

Lecture 2

Final Version

~~CONFIDENTIAL~~LECTURE 2

As I said at the close of the preceding lecture, a bit of history is always useful in introducing a subject belonging to a special and not too well known field; therefore, I'll proceed with some historical information about cryptology, which, as you learned before, comprises two closely related sciences, namely, cryptography and cryptanalysis. I will repeat and emphasize that they are but opposite faces of the same valuable coin; progress in one inevitably leads to progress in the other, and to be efficient in cryptology you must know something about each of them.

Cryptography and cryptanalysis probably go back to the dawn of the invention and development of the art of writing itself. In fact, there is reason for speculating as to which came first--the invention of writing or the invention of cryptography; it's somewhat like the question as to which came first--the hen or the egg. It is possible that some phases of cryptography came before the art of writing had advanced very far.

I've mentioned the art of writing. As in the case of other seemingly simple questions, such as, "why is grass green?", when we are asked to define writing we can't find a very simple answer, just because the answer isn't at all simple. Yet, Breasted, the famous University of Chicago historian and Orientalist, once said: "The invention of writing and of a convenient system of records on paper has had a greater influence in uplifting the human race than any other intellectual achievement in the

~~CONFIDENTIAL~~

career of man." There has been, in my humble opinion, no greater invention in all history. The invention of writing formed the real beginning of civilization. As language distinguishes man from other animals, so writing distinguishes civilized man from barbarian. To put the matter briefly, writing exists only in a civilization and a civilization cannot exist without writing. Let me remind you that animals and insects do communicate--there's no question about that; but writing is a thing peculiar to and found only as a phenomenon in which man and no animal or insect engages, and let's never forget this fact. Mankind lived and functioned for an enormous number of centuries before writing was discovered and there is no doubt that writing was preceded by articulate speech for eons--but civilization began only when men got the idea of and invented the art of writing. So far as concerns Western or Occidental civilization, writing in essence is a means of representing the sounds of what we call speech or spoken language. Other systems of writing were and some still are handicapped by trying to represent things and ideas by pictures. I'm being a bit solemn about this great invention because I want to impress upon you what our studies in cryptology are really intended to do, namely, to defeat the basic or intended purpose of that great invention: instead of recording things and ideas for the dissemination of knowledge, we want and strive our utmost to prevent this aim from being realized, except among our own brethren and under certain special circumstances, for the purpose of our mutual security, our self-preservation. And that's important.

Writing is a comparatively new thing in the history of mankind. No complete system of writing was used before about 3500 B.C.

Ordinary writing, the sort of writing you and I use, is perhaps an outgrowth or development of picture writing or rebus writing, which I'm sure most of you enjoyed as children. A rebus contains features of both ordinary and cryptographic writing; you have to "decrypt" the significance of some of the symbols, combine single letters with syllables, pronounce the word that is represented by pictures, and so on. Here's an example which I have through the courtesy of the Bell Telephone Laboratories. Let's see how much of it you can make out in half a minute.

From rebus writing there came in due course alphabetic writing and let me say right now that the invention of the alphabet, which apparently happened only once in the history of mankind, in some Middle East Semitic region, in or near the Palestine-Syria area, then spread throughout the whole of the European continent, and finally throughout most of the world, is perhaps man's greatest, most important, and most far-reaching invention because it forms the foundation of practically all our written and printed knowledge, except that in Chinese. The great achievement of the invention of the alphabet was certainly not the creation of the signs or symbols. It involved two brilliant ideas. The first was the idea of representing merely the sounds of speech by symbols, that is, the idea of what we may call phoneticization; the second was the idea of adopting a system in which,

roughly speaking, each speech sound is denoted or represented by one and only one symbol. Simple as these two ideas seem to us now, the invention was apparently made, as I've said, only once and the inventor or inventors of the alphabet deserve to be ranked among the greatest benefactors of mankind. It made possible the recording of the memory of mankind in our libraries, and from that single invention have come all past and present alphabets. Some of the greatest of men's achievements we are now apt to take for granted; we seldom give them any thought. The invention of the art of writing and the invention of the alphabet are two such achievements and they are worth pondering upon. Where would we be without them? Note that among living languages Chinese presents special problems not only for the cryptologist but also for the Chinese themselves. No Sinologist knows all the 80,000 or so Chinese symbols, and it is also far from easy to master merely the 9,000 or so symbols actually employed by Chinese scholars. How far more simple it is to use only 20 to 26 symbols! Being a monosyllabic language, it seems almost hopeless to try to write Chinese by the sort of mechanism used in an alphabetic polysyllabic language; attempts along these lines have been unsuccessful and the difficulties in memorizing a great many Chinese characters accounts for the fact that even now only about 10% of the Chinese people can read or write to any significant degree. The spread of knowledge in China is thereby much hampered.

