4-3/6

A PROGENITOR OF [redacted]

Or

CAN CRYPTOLOGIC HISTORY REPEAT ITSELF?

* * * * *

Being a personal account of a cryptanalytic challenge which involved a system very similar to [redacted] and which was successfully met before the dawn of the machine age.

By

William F. Friedman

S-243

21 July 1948

TOP SECRET

FOREWORD

In one respect, the classification of this FOREWORD and of the accompanying papers is a rather remarkable anomaly and one that may be of interest. I shall begin the story by noting that when correctly used, the currently employed [redacted] is, cryptographically, almost an exact replica of a system developed over 30 years ago by the American Telephone and Telegraph Company, for the U. S. Army in World War I. A rather detailed description of the system and its apparatus was disclosed by the American Telephone and Telegraph Company in a technical paper which was written by the principal inventor, an A. T. & T. Co. engineer named Vernam, and which he presented before the midwinter convention of the American Institute of Electrical Engineers at New York City in February 1926. The Vernam paper was later printed in the proceedings of the Institute.[1] It seems almost a certainty that the cryptographic principles on which [redacted] is based stem directly from that paper.

Our records show that the A. T. & T. Co. development was initiated in 1916, but was perfected too late to have been employed extensively for U. S. Army traffic in World War I. A set of four intercommunicating stations was established in the autumn of 1918, primarily for test purposes in the United States,[2] and a limited amount of actual traffic was handled in this system as a preliminary to possible wider usage by the U. S. Army, both in the United States and in Europe in 1918. In the spring of 1919, upon the close of World War I and for a number of reasons, one of which will soon be made clear, the system was abandoned. Some 22 years later, in the face of a real need for secure teletypewriter communications and while awaiting the completion of new equipment specially designed for the purpose, I suggested that the old "double-tape system" be resuscitated by the Signal Corps as an emergency means of teletypewriter crypto-communication. The A. T. & T. Co. was very helpful in this and the emergency system was successfully used from the middle of 1942 until early in 1943, when it was replaced by better ones using more modern equipment.

* * * * * * *

It was the contention of all concerned in the original A. T. & T. Co. development in World War I—the engineers of the company and those of the Signal Corps, as well as the cryptanalysts in the Military Intelligence Division, General Staff, in Washington—that the system and apparatus as developed and proposed for use was "absolutely indecipherable without the keys." Indeed, the Director of the Military Intelligence Division went on record officially to that effect and a copy of the letter, which was actually prepared by Yardley (author of "The American Black Chamber"), is still available in our files.

---

[1] Vernam, G. S., Cipher Printing Telegraph Systems for Secret Wire and Radio Telegraphic Communications, Trans. A.I.E.E., Vol. 45, pp. 109-15, 1926. (Vernam is the man whose name gave rise to the rule which we now call "Vernam addition.")

[2] A document dated 23 Sept. 1918 entitled "Regulations for the Test of the Printing Telegraph Cipher" is still extant.

Of possible interest to the reader are the circumstances under which the apparatus and the system were explained to me in New York, in the early part of May 1918, as I was about to embark for war service in the Code and Cipher Solution Section of G-2, GHQ-AEF, in France. From the summer of 1915 until May 1918, I had been a member of the staff of an institution known as the Riverbank Laboratories at Geneva, Illinois, a private research organization operated by a somewhat eccentric but wealthy Chicagoan named Colonel George Fabyan.[1] One of the fields in which research was conducted at the Riverbank Laboratories by a small staff was that of cryptography, a subject in which I took an interest as an avocation. But soon it became my vocation, when in the latter part of 1916 Colonel Fabyan made me Director of the Department of Ciphers in addition to certain other duties. From then until about the middle of 1918, in a quasi-official relationship with, and at no expense whatever to, the Government (Colonel Fabyan, as a patriotic citizen, footed all the bills), the Department of Ciphers conducted cryptanalytic work for the State, War, Navy, and Justice Departments. None of these large organizations had any cryptanalytic units whatever until the Army established a unit (under Yardley) in the latter part of 1917.[2] It was on the basis of this earlier quasi-official relationship that a disclosure of the details of the A. T. & T. cipher machine and its operation was made to Colonel Fabyan and to me in May 1918, as noted. (Security considerations were just in their infancy!)

As explained to us by the officials of the A. T. & T. Co., the cryptographic system they proposed was based upon the use of two Baudot random-key tapes ([redacted] one exactly 1000, the other, exactly 999 characters in length; both were to be changed daily. Single tapes were never to be used--always both tapes were to be employed simultaneously, in combination, to generate by their interaction a single very long key of 999,000 characters.

I heard nothing more about this machine until April 1919, when I was demobilized and rejoined the staff at the Riverbank Laboratories, to resume my position as head of the Department of Ciphers—with no other duties. The A. T. & T. cipher was then being carefully scrutinized by my staff.

Having had a good opportunity to study the system, the contention of invulnerability to decipherment without the key (the word cryptanalysis had not as yet been coined) was deemed to be unwarranted by the cryptanalytic staff at Riverbank. After noting the results of their theoretical studies and elaborating the results further, I became the principal contestant of the alleged invulnerability of the system. For this and for other reasons, I was directed by Colonel Fabyan to put the results of our studies on paper and thereupon wrote a brief brochure entitled "Methods for the Solution of the A. T. & T. Cipher Machine." The paper was prepared in March 1919 but no copy was sent to Washington at that

---

[1]Courtesy title (an honorary colonel on the staff of the Governor of Illinois). He died in 1935.

[2]The Department of Justice had one roving agent, on the Southern border, who from time to time solved some simple Mexican ciphers, mostly monoalphabetic in nature.

time. Instead, Colonel Fabyan began writing letters to certain people and made what appeared to them to be some rather broad claims.

In August 1919, after a considerable amount of correspondence which was becoming rather acrimonious (largely because Colonel Fabyan, purposely or inadvertently, wrapped a veil of obscurity around what he thought we were able to do), the then Director of Military Intelligence, Brigadier General Marlborough Churchill, sent Major Yardley to Riverbank to look into the claims which Fabyan was making as to the vulnerability of the system. The principles we had elaborated to solve this cipher were explained to Yardley, who returned a few days later, accompanied by Lieut. Colonel Mauborgne, the Signal Corps cryptographic expert who had been directly in charge of the development and who, 20 years later, was to become Chief Signal Officer. The proposed solution was explained to both officers, but Colonel Mauborgne contended that Riverbank really did not know the Signal Corps' method of use. Although it was true that permanently fixed lengths of key tapes (1000 and 999) had been contemplated in the original method as proposed by the A. T. & T. Co., Colonel Mauborgne stated that the Signal Corps had different ideas: the two key tapes, he said, could be variable in their lengths, prime numbers being preferable; and there were other new procedures in their usage which would invalidate the solution proposed by the Riverbank investigators. The record contains the following: "Colonel Mauborgne left with us a rough pencil sketch of the manner in which the machine is now used, reiterating his opinion that as now used, the cipher is invulnerable. ... Colonel Mauborgne said further that if we could break the cipher when used in accordance with these rules he would then acknowledge that we had broken the cipher as used by the Signal Corps."

A day or two after the departure of these officers, two copies of my paper of March 1919 were sent to Washington, one for the Signal Corps, the other for G-2. The conference also resulted in an agreement that Riverbank would accept the gauntlet thrown down by the Government and would try to prove its contention of vulnerability of the cryptographic system by solving a set of "challenge messages."

The Riverbank cipher staff studied the new situation presented by the change in procedures adopted by the Signal Corps and found it unnecessary to change its original position regarding the vulnerability of the system. Again I was asked to put the results of our studies down on paper, and wrote an addendum to the original paper (Addendum No. 1), which is dated 19 August 1919. The Riverbank staff then awaited with confidence (not unmixed, however, with some trepidation) the receipt of a promised set of 150 cipher tapes representing the "challenge messages." These were to consist of messages sent in one day's traffic among four simulated stations forming a simulated net.

Unfortunately, when the cipher tapes arrived, on 27 September 1919, there were found among the "challenge" cipher tapes four plain-text tapes, the latter having been inadvertently included. Rather than accept this "bust" and becloud the issue further, we immediately notified the authorities in Washington of the error and on 8 October 1919 received a new batch of cipher tapes.[1] This time

[1] I must admit, however, that we nevertheless derived considerable benefit from the "bust," for it told us much about the construction of the messages--the nature of the addresses, signatures, etc. It will be seen later how useful this knowledge became in solution. I do not think we could have met the challenge successfully had it not been for this error!

no plain-text tapes were among the challenge messages and the Riverbank staff began its work. The labor was somewhat arduous and after some six weeks' steady work, often 12 hours a day, my collaborators had all deserted me, when all our efforts seemed fruitless and the problem a hopeless one. However, with what appears to me today as rather dogged determination (how I yearn for those days of youth!), I stuck to the task all alone. Finally, on 8 December, exactly two months after receipt of the "good" challenge messages, I, too, came to what seemed the end of the trail--mentally "down but not out."

Reviewing the situation quietly, with my feet on top of my desk and pulling at my pipe (yes, I smoked one in those days!), I came to two conclusions: first, the principles of solution were correct and had to yield the results we were seeking; second, somebody had made an error somewhere in the work and the error had to be found before further progress could be made. What we had received from Washington were perforated tapes and these had to be transcribed into characters on sheets of paper. Could it be that one of my assistants or I had made an error in this first step? There were three crucial messages involved--they had been the raw material for endless experiment--and I decided to check the transcription from the tapes myself. No sooner thought of than I proceeded to the task.

My ruminations were quickly rewarded when I discovered that one character had indeed been omitted accidentally in transcribing one of the three tapes--but that character was at a very crucial point. Making the necessary correction, I called my staff together, explained the situation, and asked for volunteers to tackle the problem once more. There was 100% response (all six of them!), although I could easily detect that my staff remained cynical but had decided to humor me in my fatal delusion. However, it was no delusion, and I, myself, was the lucky one to dispel it. For within ten minutes and with mounting internal excitement (some of my readers will recognize the symptoms) I had obtained, as a resultant of the trial of two hypothetical addresses, the letters EQU. Not much, to be sure--we had often before obtained excellent trigraphs, tetragraphs, and even pentagraphs that turned out to be discouraging accidents. But I continued, thinking to myself: "If the next letter turns out to be a vowel, preferably an I or an A, maybe I really have something here!" The letter that turned up was the letter I--EQUI! Hardly able to repress my excitement, I went on: "In the name of all the patron saints of the Kingdom of Cipher, let the next letter be the letter P," I prayed. And a P it was! "I've got it!" I shouted, "I really have, this time." It was a bit difficult to convince my collaborators and echoes of disbelief reverberated. But soon, gathered about in a tight huddle, a convincing demonstration, consisting of adding a few "good" letters immediately before and after EQUIP, left nothing more to be desired--except the reconstruction of the key tapes. The challenge had been successfully met, but it had taken much longer than had been anticipated.[1]

The two unknown key tapes were reconstructed coincidentally with the solution of a few of the challenge messages and then, to prove beyond shadow of doubt that the system had been solved, we enciphered three messages of our own, addressed to certain officials in Washington, using the reconstructed keys. Our messages were enciphered "by hand," for we did not have any of the machines. The Telephone Company in Chicago kindly gave me access to a keyboard perforator, by means of which, very laboriously (by the "hunt and peck" method), I punched out the cipher tapes. The latter were then sent by mail to Colonel Mauborgne in Washington, where, promptly on

[1]Because of the transcribing error mentioned above. But not all the time lost on that account was sheer waste, for it was during the period of fruitless struggle that all the short cuts were developed which greatly hastened solution once the error had been found.

receipt, they were deciphered by machine with his own key tapes. Colonel Mauborgne immediately thereupon and without reservations acknowledged, as promised, that the validity of the Riverbank contention had thus been fully proved.[1] Soon Colonel Mauborgne and Major Yardley visited us once more, to learn the details. The successful outcome of this experiment naturally called for another addendum to the original paper, and this became Addendum No. 2.

By this time the cryptanalytic staff of the Military Intelligence Division, finding itself in a rather embarrassing position and insisting that the initial point of departure in the Riverbank solution was a knowledge of the starting points of the two key tapes for each message (how true!), proposed that these initial points be disguised by means of a specially prepared small code and then enciphering the code groups by three independent mixed alphabets. The proposed method (but not the code or the special alphabets) was submitted to the Riverbank staff for comment, and I wrote a third addendum to my original paper (Addendum No. 3), proving the inadequacy of the proposed method of disguising the indicators. Two copies of Addenda Nos. 1, 2, and 3 were now sent to Washington. By this time the war was receding into the dim past, the Army authorities were tired or somewhat groggy over the whole business, and thought it best to call a halt to it. As a consequence, further work on the A. T. & T. Co. Cipher Machine was stopped and the machines put in storage. Soon thereafter I left Riverbank to accept the position which was established for me in the Office of the Chief Signal Officer in Washington, as the chief (and only) cryptanalyst. I did a little research, when time permitted, on improvements in the printing telegraph cipher and proposed one which was soon made public by the issue of a patent. (How naive we were in those days! God forbid that the improvement disclosed in this patent be adopted and incorporated in [redacted]!)

* * * * *

In view of the present situation in regard to the [redacted] system, it occurred to me that the Riverbank technical papers on the A. T. & T. Cipher Machine, even though they were written many years ago, might still be of some value or would, at least, be of historical interest. A search through the old files at Arlington Hall yielded a copy of the basic paper, Addendum 1, and Addendum 3, but alas! a very thorough search of all files in Washington failed to turn up a copy of Addendum 2. A letter to the Riverbank Laboratories brought nothing. Colonel Fabyan had long ago departed to the next world, as had his secretary. The Deaprtment of Ciphers had ceased functioning soon after my departure and all its files had been destroyed. So there was no Addendum 2 to be had, which was unfortunate, because it was perhaps the most interesting one of them all: it was the one which dealt in detail with the solution of the challenge messages. The only material I could find among my old and very dusty personal papers was a badly marked up first draft of Addendum No. 2, with many diagrams missing but with considerable number of miscellaneous sheets of notes, queer "doodlings," etc. I

[1] Following is quoted from a letter dated 29 Dec. 1919 from Colonel Mauborgne to Colonel Fabyan: "You have done a great work and your contention of last March is sustained - that the method of using the printing telegraph cipher as used last year by the Signal Corps was decipherable. This is, perhaps, the toughest individual cipher you have ever had to tackle. To the victor belong the spoils!"

do not know whether it was worth the effort, but I have done my best to reconstruct Addendum 2, within the limited time at my disposal. It is not adequate, and I am sure that the final Addendum 2, when it left Riverbank, was a very much better paper. However, it is my hope that some of our workers and collaborators on [redacted] may find in these papers some tiny fragments of interest. For me, they are an echo of interesting events of a distant age; but the thrill of a successful meeting of a serious challenge is still vivid in memory.[1]

I have made no changes whatever in the texts of the basic paper, or in Addendum No. 1 and Addendum No. 3. Because of the unfortunate failure to find Addendum No. 2, I have had to use, as noted above, the first draft. This, too, I have faithfully reproduced without changes of a material nature. The papers should therefore be read, not in the light of the present state of cryptanalytic science, but in the light of the art as it was in 1919— a long time ago, when considered in terms of the progress that has been made since then.

In the light of these resuscitated papers of long ago, one fact takes on a special significance: the present usage of a system over 30 years old points to a lack of sophistication or imagination in cryptographic invention. This lack receives confirmation when we take into consideration other things that we know, and I feel that we should not be too pessimistic about the future. Currently, the [redacted] problem is, in certain respects, much more difficult than the one which confronted the Riverbank staff in 1919. [redacted] than were those involved in the Riverbank solution; but more important by far is this difference: there are [redacted] because in the latter neither key tape was ever used by itself, only in combination, and [redacted] it is frequently the case that the [redacted]; this is something which would have greatly assisted in the Riverbank solution—in fact, it would have eliminated most of the problem.

Finally, there is one more aspect well worth noting and of current interest.

The Riverbank staff solved what was for those days, I think, a very complex problem, and it accomplished the task under circumstances which, considered in the light of what can be done cryptanalytically today, were rather difficult.

In the first place, the staff was very small in numbers and, with one exception, its members had relatively little training in theory and very little practical experience in "operations" as

---

[1]As of possible interest to my readers who may care to look into it, there is on file a paper entitled: "Extracts from correspondence relating to solution of A. T. & T. Printing Telegraph Cipher," together with certain letters which explain why the Extracts were prepared. They give further details of the story and its background.

conducted in these days. In the second place, its procedures and tools were relatively weak and undeveloped, for modern methods and techniques were just in their infancy. In the third place, it had only one set of messages on which its contention of vulnerability had to stand or fall. And if it had failed on that single set, it would have completely fallen down on the job it had undertaken—for no other set of messages, I feel sure, would have been made available to permit another trial to be made. In the fourth place, and possibly of greatest import, the Riverbank staff solved the problem without the aid of machinery of any kind whatever.

Of course, we were always on the lookout for "short cuts" and "hand" aids to speed up the cryptanalytic testing. I do not think we suffered from lack of imagination, but the machine age in cryptanalysis had not yet dawned. Tabulating machinery was just in its infancy; its use as an aid in cryptanalysis was not even conceived.

But the Riverbank staff, small as it was, without adequate training and experience, lacking special machinery, using what may today seem rudimentary methods, and having only a single, relatively small sample to begin with, nevertheless successfully met the challenge offered by the Signal Corps and G-2. Today, with the aid of high-speed electrical and electronic devices, with much advanced cryptanalytic theory, methods, and techniques, with an adequate staff of enthusiastic, competent researchers, and a plurality of sources from which examples to be worked upon can be selected, it seems to me tha [redacted] should not be a hopeless problem. While the odds against our present workers may be greater than they were against the Riverbank workers, the tools and methods of the former are very much better than those of the latter; and over and beyond these considerations there is this one: the urgency, importance, and possible fruits of a successful meeting of the 1948 challenge are so much greater than those of the 1919 challenge that no comparison whatever can be made in these respects. Just as the Riverbank workers met the challenge presented to them in 1919, with far less at stake, so I feel sure our [redacted] workers will successfully meet the far more difficult but much more important challenge offered them in 1948.

W.F.F.

21 July 1948

WILLIAM F. FRIEDMAN

CONTENTS.

1. OPERATION OF CIPHER MACHINE.

Advantages, speed and ease of operation, accuracy and possibilities in the way of difficulty of decipherment.

Weaknesses, danger of overlapping portions of messages; necessity for certain characters which operate the machine and are necessarily a part of the cipher message; reciprocity in cipher square makes easy reconstruction.

2. Solution of single key messages which overlap; detecting overlapping places.

3. Solution of double running key messages which overlap; reconstruction of keys from solved or captured messages.

4. Decipherment by superimposition of cycles with nothing given except that which is inherent in the machine itself. Decipherment of subsequent messages with recovered keys.

5. Length of cycles determined by solution, depending upon key indicators.

6. Cipher square or chart.

(a) How it is constructed, primary form.

(b) Changed from primary into secondary square for convenience.

(c) Reciprocal relations however used. Makes reconstruction of square easy.

PRINCIPLES USED IN THE SOLUTION OF THE A. T. & T. MACHINE CIPHER.

In June, 1918, there was submitted for our examination by the A. T. & T. Company, and the office of the Chief Signal Officer of the United States Army, details and examples of the work of a cipher machine to be used in transmitting secret official communications. After considerable study we have formed the opinion that the system possesses certain weaknesses which permit of an attack upon the cipher and render it unsafe for matters of importance.

We shall try to show first that the slightest carelessness on the part of any individual entrusted with the actual work of enciphering will lay all the messages enciphered by means of the same keys open to easy solution. Since carelessness on the part of the personnel to be entrusted with the operation of the machine and ignorance on their part of the reasons for every precaution necessary in cipher work are to be expected, the existence of this opening for an attack must be admitted. Secondly, we shall attempt to show, granting not only an absolutely infallible operation of the machine by the personnel, but also the theoretical absolute indecipherability of a message enciphered by means of a random-mixed, single, non-repeating, running key, that the mechanics of the machine, and certain features of the system, are such that an attack is not only practicable, but easy under normal conditions.

It will be unnecessary to go into details of the operation of the machine, inasmuch as this report is addressed only to those who submitted it for examination.

We shall discuss the solution of two cases:

(1) Where messages have been enciphered incorrectly, two or more being in the same keys.

(2) Where messages have been enciphered correctly, none being in the same keys.

1. SOLUTION OF A CASE WHERE TWO MESSAGES HAVE BEEN ENCIPHERED BY THE SAME KEYS.

Let us suppose that in the two messages given below the first has been enciphered by the keys indicated and that, through an oversight or carelessness, the second message was then enciphered by the same keys, beginning at exactly the same point in each key. The result of such an error is that both messages have been enciphered by the same single key, and we may disregard for the present the fact that a double key was used. We give the details of the solution of such a case, not because there is anything original or seemingly impossible contained therein, but because certain phases of the principles elucidated will be used later in the discussion of a more complicated case.

M E S S A G E S.

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

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

We may disregard the first seven letters in both messages, since they deal with the key indicators. The next four letters, J,M,Y,Q, being common to both messages, probably represent 4425, (functions of machine: carriage return, line feed, letters). We may begin working, therefore, from that point on, as shown below, putting the messages directly beneath each other.

Mess.1 - 4 R M V M X H M O X 6 N D P Y N 3 R F V 7 G C G 3 N R X Q Y G G
Mess.2 - P R R B S J E 7 H F M 4 F 3 M N O A U F V G C M J X E C I X 3 I

Mess.1 - T E I F O R T T Y G I H J B P S 5 D F J 5 B K W M A X C G X 3 U
Mess.2 - 7 P K 3 G J I T D W I W S E 7 E 2 K Z 2 P 6 S H I 2 5 F L W Y 3

Mess.1 - E L H Y U F Y J N X L K K W U O Y S C R X I E etc. etc. C E L 2
Mess.2 - U Q H A M V L D M T G E 5 G C D V M J T X L Q etc. etc. 4 H Z U

Mess.1 - W C 3 S K C
Mess.2 - F C R 3 L X J P 6 3 Q U Q

Now in all messages we may expect to find both a series of 3's (spaces) and 442 (carriage return and line feed), repeated irregularly at intervals throughout the messages. If we can locate in one of the messages a series of 3's or the combination 442, or any other plain text, then we may find what the plain text of the corresponding portion of the other message is. The complete symmetry of the cipher square, giving rise to reciprocal relations between the three elements, key, plain text and cipher, in a manner to be explained below, makes it possible to recover the single key, given the cipher and the plain text. This is the first weakness in the cipher system.

In this example, we may start off by assuming that the plain text of one of the messages consists of nothing but a series of 3's, and then find out what the plain text of the other message would be on this assumption, by referring to the cipher square; that is, by finding the single key letters concerned for the tentatively deciphered portions and applying them to the corresponding portions in the other message. For example, the first cipher letters in the two messages as arranged for decipherment are 4 and P. If we assume that the plain text equivalent of 4 is 3, then the key letter would be N, in which case the plain text equivalent of P would be G. If, on the other hand, we assume that the plain text equivalent of P is 3, then the key letter would be L, in which case the plain text equivalent of 4 would be G also. But the result of assuming the key letter to be 3, applying it to 4, which gives N, and then applying N to P, is also G; and the result of assuming the key letter to be 3, applying it to P, which gives L, and then applying L to 4, is also G. These relations, as stated above, hold true because of the complete reciprocity of the cipher square. It is clear therefore, that we can omit, for the present, the intermediate step of determining the key letters, and find simply the plain text of the other message directly from the square, by considering only the three elements: assumed plain text, cipher of message 1, and cipher of message 2. This can be done in one operation by proceeding down the columns headed, for example by 4 and P, in the cipher square, until we come to 3 in one of the columns, whereupon it will be found that G is in the other column on the same line as 3, or we can proceed down the columns headed by 4 and 3 to P in one of the columns, whereupon G will be found to be opposite P in the other column on the same line. Any three letters may be chosen to find the fourth in like manner, since the four elements, 4, P, 3 and G, exhibit complete reciprocity. It will be noted that the letters 4, P, 3 and G appear at the four corners of a rectangle in the cipher square, and that there are six times 32, or 192 such rectangles in this square, at the corners of which the letters 4, P, 3 and G will appear. See Fig. 1.

FIG. 1. CIPHER SQUARE

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

Applying this process of assuming one of the messages to consist exclusively of 3's, the plain text of the other message is shown in Fig. 2, on the line labeled "Equivalents of 3."

FIG. 2.

```
Message 1-          4 R M V M X M M O X 6 N D P Y N 3 R F V 7 G C G 3 N R X
Message 2-          P R R B S J E 7 H F M 4 P 3 M N O A U F V G C M J X E C
Equivalents of 3-   G 7 L A X L B O 4 H A 7 7 P F 3 O F C Q G 3 3 2 J Y B Q

Message 1-          Q Y G G T E I F O R T T Y G I H J B P S 5 D F J 5 B K W
Message 2-          I X 3 I 7 P K 3 G J I T D W I W S E 7 E 2 K Z 2 P 6 S H
Equivalents of 3-   Y N G O H W F F I S L 3 O F 3 A R M L 7 B 2 O F F I C A

Message 1-          M A X C G X 3 U E L H Y U P Y J N X L K K W U O Y S C R
Message 2-          1 2 5 F L W Y 3 U Q H A M W L D M T G E 5 G C D V M J T
Equivalents of 3-   V S I 3 N R Y 3 2 E 3 L 5 E A I H D N R H F P Y K X E V

Message 1-          X I E etc. etc.
Message 2-          X L Q etc. etc.
Equivalents of 3-   3 T L
```

Note the underlined portions of what is apparently excellent plain text. The first one spells out 3OF, which suggests 3OF3. Twenty-two letters beyond that we find 3OF3ARM, which suggests 3OF3ARMYS. Five letters beyond that, we find OFFIC, which suggests 3OFFICE3, or 3OFFICER(S)3, or 3OFFICIAL3. These plain text portions may or may not belong to the same message, since we cannot tell yet to which message any tentatively deciphered portion belongs.

