission of 1100 number groups. The telegraph man replied that he considered it most reasonable. The English directors of the cable company had felt very strongly that there was something sneaking and unclean about secret code messages. It was only with the greatest difficulty and through the

personal efforts of Mr. Cyrus W. Field, the cable layer, that they had been persuaded to allow the transmission of such messages over their lines under any conditions. In order to discourage a practice they despised they had insisted that such messages be charged at double the normal rates.

Mr. Seward, not a man to be silenced on any subject for very long, inserted some observation to the effect that 1100 groups at twenty dollars a group, double the normal charge, made $22,000, and he did not call it a very reasonable reduction to boost this price by another $1,000 in billing the government.

The cable chief, harassed but firm, patiently begged to point out that his firm had established a rule that every figure in a number should be treated and charged for as a separate word. Thus 653 was not to be counted as one word, but as three—*six*, *five* and *three*. Now, he explained, there were 4600 figures all told in the cable message in question. At the rate charged to the public, double for cipher, this would come to $92,000. His company was therefore making a very great sacrifice, very great sacrifice indeed, in charging the Department of State only a quarter of this normal figure.

Mr. Seward replied that the rule about numbers was a flagrant piece of jobbery and the bill would not be paid. It was not paid; but that was the end of the famous State Department cipher, which had now been rendered useless for the only type of communication in which it would be of any value.

III

Similar, unreported incidents had probably been taking place in other parts of the world, for the majority of the transoceanic cables then being laid so rapidly were in the hands of British companies connected through dovetailing directorates. With the complete failure of the means of secret communication in the Franco-Prussian War, it probably had much to do with the maturity of the full code, which now soon made its appearance. As in many cases in the history of ciphers, no date or place can be

assigned; codes are an obvious product of the cable, with its high rates and emphasis on getting a great deal of meaning into a very few letters.

The commercial codes appear to antedate the military, and almost at once assumed their ultimate form—dictionaries of words and phrases, for which in transmission are substituted words or pronounceable groups of letters (usually five). Military codes were certainly not in use at the time of Marshal Bazaine's defeat, but seven years later one was being used and was getting the users into trouble.

It came in 1877 along the frontier where Russia was at war with a Turkey that then included most of what now forms the Balkan nations. The front was along the Danube, where that river courses through the great plains, a good march north of the Roumelian Mountains. North beyond the stream the Russians won a battle, threw a bridge of boats and began to file an army to the other bank.

West and upstream from the crossing was the fortress of Plevna, where Osman Pasha commanded for Turkey, with an army of thirty thousand men. His alternatives of action were to attack the Russians at the crossing, or to circle south to the mountain passes, adding his force to the main Turkish field army. Turkey, being what it was, the penalty for his making the wrong choice would be at least disgrace, possibly the loss of his head. He telegraphed to Constantinople for instructions; Constantinople replied in a new code that had just been prepared for the Turkish Army by experts from Germany.

The compilation of a code for naval or military purposes is a long and toilsome business. It consists of taking a fair-sized dictionary and assigning to every word in it some code-phrase, taking care that the code-signs do not themselves fall into alphabetical order:

Direct – AAEIU
Direction – QFCHJ
Director – BYMMP

A second dictionary for the translation of messages must now be

compiled, in which the code-signs are in alphabetical order, but the words in indirect:

AAEIU – Direct
AAEIV – Cavalry
AAEIW – Useless

As many copies of both books must now be printed as will be needed, and it is of the highest importance that the editions of both books shall be small and shall be intrusted only to persons who will not lose them, and can be trusted not to misuse them.

Osman Pasha himself did not have a copy of the special limited edition of the new Turkish Army code-book. The officer who did have it, one Selim Bey, had gone on an inspection trip farther upstream, not letting the code-book leave his person, as he had been most carefully instructed. Osman accordingly found the reply to his request for orders completely unreadable. He sat still for twenty-four hours, waiting for the return of Selim Bey with his code-book, but a patrol of Cossacks had cut in between the two officers and Selim did not get back that night or the next.

A day later it was too late; the Russians had pushed an army corps across their bridge, had cut Osman's own communications with Constantinople and surrounded him in Plevna. He defended the place with magnificent courage and great intelligence for four months, but that only staved off the ultimate surrender.

IV

On October 31, 1894, *La Libre Parole,* a Paris newspaper of strongly anti-Semitic tendencies, scored a scoop. It announced, under screaming headlines, that there had been treason in the General Staff of the French Army. An officer of that organization had been caught in the act of selling mobilization plans to the powers of the Triple Alliance of Germany, Austria and Italy, and was now in prison, waiting trial by a secret court-martial. Who was this scoundrel? "Look for him among the Dreyfuses, the Meyers, the Levys—the wealthy Jewish families which are ruining France."

Next morning the paper again scooped its rivals with the announcement of the name of the traitor—Captain Alfred Dreyfus. For a month and a half, or until the verdict of the court was announced, the scandal was the subject of scorching newspaper comment. On December 19 came the announcement of the verdict—guilty; and that of the punishment—public degradation and the confinement of the prisoner in perpetuity in the French penal colony of Cayenne. It satisfied everyone but the Socialist press, which complained indignantly that if a French private had been guilty of Dreyfus' crime, he would have been shot. It was only because the man was wealthy, an officer, and a Jew that he had got off so lightly. Meanwhile the sentence was carried out, Dreyfus being established in a hut on a pocket-handkerchief of land near the main prison of the colony. The name of that place was Devil's Island.

On June 1, 1895, the regular rotation of French Army commands brought Colonel Picquart to the head of the Intelligence section. In going over the files left by his predecessor, he found that the mobilization plan Dreyfus was supposed to have sold to the Triple Alliance had been prepared in the Operations Division of the Army, but had not yet been communicated to the General Staff at the time of the treason. This was puzzling; how could Dreyfus have sold a plan he had never seen? Picquart put the agents of his department to work; they turned up the original of a *pneumatique* message from Colonel Schwartzkoppen, the German military attaché at Paris, to a Captain Esterhazy of the very Operations Division which had drawn up the mobilization plan in question. The text of the message showed that at the least Esterhazy had been a good deal more dependent upon Colonel Schwartzkoppen than any French officer should be on any German.

Now thoroughly aroused, Picquart had Esterhazy's activities investigated; found that he kept an expensive mistress and was in debt; spent more money than could be accounted for by any normal means. A little quiet burglary of Esterhazy's quarters disclosed that he had in his possession the key of a cipher. It was

a complicated transposition scheme, such as had never been used by any French government department, but of a type quite common in Germany.

A year of this sort of work and Picquart went before the high Army command with what he considered adequate proof that Esterhazy had sold the mobilization plans and was still a spy in German pay. To his surprise and disgust Colonel Picquart was immediately removed from the Intelligence Department and sent on a long expedition into the interior of Tunis. His place at the head of Army Intelligence was taken by a Colonel Henry, an intimate of Esterhazy.

When Picquart returned, two years later, he found the Dreyfus affair all over the newspapers and French opinion of every shade in a state of super excitement for or against the man on Devil's Island. Emile Zola, the greatest literary figure of France, was in the midst of a terrific attack on the Army and the Government. Picquart plunged into the controversy, just as Zola was brought to trial for libel. The writer was convicted, sentenced to a huge fine and a term of imprisonment; the officer arrested and sent to a fortress. M. Cavaignac, the minister of war, appeared before the French Chambers and justified the government's action by reading several documents. The most important of these were a series of communications involving Dreyfus with Panizzardi, the Italian military attaché at Paris. Two were letters from Panizzardi, one to Dreyfus, written in 1894, the other to his home government, written in 1896. Both had been torn up, but the fragments had been resurrected by Colonel Henry and patiently pieced together. Another was a telegram in code, a numerical code, from Panizzardi to his home government, sent on November 2, 1894, the day after the Dreyfus story reached the press. The French Army decipherers had managed to break down the code and had read:

> Captain Dreyfus has been arrested. The Ministry of War has announced proofs of secrets offered to Germany. If the captain has had no direct dealings with you it would be well to publish a denial. My emissary has been warned.

This was extremely convincing, but the conviction did not last long. Less than a month later, Captain Cuignet, an Army expert on questioned documents, who had been asked by Minister Cavaignac to check the Panizzardi letters, was examining them at night. They were written on ruled paper, and Cuignet was surprised to discover that although all the faint lined markings had appeared by daylight, one set had become pale gray under artificial illumination. The astonishing thing was the discovery that neither the gray nor the true blue markings persisted through either letter. Both had been made up, then, of fragments, samplings from two different kinds of paper. The fact was so odd as to be altogether impossible, considering that both had been torn up and then pieced together, with the tears coinciding. Moreover the lines of writing in many cases crossed the tears where two pieces of paper of different types joined, a pen-stroke begun on a piece of blue-line paper continuing right over onto a piece of gray-line paper.

There was only one way this could have come about. The two pieces of paper must have been torn up together while one lay over the other; the fragments then assembled, and the writing placed on them last of all. Since one letter was dated 1894 and the other 1896 they must therefore both be forgeries. Colonel Henry, chief of the Intelligence Service of the French Army, had produced these forgeries and stood sponsor for them.

And the Panizzardi telegram? The French Black Chamber stood sponsor for the decipherment of that document. At this point it seems to have occurred to Captain Cuignet that it, too, might be a fake; before reporting to Minister Cavaignac the results of his examination of the letters, he went around to the deciphering department.

He found considerable agitation there. The Black Chamber experts explained that when Panizzardi had sent his code telegram to Rome, the Ministry of Posts and Telegraphs had, as was required by regulations, submitted a copy of it to the Black Chamber for decipherment, and in view of the excitement over the Dreyfus case, had made a special request for speed. The telegram was composed of groups of four figures. In the laboratory

where such material poured through in a daily stream, these groups were readily recognizable as those of a dictionary code made up by one Baravelli, consisting of ninety-nine pages with ninety-nine lines to a page. The message was made up by sending page and line number of the page desired—1021 signifying page 10, line 21.

When the numbers in the Panizzardi telegram were looked up in this dictionary, it was found they did not make sense. The cipher experts reasoned, as any decipherer would under the circumstances, that a mathematical formula had been used in connection with the Baravelli code. That is, a set of numbers had been prearranged between Panizzardi and his government. Before sending a message one of these numbers would be added to or subtracted from the reference number to the Baravelli code. Suppose the first number of the formula were 111. The Baravelli code-number 1021 would thus be sent as 1132.

The decipherers had a copy of the dictionary; by experiment it was possible for them to discover the formula and to read the message. This was how the translation of the Panizzardi telegram had been made. It had been handed in, the day it was made, back in 1894, as Minister Cavaignac had read it. But the formula by which the Baravelli numbers was modified had proved to be both cumulative and variable. The decipherment of the last phrase of the telegram was by no means certain when it had been handed in, and a note had been attached to this effect. During the following days a careful check on the decipherment process had been instituted. It had been found that the last phrases were probably improperly deciphered, and a new version of the decipherment was made. This new version was radically different from the first:

> Captain Dreyfus has been arrested. The Ministry of War has announced relations with Germany. If he has had no direct dealings with you, it would be well to publish a denial to prevent unfavorable newspaper comment on us. We do not know him here.

Obviously, instead of condemning Dreyfus this version completely exonerated him. Was there any certain method of telling

which was the correct reading? The French Black Chamber experts thought of a very clever one. They made up the text of a secret message, using exactly the same number of words as the Panizzardi telegram, and choosing the words from the same pages of the Baravelli dictionary. This message was supposed to be from a French spy, operating somewhere in Italy:

> Monsieur X, now operating at the city of Y, will leave for Paris within a few days. He will take with him a document relating to Italian mobilization plans which he has obtained from a government bureau there. Present address, Z Street.

This fake was allowed to fall into Panizzardi's hands through an arranged accident. It was too important for him to neglect, nor did he neglect it, telegraphing it straight to Rome. Of course he used the Baravelli code with the same mathematical formula variations. With both the clear and encoded messages before them, the latter encoded with the same pages of the Baravelli as the Dreyfus telegram, the cipher experts had no difficulty in arriving at the true mathematical formula used. When this formula was applied to the Dreyfus telegram it was clear that the second reading of the Dreyfus telegram had been correct. Dreyfus was innocent, and the Black Chamber experts had so reported.

What Captain Cuignet learned in his call was that somewhere between themselves and Minister of War Cavaignac this second version of the Panizzardi telegram and the report that Dreyfus was innocent had gone astray. To whom had these reports been given? To Colonel Henry, of course, as chief of the Army Intelligence section.

Cuignet went to Minister Cavaignac at once; Cavaignac called Henry in, and in an excruciating twenty-minute interview extracted from him confessions both of the forgeries and of the suppression of the cryptographic evidence. Henry, placed under arrest, wrote an anguished letter to his mistress and then cut his throat. Cavaignac was forced to go before the Chambers again with a statement that he had been horribly deceived by a scoundrel, and to resign with the concluding words that "the crimes of Henry do not prove the innocence of Dreyfus."

At the very least, however, they proved that Henry had found the case against Dreyfus so very weak that it needed artificial respiration. There was a long period of political profit-taking before the evidence of the telegram got before the courts, but when it did Esterhazy was condemned, Dreyfus released and honored, and Colonel Picquart promoted to general.

CHAPTER XI

THE WAR OF THE CRYPTOGRAPHERS

I

THE year 1880 is a key-date in the history of ciphers. The experience of the Franco-Prussian and the Russo-Turkish Wars had now confirmed what the American Civil War had foreshadowed—that an age of mass armies had come, in which it would no longer be possible for the general to keep his battle under observation and to control its course by aides carrying word-of-mouth orders. He must work from the map, and map strategy demands communications fast as lightning, fast as the electric telegraph, and secret as the grave. Ciphers had been raised from the status of something a soldier could have with advantage to something he must have.

For the ineffectiveness of the elaborate printed dictionary code had been spectacularly demonstrated. With somewhat less spectacular certainty it had been shown that the value of ciphers in military operations depended less upon the inherent qualities of the cipher used than upon the skill of the operators. The key-date, 1880, saw this realization sweep across Europe; every one of the great military powers added a course in cryptography to its system of military instruction.

A prodigious number of fresh minds were thus brought to bear on the problems of an art which had been as recondite as the tasting of tea. There was an outburst of books on the subject in almost every language but English and a wholesale restatement of the problems of the art.

The characteristic of cryptography in practical use which most forcibly impresses a new mind at first glance is probably the enormous amount of error in handling messages under the military conditions of hurry and strain. Yet where the conditions are

most hurried and strained is precisely the point where error can least be afforded, as was demonstrated by the Johnston-Kirby Smith message in the Civil War. The first efforts of the new cryptography, therefore, seem to have turned in the direction of the more accurate writing and reading of ciphers. Thus in France the military academy of St. Cyr produced a device which did away with one of the chief sources of error in handling Vigenère type ciphers—the reconstitution of the elaborate letter-tableau, and the user's tendency to let his attention wander for just so long as was necessary to choose a letter from the wrong line or column.

This device is known as the St. Cyr ruler, and designed after the ordinary slide rule, consists of a fixed and a sliding portion. On the fixed portion appears an alphabet. The slide has two, one after the other, with the spacing between the letters the same as in the fixed alphabet. In use, the slide is adjusted so that the first letter of the key-word (on the slide) stands beneath the A of the fixed alphabet. If the first letter of the clear be, for instance C, there will now appear on the slide under C of the fixed alphabet the correct equivalent in Vigenère cipher:

Fixed ABCDEFGHIJKLMNOPQRSTUVWXYZ
Slide...QRSTUVWXYZABCDEFGHIJKLMNOPQRST.

V is written down; the slide is maneuvered till the second letter of the key appears under the fixed A; the correct cipher equivalent will be found under the second letter of the clear, and so on. The result can readily be checked by writing alphabets on slips of paper and comparing the results of enciphering a message by this means with the results obtained from the ordinary Vigenère tableau on page 120.

The method obviously makes both writing and reading Vigenère ciphers very rapid, and greatly decreases the possibilities of error. At about the same time as its public appearance, an English admiral, Sir Francis Beaufort, was struck with another idea, both for simplifying the writing of the Vigenère and for making it harder to decipher. He built up a Vigenère tableau in

the classical fashion, but instead of placing the index letters at the top and left as Vigenère had done, put them at the right alone. His process of encipherment was now just the reverse of that used by Vigenère.

That is, he wrote down the clear with the repeated key-word beneath:

Clear	C O M E H E R E
Key	T U R N I P S T

Now he chose the column at the head of which stood the first letter of the clear; ran down it till he encountered the first letter of the key, and for the first letter of the resulting cryptogram wrote the index letter, which was in his tableau at both left and right of the line in which that letter of the key appeared. The result is quite different from that obtained by the normal Vigenère process:

Clear	C O M E H E R E	
Key	T U R N I P S T	
	R G F J B L B P	*Beaufort method*

While these elementary improvements in encipherment were taking place, decipherment also was being studied, and one day the Black Chambers of the world woke with a start to the fact that they had no more secrets. For the St. Cyr ruler was merely a method of writing the Vigenère which Kasiski's method had rendered unsafe, and very little experiment showed that the Beaufort system was the same, in effect, as the use of a St. Cyr ruler in which the letters on the slide appeared in the order:

A Z Y X W V U T S R Q P O N M L K J I H G F E D C B

In other words, every letter in the Vigenère system except A had a "complement" in the Beaufort system. In deciphering a message which had already been identified as a double substitution of the Vigenère type, it was merely necessary to draw up a table of these complements:

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z	
A Z Y X W V U T S R Q P O N M L K J I H G F E D C B	

When a decipherment was made it was only necessary to set down both the resulting letter and its complement; one or the other would be correct.

II

The step that followed was so obvious that nobody ever claimed credit for taking it. The possibility that the encipherer had used an ordered but reversed alphabet in his tableau or slide (the Beaufort) obviously forced a decipherer to double his labor. Would it not multiply the decipherer's work to the point of impracticability to place on the slide of the St. Cyr ruler a wholly disordered alphabet? Suppose a key-word be chosen, as in writing the type of simple substitution that employs this step; a key-word which uses one or more letters near the end of the alphabet so that its order will be altogether thrown out:

NEWYORKABCDFGHIJLMPQSTUVXZ

and this line of letters used on the slide. A Vigenère tableau constructed with this line of letters at the top would then begin:

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	n	e	w	y	o	r	k	a	b	c	d	f	g	h	i	j	l	m	p	q	s	t	u	v	x	z
B	o	f	x	z	p	s	l	b	c	d	e	g	h	i	j	k	m	n	q	r	t	u	v	w	y	a
C	p	g	y	a	q	t	m	c	d	e	f	h	i	j	k	l	n	o	r	s	u	v	w	x	z	b
D	q	h	z	b	r	u	n	d	e	f	g	i	j	k	l	m	o	p	s	t	v	w	x	y	a	c
E	r	i	a	c	s	v	o	e	f	g	h	j	k	l	m	n	p	q	t	u	w	x	y	z	b	d
F	s	j	b	d	t	w	p	f	g	h	i	k	l	m	n	o	q	r	u	v	x	y	z	a	c	e
G	.	.	.	.	.	.	.																			

and the result of encipherment, with the key-word TURNIPS, the clear *COME HERE* and a St. Cyr slide of the disordered alphabet in use is:

V D M O T U F Z

which is altogether different from either the VIDRP TJX obtained from the normal Vigenère or the RGFJB LBP that results from the encipherment by the Beaufort method.