Probably the earliest reliable information on the use of cryptography in connection with an alphabetic language dates from about 900 B.C., Plutarch mentioning that from the time of Lycurgus there was in use among the Lacedemonians, or ancient Greeks, a device called the scytale. This device, which I'll explain in a moment, was definitely known to have been used in the time of Lysander, which would place it about 400 B.C. This is about the time that Aeneas Tacticus wrote his large treatise on the defense of fortification, in which there is a chapter devoted specifically to cryptography. In addition to mentioning ways of physically concealing messages, a peculiar sort of cipher disk is described. Also a method of replacing words and letters by dots is mentioned.

We find instances of ciphers in the Bible. In Jeremiah Chapter 25, Verse 26 occurs this expression: "And the King of Sheshakh shall drink after them." Also, again in Jeremiah 51:41: "How is Sheshakh taken!" Well, for perhaps many years that name "Sheshakh" remained a mystery, because no such place was known to geographers or historians. But then it was discovered that if you write the twenty-two letters of the Hebrew alphabet in two rows, eleven in one row and eleven in the other, like this, you set up a substitution alphabet whereby you can replace letters by those standing opposite them. For example, "Shin", is represented by "Beth" or vice versa, so that "Sheshakh" translates "Babel", which is the old name of "Babylon." Hebrew then did not have and still doesn't have vowels; they must be supplied.

This is an example of what is called ATBASH writing, that is, where Aleph, the first letter is replaced by Teth, the last letter; Beth, the second letter, by Shin, the next-to-the-last, etc. By sliding the second row of letters one letter each time there are eleven different cipher alphabets available for use. The old Talmudists went in for cryptography to a considerable extent. Incidentally, in mentioning the Bible, I will add that Daniel, who, after Joseph in Genesis, was an early interpreter of dreams and therefore one of the first psychoanalysts, was also the first cryptanalyst. I say that he was an early psychoanalyst, because you will remember that he interpreted Nebuchadnezzar's dreams. In the Bible's own words, "Nebuchadnezzar dreamed dreams, wherewith his spirit was troubled, and sleep brake from him." But, unfortunately, when he woke up he just couldn't remember those troublesome dreams. One morning he called for his wise men, magicians, astrologers, and Chaldean sorcerers and asked them to interpret the dream he'd had during the preceding night. "Well, now, tell us the dream and we'll try to interpret it", they said. To which King Nebuchadnezzar exclaimed, "The thing is gone from me. I don't remember it. But it's part of your job to find that out, too, and interpret it. And if you can't tell me what the dream was, and interpret it, things will happen to you." What the king asked was a pretty stiff assignment, of course and it's no wonder they failed to make good, which irked Nebuchadnezzar no end. Kings had a nasty habit of chopping your head off in those days if you failed or made a mistake, just as certain arbitrary

and cruel despots are apt to do even in modern times for more minor infractions, such as not following the Party Line. So in this case it comes as no surprise to learn that Nebuchadnezzar passed the word along to destroy all the wise men of Babylon, among whom was one of the wise men of Israel, named Daniel. Well, when the King's guard came to fetch him, Daniel begged that he be given just a bit more time. Then, by some act of divination, --the Bible simply says that the secret was revealed to Daniel in a night vision--Daniel was able to reconstruct the dream and then to interpret it. Daniel's reputation was made. Some years later, Nebuchadnezzar's son Belshazzar was giving a feast, and, during the course of the feast, in the words of the Bible, "came forth fingers of a man's hand and wrote over against the candlestick upon the plaster of the wall." The hand wrote a secret message. You can imagine the spine-chilling scene. Belshazzar was very much upset, and just as his father did, he called for his wise men, soothsayers, Chaldean sorcerers, magicians and so on, but they couldn't read the message. Apparently they couldn't even read the cipher characters! Well, Belshazzar's Queen fortunately remembered what that Israelite Daniel had done years before and she suggested that Daniel be called in as a consultant. Daniel was called in by Belshazzar and he succeeded in doing two things. He succeeded not only in reading the writing on the wall: "MENE, MENE, TEKEL, UPEARSIN", but also he was successful in deciphering the meaning of those strange words. His interpretation: "Mene" -- "God hath numbered thy kingdom and finished