Let us now try a series of 442's in place of a series of 3's. In other words, we may assume that one message consists exclusively of a series of 442's, and see what the plain text would be for the other message. We may start by assuming 442 to occur at the beginning of one message, and see what it gives for the corresponding place in message 2, thus:

```
          Message 1 - 4 R M
          Message 2 - P R R
Assumed plain text  - 4 4 2
Equivalents of 442  - P 4 H
```

Since P4H does not constitute any part of a plain text word, we try the sequence 442 one space to the right. Thus:

```
          Message 1 - 4 R M V
          Message 2 - P R R B
Assumed plain text  -   4 4 2
Equivalents of 442  -   4 V S
```

This combination, 4VS, is likewise no part of a plain text word, so we try the sequence 442, one, two, three . . . . . spaces to the right, taking note of all the good combinations which result in the other message. Now, a short cut to this process is to fill out on one line the equivalents of 4; on a line below, the equivalents of 2; then the first two members of any set of the three equivalents of 442 will be found by taking two sequent letters on the first of the two lines of equivalents, and the third member of the set of three equivalents will be found directly to the right of these two letters on the lower line. Thus:

```
      Message 1 - 4 R M V M X                 ( P 4 H
      Message 2 - P R R B S J   Equivalents of 442 ( 4 V S
Equivalents of 4- P 4 V K Z V   in succession:  ( V K 6
Equivalents of 2-     H S 6 H                   ( K Z H
                                                ( etc.
```

Applying this process throughout both messages, we have what is shown in Fig. 3, which includes the equivalents of 3, since we may as well combine the results of both experiments into one figure to see if we can piece together such portions of the tentative decipherment as may be given.

FIG. 3.

```
        Message 1 - 4 R M V M X M M O X 6 N D P Y N 3 R F V 7 G C G 3 N R X
        Message 2 - P R R B S J E 7 H F M 4 F 3 M N O A U F V G C M J X E C
Equivalents of  3 - G 7 L A X L B O 4 H A 7 7 P F 3 O F C Q G 3 3 2 J Y K Q
Equivalents of  4 - P 4 V K Z V Y H 3 O K N N G E 4 H E 2 6 P 4 4 C U B A 6
Equivalents of  2 -     H S 6 H 5 V C L S I I T J 2 V J 4 Z M 2 2 3 F W D Z

        Message 1 - Q Y G G T E I F O R T T Y G I H J B P S 5 D F J 5 B K W
        Message 2 - I X 3 I 7 P K 3 G J I T D W I W S E 7 E 2 K Z 2 P 6 S H
Equivalents of  3 - Y N G O H W F F I S L 3 O F 3 A R M L 7 B 2 O F F I C A
Equivalents of  4 - B 7 P H O 5 E E R D V 4 H E 4 K I T V N Y C H E E R 2 K
Equivalents of  2 - W R M V L Y J J 7 A H 2 V J 2 S N G H I 5 3 V J J 7 4 S

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

        Message 1 - X I E . . . . . etc.
        Message 2 - X L Q . . . . . etc.
Equivalents of  3 - 3 T L
Equivalents of  4 - 4 M V
Equivalents of  2 - 2 P H
```

Immediately preceding SOF3ARM (the result of a series of seven 3's) we have L and before that ERA (the result of 442). Noting that the L can be joined to the ERA and then to the 3OF3ARM, we have the following:

Plain text of one message - O R P S 4 4 2 3 3 3 3 3 3 3 A N
Plain text of other message - 3 G E N E R A L 3 O F 3 A R M Y 4

Immediately following the place where ARM occurs, we have the following:

Plain text of one message - N Y 3 O F F I C
Plain text of other message - 4 4 2 3 3 3 3 3

We can join these two portions, and assuming that ORPS is a part of the name 3SIGNAL3CORPS, we have:

Plain text of one message - 3 S I G N A L 3 C O R P S 4 4 2 3 3 3
Plain text of other message - 3 A D J U T A N T 3 G E N E R A L 3 O

Plain text of one message - 3 3 3 3 A N Y 3 O F F I C
Plain text of other message - F 3 A R M Y 4 4 2 3 3 3 3 3

With this amount of intelligible text to build upon, it is not a difficult matter for the cryptographer to complete the decipherment of these two messages, applying the principles elucidated above, with this modification: that continuation of text in one message results in continuation of text in the other, without a recourse to the assumption of a series of 3's or 442's.

To recover the key we have but to take the plain text of either message, and one of the cipher messages and refer to the cipher square. Were the two messages exactly the same in length, it would be impossible to tell whether the cipher message labeled 1 above applies to the plain text message beginning TO ALL OFFICERS, or to the other message. In this case, however, the messages are not the same length. The endings are as follows:

1. . . . . . C E L 2 W C 3 S K C
2. . . . . . 4 H Z U F C R 3 L X J P 6 3 Q U Q

The decipherment up to the portion where the two messages no longer overlap is as follows:

```
1 . . . . . C E L 2 W C 3 S K C
2 . . . . . 4 H Z U F C R 3 L X J P 6 3 Q U Q
            O F F I C E R 6 M 5
            V O C A T E 3 G E N
```

It is evident that the second message ends ..... VOCATE3 GENERAL3, and we can now attach each cipher to the proper plain text. Cipher message 1 begins TO ALL OFFICERS; cipher message 2, COL J B EMERSON.

The completed work appears as shown in Fig. 4. The solution of such a case present no great difficulties to the decipherer, although the process may be rather slow.

FIG. 4.

```
Single key ----------------- A H Q 4 O L O X C K O 3 Y Z X 2 4 M T
Plain text of one message--  4 4 2 5 T O 3 A L L 3 O F F I C E R S
Plain text of other message- 4 4 2 5 C O L 3 J 3 B 3 E M E R S O N
Cipher - - - - E Y T P P Q P J M Y Q 4 R M V M X M M O X 6 N D P Y
Cipher - - - - E Y T P P Q P J M Y Q P R R B S J E 7 H F M 4 F 3 M

Single key - 4 M U D C H 6 R 5 2 P I V S Z H 2 G Q A S T 4 H H Z V 2
Plain text - 3 O F 3 T H E 3 S I G N A L 3 C O R P S 4 4 2 3 3 3 3 3
Plain text - 3 3 3 C A R E 3 A D J U T A N T 3 G E N E R A L 3 O F 3
Cipher - - - N 3 R F V 7 G C G 3 N R X Q Y G G T E I F O R T T Y G I
Cipher - - - N O A U F V G C M J X E C I X 3 I 7 P K 3 G J I T D W I

Single key - T K X Y D R F Y I L 5 E L P I B 4 P B H W 7 P Z W X G P
Plain text - 3 3 3 A N Y 3 O F F I C E R S 3 I N 3 T H E 3 S I G N A
Plain text - A R M Y 4 4 2 3 3 3 3 3 I T 3 I S 3 R E Q U E S T E D 3
Cipher - - - H J B P S 5 D F J 5 B K W M A X C G X 3 U E L H Y U P Y
Cipher - - - W S E 7 E 2 K Z 2 P 6 S H I 2 5 F L W Y 3 U Q H A M W L

Single key - B 4 W R S B P A Z H 7 4 7 6 R 6 . . etc. . . . . P N 5
Plain text - L 3 C O R P S 3 D E S I R I N G . . etc. . . . . O F F
Plain text - T H A T 3 I N F O R M A T I O N . . etc. . . . . V O C
Cipher - - - J N X L K K W U O Y S C R X I E . . etc. . . . . C E L
Cipher - - - D M T G E 5 G C D V M J T X L Q . . etc. . . . . 4 H Z

Single key - 3 X K C V W Z R M O P N 6 4
Plain text - I C E R 6 M 5
Plain text - A T E 3 G E N E R A L 6 M 5
Cipher - - - 2 W C 3 S K C
Cipher - - - U F C R 3 L X J P 6 3 Q U Q
```

2. SOLUTION OF A CASE GIVEN FIVE MESSAGES CORRECTLY ENCIPHERED, NONE BEING IN THE SAME KEYS.

It is clear that if one key is 1,000 letters in length and the other 999, the resultant single key could not begin to repeat itself until 999,000 letters have been enciphered. This fact obviously precludes the possibility of an attack upon the same principles as explained in the preceding section, since overlapping messages would very rarely, if ever, occur except as the result of errors. While it is true that the resultant single key is a non-repeating, random-mixed key, yet the fact that this single key results from two keys which remain constant, though shifting with regularity, permits an attack to be made upon the system.

It is clear that if a message begins with the keys 001-001, after 1,000 letters have been enciphered, the longer key will have made one complete revolution, and the shorter key will have made one complete revolution plus one letter, resulting in bringing back the longer key to 001 and the shorter key to 002. These two revolutions constitute what we shall term a <u>cycle</u>, and in this instance, the first cycle will have been completed. After 2,000 letters, the longer key will have made exactly two complete revolutions, the shorter one will have made two letters more than two complete revolutions, resulting in bringing the longer key back to 001, and the shorter key to 003. This would be the end of the second cycle. These relations existing between the two keys and the cycles are illustrated graphically in Fig. 5, in which <u>sequent cycles</u> are superimposed.

FIG. 5.

```
Cycle 1. Longer key  - B Q Z V 3 P N V 6 O R K etc. . . V X M
         Shorter key - N V A C X Q 5 R T S B Q etc. . . R K N

Cycle 2. Longer key  - B Q Z V 3 P N V 6 O R K etc. . . V X M
         Shorter key - V A C X Q 5 R T S B Q etc  . . R K N V

Cycle 3. Longer key  - B Q Z V 3 P N V 6 O R K etc. . . V X M
         Shorter key - A C X Q 5 R T S B Q etc . .  R K V N A

Cycle 4. Longer key  - B Q Z V 3 P N V 6 O R K etc. . . V X M
         Shorter key - C X Q 5 R T S B Q etc. . . R K V N A C

          etc.          etc.          etc.     etc.
```

We shall take as the measure of a complete cycle the longer key. Note that we may regard the longer key as stationary, and merely shift the shorter key one letter to the left after each cycle has been completed.

The basis of the attack on this case consists in (1) determining and superimposing sequent cycles; (2) assuming the presence of such characters as 442 and 33333, which cannot be eliminated and still have the machine function properly; and (3) recovering the keys step by step simultaneously with decipherment.

In order to simplify the explanation of this case we shall show first how the double keys are recovered and tested as to correctness, using a certain amount of cipher text with its corresponding plain text, disregarding for the present the question of how the latter is obtained. We shall assume that the portions of text given below belong to the same section of three sequent cycles, and that we have the plain text for the first two cycles.

FIG. 6.

Cipher	- G N U Q R X 5	etc.	
Plain	- 4 4 2 5 A 6 M	etc.	Cycle 1.
Cipher	- 2 S 4 W P W N	etc.	
Plain	- 6 M 5 U N L E	etc.	Cycle 2.
Cipher	- S E 4 Y K I 4	etc.	
Plain	-	etc.	Cycle 3.

Now the successive steps in the recovery of the double key are illustrated graphically in Fig. 7, and the subsequent discussion will refer to the various sections of this figure. We do not know what the combination of letters in the longer and the shorter key is which produces cipher letter G from plain text 4 as the first cipher letter in cycle 1, and cipher 2 from plain text 6 as the first cipher letter in cycle 2. But we may assume in cycle 1 that the first letter in the longer key is A, in which case the corresponding letter on the shorter key must be Z, as shown in (1) of Fig. 7; in cycle 2, remembering that the longer key remains stationary, and that the shorter one shifts one space to the left after each cycle, if the first letter in the longer key is A, then the corresponding letter in the shorter key, to produce cipher 2 from plain text 6, must be G, as shown in (2) of Fig. 7.

PLATE 1.

THE ANALYSIS OF THE A.T.&T. CIPHER MACHINE.

RIVERBANK LABORATORIES, GENEVA, ILLINOIS.

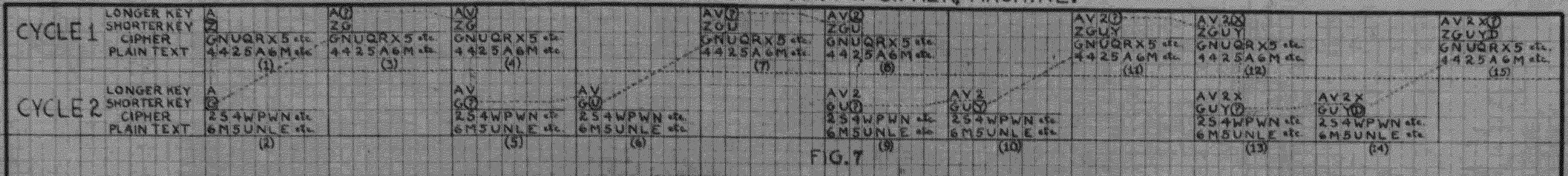


FIG. 7
SHOWING STEPS IN RECOVERY OF KEYS.

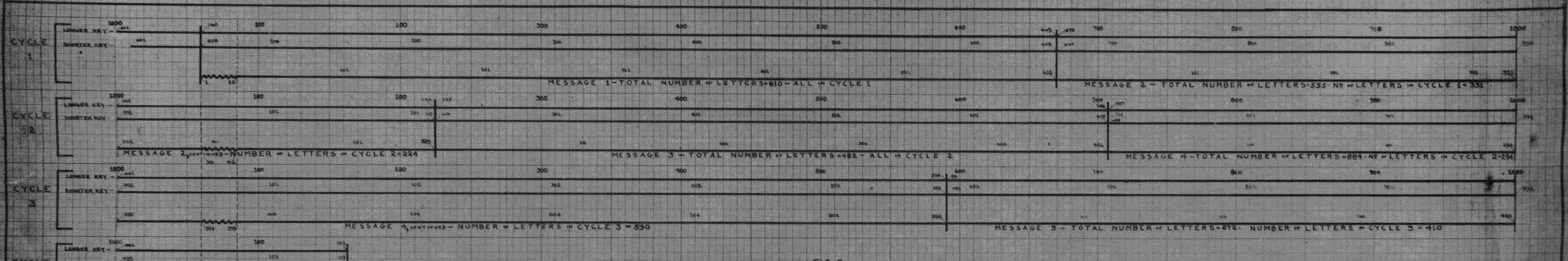


FIG. 8
SHOWING SUPERIMPOSED CYCLES AND SECTION TAKEN FOR ANALYSIS.

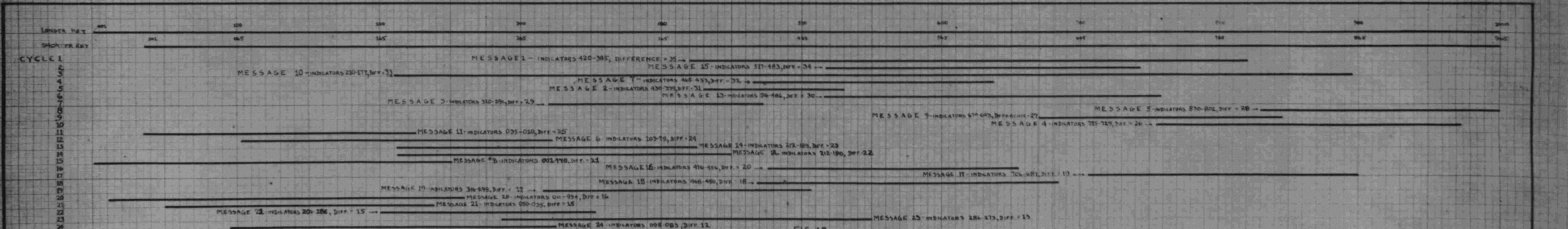


FIG. 18
SHOWING SUPERIMPOSED CYCLES ARRANGED ACCORDING TO THE KEY INDICATORS GIVEN.

This is an enlargement of preceding plate 7

W.F.F.

Now since the shorter key has shifted one letter to the left in cycle 2, the letter G can be placed next to Z on the shorter key in cycle 1. See (3) of Fig. 7. If the letter in the second position on the shorter key in cycle 1 is G, in order to produce cipher N from plain text 4, the corresponding letter in the same cycle on the longer key must be V. See (4) of Fig. 7. We may now place V next to A on the longer key in cycle 2. See (5) of Fig. 7.

In order to produce cipher letter S from plain text M in conjunction with V as the letter in the longer key, the second letter on the shorter key in cycle 2 must be U. See (6) of Fig. 7. We may now place U next to G on the shorter key in cycle 1, as shown in (7) of Fig. 7, and find the corresponding letter on the longer key. It is 2. See (8) of Fig. 7.

The process set forth is continued, resulting finally in the reconstruction of a double key which will produce from the cipher letters given in both cycles the correct corresponding plain text. Thus:

Cycle 1.	Longer key -	A V 2 X 7 M V
	Shorter key -	Z G U Y D G X
	Cipher - - -	G N U Q R X 5
	Plain text -	4 4 2 5 A 6 M
Cycle 2.	Longer key -	A V 2 X 7 M V
	Shorter key -	G U Y G G X W
	Cipher - - -	2 S 4 W P W N
	Plain text -	6 M 5 U N L E

We may test the correctness of these keys by applying them to cycle 3. Thus:

Cycle 3	Longer key -	A V 2 X 7 M V
	Shorter key -	U Y D G X W
	Cipher - - -	S E 4 Y K I
	Plain text -	E R A L L Y

We see here the ending of a word like GENERALLY and we may feel sure of our keys.

Now in the reconstruction of our keys above, we began arbitrarily with A as the first letter in the longer key. We might have begun with any other one of the 32 possible letters of which the cipher square is composed, and thus build up another pair of keys which, though in external appearance althogether different from the pair recovered above, would serve just as well as the latter. In short, it is possible to derive 32 different pairs of keys, any pair of which might be the original pair, but since all pairs give equivalent results, it will be unnecessary to find out which pair was really the original.

In the preceding example, the decipherment of superimposed portions of cycles 1 and 2 was given, it having been stated that we should disregard for the moment the question of how this decipherment was procured. We shall now proceed to the next step, which is to decipher and reconstruct the keys simultaneously, given no decipherment whatever to start with. For this case we shall show the steps in the actual solution of a problem where only five messages have been intercepted. Since the principles to be elucidated require but a small part of a larger body of text, it will not be necessary to give the whole of each of these five messages. We shall show first merely the key indicators and the length of each message.

KEY INDICATORS AND LENGTH OF MESSAGES.

1. 060-050. Length, 610 letters.

2. 670-660. Length, 555 letters.

3. 225-216. Length, 482 letters.

4. 707-698. Length, 884 letters.

5. 591-583. Length, 572 letters.

Assuming keys of 1,000 and 999 letters, we may indicate graphically the relative positions in which these messages will fall by a diagram such as that shown in Fig. 8. In this diagram we show exactly where each message begins and ends, what the key indicators are, etc. We can take for experiment any vertical section of these superimposed cycles. Let us take the section consisting of 25 letters in each of messages 1, 2, 4 and 5 as indicated by the serrated lines in Fig. 8. This diagram shows that letters 1 to 25 of message 1, 391 to 416 of message 2, 354 to 379 of message 4 and 470 to 495 of message 5 fall within this section. We therefore take those letters from our messages. They are as follows:

Message 1. Letters 1-25.

5Y27C 3RNK6 R72QA J4UX6 CJOAJ

Message 2. Letters 391-416.

5JBOB G3L77 D7SVZ BTVIR 5OBRG

Message 4. Letters 354-379.

XCHLT JQJUH WA5C3 WWMBF ST7UI

Message 5. Letters 470-495.

CXURW K3Z2Y F7ON2 GVRNP 26NTR

Let us place these four portions directly beneath one another. Thus:

FIG. 9.

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

Now if we can find the plain text for the series of letters which fall directly beneath one another in cycles 1 and 2 we can begin to reconstruct the keys. It becomes a question therefore of assuming the plain text for the first few letters of cyles 1 and 2, recovering the keys upon the basis of such tentative decipherment and then testing them upon cycles 3 and 4. If the tentative decipherment is correct, the application of the double key to cycles 3 and 4 must result in the production of intelligible text. If such a result is not attained then it means that the tentative decipherment upon which the recovered double key is based is not correct, and we proceed to try a different tentative decipherment for cycles 1 and 2. The incorrect assumption can involve eithereor both of the series of tentatively deciphered letters. Obviously, if we can be certain of the decipherment of one of the series we will be on surer ground and will have to modify our assumption only for the other of the series when our trials of recovered keys prove the tentative decipherment to be incorrect. Now the beginning of nearly every message can be assumed to be 4425, in order to insure a proper adjustment of the receiving machine. Let us begin therefore by assuming that our message 1 starts with 4425, and since the portion of this message which falls within the section to be analyzed contains letters 1 to 25, we may insert tentatively the decipherment of the first four letters of message 1 as 4425. Then let us assume for the moment that the portion directly beneath in message 2 consists of a series of 3's, reconstruct the keys for these two portions (as illustrated in Fig. 7) and test them on cycles 3 and 4. The result of these steps is shown in Fig. 10.

FIG. 10

Longer key - A S R 4
Shorter key - H O R Q
Cycle 1. Cipher - 5 Y 2 7 C 3 R N etc.
Assumed plain text - 4 4 2 5

Longer key - A S R 4
Shorter key - O R Q H
Cycle 2. Cipher - 5 J B O B G 3 L etc.
Assumed plain text - 3 3 3 3

Longer key - A S R 4
Shorter key - R Q H
Cycle 3 Cipher - X C H L T J Q J etc.
Resultant plain text-H M R

Longer key - A S R 4
Shorter key - Q H
Cycle 4. Cipher - C X U R W K 3 Z etc.
Resultant plain text-G N

These results prove that the assumption of a series of 3's for the beginning of cycle 2 is incorrect, since the letters given for cycles 3 and 4 form unintelligible text. We therefore try out another probable combination for message 2, such as RE3, retaining as our decipherment of the corresponding portion of message 1 the combination 4425, and see what result this gives. A list of the polygraphs which would recur most frequently, and which would be tested in conjunction with 4425 for message 1, is given in the following table:

33333	3OF3T	IN3T	3WIT
3THE3	ATI	WA-S,R	D3TH
3AND3	HAT3	VER	S3IN
ING3	EST3	IT-3,H	S3TH
ERE3	HE(3)S	T3TH	TER (3)
3THA	TION3	3ARE3	RE(3)A
ENT3	E3TH	N3TH	6M53
HE(3)R(3)	HIS3	3ALL3	6N53
	3ON3		

The successive trials take very little time, since the correctness of any trial is speedily proved or disproved by applying the resultant keys to cycles 3 and 4. In this case, the trial of the polygraph 3ON3 results in excellent combinations in cycles 3 and 4. Thus:

FIG. 11.

```
                Longer key      - A S P M
                Shorter key     - H O P A
Cycle 1.        Cipher          - 5 Y 2 7 C 3 R N etc.
                Assumed plain text - 4 4 2 5

                Longer key      - A S P M
                Shorter key     - O P A 7
Cycle 2.        Cipher          - 5 J B O B G 3 L etc.
                Assumed plain text - 3 O N 3

                Longer key      - A S P M
                Shorter key     - P A 7
Cycle 3.        Cipher          - X C H L T J Q J etc.
                Resultant plain text - 4 4 2

                Longer key      - A S P M
                Shorter key     - A 7
Cycle 4.        Cipher          - C X U R W K 3 Z etc.
                Resultant plain text - C O
```

It is evident that in cycle 3 we have struck a "carriage return and line feed;" in cycle 4, we probably have a word beginning with CO, and we can try to build upon this digraph such words as suggest themselves, as the following:

CODE	COMMAND	CONTRACT	
COLUMN	COMPANY	CONVOY	
COLLECT	CONDITION	COPY	
COME	CONNECT	CORRECT	
COMING	CONSIDER	COST	etc. etc.

It may take considerable time to test out all of the words which suggest themselves, but it is only the start which is laborious, for after this the messages almost solve themselves. Let us see what happens when we try COMMAND. Given (P / ? / U / M) in cycle 4, the blank letter is F. This enables us to place F beneath M in the lower key in cycle 3, and gives A as the plain text letter. Given (M / ? / R / M) in cycle 4, the blank letter is R.

With these additional lower key letters in place throughout our decipherment we have the following:

FIG. 12

Cycle 1.	Longer key	A S P M
	Shorter key	H O P A 7 F R
	Cipher	5 Y 2 7 C 3 R N etc.
	Assumed plain text	4 4 2 5
Cycle 2.	Longer key	A S P M
	Shorter key	O P A 7 F R
	Cipher	5 J B O B G 3 L etc.
	Assumed plain text	3 O N 3
Cycle 3	Longer key	A S P M
	Shorter key	P A 7 F R
	Cipher	X C H L T J Q J etc.
	Resultant plain text	4 4 2 A
Cycle 4	Longer key	A S P M
	Shorter key	A 7 F R
	Cipher	C X U R W K 3 Z etc.
	Resultant plain text	C O M M A N D

We are now ready to determine the next letter in the longer key. In the column headed by the letter to be sought, in cycle 1 we have (? (7 (C (? ; in cycle 2, (? (F (B (? ; in cycle 3, (? (R (T (? .

It is evident that we want such a letter in the upper key as will produce the best plain text letters from the given cipher letters to add to the already deciphered text. We could try out all the letters of the alphabet in turn, beginning with A, thus:

If A is the upper key letter then) in cycle 1, (A (7 = F; (C in cycle 2, (A (F = Q; (B in cycle 3, (A (R = B (T

If B is the upper key letter then) in cycle 1, (B (7 = Q; (C in cycle 2, (B (F = F; (B in cycle 3, (B (R = A (T

If C is the upper key letter then) in cycle 1, (C (7 = 7; (C in cycle 2, (C (F = G; (C in cycle 3 (C (R = H (T

etc. etc. etc.