It was soon discovered that this result eliminated nothing but the Kerckhoffs short cut with its search for the key-word. A

cipher written in this fashion was still as vulnerable as the straight Vigenère to treatment by the Kasiski system of decipherment which does not ask that the letters of the tableau be in any particular order. This eliminated the Irrational Alphabet Vigenère (as it is called) as a military cipher; the number of messages from even a divisional headquarters in time of war is such that there would be plenty of material for the application of the Kasiski decipherment system.

Therefore another school of cryptographers arose, who attacked the problem of the military cipher from a different angle. Their point of departure was the desirability of eliminating the specific weakness of which the Kasiski method made use—the length of the key-word. It is obvious that the use of a long key-phrase instead of a simple word—say a line of poetry or an easily memorized proverb—will greatly complicate the task of a decipherer who uses the Kasiski system. The idea became very popular for a while (it will appear here later), but it only avoided Kasiski to fall in the lap of Kerckhoffs unless an irrational alphabet were used on the slide (in the tableau), and in that case proved to complicate the task of writer and reader of the message quite as much as it did that of a possible decipherer.

For Kerckhoffs advised using the key-word's length only when that could be readily obtained; in other cases, he recommended attack through collecting several messages presumably enciphered with the same long key, writing them down in such a manner that the first letter of message No. 1 fell in line with the first of messages Nos. 2, 3, 4, 5, etc., and extracting the key by this method.

The next new concept was one to render this method inoperative, by allowing every message to have a different and very long key, not possible if the keys had to be memorized, but easily possible in another way. Each message was to provide its own key, and the key was to be as long as the message with which it is written. This is the Autoclave cipher.

It starts with a key of a single letter. This letter is used to encipher the first letter of the clear. Either the resulting enciphered letter, or the first letter of the clear itself is used as

key-letter to encipher the second letter of the clear; again the result, or else the second letter of the clear, is used as key-letter for the third of the clear, and so on. Using the straight Vigenère and the key-letter B, *COME HERE* thus enciphers itself in the two versions:

Result of encipherment as key	D	R	D	H	O	S	J	N
Clear as key	D	Q	A	Q	L	L	V	V

The system has the advantages of overthrowing both the Kasiski and Kerckhoffs methods of solution. It permits frequent and rapid changes of key—by using a twelve-letter word as main key, it is possible to use a different key letter for each hour of the day, the letter used depending upon the hour of the dispatch of the message. On the other hand the Autoclave has the serious operational difficulty that whichever of the two methods is used, error vaults on the back of error; one mistake in encipherment is enough to throw all the rest of the message out as gibberish.

Also it develops a method of decipherment all its own. When the cipher has been used as a key, an interceptor, given that he suspects an Autoclave, has only to try decipherment of each letter in turn using the one preceding it in the message as key. Four or five letters are enough to prove whether he is right—an absurdly simple process. Autoclaves in which the clear has been used as key solve out readily through the peculiar behavior of the letter A. Obviously when any letter has been enciphered with A as a key the result is the letter itself; and when *A* of the clear has been enciphered with any letter as key, the result is again the letter itself. Thus, when A occurs in the clear, the resulting cryptogram will contain two letters of the clear, just as they were, but without A between them:

Key (beginning with C)	C	L	E	A	V
Clear	L	E	A	V	E
Autoclave message	N	P	E	V	Z

Note the presence of EV in the message, letters which were part of the clear, here reproduced without their intervening A. The decipherer has only to run along the message, inserting A

in each successive bigram and trying the resulting trigram as a key. In the present case NAP would yield nothing of value; PAE also nothing, but when EAV was reached the message would solve out both forward and backward, for an Autoclave has the peculiarity that when one letter is correctly solved all the rest follow.

III

There remains one more system of all those that rose from the death of the Vigenère tableau, the best and most persistent of all—the Pinwheel or Disc cipher. It is still popular today, and most of the ciphering machines marketed by various European firms are no more than mechanical devices for producing particularly elaborate disc ciphers.

No more than in the case of irrational alphabets or the Autoclave has anyone laid claim to the invention, but it probably developed out of the St. Cyr ruler, for the device is no more than a St. Cyr ruler turned around to bite its tail. It consists of a fixed or "clear" disc, like the fixed alphabet on the ruler, with the letters written round the rim, and a mobile or "cipher" disc concentric with it, which fulfills the function the slide does in the ruler. In the simplest form of disc cipher the operator begins by placing A of the mobile "cipher" disc opposite A of the fixed "clear" disc; enciphers one letter (substituting for the letter of the clear the letter which appears opposite it on the mobile "cipher" disc); rotates the mobile disc one space, to bring B of the mobile opposite A of the clear disc; enciphers another letter; rotates one place again and enciphers his third letter, and so on. *COME HERE* comes out as:

C P O H L J X L

which is the same result that would be reached by enciphering with a straight St. Cyr ruler, Vigenère system and a key twenty-six letters long, beginning ABCDEFGHI . . . and continuing through the alphabet.

Of course, the period of rotation need not be one space; it can be two, three, four, any number. But whatever the number this type of Disc cipher is even easier to solve than the Gronsfeld by the method of repeated alphabets. (See page 123.) When a message of this type is placed before a cryptographer he identifies it as double substitution by the abnormal letter frequencies (no frequencies much higher than the rest, none outstandingly lower); eliminates the possibilities of straight Vigenère, Gronsfeld or Beaufort by the lack of repeated bigrams and trigrams, and eliminates the possibility of an Autoclave when the cipher fails to respond to treatment with the letter A. Disc cipher is now a strong possibility. The message is written down with an alphabet backward under each letter as for the Gronsfeld:

C	P	O	H	L	J	X	L
B	*O*	N	G	K	I	W	K
A	N	*M*	F	J	H	V	J
Z	M	L	*E*	I	G	U	I
Y	L	K	D	*H*	F	T	H
X	K	J	C	G	*E*	S	G

The interceptor has only to lay a ruler along a diagonal line from the first letter down. If a period of two rotations between each pair of letters has been used, the ruler, which can be fixed on a pivot at the first letter of the message, need only be swung till it covers the oblique representing such a period:

C	Q	Q	K	P	O	D	S
.	P	P	J	O	N	C	R
.	*O*	O	I	N	M	B	Q
.	.	N	H	M	L	A	P
.	.	*M*	G	L	K	Z	O
.	.	.	F	K	J	Y	N
.	.	.	*E*	J	I	X	M

Thus the length of the period makes no difference; the ruler solves all difficulties.

This became obvious quite early in the game, and the cipherers began to discount the repeated alphabet by applying Gronsfeld mathematical formulas to Disc ciphers, which made it quite an-

other matter. Suppose the key requires the encipherer to rotate the mobile disc one place after the first letter; then successively, three places, none, back one, and forward two, making the complete key 1–3–0–minus 1–2. The result of enciphering *COME HERE* with a disc now becomes:

C R P G L J Z M

and when the repeated alphabets are set up the clear follows a rambling path through them:

C	R	P	G	L	J	Z	M
B	Q	O	F	K	I	Y	L
A	P	N	*E*	J	H	Y	K
Z	*O*	*M*	D	I	G	W	J
Y	N	L	C	*H*	F	V	I
X	M	K	B	G	*E*	U	H
W	L	J	A	F	D	T	G
V	K	I	Z	E	C	S	F
U	J	H	Y	D	B	*R*	*E*

The weaknesses of such a message are concentrated at its beginning, where the letters of the clear necessarily come close to the tops of the columns. This makes it possible to analyze the beginning of the cipher for bigrams and trigrams by mathematical probability, as described in the method for the Gronsfeld cipher (Chapter Six, III), but cryptographers were not long in discovering and correcting this weakness. One method is to place a prearranged number of nulls at the head of every message; another and still better one is to cut the message in two or three parts after enciphering it and send the latter parts first.

In addition, it has occurred to various persons at various times that a Disc cipher could be made almost unsolvable by lettering around the mobile disc, not an alphabet in normal order, but an irrational or incoherent alphabet. No solution through repeated alphabets will now solve the cipher, particularly if the latter part be sent first. There remains, however, a method of solution called that "of mathematical co-ordinates," based on the fact that no matter how a Disc cipher be complicated, it still produces the same results as a Vigenère with a long and incoherent key.

This method can be briefly described without specific illustration. Suppose a doubled letter be enciphered on the straight Vigenère system, with any two letters for a key:

Key	B	E		D	A		J	M	
Clear	L	L		L	L		L	L	
Message	M	P		O	L		U	X	

The distance from B to E in the alphabet is 3 letters; that from D to A, minus 3 (or 23, around the circle); from J to M, 3. Since the difference from L to L is zero, the result of enciphering the pairs of L's with these letters as keys makes the resulting letters of the cryptogram fall exactly the same distance apart in the alphabet as the letters of the key. That is, the "mathematical co-ordinates" of the key are unchanged.

This shows the use of mathematical co-ordinates in their simplest form, but the same method of co-ordinates is operative against any set of letters. Suppose the clear contains two letters, any two letters whatever, whose mathematical relation to each other can be determined, say S and T, where the mathematical co-ordinate is 1.

Key	B	E	Mathematical co-ordinate, 3
Clear	S	T	Mathematical co-ordinate, 1
Message	T	X	Mathematical co-ordinate, 4
Key	D	A	Mathematical co-ordinate, −3 (or 23)
Clear	S	T	Mathematical co-ordinate, 1
Message	V	T	Mathematical co-ordinate, −2 (or 24)

The co-ordinate of the resulting bigram in the message is thus the sum of the co-ordinates in key and clear. In a message of any length it will frequently occur that common bigrams of the clear (*TH* or *AN*) will be enciphered in several cases by similar sections of the key, that is, portions of the key having the same mathematical co-ordinates as each other. By an analysis of all the mathematical co-ordinates in a given message, it is possible to establish the most common sets of co-ordinates. The distances, in the message, between these pairs of repeated co-ordinates, can

now be factored, as the distances between repeated bigrams are factored in the Kasiski method. The result is the length of the formula used for encipherment; and when this is obtained, the formula can be broken down into its constituent elements and used to re-encipher the message in straight Vigenère, after which it can be broken down like any Vigenère cipher.

IV

The method is of German origin; is ingenious, tortuous, difficult of application and fairly certain in the right hands. Long before it became public knowledge a better one had been discovered, which rendered all ciphers based on the Vigenère tableau forever unsafe.

The 1890's saw a series of terrific financial scandals in France. Cabinet members were involved, a president of the republic had to resign under a cloud, and the Dreyfus case seemed to connect the great financial families with treason as well as with shady monetary transactions. The royalist party was strong and had received the support of the powerful anti-Semitic movement. In 1899, with the help of Colonel Henry and his forged documents they were triumphantly keeping Dreyfus on Devil's Island, and they had the support of most of the press and the larger portion of the public. When doubts began to be thrown on Dreyfus' guilt, the first reaction was that the government had been bought out to prove his innocence.

If the Royalists were to strike they could hardly choose a better time, and as a matter of fact the royalist press became very violent about this time in pointing out that the republic was hopelessly rotten and the only salvation for France lay in the restoration of the Bourbons. At the same time the French police learned a good deal that led them to doubt whether the movement for a king was confined to the press. The leader of the royalist party was Déroulède, the poet; for several weeks he had been receiving mysterious communications, consisting of series of numbers, the origin of which was traced with certainty to the group surround-

ing the Duc d'Orléans, pretender to the throne, who was living in exile. Copies of these messages were obtained steadily; the difficulty was that it was beyond the powers of the police to decipher them.

They turned the Orléans letters over to the Army Cryptographic Department, at the head of which then stood the same Commandant Bazeries who had deciphered the Great Cipher of Rossignol. His preliminary examination of the documents showed that the messages consisted of four-number groups, in which there was no number below 1111 and none above 3737; nor for that matter was any number represented between 1137 and 1211; 1237 and 1311, and so on. As any sensible man would, Bazeries concluded that these were sets of two-number groupings, and when he broke them up he had a series of numbers from 11 to 37. The variation was not wide enough to be a code. A frequency count showed the irregularities characteristic of the Vigenère type cipher, and the fact that there were twenty-seven different numbers instead of twenty-six made it look like a Beaufort, since in the Beaufort system the index letters form part of the tableau itself, with the A-column repeated at the end of the tableau.

But the messages had apparently been composed with great care to avoid repeated bigrams and the keys of the five messages that reached Bazeries were evidently different, for they failed to give up their secrets to the Kasiski method of decipherment. Mathematical analysis would probably break them down in time, but the process was slow. Bazeries accordingly translated the messages into letters, treating 11 and 37 as A, 12 as B, etc., and attacked the problem with a St. Cyr ruler.

The peculiarity of all Vigenère type ciphers is this: the positions in the tableau of the three letters that go into the making up of any cryptogram (that is, the letters of key, clear and message), form a right-angled triangle, and with or without the rule, anyone knowing two of these elements can obtain the third, since the problem is merely the geometrical one of deducing the whole of a triangle when one is in possession of two angles and a side. In the ordinary Vigenère, the letter of clear or key occupies a

point at the top of the tableau (or at the side), that of the clear at the side or the top. To the sender of a message in straight Vigenère the message point is lacking:

	K			C	
		or			
C	?		K	?	

The recipient of the message also has two elements of the triangle to find the third:

	?			K	
		or			
K	M		?	M	

In the Beaufort system the process of enciphering and deciphering is the same, with only the designations changed. To encipher in Beaufort one has:

	K	
?	C	

and to read a message:

	K	
M	?	

Bazeries had only one of the three elements—M. Would it not, he asked himself, greatly speed his work, to assume that he had two, find the third resulting from the two assumed, and inquire whether this third element had logic and consistency? In other words, Bazeries sought to choose some word that was probably present in the clear, bring it into its proper relation with part of the message, and examine for probabilities the resulting key that solved out. He was, in short, assuming that his triangle was:

	?	
M	C	

The process was essentially the same as that of encipherment or decipherment in the Vigenère system and could be performed with the ordinary St. Cyr ruler.

He, therefore, started by assuming that the name of Déroulède began the first of the five messages before him, and tried the extraction of the result by putting that name on the ruler with the first group of letters in the message, which happened to be AWKNZP. The result, if the supposition of Déroulède's name were correct, should be the key; but the result in this case was DABBTA, which seemed most unlikely to have been the key and did not work when applied to the remainder of the message.

If Déroulède's name did not begin the message, perhaps that of Thuret, another prominent royalist, did. Bazeries tried the same process again. The result was TDEEDI, which was quite as unlikely as the first effort. Or not quite; for the *-EDI* termination to this gibberish word is the common ending for the names of the days of the week in French as *-DAY* is in English. Of all the French names of the days of the week, only one, *SAMEDI,* was six letters long, as required for the opening group of the message to make the *-EDI* fall in the proper place. Bazeries tried it as a key; the first word of the message solved out neatly as *SECRET,* and all the rest of it fell into line. When the names of the days of the week on which they were written had been tried as keys for the other messages they also broke down.

In less than twenty-four hours Bazeries laid before the police a partial, but highly significant, narration of royalist plans to take advantage of the agitation accompanying the Dreyfus scandals. On the first occasion that would bring crowds into the street in a state of emotion, open revolt against the republic was to be proclaimed. Certain elements in the Paris regiments of the Army had been approached and would place themselves at the head of the rising if it showed signs of being a going concern. The plot was complete and detailed enough to cause serious worry to both police and the higher departments of the government, and while they were worrying, the president of France, Felix Faure, suddenly died. A big public funeral was obligatory—exactly the kind of occasion the royalists had been waiting for.

The funeral was a very imposing affair. Even Paris, accustomed as it was to great displays, was astonished at the number of troops

that followed through the streets in full war equipment, many of them from stations as far distant as Belfort, Maubeuge and Brest. Déroulède was there to set things going; he delivered a wild harangue, urging Frenchmen to rise against the republic. The crowds were sympathetic; they even cheered him, then looked at the rumbling artillery in the streets and went home to dinner. The poet-conspirator rushed off to the barracks where the Paris regiments were quartered, delivered another speech and attempted to parley with General Roget. He was instantly arrested for treason; so were the few men who left their quarters to join him.

The trial ended with acquittals all around. In the government offices it was felt better to keep Bazeries under cover than to reveal anything about the Déroulède messages, and without these messages, there was practically no evidence against the poet. His rambling, flowery speeches had not been taken down by stenographers, and he had cloaked his exhortations in an imagery that made it easy for him to deny that he meant anything other than that the people should use the perfectly legitimate methods of the ballot box in attacking the government.

In spite of the care the government had exercised in keeping its cryptographic expert under cover either the secret leaked out or the royalists deduced that their messages were being deciphered. The days following the president's funeral were particularly rich in cipher messages from the royalist heads beyond the frontier; but when they reached the Black Chamber it was discovered that the key of the day of the week would no longer unlock them. Commandant Bazeries drew up a new list of probable words and tried again. Very little effort was needed to show him he was still dealing with a Beaufort cipher, now with a very long key, as long as the message itself; and very little more to show that this key was a long and involved sentence, in which Bazeries soon recognized one of the poems of Alfred de Musset. The next day's message proved to have as a key the succeeding stanza of the same poem, and when a standard edition of de Musset's works was consulted, each stanza right down the line

was clearly the right key to a day's correspondence. Once more the whole royalist communications system was laid bare.

But only for a short time. As the police drew in upon their operations the plotters changed systems again. Up to this time the de Musset poems had worked beautifully; now they suddenly began to yield utter gibberish. All the probable words Bazeries could think of gave the same result. Yet the cipher before him was so much like the rest, in frequency-count and general character that it was inadmissible that it should not be of the same type.

To the experienced cryptographer such a combination of circumstances has only one meaning: the royalists must have changed tableaux. Instead of using the plain alphabet of Vigenère they had employed an incoherent, or irrational, alphabet. (See page 204.) The classical solution for this type of cipher is the straight Kasiski method, for it is difficult to use with anything but a short key-word. Yet the key-word was not short in this case as a little experiment showed.

Herbert O. Yardley, the American cryptographer, has remarked that every cryptogram is in effect a separate problem for the solution of which the decipherer must devise a method of his own. It was the brilliance of Commandant Bazeries seldom to be at a loss for a new method. He reasoned that in this case, the key being a long one, the royalists had used the next stanza from the collected works of de Musset, for men's minds run in grooves. Therefore, the correct de Musset stanza for the day was K in the triangle of solution. He was assuming probable words, which gave him C in the triangle. Before him was the message, M of the triangle. What he really lacked then was only knowledge of how long the triangle's legs were:

K

.