it." "Tekel" -- "Thou are weighed in the balances and found wanting."
 "Upharsin" -- "Thy kingdom shall be divided and given to the Medes and
 Persians." Apparently the chap who did the handwriting on the wall knew
 a thing or two about cryptography, because he used what we call "variants",
 or different values, for in one case the last word in the secret writing on
 the wall is "Upharsin" and in the other it is "Peres"; the commentators are
 a bit vague as to why there are these two versions of the word in the Bible.
 At any rate, Babylon was finished, just as the inscription prophesized; it
 died with Belshazzar.

I think this curious biblical case of the use of cryptography is
 interesting because I don't think anybody has really found the true meaning
 of the sentence in secret writing, or explained why the writing on the wall
 was unintelligible to all of Belshazzar's wise men. Here's a slide which
 is supposed to give the best explanation of the enigmatical sentence that
 has always been considered one of the most obscure of the many difficult
 scriptural passages which have awakened the interest and baffled the ingenuity
 of scholars. You see that this savant thinks that the cuneiform ideograms
 were written without any division between the individual words, so that the
 sentence "would be just as hard to read as a rebus and would puzzle the
 most skillful decipherer." He goes on to say: "The difficulty would have
 been still more increased if the ideograms had been grouped in some unusual
 way, severing the natural connection of the component elements. If the

signs had been written in this manner it would have been almost impossible to arrive at their true meaning." But why could Daniel read and interpret the writing when his competitors couldn't? This our savant doesn't explain. Another savant offers as his explanation of the mystery the following hypothesis: That the words were written in columns, as shown in this slide, and that Daniel in solving the mystery read downwards or rather down, up, down. This explanation doesn't satisfy me any more than the other one.

The next slide I show you is the scytale, which I've already mentioned as one of the earliest cipher devices history records. The scytale was a wooden cylinder of specific dimensions around which they wrapped spirally a piece of parchment or leather; they then wrote the message on the parchment, unwound it, and sent it to its destination by a safe courier, who handed it over to the commander for whom it was intended and who, having been provided with an identically-dimensioned cylinder, would wind the strip of leather or parchment around his cylinder and thus bring together properly the letters representing the message. This diagram may not be accurate. I don't think anyone really understands the scheme. The writing was done across the edges of the parchment, according to some accounts, and not between the edges, as shown in this slide. Incidentally, you may be interested to learn that the baton which the European field marshal still carries as one of the insignia of his high office derives from this very instrument.

We don't know much about the use of cryptography by the Romans, but it is well known that Caesar used an obviously simple method; all he did was to replace each letter by the one that was fourth from it in the alphabet. For example, A would be represented by D, B by E, and so on. Augustus Caesar is said to have used the same sort of thing, only even more simple; each letter was replaced by the one that followed it in the alphabet. Cicero was one of the inventors of what is now called shorthand. He had a slave by the name of Tyro, who wrote Cicero's records in what are called Tyronian notes. Modern shorthand is a development of Tyro's notation system.

The next slide shows some cipher alphabets of olden times, alphabets used by certain historical figures you'll all remember. The first cipher alphabet on the slide was employed by Charlemagne, who lived from 768 to 814 A.D. The second one was used in England during the reign of Alfred the Great, 871 to 899. The third alphabet is called ogam writing and was used in ancient Ireland. The alphabets below that were used much later in England: the fourth one by Charles the First, in 1646; the fifth, the so-called "clock cipher", was used by the Marquis of Worcester in the 17th Century; finally, the last one was used by Cardinal Wolsey in about 1524.