A short cut to the finding of these successive equivalents is accomplished by the use of the alphabets of the cipher square cut apart and mounted upon strips. It will be noticed that the successive equivalents for the combination 7/C in cycle 1 are F, Q, 7, ... ; for the combination F/B in cycle 2, Q, F, G, ... ; for the combination R/T in cycle 3, B, A, H, ...

Now note the alphabets in the cipher square headed by the intersection letters of the combinations 7/C, F/B and R/T, viz., C, H, and G, respectively. In the C alphabet the sequence begins F, Q, 7, ... It is evident that this alphabet will give the complete sequence of letters resulting from the application of the successive letters of the alphabet to the combination $\overset{7}{C}$. The H alphabet will likewise give the complete sequence of letters resulting from the application of the successive letters of the alphabet to the combination $\overset{F}{B}$; and the G alphabet will give those applying to $\overset{R}{T}$. Therefore, if we take the alphabets of the cipher square, cut them apart, mount them on strips, select those headed by the letters C, H, and G, and set them so that the letters of all three coincide throughout their length, we have the complete series of letters resulting from the application of the successive letters of the alphabet to these combinations. The successive letters or equivalents of this operation will all be found on the same horizontal lines. By setting the 7 alphabet opposite our strips, the letter in the longer key necessary to produce the equivalents which fall on the same line will be indicated on the 7 alphabet at the same time, as shown in Fig. 13.

FIG. 13.

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

If the high frequency letters appear in red on these strips, we can begin by selecting that horizontal line which contains all red letters. In this case, with V as the letter in the longer key for the column under discussion, the three high frequency letters, T, R, and 3 are given. These, added to our partial decipherment, give the following:

FIG. 14

Cycle 1	Longer key -	A S P M V
	Shorter key -	H O P A 7 F R
	Cipher -	5 Y 2 7 C 3 R N etc.
	Plain text -	4 4 2 5 T
Cycle 2.	Longer key -	A S P M V
	Shorter key -	O P A 7 F R
	Cipher -	5 J B O B G 3 L etc.
	Plain text -	3 O N 3 R
Cycle 3.	Longer key -	A S P M V
	Shorter key -	P A 7 F R
	Cipher -	X C H L T J Q J etc.
	Plain text -	4 4 2 A 3
Cycle 4.	Longer key -	A S P M V
	Shorter key -	A 7 F R C
	Cipher -	C X U R W K 3 Z etc.
	Plain text -	C O M M A N D

```
                  (V
                  (?
In cycle 4 we have (W which gives C as the corresponding let-
                  (A
```

ter in the shorter key, as shown already in Fig. 14. We may try out in cycle 2 the letter E after R. This would give Z as the letter in the longer key for that column. Applying Z to all the combinations in this column, we have the following:

FIG. 15

```
              Longer key - A S P M V Z
             Shorter key - H O P A 7 F R C
Cycle 1.          Cipher - 5 Y 2 7 C 3 R N etc.
              Plain text - 4 4 2 5 T O

              Longer key - A S P M V Z
             Shorter key - O P A 7 F R C
Cycle 2.          Cipher - 5 J B O B G 3 L etc.
              Plain text - 3 O N 3 R E

              Longer key - A S P M V Z
             Shorter key - P A 7 F R C
Cycle 3.          Cipher - X C H L T J Q J etc.
              Plain text - 4 4 2 A 3 H

              Longer key - A S P M V Z
             Shorter key - A 7 F R C L
Cycle 4.          Cipher   C X U R W K 3 Z etc.
              Plain text   C O M M A N D
```

The first message begins with TO, and we may place a 3 after it. This gives the letter in the longer key which applies to that column, viz., 3; and this, in turn, gives the plain text letter C following E in cycle 2, making it probable that the word is RECEIPT or RECEIVING or RECORD etc. Thus:

FIG. 16.

```
              Longer key - A S P M V Z 3
             Shorter key - H O P A 7 F R C
Cycle 1.          Cipher - 5 Y 2 7 C 3 R N etc.
              Plain text - 4 4 2 5 T O 3

              Longer key - A S P M V Z 3
             Shorter key - O P A 7 F R C
Cycle 2.          Cipher - 5 J B O B G 3 L etc.
              Plain text - 3 O N 3 R E C

              Longer key - A S P M V Z 3
             Shorter key - P A 7 F R C
Cycle 3.          Cipher   X C H L T J Q J etc.
              Plain text   4 4 2 A 3 H

              Longer key - A S P M V Z 3
             Shorter key - A 7 F R C
Cycle 4.          Cipher - C X U R W K 3 Z etc.
              Plain text - C O M M A N D
```

From the combination (Z (? (K in cycle 4, L is given as the letter in the shorter key, which, in turn, in cycle 3, in (N (3 (L (Q (?, gives the plain text letter E, suggesting the word HEAVY. We can test out the words which suggest themselves in cycles 2 and 3, and see what we get in cycles 1 and 4; or we can test out the words which suggest themselves in one cycle by applying the resultant key letters to any other cycle at the proper point.

Enough of the procedure has been shown to prove that the method is perfectly practicable. If 4425 tried out at the beginning of the message does not yield good results, there are many other places to try out the same combination further along; for this combination, 442, must appear at intervals of approximately 55 to 70 letters. Or, this failing, the ends of messages can be tested for 6M5, i. e., "period." Should the decipherer be fortunate enough to find two messages which begin within one or two letters of one another in sequent cycles, then it will be unnecessary to assume any plain text other than 4425. Or, if he should find that the beginning of one message falls within the same section as the end of another, the plain text will be 4425 and 6M5. When a place is reached where the proper continuation of the messages is difficult by reason of the failure of the preceding text to suggest the succeeding text, recourse is had again to the alphabet strips.

It is to be noted further that these alphabet strips may be used to find the letters in the shorter key as well as those in the longer key. The arrangement of the messages into sequent cycles is such that the letters of the shorter key are similar on diagonal lines. Given the letters of the longer key and the cipher on a diagonal line, one proceeds to set the strips, applying the same principles as before, remembering only to add the high frequency combinations found diagonally on the strips in the messages as arranged for decipherment. The letter opposite the high frequency combination on the 7 alphabet, will be the diagonally constant letter of the shorter key.

The complete decipherment together with the double key for these partial messages is shown in Fig. 17.

FIG. 17.

Longer Key	- A S P M V Z 3 E K 7 O J N A L I R B G U 3 H W F D
Shorter Key	- H O P A 7 F R C L D P E K Z T U M P A 3 U L F 7 A
Cipher	- 5 Y 2 7 C 3 R N K 6 R 7 2 Q A J 4 C X 6 C J O A J
Plain text	- 4 4 2 5 T O 3 A L L 3 R E S E R V E 3 O F F I C E
Longer Key	- A S P M V Z 3 E K 7 O J N A L I R B G U 3 H W F D
Shorter Key	- O P A 7 F R C L D P E K Z T U M P A 3 U L F 7 A V
Cipher	- 5 J B O B G 3 L 7 7 D 7 S V Z B T V I R 5 O B R G
Plain text	- 3 O N 3 R E C E I P T 3 O F 3 A N 3 O R D E R 3 F
Longer Key	- A S P M V Z 3 E K 7 O J N A L I R B G U 3 H W F D
Shorter Key	- P A 7 F R C L D P E K Z T U M P A 3 U L F 7 A V C
Cipher	- X C H L T J Q J U H W A 5 C 3 W W M B F S T 7 U I
Plain text	- 4 4 2 A 3 H E A V Y 3 B A R R A G E 3 O N 3 T H E
Longer Key	- A S P M V Z 3 E K 7 O J N A L I R B G U 3 H W F D
Shorter Key	- A 7 F R C L D P E K Z T U M P A 3 U L F 7 A V C 2
Cipher	- C X U R W K 3 Z 2 Y F 7 O N 2 G V R N P 2 6 N T R
Plain text	- C O M M A N D I N G 3 6 W W I 5 T H 3 M I N E W E

We have seen that the knowledge of the length of the key was necessary in order to arrange the messages in the preceding case for decipherment. Granting that the lengths of the tapes bearing the keys would be changed from day to day, and that "breaks" between messages would be made, it would nevertheless be an easy matter for the enemy to superimpose cycles correctly, without a knowledge of these lengths or these "breaks", since the key indicators which must accompany each message afford ample data for the placement of messages. For instance in the preceding case we can determine the cycles to which each message belongs relative to the first message, merely by finding the difference between the key indicators for the several messages, though we may not know how much of a message is to be found in one cycle and how much in the next cycle. Thus, the indicators for message 1 are 060 and 050, the difference being 10. Those for message 2 are 670 and 660, the difference also being 10. Therefore, the beginning of the second message is in the same cycle as the whole of message 1. The indicators for message 3 are 225 and 216, the difference being 9. This shows that message 3, with respect to message 1, is in cycle 2; since in the first message the two key tapes are 10 letters apart as regards their points of origin, and in the third message only nine letters apart. Now the difference between 225 and 060 is 165. So that we may place the first letter of message 3, which belongs to cycle 2, under the 165th letter of message 1. We can now fit in the portion of message 2 which belongs in the second cycle, since we note that the placement of message 3 allows room for 225 letters of message 2 in cycle 2, leaving 330 letters, which will be exactly enough to fill up 1,000 letters in the first cycle. However, we do not need to do even this much, for we can work with beginnings of messages. Thus, given the following series of key indicators for as many messages, they can be arranged as shown in Fig. 18.

MESSAGES

Message	Indicators	Difference	Cycle	Message	Indicators	Difference	Cycle
1	420-385	35	1	14	212-189	23	13
2	430-399	31	5	15	517-483	34	2
3	320-291	29	7	16	476-456	20	16
4	755-729	26	10	17	706-687	19	17
5	830-802	28	8	18	468-450	18	18
6	103-079	24	12	19	316-299	17	19
7	465-433	32	4	20	011-994	16	20
8	001-978	21	15	21	050-035	15	21
9	670-643	27	9	22	200-186	14	22
10	210-177	33	3	23	286-273	13	23
11	035-010	25	11	24	095-083	12	24
12	212-190	22	14	25	001-989	11	25
13	516-486	30	6				

There are several points where an attack may be made, when the messages are arranged as shown in Fig. 18. Both keys may be recovered completely or nearly so. No matter how the key indicators may be used, given a sufficient amount of intercepted traffic, enough text can be obtained to make it possible to arrange the cycles with reference to one another so that a solution may be achieved. The cryptographer is guided by the key indicators in his arrangement of messages preparatory to decipherment and not by the order in which they happened to have been sent.

ADDENDUM I.

OPINION BASED UPON THE SIGNAL CORPS' MODIFIED METHOD OF USING

THE A. T. & T. MACHINE CIPHER.

The purpose of this memorandum is to set forth our opinion, with the reasons, that the A. T. & T. machine cipher as now used by the Signal Corps is decipherable by the same principles as already established and as already admitted to be effective by the representatives of the M. I. D. and the Signal Corps.

The following is a transcript of the rules for the operation of the machine for cipher purposes, as set forth in a pencil memorandum by Lt. Col. J.O.Mauborgne.

Order of Punching Tape.

10 line feeds
6 letters representing numerals of tape settings
as PPPTWT (000525)

During Capt.
Fowler's time
enciphering began here.
Letter — or letters designating cipher office, as "X", "NP" etc.
Figure shift (6)
Cipher bureau serial number of message
Space (3)
Figures (6)
Check or word count in numerals
Letters — line feed (5-2)
Place from —
Date
Time filed
Carriage return — line feed.

Early 1919
Enciphering
begins
Name — address — body of message — signature
Enciphering ends.
One line feed — 15 carriage returns.

Note — Tapes A and B vary in length depending upon number of letters to be sent in one day. For example, we might use 700 on the A tape and 699 on the B, or 650 on the A tape and 365 on the B, etc.

* * * * *

The differences between the original method and the modified method of using the machine can be summarized as follows:

ORIGINAL METHOD	MODIFIED METHOD
TAPES	
1. One tape is one letter longer than the other tape.	1. One tape may be any number of letters longer than the other tape.
2. The number of letters in each tape is constant from day to day.	2. The tapes vary from day to day.

SHIFTING THE TAPES

3. The tapes are either not shifted at all between messages or are shifted together the same number of letters.

3. The tapes are shifted an unequal number of letters after each message. For example, the A tape may be shifted 10 spaces, the B tape 14.

BEGINNING OF ENCIPHERED MESSAGE

4. Each message begins with the functions represented by 4425.

4. The enciphered portion of message begins at once with the name and address of the person to whom the message is sent.

USE OF FUNCTIONS AND PUNCTUATION

5. All functions and punctuation are used as in ordinary typewritten matter.

5. Some functions and punctuation may or may not be used, i. e., there may be spaces (3) between words, commas (6N5), paragraphs (44233333) etc., with the exception of (442) which is absolutely necessary for the functioning of the machine.

We shall now show that these differences as set forth above do not change the nature of the cipher in a manner so as to prevent an attack by exactly the same principles as elucidated before, first, because it is unnecessary to know either the lengths of the tapes, or by how much they differ, secondly, because the shifting of the two tapes an unequal number of letters has no bearing upon the case at all, third, that even should the encipherment begin with some unknown text and not with the functions 4425 that there is a sufficient number of possibilities to try out in other places; and fourth, that the presence or absence of certain functions and of punctuation may make the problem a little more difficult but by no means unsolvable.

1. THE TAPES.

In order to eliminate all ambiguity we shall define the word "cycle" and the phrase "sequent cycles" as follows:

(a) CYCLE. That relation which exists between the two key tapes after one tape has made one complete revolution. Cycles may be measured by either the longer tape or the shorter tape, and in our work we have used the longer tape as the measure of a cycle.

(b) SEQUENT CYCLES. Two cycles are sequent when the longer tape occupies the same absolute position in both cycles and the shorter tape is displaced one and only one letter in one cycle as compared with the other. In all the drawings and figures this displacement is to the left. When the key indicators for one message differ by an amount, X, and those for another message differ by X + 1 or X - 1, then we have a case of sequent cycles. When the lengths of the key tapes are unknown this difference must be expressed in terms of either a positive or a negative quantity. Example: Key indicators 075 - 125, difference = -50. Key indicators 125 - 075, difference = + 50.

In the original method the knowledge that the two tapes differed by but one letter in length enabled us to say that sequent cycles represented a displacement of the shorter tape of but one letter each time. This, in turn means that sequent revolutions of the longer tape coincide with sequent cycles. In other words, a progression from say the end of the second revolution to the end of the third revolution means a progression of one complete cycle and represents a displacement of one letter of the shorter tape.

If the tapes differ in length by more than one letter, for example, if the two tapes differ by 50 letters, then the displacement of the shorter tape will be 50 letters per revolution of the longer tape, in which case it is clear that sequent revolutions of the longer tape will not coincide with sequent cycles.

Fig. 18 and the discussion applying to it shows clearly that these messages were superimposed by reference to the key indicators only. The crucial point is this, that in the solution of a single long message a knowledge of the lengths of the key tapes is absolutely essential; without this knowledge the length of a cycle and the displacement in sequent cycles never can be determined, which in turn means an inability to superimpose cycles so that the principles of solution can be applied. But in the solution of a series of messages a knowledge of the lengths of the key tapes is entirely unnecessary, since sequent cycles are determined not from such a knowledge but solely from the key indicators for the respective messages. The displacement in sequent revolutions may be any number of letters, a matter of no concern to us, but the displacement in sequent cycles (according to our definition of the phrase) is always one letter, and there can be no doubt that that messages in sequent cycles can be found, as will be illustrated below. To sum up, therefore, a knowledge of the lengths of the two tapes is entirely unnecessary for the superimposition of cycles, preparatory to decipherment of a series of messages.

2. DAILY VARIATION IN LENGTHS OF TAPES.

The fact that there is a daily variation in the lengths of the tapes in the modified method as compared with a constant length in the original method has no bearing upon the case because as stated in the preceding section, a knowledge of the lengths of the tapes is unnecessary for the solution of a series of messages, and secondly, because the fact of constancy in the lengths (as was the case in the original method) is per se of no importance in such a solution.

3. SHIFTING THE TAPES.

The shifting of the tapes, together or singly, equal or unequal distances in all instances has no bearing upon the case, because such shifting does not preclude the possibility of the occurrence of sequent cycles. As a matter of fact, the unequal shifting of the tapes, after each message, is a highly dangerous procedure because it makes possible the accidental encipherment of two messages by an identical resultant single key, i. e., such proceeding introduces many possibilities of "overlaps." Every case in which the difference between the key indicators is the same represents a case of an "overlap".

4. FUNCTIONS ELIMINATED AT BEGINNING.

The fact that in the original method messages began to be enciphered with the functions 4425 only eliminated the necessity of assuming plain text for the beginning of a message, i. e., if we know that each message begins with 4425, the trial of the most frequently recurring polygraphs in the corresponding position in the next sequent cycle is all that is necessary to get a start. However, in the modified method there remain many other points of attack, for the encipherment begins with a name and an address. This must contain, in military messages, titles, initials, punctuation and functions such as figure and letter shifts, period, spaces. All of these afford easy openings for attack, especially in view of the fact that the sending and the receiving stations can be determined with a fair degree of probability.

5. ELIMINATING PUNCTUATION etc.

The elimination of all punctuation, and such functions as space and paragraph would not complicate the solution any more than their absence in ordinary cipher messages does. However, the functions 442 (carriage return and line feed) are absolutely necessary for the proper operation of the machine and therefore their elimination is impossible. The length of lines is not highly variable in nature, and it is reasonably certain that in the body of the message the functions 442 must recur at intervals approximating 60 letters.

The indicators and lengths of the following series of 17 messages illustrate the foregoing points. This series of hypothetical messages was drawn up according to the rules as laid down in the memorandum submitted by the Signal Corps, and represent what happens in the traffic of only one station of possibly four. This station has been assigned one fourth of the length of one tape, in accordance with the plan set forth. The tapes for the day are 700 and 670 letters in length. Station 1 has been assigned the region from 001 to 160 on the shorter tape. At no time must the difference between the key indicators exceed 160, otherwise Station 1 will be encroaching upon the region assigned to another station, or as we shall say, he will be "out of bounds." The data for this series of hypothetical messages are as follows:

TAPES

700 - 670

Message 1.
076 - 055 (a) = 21 (b)
361 - 361 (c)
437 - 416 (d)

2.
442 - 417 (a) =25 (b)
206 - 206 (c)
648 - 623 (d)

3.
418 - 362 (a) =56 (b)
368 - 368 (c)
786 - 730
700 - 670 (e)
086 - 060 (d)

4.
090 - 068 (a) = 22 (b)
585 - 585 (c)
675 - 653 (d)

5.
362 - 262 (a) = 100 (b)
287 - 287 (c)
649 - 549 (d)

6.
655 - 550 (a) = 105 (b)
688 - 688 (c)
1343 -1238
700 - 670 (e)
643 - 568 (d)

7.
649 - 597 (a) = 52 (b)
305 - 305 (c)
954 - 902
700 - 670 (e)
254 - 232 (d)

8.
259 - 232 (a) = 27 (b)
323 - 323 (c)
582 - 555 (d)

9
195 - 076 (a) = 119 (b)
447 - 447 (c)
642 - 523 (d)

10.
658 - 532 (a) = 126 (b)
487 - 487 (c)
1145 -1019
700 - 670 (e)
445 - 349 (d)

11.
449 - 385 (a) = 64 (b)
508 - 508 (c)
957 - 893
700 - 670 (e)
257 - 223 (d)

12.
260 - 236 (a) = 24 (b)
418 - 418 (c)
678 - 654 (d)

13.
480 - 350 (a) = 130 (b)
216 - 216 (c)
696 - 566 (d)

14.
698 - 571 (a) = 127 (b)
267 - 267 (c)
965 - 838
700 - 670 (e)
265 - 168 (d)

15.
272 - 170 (a) = 102 (b)
208 - 208 (c)
480 - 378 (d)

16.
495 - 399 (a) = 96 (b)
416 - 416 (c)
911 - 815
700 - 670 (e)
211 - 145 (d)

17.
225 - 202 (a) = 23 (a)
408 - 408 (c)
633 - 610 (d)

KEY TO EXPLANATORY MARKS:
(a) Indicators at beginning of message.
(b) Cycle as determined from their difference.
(c) Length of message.
(d) Positions of tapes at end of message.
(e) Subtraction for length of tapes.

REF ID:A516913

SOLUTION OF A.T.&T. MACHINE CIPHER

ADDENDUM I

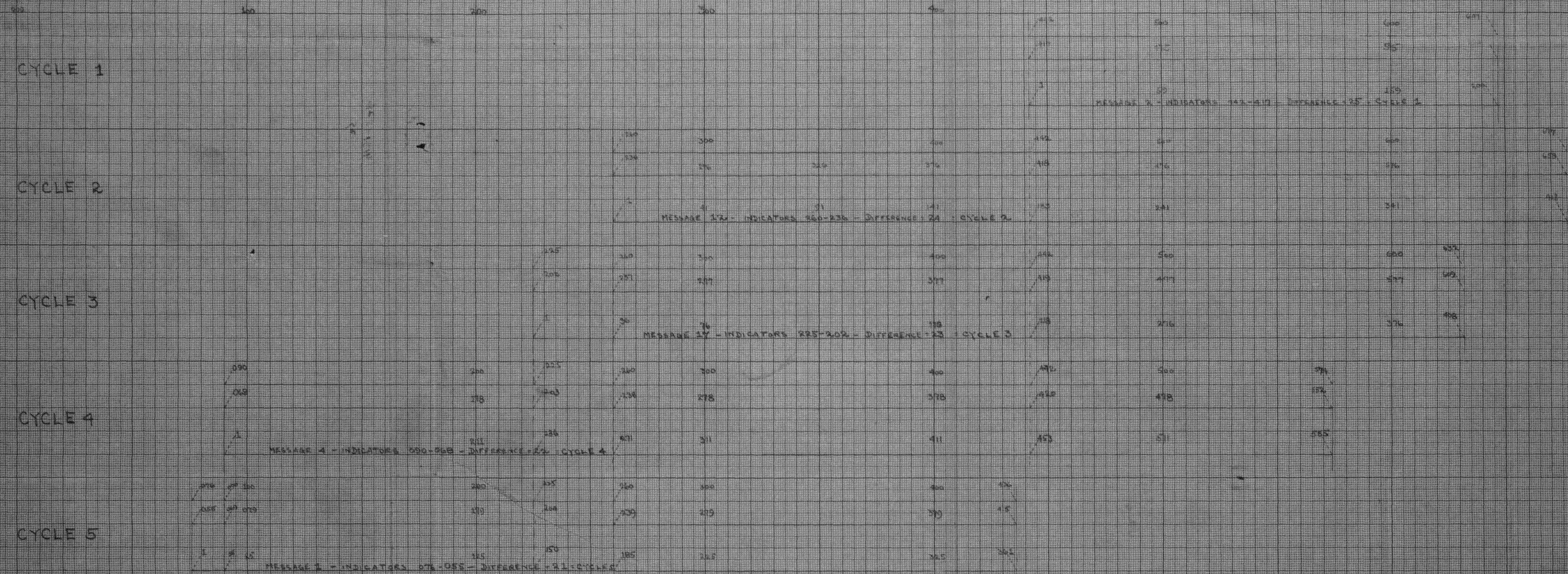


FIG. 19

SHOWING SUPERIMPOSITION OF SEQUENT CYCLES AS DETERMINED BY KEY INDICATORS

RIVERBANK LABORATORIES

ADDENDUM 2

SUMMARY

In this Addendum we shall show:

a. how the test messages submitted by the Signal Corps were deciphered.

b. that the present system, which employs key tapes differing in length by more than one letter, is much more unsafe than the former method in which key tapes differing in length by one and only one letter were used.

c. how the trials for possible plain text are reduced to simple terms, enabling a great number of trials to be made within a short time.

d. methods of solving cases not involving sequent cycles.

1. PRINCIPLES USED IN THE SOLUTION OF THE TEST MESSAGES

It may be said at the outset that the principles which were involved in the solution were basically those set forth in the original manuscript and its Addendum 1. The steps were as follows:

a. First, the plain text preamble for each message was read. This gave the key indicators, the serial number of the message, the number of words, the place of origin and date. For example, the first message sent by the station at Hoboken gave the following preamble:

EWWPPQA6Q53656QR52HQ3P30F3E3HOBOKEN3NJ3SEPT36WW36TRP55P442

"Translated," this would read as follows:

322 * 001 (Series)A (No.)1 14(words) HQ P(ort) of E(mbarkation) Hoboken NJ Sept 22 5:40 P(M)

Then the total number of characters in the message was determined by count, beginning with the character immediately following the 442 and extending to the beginning of the series of 2's or 4's at the end of the message.