? spaces

.

M . ? spaces . C

Also he knew C (by hypothesis) only for a very limited space in the message.

V

The problem before the French officer was one of the most difficult in all cryptography, and the method he used to solve it can best be illustrated by an example. Suppose the message to have been:

1	2	3	4	5	6
LAQFQ	YNSUA	XCWZI	JIJQU	GKXWV	EUTEN
7	8	9	10	11	12
IGQHB	WDZHI	HELBG	PNEOH	ASOSJ	ICEFD
13	14	15	16	17	18
BOZWB	RCZDH	KVGNP	VBKAC	FQRCH	QMFKT
19	20	21	22	23	24
BEYJJ	EAOHE	HGDFF	FZMHH	TPDGB	GVOWW
25	26	27	28	29	30
XMXFA	CBGAI	EKWXR	FCQLB	RYFKU	MPEJP
31	32	33	34	35	36
AJSFO	XXMGT	VUITL	FPUAE	APSQI	EQZBD
37	38	39	40	41	42
KIZTH	OOAGH	YMHCU	JCYWA	WXOMF	EPZSO
43	44	45	46	47	48
KRYWR	DQXGJ	UIHWQ	UQTQP	YDTPN	QUOJE
49	50	51	52	53	54
KKYYA	HZKDG	GCAUU	AHXGI	BYVCX	GFDYE
55	56	57	58	59	60
INFHO	CWSHS	GQVIU	SDZAW	TLPKV	NCAON

61
AZ

For the purposes of this demonstration it may be assumed that as in the case of the royalist messages the cryptographer has become reasonably certain: 1) that the cipher is a Vigenère, written with an irrational tableau; 2) that a very long key has been used, probably Mark Antony's speech over Caesar's body from Shakespeare's *Julius Caesar*—the "Friends, Romans, countrymen"

speech. In view of the contents of other messages and of the fact that this one has been sent through by the shortest possible route, it may further be assumed that this message begins with the word *URGENT*, followed by the name of Déroulède.

The first step is to set up parallels of key, clear and message for as much of the message as these hypotheses will cover:

Key	F	R	I	E	N	D	S	R	O	M	A	N	S	C	O
Probable clear	*U*	*r*	*g*	*e*	*n*	*t*	*D*	*e*	*r*	*o*	*u*	*l*	*e*	*d*	*e*
Message	L	A	Q	F	Q/Y		N	S	U	A/X		C	W	Z	I
Groups			1					2					3		

The important question to be solved is the arrangement of the letters in the tableau used for encipherment; that is, the order in which the letters appeared on the slide of a St. Cyr ruler, or around a pair of ciphering discs.

Thus, granting the hypothesis of the probable word, the encipherer of this message chose column F of his disordered tableau in ciphering the first letter, ran down it to line U and at the junction found *L*, the first letter of the message. The position of F among the letters at the top of the tableau is unknown, because the tableau has been disordered. But the index-letters at the side must be in their normal, rational order. If it were inverted to correspond with the inverted order at the top of the tableau, the result would be the same as though a normal tableau had been used.

To put it otherwise, and perhaps more comprehensibly, the index letters on the fixed portion of the St. Cyr ruler retain their normal order. Only the alphabet on the slide has been disarranged. Thus we know that a small portion of the tableau looks like this:

A	? spaces F
B	?
C	?
to	to
U	L
V	?

Or, that when F on the slide of the St. Cyr ruler was placed

under A of the fixed alphabet, L on the slide fell under U of the fixed alphabet:

```
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
. . . F . . . . . . . . . . . . . . . . . . L . . . . . .
```

Thus the distance from F to L in the irrational alphabet used in this case was the same as the mathematical co-ordinate A–U (Table XIII) or 20. This relation can be shown in a figure:

```
Equation   0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20
   I       F                                                  L
```

The reason for this will appear presently. Meanwhile the second letters of key, cipher and probable word are taken; and it is discovered that the St. Cyr ruler looked like this for enciphering the *R* of *URGENT*:

```
Fixed  A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Slide . . R . . . . . . . . . . . . . . . . A . . . . . . . .
```

Using the mathematical co-ordinate A–R, this can be figured:

```
Equation  0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17
   II     R                                        A
```

The process is now repeated with each of the sets of letters yielded by the probable words, and yields the following results:

```
III  0 1 2 3 4 5 6
     I         Q

IV   0 1 2 3 4
     E     F

V    0 1 2 3 4 5 6 7 8 9 10 11 12 13
     N                       Q

VI   0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19
     D                                           Y

VII  0 1 2 3
     S   N

VIII 0 1 2 3 4
     R     S

IX   0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17
     O                                        U
```

X 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14
M A

XI 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20
A X

XII 0 1 2 3 4 5 6 7 8 9 10 11
N C

XIII 0 1 2 3 4
S W

XIV 0 1 2 3
C Z

XV 0 1 2 3 4
O I

It is observable that several of these figures have letters in common. For example, IX and XV both embody O, and can be combined to make:

XVI 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17
O I U

The result is that the decipherer has obtained I's position with relation to U in the irrational alphabet used for the encipherment, a fact not before known. When all the possible combinations are made, the following results are obtained:

II 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17
R A
X 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14
M A
VIII 0 1 2 3 4
R S
VII 0 1 2 3
S N
XIII 0 1 2 3 4
S W
XII 0 1 2 3 4 5 6 7 8 9 10 11
N C
XIV 0 1 2 3
C Z
V 0 1 2 3 4 5 6 7 8 9 10 11 12 13
N Q
III 0 1 2 3 4 5 6
I Q
XV 0 1 2 3 4
O I
IX 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17
O U

All these figures can be combined into one omnibus equation:

XVII
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28
R M S N W O I A C Q Z U

Since there are only twenty-six letters in the alphabet U will have to be bent round to take its place beside R:

```
XVII
 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26
 R U   M S     N W   O          I        A C    Q Z
```

Three of the figures I, IV and VI have no letters in common with those of the omnibus figure XVII, but of these, I and IV will themselves combine separately:

```
IV  0 1 2 3 4
     E     F
I            0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21
             F                                                    L
```

to make a new figure:

```
XVIII
    0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25
    E       F                                                       L
```

There is no way of deciding where the E–F–L combination of figure XVIII and the D–Y of equation VI fit into equation XVIII. But within each of the completed figures that have resulted from the process, the letters bear to one another the same relations they did on the slide that went into the St. Cyr ruler with which the message was enciphered. From this fact values for many letters of the message can now be deduced. This can be made clear by diagramming the position of fixed alphabet and slide when *E* of figure XVIII is placed opposite A of the fixed alphabet:

```
Fixed  A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Slide..  E . . . F . . . . . . . . . . . . . . . . . . L .
```

This is essentially the same as figure XVIII, the only difference being that the numbers of the figure have been replaced by letters. In other words when E in this particular cipher is the key, F (of the message) = *E* (of the clear), and L = *Y*. Similarly:

```
Fixed  A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Slide..  F . . . . . . . . . . . . . . . . . . . . . L . E . . .
```

That is, when the key letter is F, F = *A*; L = *U* and E = *W*.

These relations can be expressed in tabular form for figure XVIII:

Key letter	E	E	E		F	F	F		L	L	L
Cipher letter	E	F	L		E	F	L		E	F	L
Clear	*A*	*E*	*Y*		*W*	*A*	*U*		*C*	*G*	*A*

Equation VI provides a smaller table:

Key letter	D	D		Y	Y
Cipher letter	D	Y		D	Y
Clear	*A*	*T*		*H*	*A*

And the omnibus equation, XVII, a very important one:

Key letter	R	R	R	R	R	R	R	R	R	R	R
Cipher letter	R	U	M	S	N	W	O	I	A	C	Q	Z
Clear	*A*	*B*	*D*	*E*	*H*	*I*	*K*	*O*	*R*	*S*	*U*	*V*
Key letter	U	U	U	U	U	U	U	U	U	U	U	U
Cipher letter	R	U	M	S	N	W	O	I	A	C	Q	Z
Clear	*Z*	*A*	*C*	*D*	*G*	*H*	*J*	*N*	*Q*	*R*	*T*	*U*
Key letter	M	M	M	M	M	M	M	M	M	M	M	M
Cipher letter	R	U	M	S	N	W	O	I	A	C	Q	Z
Clear	*X*	*Y*	*A*	*B*	*E*	*F*	*H*	*L*	*O*	*P*	*R*	*S*
Key letter	S	S	S	S	S	S	S	S	S	S	S	S
Cipher letter	R	U	M	S	N	W	O	I	A	C	Q	Z
Clear	*W*	*X*	*Z*	*A*	*D*	*E*	*G*	*K*	*N*	*O*	*Q*	*R*
Key letter	N	N	N	N	N	N	N	N	N	N	N	N
Cipher letter	R	U	M	S	N	W	O	I	A	C	Q	Z
Clear	*T*	*U*	*W*	*X*	*A*	*B*	*D*	*H*	*K*	*L*	*N*	*O*
Key letter	W	W	W	W	W	W	W	W	W	W	W	W
Cipher letter	R	U	M	S	N	W	O	I	A	C	Q	Z
Clear	*S*	*T*	*V*	*W*	*Z*	*A*	*C*	*G*	*J*	*K*	*M*	*N*
Key letter	O	O	O	O	O	O	O	O	O	O	O	O
Cipher letter	R	U	M	S	N	W	O	I	A	C	Q	Z
Clear	*Q*	*R*	*T*	*U*	*X*	*Y*	*A*	*E*	*H*	*I*	*K*	*L*
Key letter	I	I	I	I	I	I	I	I	I	I	I	I
Cipher letter	R	U	M	S	N	W	O	I	A	C	Q	Z
Clear	*M*	*N*	*P*	*Q*	*T*	*U*	*W*	*A*	*D*	*E*	*G*	*H*
Key letter	A	A	A	A	A	A	A	A	A	A	A	A
Cipher letter	R	U	M	S	N	W	O	I	A	C	Q	Z
Clear	*J*	*K*	*M*	*N*	*Q*	*R*	*T*	*X*	*A*	*B*	*D*	*E*

Key letter	C	C	C	C	C	C	C	C	C	C	C	C
Cipher letter	R	U	M	S	N	W	O	I	A	C	Q	Z
Clear	*I*	*J*	*L*	*M*	*P*	*Q*	*S*	*W*	*Z*	*A*	*C*	*D*
Key letter	Q	Q	Q	Q	Q	Q	Q	Q	Q	Q	Q	Q
Cipher letter	R	U	M	S	N	W	O	I	A	C	Q	Z
Clear	*G*	*H*	*J*	*K*	*N*	*O*	*Q*	*U*	*X*	*Y*	*A*	*B*
Key letter	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z
Cipher letter	R	U	M	S	N	W	O	I	A	C	Q	Z
Clear	*F*	*G*	*I*	*J*	*M*	*N*	*P*	*T*	*W*	*X*	*Z*	*A*

By hypothesis, the key is a known quantity. The equations have given the decipherer many new values for cases in which given key letters coincide with given letters in the message; and with these in hand many substitutions can be made in the message itself:

Groups	1	2	3	4	5
Key	F r i e n	d s R o m	a n s c o	u n t r y	m e n l e
Message	LAQFQ	YNSUA	XCWZI	JIJQU	GKXWV
Resultant clear	*URGEN*	*TDERO*	*ULEDE*	*.H.U.*	. . . . .

6	7	8	9	10	11	12
n d m e y	o u r e a	r s I c o	m e t o b	u r y C a	e s a r n	o t t o p
EUTEN	IGQHB	WDZHI	HELBG	PNEOH	ASOSJ	ICEFD
. . . *A*.	*E.U*. .	*I .H.E*	*.A* . . .	*.H.S*.	*.ATE*.	*E* . . . .

13	14	15	16	17	18
r a i s e	h i m T h	e e v i l	t h a t m	e n d o l	i v e s a
BOZWB	RCZDH	KVGNP	VBKAC	FQRCH	QMFKT
.THE.	*.ES*. .	. . . *T*.	. . . . *P*	*EN.I*.	*G.E*. .

19	20
f t e r t	h e m t h
BEYJJ	EAOHE
. . . . .	*. .H* . .

. . . . .

The process could be carried to the end, but already there is a good deal of material to work on. Identical letters in key and message can result only from the encipherment of the letter *A*. Therefore, H of group 14 = *A*.

A.E in groups 6-7 cries for *R* the only letter that occurs frequently between these two; and *H.S* in group 10 similarly de-

mands *I*. (See table XII.) When these values are assumed, two more figures result:

XIX 0 1 2 3 4 5 6 7 S 9 10 11 12 13 14 15 16 17
Y N

XX 0 1 2 3 4 5 6 7 S
Y E

The value of these figures is that they link up the two minor figures (VI and XVIII) with the omnibus figure (XVII). The appearance of the slide, as far as it is now known, is thus:

R U F M S . . N W . O . . . I . Y A C . Q Z L D E .

This permits many new values to be deduced—too many to set down in tabular form. An easier procedure is to make up a fixed alphabet on a strip of paper with a slide of the form given above on another and, applying the one to the other, make substitutions all through the message. The result:

Groups	1	2	3	4
Key	F r i e n d s/R o m a n s/c o u n t
Message	L A Q F Q/Y N E U Z/X C W Z I/J I J
Resultant clear	*U R G E N T/D E R O U L E D E/. H .*

	5	6	7	8
	r y m e n/l e n d/m e/y o u r/e a r s/I/c o
	Q U/G K X W V/E U T E N/I G Q H B/W D Z H I/
	U L . . . M . R E . A R E . U . . I T H . E

	9	10	11	12	13
	m e/t o/b u r y/C a e s a r/n o t/t o/p r a i
	H E L B G/P N E O H/A S O S J/I C E F D/B O Z
	. A . . . . H I S . T A T E . E . . S . . TH

	14	15	16	17
	s e/h i m/t h e/e v i l/t h a t/m e n/d o/ l
	W B/R C Z D H/K V G N P/V B K A C/F Q R C H/
	E . . E S . A . . . . . P E N D I .

	18	19	20	21	22
	i v e s/a f t e r/t h e m/t h e/g o o d/i s/o
	Q M F K T/B E Y J J/E A O H E/H G D F F/F Z M
	G . E . . . . S . . . T H . . . A N S F O R T

```
      23          24          25          26
  f t/i n t e r r e d/w i t h/t h e i r/b o n
  H H/T P D G B/G V O W W/X M X F A/C B G A I/
  . . . . . . . . . . N A U . . . . T E . . H H

      27          28          29          30          31
  e s/s o/l e t/i t/b e/w i t h/C a e s a r/t h
  E K W X R/F C Q L B/R Y F K U/M P E J P/A J S
  A . E . E E . G . A C I O . . L . A . . R . .

      32          33          34          35
  e/n o b l e/B r u t u s/h a t h/t o l d/y o u/
  F O/X X M G T/V U I T L/F P U A E/A P S Q I/E
  E D . . H . . . A . . S . . . . . H . H E E X

   36          37          38          39          40
  C a e s a r/w a s/a m b i t i o u s/i f/i t/w
  Q Z H D/K I Z T H/O O A G H/Y M H C U/J C Y W
  C E . T . O N . . T H . . . C T . O N . E . A

      41          42          43          44
  e r e/s o/i t/w a s/a/g r i e v o u s/f a u l
  A/W X O M F/E P Z S O/K R Y W R/D Q X G J/U I
  T I . G T O . . E A T . A C K . N T . . . A S

  45          46          47          48          49
  t/a n d/g r i e v o u s l y/h a t h/C a e s a
  H W Q/U Q T Q P/Y D T P N/Q U O J E/K K Y Y A/
  . R N E . . G . . N . . L E . T . . . . S M A

      50          51          52          53          54
  r/a n s w e r d/i t/h e r e/u n d e r/l e a v
  H Z K D G/G C A U U/A H X G I/B Y V C X/G F D
  . E . T . . S U N . . . . . N . T . S . . L .

      55          56          57          58
  e/o f/B r u t u s/a n d/t h e/r e s t/f o r/B r
  Y E/I N F H O/C W S H S/G Q V I U/S D Z A W/T L
  S O M . C . . R E N . H . . . O D A . T H I . W

  59          60          61
  u t u s/i s/a n/h o
  P K V/N C A O N/A Z
  . . . D E N T A . L
```

Nearly the whole cipher now becomes perfectly clear. In group 7, *?ITH* is easily *WITH*, adding B to the lineup on the slide, just ahead of I. *PENDI?G*, in groups 17-18 similarly makes sense only as *PENDING* and gives H between W and O on the slide.

This adds more values, and when these are substituted in groups 20-22 of the message the result is *?TH?/PLANS/FOR/THE* of which the first word can only be filled out by making it *THE* (with a still-questionable letter before it), and this gives T on the slide, just after S. Similarly *HA?E* in groups 26-27 can only be *HAVE*, and K falls into position, last letter on the slide, following E. When the values thus won are substituted, the result in groups 28-29 is *GRACIOUSL?* which must be *GRACIOUSLY*, and P is placed on the slide, between I and Y.

There remain only G, V, X and J to locate. When the letters just extracted are placed in position, groups 5-6 read *M?RE/CARE?UL/WITH—MORE CAREFUL WITH*, placing G between T and W, and V just before I. J is now placed between C and Q by solving groups 4-5 where the combination *?H?ULD* can be read as *SHOULD*, and X takes the one place remaining. The slide, then, reads:

R U F M S T G N W H O X V B I P Y A C J Q Z L D E K

and the message is solved.*

The method is long and somewhat laborious, but worth being given here and being followed with some attention because it is typical of the complexities of modern cryptography. It is the most difficult that will be given here—and the last.

VI

It would have been possible to solve this message, or those Bazeries actually handled, without the key by a process of elaborate mathematical analysis. In the case of the royalist ciphers this proved unnecessary; Bazeries was right both about the key and the probable word, and he soon had before him a narrative of the plans for an armed rising to take place in August.

* With full translation at end of volume as usual.

On the tenth of that month Déroulède, with two of his minor leaders, Thuret and Buffet, was arrested, and a police raid on the headquarters of their "League of Patriots" put quantities of papers into the hands of the authorities. At the headquarters of the anti-Semite league, which had worked with the royalists, there was trouble. The members barricaded themselves in the building and stood a siege a week long by regular troops before they surrendered.

At the trials which followed there was no more chance-taking. The government brought forward its prize cryptographer and put him on the witness stand, to which detail we owe the public knowledge of his methods. In open court he described them; all the conspirators were condemned, Déroulède to perpetual banishment, Thuret and Buffet to Algeria and various small fry to prison.

In the strict sense Bazeries can hardly be said to have invented the probable word method. It was used by the Union cryptographers in the Civil War who deciphered the Kirby Smith message. But he it was who raised the thing to a system, making it applicable to all decipherments of whatever character. No cipher written with variations of the Vigenère tableau can long withstand it, and there are very few others it will not solve when handled capably.