In the Middle Ages cryptography appears first as a method of concealing proper names, usually by the simple substitution of each letter by the next one in the alphabet, just about as Augustus Caesar did hundreds of years

before. At other times the vowels were replaced by dots, without changing the consonants--a method that was used throughout Europe to about 1000 A.D., when letters began to be replaced by various signs, by other letters, by letters from another language, by runes which are found in abundance in Scandinavia, and by arbitrary symbols. Here's an example of a runic inscription on a stone that stands before Gripsholm Castle near Stockholm, Sweden. The word rune means "secret".

Within a couple hundred years the outlines of modern cryptography began to be formed by the secret correspondence systems employed by the small Papal States in Italy. In fact, the real beginnings of systematic, modern cryptology can be traced back to the days of the early years of the 13th Century, when the science began to be extensively employed by the princes and chanceries of the Papal States in their diplomatic relations amongst themselves and with other countries in Europe. The necessity for secret communication was first met by attempts inspired by or derived from ancient cryptography, as I've outlined so far. There was a special predilection for vowel substitution but there appeared about this time one of the elements which was later to play a very prominent role in all cipher systems, an element we now call a syllabary, or a repertory. These were lists of letters, syllables, frequently-used parts of speech and words, with additions of arbitrary equivalents for the names of persons and places. There is still in existence one such syllabary and list of arbitrary

equivalents which was used about 1236 A.D. and there are other examples that were used in Venice in 1350.

Among examples of ciphers in medieval cryptography is a collection of letters of the Archbishop of Naples, written between 1363 and 1365, in which he begins merely with symbol substitutions for the vowels and uses the letters that are actually vowels to serve as nulls or non-significant letters to throw the would-be-cryptanalyst off the right track. As a final development, the high-frequency consonants L, M, N, R, and S, and all the vowels, are replaced not only by arbitrary symbols but also by other letters.

About 1378 an experienced cryptologist named Gabriele Lavinde of Parma was employed as a professional by Clement VII and in the Vatican Library there is a collection of ciphers devised and used by Lavinde about 1379. It consists of repertoires in which every letter is replaced by an arbitrary symbol. Some of these ciphers also have nulls and arbitrary equivalents or signs for the names of persons and places. There is a court cipher of Mantua dated 1395 that used this system.

At the beginning of the 15th Century the necessity of having variants for the high-frequency letters, especially the vowels, became obvious. Here is an alphabet of that period which is interesting because it shows that even in those early days of cryptology there was already a recognition of the basic weakness of what we call single or monoalphabetic substitution, that is, where every letter in the plain-text message is represented by another and always the same letter. Solution of this type of cipher, as many of you may know,

is accomplished by taking advantage of the fact that the letters of an alphabetic language are used with greatly differing frequencies. I don't have to go into that now because many of you, at some time or other, have read Edgar Allan Poe's "Gold Bug", and understand the principles of that sort of analysis. This slide clearly shows that the early Italian cryptographers understood the fact of varying frequencies and introduced stumbling blocks to quick and easy solution by having the high-frequency letters represented by more than a single character, or by several characters, as you see in this slide. I will add that the earliest tract that the world possesses on the subject of cryptography, or for that matter, cryptanalysis, is that which was written in 1474 by a Neapolitan, whose name was Sicco Simonetta. He set forth the basic principles and methods of solving ciphers, simple ciphers no doubt, but he describes them and their solution in a very clear and concise form.

Cipher systems of the type I've described continued to be improved. In this slide is shown what we may call the first complete cipher system of this sort. There are substitution symbols for each letter; the vowels have several equivalents; there are nulls; and there is a small list of arbitrary symbols, such as those for "the Pope", the word "and", the conjunction "with", and so on. This cipher, dated 1411, was used in Venice, and is typical of the ciphers used by the Papal chanceries of those days. ✓

The step remaining to be taken in the development of these ciphers was to expand the "vocabulary", that is, the list of equivalents for frequently-used words, and syllables, the names of persons and places, parts of speech, and so on. This step was reached in Italy during the first half of the 15th Century and became the prototype of diplomatic ciphers used in practically all the states of Europe for several centuries. Here is one of 70 ciphers collected in a Vatican codex and used from about 1440 to 1469. Note that the equivalents of the plain-text items in this slide are Latin words and combinations of two and three letters, and that they are listed in an order that is somewhat alphabetical but not strictly so. I suppose that by constant use the cipher clerk would learn the equivalents almost by heart, so that an adherence to a strict alphabetic sequence either for the plain-text items or for their cipher equivalents didn't hamper their operations too much. In this next slide there is much the same sort of arrangement, except that now the cipher equivalents seem to be digraphs and these are arranged in a rather systematic order, for ease in enciphering and deciphering. Now we have the real beginnings of what we call a one-part code, that is, the same list will serve both for encoding and decoding. These systems, as I've said, remained the prototypes of the cryptography employed throughout the whole of Europe for some centuries. The Papal States used them and as late as 1793 we find them used in France. I wish here to mention specifically the so-called King's General Cipher used in 1572 by the Spanish Court, and I show here a picture of it.