By classifying the tapes in accordance with their points of origin, and then in accordance with their serial numbers, the following list resulted:

List of Messages

WASHINGTON SERIES

Message No.	Indicators	Length	Message No.	Indicators	Length
1	126 * 001	278	8	687 * 228	491
2	406 * 281	321	9	393 * 082	182
3	729 * 604	380	10	577 * 266	438
4	324 * 347	213	11	230 * 067	252
5	539 * 562	230	12	484 * 321	304
6	771 * 155	276	13	002 * 626	331
7	261 * 432	423	14	335 * 320	484

Message No.	Indicators	Length	Message No.	Indicators	Length
15	034 * 167	314	46	474 * 123	421
16	350 * 483	341	47	110 * 546	319
17	693 * 187	237	48	431 * 228	359
18	145 * 426	264	49	005 * 589	400
19	887 * 053	333	50	407 * 352	326
20	746 * 388	281	51	735 * 041	582
21	242 * 032	182	52	532 * 625	273
22	426 * 216	326	53	020 * 261	309
23	754 * 544	270	54	331 * 572	150
24	239 * 177	629	55	483 * 085	403
25	083 * 169	1959	56	101 * 490	403
26	470 * 213	228	57	506 * 256	378
27	700 * 443	304	58	099 * 636	783
28	219 * 110	437	59	097 * 143	492
29	658 * 549	308	60	591 * 004	221
30	181 * 220	481	61	027 * 221	381
31	664 * 064	214	62	408 * 602	237
32	093 * 280	410	63	647 * 202	327
33	505 * 053	254	64	189 * 531	295
34	698 * 309	236	65	486 * 189	300
35	212 * 547	244	66	001 * 491	195
36	458 * 154	275	67	198 * 049	424
37	735 * 431	362	68	624 * 475	411
38	312 * 156	323	69	250 * 259	318
39	637 * 481	491	70	570 * 579	262
40	350 * 335	142	71	047 * 204	161
41	487 * 479	318	72	210 * 367	208
42	020 * 160	275	73	420 * 577	202
43	297 * 437	374	74	624 * 142	149
44	673 * 984	206	75	775 * 293	133
45	094 * 382	378			

HOBOKEN SERIES

Message No.	Indicators	Length	Message No.	Indicators	Length
1	322 * 527	191	19	772 * 605	294
2	515 * 194	532	20	186 * 971	215
3	971 * 089	195	21	403 * 479	456
4	460 * 287	203	22	733 * 298	370
5	665 * 492	253	23	446 * 031	314
6	133 * 108	229	24	762 * 578	407
7	364 * 339	429	25	479 * 117	165
8	008 * 131	388	26	552 * 285	354
9	398 * 521	3370	27	121 * 002	366
10	770 * 254	213	28	489 * 370	751
11	198 * 469	177	29	455 * 484	1089
12	377 * 009	245	30	759 * 297	396
13	624 * 256	235	31	370 * 056	1200
14	733 * 493	358	32	785 * 619	562
15	434 * 214	275	33	942 * 544	523
16	711 * 491	345	34	300 * 430	512
17	271 * 199	178	35	027 * 305	495
18	451 * 379	224			

NEW YORK SERIES

Message No	Indicators	Length	Message No	Indicators	Length
1	714 * 001	157	13	576 * 002	236
2	086 * 160	307	14	714 * 240	272
3	395 * 469	235	15	201 * 514	302
4	891 * 067	761	16	505 * 179	235
5	618 * 191	205	17	742 * 416	231
6	038 * 398	365	18	188 * 010	276
7	405 * 126	329	19	418 * 288	284
8	736 * 457	577	20	752 * 574	134
9	528 * 397	316	21	101 * 071	128
10	059 * 076	585	22	231 * 201	133
11	646 * 024	359	23	366 * 336	143
12	220 * 385	253	24	511 * 481	91

NORFOLK SERIES

Message No.	Indicators	Length
1	518 * 001	514
2	247 * 517	320
3	569 * 200	271
4	055 * 473	274
5	331 * 110	279
6	612 * 391	388
7	215 * 142	163
8	380 * 307	139
9	521 * 448	446
10	182 * 257	677
11	074 * 297	407
12	483 * 067	227
13	712 * 296	273
14	200 * 571	279
15	481 * 213	195
16	678 * 410	990

b. Next, the lengths of the two keys were determined from a mathematical analysis of the foregoing lists. Consider, for example, the first few messages emanating from Washington, paying particular attention to the key indicators, and the length of each message. For example, Washington 1 begins at 126 * 001 and contains 278 letters[1]. It is evident that at the end of the message the keys would be at points, hereafter designated as "loci," 278 letters beyond the original loci. Thus:

Washington 1	....	126 *	001
Length	....	278	278
		404 *	279

The key indicators for Washington 2 are 406 * 281, two in advance, respectively, of the loci where Washington 1 left off. It is evident that before beginning on the next message Washington 2, which has 322 letters, the encipherer "slipped" both key tapes two letters. Adding the number of letters here again to the key indicators, we have the following:

Washington 1	....	126 *	001
Length	....	278	278
		404 *	279
Slip	....	(2	2)
Washington 2	....	406 *	281
Length	....	322	322
		728 *	603

Washington 3 begins at 729 * 604, in other words, after a "slip" of 1 letter in each key.

Now Washington 3 has 380 letters. Let us add 380 to the key indicators. Thus:

Washington 3	....	729 *	604
Length	....	380	380
		1109 *	984

The result should correspond approximately with the key indicators for the next message, but Washington 4 gives as indicators 324 * 347. It is evident, therefore, that both key tapes have completed one revolution and are 323 and 346 letters, respectively, beyond their initial loci, viz, 001. If now we find the difference between the theoretical pair of indicators, 1109 * 984, and the actual pair, 324 * 347, we shall begin to approximate the lengths of the keys. Thus:

Washington 4	(theoretical initial loci)	1109 *	984
	(actual " ")	324 *	347
		785 *	637

We begin to suspect that the longer key is about 785 letters in length, the shorter, about 637. We must, therefore, determine not their approximate lengths, but their exact lengths. If there were no slip between Washington 3 and Washington 4, then the numbers 785 and 637 would coincide with the exact lengths of the keys. We do not know whether there has been a slip between these two messages, or, if there has been, whether the slip was the same for both keys. But we do not have to determine that

[1]We shall use the word "letters" to include all the characters and "functions" of the machine, as they appear on the cipher tapes.

immediately. Let us turn our attention to a case in which only one of the key tapes completes a revolution within a message. For example, consider Washington 5, with key indicators 539 * 562, length 230 letters; and Washington 6, with key indicators 771 * 155, length 276 letters. Let us calculate as before.

Washington 5	539	* 562
Length	230	230
	769	* 792

If there has been a slip of two letters on both key tapes, then Washington 6 should begin at 771 * 794. But in reality, the key indicators for this message are 771 * 155. Still assuming an equal slip of two letters, then locus 792 + 2 = 794, which coincides with locus 155. Taking the difference, 794-155 = 639, which would be the exact length of the short key. Above, we had determined the approximate length as 637.

Applying the same process to determine the exact length of the long key, taking Washington 6 and 7 for calculation, we find the following:

Washington 6	771	* 155
Length	276	276
	1047	* 431

Washington 7 begins at 261 * 432. Since the indicators as regards the short key differ only by 1, we assume an equal slip of 1 for both keys. Therefore locus 1047 + 1 = 1048, which coincides with locus 261. Then, likewise, 1048-261 = 787, the exact length of the long key. Our approximate length was 785, as determined above.

It now remains to test these determinations on all messages, their correctness being based upon the consistency with which the theoretical key indicators for each message agree with the actual, taking into account the assumption that the two key tapes were slipped an equal distance in every case. There may be a variation in the amount of slip between successive messages, but so long as in each case both tapes are slipped through the same distance, the result would be exactly the same as though each message were 1, 2, 3 ... letters longer than is actually the case, with no slip whatever involved. A careful study of the calculations which follow will show that there could not possibly be any doubt about the correctness of the two determinations, 787 and 639. There are several discrepancies, it is true, but they were due to errors, or carelessness on the part of the encipherer, as will be discussed later.

Before giving the complete calculations for the series of messages, we shall introduce into the discussion a feature which concerns what we have termed latent cycles. (For definition of the ordinary cycle see page 2 of Addendum 1.)

Consider Washington 3, for example; it begins at 729 * 604, or in the 125th cycle and ends at 322 * 345, or in the minus 23rd cycle. The message involves, therefore, at least two cycles. But there is in reality an additional cycle involved. For, after the message has proceeded for 36 letters, the short key is at locus 640, which coincides with locus 001, since the key is 639 letters in length. But while the short key is at locus 001, the long key is at locus 729 36, or 765. After the 36th letter, therefore, the message proceeds in cycle 765-001, or cycle 764. This we term the hidden or <u>latent cycle</u>, in contradistinction with the open or patent cycles (which are shown by the key indicators themselves), because the existence of the latent cycle is disclosed only by the calculations made as a result of the determination of the exact lengths of the two key tapes. These relations can be demonstrated very simply, thus:

Washington 3	.... 729 * 604	Cycle 125
(length 380 letters)	.... 36 36	
	765 * 640	
	or	
	765 * 001	Cycle 764

But this message is 380 letters in length and continues to be enciphered after the 36th letter. Proceeding for 23 letters more, the long key reaches the locus 788, which is in reality locus 001, since the long key is 787 letters in length. The short key, after 23 letters, is at locus 024. The difference between the two loci 001 and 024 is therefore -23, and the message is now proceeding in the latent -23rd cycle. It continues to do so until the end of the message. These relations are summarized mathematically in a standard form as follows:

Message No.	Indicators	Length Partial	Length Total	Cycle
Washington 3	729 * 604			125
	36 36	36		
	765 * 640			
	765 * 001			764
	23 23	23.		
	788 * 024			
	001 * 024			-23
	321 321	321	380	
End of Wash. 3 ..	322 * 345			

The calculations which apply to the entire series of messages are as follows:

WASHINGTON SERIES

Message No.	Indicators	Length Partial	Length Total	Cycle
1	126 * 001			125
	278 278	278	278	
	404 * 279			
	(2 2)			
2	406 * 281			
	322 322	322	322	
	728 * 603			
	(1 1)			
3	729 * 604			
	36 36	36		
	765 * 604			

Message No.	Indicators	Length Partial	Length Total	Cycle
3 cont'd.	765 * 640			
	765 * 001			764
	23 23	23		
	788 * 024			
	001 * 024			-23
	321 321	321	380	
	322 * 345			
	(2 2)			
4	324 * 347			
	213 213	213	213	
	537 * 560			
	(2 2)			
5	539 * 562			
	78 78	78		
	617 * 640			
	617 * 001			616
	152 152	152	230	
	769 * 153			
	(2 2)			
6	771 * 155			
	17 17	17		
	788 * 172			
	001 * 172			-171
	259 259	259	276	
	260 * 431			
	(1 1)			
7	261 * 432			
	208 208	208		
	469 * 640			
	469 * 001			468
	215 215	215	423	
	684 * 216			
	(3 12)			
8	687 * 228			
	101 101	101		
	788 * 329			
	001 * 329			-328
	311 311	311		
	312 * 640			
	312 * 001			311
	79 79	79	491	
	391 * 080			
	(2 2)			
9	393 * 082			
	182 182	182	182	
	575 * 264			
	(2 2)			
10	577 * 266			
	211 211	211		
	788 * 477			
	001 * 477			-476
	163 163	163		
	164 * 640			
	164 * 001			163
	64 64	64	438	
	228 * 065			
	(2 2)			
11	230 * 067			

Message No.	Indicators	Length Partial	Length Total	Cycle
11	230 * 067			
	252 252	252	252	
	488 * 319			
	(2 2)			
12	484 * 321			
	304 304	304	304	
	788 * 625			
	001 * 625			-624
	(1 1)			
13	002 * 626			
	14 14	14		
	016 * 640			
	016 * 001			15
	317 317	317	331	
	333 * 318			
	(2 2)			
14	335 * 320			
	320 320	320		
	655 * 640			
	655 * 001			654
	133 133	133		
	788 * 134			
	001 * 134			-133
	31 31	31	484	
	032 * 165			
	(2 2)			
15	034 * 167			
	316 316	316	316	
	350 * 483			
	(0 0)			
16	350 * 483			
	157 157	157		
	507 * 640			
	507 * 001			506
	184 184	184	341	
	691 * 185			
	(2 2)			
17	693 * 187			
	95 95	95		
	788 * 282			
	001 * 282			-281
	143 143	143	238	
	144 * 425			
	(1 1)			
18	145 * 426			
	214 214	214		
	359 * 640			
	359 * 001			358
	50 50	50	264	
	409 * 051			
	(2 2)			
19	411 * 053			
	333 333	333	333	
	744 * 386			
	(2 2)			
20	746 * 388			

Message No.	Indicators	Length		Cycle
		Partial	Total	
20	746 * 388			
	42 42	42		
	788 * 430			
	001 * 430			-429
	210 210	210		
	211 * 640			
	211 * 001			210
	29 29	29	281	
	240 * 030			
	(2 2)			
21	242 * 032			
	182 182	182	182	
	424 * 214			
	(2 2)			
22	426 * 216			
	326 326	326	326	
	752 * 542			
	(2 2)			
23	754 * 544			
	34 34	34		
	788 * 578			
	001 * 578			-577
	62 62	62		
	063 * 640			
	063 * 001			62
	174 174	174	270	
	237 * 175			
	(2 2)			
24	239 * 177			
	463 463	463		
	702 * 640			
	702 * 001			701
	86 86	86		
	788 * 087			
	001 * 087			-86
	80 80	80	629	
	081 * 167			
	(2 2)			
25	083 * 169			
	471 471	471		
	554 * 640			
	554 * 001			553
	234 234	234		
	788 * 235			
	001 * 235			-234
	405 405	405		
	406 * 640			
	406 * 001			405
	382 382	382		
	788 * 383			
	001 * 383			-382
	257 257	257		
	258 * 640			
	258 * 001			257
	211 211	211	1960	
	469 * 212			
	(1 1)			
26	470 * 213			

Message No.	Indicators	Length Partial	Length Total	Cycle
26	470 * 213			
	228 228	228	228	
	698 * 441			
	(2 2)			
27	700 * 443			
	88 88	88		
	788 * 531			
	001 * 531			-530
	109 109	109		
	110 * 640			
	110 * 001			109
	108 108	108	305	
	218 * 109			
	(1 1)			
28	219 * 110			
	437 437	437	437	
	656 * 547			
	(2 2)			
29	658 * 549			
	91 91	91		
	749 * 640			
	749 * 001			748
	39 39	39		
	788 * 040			
	001 * 040			-39
	175 175	175	305	
	176 * 215			
	(5 5)			
30	181 * 220			
	420 420	420		
	601 * 640			
	601 * 001			
	56 56	56	476	
	657 * 057			
	(7 7)			
31	664 * 064			
	124 124	124		
	788 * 188			
	001 * 188			-187
	87 87	87	211	
	088 * 275			
	(5 5)			
32	093 * 280			
	360 360	360		
	453 * 640			
	453 * 001			452
	46 46	46	406	
	499 * 047			
	(6 6)			
33	505 * 053			
	251 251	251	251	
	756 * 304			
	(5 5)			
34	761 * 309			
	27 27	27		
	788 * 336			
	001 * 336			-335
	206 206	206	233	
	207 * 542			
	(5 5)			
35	212 * 547			

Message No.	Indicators	Length Partial	Length Total	Cycle
35	212 * 547			
	93 93	93		
	305 * 640			
	305 * 001			304
	148 148	148	241	
	453 * 149			
	(5 5)			
36	458 * 154			
	272 272	272	272	
	730 * 426			
	(5 5)			
37	735 * 431			
	53 53	53		
	788 * 484			
	001 * 484			-483
	156 156	156		
	157 * 640			
	157 * 001			156
	149 149	149	358	
	306 * 150			
	(6 6)			
38	312 * 156			
	323 323	323	323	
	635 * 479			
	(2 2)			
39	637 * 481			
	151 151	151		
	788 * 632			
	001 * 632			-631
	8 8	8		
	009 * 640			
	009 * 001			8
	327 327	327	486	
	336 * 328			
	(7 7)			
40	343 * 335			
	140 140	140	140	
	483 * 475			
	(4 4)			
41	487 * 479			
	161 161	161		
	648 * 640			
	648 * 001			647
	140 140	140		
	788 * 141			
	001 * 141			-140
	13 13	13	314	
	014 * 154			
	(6 6)			
42	020 * 160			
	272 272	272	272	
	292 * 432			
	(5 5)			
43	297 * 437			
	203 203	203		
	500 * 640			
	500 * 001			499
	167 167	167	370	
	667 * 168			
	(6 6)			
44	673 * 174			

Message No.	Indicators	Length Partial	Length Total	Cycle
44	673 * 174			
	115 115	115		
	788 * 289			
	001 * 289			-288
	89 89	89	204	
	090 * 378			
	(4 4)			
45	094 * 382			
	258 258	258		
	352 * 640			
	352 * 001			351
	116 116	116	374	
	468 * 117			
	(6 6)			
46	474 * 123			
	314 314	314		
	788 * 437			
	001 * 437			-436
	102 102	102	416	
	103 * 539			
	(7 7)			
47	110 * 546			
	94 94	94		
	204 * 640			
	204 * 001			203
	221 221	221	315	
	425 * 222			
	(6 6)			
48	431 * 228			
	355 355	355	355	
	786 * 583			
	(6 6)			
49	792 * 589			
	005 * 589			-584
	51 51	51		
	056 * 640			
	056 * 001			55
	345 345	345	396	
	401 * 346			
	(6 6)			
50	407 * 352			
	288 288	288		
	695 * 640			
	695 * 001			694
	34 34	34	322	
	729 * 035			
	(6 6)			
51	735 * 041			
	53 53	53		
	788 * 094			
	001 * 094			-93
	523 523	523	576	
	524 * 617			
	(8 8)			
52	532 * 625			
	15 15	15		
	547 * 640			
	547 * 001			546
	241 241	241		
	788 * 242			

Message No.	Indicators	Length Partial	Length Total	Cycle
52 cont'd.	788 * 242			
	001 * 242			-241
	13 13	13	269	
	014 * 255			
	(6 6)			
53	020 * 261			
	306 306	306	306	
	326 * 567			
	(5 5)			
54	331 * 572			
	68 68	68		
	399 * 640			
	399 * 001			398
	80 80	80	148	
	479 * 081			
	(4 4)			
55	483 * 085			
	305 305	305		
	788 * 390			
	001 * 390			-389
	94 94	94	399	
	095 * 484			
	(6 6)			
56	101 * 490			
	150 150	150		
	251 * 640			
	251 * 001			250
	249 249	249	399	
	500 * 250			
	(6 6)			
57	506 * 256			
	282 282	282		
	788 * 538			
	001 * 538			-537
	92 92	92	374	
	093 * 630			
	(6 6)			
58	099 * 636			
	4 4	4		
	103 * 640			
	103 * 001			102
	639 639	639		
	742 * 640			
	742 * 001			741
	46 46	46		
	788 * 047			
	001 * 047			-46
	86 86	86	775	
	087 * 133			
	(10 10)			
59	097 * 143			
	487 487	487	487	
	584 * 630			
	(7 7)			
60	591 * 637			

Message No.	Indicators	Length Partial	Length Total	Cycle
60	591 * 637			
	3 3	3		
	594 * 640			
	594 * 001			593
	194 194	194		
	788 * 195			
	001 * 195			-194
	21 21	21	218	
	022 * 216			
	(5 5)			
61	027 * 221			
	377 377	377	377	
	404 * 598			
	(4 4)			
62	408 * 602			
	38 38	38		
	446 * 640			
	446 * 001			445
	197 197	197	235	
	643 * 198			
	(4 4)			
63	647 * 202			
	141 141	141		
	788 * 343			
	001 * 343			-342
	182 182	182	323	
	183 * 525			
	(6 6)			
64	189 * 531			
	109 109	109		
	298 * 640			
	298 * 001			297
	183 183	183	292	
	481 * 184			
	(5 5)			
65	486 * 189			
	297 297	297	297	
	783 * 486			
	(5 5)			
66	788 * 491			
	001 * 491			-490
	149 149	149		
	150 * 640			
	150 * 001			149
	44 44	44	193	
	194 * 045			
	(4 4)			
67	198 * 049			
	420 420	420	420	
	618 * 469			
	(5 5)			
68	624 * 475			
	164 164	164		
	788 * 639			
	001 * 639			-638
	1 1	1		
	002 * 640			

Message No.	Indicators	Length Partial	Length Total	Cycle
68 cont'd.	002 * 640			
	002 * 001			1
	242 242	242	407	
	244 * 243			
	(6 16)			
69	250 * 259			
	315 315	315	315	
	565 * 574			
	(5 5)			
70	570 * 579			
	61 61	61		
	631 * 640			
	631 * 001			630
	157 157	157		
	788 * 158			
	001 * 158			-157
	42 42	42	259	
	043 * 200			
	(4 4)			
71	047 * 204			
	159 159	159	159	
	206 * 363			
	(4 4)			
72	210 * 367			
	206 206	206	206	
	416 * 573			
	(4 4)			
73	420 * 577			
	63 63	63		
	483 * 640			
	483 * 001			482
	137 137	137	200	
	620 * 138			
	(4 4)			
74	624 * 142			
	147 147	147	147	
	771 * 289			
	(4 4)			
75	775 * 293			
	13 13	13		
	788 * 316			
	001 * 316			-315
	120 120	120	133	
	121 * 436			

HOBOKEN SERIES

Message No.	Indicators	Length Partial	Length Total	Cycle
1	322 * 001			321
	191 191	191	191	
	513 * 192			
	(2 2)			
2	515 * 194			
	273 273	273		
	788 * 467			
	001 * 467			-466
	173 173	173		
	174 * 640			
	174 * 001			173
	86 86	86	532	
	260 * 087			
	(2 2)			
3	262 * 089			
	197 197	197	197	
	459 * 286			
	(1 1)			
4	460 * 287			
	203 203	203	203	
	663 * 490			
	(2 2)			
5	665 * 492			
	123 123	123		
	788 * 615			
	001 * 615			-614
	25 25	25		
	026 * 640			
	026 * 001			25
	105 105	105	253	
	131 * 106			
	(2 2)			
6	133 * 108			
	229 229	229	229	
	362 * 337			
	(2 2)			
7	364 * 339			
	301 301	301		
	665 * 640			
	665 * 001			664
	123 123	123		
	788 * 124			
	001 * 124			-123
	5 5	5	429	
	006 * 129			
	(2 2)			
8	008 * 131			
	388 388	388	388	
	396 * 519			
	(2 2)			
9	398 * 521			
	119 119	119		
	517 * 640			
	517 * 001			516
	251 251	251	370	
	768 * 252			
	(2 2)			
10	770 * 254			

Message No.	Indicators	Length Partial	Length Total	Cycle
10	770 * 254			
	18 18	18		
	788 * 272			
	001 * 272			-271
	195 195	195	213	
	196 * 467			
	(2 2)			
11	198 * 469			
	177 177	177	177	
	375 * 646			
	375 * 007			368
	(2 2)			
12	377 * 009			
	245 245	245	245	
	622 * 254			
	(2 2)			
13	624 * 256			
	164 164	164		
	788 * 420			
	001 * 420			-419
	71 71	71	235	
	072 * 491			
	(2 2)			
14	074 * 493			
	147 147	147		
	221 * 640			
	221 * 001			220
	211 211	211	358	
	432 * 212			
	(2 2)			
15	434 * 214			
	275 275	275	275	
	709 * 489			
	(2 2)			
16	711 * 491			
	77 77	77		
	788 * 568			
	001 * 568			-567
	72 72	72		
	073 * 640			
	073 * 001			72
	196 196	196	345	
	269 * 197			
	(2 2)			
17	271 * 199			
	178 178	178	178	
	449 * 377			
	(2 2)			
18	451 * 379			
	224 224	224	224	
	675 * 603			
	(2 2)			
19	677 * 605			
	35 35	35		
	712 * 640			
	[712 * 001]			
	76 76	76		
	788 * 077			
	001 * 077			-76
	183 183	183	294	
	184 * 260			

Message No.	Indicators	Length Partial	Length Total	Cycle
19 cont'd.	184 * 260			
	(2 2)			
20	186 * 262			
	215 215	215	215	
	401 * 477			
	(2 2)			
21	403 * 479			
	161 161	161		
	564 * 640			
	564 * 001			563
	224 224	224		
	788 * 225			
	001 * 225			-224
	71 71	71	456	
	072 * 296			
	(2 2)			
22	074 * 298			
	342 342	342		
	416 * 640			
	416 * 001			415
	28 28	28	370	
	444 * 029			
	(2 2)			
23	446 * 031			
	314 314	314	314	
	760 * 345			
	(2 2)			
24	762 * 347			
	26 26	26		
	788 * 373			
	001 * 373			-372
	267 267	267		
	268 * 640			
	268 * 001			267
	114 114	114	407	
	382 * 115			
	(2 2)			
25	384 * 117			
	165 165	165	165	
	549 * 282			
	(3 3)			
26	552 * 285			
	236 236	236		
	788 * 521			
	001 * 521			-520
	118 118	118	354	
	119 * 639			
	(2 2)			
27	121 * 641			
	121 * 002			119
	366 366	366	366	
	487 * 368			
	(2 2)			
28	489 * 370			
	270 270	270		
	759 * 640			
	759 * 001			758
	29 29	29		
	788 * 030			

Message No.	Indicators	Length Partial	Length Total	Cycle
28 cont'd.	788 * 030			
	001 * 030			-29
	452 452	452	751	
	453 * 482			
	(2 2)			
29	455 * 484			
	156 156	156		
	611 * 640			
	611 * 001			610
	177 177	177		
	788 * 178			
	001 * 178			-177
	462 462	462		
	463 * 640			
	463 * 001			462
	294 294	294	1089	
	757 * 295			
	(2 2)			
30	759 * 297			
	29 29	29		
	788 * 326			
	001 * 326			-325
	314 314	314		
	315 * 640			
	315 * 001			314
	53 53	53	396	
	368 * 054			
	(2 2)			
31	370 * 056			
	418 418	418		
	788 * 474			
	001 * 474			-473
	166 166	166		
	167 * 640			
	167 * 001			
	604 604	604	1188	
	771 * 605			
	(14 14)			
32	785 * 619			
	3 3	3		
	788 * 622			
	001 * 622			
	18 18	18		
	019 * 640			
	019 * 001			18
	535 535	535	556	
	554 * 536			
	(8 8)			
33	562 * 544			
	96 96	96		
	658 * 640			
	658 * 001			657
	130 130	130		
	788 * 131			
	001 * 131			-130
	292 292	292	578	
	293 * 423			
	(7 7)			
34	300 * 430			