Chapter XII

THE CRYPTOGRAPHERS' WAR

I

At the turn of the century a kind of general new deal took place in the ciphering departments of all the large nations except the United States, which continued to use the ciphers and codes of the '90's till World War dates. The literature of cryptography, both in the form of secret government manuals and openly published books, had augmented enormously since 1880. Most of that literature concentrated on the decipherment of the Vigenère system and its outgrowths. Simultaneously, the invention of the latest of the great communications systems—wireless—placed more emphasis than ever on the necessity of throwing confidential correspondence into cipher, for it is the special property of wireless that it turns over to the enemy a copy of every dispatch.

The result of these two forces of development seems to have been, everywhere but in France, a rush to dictionary codes, of the same general type as that produced by the Germans for Turkish use in 1877. But the Boer War soon showed that the dictionary code was not enough. It does very well for communications among the higher units of command, but as the experience in Africa promptly disclosed, the need for secret communications among minor units—regiment, battalion and even company—is as acute as that higher up. Temporarily, British officers in South Africa met the need by using Latin as a cipher, an interesting system based on the fact that English officers were educated men and the Boers little learned.

(Parenthetically, the thing had a good precedent in the British Army. In the old days in India, Sir Charles Napier telegraphed *Peccavi,* the shortest cipher message on record, from the front where he was commanding the siege of Sindh.)

But Latin was at best a stopgap, and the years between 1900 and 1914 saw a scramble for a practical "field cipher." The requirements were that: 1) it must be simple enough to be readily understood by and quickly taught to inexperienced men; 2) it must minimize error through ease of operation; 3) it must not require the use of special apparatus, the capture of a piece of which would betray the secret of the cipher; 4) it must be capable of holding its secret for as long as it took to execute an order written in it, even if the enemy received the message at the same time as the person for whom it was destined.

There was not any cipher that fully met these requirements in 1900 and there is not today; it became a case of compromising in one direction or another with the requirements. In Germany the second and third were most frequently neglected. The Kaiser's armies entered the World War with elaborate double and triple transposition systems grafted onto Vigenère tableaux with irrational alphabets in a manner that made it almost as difficult for persons in possession of the key to read their messages as for the unauthorized. In France the third requirement suffered frequently; Disc ciphers were long in favor. Most of the other states imitated one of these two or clung to outworn methods; only England produced something new—the famous Playfair cipher, one of the simplest and best ever devised.

It is based on a key-word which is placed in the first positions of a square containing the alphabet (from which J is omitted.) Suppose the key-word be EDINBURGH; the alphabet square is then made up in the following manner, letters not in the key-word being written after those in it:

E D I N B
U R G H A
C F K L M
O P Q S T
V W X Y Z

The message is now divided into two-letter groups:

CO ME HE RE

When two letters (*CO* of the clear) occur in the same column

of the square, the letter below each is substituted for it in enciphering. Thus the encipherment for *CO* would be OV. When two letters occur neither in the same line nor column (*ME* of the clear) the pair of letters at the opposite corners of the rectangle formed by taking them as a diagonal is used for encipherment. Thus the encipherment for *ME* is CB, that for *HE* is UN, and that for *RE* UD, making the message:

OV CB UN UD or, rewritten for transmission:

OVCBU NUD

When two letters occur in the same line the letter to the right of each is used for encipherment; if the last letter in either line or column occurs in the clear the encipherer takes the first letter of line or column as that following the last; and finally doubled letters are broken up by inserting X (or Z) between the pairs. Thus, if the clear were *THE ENEMY*– the breakup for encipherment would be:

TH EX EN EM YX

and the encipherment:

SA IV DB BC ZY, rewritten SAIVD BBCZY

The Playfair is one of the best field ciphers yet devised, though it is not nearly so safe as it looks. With the accumulation of material, it becomes fairly easy to break it down by the use of the bigram frequency tables and the reconstruction of the ciphering square.

II

In the E. Phillips Oppenheim world of prewar Europe, only a few experts appear to have concerned themselves with field ciphers whose vital importance was as unforeseen as the enormous development of military wireless. The diplomats and the secret agents who served them were concentrating on the great dictionary codes used for military, naval and, above all, for diplo-

matic purposes. Cryptographically the years 1900-1914 might be called the "Age of the Stolen Codes."

This activity seems to have centered around Vienna, itself a capital of heterogeneous races and divided loyalties, and located at the rim of the Balkans, where the international maneuvers of the period were concentrated. It was in Vienna that an astute Russian spy observed that Colonel Alfred Redl, head of the Austrian espionage and counter-espionage, preferred the society of boys to that of women, and used this observation to blackmail the colonel into one of the greatest treacheries of history. Austria's war plans for the eastern front were betrayed in their entirety, every Austrian spy in Russia delivered up, and the Austrian military dictionary code, the only one of its kind to be lost before the war, was turned over to the Russians.

The treason, which had been a continuing affair for many years, was not discovered till late in 1912, and ultimately had much to do with the frightful Austrian defeats in Galicia during the early part of the war. Austrian fortresses and military railways had been built according to plans known to their enemies, and the Austrian military wireless held no secrets till its whole system was changed, in November, 1914.

While the Redl scandal was still at its height another rumor ran through the government offices in Vienna. The head of the Code Department (they said) had gone to the safe where the great master code-book was kept with the key to all the communications of the Empire. Within that safe he had found a volume which duplicated the master code-book in every detail of external appearance but which, on being opened, was found to contain nothing but blank paper.

The story was perfectly true. A hectic time was enjoyed by everyone in the minor ranks of officialdom during the next week, for no one dared tell old Kaiser Franz Josef, or even tell the higher Army officials, on the heels of the Redl case. The mystery was solved in the most brilliantly ridiculous manner imaginable. The Russian military attaché turned up at Austrian secret-service headquarters to give them the name of a man who had

offered to sell him the code-book for 400,000 rubles. The would-be seller was traced, and through him, the thief, a fair and frail Italian countess, who had become the mistress of a staff lieutenant and saw a chance to make a fortune from the connection. She noted the position of the code-book in its safe during one of her calls, prepared the dummy and engineered the switch, then sent her emissary to the embassy where she was sure she would find a market for the stolen goods.

Unfortunately for her the Russians, though nobody in Austria yet knew it, had already purchased a copy of that code from Colonel Redl. They laughed at her and informed the Austrians; there was nothing left for the countess to do but return the code-book and get out of the country.

The Austrians were also neatly caught by a Balkan adventurer who secured an interview with the head of their code department, and after protesting that he was an honorable man who would deal only with an honorable official, offered to sell a copy of the Serbian diplomatic code. It was in manuscript, copied off in longhand by his nephew who was an employee in the code laboratory of Austria's little neighbor. The Austrian, who had long since learned that protests of honorable intentions are usually the prelude to a trick, demanded some guarantee that the code was genuine and in use. The Serb offered to leave it with him for a few days' free trial. This seemed a reasonable arrangement, and when a couple of diplomatic telegrams came from Belgrade to the Serbian ambassador in Austria during the next two days, they were readily deciphered by means of the code, and the honorable man received 10,000 kroner.

It was not till five days later that another official telegram came through for the Serbian ambassador at Vienna. The Austrians got out their new code to read it, and received the astonishing information that *THE MALE MOTHER OF THE WARSHIP HAS BEEN BUILT*. Something was evidently wrong. To find out what and where the trouble was the Austrians composed a telegram of their own in the purchased code, and had one of their agents send it from Belgrade to the Serbian ambassador in

Vienna, marked "Urgent." Within an hour of its receipt an angry secretary of the Serbian embassy bounced into the Austrian telegraph office with three messages and demanded that they be repeated, as they had arrived in hopelessly garbled condition.

They were the two messages that had been read with the aid of the purchased code and the one sent by the Austrians themselves. The code had been a pure fake, cooked up by the honorable man, whose accomplice in Belgrade sent along the first two telegrams. The ambassador who received them was noted for his gaiety and laziness; he merely let them lie till he received a third, marked "Urgent," before attempting the work of decipherment.

Yet the Vienna cryptographers also had some notable successes in those last years of peace. It was one of them who noted that in dispatches sent in clear the diplomats of every great power used a certain opening formula—"I have the honor to inform your Excellency"—for the English, *"J'ai l'honneur de vous signaller"*—for the French. It occurred to him that the same formula might be used in coded telegrams, and using the formula as a probable phrase, the communications of all the ambassadors with their home governments were attacked. The Austrians were aided in this search by the fact that all the great powers thought their diplomatic codes so safe they did not bother to change them, and, with the aid of the probable phrases, encoded names and other weaknesses, they managed to break most of them down and compile for each of the countries maintaining embassies in Vienna code dictionaries almost as good as those the ambassadors themselves used.

The Vienna government was clever enough to make little or no use of the information thus obtained, saving it for an emergency. Yet the result was fatal; in August, 1914, Vienna became convinced that Italy would enter the war at the side of Austria and Germany and that England would stay out of it, and this conviction was, in the long run, based on what was learned from the decoding of diplomatic telegrams. What the Austrians failed to take into account was the fact that an ambassador is frequently better informed about events in the country to which he is accredited than events in his own.

III

More than any other in history the war that began in 1914 was a cryptographers' conflict. From the day in August of 1914 when German-controlled radio stations all over the world flashed out the message *A SON IS BORN,* code-phrase for "War," no great event but was preceded by feverish activity in the code-rooms of the nations; and in many cases victory or defeat was underwritten in those code-rooms before it took place on the battlefield or across the seas.

As the German armies marched to the Marne in the first days of the war, their communications section was faced with totally unexpected difficulties. Von Kluck and von Bülow, commanding the two armies out on the right wing of the wide sweep through Belgium, soon found themselves beyond the reach of personal communication with the main Army headquarters at Coblenz, moving too fast for messengers to come and go, and with all wires down in their rear. They had to use radio to reach both the high command and each other; had to use it even in communicating with the corps and divisional headquarters under their orders.

When radio was used, the weakness of their cipher system became apparent. Two-step ciphers, the substitution-transposition systems they were using, are quite good when messages can be clearly written out, not quite so good when they must be sent by some form of telegraphy, with the possibilities this entails of confusing one letter with another, and definitely bad under the actual conditions of this war. The air was filled with radio traffic, French, British, Belgian, German, often with several instruments working the same wave-length, jamming one another. Whole sections of messages became lost or unintelligible, and the loss of even one letter in a two-step message which involves double substitution as one of the steps, renders the whole message gibberish. Everything had to be repeated, up to five, ten or a dozen times, and even then some of the most important communications

failed to get through, so the whole of the German march through North France became a chronicle of missed opportunities and faulty co-operation.

At Mons the II and IV German Reserve Corps did not get their orders in time to make a movement von Kluck had astutely planned and the British escaped a trap that had been set for them without being crushed. At Guise, six days later, von Kluck failed to understand orders that came through for him and the French 5th Army slipped from another trap; and meanwhile the French cryptographers, headed by Colonel Givièrge, General Cartier and Dr. Locard, the famous criminologist, had broken down the German ciphers.

Thus it came about that on the night of September 2, 1914, von Kluck was sent by radio a dispatch from the German high command, which ordered him to close up on von Bülow to his left, and to press the French southeast away from Paris. He never received the message but the French did and understood it. Next morning von Kluck radioed his headquarters that he was carrying out the plan of campaign given him when the march through France began—to cross the Marne and swing southwestward against the city. German headquarters did not get that message for another thirty-six hours and only after numerous repetitions, and again the French radios intercepted it and the French decipherers worked out its meaning.

With the messages laid side by side Joffre could see there would be a wide gap between von Kluck's army, moving according to the original plan, and von Bülow's next left, moving southeast according to the new orders. Scouting and aerial observation confirmed the fact; and out of it grew the battle of the Marne. A French army poured from the gates of Paris and clutched von Kluck so close in frontal battle he could not rectify his error when his message tardily reached German headquarters and theirs came to him. Another held von Bülow, while into the gap between the two poured the British with still another French army on their heels, and the Germans did not win their war that fall.

IV

In the east, the Russians, experts of intrigue, knew well before the war started that the Germans had, or would have, their ciphers, but blandly used them right down to the declaration of hostilities as though they suspected nothing. They had worked out a clever plan: several years before the war, their experts had prepared a new and very secret cipher that was partly a code. Only one copy was made, and that locked away in a safe in St. Petersburg. On the day of the declaration this new cipher was taken from its hiding place and turned over to General Jilinsky, the Army's high commander, who sent down orders that copies of the old cipher were to be destroyed.

The Russian war plan called for the invasion of the East Prussian province where it juts like a horn over what was then Russian Poland, by two armies. The First, under General Rennenkampf, was to march in from the east; the Second, commanded by General Samsonov, was to come up from the south, but the two were separated by the forty-mile gap of the region of the Masurian Lakes, a region wild as the Yukon, without railroads, roads or telegraph lines. The two armies could communicate with each other only by field radio, but the Russian field radio service with those two armies was excellent, for they were the flower of the Tsar's troops, almost the only good troops the Russian Army had, fully trained and fully equipped. They drove in the German outposts and began the advance.

It has been said that General Jilinsky chose this occasion to go on a series of superlative champagne parties, but the story comes from the Bolsheviks, tremendously anxious to discredit everyone in the old regime, and is possibly not true. The only thing certain is that Jilinsky gave the single copy of the new secret field cipher to Rennenkampf of the First Army. German radio listeners on the two fronts began to pick up signals from Rennenkampf to Samsonov in the new cipher, of which they could make nothing; then messages from Samsonov to Rennenkampf in the old

peacetime army cipher. But Rennenkampf's operators had already followed orders to destroy their copies of that old cipher; they could no longer read it; and soon there were on the air requests from either Russian commander to the other to send his messages in clear, as the cipher was illegible.

The date had now reached August 20, 1914; that night there came through the air in radio clear a message from Rennenkampf to Samsonov saying the former was halting his advance for three days to let his supply trains catch up with the troops. Hindenburg and Ludendorff had just taken over command of the Germans on the front, with armies superior to either of the Russians alone, desperately inferior to the two together. At first they could not believe the Russians were publicly announcing their plans in this fashion. But as with von Kluck's move to the Marne, airplane and cavalry reconnaissance confirmed the fact of Rennenkampf's halt. Hindenburg flung out a screen of horsemen to keep the Rennenkampf army under observation, switched his divisions toward Poland along the excellent German military railroads, and on August 26th was in position against Samsonov, gripping him tight in front, with strong forces circling both his flanks. The three days following were known as the Battle of Tannenburg, not a battle but a massacre, for Samsonov's army was wiped out with a hundred thousand men dead or prisoners, and in the wild night of rain and defeat on the third day, the Russian commander shot himself. Three weeks later Rennenkampf also was crushed and Russia slid down the long gradient into ruin and revolution.

V

Yet while Russian soldiers were dying or marching off to prisons, Russian sailors were winning one of the most spectacular victories of the code-war behind the war. Germany began the conflict as a blue-water nation, keeping her ships at sea and clashing with the British along the line of the blockade, and in the Baltic, where they had the upper hand, raiding along the

Russian coast. It was on such a raid that their light cruiser *Magdeburg* ran hard aground during a fog.

When the mists cleared the Russian fleet was bearing down. The *Magdeburg's* case was evidently hopeless and her captain sent an officer down for the secret naval code-books, bound in lead. They were to be taken in a boat as far from the ship as possible and thrown in deep water. The approaching Russians began to shoot; there was some confusion on the wrecked cruiser, and as the officer with the code-books in his arms stood by the rail the heave of a swell pitched him into the water. An hour later the Russians had taken possession of the ship. One of their officers, in the old gentlemanly tradition of sea warfare, ordered the bodies round the ship taken up for decent burial. Seldom has an act of humanity been better rewarded; one of the first things the dredge drew up was the body of an officer with the lead bindings of code-books in his arms.

The Russian captain rightly reasoned that where the bindings were found the stuffing could not be far away; he sent down a diver and within another hour had the German naval code-books complete, somewhat damaged by seawater, but perfectly readable. England, as the head of the Allied naval effort, was notified at once, and a fast destroyer carried the books to London by way of the White Sea.

At this time the British Admiralty had already set up its famous decoding department—"Room 40"—under charge of Admiral Sir Reginald Hall, perhaps the best and most famous of all World War experts in secret service, cipher and espionage. Room 40 had been fumbling with German naval codes already; had made some slight progress, but not enough to be of importance when the godsend of the *Magdeburg's* books appeared. Not only did they furnish the code then in use, but also the key to the whole system on which the German naval codes were built, for Germany was using not one code but several.

They were all dictionary codes, consisting of a series of parallel columns, arranged somewhat in the following order, the left-hand column a list of words in dictionary order, the right-hand columns lists of code-signs:

	A	B &C
Kreuzen	JACAB	LURLU
Kreuzer	MUNTA	ACHEL
Kriechen	NITZI	BELEB
Krieg	ONIRD	ZURIT

The code-words were in disordered arrangements and the several columns of them were obviously for the purpose of enabling codes to be changed from time to time. But the experts of Room 40 noticed that the B column opposite the words beginning with K in the clear (for instance) was the same as the A column opposite words beginning with M of the clear and the C column opposite words beginning with W of the clear. In other words, although a code group might signify different words on different days or even different hours, the same sequence of code-signs always stood for an alphabetical sequence of words.

This, in turn, meant that if a single code-sign could be identified with a clear word, after keys had been changed, all the code-signs in that column could be identified by merely setting down opposite the other signs in the column German words in alphabetical order. This was the decoding procedure Room 40 adopted; though the Germans changed keys fast and furiously, their radio messages were seldom a mystery for the two years following—or from the capture of the *Magdeburg* till after the battle of Jutland—when the system was entirely recast.

This was to have the most important effects on the German naval effort, and through it on the whole course of the war. Twice in the early days the Germans tried slipping flotillas of destroyers down along the coast of Holland in an effort to raid British troop convoys across the Channel. Each time Room 40 read their radio signals and knew of the project. The first time fog and a storm forced the raiders back to harbor; the second time a fast and powerful British light cruiser waited across their path and sank four of the German ships before they could get away.

Twice, German battle-cruiser formations tried lightning raids across the North Sea against the English coast; each time England knew they were coming before they left harbor. On the first occasion missed orders and the Germans' own speed saved them

from mishap, but on the second the British battle-cruisers came swooping onto them from the morning mists at Dogger Bank. One German ship was sunk; two more staggered into port with flames leaping above their funnels, not to stir again till the last day of May in 1916, when they tried a trap for the British battle-cruisers and were themselves trapped into the general fleet action off Jutland because Room 40 had again read their code signals.

The tragedy of that battle from the British point of view was that Room 40 knew perfectly well where the German fleet was during the night of the fight, when Sir John Jellicoe was hunting for it. They tried to inform him but there was so much radio traffic in the air the message never got through; and the destroyers who did find the German battleships could do nothing. For the Germans, not bad at code-work themselves, had noted during the long twilight the recognition signals flashed by one British ship to another for identification in the dark. When night came they flashed these same signals, and in the time thus gained blew the British destroyers out of the water, before they could warn their main fleet or fire torpedoes.