But there were two exceptional cases which show that the rigidity of cryptographic thought was now and then broken during the four centuries we have been talking about in this brief historical survey. Some of the Papal ciphers of the 16th Century and those of the French Court under Kings Louis XIII and XIV exemplify these exceptions. In the case of these French Court ciphers we find that a French cryptologist named Antonio Rossignol, who was employed by Cardinal Richelieu, understood quite well the weaknesses of the one-part codes and syllabaries. It was he who, in about 1648, introduced a new and important improvement, the idea of the two-part code or syllabary, in which for encoding a message the items in the vocabulary are listed in some systematic order, nearly always alphabetical; the code equivalents, whatever they may be, are assigned to the alphabetically-listed items in random order. This means that there must be another arrangement or book for ease in decoding, in which the code equivalents are listed in systematic order, numerically or alphabetically as the case may be, and alongside each appears its meaning in the encoding arrangement, or book. The significance of this improvement you'll find out sooner or later. Codes of this sort also had variants--Rossignol was clever, indeed. One such code, found in the 1691 correspondence of Louis XIV had about 688 items, with code groups of two and three digits. Not at all bad, for those days!

Now this sort of system would appear to be quite secure, and I suppose it was indeed so, for those early days of cryptographic development--but it

wasn't proof against the cleverness of British brains, for the eminent mathematician John Wallis solved messages in it in 1689. Never underestimate the British in this science--as we'll have reason to note in another lecture in this series.

French cryptography under Kings Louis XV and XVI declined, reaching perhaps its lowest level under Napoleon the Great. It is a fact that in Napoleon's Russian enterprise the whole of his army used by a single code book of only 200 groups, practically without variants, even for the high-frequency letters. Furthermore, not all the words in a message were encoded--only those which the code clerk or the writer of the message thought were important. It's pretty clear that the Russians intercepted and read many of Napoleon's messages--this comes from categorical statements to this effect by Czar Alexander I himself. We won't be far wrong in believing that the weaknesses of Napoleon's crypto-communications formed an important factor in Napoleon's disaster. A hundred and twenty-five years later, Russian ineptitude in cryptographic communications lost them the Battle of Tannenberg and knocked them out of World War I.

The other 16th Century Papal ciphers that constituted the second exception to the general similarity of cryptographic systems of those days were quite different from those I've shown you. In this exception the ciphers were monalphabetic, but some letters had the same equivalent, so that on decipherment the context had to be used to decide which of two or more

possible plain-text values was the one meant by each cipher letter. Here's a slide which shows one such cipher used by the Maltese Inquisitor in 1585. You'll note that the digit 0 has two values, A and T; the digit 2 has three values, U, V, and B, and so on. There were two digits used as nulls, 1 and 8; digits with dots above them stood for words such as Qua, Que, Qui, and so on.

Here's a slide which shows how a message would be enciphered, and also how one would be deciphered. A bit tricky, isn't it? Many, many years later Edgar Allan Poe describes a cipher of this same general type, where the decipherer must choose between two or more possible plain-text equivalents in building up his plain text, the latter guiding the choice of the right equivalent. The trouble with this sort of cipher is that you have to have pretty smart cipher clerks to operate it and even then I imagine that in many places there would be doubtful decipherments of words. It wasn't really a practical system even in those days but it could, if used skillfully and with only a small amount of text, give a cryptanalyst plenty of headaches. But such systems didn't last very long because of the practical difficulties in using them.