Message No.	Indicators	Length Partial	Length Total	Cycle
34	300 * 430			
	210 210	210		
	510 * 640			
	510 * 001			509
	278 278	278		
	788 * 279			
	001 * 279			-278
	19 19	19	507	
	020 * 298			
	(7 7)			
35	027 * 305			
	335 335	335		
	362 * 640			
	362 * 001			361
	160 160	160	495	

NEW YORK SERIES

Message No.	Indicators	Length Partial	Length Total	Cycle
1	[714 * 001]			713
	74 74	74		
	788 * 075			
	001 * 075			-74
	83 83	83	157	
	084 * 158			
	(2 2)			
2	086 * 160			
	307 307	307	307	
	393 * 467			
	(2 2)			
3	395 * 469			
	171 171	171		
	566 * 640			
	566 * 001			565
	64 64	64	235	
	630 * 065			
	(2 2)			
4	632 * 067			
	156 156	156		
	788 * 223			
	001 * 223			-222
	417 417	417		
	418 * 640			
	418 * 001			417
	188 188	188	761	
	606 * 189			

Message No.	Indicators	Length Partial	Length Total	Cycle
4	606 * 189			
cont'd.	(12 12)			
5	618 * 191			
	170 170	170		
	[788 * 361]			
	001 * 361			-360
	35 35	35	205	
	036 * 396			
	(2 2)			
6	038 * 398			
	242 242	242		
	280 * 640			
	280 * 001			279
	123 123	123	365	
	403 * 124			
	(2 2)			
7	405 * 126			
	329 329	329	329	
	734 * 455			
	(2 2)			
8	736 * 457			
	52 52	52		
	788 * 509			
	001 * 509			-508
	131 131	131		
	132 * 640			
	132 * 001			131
	394 394	394	577	
	426 * 395			
	(2 2)			
9	428 * 397			
	243 243	243		
	671 * 640			
	671 * 001			670
	17 17	17		
	688 * 018			
	001 * 018			-17
	56 56	56	316	
	057 * 074			
	(2 2)			
10	059 * 076			
	564 564	564		
	623 * 640			
	623 * 001			622
	21 21	21	585	
	644 * 022			
	(2 2)			
11	646 * 024			
	142 142	142		
	788 * 166			
	001 * 166			-165
	217 217	217	359	
	218 * 383			
	(2 2)			
12	220 * 385			

Message No.	Indicators	Length Partial	Length Total	Cycle
12	220 * 385			
	253 253	253	253	
	473 * 638			
	(3 3)			
13	476 * 641			
	476 * 002			474
	236 236	236	236	
	712 * 238			
	(2 2)			
14	714 * 240			
	74 74	74		
	788 * 314			
	001 * 314			-313
	198 198	198	272	
	199 * 512			
	(2 2)			
15	201 * 514			
	126 126	126		
	327 * 640			
	327 * 001			326
	176 176	176	302	
	503 * 177			
	(2 2)			
16	505 * 179			
	235 235	235	235	
	740 * 414			
	(2 2)			
17	742 * 416			
	46 46	46		
	788 * 462			
	001 * 462			-461
	178 178	178		
	179 * 640			
	179 * 001			178
	7 7	7	231	
	186 * 008			
	(2 2)			
18	188 * 010			
	276 276	276	276	
	464 * 286			
	(2 2)			
19	466 * 288			
	284 284	284	284	
	750 * 572			
	(2 2)			
20	752 * 574			
	36 36	36		
	788 * 610			
	001 * 610			-609
	30 30	30		
	031 * 640			
	031 * 001			30
	68 68	68	134	
	099 * 069			
	(2 2)			
21	101 * 071			

Message No.	Indicators	Length Partial	Length Total	Cycle
21	101 * 071			
	128 128	128	128	
	229 * 199			
	(2 2)			
22	231 * 201			
	133 133	133	133	
	364 * 334			

NORFOLK SERIES

Message No.	Indicators	Length Partial	Length Total	Cycle
1	518 * 001			517
	270 270	270		
	788 * 271			
	001 * 271			-270
	244 244	244	514	
	245 * 515			
	(2 2)			
2	247 * 517			
	123 123	123		
	370 * 640			
	370 * 001		369	369
	197 197	197	320	
	567 * 198			
	(2 2)			
3	569 * 200			
	219 219	219		
	788 * 419			
	001 * 419			-418
	52 52	52	271	
	053 * 471			
	(2 2)			
4	055 * 473			
	167 167	167		
	222 * 640			
	222 * 001			221
	107 107	107	274	
	329 * 108			
	(2 2)			
5	331 * 110			
	279 279	279	279	
	610 * 389			
	(2 2)			
6	612 * 391			
	176 176	176		
	788 * 567			
	001 * 567			-566
	73 73	73		
	074 * 640			

Message No.	Indicators	Length Partial	Length Total	Cycle
6 cont'd.	074 * 640			
	074 * 001			73
	139 139	139	388	
	213 * 140			
	(2 2)			
7	215 * 142			
	163 163	163	163	
	378 * 305			
	(2 2)			
8	380 * 307			
	139 139	139	139	
	519 * 446			
	(2 2)			
9	521 * 448			
	192 192	192		
	713 * 640			
	713 * 001			712
	75 75	75		
	788 * 076			
	001 * 076			-75
	179 179	179	446	
	180 * 255			
	(2 2)			
10	182 * 257			
	383 383	383		
	565 * 640			
	565 * 001			564
	223 223	223		
	788 * 224			
	001 * 224			
	71 71	71	677	
	072 * 295			
	(2 2)			
11	074 * 297			
	343 343	343		
	417 * 640			
	417 * 001			416
	64 64	64	407	
	481 * 065			
	(2 2)			
12	483 * 067			
	227 227	227	227	
	710 * 294			
	(2 2)			
13	712 * 296			
	76 76			
	[788 * 372]			
	001 * 372			-371
	197 197	197	273	
	198 * 569			
	(2 2)			
14	200 * 571			
	69 69	69		
	269 * 640			
	269 * 001			268
	210 210	210	279	
	479 * 211			
	(2 2)			
15	481 * 213			

Message No.	Indicators	Length Partial	Length Total	Cycle
15	481 * 213			
	195 195	195	195	
	676 * 408			
	(2 2)			
16	678 * 410			
	110 110	110		
	788 * 520			
	001 * 520			-519
	120 120	120		
	121 * 640			
	121 * 001			120
	639 639	639		
	760 * 640			
	760 * 001			759
	28 28	28		
	788 * 029			
	001 * 029			-28
	93 93	93	990	
	094 * 122			

Remarks on Calculations

It is to be noted that these calculations exhibit a remarkable consistency, and corroborate the calculated lengths of the two keys, 787 and 639, respectively. By the consistency of the calculations we mean that it would be utterly impossible to have the calculated slip between messages equal for both keys in every case as a result of coincidence; for, unless the assumed lengths of the two keys be correct, the slip would be unequal and inconsistent in many places. The fact that they are equal means that the encipherer was consistent in slipping both tapes an equal distance every time. The idea behind an equal slip is not clear, for it entirely defeats its own purpose, which is to prevent the enemy from determining the lengths of the keys. Had the encipherer slipped them unequal distances in every case, being careful, of course, to slip the short tape further than the long, no such consistency would have been possible to uncover. But, in this case, the possibility of overlapping messages, would be greatly increased, as will be shown subsequently.

As mentioned above, there are several discrepancies, due to errors on the part of the encipherer. That they are errors, and not intentional operations intended to deceive the enemy is shown by their nature. For example, the slip between Washington 68 and 69 is 2 * 12. Evidently the encipherer meant to have Washington 69 begin at loci intervals away from where Washington 68 ended, and probably misread the number 249 on the short tape, making it 259. This becomes the same as though he had slipped the long tape 2 letters and the short one 12. In the New York messages another error of 10 is involved between messages 4 and 5. Had this error not occurred there would have been afforded about twice as many possible points of attack as were actually the case, as will be shown later.

Excellent corroboration for the determined lengths of keys is afforded by finding the total numbers of letters in all messages emanating from each station, adding the total amount of slip and then calculating as if only one message were concerned. The final result should coincide with the result obtained from calculations for the individual messages. Thus:

(1) Washington Series

Initial loci	126	*	001
Total number of letters enciphered ...	25834		25834
Total slip	132		132
Sum	26092		25986
Minus 33 revs. of long key and 40 " " short "	-25971		-25560
Final loci	121	*	426

(2) Hoboken Series

Initial loci	322	*	001
Total number of letters enciphered ...	13503		13503
Total slip	76		76
Sum	13901		13580
Minus 17 revs. of long key and 21 " " short "	-13379		-13419
Final loci	522	*	161

(3) New York Series

Initial loci	714	*	001
Total number of letters enciphered ...	6914		6914
Total slip	57		57
Sum	7685		6962
Minus 9 revs. of long key and 10 " " short "	-7083		-6390
Final loci	602	*	572

(4) Norfolk Series

Initial loci	518	*	001
Total number of letters enciphered ...	5841		5841
Total slip	31		31
Sum	6490		5873
Minus 8 revs. of long key and 9 " " short "	-6296		-5751
Final loci	094	*	122

In each case it will be noted that the final loci coincide with those given by the individual calculations, in perfect accord with the requirements based upon keys 787 and 639 letters in length.

The purpose of all these calculations was to find such cycles as would form the basis of an attack. A table was made, therefore, showing all the cycles, both plus and minus, involved in the series of messages (see Table 1).

The most favorable relation of cycles for an attack being three sequent cycles (for definition see page 2 of Addendum 1), an examination of this table was made with a view to finding three sequent cycles. These were found, showing first in Table 1 in cycles 415, 416, and 417, messages Hoboken 22, Norfolk 11, and New York 4, respectively.

By referring to the calculations on pages 6-25, it will be seen that the three sequent cycles begin in reality with Hoboken 19, latent cycle 711; Norfolk 9, latent cycle 712; and New York 1, latent cycle 713. They end with Hoboken 24, latent cycle 415; Norfolk 13, latent cycle 416; and New York 4, latent cycle 417. The extent of the three sequent cycles is indicated in the calculations for these messages by the brackets.

Had no errors been made in encipherment, these three sets of messages would have proceeded along in three sequent cycles to the following points: Hoboken 29, latent cycle -29; Norfolk 16, to its completion in latent cycle -28; New York 10, latent cycle (theoretical or what it should have been) -27. The error referred to on page 25 made between New York 4 and 5 therefore cuts the number of possible points of attack in half.

c. The messages involved were immediately transcribed in the usual manner in the form of three sequent cycles. There were two excellent points of attack in these messages when arranged in this form. They were excellent because two messages began in one case at exactly the same point; in the other case, very near the same point. One of these cases is shown below. (The initial points of all messages shown hereinafter will be designated by a vertical double bar surmounted by an asterisk.)

```
Upper key loci         182 186
Lower key loci         256 260
NEW YORK 2      ...     6XTSQWQZKWCMCPWIDY3GD3A6JM ...    Cycle -74

                      *
Upper key loci        ||182 186
Lower key loci        ||257 261
NORFOLK 10      ...   || SXH7GMERHP3QSNI3MCZVCTRVOU ...    Cycle -75

                          *
Upper key loci            ||186
Lower key loci            ||262
HOBOKEN 20      ...       || 3CTFJIXXLK3F4PKQ5LDYEQ ...    Cycle -76
```

TABLE 1

Distribution of Cycles

Plus (0-100)		Minus (0-100)	
1	(Washington 68)	-17	(New York 9)
8	(Washington 39)	-23	(Washington 3)
15	(Washington 13)	-28	(Norfolk 16)
18	(Hoboken 32)	-29	(Hoboken 28)
25	(Hoboken 5)	-39	(Washington 29)
30	(New York 20)	-46	(Washington 58)
55	(Washington 49)	-74	(New York 1)
62	(Washington 23)	-75	(Norfolk 9)
72	(Hoboken 16)	-76	(Hoboken 19)
73	(Norfolk 6)	-86	(Washington 24)
		-93	(Washington 51)

Plus (101-200)		Minus (101-200)	
102	(Washington 58)	-123	(Hoboken 7)
109	(Washington 27)	-130	(Hoboken 33)
119	(Hoboken 27)	-133	(Washington 14)
120	(Norfolk 16)	-140	(Washington 41)
131	(New York 8)	-157	(Washington 70)
149	(Washington 66)	-165	(New York 11)
156	(Washington 37)	-171	(Washington 6)
163	(Washington 10)	-177	(Hoboken 29)
173	(Hoboken 2)	-178	(New York 17)
		-187	(Washington 31)
		-194	(Washington 60)

Plus (201-300)		Minus (201-300)	
203	(Washington 47)	-222	(New York 4)
210	(Washington 20)	-224	(Hoboken 21)
220	(Washington 14)	-234	(Washington 25)
221	(Norfolk 4)	-241	(Washington 52)
250	(Washington 56)	-270	(Norfolk 1)
257	(Washington 25)	-271	(Hoboken 10)
267	(Hoboken 24)	-278	(Hoboken 34)
268	(Norfolk 14)	-281	(Washington 17)
279	(New York 6)	-288	(Washington 44)
297	(Washington 64)		

Plus
(301-400)

304 (Washington 35)
311 (Washington 8)
314 (Hoboken 30)
321 (Hoboken 1)
326 (New York 15)
351 (Washington 45)
358 (Washington 18)
361 (Hoboken 35)
368 (Hoboken 11)
369 (Norfolk 2)
398 (Washington 54)

Minus
(301-400)

-313 (New York 14)
-315 (Washington 75)
-325 (Hoboken 30)
-328 (Washington 8)
-335 (Washington 34)
-342 (Washington 63)
-360 (New York 5)
-371 (Norfolk 13)
-372 (Hoboken 24)
-382 (Washington 25)
-389 (Washington 55)

Plus
(401-500)

405 (Washington 25)
415 (Hoboken 22)
416 (Norfolk 11)
417 (New York 4)
445 (Washington 62)
452 (Washington 32)
462 (Washington 29)
468 (Washington 7)
482 (Washington 73)
499 (Washington 43)

Minus
(401-500)

-418 (Norfolk 3)
-419 (Hoboken 13)
-429 (Washington 20)
-436 (Washington 46)
-461 (New York 17)
-466 (Hoboken 2)
-473 (Hoboken 31)
-474 (New York 13)
-476 (Washington 10)
-483 (Washington 37
-490 (Washington 66)

Plus
(501-600)

506 (Washington 16)
509 (Hoboken 34)
516 (Hoboken 9)
517 (Norfolk 1)
546 (Washington 52)
553 (Washington 25)
563 (Hoboken 21)
564 (Norfolk 10)
593 (Washington 60)

Minus
(501-600)

-508 (New York 8)
-519 (Norfolk 16)
-520 (Hoboken 26)
-530 (Washington 27)
-537 (Washington 57)
-565 (New York 3)
-566 (Norfolk 6)
-567 (Hoboken 16)
-577 (Washington 23)
-584 (Washington 49)

Plus
(601-700)

610 (Hoboken 29)
616 (Washington 5)
622 (New York 10)
630 (Washington 70)
647 (Washington 41)
657 (Hoboken 33)
664 (Washington 7)
670 (New York 9)
694 (Washington 50)

Minus
(601-700)

-609 (New York 20)
-614 (Washington 5)
-624 (Washington 12)
-631 (Washington 39(
-638 (Washington 68)
-654 (Washington 14)

Plus (701-800)	Minus (701-800)
701 (Washington 24)	
712 (Norfolk 9)	
713 (New York 1)	
741 (Washington 58)	
748 (Washington 29)	
758 (Hoboken 28)	
759 (Norfolk 16)	
764 (Washington 3)	

d. Since the messages begin with an address, it was only necessary to try out all the addresses that would be likely to occur in such messages. The modus operandi of these trials is given in Section 3 of this Addendum. Suffice it here to say that the assumption of TRANSPORTATION3SERVICE, as the beginning of Hoboken 20, and ADJUTANT3GENERAL, as the beginning of Norfolk 10, yielded LEY3EQUIPMENT for New York 2. There was no doubt now that the messages were broken. Subsequent work meant merely the continuation of plain text in three cycles and the simultaneous reconstruction of the keys. As an aid in this process, one of labor and patience, it was found necessary to decipher parts of many other messages in cycles as close as possible to these three. For example, the closest cycle to cycle -76 was cycle -86, represented by Washington 25. As soon as the first fifteen letters of the short key had been reconstructed, viz, 260 to 275, these in conjunction with longer key letters in loci 186 to 201 were applied to Washington 25 at locus 186 in the longer key. They yielded as plain text 3EACH3DAY3AS3THE. By applying the same steps to other messages, places in cycles -93, -123, -130, -133, -141, and also in -46, -39, -29, -28, -17, and -9 were deciphered, all with a view to expediting the work of rebuilding the keys, which was all that was necessary to complete solution since we had no interest in the messages, per se. The work was divided between two sections of operators, one section working forward from locus 186 of the long key, the other working backward until the work joined. Even with this number of cycles to work upon, the work went slowly because of errors in the encipherment. It was completed, however, in a comparatively short time, and the resultant keys were tested upon isolated fragments of new messages and found to be correct.

It is ncessary to add that the messages were broken within ten minutes after one of those very slight but ever-present errors in transcribing the letters of the original three sequent cycles had been uncovered. This error involved the inadvertent omission, by one of our clerical staff, of a single letter from Norfolk 9 at a locus in advance of 186, and resulted in baffling all efforts to solution for every hour subsequent to the finding and the transcription of the three sequent cycles.

2. WHY KEY TAPES DIFFERING IN LENGTH BY MORE THAN ONE LETTER ARE CRYPTOGRAPHICALLY UNSAFE

In the preliminary summary of this addendum it was stated that the present system of using this machine employing key tapes which differ in length by more than one letter is much more unsafe than the original method employing key tapes which differ in length by only one letter. The reason for this is that the present system not only makes the production of overlaps very possible, but also makes their production, under certain circumstances, a legitimate function of the machine. In fact, the messages presented for test made a hairbreadth escape from such a fate! The point is well worth detailed explanation.

The question which first arises in this connection is: Given the initial indicators for each of four stations, can the cycles through which all messages will pass be determined beforehand? The answer is in the affirmative. In fact, the cycles through which each series of messages will pass themselves go through definite cycles. Let us refer to the calculations for the Hoboken series and set down in the form of a list the successive plus cycles involved:

HOBOKEN SERIES OF CYCLES

321
173
25
664
516
368
220
72
711
563
415
267
119
758
610
462
314
166
18
657
509
361

The numbers in this list bear definite relations to one another, relations which are absolutely determined by the displacement, or difference in the lengths of the two key tapes. In this case the difference between the lengths of the two key tapes is 787 - 639 148. This means that if we make our calculations upon the basis of a stationary long key tape, the displacement of the short key tape will be 148 letters per revolution of the long key tape. This in turn means that the progression of cycles for each series of messages, as determined by the difference between the key indicators, will differ by the constant factor 148. Let us see if this is exemplified in the series of cycle numbers given above for the Hoboken messages.

	Series as calculated	Series as observed
Initial cycle	321	321
2nd cycle of series	148 173	173
3rd cycle of series	148 25	25

If we continue to subtract 148, we would begin to introduce minus cycles, and since it is more advantageous to deal only with plus cycles, let us convert cycle 25 to the next higher multiple of this cycle number, by adding the length of the longer key tape to it.[1] Then:

[1] This is legitimate since all the calculations are based upon the revolutions of the long key tape.

$$\begin{array}{r} 25 \\ \underline{787} \\ 812 \end{array}$$

That is, cycle 25 is exactly the same as cycle 812. Now let us deduct 148, as before:

$$\begin{array}{r} 812 \\ \underline{148} \\ 664 \end{array}$$

This agrees with the cycle number given by our list. We could have combined the two steps of adding 787 and then deducting 148 in one step, by adding 639, the length of the short key, to 25. This would give the next cycle number. Thus,

$$\begin{array}{r} 25 \\ \underline{639} \\ 664 \end{array}$$

Let us continue

	Series as calculated	Series as observed
1.	321	321
	148	
2.	173	173
	148	
3.	25	25
	787	
	812	
	148	
4.	664	664
	148	
5.	516	516
	148	
6.	368	368
	148	
7.	220	220
	148	
8.	72	72
	787	
	859	
	148	
9.	711	711
	148	
10.	563	563
	148	
11.	415	415
	etc.	etc.

Thus, it is apparent that every cycle through which each series of messages will pass can be predetermined, provided always that no errors are made in the encipherment. For, if the relative positions of the two key tapes be changed in the slightest degree at any time in the enciphering process, the natural or predetermined series of cycles will be modified. Such modifications actually occurred in the four series of test messages, entirely as a result of errors on the part of the encipherer.

We give in the two lists which follow the series of cycles which actually resulted from the encipherment, together with the series which theoretically should have resulted. Each series has been arranged with reference to the others in a manner designed to show the production of sequent cycles.

TABLE 2

THEORETICAL SERIES

Wash. (126*001)	Hoboken (322*001)	Norfolk (518*001)	New York (714*001)
125			
764			
616			
(468)[1]			
(459)			
311	321		
163	173		
15	25		
654	664		
506	516	517	
358	368	369	
210	220	221	
62	72	73	
701	711	712	713
553	563	564	565
405	415	416	(417)[3]
257	267	268	(427)
109	119	120	279
758	758	759	131
600	610		770
452	462		622
304	314		474
156	166		326
8	18		178
647	657		30
499	509		
351	361		
203			
55			
694			
546			
398			
250			
102			
741			
593			
445			
297			
149			
(1)[2]			
(778)			
630			
482			

ACTUAL SERIES

Wash. (126*001)	Hoboken (322*001)	Norfolk (518*001)	New York (714*001)
125			
764			
616			
468			
320	321		
172	173		
24	25		
663	664		
515	516	517	
367	368	369	
219	220	221	
71	72	73	
710	711	712	713
562	563	564	565
414	415	416	417
266	267	268	269
118	119	120	121
757	758	759	760
609	610		612
461	462		464
313	314		316
165	166		168
17	18		20
656	657		
508	509		
360	361		
212			
64			
703			
555			
407			
259			
111			
750			
602			
454			
306			
158			
10			
649			
501			

[1]Error made in slipping the two key tapes between Washington 7 and 8.

[2]Error made in slipping the two key tapes between Washington 68 and 69.

[3]Error made in slipping the two key tapes between New York 4 and 5.

A careful study of Table 2 discloses some very important facts.

In the first place, the possibility of the production of overlaps is demonstrated very readily. Washington 1 began with the key indicators 126 * 001, and Hoboken 1 began with the key indicators 322 * 001. Had Hoboken 1 begun with the long key at 321 instead of 322, the Hoboken series would have begun immediately to overlap the Washington series from the latter's cycle 320 on to the end of the Hoboken messages. Again, Norfolk 1 began with the key indicators 518 * 001. Had Norfolk 1 begun with the long key at 517 instead of 518, or had Hoboken 1 begun with the long key at 323 instead of 322, the Hoboken and Norfolk series would have overlapped for the whole length of the Norfolk series. Again, New York began with key indicators 714 * 001, and Norfolk 1 began with key indicators 518 * 001. Had New York 1 begun with the long key at 713 instead of 714, or had Norfolk 1 begun with the long key at 519 instead of 518, the Norfolk and New York series would have overlapped.

The beginning points for each series were undoubtedly determined by dividing the length of the long key by four (in order to divide the long tape into four nearly equal parts) and adding this number to the long key starting point for each series consecutively. Thus, 787 ÷ 4 = 196. Given the long key starting point for Washington 1 as 126, the long key starting point for Hoboken 1 was 126 + 196 = 322; that for Norfolk 1 was 322 + 196 = 518; that for New York 1 was 518 + 196 = 714.

It is impossible, of course, to divide a prime number into four equal integral parts. In the case under study the length of the long tape is 787. The number 196 is the nearest integral fourth part of 787, it is true, but the division of the long tape into four parts is meant to be only approximate. The intention, as understood by us, is to allot to each station a length of the long key proportionate to its requirements as regards its day's activity. With certain key lengths, the allotment on the basis of equal activity of four stations will result in the production of overlaps. Likewise, with other key lengths, the allotment on the basis of unequal activity will result in the production of overlaps. Examples will be given.

Returning to this case, had the number 195 been taken as the amount to be added consecutively, instead of 196, here are the starting points that would have resulted for the four series:

Washington	Hoboken	Norfolk	New York
(126 * 001	(321 * 001)	(516 * 001)	(711 * 001)

Had this been the case a four-fold overlap would have been produced. Note the sequences of cycle numbers.

TABLE 3

Washington (126 * 001)	Hoboken (321 * 001)	Norfolk (516 * 001)	New York (711 * 001)
125			
764			
616			
468			
320	320		
172	172		
24	24		
663	663		
515	515	515	
367	367	367	
219	219	219	
71	71	71	
710	710	710	710
562	562	562	562
etc.	etc.	etc.	etc.

The cycle numbers would have coincided for the four series from cycle 710 onwards, and the four series of messages would have overlapped one another.

That this is not stretching the possibilities of the situation, consider the results of the adoption of 787 and 669 as the two lengths. These numbers do not possess a common factor and are not multiples of one another, so that their choice as key lengths is legitimate and likely. The displacement is 787 - 669 118. The allotment we will assume to be equal; the starting point for Washington 1, as 126 * 001. The starting points for the other series and the cycles are as follows:

TABLE 4

Washington 1 (126 * 001) Cycles		Hoboken 1 (322 * 001) Cycles		Norfolk 1 (318 * 001) Cycles		New York 1 (714 * 001) Cycles	
1	125	1	321	1	517	1	713
2	7	2	203	2	399	2	595
3	676	3	85	3	281	3	477
4	558	4	754	4	163	4	359
5	440	5	636	5	45	5	241
6	322	6	518	6	714	6	123
7	204	7	400	7	596	7	5
8	86	8	282	8	478	8	674
9	755	9	164	9	360	9	556
10	637	10	46	10	242	10	438
11	519	11	715	11	124	11	320
12	401	12	597	12	6	12	202
13	283	13	479	13	675	13	84
14	165	14	361	14	557	14	753
15	47	15	243	15	439	15	635
16	716	16	125	16	321	16	517
etc.		etc.		etc.		etc.	