VI

The event of Jutland seems to have brought Germany for the first time to the realization that her opponents must have solved her whole naval code system, but despite this slowness the Germans were by no means incompetent adversaries in the war of secret communications. By the middle of 1915 they had completely broken down both the British Playfairs and the ciphers then being used by the French, and German forces in the Black Sea worked a prodigious military joke on the Russians as a sequel to their success in solving Russian naval ciphers. The German ships *Göben* and *Breslau,* nominally under Turkish colors, were then based on Constantinople, and particularly anxious to accomplish something, though outnumbered by the Russian fleet. They waited till the latter put to sea, sneaked the speedy light cruiser *Breslau* in between the Russians and their base, and in Russian naval code, as though coming from home, wirelessed the Russian

admiral orders to hurry his fleet to Trebizond, far at the eastern end of the Black Sea. When the puzzled Russian armada returned from this wild-goose chase they discovered the two German ships had raided their shore establishments and quite broken up their coastwise merchant shipping.

German also was one of the most brilliant cipher coups of the war. For months the great radio station at Nauen followed its regular evening broadcast of the daily communiqué with a series of signals emitted so rapidly they could hardly be considered separate sounds and resembled static more than anything else. The Allied code-rooms studied these signals for a long while, and came to believe they must represent some method of testing the apparatus, for this "lightning gibberish" came too fast and too incoherent to give any starting point toward solutions.

Accident, as not infrequently happens, furnished the clue. It was on a small British monitor, floating under the hot sun of an eastern Mediterranean harbor. The wardroom officers were trying to keep cool with the aid of long drinks and short musical selections played on a portable phonograph. Finally the officer in charge of the concert remarked:

"That's all except a record of some of Nauen's lightning gibberish."

"Put it on," said someone else. "Anything is better than nothing."

He put it on but forgot to rewind the phonograph, and everybody was too hot and tired to get up and wind it for him. As the instrument slowed toward the stopping point the record slowed with it; and as the record slowed, the high-pitched screech of the lightning gibberish turned into a perfectly rational series of radio code-groups. A code officer was among those present; he tried not only the single record but others of the lightning gibberish in dead slow time—and discovered that here was a series of messages from Germany's high command to General von Lettow-Vorbeck, commanding in German East Africa. They were in the prewar German Army cipher, which the Allies had long ago cracked. But it had been, of course, impossible to get the new ciphers through to him, and the Germans had adopted the

ingenious trick of concealing the messages under speed. They were first recorded by means of a buzzer and the record played over the air at five or six times the normal velocity.

Yet it was a German wireless code that helped greatly in bringing American indignation to the boiling point at which a declaration of war was asked. At Brussels a big radio station had been established for the dissemination of messages to German diplomats throughout the world. One of the operators at this station was an extremely talented young Austrian technician named Alexander Szek. The Germans had checked his background before placing him in so important a post, but they had not checked it carefully enough to discover that his mother was English and his personal sympathies bitterly anti-German.

In some manner the British Intelligence Service lighted on these important facts, and managed to get an emissary through the lines to Szek, who agreed to steal the German diplomatic code. It was a slow, painful and dangerous job; Szek could only copy down from the big code-book a few words a day, seizing moments when he was alone, and hiding the slips with the results about his person till he could get home and pass them on to the English spy. The task took weeks and months, and when it had been completed Szek was informed he would have to stay at the Brussels station to prevent any suspicion reaching the Germans that their most secret diplomatic messages were being read in Room 40.

Of course, there came a time when the cat had to be let from the bag. It was the occasion of the famous Zimmermann message, early in 1917, when the German ambassador to Mexico was instructed to work up an alliance with Japan to attack the United States with the aid of Mexico, and Mexico was offered three American states as her price. The news would do so much more damage to Germany if made public than if kept secret that Admiral Hall called in the reporters and gave them the text of the message.

At the end of the interview, "Wasn't it clever of the Americans," he asked, "to do just what we have been trying to do ever

since the war started? They succeeded in stealing the original text of a German diplomatic telegram."

The press, British, French and American, was taken in by this piece of fake ingenuousness, but not the Germans. They began an investigation at the Brussels station and it became time for Alexander Szek to vanish. He met his friend the British agent, who got him out of Belgium and arranged passage to England and safety, but he never arrived in the British Isles. French sources say the British Intelligence Service themselves pushed him over the side of the boat during the trip to keep the Germans from finding out for certain what had happened. The only English writer who has touched the subject says German secret-service detectives followed the young man and caught up with him during the trip.

VII

By the beginning of the 1917 campaigns it was evident on all fronts that even field ciphers could only be protected by changing not merely the keys, but the ciphers themselves, every few days. New German ciphers collapsed in the Allied Black Chambers under a few hours of analysis. The process was greatly helped by the Teutonic habit of wirelessing fixed test messages in each new cipher as it was issued. These test messages were usually proverbs, "A bird in the hand is worth two in the bush" (in its German version) being a great favorite. With a known text thus furnishing a whole series of probable words, Allied experts seldom had to do more than wait till they had their bird in hand with regard to any new cipher.

Transmitters' errors also played a part in breaking down German cipher messages. The Allies had warning of the great German drive of March 21, 1918, through a German cipher operator who used the wrong cipher, and the July Champagne drive which was turned into such a bloody defeat by the "Gouraud defense" is said to have been betrayed in its entirety through a ciphered wireless message. A new cipher had just been issued to all units along the German front, with the object of holding

the orders for that drive secret. "New cipher not yet received" replied one of the German radio men in clear. "Please repeat message in old cipher." The message was repeated; the Allies had already broken the old cipher, and hence had parallel texts which completely destroyed the new.

Data with regard to the German methods of decipherment is rare, but it seems they made some use of the ciphering machines, occasionally in encipherments, more usually as calculating machines for operating decipherments. A number of these machines have appeared since the war; they are mostly alike in having a typewriter keyboard, with the keys connected through a series of cogs and cams to a set of adjusting screws or some device that fulfills the same purpose. When a message is typed on one of these machines, as the operator would type it on an ordinary typewriter, the cogs and cams operate automatically, imprinting on a tape a message in cipher. The recipient of such a message sets the variables on his own machine to the same points as the sender and types the message as received; the result recorded on his tape is the clear.

Theoretically these machines should produce a perfect cipher, as a given bigram of the clear, *TH* for example, will not appear enciphered by the same bigram more than once in four or five hundred appearances. Practically the machines are of very little use, particularly with an army. They are heavy and bulky, more difficult to transport than a dictionary code, get out of order readily, require a good supply of electric current, which is not always available in war. Finally, they are peculiarly subject to cipherers' errors; one touch on the wrong letter and the resulting message is gibberish. But there are variants on the same machines very useful for deciphering purposes in some classes of ciphers, particularly the complex disc ciphers, by automatically calculating numerical relations among the letters of a given cryptogram and sorting out resemblances. They can be defeated only by something that is not systematic at all—a full code—or something that is systematic only in a way of which a machine cannot take account—substitution combined with partial transposition.

Partial codes, in fact, were the universal development on all

the fighting fronts in the last two years of the war for communications even among minor units. The development of listening posts, wire-tapping devices and the induction coils that suck a telephone message into the enemy's lines made even ordinary conversation dangerous during the trench warfare period. "The greatest trouble experienced thus far on our front," says a general order sent to all German units in 1918, "has been due to intercepted telephone messages."

When the United States entered the war, our government thought it had the answer to this. A number of Choctaw Indians were sent into the trenches to 'phone messages to one another in their own tongue, with the idea that the Germans would have to go a long distance before finding Choctaw interpreters. The idea was a success as far as concealing the context of messages from the Germans, but it was too much of a success; the Indians were unable to understand one another over the telephone, and their language held no equivalents for such un-Indian devices as "barrage," "machine gun" and "zero hour."

Thus 1917 and 1918 saw the return of the old jargon-codes of the eighteenth century for all types of messages. Only a few words, and these the more important ones that would identify organizations and troop movements were included in these jargon-codes, which were short enough to be memorized or to be written on a single sheet of paper. A typical message by 'phone to a front-line battalion might be:

"Old Dreadnaught to Red Bonehead. You are receiving six jars of marmalade. In the pantry by forty-two o'clock."—Signifying that the divisional commander was sending three companies (subtract 3 from the 6 of the code) to support a front-line battalion, which was to start toward its objective at *6* A.M. (divide the code figure given by 7).

VIII

After the Germans changed their naval code, as the aftermath of Jutland Battle, there was a considerable space of time during which Room 40 of the British Admiralty had a good deal of

difficulty. Then unrestricted submarine warfare began, and war against the submarines on a basis as unrestricted. One of the undersea boats—it has never been told which or when—was sunk in shallow water near the British coast. She lay so near the surface that England sent down divers to learn what they could of the latest devices aboard, and one of these divers found on the wrecked submarine, in a watertight compartment near the conning tower, the latest code-book of the submarine service.

Submarine commanders, whether from the loneliness of their business or from a natural desire to boast of their exploits, were notoriously chatty men. They usually came to the surface at night and talked by the hour with one another and home in radio code. Now that the British had the new codes, the key of these communications was unlocked; but it soon became evident to the Germans that their enemies had the secret and they changed codes. The British had found the answer to that: every time a submarine was sunk in waters at all possible for diving operations men were sent down. Sure enough, the systematic Teutons kept their code-books in the same place aboard every submarine, and though the work of extracting them was hard and dangerous, British divers got enough of these code-books to keep them well abreast of the latest developments.

Two things were lacking. One was a list of the submarines' call letters, the identifying signatures with which every message opened. Sometimes these letters could be identified from other sources—remarks in the submarine radio conversations themselves, ships that had been attacked, but escaped with notes as to the numbers painted on the conning towers of the tin fish that had tried to sink them. Thus *LOL* would be identified as *UB-46*. But a radio station might pick up *LOL* a week later, and discover that it was not *UB-46* at all, but *U-108*; and changes like this seemed to take place at irregular intervals without rhyme or reason.

The other point lacking was with regard to the positions of the submarines. One of the undersea boats would come to the surface and chatter for a time, then dive before British directional wireless could do more than approximately locate the posi-

tion from which she was talking. In her messages there would always be certain letter groups which were presumably code for her position. But these position code-signs were constructed on an arbitrary system, and no key to them was found in any of the sunken boats. Apparently it was something that submarine commanders were required to memorize, or which they carried in some other place than the ordinary haunt of the code-books.

In October, 1917, came the last of the great Zeppelin raids on London. Returning from the raid the big gas-bags ran into an unexpected head storm over the English Channel. Four of them used up all their fuel bucking the gale and, toward dawn of the next day, drifted helplessly south across France with their motors dead. Two of these four kept close together, L-49 and L-51. The latter bumped and scratched through the upper branches of a swampy wood, tore loose one of her power cars and, relieved of this weight, rose again and drifted off to disappear forever in the Mediterranean. L-49 settled gently and, after scraping the trees in her turn, nestled in a field near Chaumont, where she was captured by an astonished and ancient *garde champêtre.*

Chaumont was American Army headquarters, and within half an hour of the Zeppelin's descent, the place was swarming with staff officers. One of these officers was Colonel Richard Williams of the United States Army Intelligence section, to whom it occurred that the men of the wrecked airship must have been considerably embarrassed by the presence of their code-books. They could hardly have sunk them in the manner of a failing ship; the last water they had crossed was the English Channel. Neither could the books have been burned aboard that hydrogen-filled bag, and when a search failed to reveal any traces of code-books, orders or other official papers on the prisoners Williams deduced they must have been torn up and thrown overboard in fragments.

Carrying his reasoning one step farther, he believed that this job must have been carried out as L-49 skimmed the treetops on the way to her last landing, and gathering a detail of men, he set out on the back track the balloon had left through the trees. A quarter of a mile back he began to find scraps of paper and

then a perfect snowfall. Before night he and his detail had gathered no less than twenty-two gunnysacks full of pieces.

It was too much. When Lieutenant Samuel Hubbard of the staff entered the barnlike map-room at headquarters about midnight that night to see what was going on, he found Williams and half a dozen privates working gigantic jigsaw puzzles all over the place and not having much luck with them. There were so many different papers represented, with parts of all missing, that it seemed impossible to match them up coherently. Hubbard was an amateur yachtsman, who before the war had sailed a small boat through the Danish Islands. The faintly blue color of a fragment about the size of the palm of his hand attracted his attention. When he picked it up he recognized a line that jagged across the piece as the outline of a bay where he had put in with his boat. It was, then, a piece of a chart; yet different from any chart he had ever seen, for it was crossed by fine ruled lines, at the intersection of which were sets of letters.

This seemed to him important. He persuaded Colonel Williams to have the men dig out more fragments of the chart, readily recognizable by their blue color, and easy to piece together because of its map character. It was a big chart, covering all German waters, the whole North Sea and all the sections of ocean that washed the British Isles and northern France. It was, in fact, the thing the Allies had been hunting for for two years—a code-chart, the complete key to those mysterious code-signs giving the positions of the submarines. Nor was this all; as Hubbard, Williams and the detail labored at piecing together the big chart, one of the men produced from his pocket a little book and inquired whether it had anything to do with the chart. He had found it among the pieces of paper and "saved it as a sort of souvenir." It contained a photograph of every surface ship and submarine in the Imperial German Navy, with a list of the call letters for each and a key to the changes in the call letters.

This was how it came about that November, 1917, was the black month of the submarines, with six sent to the bottom and their own sinkings falling to a low from which they never recovered.

IX

The story of ciphers and codes since the World War is still locked in the secret records of the world's Black Chambers. When portions of that story get out there are wigs on the green, as when Major H. O. Yardley told how he had deciphered the messages of the Japanese government to their delegates at the Washington Naval Conference of 1922, and how by the use of the information thus obtained the other powers had succeeded in imposing the 5:5:3 ratio on the balky Japanese. The tale had not a little to do with the Japanese denouncement of the naval treaties.

It is also worth noting that the Japanese ciphers for the occasion were composed on a system of irrational bigram substitutions, not violently different from the Great Cipher designed by Rossignol for Louis XIV. Jargon field-codes and the Great Cipher again; not even in cryptography is there anything new under the sun.

NOTES

Page 56. Frederick's invitation and Voltaire's reply: the invitation, interpreted, reads

Ce soir souper (*sous P*) *à Sans Souci* (*sous Ci*)

and the acceptance:

J'ai grand (*J grand*) *appetit* (*a petit*)

Page 75. The Henri IV cipher. The full text, for those who are interested:

> You are instructed to inform his excellency the Elector of Brandenburg that the French Army is now prepared to march on ten days' notice. The King of Savoy has mobilized his troops and will throw ten thousand men into the Milanese as soon as his excellency's armies have moved. Assure his excellency that the King will take the field in person. The King is unable to move without the Elector of Brandenburg's assurances.

It may be objected that a diplomatist looking for secrecy would hardly encipher the repetitions of the word "Excellency" in so nearly the same manner. The answer is that practice shows they would do exactly that; surviving examples of ciphers of the period are not nearly so carefully composed as the one given in the text.

Page 107. The Fabyan decipherment. "Fr. of VE." of course, is understood to stand for "Francis of Verulam," Bacon's title. But why "WMR"? One would expect Bacon's gravestone message, if he left one there at all, to close "within Wm. S."

Page 111. The quotation is from the Soviet official history.

Page 116. The Nihilist Bacon biliteral cipher. Of course the Russians would not use an English alphabet; their own contains thirty-six letters, so that with the addition of one figure both to the line and column, the result would be the same.

Page 144. The zigzag cipher. The clear was: "I have three grand in a safe deposit box in the First National." The order of the letters at the heads of the columns was normal.

Page 150. The Argyle rising. The usual historical version is that the place and date of the landing were revealed when Argyle's secretary, Spencer, and the surgeon of the expedition, Mr. Blackadder (magnificent name!) were captured when the Duke stopped at Cariston in the Orkneys. A very little consideration of the time element will show this does not do. The two men were taken on May 6, 1685; the proclamation calling out the militia and the seizure of the hostages were on April 28, a week before this date. Argyle actually made his landing on May 7-8, only one day later, and long before news obtained from Spencer and Blackadder could have reached Edinburgh, to say nothing of the fact that all preparations were made to oppose the landing by that time.

Page 167. The typical crypt. Translation: "Sessile Senegambians swiftly smelt smorgasbord, saluting Selassie." This is not a bit more absurd than the usual specimen.

Page 177. The Vigenère cipher solved by the Kasiski method. The full translation reads: "Have your advance battalion in position to attack north from Hamel at seven. Barrage begins at six-thirty. You will be supported on your left by a battalion of chasseurs. Reorganize at Little Hamel for new attack and make liaison to right."

Page 184. The Kirby Smith message from Jefferson Davis. Full translation: "What are you doing to execute the instructions sent you, to forward troops to the east side of the Mississippi? If success will be more certain, you can substitute Wharton's cavalry command for Waller's infantry division. By which you may effect a crossing above that part of the river patrolled by the larger class of gunboats."

Page 226. The royalist message solved by the probable word. Full translation of the message: "Urgent. Déroulède should be more careful with regard to his statements in the press about the impending revolt Stop The plans for the rising on August tenth have been graciously approved by His Majesty with the exception of the section relating to the attack on the caserne of Grenelle Stop His Majesty is unwilling to spill so much French blood as this would entail."

Page 228. *"Peccavi."* "I have sinned." [*Sindh*]

TABLE I

FREQUENCY OF OCCURRENCE OF LETTERS IN ENGLISH

	Letter	Frequency of occurrence in 1000 words	Frequency of occurrence in 1000 letters
1.	E	591	131.05
2.	T	473	104.68
3.	A	368	81.51
4.	O	360	79.95
5.	N	320	70.98
6.	R	308	68.32
7.	I	286	63.45
8.	S	275	61.01
9.	H	237	52.59
10.	D	171	37.88
11.	L	153	33.89
12.	F	132	29.24
13.	C	124	27.58
14.	M	114	25.36
15.	U	111	24.59
16.	G	90	19.94
17.	Y	89	19.82
18.	P	89	19.82
19.	W	68	15.39
20.	B	65	14.40
21.	V	41	9.19
22.	K	19	4.20
23.	X	7	1.66
24.	J	6	1.32
25.	Q	5	1.21
26.	Z	3	.77

The average length of English words is 4.5 letters per word.

It will be noted that the letters, when arranged by relative frequency, fall into certain well-defined groups.

In short messages, and in all text where there are less than 1500 words, any letter in one of these groups may show a higher frequency than another letter of the group though in text consisting of more than 200 words a letter rarely shows such frequency or infrequency as to fall in the wrong group.

For convenience' sake the groups may be listed as follows:

I. – E
II. – T
III. – A, O, N, R, I, S
IV. – H
V. – D, L, F, C, M, U,
VI. – G, Y, P, W, B
VII. – V, K, X, J, Q, Z

If the word "the" is omitted from a given cipher message, T drops into the third group and H into the fifth.