The first regular or official cipher bureau in the Vatican was established in about 1540, and in Venice at about the same time, about one hundred years before a regular cipher bureau was established in France by Cardinal Richelieu. It is interesting to observe that no new or remarkable ideas for cryptosystems were developed for a couple of hundred years after the complex ones I've

described as having been developed by the various Papal cryptologists. One-part and two-part syllabaries and simple or complex ones with variants were in use for many decades, but later on, in a few cases, the code equivalents were superenciphered, that is, the code groups formed the text for the application of a cipher, generally by rather simple systems of additives. Governmental codes were of the two-part type and were superenciphered by the more sophisticated countries.

The first book or extensive treatise on cryptography is that by a German abbot named Trithemius, who published in 1531 the first volume of a planned 4-volume monumental work. I said that he planned to publish four volumes; but he gave up after the third one, because he wrote so obscurely and made such fantastic claims that he was charged with being in league with the Devil, which was a rather dangerous association in those or even in these days. They didn't burn Trithemius but they did burn his books. This may be a good place to present a slide which shows that the necessity for secrecy in this business was recognized from the very earliest days of cryptology, and certainly by Trithemius. Here is the sort of oath that Trithemius recommended be administered to students in the science of cryptology. All of you have subscribed to a somewhat similar oath, but we now go further and back up the oath with a rather strict law. You've all read it, I'm sure.

We come now to some examples from more recent history. This slide shows a cipher alphabet used by Mary, Queen of Scots, who reigned from 1542 to 1567

and was beheaded in 1587. In this connection it may interest you to learn that question has been raised as to whether the Queen was "framed" by means of this forged postscript in a cipher that was known to have been used by her.

The Spanish Court under Phillip II, in the years 1555-1598, used a great many ciphers and here's one of them. You see that it is quite complex for those early days and yet ciphers of this sort were solved by an eminent French mathematician named Vieta, the father of modern algebra. In 1589 he became a Councelor of Parliament at Tours and then Privy Councelor. While in that job he solved a Spanish cipher system using more than 500 characters, so that all the Spanish dispatches falling into French hands were easily read. Phillip was so convinced of the security of his ciphers that when he found the French were aware of the contents of his cipher dispatches to the Netherlands, he complained to the Pope that the French were using sorcery against him. Vieta was called on the carpet and forced to explain how he'd solved the ciphers in order to avoid being charged with sorcery, a serious offense.

The next cryptologist I want you to know something about is another Italian savant who wrote a book, published in 1563, in which he showed certain types of cipher alphabets that have come down in history and are famous as Porta's Alphabets. Here's an example of the Porta Table, showing one alphabet with key letters A or B, another alphabet with key letters C

or D, and so on. I don't want to go into exactly how the key letters are used; it is sufficient to say that even to this day cryptograms using the Porta alphabets are occasionally encountered.

That Porta's table was actually used in official correspondence is shown by this slide, which is a picture of a table found among the state papers of Queen Elizabeth's time; it was used for communicating with the English Ambassador to Spain. Porta was, in my opinion, the greatest of the old writers on cryptology. I also think he was one of the early but by no means the first cryptanalyst able to solve a system of keyed substitution, that is, where the key is changing consistently as the message undergoes encipherment. Incidentally, Porta also was the inventor of the photographic camera, the progenitor of which was known as the camera obscura.

The next slide shows a picture of what cryptographers usually call the Vigenere Square, the Vigenere Table, or the Vigenere Tableau. It consists of a set of twenty-six alphabets successively displaced one letter per row, with the plain-text letters at the top of the square, the key-letters at the side, and the cipher letters inside. The method of using the table is to agree upon a key word, which causes the equivalents of the plain-text letters to change as the key changes. Vigenere is commonly credited with having invented that square and cipher but he really didn't and, what's more, never said he did. Here's a picture of his table as it appears in his book, the first edition of which was published in 1586. It is more complicated than as described in ordinary books on cryptology.

Here is one more example of another old official cipher. Here are the alphabets on a card which could be slid up and down, as a means of changing the key. Here is another, called the "two-square cipher", or "two-alphabet cipher". It is a facsimile of a State Cipher used in Charles the First's time, in 1627, for communicating with France and Flanders. It involves coordinates and I want you to notice that there are two complete alphabets inside it, intended to smooth out frequencies. The letters of the keywords OPTIMUS and DOMINUS serve as the coordinates used to represent the letters inside the square. Here's part of a cipher used by George III dated the 1st of September 1799.