Note now that a four-fold overlap would be the legitimate result of the choice of these lengths. This case is interesting also because it would produce four sequent cycles in addition to the overlaps. In other words, had the length of the short key in the series of test messages been 30 letters more than it was, not only would there have been produced four sequent cycles but also a four-fold overlap!

It may be desirable to give further instances. Let us assume two key lengths 811 and 753, two legitimate lengths. On the basis of equal activity, the allotment would be 811 ÷ 4 = 202 letters of the long tape per station. Suppose we start with the indicators 126 * 001 for the first message of the Washington series. The initial points for the other series will be as shown below:

Washington 1	Hoboken 1	Norfolk 1	New York 1
(126 * 001)	(328 * 001)	(530 * 001)	(732 * 001)

Now let us calculate the various cycles and tabulate them. The displacement is 811 - 753 = 58.

TABLE 5

Washington (126 * 001)		Hoboken (328 * 001)		Norfolk (530 * 001)		New York (732 * 001)	
1	125	1	327	→ 1	529	-+→ 1	731
2	67	2	269	2	471	2	673
3	9	3	211	3	413	3	615
4	762	4	153	4	355	4	557
5	704	5	95	5	297	etc.	
6	646	6	37	6	239		
7	588	7	790	etc.			
8	530	8	732				
9	472	9	674				
10	414	10	616				
11	356	11	558				
12	298	12	500				
13	240	13	442				
14	182	14	384				
15	124	15	326				
16	66	16	268				
17	8	17	210				
18	761	18	152				
19	703	19	94				
20	645	20	36				
21	587	21	789				
→ 22	529	-+→ 22	731				
23	471	23	673				
24	413	24	615				
etc.		etc.					

Note that two overlaps would be produced; the first cycle of the Norfolk series would overlap the 22nd cycle of the Washington series; the first cycle of the New York series would overlap the 22nd cycle of the Hoboken series.

Let us now take a case of differential allotment, assuming that the relative activities of four stations are in the proportion of 4:2:1:1. These proportions approximate the actual proportions in the series of test messages. We will adopt as key lengths 751 and 651. The displacement is 100 per revolution of the long tape. Allotment on the basis of the ratios 4:2:1:1 gives as the initial points for the four stations the following indicators:

TABLE 6

Washington 1 (100 * 001)		Hoboken 1 (472 * 001)		Norfolk 1 (658 * 001)		New York 1 (751 * 001)	
Cycles		Cycles		Cycles		Cycles	
1	99	1	471	1	657	→1	750
→2	750	2	371	2	557	2	650
3	650	3	271	3	550	3	550
4	550	4	171	4	450	4	450
5	450	5	71	5	350	5	350
6	350	6	722	6	250	6	250
etc.		etc.		etc.		etc.	

The New York series of messages overlap the Washington series immediately after the latter has entered its second revolution of the long tape.

Here is another instance. Let the allotment be in the proportion 1½:1:1:, and let the keys be 769 and 598. The initial points would be as follows:

TABLE 7

Washington 1 (100 * 001) Cycles		Hoboken 1 (355 * 001) Cycles		Norfolk 1 (525 * 001) Cycles		New York 1 (695 * 001) Cycles	
1	99	→ 1	354	+→ 1	524	++→ 1	694
2	697	2	183	2	353	2	523
3	526	3	12	3	182	3	352
4	355	4	610	4	11	4	181
5	184	5	439	5	609	etc.	
6	13	6	268	6	438		
7	611	7	97	7	267		
8	440	8	695	8	96		
9	269	+→ 9	524	++→ 9	694		
10	98	10	353	etc.			
11	696	11	182				
12	525	12	11				
→ 13	354	13	609				
14	183	14	438				
15	12	15	267				
16	610	16	96				
17	439	++→ 17	694				
18	268	etc.					
19	97						
20	695						
+→ 21	524						
22	353						
23	182						
24	11						
25	609						
26	438						
27	267						
28	96						
++→ 30	694						
31	523						
32	352						
33	181						
etc.							

Here the Hoboken series would make a single overlap with the Washington series beginning with cycle 354; a three-fold overlap would be produced with the Norfolk series when cycle 524 would be reached; and when cycle 694 would be reached the New York series would join and make a four-fold overlap.

Another case where overlaps would be produced legitimately in an equal allotment is as follows: Let us assume two keys 917 and 723. Equal allotments of the long tape would give the following initial points:

TABLE 8

Washington 1 (100 * 001) Cycles		Hoboken 1 (329 * 001) Cycles		Norfolk 1 (558 * 001) Cycles		New York 1 (787 * 001) Cycles	
1	99	1	328	1	557	1	786
2	822	2	134		etc.		etc
3	628	3	857				
4	434	4	663				
5	240	5	469				
6	46	6	275				
7	769	7	81				
8	575	8	804				
9	381	9	610				
10	187	10	416				
11	910	11	222				
12	716	12	28				
13	522	13	751				
14	328	14	557				

Here we would have a three-fold overlap; the Hoboken and Washington series would first overlap, then the Norfolk series would join in.

Take the case of the lengths of tapes involved in these test messages. Let us assume an allotment on the basis of 3:1:1:. The beginning points and the cycles for the four stations are as follows:

TABLE 9

Washington 1 (126 * 001) Cycles		Hoboken 1 (519 * 001) Cycles		Norfolk 1 (650 * 001) Cycles		New York 1 (781 * 001) Cycles	
1	125	1	518	1	649	1	780
2	764	2	370	2	501	etc.	
3	616	3	222	etc.			
4	468	4	74				
5	320	5	713				
6	172	6	565				
7	24	7	417				
8	663	8	269				
9	515	9	121				
10	367	10	760				
11	219	etc.					
12	71						
13	710						
14	562						
15	414						
16	266						
17	118						
18	757						
19	609						
20	461						
21	313						
22	165						
23	17						
24	656						
25	508						
26	360						
27	212						
28	64						
29	703						
30	555						
31	407						
32	259						
33	111						
34	750						
35	602						
36	454						
37	306						
38	158						
39	10						
40	649						
41	501						

The Norfolk series would overlap the Washington series when the latter enters cycle 649.

Such cases are not at all merely theoretical instances, but would be bound to happen. The solution of a case involving a single overlap, even for a short distance is very easy. To demonstrate, let us assume that the New York series of messages had begun with the key indicators 713 * 001 instead of 713 * 001 in Norfolk 9. A brief trial of possible beginnings for New York 1 would have resulted in yielding the excellent plain text shown below, when the address TRANSPORTATION3SERVICE had been assumed.

	Long key loci	713	723	733	
	Short key loci	001	010	020	
New York 1	Cipher	NTEXDRMUCIZGUH6M4YNFP5 ...			Cycle 712
	Assumed plain text	TRANSPORTATION3SERVICE ...			
	Long key loci	713	723	733	
	Short key loci	001	010	020	
Norfolk 9	Cipher	VBUHRI4Z5DZOK76INZIW7N ...			Cycle 712
	Resultant plain Text	2ASSIGNMENT3TO35SCHOOL ...			

As has already been stated the occurrence of such overlaps is not due to carelessness or errors, but is a legitimate function of the method, viz, the introduction of a difference of more than 1 between successive revolutions. The mathematical conditions under which these legitimate overlaps will be produced may be stated as follows:

When, during the enciphering process in two series of messages, the displacement becomes equal to the initial difference between the cycle numbers of the starting points, the two series of messages will begin to overlap. For example, given two series of messages, A and B, with the starting points 375 * 001 and 765 * 001, respectively, (keys 787 and 639 in length), after 5112 letters have been enciphered in Series A, an overlap will be produced with series B. Thus:

	Series A	Series B
	373 * 001	765 * 001
	5112 5112	
	5487 5113	
Deduct (787 x 6) and (639 x 8)	4722 5112	
	765 * 001	765 * 001

This result could have been predicted from the rule given above. The calculations which would show the same result theoretically are as follows:

Cycle difference of initial points	764 - 374 = 390
Displacement after 8 revolutions of the short tape and 6 revolutions of the long tape, that is, (639 x 8) - (787 x6)	5112 -4722 = 390

The calculations for the case in which the two key lengths were 787 and 669 are as follows:

Hoboken 1	322 * 001	Cycle 321	787 x 13 = 10231
Wash. 1	126 * 001	Cycle 125	669 x 15 = 10035
		196	Displacement - 196

In other words, given the starting points of the Hoboken and Washington series as 322 * 001 and 126 * 001, respectively, after 15 revolutions of the short tape (and 13 of the long at the same time), the Hoboken series would begin to overlap the Washington series.

Another important fact disclosed by a study of Table 2, giving the series of cycles produced in the test messages, is that the cycles produced as the two key tapes progress go through definite cycles themselves. It is clear that from any given starting points, if the encipherment proceeds without interruption or error until the total possible number of different pairs of key letters has been exhausted, the two key tapes would go through every one of the possible cycles, in this case 787. It would be possible in such a case to select any number of sequent cycles for analysis, since every cycle would be included in the series of cycles used by the station. But since the method of using the tapes by allotment is intended to keep each station within certain limits as regards the number of cycles at its disposal, it follows that this normal relation does not hold, and the series of cycles used by one of four stations may or may not include two or more sequent cycles. Since the members of the chain of cycles differ by a constant interval (governed by the displacement), it is possible to select messages the cycles for which are separated by the "smallest possible interval." For example, note the Washington list in Table 2. In this series of messages the smallest possible interval between any two cycles is 7; that is, the nearest cycle to cycle 125 is cycle 118; the nearest cycle to 764 is 757, or 7 removed, etc. The smallest possible interval is a function of two factors: (1) the displacement and (2) the allotment. The smallest possible interval is really determined by the least possible displacement within the limits set by the allotment as the encipherment continues. This, we may explain as follows:

Given 001 * 001 as the starting point, after 787 letters have been enciphered, the long key is at 001, the short key at [(001 + 787) - 639] = 149. The displacement of the short key is therefore 149 - 001 = 148. After 787 more letters have been enciphered, the long tape is again at 001, the short tape at [(149 + 787) - 639] = 297. The displacement of the short tape is therefore 297 - 001 = 296. Continuing this calculation, let us find the relative positions of the two tapes at the end of a few more revolutions.

		Displacements
Relative positions at end of 2nd rev. of long tape	001 * 297	296
" " " " " 3rd " " " "	001 * 445	444
" " " " " 4th " " " "	001 * 593	592
" " " " " 5th " " " "	001 * 741	640 = 101

Since the short key is only 639 letters in length, then locus 741 is the same as locus 102. Therefore the displacement after the 5th revolution of the long tape is 101 letters. Now the successive displacements as determined above may be found by adding 148 successively and making proper deduction for the length of the short key. Let us see what the displacement is after a few more revolutions.

Revolutions of Long Key	Displacement
1	148
2	296
3	444
4	592
5	101
6	249
7	397
8	545
9	54
10	202
11	350
12	498
13	7

As a check on this calculation, note the following:

```
  787        639
   13         16
 2361       3834
 787        639
10231      10224
```

Displacement = 10231 - 10224

That is, after 13 revolutions of the long key tape, during which the short tape has made 16 revolutions, the displacement of the short tape is 7. We may say, therefore, that with the two key lengths given, viz, 787 and 639, after approximately 10250 letters have been enciphered, the cycle in which the message will be proceeding at the time will be 7 removed from the initial cycle. If the amount of traffic for any station reaches or exceeds this number of letters, it becomes possible to select messages, all emanating from the same station, the cycles for which are only 7 intervals apart. This is actually the case in the series of test messages. If only one station were concerned, when the long tape would have made 639 complete revolutions, the short tape would have made 787 complete revolutions, the displacement would be 0, and every possible cycle would have been represented.

It is clear, therefore, that by alloting a definite number of cycles to each station, the smallest possible interval between any of its cycles is a function of the least possible displacement and the number of cycles which has been allotted to the station. With certain lengths the least possible displacement may become unity within the limits of the allotment of a station, and thus sequent cycles for messages from the same station become possible as a legitimate function of the system. For example, the two key lengths 811 and 753 yield the list of cycles given in Table 5. The list of the Washington series shows that the smallest possible interval is 1; for example, we have cycle 125 at the start, and cycle 124 as the fifteenth cycle in the series. The following list gives the series of displacements for these two key lenths.

Revolutions of Long Tape	Displacement
1	58
2	116
3	174
4	232
5	290
6	348
7	406
8	464
9	522
10	580
11	638
12	696
13	754

That is, after 13 revolutions of the long tape the net displacement would be 1, and the cycle upon which the message would then be about to enter would be directly sequent with the initial cycle. After 26 revolutions of the long tape, there would be three sequent cycles, and the series of messages would then run along in three sequent cycles.

It would be very easy to find a great many cases where the least possible displacement within the allotment limits is 2, 3, 4, or 5 intervals. In another section of this Addendum we shall show how the possession of three sequent cycles is no longer absolutely essential before a solution can be achieved. Cases where the cycles are separated by the same interval greater than 1 or by different intervals (within certain limits) are susceptible of solution.

3. METHODS FOR EXPEDITING THE TRIALS NECESSARY TO MAKE THE INITIAL BREAK IN THE DECIPHERMENT

It is quite true that there are difficulties in making the first break, but these are by no means so great as would seem.

It is necessary, before the decipherer can make the first break, that he find the correct plain text at the correct loci for two cycles. He may have the correct plain text for both cycles, but unless he applies it at the correct loci, all his efforts are of no avail.

Now, in the original explanation it was shown how the correctness of the assumptions of plain text for two cycles, hereafter to be designated as the "Experimental Cycles," was tested on the third, hereafter to be designated as the "Confirmative Cycle." This step necessitates the reconstruction of the long and short keys for the points where the plain text is assumed in the two experimental cycles and testing the reconstructed keys upon the third or confirmative cycle, at the proper loci. This process is very laborious and time-consuming, and where a great number of trials must be made, the recovery of the individual key letters by the process illustrated in Plate 1, Fig. 7 of the original paper is out of the question, unless a very large force of operators is at hand.

However, it is possible to reduce the process to such simple terms that a single operator can make as many as two thousand trials in three to four hours.

The easiest way to explain the process is to discuss the actual example afforded by the following three sequent cycles, with messages beginning at the points indicated by the stars and bars, as was the case with Norfolk 10 and Hoboken 20.

Upper key loci	186 196		
Lower key loci	260 270		
NEW YORK 2	... 6XTSQWQZKWCMCPWIDY3GD3A ...		Cycle -74
Upper key loci	* ‖ 186 196		
Lower key loci	‖ 261 271		
NORFOLK 10	... ‖ 3XH7GMERHP3QSNI3MCZVCTR ...		Cycle -75
Upper key loci	* ‖ 186 196		
Lower key loci	‖ 262 272		
HOBOKEN 20	... ‖ 3CTFJIXXLK3F4PKQ5LD ...		Cycle -76

In this case it is necessary to assume beginnings for Norfolk 10 and Hoboken 20, the experimental cycles, then test the assumptions upon New York 2, the confirmative cycle.

This testing may be done through the agency of reconstructed keys, but it is patent that the keys so reconstructed are of value not in themselves, but only insofar as they do or do not yield good plain text for New York 2. We may, therefore, omit the step of reconstructing the keys, <u>if we can test whatever assumptions are made with respect to the experimental cycles directly on the confirmative cycle without their intermediacy</u>, and thus save a great deal of time and labor.

In order to understand the method, it will be necessary to consider the relations existing between certain sets of letters in the long and short keys in three sequent cycles. In the subsequent discussion, for the sake of clearness, the long and the short keys will be designated as the upper and the lower keys, respectively.

CYCLE 1	Upper key	. . . . A R Q N V . . . .
	Lower key	. . . . Z X T P O R N . .
	Plain text	. . . . I N G 3 T . . . .
	Cipher	. . . . H 6 X V P . . . .
CYCLE 2	Upper key	* ‖ A R Q N V . . . .
	Lower key	‖ X T P O R N . . .
	Plain text	‖ C O M M A . . . .
	Cipher	‖ T Z X 4 Q . . . .
CYCLE 3	Upper key	* ‖ A R Q N V . . . .
	Lower key	‖ T P O R N . . . .
	Plain text	‖ A D J U T . . . .
	Cipher	‖ T Y 3 E 2 . . . .

Note that in Cycle 1 the plain text letter G is enciphered by the conjunction of the pair of key letters Q and T; in Cycle 3, the plain text letter D enciphered by the conjunction of the pair of key letters R and P. Now these two pairs of letters, viz, Q, T, and R, P form a single set of letters which encipher two adjacent letters of the plain text in Cycle 2, in criss-cross fashion. That is, in the second cycle, Q of the upper key in the first cycle unites with P of the lower key in third cycle; while T of the lower key in the first cycle unites with R of the upper key in the third cycle. Now the nature of the enciphering square, being completely symmetrical, is that no matter in what manner the letters of a set are united, the final or resultant letter is the same. For example, taking the four letters Q, T, R, and P, no matter how these letters come into juxtaposition or in what order they are taken, the result of the summation of the four of them will be "6". The result of these relations is that the second or middle cycle in any three sequent cycles represents a series of sets of letters which form a symmetrical or balanced system with certain sets of letters in the upper and lower cycles. It is analogous to the manner in which the two extremes in a proportion balance the two means. Such a set of letters will be designated hereafter as a "Balanced Set." This balanced relation holds true not only for the key letters; it holds also for the correct plain text letters with their respective cipher letters, because in every case the plain text with its cipher letter is balanced or is symmetrical with the two key letters involved. For example, the resultant of Q and T, viz, U, coincides with the resultant of G and X, viz, U. Therefore, the balanced or symmetrical relation existing between the key letters in the three sequent cycles, as pointed out above, exists also between the plain text and respective cipher letters involved.

Just as in the case of proportion (in mathematics) one can determine the unknown mean or the unknown extreme from the given relations between the three known quantities, so one can determine from these relations, without the intermediacy of the key letters, the unknown plain-text letter in the fourth set, assuming the correct plain-text letters in the proper loci in the other three sets. When the correct assumptions are made for the experimental cycles, therefore, the correct plain text must result in the confirmative cycle; the key letters can be reconstructed afterwards.

Let us apply the obvious steps to the example above, giving only the cipher letters first:

CYCLE 1	Confirmative Cycle	H	6	X	V	P
CYCLE 2	Experimental Cycle	T	2	X	4	Q
CYCLE 3	Experimental Cycle	T	Y	3	E	2

In the following explanation we shall indicate by the Greek letter Sigma (Σ) that the summation of the series of letters is to be taken. Thus:

$$\Sigma\begin{cases}6\\2\\T\\T\end{cases}\quad \Sigma\begin{cases}X\\X\\2\\Y\end{cases}\quad \Sigma\begin{cases}V\\4\\X\\3\end{cases}\quad \Sigma\begin{cases}P\\Q\\4\\E\end{cases}$$

Base -	B	Q	K	4

The resultant series of letters B Q K 4 ... , which we have termed the BASE, forms the framework upon which the assumptions are made and the results noted. Let us assume that the message in one of the experimental cycles, viz, Cycle 2 begins COMMANDING, and then let us try all other possible beginnings for the other experimental cycle, viz, Cycle 3, in conjunction with it. First, it is necessary to "add" the letters of COMMANDING to the base, in the manner shown below, which gives the resultant of the first assumption, or, as we shall term it merely, the FIRST RESULTANT.

Base		B	Q	K	4
Assumed plain text for one experimental cycle 2	C	O	M	M	A

	B	Q	K	4
	C	O	M	M
	O	M	M	A
FIRST RESULTANT	K	W	K	Q

We are ready now to try in conjunction with the first resultant all possible beginnings for the other experimental cycle (Cycle 3). Let us assume that this message also begins with COMMANDING and find the second resultant. If the plain text assumed for both experimental cycles is correct, and in the correct loci, then the second resultant must yield intelligible plain text.

FIRST RESULTANT	K	W	K	Q
Assumed plain text for other experimental cycle 3	C	O	M	M
SECOND RESULTANT	E	J	W	J

This gives E J W J as the second resultant, or the plain text of the confirmative cycle (Cycle 1), and we realize at once that one or both of our assumptions for the experimental cycles are incorrect. Let us retain COMMANDING as the beginning of Cycle 2, and assume THE3 as the plain-text beginning of Cycle 3, instead of COMMANDING. The results are as follows:

FIRST RESULTANT	K	W	K	Q
Assumed plain text for other experimental cycle	T	H	E	3
SECOND RESULTANT	5	U	C	W

This, too, is clearly incorrect. Thus we proceed until the trial of ADJUTANT:

FIRST RESULTANT	K	W	K	Q
Assumed plain text for other experimental cycle	A	D	J	U
SECOND RESULTANT	N	G	3	T

Here is a good possibility, and we proceed at once to add to it.

Now all these trials can be made very rapidly by the use of certain sliding alphabets. These are prepared by cutting apart the columns of the cipher square, accompanying each alphabet by the straight alphabet including the "functions," and arranging the letters as shown below, where only the first five and last five pairs of the A, B, and C alphabets are given, (Fig. 20).

Taking the sliding alphabets indicated by the first resultant, viz, K, W, K, and Q alphabets, we slide them in such a manner as to align the letters of the assumed plain text, using the upper (normal sequence) member of each pair of letters for this, whereupon the resultant plain text for Cycle 1 (the second resultant, or the text of the confirmative cycle) appears on a line made up of the other (mixed sequence) member of each set of letters composing the pairs. Thus, the trial of the first four letters, ADJU, of the assumed plain-text beginning for the one message, would place the sliding alphabets in the position shown in Fig. 21, wherein the four letters of the resultant plain text for the other message is immediately apparent: N G 3 T. Thus, by sliding the alphabets, all the possible beginnings for Cycle 3 are tested with the assumed beginning, COMMANDING, for Cycle 2. If no good results are obtained, then one assumes some other beginning for Cycle 2 and goes through the same steps again. If no errors have been made in calculations, when the correct beginnings have been assumed in the correct loci of the experimental cycles, the correct plain text must appear in the confirmative cycle.

While it may not be apparent, it is nevertheless true that this process viewed in its proper light reduces the three sequent cycles to the terms of an "overlap." When an overlap occurs, it is necessary to assume the correct plain text in the correct locus for one message, whereupon the correct plain text for the other message appears. In this method, it is necessary to assume the correct plain text in two loci.

Let us go through the solution of the test messages, as it actually was achieved. The three messages involved are New York 2, Norfolk 10, and Hoboken 20, of which the last two mentioned are the experimental cycles; the first, the confirmative cycle. This is one of the two excellent points of attack referred to on page 27. The steps are summarized below:

```
Upper key loci           186       196
Lower key loci           260       270
NEW YORK 2      ... 6XTSQWQZKWCMCPWIDY3GD3A ... Cycle -74 (Confirmative)

Upper key loci           186       196
Lower key loci           261       271
NORFOLK 10      ...|SXH7GMERHP3QSNI3MCZVCTR ... Cycle -75 (Experimental)

Upper key loci        |186       196
Lower key loci        |262       272
HOBOKEN 20      ...   | 3CTFJIXXLK3F4PKQ5LD ... Cycle -76 (Experimental)
```

```
        W Q Z K W C M C . . .
        G M E R H P 3 Q . . .
        M E R H P 3 Q S . . .
        3 C T F J I X X . . .
Base    Z 3 R M G G L E . . .
```

Since in Norfolk 10 the first letter which enters into the balanced relations discussed above is G, we must place the letters of whatever we assume for that message in their proper loci, viz, the 5th letter of the assumed beginning must go under its cipher letter G; the 6th, under M; etc. Assuming ADJUTANT3GENERAL for the beginning of Norfolk 10, we must add the proper letters as shown below:

A	B	C
A	A	A
7	G	F
B	B	B
G	7	Q
C	C	C
F	Q	7
D	D	D
R	T	U
E	E	E
2	O	K
.	.	.
.	.	.
.	.	.
3	3	3
U	X	R
4	4	4
J	Z	1
5	5	5
M	I	Z
6	6	6
O	2	Y
7	7	7
A	B	C

FIG. 20

K	W	K	Q
			AH
			BC
			CB
			DV
			EP
			FG
			GF
			HA
			IZ
			JM
			KO
		AN	LS
		BP	MJ
		CE	N6
		DI	OK
		EC	PE
		F2	Q7
	AT	GY	RX
	BR	H6	SL
	CX	ID	TU
AN	DG	J3	UT
BP	EL	K7	VD
CE	FV	LX	W3
DI	GD	MW	XR
EC	HU	NA	Y2
F2	IY	OQ	ZI
GY	JO	PB	2Y
H6	KM	QO	3W
ID	LE	RS	45
J3	MK	SR	54
K7	N5	T5	6N
LX	OJ	U4	7Q
MW	PS	VZ	
NA	Q3	WM	
OQ	RB	XL	
PB	SP	YG	
QO	TA	ZV	
RS	UH	2F	
SR	VF	3J	
T5	W7	4U	
U4	XC	5T	
VZ	YI	6H	
WM	Z2	7K	
XL	2Z		
YG	3Q		
ZV	46		
2F	5N		
3J	64		
4U	7W		
5T			
6H			
7K			

= { A D J U . . .
{ N G 3 T . . .

FIG. 21

Base	Z 3 R M G G L E . .
Assumed plain text for Norfolk 10 experimental cycle	T A N T 3 G E N E . .
Base	Z 3 R M G G L E . . .
Assumed plain text for Norfolk 10	T A N T 3 G E N . . . A N T 3 G E N E . . .
1st resultant	2 J P 4 3 E 5 N . . .

Let us now set up the sliding alphabets 2, J, P, 4, 3, E, 5, and N, and then try out the various possible beginnings for Hoboken 20, the other experimental cycle. When TRANSPORTATION is tried, the results are as shown in Fig. 22.