TABLE II

FREQUENCY OF OCCURRENCE OF LETTERS IN FRENCH

	Letter	Frequency of occurrence in 1000 words	Frequency of occurrence in 1000 letters
1.	E	850	175.64
2.	A	395	81.47
3.	S	388	80.13
4.	I	366	75.59
5.	T	356	73.53
6.	N	355	73.22
7.	R	305	62.91
8.	U	285	59.91
9.	L	278	57.33
10.	O	255	52.89
11.	D	200	41.25
12.	C	148	30.63
13.	M	145	29.90
14.	P	144	29.80
15.	V	75	15.57
16.	Q	61	13.61
17.	G	51	10.51
18.	F	46	9.59
19.	B	42	8.76
20.	H	35	7.21
21.	J	29	5.98
22.	X	17	3.50
23.	Y	10	1.16
24.	Z	3	.72
25.	K	2	.41
26.	W	1	.20

The average length of French words is 4.84 letters.

In making the computation the apostrophied l' was not treated as a separate word, and such combinations as qu'une were treated as single words. If these were separated the average length would approach the 4.5 of English, but they are usually treated as single words in cipher and telegraph messages.

It will be noted that the letters, when arranged by relative frequency, fall into certain well-defined groups.

In short messages, any letter is likely to come ahead of another in the same group. For convenience' sake the groups may be listed as follows:

I. – E
II. – A, S, I, T, N
III. – R, U, L, O
IV. – D
V. – C, M, P
VI. – V, Q, G, F, B, H
VII. – J, X
VIII. – Y, Z
IX. – K, W

If "la" and "le" are omitted, L drops into the fourth group; however, this is rarely done, even in cipher messages.

Samples of less than 500 words are insufficient for accurate determination by fre-

TABLE II (*Continued*)

quencies in French. Text in French shows a tendency to repeat the same word, phrase or letter several times in the course of a short message, and this causes several letters, particularly M, U, V and Q to occupy places in a frequency table out of all relation to their actual frequency in the language.

Leading peculiarities by which French may be identified from English (in transposition ciphers):

High frequency of Q
Low frequency of H
K and W almost never occur

L is nearly always followed by a vowel or another L.
Doubled letters are very frequent in French, particularly L, T, S, C and M.

TABLE III

FREQUENCY OF OCCURRENCE OF LETTERS IN SPANISH

	Letter	Frequency of occurrence in 1000 words	Frequency of occurrence in 1000 letters
1.	E	678	136.76
2.	A	622	125.29
3.	O	431	86.84
4.	S	391	79.8
5.	R	341	68.73
6.	N	333	67.12
7.	I	310	62.49
8.	D	291	58.56
9.	L	247	49.71
10.	C	232	46.79
11.	T	230	46.29
12.	U	195	39.34
13.	M	156	31.5
14.	P	124	25.05
15.	B	70	14.2
16.	G	50	10.06
17.	Y	44	8.95
18.	V	44	8.95
19.	Q	43	8.75
20.	H	35	7.04
21.	F	34	6.94
22.	Z	26	5.23
23.	J	22	4.43
24.	X	11	2.21
25.	W	1	.23
26.	K	.5	.04

The average length of Spanish words is 4.96 letters.

It will be noted that the letters, when arranged by relative frequency, fall into certain well-defined groups.

In short messages, any letter is likely to show a frequency higher than another letter of the same group.

For convenience' sake the groups may be listed as follows:

TABLE III (*Continued*)

I. – E, A
II. – O, S
III. – R, N, I, D
IV. – L, C, T, U
V. – M, P
VI. – B, G, Y, V, Q, H, F, Z, J, X
VII. – K, W

If the article "el" is omitted, L drops into the fifth group, and A shows a frequency higher than E.

In Spanish, samples of less than 500 words are very inadequate for determinations by use of frequency tables.

Even in samples of this length, A is quite apt to show a frequency higher than E, and C, D and P (which exhibit the sharpest variation from the frequencies given in the table) often rank directly after E in frequency.

Leading peculiarities by which Spanish may be identified from English (in transposition ciphers):

High frequency of Q
High frequency of A
Low frequency of T

Absence of K and W (which seldom occur in Spanish except in proper names of foreign origin).

Leading peculiarities by which Spanish may be identified from French:

High frequency of O
Low frequency of T
Low frequency of U

Doubled letters are very infrequent in Spanish.

TABLE IV

FREQUENCY OF OCCURRENCE OF LETTERS IN GERMAN

	Letter	Frequency of occurrence in 1000 words	Frequency of occurrence in 1000 letters
1.	E	988	166.93
2.	N	586	99.05
3.	I	463	78.12
4.	S	401	67.65
5.	T	399	67.42
6.	R	387	65.39
7.	A	385	65.06
8.	D	321	54.14
9.	H	241	40.64
10.	U	219	37.03
11.	G	216	36.47
12.	M	178	30.05
13.	C	168	28.37
14.	L	167	28.25
15.	B	152	25.66
16.	O	132	22.85
17.	F	126	20.44
18.	K	112	18.79
19.	W	83	13.96
20.	V	63	10.69
21.	Z	59	10.02
22.	P	55	9.44
23.	J	11	1.91
24.	Q	3	.55
25.	Y	2	.32
26.	X	1	.22

The average length of German words is 5.92 letters.

Letters with the umlaut have been treated as though they had no umlaut in this table. A, O and U are umlauted at times, but the frequency of all three is very small, being about that of J in the table. When the umlaut is not used, words containing an umlauted letter are usually spelled with an E after the letter; if this is done the frequency of E in the table should be slightly higher.

It will be noted that the letters, when arranged by relative frequency fall into certain well-defined groups.

In short messages, any letter is likely to show a higher frequency than another letter of the same group.

For convenience' sake the groups may be listed as follows:

I. – E
II. – N, I
III. – S, T, R, A, D
IV. – H, U, G
V. – M, C, L, B
VI. – O, F, K
VII. – W, V, Z, P
VIII. – J, Z, Y, X

TABLE IV (*Continued*)

If the articles are omitted, there is less change in German than in any other language, owing to the declension of the articles. D and E are the letters whose frequency is most affected. However, articles are not usually omitted even in cipher messages in German, as their omission frequently changes the meaning of a sentence.

C, U and O are the letters whose frequency shows the sharpest variation in short messages, but messages of even 100 words in length exhibit fairly normal frequencies.

Leading peculiarities by which German may be identified from English (in transposition ciphers):

High frequency of N
High frequency of I
Low frequency of O
Low frequency of A

Leading peculiarities by which German may be identified from French:

High frequency of K
High frequency of W
Low frequency of O
Low frequency of L
Low frequency of A

Leading peculiarities by which German may be identified from Spanish:

High frequency of K
High frequency of W
High frequency of N
Low frequency of A
Low frequency of P

Double M is very frequent in German, as is double S, and the combination SZ which occurs in no other language is common.

In German, C is always followed by H or K, and G is nearly always followed by E.

TABLE V

FREQUENCY OF OCCURRENCE OF LETTERS AS INITIALS AND TERMINALS OF WORDS IN ENGLISH

(Figured to basis of occurrence in 1000 words of standard text)

	Initials		Terminals	
	Letter	Frequency in 1000 words	Letter	Frequency in 1000 words
1.	T	181.3	E	222.9
2.	A	123.6	S	137.
3.	O	70.8	D	111.
4.	S	69.1	T	98.1
5.	W	63.3	N	67.6
6.	I	59.	Y	66.2
7.	H	47.5	F	49.3
8.	C	47.	R	47.5
9.	B	42.4	O	41.4
10.	F	41.9	H	34.2
11.	P	40.9	G	25.1
12.	M	39.2	A	24.7
13.	R	31.2	L	24.7
14.	E	27.7	M	20.1
15.	L	22.4	K	8.7
16.	N	21.6	P	6.4
17.	D	20.6	C	3.7
18.	U	14.1	W	3.7
19.	G	12.3	U	2.3
20.	Y	7.5	X	1.4
21.	J	7.	I	.9
22.	V	4.1	B	.9
23.	Q	2.2		
24.	K	1.8	V, Q, J and Z occur so rarely as terminals that their frequency cannot be expressed in this table.	
25.	X	.4		
26.	Z	.4		

NOTE: The high frequency of T as an initial and of E as a terminal in English is partly due to the frequency of the word "the." If this is omitted from a given text, both letters show smaller frequencies than those expressed in this table, but E remains the most frequent terminal letter.

A as a terminal rarely occurs except when it represents the word "a."

U almost never occurs as a terminal except in the word "you."

It will be noted that more than fifty per cent of all English words end in E, S, D or T.

It will be noted that more than fifty per cent of all English words begin with T, A, O, S or W.

F as a terminal generally represents the word "of."

G as a terminal generally represents a word ending in "ing."

H as a terminal generally represents an ending in "gh."

W as an initial generally represents a word beginning "wh-" or "we-."

TABLE VI

Most Common Doubled Letters in English

(Figures represent frequency of occurrence in 1000 words)

LL	19	FF	9	MM	4
EE	14	RR	6	GG	4
SS	15	NN	5	DD	1.5
OO	12	PP	4.5	AA	.5
TT	9	CC	4	BB	.25

V and Z sometimes occur doubled in proper names. No other letters occur as doublets.

TABLE VII

Occurrence of Pairs of Letters in English

The figures represent approximate frequencies for 1000 words. Read from side to top: that is, ET will be found in line E, column T.

These figures from normal text, and with divisions between words respected. Thus in such a phrase as "If you—" IF is recorded and YO, but not FY.

	E	T	A	O	N	R	I	S	H	D	L	F	C	M	U	G	Y	P	W	B	V	K	X	J	Q	Z
E	14	14	31	4	51	88	7	52	2	46	18	9	17	18	3	7	7	9	4		10		9			
T	46	9	29	41		29	45	12	168		5	1	2	1	9		8		4							
A		68		1	92	40	16	42		21	33	3	18	9	6	11	9	8	3	8	10	7				
O	3	13	2	12	71	45	4	8	1	6	15	49	5	30	40		3	23	8	4	5	2		1		
N	31	37	13	11	5		16	24		61	4	3	19		1	27	6				2					
R	91	20	26	31	8	5	36	18		10	4		5	9	7	2	11	2	2	1	4	3				
I	14	38	16	31	86	16		41		13	17	3	24	18	1	9		8		3	13	3	2			1
S	35	53	5	19	1		21	14	14		1		6	2	14	1	3	5	2			3		1		
H	132	7	33	15	1	3	43			1	2				5		3		1							
D	32		8	4		5	14	5		1	2			2	8	1	1									
L	39	7	21	13		2	22	5		11	19	2		1	5		17		1		1					
F	9	2	7	17		12	11				2	9			3											
C	26	12	20	27		6	9		22		9		5		8		3					10				
M	27		27	14		2	13	3						5	4		3	9	6							
U	4	24	6		22	19	2	23		2	10	2	9	3		9		8		1						
G	12	1	5	6	1	7	5	3	12		2				2	4	1									
Y	4		3	4			1	4		1																
P	13	6	14	17		18	4	6	3		13			3	2			5								
W	29		22	10	3	2	15		16																	
B	23		10	10		5	2	2		9					7		7									
V	29		7	2			9										1									
K	8		2	1			5	3																		
X	3	3					1						1					3								
J	3		4	2											2											
Q															5											
Z	1																									

TABLE VIII

OCCURRENCE OF BIGRAMS IN ENGLISH; NORMAL TEXT AND MILITARY TELEGRAPHIC.

The most frequent bigrams are listed in the order of their frequency in normal text (1000 words) with the same figures for military telegraphic text, for comparison.

Bigram	Normal text	Military telegraphic	Bigram	Normal text	Military telegraphic
TH	168	106	VE	29	37
HE	132	76	TA	29	51
AN	92	94	TR	29	20
RE	91	77	CO	27	39
ER	88	73	ME	27	38
IN	86	74	NG	27	30
ON	71	76	MA	27	25
AT	68	71	CE	26	20
ND	61	58	RA	26	27
ST	53	41	IC	24	10
ES	52	49	NS	24	22
EN	51	50	UT	24	15
OF	49	28	US	23	13
TE	46	38	BE	23	18
ED	46	36	UN	22	21
OR	45	63	CH	22	20
TI	45	46	WA	22	11
HI	43	31	SI	21	22
AS	42	22	LA	21	18
TO	41	69	AD	21	14
AR	40	39	LI	22	20
OU	40	69	RT	20	33
IS	40	28	CA	20	15
IT	36	38	NC	19	19
LE	39	27	SO	19	21
NT	37	47	LL	19	33
RI	36	21	UR	19	37
SE	35	33	EL	18	21
HA	33	44	RS	18	30
AL	33	26	EM	18	17
DE	32	23	AC	18	21
EA	31	31	IM	18	13
NE	31	33	PR	18	12
RO	31	41			38
OM	30	37	TT	9	24
IO	31	30	OT	13	32
WE	29	3	WI	15	28
			EC	17	

TABLE IX

Most Frequent Words in English

This table shows frequencies for 10,000 words of normal text, words that occur five or more times in this amount of text being listed.

a	108	good	5	my	11	there	15
about	11	great	7	new	6	these	7
after	11	had	13	no	10	they	9
all	18	has	24	not	22	this	24
an	16	have	22	now	6	through	6
and	142	he	31	of	222	time	12
are	40	her	6	on	30	to	132
as	31	here	6	one	23	today	13
at	25	him	5	only	10	under	6
be	43	his	29	or	19	up	6
been	14	I	16	other	11	upon	5
before	5	if	11	our	5	very	10
being	10	in	111	out	8	war	6
between	5	interest	5	over	10	was	32
but	24	into	9	people	6	we	12
by	42	is	72	public	6	well	6
can	6	it	43	said	6	were	20
country	5	its	10	since	6	what	5
day	8	large	5	so	14	when	14
days	6	last	6	some	11	where	6
debts	5	like	5	still	6	which	25
dollars	11	made	8	such	6	while	6
even	8	make	5	take	5	who	13
every	6	many	14	than	9	will	24
first	7	may	13	that	61	with	31
for	49	more	14	the	420	would	13
found	6	most	9	their	18	years	6
from	24	must	7	them	11	you	10
general	6						

In addition the numerical words, frequently expressed in numbers, show the following frequencies for 10,000 words of text

two	20	three	9
four	6	five	10
six	3	seven	5
eight	3	nine	3
ten	3		

eleven, twelve, thirteen, fourteen, fifteen, sixteen, seventeen, eighteen, nineteen—2 each

twenty, thirty, forty, fifty, sixty, seventy, eighty, ninety—10 each

hundred—17

thousand—12

TABLE X

MOST FREQUENT BIGRAMS AND TRIGRAMS IN VARIOUS EUROPEAN LANGUAGES
Listed in the order of their relative frequency.

Bigrams

French....	ES - EN - SE - ON - DE - TE - NT - LE - ET - AT - ON
German...	EN - ER - CH - DE - GE - IE - EI - ND - IN - TE - RE
Spanish...	ES - EN - EL - DE - LA - OS - AR - UE - RA - RE - ER
Italian....	ER - ES - ON - RE - EL - EN - DE - DI - TI - SI - AL

Trigrams

French....	ENT - QUE - LES - ION - AIT - TIO - ONT - ANS - ART - AIN - OUR - OUS
German...	EIN - ICH - DEN - DER - TEN - CHT - SCH - CHE - DIE - UNG - GEN - UND
Spanish...	QUE - EST - ARA - ADO - AQU - DEL - CIO - ETE - OSA - EDE - PER - IST
Italian....	CHE - ERE - ZIO - DEL - ECO - QUE - ARI - ATO - EDI - IDE - ESI - IDI

TABLE XI

COMMON PATTERN-WORDS IN ENGLISH

Note:—This is not intended to be a complete list of all words corresponding to a given pattern. Words listed here occur on the average more frequently than once in ten thousand words of normal text. Words have been given their simplest form; derivatives frequently extend the pattern.

1 1 2 1

aDDeD
agrEEmEnt
scrEEnEd
sEEmEd
swEEpEr
baGGaGe
ceLLuLose
caNNoN
plaNNiNg
ruNNiNg
eRRoR
loSSeS
paSSeS
maSSeS

1 1 2 1 1 2 1

poSSESSES

1 1 2 1 2

nEEDED

1 1 2 2

coFFEE
commiTTEE

1 1 2 3 1

aGGreGate
aTTenTion
huDDleD

1 1 2 3 2

aCCEl Erate
aCCOmmOdate
oFFEr Ed
oFFIc Ial
suFFEr Ed
suFFIc Ient
flOODe D

1 1 2 3 3

aC CeSS
oC CuRRed
suC CeSS
coMMiSSion
coMMiTTee

1 1 2 3 4 4

aDDreSS
aNNuaLLy

1 2 1 1

forEsEEn
ninEtEEn

1 2 1 2

crISIS
shININg
traININg
PAPAl
VIVId

1 2 1 3 1

sEvErE
whEnEvEr
vIsItIng
vIcInIty
cIvIlIan
dIrIgIble
exhIbItIng
InItIal
mIlItIa
polItIcIan
possIbIlIty
prohIbItIon
sensIbIlIty
mOnOtOnous
perSiStS
insTiTuTion
sTaTuTe
UnUsUal

TABLE XI (*Continued*)

1 2 1 3 2

cA T A s Trophe
MEMbEr

12133 421

dISILLuSIon

1 2 1341

A v A il Able
rEc EivE

121344

FiFtEEn

1213453

AbANdoN

1 2 2 1

A F F A ir
bAGG A ge
A P P A rent
A R R A nge
A T T A ch
A T T A ck
A T T A in
abE T T E d
addrE S S Es
confE R R E d
defE R R E d
E F F E ct
stE P P E d
E S S Ence
mE S S E nger
strE S S E d
vE S S E ls
lE T T E r
forb I D D I ng
b I L L I ng
br I L L I ant
d I F F I cult
fulf I L L I ng
k I L L I ng
m I L L I on
sh I L L I ng
w I L L I ng
beg I N N I ng
sp I N N I ng
cl I P P I ng
sh I P P I ng
m I S S I ng
m I S S I on
h I T T I ng
N O O N
fO L L Ow
cOMMOn

1 2 2 1 Cont.

OPPOsition
cORROde
tomORROw
bOTTOm
caREER
sUCCUmb

1 2 2 1 2

bAGGAGe
w I NN I Ng

1 2 2 3 1

A P Pe Ar
A P Pe Al
ANNuAl
sET T l Ement
chaUF F e Ur

1 2 2 3 2 1

cANNoNAde

12311

bEtwEEn
dEgrEE
EstEEm
ExcEEd
wiLfuLLy

1 2 3 1 2

obsERvER
tENdENcy
grINdING
poINtING
thINkING
beloNGiNG
iNTeNT
LONdON
PErPEtual
REpREsent
SEnSE
negoTIaTIon

123122

dISmISS

1 2 3 1 2 3

brINGING

123142

vALuAbLe

1 2 3 1 4 2 3

PREPaRE

12321

MAdAM
preC I pI Ce
inD I v I Dual

1 2 3 2 1 Cont.