One writer deserving special attention as a knowledgeable cryptologist in the 17th Century, and the one with whose cipher I'll close this lecture, is Sir Francis Bacon, who invented a very useful cipher and mentioned it for the first time in his Advancement of Learning, published in 1604, in London. The description is so brief that I doubt whether many persons understood what he was driving at. But Bacon described it in full detail, with examples, in his great book De Augmentis Scientiarum, which was published almost 20 years later, in 1623, and which first appeared in an English translation by Gilbert Wats in 1640 under the title The Advancement of Learning. Bacon called his invention the Bilateral Cipher and it is so ingenious that I think you should be told about it so that you will all fully understand it.

In his De Augmentis Bacon writes briefly about ciphers in general and

says that the virtues required in them are three: "that they be easy and not laborious to write; that they be safe, and impossible to be deciphered without the key; and lastly, that they be, if possible, such as not to raise suspicion or to elude inquiry." He then goes on to say: "But for avoiding suspicion altogether, I will add another contrivance, which I devised myself when I was at Paris in my early youth, and which I still think worthy of preservation." Mind you, this was 40 years later! Let's consult Bacon for further details. Here is a slide showing a couple of pages of the Gilbert Wats' translation of Bacon's De Augmentis Scientiarum. Bacon shows what he calls "An Example of a Bi-literarie Alphabet", that is, one composed of two elements, which, taken in groupings of fives, yields 32 permutations. You can use these permutations to represent the letters of the alphabet, says Bacon, but you need only 24 of them, because I and J, U and V, were then used interchangeably. These permutations of two different things--they may be "a's" and "b's", "1's" and "2's", pluses and minuses, apples and oranges, anything you please--can be used to express or signify messages. Bacon was, in fact, the inventor of the binary code which forms the basis of modern electronic digital computers. Bacon gives a brief example in the word "FUGE" --the Latin equivalent for our modern "SCRAM". Here it is, as you see. Here's another example, which quite obviously isn't what it appears to be--a crude picture of a castle, in which there are shaded and unshaded stones. It was drawn by a friend who was a physician and the

message conveyed by it is:

My business is to write prescriptions
And then to see my doses taken;
But now I find I spend my time
Endeavoring to out-Bacon Bacon.

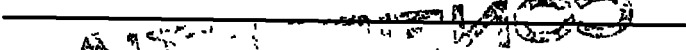
And here's another example, not quite so obvious. The message conveyed is:

KNOWLEDGE IS POWER.

So far all this is simple enough--to much so, Bacon says, for the ✓
example he used in the case of the word FUGE is patently cryptic and would
not avoid suspicion under examination. So Bacon goes on to describe the next
step, which is to have at hand a "Bi-formed Alphabet", that is, one in which
all the letters of the alphabet, both capital and small, are represented by
two slightly different forms of letters. Having these two different forms
at hand, when you want to encipher your secret message you write another
external and innocuous message five times as long as your secret message, using
the appropriate two forms of letters to correspond to the "a's" and "b's"
representing your secret message. Here's FUGE, enciphered within an external
message saying "Manere te volo denac venero", meaning "Stay where you are
until I come." In other words, whereas the real message says "SCRAM", the
phony one says "Stick around awhile; wait for me." Bacon gives a much
longer example, the SPARTAN DISPATCH; here it is, and here's the secret message
which it contains.

Bacon's biliteral cipher is an extremely ingenious contrivance. There
can be no question whatsoever about its authenticity and utility as a valid

cipher. Thousands of people have checked his long example and they all find the same answer--the one that Bacon gives.

Here's a modern example which uses two slightly different fonts of type

 called Garamond and Imprint, and which are so nearly alike that it takes good eyes to differentiate them.

The fact that Bacon invented this cipher and described it in such detail lends plausibility to a theory entertained by many persons that Bacon wrote the Shakespeare Plays and that he inserted secret messages in those plays by using his cipher. If you'd like to learn more about this theory I suggest with some diffidence that you read a book entitled The Shakespearean Ciphers Examined. I use the word diffidence because my wife and I wrote the book which was published in late 1957 by the Cambridge University Press.

In the next lecture we'll take up cryptology as used during the period of the American Revolution by both the Colonial and the British Forces in America.