2	J	P	4	3	E	5	N
AE	A4	AY	AJ	AU	A2	AM	AK
B6	BL	BK	BZ	BX	BO	BI	BY
CN	CS	CO	CI	CR	CK	CZ	C2
DJ	D2	D5	DE	DF	D4	DP	DS
EA	ER	EQ	ED	ES	E7	EV	EF
FK	FI	F6	FS	FD	FN	FL	FE
GO	GZ	GN	GL	GV	G6	GS	GP
HP	H5	H2	HM	HT	HY	HJ	HO
I3	IF	IT	IC	I2	IU	IB	IR
JD	J7	JX	JA	JK	JR	JH	JU
KF	K3	KB	KU	KJ	KC	KT	KA
LT	LB	L3	LG	LP	LW	LF	LV
MV	MQ	MR	MH	MO	MX	MA	MT
NC	NU	NG	N3	N4	NF	NW	N7
OG	OW	OC	OT	OM	OB	OU	OH
PH	PX	P7	PV	PL	PQ	PD	PG
QY	QM	QE	Q5	QW	QP	Q4	Q6
R4	RE	RM	R2	RC	RJ	RY	RI
SU	SC	SW	SF	SE	S3	SG	SD
TL	T6	TI	TO	TH	TZ	TK	TM
US	UN	UZ	UK	UA	UI	UO	UJ
VM	VY	V4	VP	VG	V5	VE	VL
WZ	WO	WS	W6	WQ	WL	WN	W5
X5	XP	XJ	XY	XB	XM	X2	XZ
YQ	YV	YA	YX	YZ	YH	YR	YB
ZW	ZG	ZU	ZB	ZY	ZT	ZC	ZX
27	2D	2H	2R	2I	2A	2X	2C
3I	3K	3L	3N	37	3S	36	34
4R	4A	4V	47	4N	4D	4Q	43
5X	5H	5D	5Q	56	5V	57	5W
6B	6T	6F	6W	65	6G	63	6Q
72	7J	7P	74	73	7E	75	7N

TL RE AY N3 SE PQ OU RI = (T R A N S P O R / L E Y 3 E Q U I)

FIG. 22

From the sequence L E Y 3 E Q the word EQUIPMENT soon made itself apparent. A few more letters (PMENT3) were tried out to make sure, and very soon, since these yielded good plain text in the other two cycles, it was clear that the cipher system had indeed been solved and the challenge successfully met.

The keys were then reconstructed, additional messages being utilized to expedite the process; they were then tested on new messages and found to be correct.

It should be clear that this method of using sliding alphabets can be applied to a case where the beginning points of two messages are not close together. In such a case, given one of the experimental cycles as involving a beginning of a message, possible beginnings are assumed for it and then the sliding alphabets are brought into play by assuming high frequency polygraphs for the interior of the other experimental cycle and testing the results on the third confirmative or third cycle.

* * * *

In the preceding method it was necessary to assume plain text for two cycles and test the assumptions on the third. We shall now show how plain text may be assumed for only one cycle and the correctness of the assumption tested on the other two cycles simultaneously. We shall use for examples New York 2, Norfolk 9, and Hoboken 19.

	Upper key loci	179
NEW YORK 2	Lower key loci	↓ 253
Cycle -74	Cipher	. . . T N P W B Q F V L R G 6 X T . . .
	Upper key loci	179
NORFOLK 9	Lower key loci	← 254
Cycle -75	Cipher	. . . 2 E P Q U 2 3 U N
	Upper key loci	179
HOBOKEN 19	Lower key loci	255
Cycle -76	Cipher	. . . W D P Z M C Z W H E A 3 3

The base is as follows:

	P	W	B	Q	F	V	L
	P	Q	U	2	3	U	N
	E	P	Q	U	2	3	U
	D	P	Z	M	C	Z	W
Base	4	3	0	C	S	N	R

Let us assume for the plain text of Norfolk 9 the likely ending, 3OFFICER, and find the first resultant. In order to apply the assumed text to the base in this case, it will be necessary to find what we have termed the MEAN VALUES of the assumed text. These are simply the sums of the successive letters of the plain text taken in pairs. They have been termed mean values because they constitute the means in our balanced sets or proportions.

For example, the mean values of the word 3OFFICER are as follows:

Plain text	3		O		F		F		I		C		E		R
Mean values		M		Y		7		J		4		K		J	

The mean values are now applied to the base, yielding the first resultant as follows:

Base	4 3 0 C S N R
Mean values	M Y 7 J 4 K J
First resultant	H Z O S F A E

The sliding alphabets are now brought into play, and an attempt is made to produce intelligible text on two lines made up of a pair of letters on each alphabet. Note the following set up in Fig. 23 and the plain text given by the lines indicated.

This method of making an initial break into three sequent cycles makes it very practicable to work with the case where the beginning points of two messages are not close together. Given one of the experimental cycles as involving the beginning of a message, assumptions of probable addresses are made, and then the sliding alphabets are brought into play by assuming for the interior of the other experimental cycle high frequency polygraphs such as 44233333, 6M533, 6N53, 3THE3, 3OF3THE3, etc. The results of the assumptions are tested on the confirmative cycle.

* * * *

The relations existing between the experimental and the confirmative cycles may assume three general cases:

1. the two experimental cycles may be the first and second of three sequent cycles, whereupon the confirmative cycle is the third of the series;

2. the two experimental cycles may be the second and third of three sequent cycles, whereupon the confirmative cycle is the first of the series;

3. the two experimental cycles may be the first and third of three sequent cycles, whereupon the confirmative cycle is the second or middle one of the series.

To continue the analogy with the relations in a proportion, in the first case, the upper experimental cycle constitutes one of the extremes; the second experimental cycle constitutes the two means; and the confirmative cycle constitutes the other extreme. The second case is the same as the first. In the third case the experimental cycles constitute the extremes, the confirmative, the two means. The third case is therefore considerably different from the first two in that in the first two cases we have given (or rather assumed) one extreme and both means, leaving only one unknown, viz, the other extreme, to be determined; whereas in this case we have given (or rather assumed) both extremes and still have two unknowns, viz, both means, to be determined. Were it the case that one and only one isolated balanced set were concerned in Case 3, there would be no way of finding both means; but the fact is that a series of balanced sets is involved, and that fact coupled with the fact that the two unknown means of each balanced set combine with the adjacent pair of unknown means to form intelligible text enables us to select from thirty-two pairs of unknowns for each balanced set the pair which, when united with one of thirty-two pairs for its neighboring balanced set forms intelligible text; and this process continued results in the production of plain text for the confirmative cycle. Exactly what is meant will become clearer in an example. We shall give the correct plain text for all three cycles first, and then take up the cipher letters alone.

H	Z	O	S	F	A	E
		A6				
		BE		AC		
		CP		BH		
		DZ		CA		
		EB		D3	A7	
		FY		EN	BG	
		G2		F7	CF	
		HN		GQ	DR	
		IV		HB	E2	
		JW		IJ	FC	
		KQ		JI	GB	
AQ		LR		K2	HQ	
BF		M3		L5	IS	A2
CG		NH		MZ	J4	BO
DX		O7		NE	KN	CK
EY		PC		OY	LZ	D4
FB		QK		P6	M5	E7
GC		RL		QG	NK	FN
H7		SX	AT	RU	O6	G6
IL		T4	BM	S4	PY	HY
J5		U5	CJ	TX	QH	IU
K6		VI	DN	UR	RD	JR
LI		WJ	E3	VW	SI	KC
M4		XS	F4	WV	TW	LW
NO		YF	G5	XT	U3	MX
ON		ZD	HZ	YO	VX	NF
P2	AL	2G	IA	ZM	WT	OB
QA	BA	3M	JC	2K	XV	PQ
RV	C5	4T	KR	3D	YP	QP
SZ	DQ	5U	LQ	4S	ZL	RJ
T3	**ET**	**6A**	**MB**	**5L**	**2E**	**S3**
UW	FM	7O	ND	6P	3U	TZ
VR	GJ		OX	7F	4J	UI
WU	HS		PW		5M	V5
XD	IQ		QL		6O	WL
YE	JG		RK		7A	XM
ZS	KV		S7			YH
2P	LA		TY			ZT
3T	MF		U2			2A
4M	NX		V6			3S
5J	OD		WP			4D
6K	PU		XO			5V
7H	QI		YT			6G
	R6		ZH			7E
	SH		2U			
	TE		3E			
	UP		4F			
	VK		5G			
	W2		6V			
	XN		7S			
	Y3					
	Z7					
	2W					
	3Y					
	4B					
	5C					
	6R					
	7Z					

= { T E 6 M 5 2 S . . .
  { 3 T A B L E 3 . . .

FIG. 23

MESSAGES

CYCLE 1	Upper key	S Q T P N V R
	Lower key	O B N T O K A B D
	Plain text	Z O N E 3 F I
	Cipher	N P T U T M K
CYCLE 2	Upper key	S Q T P N V R
	Lower key	B N T O K A B D
	Plain text	R T M E N T 3
	Cipher	P J M K K F Q
CYCLE 3	Upper key	T P N V R
	Lower key	O K A B D
	Plain text	C H I E F
	Cipher	I F D I C

* * * * * *

Cycle 1 (Experimental): N P T U T M K
Cycle 2 (Confirmative): P J M K K F Q
Cycle 3 (Experimental): I F D I C

	U T M K . . .
	K K F Q . . .
	M K K F . . .
	I F D I . . .
Base:	L X Q W . . .
Assumed plain text for Cycle 3:	C H I E F 3 .
First resultant:	M D Z L . . .

To the first resultant let us add ZONE3FINANCE, the assumed plain text of the other experimental cycle, viz, Cycle 1. The first letter which enters into the relations is the E of ZONE.

First resultant:	M D Z L . . .
Assumed plain text for Cycle 1:	E 3 F I . . .
Second resultant:	X F M H . . .

Let us consider now the first three balanced sets in our relations:

CYCLE 1	Cipher	U T M	EXPERIMENTAL CYCLE
	Plain text	E 3 F	
CYCLE 2	Cipher	M K K F Q	CONFIRMATIVE CYCLE
	Plain text	$P_1 P_2 P_3 P_4 P_5$	
		X F M H	
CYCLE 3	Cipher	I F D	EXPERIMENTAL CYCLE
	Plain text	C H I	

The letters of the second resultant are shown in their proper places in Cycle 2. The first letter of the series, viz, X is the sum of two plain text letters represented by P_1 and P_2 ; the second letter of the series, viz, F, is the sum of two plain text letters represented by P_2 and P_3. If, therefore, we assume P_1 to have any value, say A, we can derive, successively, the values of P_2, P_3, P_4, P_5 . . . . Thus:

If $P_1 = A$, then $P_2 = A + X = \underline{V}$; $P_3 = V + F = \underline{W}$; $P_4 = W + M = K$; $P_5 = K + H = \underline{6}$

Upon this assumption the plain text of the confirmative cycle would read A V W K 6, which is obviously incorrect.

We could proceed to find the value of this series based upon various assumed initial values of P_1, taking the letters of the alphabet in succession. Let us see what we get when we assume $P_1 = M$.

If $P_1 = M$, then $P_2 = M + X = \underline{E}$; $P_3 = E + F = N$; $P_4 = N + M = T$; $P_5 = T + K = 3$

Here we have excellent plain text, M E N T 3.

We may eliminate all the trials necessary to find the value of P_1 by the use of sliding alphabets. Assuming P_1 to have the value of 7, the value of P_2, P_3 ... is found in the following manner, starting with the second resultant X F M H derived as shown on page 55:

Second resultant	X	F	M	H
	7	X	T	N
Third resultant	X	T	N	O

or

P_1		P_2		P_3		P_4		P_5
	X		F		M		N	
7		X		T		N		O

Setting up the letters indicated in the third resultant on the ordinary sliding alphabets of the cipher square, we have what is shown in Fig. 24.

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

FIG. 24

Here the correct generatrix becomes visible almost instantly by giving intelligible text.

The choice of 7 as the basic or assumed value of P means nothing in itself, for any other of the thirty-two letters of the alphabet might be used as a base, with the same results. For example, supposing, as before, we start with a as a base, we get the third resultant shown below:

	P_1		P_2		P_3		P_4		P_5
Second resultant		X		F		M		H	
Third resultant	A		V		W		K		6

Setting these alphabets up, we find that the generatrices are exactly the same as those produced above, but they are in a different order, as shown in Fig. 25.

The mechanics of the process should be clear. Each of the letters of the second resultant, X, F, M, H, ... represents the union of a pair of means in the proportions mentioned on page 52. The pair of means of adjacent proportions have one member in common. This fact, together with the fact that the succession of means must form intelligible text, makes the process capable of yielding the desired results.

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

FIG. 25

* * * * * *

SLIDING OF ASSUMED PLAIN TEXT TO FIND ITS CORRECT LOCUS

It has been stated above that not only must the correct plain texts be assumed in two different cycles but also these texts must, of course, be assumed in the correct loci in those cycles.

Proceeding upon the theory that messages emanating from Norfolk, New York, and Hoboken are more likely to go to Washington than to other points, it seemed feasible to assume as the plain text of the beginnings of certain messages WAR3DEPARTMENT2WASHINGTON 3DC3, the problem then being to find the correct loci of the phrase in each of two cycles. An example will serve to make the process clear. Note the three sequent cycles below, in which WAR3DEPART MENT2WASHINGTON3DC3 is assumed to occur in experimental cycles 2 and 3 near the beginning of the messages.

```
Upper key loci                        192      202      212
Lower key loci                        266      276      286
N.Y. 2 (Cycle -74) ...6XTSQWQZKWCMCPWIDY3GD3A6JM3ZE6EKTD4FZRLR... Con.

Upper key loci      ||*               192      202      212
Lower key loci      ||                267      277      287
NOR. 10 (Cycle -75) ||SXH7GMERHP3QSNI3MCZVCTRVOUOMVNUS4T64AAZY... Exp.

Upper key loci        ||*             192      202      212
Lower key loci        ||              268      278      288
HOB. 20 (Cycle -76)   ||3CTFJIXXLK3F4PKQ5LDYEQUGEPWGVOL34VVV... Exp.
```

It is possible, of course, to begin by placing WAR3DEPARTMENT2 WASHINGTON at any of the likely loci of Cycles -75 and -76, reconstruct the keys and try them on Cycle -74. If no good text results, the phrase would be moved one space to the left or right in one of the cycles, say the second, and the keys reconstructed again. This process would be continued until the phrase had been shifted to all possible loci in Cycle -76 (within the section under examination), keeping the locus of the phrase stationary in Cycle -75. If no good results were obtained, then the phrase in Cycle -75 would be shifted one space to the right or left and the whole process of shifting the same phrase in Cycle -76 would be gone through again. In a section of 25 letters in length with a phrase 25 letters in length also, 50 x 50 or 2500 trials would be necessary to exhaust every possibility. The labor and time of making such a test being very great, a short cut was devised, which reduces the work enormously. Sliding alphabets of a special kind are used. They consist of a simple rearrangement of the horizontal lines of the cipher square, according to the order of the letters of the phrase to be tested. If the phrase be WAR3DEPARTMENT2 WASHINGTON, then the W row of the cipher square is written first, followed by the A row, then by the R row, etc., until all the rows have been arranged accordingly. The modified cipher square then has the following form:

WAR3DEPARTMENT2WASHINGTON

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

FIG. 26

The columns are then cut apart, and mounted on strips in the form of sliding alphabets, ready for use. The method of use, employing the principle of balanced sets, will be illustrated in the case of the three cycles forming the basis of the preceding analysis. We shall start by assuming that the phrase WAR3DEPARTMENT2WASHINGTON is in locus 192/267 of experimental cycle -75, as the beginning phrase of Norfolk 10. The base and the first resultant are derived in the usual manner, and are as shown below:

NEW YORK 2	Upper key loci	192
CYCLE -74	Lower key loci	266
(CONFIRMATIVE)	Cipher	...6XTSQWQZKWCMCPWIDY3GD3A6JM3ZE6EKTD4FZRL..
NORFOLK 10	Upper key loci	192
CYCLE -75	Lower key loci	267
(EXPERIMENTAL)	Cipher	...3QSNI3MCZVCTRVOUOMVNUS4T64AAZY...
	Assumed p. t.	...WAR3DEPARTMENT2WASHINGTON...
HOBOKEN 20	Upper key loci	192
CYCLE -76	Lower key loci	268
(EXPERIMENTAL)	Cipher	...XXLK3F4PKQ5LDYEQUGEPWGVOL34VVV...

	M	C	P	W	I	D	Y	3	G	D	3	A	6	J	M	3	Z	E	6	E	K	T	D	4
	Q	S	N	I	3	M	C	Z	V	C	T	R	V	O	U	O	M	V	N	U	S	4	T	6
	3	Q	S	N	I	3	M	C	Z	V	C	T	R	V	O	U	O	M	V	N	U	S	4	T
	X	X	L	K	3	F	4	P	K	Q	5	L	D	Y	E	Q	U	G	E	P	W	G	V	O
Base	L	E	F	P	7	M	K	F	G	C	S	J	I	O	2	N	L	B	4	M	V	U	K	6
Assumed plain	W	A	R	3	D	E	P	A	R	T	M	E	N	T	2	W	A	S	H	I	N	G	T	O
text for NOR. 10	A	R	3	D	E	P	A	R	T	M	E	N	T	2	W	A	S	H	I	N	G	T	O	N
First resultant	2	4	A	6	4	J	G	3	7	2	O	I	G	R	W	M	H	4	C	P	4	F	U	K

The sliding alphabets indicated in this first resultant are then set up in a "staggered" manner, as shown below in Fig. 27. If the hypothetical phrase in Cycle -75 is really in the locus assumed, and if it also is contained anywhere within the section included in Cycle -76, then intelligible text must appear on some generatrix of the set-up.

Should it happen that the locus of the first letter of the phrase in both cases falls within the same column, that is under the same "long key" letter, the uncovered plain text for Cycle -74 will occupy the longest generatrix; that is it will begin with the second letter on the first strip (the letter immediately below the letter designating the alphabet) and will continue all along the generatrix, provided no breaks occur in the phrase WAR3DEPART MENT2WASHINGTON, as assumed. If a break should occur, for example, should the phrase be WAR3DEPARTMENT6N53WASHINGTON, then the uncovered plain text for Cycle -74 will appear on two generatrices, separated by four letters giving unintelligible text.

Should the phrase in Cycle -76 begin one letter to the right of where it begins in Cycle -75, the plain text will appear on the generatrix which begins with the second letter on the second strip, and so on upwards until, if the phrase in Cycle -76 should begin under the next to the last letter of the phrase in Cycle -75, only one letter of the plain text for Cycle -74 will be given by the set-up, viz, the second letter on the last strip. Should the

																								K
																							U	M
																						F	H	N
																					4	V	3	S
																				P	6	C	F	J
																			G	S	J	U	A	T
																		4	D	Y	2	D	C	C
																	H	6	B	M	N	3	I	B
																M	U	J	T	L	E	N	Z	N
															W	K	Q	2	V	5	D	6	3	S
														R	7	5	V	N	W	Q	V	C	F	5
													G	B	T	P	T	E	6	7	J	U	Q	W
												I	D	D	B	O	X	D	N	Y	2	X	6	C
											Q	Y	B	7	Q	Y	Y	V	B	M	O	Z	I	A
										2	J	S	T	C	G	X	2	J	T	I	H	N	J	5
									7	Z	6	N	V	A	L	R	Q	2	R	R	D	E	Q	F
								3	W	E	L	2	W	J	S	5	V	O	I	Q	3	X	S	M
							G	Q	A	4	M	K	6	M	T	P	3	H	6	G	O	K	H	N
						J	D	U	R	I	Z	U	N	D	B	N	4	D	P	I	R	V	3	R
					4	O	B	C	3	J	B	T	B	7	A	7	Y	3	R	H	6	C	2	6
				6	6	4	T	7	D	A	C	S	T	G	K	X	O	O	O	S	J	4	W	D
			A	4	J	E	V	F	E	H	6	N	R	P	L	T	3	R	D	Y	F	B	E	A
		4	T	O	2	K	W	S	P	E	L	P	I	J	5	N	P	6	B	W	M	J	J	Y
	2	6	7	Z	N	2	6	L	A	4	4	G	6	I	A	V	U	J	5	2	C	E	X	5
1.	Z	J	D	5	E	R	N	U	R	L	3	U	P	G	Z	K	Q	F	C	T	3	Q	Q	Q
2.	E	2	U	L	D	X	B	C	T	V	B	R	R	4	7	5	Z	M	M	G	L	X	5	A
3.	4	N	R	G	V	4	T	H	M	A	H	P	O	B	T	B	7	C	P	N	O	Y	J	
4.	I	E	2	F	J	E	R	O	E	C	4	3	D	D	P	A	L	3	7	I	T	E		
5.	J	D	Y	O	2	6	I	S	N	L	G	Y	B	K	U	G	O	L	R	C	3			
6.	A	V	7	Z	O	Q	6	4	T	7	J	S	5	V	Y	T	C	O	2	G				
7.	H	J	D	J	H	R	P	H	2	Z	6	A	C	N	5	I	3	T	P					
8.	E	Z	W	U	D	U	R	I	W	E	X	L	M	I	D	N	N	3						
9.	4	O	5	G	3	6	O	Q	A	U	N	7	P	T	A	3	O							
10.	L	H	2	Q	O	D	D	U	S	P	V	R	7	G	J	T								
11.	V	D	K	J	R	O	B	E	H	3	H	M	R	L	5									
12.	A	3	W	B	6	4	5	T	I	C	2	P	2	I										
13.	C	O	E	4	J	C	C	2	N	O	4	V	P											
14.	L	R	T	C	F	5	M	4	G	L	7	R												
15.	7	6	7	V	M	F	P	V	T	G	H													
16.	Z	J	I	K	C	U	7	H	O	C														
17.	E	F	Q	X	3	Z	R	M	N															
18.	U	M	S	Q	L	6	2	4																
19.	P	C	K	E	O	W	P																	
20.	3	3	B	J	T	U																		
21.	C	L	W	A	3																			
22.	O	O	6	Q																				
23.	L	T	K																					
24.	G	3																						
25.	C																							

FIG. 27

phrase in Cycle -76 begin one letter to the left of where it begins in Cycle -75, the plain text will appear on the generatrix which begins with the third letter of the first strip and so on downwards, the reverse of what was set forth above. In other words, by keeping WAR3DEPARTMENT2WASHINGTON in the locus shown in Cycle -75 in the textual diagram above, this one set-up of the special sliding alphabets is equivalent to having slid the same phrase in Cycle -76 fifty times. Examining Fig. 27 in the light of the foregoing discussion, no good plain text is discovered on any generatrix, nor do we find even a fragment of intelligible text sufficient to justify further experiment with this set-up. We proceed thereupon to move the phrase one space to the right in Cycle -75.

Going through the same steps as shown on page 59, with the same assumed phrase in Cycle -75 (WAR3DEPARTMENT2WASHINGTON) but beginning under the letter Q instead of 3, we have the following:

Upper key loci	192	
Lower key loci	266	
N.Y. 2, Cycle -74	6XTSCMCPWIDY3GD3A6JM3ZE6EKTD4FZRLR	CONFIRMATIVE
Upper key loci	192	
Lower key loci	267	
NORFOLK 10, Cycle -75	3QSNI3MCZVCTRVOUOMVNUS4T64AAZY WAR3DEPARTMENT2WASHINGTON	EXPERIMENTAL
Upper key loci	192	
Lower key loci	268	
HOBOEKN 20, Cycle -76	XXLK3F4PKQ5LDYEQUGEPWGVOL34VVV	EXPERIMENTAL
BASE	Z3OFHOOWHDPJ3YX25BCHZSWO	

If the second generatrix, omitting the first letter, of the preceding set-up of alphabets (Fig. 27) be united with the phrase WAR3DEPARTMENT2WASHINGTON, we get the same base as is indicated here when the phrase is moved one letter to the right in Cycle -75. Thus:

2d Gen. of Fig. 27	(E)	2	U	L	D	X	B	C	T	V	B	R	R	4	7	5	Z	M	M	G	L	X	5	A	7
Assumed plain text		W	A	R	3	D	E	P	A	R	T	M	E	N	T	2	W	A	S	H	I	N	G	T	O
Derived new base		Z	3	O	F	H	O	O	W	H	D	P	J	3	T	X	2	5	B	C	H	Z	S	W	O

This means that once a set-up such as that of Fig. 27 is made, new or additional write-outs of cycles as the assumed phrase is slid, need not be made: the proper bases can be derived as shown by the foregoing example from a single write-out of cycles and assumed plain text.