L EvEL
pREfER
REfER
REsERve
uSE l ESs
acT I v I Ty
uT I l I Ty

12313

PrOPOse

1 2 3 1 3 2

oRDERED
PROPORtion

123141

sIgn I f I cant
TenTaTive

123241

G I v I nG
STaTuS
STaTiStic

12331

PaSSPort

1 2 3 3 2 3 1

beGINNING

123341

TeRRiTory

1 2 3 4 1 2

CHurCH
frEShnESs
POstPOne
rEDucED
schEDulED
mA I ntA I n

1 2 3 4 2 1

MUseUM
prA CtiCAl
R EadE R

1234221

dIScuSSIon

1234412

rECoLLECt

1234421

STrEETS

TABLE XII

English Trigrams

Figures represent approximate frequencies for 20,000 words, but are more important in their relation to one another.

A		agn	2	ame	53	aro	7
Aam	1	ago	6	amh	1	arp	1
		agr	8	ami	6	arr	19
Aba	6	agu	2	aml	1	ars	46
abd	1			amn	1	art	48
abe	1	Ahe	2	amo	8	arv	3
abi	3	aho	1	amp	10	ary	34
abl	39	ahu	1	ams	6		
abo	28	ahy	1	amy	1		
abr	1					Asa	1
abs	1	Aid	24	Ana	6	asc	3
		aig	3	anc	39	ase	20
Aca	3	aii	3	and	154	ash	14
acc	20	ail	16	ane	15	asi	9
ace	20	aim	6	ang	17	ask	6
acf	1	ain	60	ani	21	asl	1
ach	21	air	16	ank	10	asm	1
aci	8	ais	5	ann	13	aso	6
ack	18	ait	3	ano	10	asp	1
acq	1			anq	1	asq	1
acr	4	Aje	1	ans	25	ass	31
act	41	ajo	5	ant	55	ast	36
acu	2			anu	4	asu	6
acy	3	Ake	35	anv	1		
		aki	5	anx	1	Ata	1
Ada	4	akn	1	any	54	atb	1
add	10	akr	1			atc	9
ade	32	aks	1	Aor	1	ate	139
adi	15					ath	17
adj	5	Ala	5	Apa	10	ati	128
adl	3	alb	1	ape	16	atl	4
adm	10	alc	1	aph	1	atm	1
ado	3	ald	2	api	5	ato	22
ads	4	ale	14	apo	5	atr	5
adu	3	alf	3	app	40	ats	2
adv	4	ali	17	apr	2	att	41
ady	7	alk	2	aps	1	atu	19
		all	99	apt	7	aty	1
Aes	1	alm	10				
		alo	9	Ara	16	Auc	1
Afe	2	alr	2	arc	12	aud	4
aff	9	als	19	ard	53	auf	2
aft	30	alt	16	are	105	aug	4
		alu	7	arg	34	aul	4
Aga	16	alv	1	ari	29	aum	1
age	20	alw	5	ark	6	aur	2
agg	3			arl	18	aus	17
agi	3	Ama	2	arm	13	aut	17
		amb	4	arn	8		

TABLE XII (*Continued*)

Ava	11	bes	6	bur	4	cid	6
ave	60	bet	13	bus	7	cie	17
avi	12	bex	1	but	54	cif	2
avo	5	bey	2	buy	3	cil	6
avy	6					cim	1
		Bia	4	C		cin	5
Awa	8	bic	1	Cab	3	cio	4
awi	1	bid	2	cac	1	cip	13
awl	1	bie	1	cad	5	cis	7
aws	3	big	4	cae	1	cit	13
		bil	13	cag	2	civ	5
Axe	1	bim	5	cal	28		
axi	1	bis	3	cam	15	Cka	2
		bit	12	can	40	cke	22
Ayb	1			cap	5	cki	6
aye	6	Bje	7	car	18	ckn	2
ays	17			cas	13	cko	1
		Bla	1	cat	28	ckp	1
Aza	1	ble	43	cau	24	cks	8
azi	1	bli	36	cay	1	cky	1
		bll	1				
B		bly	12	Cca	2	Cla	9
Bab	4			cce	8	cle	10
bac	7	Boa	6	cco	13	cli	5
bad	1	bod	8	ccu	6	clo	8
baf	3	bol	5			clu	16
bag	1	bom	3	Cdo	1		
baj	1	bon	1			Coa	5
bal	6	boo	11	Cea	3	cob	1
ban	12	bor	8	ced	15	coc	2
bar	7	bos	1	cee	1	cof	2
bas	7	bot	8	cei	13	cog	4
bat	8	bou	2	cel	10	coi	1
		bow	2	cem	2	col	23
Bbe	1	box	2	cen	34	com	56
bbi	2	boy	5	cep	8	con	104
bby	3			cer	21	coo	5
		Bra	12	ces	42	cop	3
Bdu	1	bro	8			cor	17
		bru	7	Cha	29	cos	2
Bea	7			che	27	cot	1
bec	15	Bsc	1	chi	22	cou	36
bed	2	bse	2	chl	1	cov	9
bee	32	bso	1	chm	3		
bef	8	bst	1	chn	1	Cqu	2
beg	5			cho	6		
beh	2	Bta	3	chs	3	Cra	17
bei	19	bts	8	cht	1	cre	20
bel	14			chu	8	cri	10
ben	3	Bui	11			cro	7
beq	4	bul	3	Cia	23	cru	3
ber	35	bun	1	cib	1		

TABLE XII (*Continued*)

Cta	8	deq	1	doo	1	Ebb	1
cte	22	der	60	dop	4	ebc	2
cti	31	des	31	dor	1	ebr	5
ctl	3	det	4	dot	1	ebt	10
cto	13	dev	9	dou	5	eby	2
ctr	5			dow	8		
cts	5	Dfa	2			Eca	13
ctu	17	dfu	1	Dra	10	ecd	1
				dre	45	ece	30
Cub	1	Dge	2	dri	2	ech	6
cud	1	dgi	1	dro	3	eci	15
cue	1	dgm	1	drt	2	eck	4
cul	16			dry	2	ecl	6
cum	3	Dia	10			eco	24
cup	2	dic	8	Dsi	1	ecr	3
cur	10	did	4	dso	1	ect	81
cus	10	die	7	dst	10	ecu	7
cut	12	dif	13			ecw	1
cuu	1	dig	4	Dua	6		
		dil	9	duc	20		
Cyt	1	dim	2	due	6	Eda	1
		din	60	dui	1	ede	5
Cza	1	dio	1	dul	1	edg	5
		dir	9	dun	2	edi	12
D		dis	48	duo	1	edl	1
Dah	2	dit	12	dup	1	edn	2
dai	1	diu	1	dur	6	eds	12
dam	5	div	3	dus	4	edu	12
dan	7			dut	3	edv	2
dap	1	Dja	1				
dar	2	djo	1	Dva	2	Eec	2
dat	5	dju	3	dvo	1	eed	9
dau	1					eef	1
dav	1	Dle	4	Dwa	1	eek	4
day	64	dll	1	dwi	1	eel	3
daz	1	dlo	1			eem	8
		dly	9	Dys	1	een	56
Dde	11					eep	12
ddi	2	Dme	1	E		eer	8
ddl	1	dmi	9	Eac	13	ees	11
ddr	4			ead	38	eet	10
		Dna	4	eag	3	eez	1
Dea	13	dne	2	eak	12		
deb	10	dnt	1	eal	20		
dec	10			eam	17	Efe	10
ded	24	Doc	2	ean	10	eff	20
def	12	doe	4	eap	1	efi	4
deg	4	dog	1	ear	63	efl	2
del	11	doi	1	eas	35	efo	12
dem	10	dol	22	eat	37	efs	1
den	37	dom	4	eau	6	eft	5
dep	10	don	17	eav	12	efu	5

TABLE XII (*Continued*)

Ega	11	Ena	16	err	16	ewv	1
ege	6	enb	4	ers	124	ewy	6
egi	20	enc	49	ert	25		
egl	2	end	44	eru	17	Exa	11
ego	5	ene	29	erv	2	exc	6
egr	4	eng	14	ery	36	exe	6
egu	6	eni	11			exh	3
egy	3	enj	2	Esa	1	exi	4
		enl	4	esc	12	exp	26
Eha	1	enn	3	esd	5	ext	8
ehe	1	eno	9	ese	35	exu	1
ehi	2	enr	2	esh	5		
eho	3	ens	35	esi	14	Eye	4
ehu	1	ent	234	esk	2	eyo	1
		enu	2	esm	2	eyr	1
Eic	1	env	3	eso	5	eys	4
eig	22			esp	9	eyv	1
ein	19	Eof	2	ess	77		
eip	4	eol	1	est	96	Eze	1
eir	36	eon	1	esu	3		
eit	7	eop	13			F	
eiv	9	eor	1	Eta	6	Fac	21
		eou	2	etb	1	fad	1
Eki	2			etc	2	fai	9
		Epa	9	ete	14	fal	5
Ela	4	epe	8	eth	7	fam	6
elc	1	eph	8	eti	15	fan	4
eld	5	epi	1	eto	1	far	14
ele	40	epl	2	etr	2	fas	1
elf	13	epo	5	ets	17	fat	3
elg	4	epp	1	ett	20	fau	1
eli	17	epr	12	etu	3	fav	4
ell	43	eps	2	etw	10		
elo	19	ept	10	ety	7	Fea	5
elp	1	epu	9			feb	4
elr	1			Eug	1	fec	13
els	7	Equ	16	eum	1	fed	2
elt	6			eur	8	fee	9
elu	1	Era	45	eut	1	fel	7
elv	4	ero	13	euv	4	fen	4
ely	29	erd	6			fer	28
		ere	162	Eva	5	fes	2
Ema	14	erf	7	eve	107	feu	2
emb	13	erg	5	evi	7	few	7
eme	24	erh	4	evo	3		
emi	6	eri	36			Ffa	1
emm	1	erk	2	Ewa	3	ffd	4
emn	2	erl	3	ewb	2	ffe	34
emo	10	erm	23	ewh	1	ffi	24
emp	20	ern	34	ewi	2	ffl	4
ems	5	ero	7	ewj	4	ffo	6
emy	1	erp	3	ews	4	ffs	1

TABLE XII (*Continued*)

Fib	5	gav	2	goe	1	hee	1
fic	36	gay	1	goi	2	hei	36
fie	12			gol	4	hel	11
fif	23	Ged	6	gon	1	hem	30
fig	4	gel	2	goo	13	hen	31
fil	7	gem	3	gor	1	heo	3
fin	28	gen	30	got	9	her	145
fir	25	geo	1	gov	15	hes	25
fis	4	ger	31			het	5
fit	3	ges	13	Gra	18	hew	1
fiv	21	get	7	gre	34	hey	39
				gri	5		
Fla	2	Gga	1	gro	8	Hfu	3
fle	6	gge	2	gru	1		
fli	5	ggl	2			Hib	6
flo	10	ggr	2	Gth	2	hic	53
flu	7			gto	2	hie	6
fly	8	Ghb	1			hig	10
		ghe	2	Gua	2	hil	16
Fog	3	ghl	2	gue	4	him	15
fol	8	gho	1	gui	10	hin	38
foo	6	ght	41	gul	5	hip	7
for	177			gun	1	hir	17
fou	27	Gia	5	gur	5	his	105
		gib	2	gus	2	hit	12
Fra	12	gil	2				
fre	17	gim	4	Gyo	1	Hla	1
fri	7	gin	21	gyr	5	hle	2
fro	43	gio	1			hli	1
		gir	2	H		hly	2
Fte	34	gis	5	Hab	1		
fth	2	git	1	had	26	Hme	4
fty	8	giv	8	hai	5		
				hal	14	Hne	1
Fue	1	Gla	5	ham	5	hno	1
ful	27	gle	9	han	32		
fun	2	gli	2	hap	11	Hoa	1
fur	5	glo	2	har	22	hoi	1
fus	1	glu	1	has	52	hok	1
fut	1	gly	2	hat	134	hol	11
				hau	5	hom	13
Fyi	2	Gme	1	hav	47	hon	11
				haw	3	hoo	8
G		Gna	3	hay	1	hop	6
		gne	7			hor	8
Gag	1	gni	5	Hbo	1	hos	9
gai	13	gno	2			hot	2
gal	4	gns	2	Hco	3	hou	70
gam	1					hov	1
gar	12	Goa	1	Hea	28	how	23
gas	10	gob	1	hec	2		
gat	7	god	2	hed	38		

TABLE XII (*Continued*)

Hre	19
hro	13
Hsc	3
hst	2
Hte	5
htf	2
hts	1
hty	6
Hub	1
hud	2
hue	1
hug	3
hum	7
hun	39
hur	8
hus	5
hut	1
Hwe	2
Hyd	1
hys	3
I	
Iab	4
iah	1
ial	30
iam	4
ian	14
iar	1
ias	1
iat	15
Ibe	10
ibi	12
ibl	11
ibr	7
ibu	7
Ica	55
ice	33
ich	54
ici	26
ick	24
icl	4
ico	1
ics	6
ict	18
icu	11
icy	3
Ida	4
idd	2
ide	51
idg	1
idi	4
idl	2
idn	5
ido	2
idu	2
Iec	3
ied	15
ief	9
ieh	1
iel	4
iem	29
ier	11
ies	26
iet	4
ieu	4
iev	8
iew	3
Ife	6
iff	14
ifi	13
ifl	1
ift	13
ifu	2
ify	4
Iga	1
ige	4
igg	1
igh	49
igi	6
ign	21
igu	3
Ike	13
iki	1
Ila	4
ilb	2
ild	12
ile	33
ilf	2
ili	21
ilk	1
ill	110
ilo	4
ilr	4
ils	3
ilt	6
ilu	2
ilv	1
ily	9
Ima	15
imb	1
ime	48
imi	8
imm	4
imo	1
imp	15
ims	8
Ina	31
inc	41
ind	30
ine	68
inf	12
ing	317
inh	1
ini	27
inj	1
ink	9
inl	2
inm	1
inn	4
ino	4
inq	3
inr	35
int	62
inu	8
inv	10
iny	1
Ion	232
ior	4
iou	10
Ipa	6
ipi	1
ipl	5
ipm	1
ipp	5
ips	3
ipt	6
ipu	1
Iqu	1
Ira	6
irc	3
ird	2
ire	33
iri	5
irl	3
irm	7
iro	2
irs	22
irt	14
Isa	10
isc	15
ise	14
isf	2
ish	34
isi	16
isk	1
isl	12
ism	10
iso	2
iss	14
ist	41
isy	1
Ita	14
itc	1
ite	41
ith	90
iti	48
itl	4
itn	1
ito	6
its	26
itt	15
itu	17
ity	44
itz	1
Ius	1
Iva	12
ive	90
ivi	14
ivu	1
Ixt	5
Iza	5
ize	16
izo	1
izz	1

TABLE XII (*Continued*)

J

Jac	2
jam	1
jap	9
jar	1
Jea	4
jec	9
jeh	1
jer	4
jes	1
Jim	3
Job	2
joh	3
joi	1
jol	1
jor	4
joy	2
Jud	2
jur	1
jus	5

K

Kab	2
kal	1
kam	1
kar	1
Kca	1
Kea	1
ked	14
kee	4
kel	4
kem	8
kep	1
ker	11
kes	4
ket	17
key	2
Kid	4
kil	4
kim	9
kin	15
kis	3
kit	2
kiv	1
Kle	1
kly	2
Kma	1
Kne	1
kno	18
Kob	1
kou	1
Kpi	1
Kro	1
Kst	1
Kut	1

L

Lab	7
lac	15
lad	3
lag	1
lai	8
lak	5
lam	1
lan	45
lap	1
lar	56
las	16
lat	28
lau	2
lav	4
law	5
lay	9
laz	1
Lbe	4
Lca	2
lco	2
Lde	7
ldh	1
ldr	2
lds	7
Lea	29
leb	1
lec	24
led	35
lee	4
lef	5
leg	7
lem	4
len	10
lep	7
ler	10
les	52
let	16
lev	3
lex	2
ley	4
Lfa	1
lfi	3
lfr	1
lft	1
lfu	1
Lga	1
lgi	5
Lia	10
lib	8
lic	43
lid	2
lie	19
lif	3
lig	10
lik	11
lim	11
lin	42
lio	14
lip	2
liq	1
lis	19
lit	39
liv	4
liz	10
Lke	1
Lla	21
lle	22
lli	30
llm	1
llo	22
lls	7
llu	8
lly	44
Lma	2
lmo	8
Lne	1
Loa	1
lob	5
loc	11
lod	1
lof	1
log	4
lon	26
loo	7
lop	10
lor	3
los	19
lot	6
lou	12
lov	2
low	28
loy	9
Lph	1
lpi	1
lpy	1
Lre	2
lro	4
lry	1
Lse	1
lsi	1
lso	6
Lte	9
lth	7
lti	3
lto	1
ltr	1
ltu	3
lty	4
Lua	3
lub	1
lud	11
lue	6
lug	1
lui	1
lul	5
lum	4
lun	2
lur	2

TABLE XII (*Continued*)

lus..... 10
lut..... 5
lux..... 1

Lwa..... 5

Lye..... 1
lyi..... 7
lyn..... 2
lys..... 1

M

Maa..... 1
mac..... 5
mad..... 16
mag..... 7
mai..... 8
maj..... 5
mak..... 13
mal..... 10
man..... 93
map..... 2
mar..... 20
mas..... 8
mat..... 23
may..... 27

Mba..... 1
mbe..... 18
mbi..... 8
mbl..... 2
mbo..... 4
mbr..... 1
mbs..... 1
mbu..... 1

Mea..... 11
mec..... 3
med..... 22
mee..... 2
meh..... 1
mel..... 4
mem..... 11
men..... 70
mer..... 31
mes..... 16
met..... 12
mew..... 1

Mhe..... 1

Mic..... 6
mie..... 3
mig..... 5
mil..... 26
min..... 42
mir..... 4
mis..... 17
mit..... 18

Mle..... 1
mly..... 2

Mma..... 2
mme..... 8
mmi..... 5
mmo..... 3
mmu..... 1

Mna..... 2

Mob..... 2
moc..... 7
mod..... 8
mom..... 4
mon..... 22
mop..... 2
mor..... 39
mos..... 31
mot..... 6
mou..... 19
mov..... 7

Mpa..... 11
mpe..... 8
mph..... 2
mpi..... 1
mpl..... 22
mpo..... 9
mpr..... 4
mpt..... 10
mpu..... 1
mpy..... 1

Mrs..... 8

Mse..... 6

Muc..... 7
mug..... 1
mul..... 2
mun..... 3
mur..... 1

mus..... 16
mut..... 1

Mys..... 4

N

Nab..... 3
nac..... 1
nad..... 2
nag..... 3
nai..... 1
nal..... 30
nam..... 1
nan..... 10
nap..... 5
nar..... 11
nas..... 1
nat..... 40
nav..... 13
naz..... 1

Nba..... 1
nbe..... 3
nbu..... 1

Nca..... 1
nce..... 96
nch..... 15
nci..... 19
ncl..... 15
nco..... 3
ncr..... 4
ncs..... 1
nct..... 6
ncy..... 5

Nda..... 6
nde..... 45
ndf..... 3
ndi..... 30
ndl..... 5
ndm..... 1
ndo..... 9
ndr..... 36
nds..... 30
ndu..... 11
ndw..... 1
ndy..... 2

Nea..... 9
nec..... 8
ned..... 46

nee..... 6
nef..... 1
neg..... 5
nei..... 2
nel..... 7
nem..... 1
nen..... 4
neo..... 1
nep..... 1
ner..... 21
nes..... 32
net..... 11
nev..... 14
new..... 30
nex..... 2
ney..... 7

Nfa..... 3
nfe..... 5
nfi..... 7
nfl..... 4
nfo..... 6
nfu..... 1

Nga..... 2
nge..... 26
ngi..... 10
ngl..... 8
ngo..... 2
ngs..... 11
ngt..... 4
ngu..... 6

Nha..... 1

Nia..... 6
nic..... 5
nif..... 2
nig..... 5
nim..... 2
nin..... 40
nio..... 4
nis..... 16
nit..... 22
niu..... 1
niv..... 6
niw..... 7

Njo..... 2
nju..... 1

TABLE XII (*Continued*)

Nke.....	4	nsp.....	4	obe.....	2	okl.....	2
nki.....	4	nst.....	29	obi.....	2	oks.....	7
nkl.....	1	nsu.....	2	obj.....	3		
nkm.....	1	nsw.....	2	obl.....	4	Olc.....	2
nks.....	5	nsy.....	2	obo.....	2	old.....	22
				obr.....	1	ole.....	6
Nls.....	4	Nta.....	33	obs.....	7	olg.....	1
nly.....	26	nte.....	53	obt.....	3	oli.....	31
		nth.....	8			oll.....	41
Nma.....	1	nti.....	44	Oca.....	8	olm.....	1
nme.....	7	ntl.....	12	occ.....	5	olo.....	7
nmo.....	1	ntm.....	1	oce.....	8	ols.....	2
		nto.....	19	och.....	1	olu.....	9
Nna.....	3	ntr.....	33	oci.....	5	olv.....	5
nne.....	8	nts.....	28	ock.....	15		
nni.....	7	ntu.....	3	oco.....	2	Oma.....	7
nno.....	8	ntv.....	5	ocr.....	5	omb.....	5
nns.....	2	nty.....	32	oct.....	2	ome.....	52
nnu.....	3					omi.....	22
nny.....	1	Nua.....	3	Oda.....	28	oml.....	1
		nue.....	5	ode.....	6	omm.....	14
Nob.....	2	nuf.....	2	odi.....	8	omn.....	5
noc.....	2	nui.....	3	ods.....	4	omp.....	25
noe.....	5	num.....	8	odu.....	4	oms.....	10
nog.....	1	nun.....	4	ody.....	5	omy.....	1
noi.....	1	nus.....	4				
nol.....	2	nut.....	2	Oes.....	6	Ona.....	18
nom.....	6			oeu.....	4	onc.....	23
non.....	5	Nva.....	2			ond.....	32
noo.....	3	nve.....	14	Off.....	26	one.....	78
nor.....	23	nvi.....	2	ofi.....	2	onf.....	10
nos.....	6	nvo.....	3	oft.....	4	ong.....	27
not.....	67					oni.....	5
nou.....	12	Nwa.....	2	Oge.....	2	onk.....	1
nov.....	1			ogi.....	1	onl.....	21
now.....	31	Nxi.....	1	ogn.....	5	onn.....	8
noy.....	1			ogr.....	2	ono.....	14
		Nyi.....	1	ogs.....	3	onp.....	1
Npl.....	1	nyo.....	3	ogy.....	6	onq.....	2
npo.....	1	nyt.....	2			onr.....	1
				Ohi.....	5	ons.....	78
Nqu.....	7	O				ont.....	30
		Oac.....	2	Oic.....	2	onu.....	3
Nro.....	1	oad.....	10	oid.....	1	onv.....	6
nry.....	2	oal.....	1	oil.....	7	ony.....	1
		oam.....	2	oin.....	10		
Nsa.....	8	oan.....	1	ois.....	1	Ood.....	25
nse.....	8	oar.....	7			oof.....	2
nsf.....	1	oat.....	1	Oje.....	2	ook.....	23
nsi.....	20					ool.....	6
nsk.....	1	Oba.....	6	Oke.....	4	oom.....	8
nso.....	1	obb.....	4	oki.....	2	oon.....	5

TABLE XII (*Continued*)

oor	2	ots	4	pat	12	ppe	23
oos	1	ott	4	pau	2	ppi	4
oot	8	oty	1	pay	5	ppl	11
oov	2					ppm	1
		Oub	6	Pea	20	ppo	6
Opa	1	ouc	1	pec	16	ppr	12
ope	30	oud	1	ped	7	ppt	1
oph	3	oug	28	pee	2		
opi	1	oui	4	pen	22	Pra	4
opl	13	oul	38	peo	11	pre	52
opm	5	oun	60	per	79	pri	23
opo	8	oup	1	pes	1	pro	67
opp	2	our	56	pet	2	pru	1
opr	1	ous	66				
ops	4	out	54	Pha	2	Pta	1
opt	6			phe	5	pte	7
opu	3	Ova	1	phi	3	pti	8
		ove	65	pho	8	pto	1
Ora	8	ovi	5	phy	3	pts	1
orb	3					ptu	1
orc	14	Owa	1	Pic	11	pty	1
ord	32	owb	1	pid	4		
ore	63	owd	2	pie	3	Pub	26
org	5	owe	32	pik	1	pul	11
ori	15	owf	1	pil	7	pun	1
ork	18	owh	1	pim	12	pur	5
orl	13	owi	6	pir	3	pus	1
orm	31	own	24	pit	8	put	5
orn	9	ows	8				
oro	1	owt	2	Pla	46	Pwa	1
orr	12			ple	37		
ors	17	Oxe	1	pli	16	Pya	1
ort	60	oxi	8	plo	9		
oru	1			plu	1	Q	
orv	6	Oya	1	ply	6		
		oyc	1			Qua	13
Osc	2	oye	8	Pma	1	que	25
ose	41	oyi	1	pme	6	qui	10
osi	10	oym	1			quo	2
osl	2	oys	3	Poc	2		
osn	1			poi	5	R	
osp	3	P		pok	1	Rab	4
oss	18	Pac	2	pol	25	rac	16
ost	34	pad	1	pon	16	rad	11
		pag	2	poo	1	raf	7
Ota	10	pai	12	pop	6	rag	4
otb	1	pal	6	por	27	rah	1
ote	22	pan	21	pos	26	rai	17
otf	1	pap	12	pou	1	rak	1
oth	40	paq	1	pow	10	ral	38
oti	10	par	36			ram	2
oto	2	pas	21	Ppa	2	ran	40

TABLE XII (*Continued*)

rsp	5	rgo	1	rod	5	Rua	4
rsr	3	rgs	1	roe	1	rub	1
rss	6	rgu	1	rof	2	ruc	11
rst	54			rog	2	rud	1
rsu	1	Ria	13	roh	5	rue	2
rsv	5	rib	10	roj	2	rug	1
rsw	4	ric	33	rol	9	rui	2
rsy	3	rid	3	rom	65	rul	4
		rie	29	ron	10	rum	4
Rbi	4	rif	1	roo	3	run	6
rbo	1	rig	19	rop	15	rup	1
		rik	2	ror	1	rur	1
Rca	18	ril	3	ros	14	rus	2
rch	14	rim	6	rot	3	rut	1
rci	7	rin	39	rou	28		
rcl	1	rio	13	rov	10	Rva	4
rcs	12	rip	4	row	11	rve	8
rcu	1	ris	23	rox	7	rvi	9
rcy	1	rit	23	roy	5		
		riv	15			Rwa	2
Rda	3	riz	3	Rpe	2	rwo	2
rde	14			rpi	1		
rdi	15	Rka	2	rpl	2	Ryb	2
rdl	1	rke	5	rpo	1	ryi	2
rds	12	rki	2	rpr	1	ryo	2
rdu	1	rkm	2			rys	3
rdy	1	rks	1	Rra	5		
				rre	16	S	
Rea	82	Rld	13	rri	13		
reb	2	rle	5	rro	8	Sad	1
rec	45	rli	6	rru	1	saf	2
red	101	rlo	1	rry	3	sag	2
ree	45	rly	8			sai	15
ref	20			Rse	11	sal	8
reg	19	Rma	26	rsh	4	sam	4
reh	1	rme	12	rsi	8	san	33
rei	8	rmi	8	rso	8	sap	5
rel	12	rml	1	rsp	2	sar	7
rem	20	rmo	8	rst	21	sas	1
ren	39	rms	6	rsy	1	sat	11
reo	2	rmt	1			sav	1
rep	28			Rta	16	saw	3
rer	8	Rna	9	rte	10	say	3
res	114	rne	19	rth	22		
ret	13	rni	10	rti	32	Sca	7
rev	14	rnm	8	rtl	3	sce	3
		rno	7	rtm	2	sch	13
Rfe	4	rnt	1	rto	1	sci	11
rfu	3			rtr	1	scr	9
		Roa	13	rts	8	scu	9
Rga	5	rob	10	rtu	4		
rge	26	roc	14	rty	17	Sda	5

TABLE XII (*Continued*)

Sea	12	Ska	6	sti	61	Tch	11
sec	15	ske	6	stl	4		
sed	13	ski	1	sto	13	Tea	16
see	15	sks	1	stp	1	teb	2
seg	2	sky	2	str	57	tec	5
seh	2			sts	18	ted	104
sei	29	Sla	11	stu	6	tee	17
sem	2	sle	7			tef	1
sen	50	sli	4	Sua	6	teg	4
sep	3	slo	2	sub	6	tel	28
seq	5	sly	3	suc	16	tem	22
ser	20			sud	4	ten	46
ses	23	Sma	4	sue	6	teo	1
set	10	sme	1	suf	2	ter	143
seu	1	smi	6	sug	2	tes	46
sev	21	smo	1	sui	1	tet	4
sew	1	smu	1	sul	5	tew	3
sex	1			sum	6	tex	1
sey	4	Sne	1	sun	5		
		sno	1	sup	11	Tfa	1
Sfa	2	snp	1	sur	20	tfu	2
sfc	1			sus	4		
sfo	3	Soa	2			Tha	143
		soc	4	Swa	1	the	2
Sha	8	sod	1	swe	10	thd	1
shc	1	soo	2	swi	2	the	1054
she	33	sot	1			thf	2
shi	19			Syl	3	thi	83
shm	1	Spa	6	sym	4	thl	3
shn	1	spe	25	sys	5	tho	60
sho	12	sph	1			thr	33
shu	1	spi	14	T		ths	7
shy	1	spl	1			thu	5
		spo	13	Tab	13	thw	2
Sia	4	spr	4	tac	14	thy	3
sib	12	spu	1	tad	3		
sic	6			taf	1	Tia	7
sid	23	Squ	9	tag	4	tib	1
sie	5			tai	26	tic	61
sif	1	Sre	1	tak	16	tid	1
sig	9			tal	18	tie	15
sil	7	Ssa	4	tam	1	tif	12
sim	3	sse	38	tan	26	til	17
sin	34	ssf	2	tap	1	tim	40
sio	33	ssi	33	tar	21	tin	64
sip	1	ssm	1	tas	2	tio	177
sir	2	sso	2	tat	44	tip	2
sis	12	ssu	8	tau	1	tir	8
sit	17			tax	1	tis	12
siv	3	Sta	67	tay	1	tit	20
six	10	ste	50			tiv	30
siz	2			Tba	1	tiz	1
				tbr	1		

TABLE XII (*Continued*)

Tla	4	tus	1	Uga	1	unq	1
tle	23	tut	12	uge	5	uns	3
tli	1			ugg	3	unt	31
tly	20	Twa	1	ugh	40		
		twe	45	ugu	2	Uot	1
Tme	3	twi	1			uou	1
tmo	2	two	40	Uid	2		
				uie	1	Upa	2
Tne	1	U		uil	15	upe	2
		Uab	3	uim	3	upi	1
Tos	1	uad	3	uip	2	upl	2
tod	25	ual	20	uir	4	upo	10
tog	7	uan	1	uis	10	upp	10
tol	1	uar	13	uit	4	upt	2
tom	19	uat	4			upw	1
ton	12			Uke	4	upy	1
too	12	Ubb	1	uki	1		
top	3	ube	10			Ura	7
tor	40	ubi	1	Ula	19	urb	2
tot	6	ubj	4	uld	27	urc	8
tou	2	ubl	25	ule	7	urd	2
tow	10	ubs	2	ulf	2	ure	55
toy	1	ubt	2	ulg	2	urg	4
				uli	2	uri	13
Tra	40	Uca	3	ull	14	urk	1
tre	23	ucc	4	uln	1	url	1
tri	31	uce	8	ulo	4	urn	13
tro	17	uch	19	ulp	6	uro	4
tru	20	ucl	1	uls	1	urp	3
try	21	uck	4	ult	12	urr	7
		ucr	1	uly	1	urs	7
Tse	1	uct	15			urt	8
tsm	1			Uma	4	urv	1
tso	1	Uda	1	umb	13	ury	7
tst	3	udd	6	ume	6		
		ude	12	umm	3	Usa	27
Tta	9	udg	1	ump	2	usc	2
tte	40	udi	10	ums	2	use	37
tti	6	udy	1	umu	2	ush	7
ttl	16					usi	13
tto	3	Uea	2	Una	3	usk	1
tty	2	ued	8	unb	1	usl	3
		uee	1	unc	13	usp	2
Tua	7	uel	1	und	78	uss	10
tub	8	uen	9	une	3	ust	38
tud	7	uer	2	unf	2	usu	5
tue	4	ues	18	ung	8	usy	2
tum	1	uey	1	uni	20		
tun	3			unk	3	Uta	2
tuo	1	Ufa	2	unl	3	ute	15
tur	49	uff	4	unn	3	uth	10
				unp	1	uti	21

TABLE XII (*Continued*)

utm..... 1
uto..... 9
uts..... 3
utt..... 2
utu..... 1
utw..... 1
uty..... 4

Uum..... 1

Uva..... 1
uvr..... 4

Uxu..... 1

Uye..... 1
uys..... 1

V

Vab..... 2
vac..... 1
vad..... 1
vai..... 4
val..... 22
van..... 6
vap..... 3
var..... 7
vas..... 3
vat..... 10
vau..... 1

Vea..... 4
ved..... 18
vee..... 3
vel..... 17
vem..... 5
ven..... 63
ver..... 147
ves..... 30
vey..... 2

Vic..... 12
vid..... 9
vie..... 7
vig..... 1
vil..... 6
vim..... 14
vir..... 2
vis..... 9
vit..... 7
viv..... 2

Voc..... 1
voi..... 2
vok..... 1
vol..... 6
vor..... 5
vot..... 5

Vre..... 4

Vus..... 1

Vys..... 1

W

Wai..... 5
wal..... 7
wam..... 1
wan..... 1
war..... 32
was..... 74
wat..... 19
wav..... 2
way..... 16

Wbe..... 1
wbr..... 2

Wde..... 1

Wea..... 6
wed..... 9
wee..... 15
wei..... 1
wel..... 14
wen..... 27
wep..... 1
wer..... 60
wes..... 4
wet..... 3
wev..... 11

Wfl..... 1

Wha..... 11
whe..... 51
whi..... 67
who..... 33

Wic..... 2
wid..... 8
wif..... 4
wig..... 2

wil..... 54
win..... 19
wir..... 1
wis..... 1
wit..... 75
wiv..... 1

Wje..... 1

Wla..... 3
wle..... 2
wli..... 1
wly..... 1

Wne..... 3
wnw..... 2

Wol..... 1
wom..... 4
won..... 2
woo..... 5
wor..... 40
wou..... 23

Wre..... 2
wri..... 4

Wsp..... 3
wsu..... 1

Wth..... 2

Wyo..... 7

X

Xac..... 3
xam..... 7
xan..... 1

Xce..... 5
xcl..... 2

Xec..... 2
xem..... 1
xer..... 3
xes..... 2

Xha..... 2
xhi..... 1

Xib..... 1
xim..... 7

xin..... 1
xio..... 1
xis..... 3

Xpe..... 11
xpl..... 7
xpr..... 7
xpu..... 1

Xte..... 5
xth..... 2
xtr..... 2
xty..... 3

Xua..... 1
xur..... 2

Y

Yac..... 1
yal..... 3
yan..... 1
yar..... 6

Ybo..... 1
ybr..... 1

Yco..... 1

Ydr..... 1

Yea..... 19
yed..... 8
yee..... 3
yel..... 1
yer..... 3
yes..... 11
yet..... 7

Yin..... 15

Ylp..... 1
yly..... 2

Yma..... 1
ymb..... 4
yme..... 1

Yom..... 1
yon..... 5
yor..... 8
you..... 33

TABLE XII (*Continued*)

Ype	5	ysh.....	1	Z		Zin.....	1
yps	1	ysi.....	5	Zar.....	3	zis.....	1
		yst.....	7	zat.....	3		
Yre	1					Zli.....	1
yru.....	5	Yth.....	2	Zed.....	11		
				zen.....	1	Zon.....	2
Yso.....	1	Yve.....	1	zer.....	1		
yse.....	2					Zza.....	1
						zzl.....	1

TABLE XIII

Numerical Co-ordinates of the Alphabet

This table—to be read from the side—shows the numerical relation of the letters to one another.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
B	25	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
C	24	25	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
D	23	24	25	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
E	22	23	24	25	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
F	21	22	23	24	25	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
G	20	21	22	23	24	25	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
H	19	20	21	22	23	24	25	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
I	18	19	20	21	22	23	24	25	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
J	17	18	19	20	21	22	23	24	25	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
K	16	17	18	19	20	21	22	23	24	25	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
L	15	16	17	18	19	20	21	22	23	24	25	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
M	14	15	16	17	18	19	20	21	22	23	24	25	0	1	2	3	4	5	6	7	8	9	10	11	12	13
N	13	14	15	16	17	18	19	20	21	22	23	24	25	0	1	2	3	4	5	6	7	8	9	10	11	12
O	12	13	14	15	16	17	18	19	20	21	22	23	24	25	0	1	2	3	4	5	6	7	8	9	10	11
P	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	0	1	2	3	4	5	6	7	8	9	10
Q	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	0	1	2	3	4	5	6	7	8	9
R	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	0	1	2	3	4	5	6	7	8
S	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	0	1	2	3	4	5	6	7
T	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	0	1	2	3	4	5	6
U	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	0	1	2	3	4	5
V	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	0	1	2	3	4
W	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	0	1	2	3
X	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	0	1	2
Y	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	0	1
Z	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	0

INDEX