The sliding alphabets indicated by the foregoing derived base (it is really a "first resultant") are then set up as before, and the various generatrices are examined with a view to finding plain text. The set-up given in Fig. 28 shows a generatrix containing intelligible text consisting of a sequence of eight letters, N G 3 T O 3 S 6. Note the generatrix which is underscored. It means that we have struck the correct loci of at least a part of our hypothetical phrase in Cycle -75 and Cycle -76. We can ascertain what parts are involved from the position of the plain text in Fig. 28. For the fact that the plain text, viz, N G 3 T O 3 S 6, begins immediately after the "letter" 2, designating the generatrix, means that the hypothetical phrase in Cycle -76 begins with WAR3DE ... etc. The fact that this generatrix is the 16th of the set-up means that in Cycle -75 the hypothetical phrase begins with the 16th letter, which is the W of WASHINGTON. In other words, the loci of the hypothetical phrase are as shown herewith:

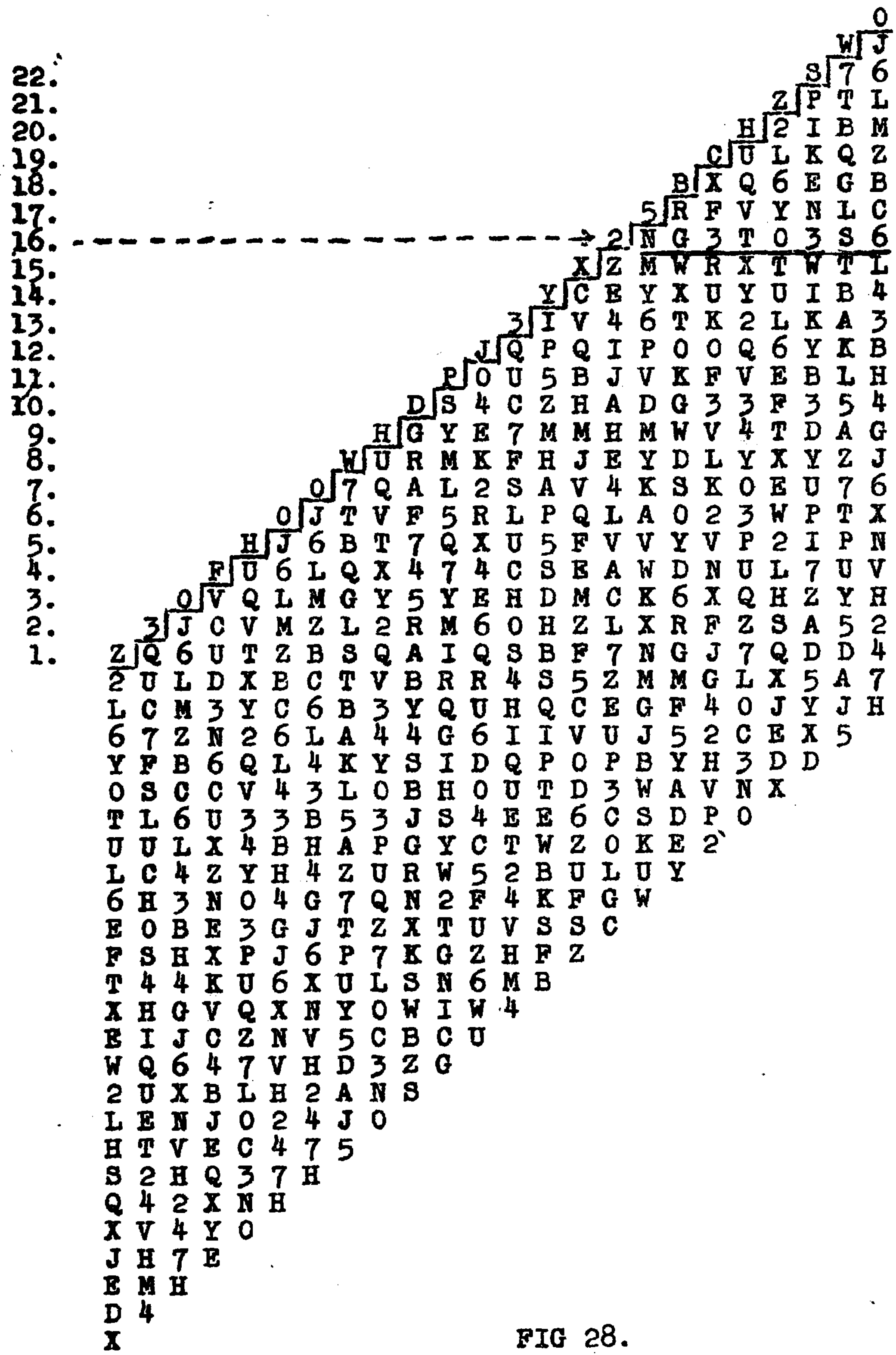


FIG 28.

NEW YORK 2	Upper key loci	186 196 206 216
CYCLE -74	Lower key loci	260 270 280 290
(CONFIRMATIVE)	Cipher	...6XTSQWQZKWCMCPWIDY3GD3A6JM3ZE6EKTD4FZRLR ...
	Plain text	...NG3TO3S6...

NORFOLK 10	Upper key loci*	186 196 206 216
CYCLE -75	Lower key loci	261 271 281 291
(EXPERIMENTAL)	Cipher	‖SXH7GMERHP3QSNI3MCZVCTRVOUOMVNUS4T64AAZY ...
	Plain text	...WASHINGTON...

HOBOKEN 20	Upper key loci	186 196 206 216
CYCLE -76	Lower key loci	262 272 282 292
(EXPERIMENTAL)	Cipher	‖3CTFJIXXLK3F4PKQ5LDYEQUGEPWGVOL34VVV ...
	Plain text	*...WAR3DEPARTMENT...

With this as a start, the keys can be reconstructed and the decipherment continued.

* * * * *

A variation of the foregoing method makes use of special sliding alphabets based upon the hypothetical phrase, the presence of which is suspected in both experimental cycles. These sliding alphabets are built exactly like those based upon the phrase WAR3DEPARTMENT2 WASHINGTON, except that instead of using the sequent letters of this phrase in constructing the alphabets, the mean values of the letters of the assumed plain text are used. The mean values of the phrase under discussion are as follows:

```
             W A R 3 D E P A R T M E N T 2 W A S H I N G T O N 3 D C
[illegible]  A R 3 D E P A R T M E N T 2 W A S H I N G T O N 3 D C 3
Mean values  T D C F 4 Q Y D G N X F M L Z T I Z L R P R 4 H 4 F U R
```

Sliding alphabets are now made by first constructing the square shown in Fig. 29 and then cutting the columns apart.

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

FIG. 29

Then by setting up the alphabets indicated by the letters of the base in staggered fashion as before, the successive first resultants will be found in successive generatrices. Note that the two generatrices used in the preceding discussion appear in the set-up in Fig. 30.

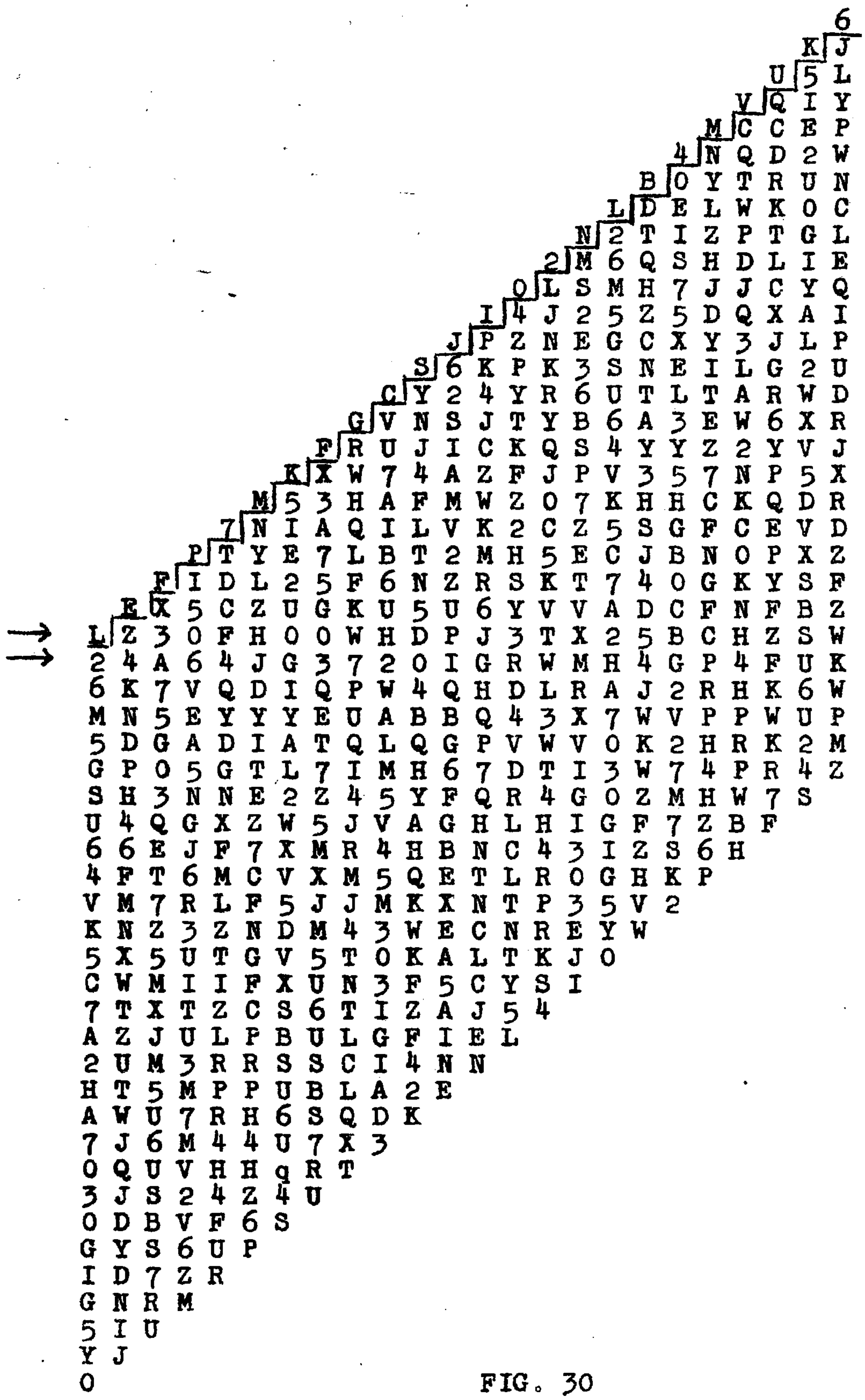


FIG. 30

In the preceding example the assumptions for the plain text involved the hypothetical presence of the same phrase in both experimental cycles. We shall now proceed to a consideration of the case where the assumed plain text is not the same for both experimental cycles. The procedure is basically the same as in the preceding case. The messages to be used for the demonstration are three actual messages of the series. The base has been derived in the usual manner, and to it is applied the assumed beginning, TRANSPORTATION3SERVICE, for Cycle -76, one of the experimental cycles, yielding the first resultant shown below:

Upper key loci	* 395	403
Lower key loci	469	477
N.Y. 3 (Cycle -75)	. . . . .	Z T D M 7 J X U P K K . . .
Upper key loci		403
Lower key loci		478
NOR. 10 (Cycle -75)	. . . .	D 4 G 7 Q Y M K 7 H 7 F . . .
Upper key loci		* 403
Lower key loci		479
HOB. 21 (Cycle -76)		G T X A Q X N N U F R T . . .
Assumed p.t.		T R A N S P O R T A T I O N . . .

	Z T D M 7 J X U P K K
	D 4 G 7 Q Y M K 7 H 7
	4 G 7 Q Y M K 7 H 7 F
	G T X A Q X N N U F R
Base	R L C 4 Y 5 2 3 S P 4
Assumed p.t. for Cycle -76	T R A N S P O R T A T
1st resultant	G O F 3 T D G C Y Y O

Since New York begins somewhat in advance of the locus where Hoboken 21 begins, and since it is probable that the former message is going to Washington, we assume that the phrase WAR3DEPARTMENT2 WASHINGTON3DC3 occurs somewhere in the vicinity of loci 395 to 425 of the upper key.

The special alphabets based upon the phrase WAR3 etc. are set up in the manner shown below in Fig. 31. Of course, no plain text can be visible as yet because the confirmative cycle in this case is the middle cycle, and we must apply the principles elucidated on pages 53-56.

The steps are the same for every generatrix of the set-up, and we will take only the correct generatrix for the demonstration of the method. The correct generatrix is, of course, found only by trial. The method in brief is as follows:

Taking the correct generatrix, which is as follows:

O J C E 3 K P H S F H

and going through the usual steps, to determine the series of unknown means, we have:

p_1	p_2	p_3	p_4	p_5	p_6	p_7	p_8	p_9	p_{10}	p_{11}	p_{12}
O	J	C	E	3	K	P	H	S	F	H	
7	O	W	X	M	O	Q	E	Y	T	X	

Setting up this series of letters in the ordinary alphabets we have the following(FIG, 32):

```
                         O
                       Y J
                     Y I 6
                   C I P L
                 G X P 5 M
               D D F 5 Z Z
             T G B 3 Z M B
           3 A R T R M H C
         F Q W A V U H A 6
       O V U G F W K A P L
 1.  G J C C H 7 6 O P 5 4
 2.  D 6 U 7 B 4 N F 5 S 3
 3.  B L D F Z 5 B 3 S D B
 4.  T M 3 S I R T V D H H
 5.  V Z N L W A R L H B 4
 6.  W B 6 U G B I K B S G
 7.  6 C C C 7 Y 6 2 S Q J
 8.  N 6 U H N 4 P V Q I 6
 9.  B L X O Z S R N I P X
10.  T 4 Z S M B O X P T N
11.  R 3 N 4 7 J D F T E V
12.  I B E H L G B J E W H
13.  6 H X I A R 5 G W B 2
14.  P 4 K Q W N C 4 B K 4
15.  R G V U Y X M 2 K S 7
16.  O J C E 3 K P H S F H
     ---------------------
     D 6 4 T P S 7 V F B
     B X B 2 M W R P B
     5 N J 4 R B 2 2
     C V E V 7 Z P
     M H Q H 4 S
     P 2 X M M
     7 4 Y 4
     R 7 E
     2 H
     P
```

FIG. 31

```
     7 O W X M O G E Y T X D
     -----------------------
     A 6 T V 5 6 H 2 P W V R
---> B E R 3 S E C O N D 3 T <---
     C P X W L P B K 6 V W U
     D Z G H Y Z V 4 M B H 7
     E B L M X B P 7 H Z M 4
     F Y V T Z Y G N O X T 3
     G 2 D U I 2 F 6 K R U W
     H N U D 4 N A Y E 3 D X
     I V Y 6 G V Z U W P 6 K
     J W O P Q W M R V 6 P 2
     K Q M L W Q O C G 5 L I
     L R E K C R S W U 2 K 6
     M 3 K E 7 3 J X D N E Y
     N H 5 Z T H 6 F B M Z S
     O 7 J S 3 7 K B F 4 S Z
     P C S J R C E Q A I J 5
     O K 3 R J K 7 P 2 U R V
     R L B Q P L X J 5 G Q A
     S X P O B X L 3 T Y O N
     T 4 A F N 4 U Z S 7 F B
     U 5 H G 6 5 T I L Q G C
     V I F A 2 I D 5 J C A Q
     W J 7 C K J 3 L I A C G
     X S C 7 E S R M 4 F 7 H
     Y F I 4 D F 2 H 7 S 4 M
     Z D 2 N F D I T 3 E N O
     2 G Z 5 V G Y A Q L 5 J
     3 M Q B O M W S Z H B F
     4 T 6 Y H T 5 D X O Y E
     5 U N 2 A U 4 V R K 2 P
     6 A 4 I U A N G C J I L
     7 O W X M O Q E Y T X D
```

FIG. 32

The plain text BER3SECOND3T stands out very prominently. Counting down the first alphabet of the set-up shown in Fig. 31, we find that it is the 16th letter of our phrase WAR3DEPARTMENT2 WASHINGTON, which begins the hypothetical phrase in Cycle -74, i.e., the word WASHINGTON occurs in New York 3, beginning with locus 405. With the section BER3SECOND3T as a start, it is not difficult to add to the plain texts of all three cycles. The keys can be reconstructed simultaneously with the building of the plain texts. The proper placements of the initial texts are shown herewith:

```
Upper key loci          395   403
Lower key loci          469   477
N.Y. 3 (Cycle -74)      . . . . Z T D M 7 J X U P K K . . .
Plain text              . . . . 2 W A S H I N G T O N . . .

Upper key loci                  403
Lower key loci                  478
NOR. 10 (Cycle -75)     . . . D 4 G 7 Q Y M K 7 H 7 F . . .
Plain text              . . . B E R 3 S E C O N D 3 T . . .

Upper key loci                  403
Lower key loci                  479
HOB. 21 (Cycle -76)             G T X A Q X N N U F R T . . .
Plain text                      T R A N S P O R T A T I O N .
```

* * * * *

Upon proper occasion it may be desirable to slide two different phrases against one another. For example, WASHINGTON against NEW3YORK. The methods discussed in the two preceding cases have been elucidated sufficiently, it is believed to show that such a process would be perfectly practicable. Special sliding alphabets would be prepared and kept on file for use when the occasion arose.

By means of this process, it is possible to test all sorts of phrases, such as names of persons or places likely to occur in addresses or signatures. Given a sufficient number of messages favorable to the application of such a test, the process becomes a very valuable adjunct to other methods of attack.

4. SOLUTION OF CASES NOT INVOLVING THREE SEQUENT CYCLES

The possession of three cycles in unbroken sequence is no longer absolutely essential to solution. We shall discuss the following four cases likely to arise in practice.

A. The two experimental cycles sequent, the confirmative cycle at a short distance removed from either of the experimental cycles.

B. The experimental and confirmative cycles equidistant.

C. The distance between the confirmative cycle and the nearer experimental cycle is a multiple of the distance between the two experimental cycles.

D. Cycles at irregular intervals from one another.

The four cases will be studied in succession.

A. (Case 1)--The two experimental cycles sequent, the confirmative cycle at a short distance removed from either of the experimental cycles.

The solution of this case is dependent upon two factors; first, how far removed the confirmative cycle is from the two experimental cycles; and second, the length of the assumed text. Let us study three actual messages.

Messages

Upper key loci	186	196	206	
Lower key loci	261	271	281	
NOR. 10 (Cycle -75)	SXH7GMERHP3QSNI3MCZVCTRVO ...			Experimental
Upper key loci	186	196	206	
Lower key loci	262	272	282	
HOB. 20 (Cycle -76)	3CTFJIXXLK3F4PKQ5LDYE ...			Experimental
Upper key loci	186	196	206	
Lower key loci	272	282	292	
WASH. 25 (Cycle -86)	...KCF7TRQJU3NRMOZJ6SXXQ ...			Confirmative

In this case we have Norfolk 10 beginning in Cycle -75; Hoboken 20, beginning in Cycle -76; and Washington 25, in Cycle -86, or ten cycles removed from Hoboken 20; that is, the confirmative cycle is ten cycles removed from the nearer experimental cycle, instead of being directly sequent, as has been the case in all the examples discussed heretofore. It was desirable to obtain a method by means of which possible beginnings for Norfolk 10 and Hoboken 20 could be tested very rapidly on Washington 25, and the following method was devised.

Reconstruct the two keys without reference to any plain text whatever, using the series of cipher letters only in Cycles -75 and -76 for the first 15 letters, beginning with 7 as a base in loci 186 * 262, Cycle -76. Thus:

Upper key loci	186	196	
Lower key loci	261	271	
Upper key (hypothetical)	OQFHDJEBUCC5BVK		
Lower key "	3PU75KPMJ4RAQKZ		
Norfolk 10 (Cycle -75)	SXH7GMERHP3QSNI3MCZV...		Experimental
Upper key loci	186	196	
Lower key loci	262	292	
Upper key (hypothetical)	7OQFHDJEBUCC5BVK		
Lower key "	3PU75KPMJ4RAQKZO		
Hoboken 20 (Cycle -76)	3CTFJIXXLK3F4PKQ...		Experimental
Upper key loci	186	196	
Lower key loci	272	282	
Wash. 25 (Cycle -86)	...KCF7TRQJU3NRMO2J...		

For example, starting with 7 as the upper key letter of locus 186 in Cycle -76, the resultant of 7 and 3 is 3, which becomes the lower key letter of locus 262. This then becomes the lower key letter above M in Cycle -75. The resultant of 3 and M is O, upper key letter 187, which is now placed above C, the second letter in Cycle -76, etc. The process is exactly the same as that in reconstructing normal keys, except that no plain text is used as yet. Keys produced in this manner, we have termed IMPERFECT KEYS, because they are not completed, or made symmetrical by the plain text letters which apply, and will therefore not produce plain text when shifted. Normal keys, or keys which will produce plain text we have termed PERFECT KEYS.

Since Washington 25 is ten cycles removed from Hoboken 20, then the lower imperfect keys of the latter beginning with R A Q K Z (after the bar in the diagram) must be united with the upper imperfect keys of the beginning point of Hoboken 20, and these must be applied as shown below, to the cipher in Washington 25, beginning with K C F 7 . . . . The series of letters which are produced we term, as before, the BASE:

	Upper key loci	186
Washington 25	Lower key loci	272
(Cycle -86)	Upper imperfect keys	7 0 Q F H D . . .
	Lower imperfect keys	R A Q K Z 0 . . .
	Cipher	K C F 7 T R . . .
	Base	S Y F 2 Y 6

Now it is patent that if we had included the assumed plain text for Norfolk 10 and Hoboken 20 in constructing the keys, the base would have become the plain text for Washington 25; and had the assumed plain text been the correct plain text for those two cycles, then the base would have to be intelligible plain text. However, whether we include such assumed plain text in the first steps, working with perfect keys, or apply it after imperfect keys have yielded the base, the final result will be the same, providing we go through the correct steps.

It is also patent that although the assumed plain text consists of two distinct parts, one applying to Norfolk 10, the other to Hoboken 20, it is perfectly correct to test the effect of these two parts separately. That is, we may assume one phrase as the beginning of Hoboken 20 and try it in combination with all possible beginnings for Norfolk 10, exactly as was done in Section 3.

Now as far as the first few loci of Washington 25 are concerned, the assumption of plain text for Hoboken 20 will have two effects: first, upon loci 186 & 187 ... of the upper keys, and secondly, upon loci 272 & 273 ... of the lower keys. Let us analyze these effects in detail, assuming Hoboken 20 to begin with TRANSPORTATION3SERVICE.

Locus 186 of the upper key is unchanged, since we still retain 7 as the base for reconstruction of the keys. Locus 262 of the lower key is affected by the first letter of the assumed beginning, viz, T. It would result in producing a letter different than the one shown (3) for locus 262 of the lower key and this in turn would give a different letter in locus 187 of the upper key. Locus 263 of the lower key would be affected again by the second letter of the assumed plain text beginning for Hoboken 20, and this in turn would affect locus 188 of the upper key. In short, the effect is progressive and cumulative. This series of effects will be produced by the following series of letters:

```
T T T T T . . .
  R R R R . . .
    A A A . . .
      N N . . .
        S . . .
T G B Y T . . .
```

Such a series of summations has been termed the PROGRESSIVE VALUE of a phrase, and the integral sign placed before a series of letters will indicate that the progressive value of the series is to be taken. Thus, $\int$ TRANSPORTATION means that the progressive values, letter by letter, are to be taken.

This progressive value must be applied to the base, and since the first locus of the upper key to be affected by the plain text assumed is 187, we apply the progressive value as shown below:

Upper key loci	186	187	188	189	190	191
Lower key loci	272	273	274	275	276	277
Base	S	Y	F	2	Y	
Progressive value of assumed plain text for Cycle -76		T	G	B	Y	T
Sums	S	S	Q	6	7	J

We have so far found the effect of the assumption of plain text in Hoboken 20 only upon the upper key loci 186 to 190. Now we must find the effect upon the lower key loci from 272 to 276, for they, too, are involved in the process of finding the plain text for Washington 25.

The first lower key locus affected is 262, by the letter T of TRANSPORTATION. The next is locus 263, by the letter R, and so on. The effect is likewise progressive and cumulative. It will be as follows, in detail:

262	263	264	265	266	267	268	269	270	271	272	273	274	275	276	277
T	T	T	T	T	T	T	T	T	T	T	T	T	T	T	T
	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R
		A	A	A	A	A	A	A	A	A	A	A	A	A	A
			N	N	N	N	N	N	N	N	N	N	N	N	N
				S	S	S	S	S	S	S	S	S	S	S	S
					P	P	P	P	P	P	P	P	P	P	P
						O	O	O	O	O	O	O	O	O	O
							R	R	R	R	R	R	R	R	R
								T	T	T	T	T	T	T	T
									A	A	A	A	A	A	A
										T	T	T	T	T	T
											I	I	I	I	I
												O	O	O	O
													N	N	N
														3	3
															S
T	G	B	Y	T	I	V	H	3	U	Q	Z	D	S	E	3

Since the first lower key locus involved in Washington 25 is 272, we begin with the letter Q of the progressive value, and apply the series to the base already corrected as regards upper keys. Thus:

Upper key loci	186
Lower key loci	272
Base, corrected for imperfect upper key	S S Q 6 7 J . . .
Correction for imperfect lower key	Q Z D S E 3 . . .
First resultant	L H V V F K . . .

This series of letters, corrected for upper and lower key letters as affected by the plain text assumed for Hoboken 20, we term, as before, the FIRST RESULTANT.

The steps illustrated above are summarized below in standard form:

Upper key loci	..	186	187	188	189	190	191	192	193	194	195	196	197	198	199	200
Lower key loci	..	262	263	264	265	266	267	268	269	270	271	272	273	274	275	276

Progressive value:

```
T R A N S P O R T A T I O N 3 S
T G B Y T I V H 3 U Q Z D S E 3
```

Upper key loci	186	187	188	189	190	191	. . .
Lower key loci	272	273	274	275	276	277	. . .
Base	S	Y	F	2	Y	6	. . .
Correction for imperfect upper key		T	G	B	Y	T	. . .
Correction for imperfect lower key	Q	Z	D	S	E	3	. . .
First resultant	L	H	V	V	E	K	. . .

We are now ready to assume beginnings for Norfolk 10. We may omit the incorrect trials and proceed at once with the correct phrase, ADJUTANT3GENERAL3ARMY. The steps are practically the same as above. The progressive values are sought, beginning with the second A of ADJUTANT, since it falls under upper key locus 187, and is therefore the first letter which enters into calculation.

```
                 A D J U T A N T 3 G E N E R A L 3 A R M Y . . .
Progressive value          A K 5 6 E 7 N F U 3 P L Z 6 U L . . .
```

Upper key loci	186	187	188	189	190	191	. . .
Lower key loci	272	273	274	275	276	277	. . .
Second resultant	L	H	V	V	E	K	. . .
Correction for imperfect upper key		A	K	5	6	E	. . .
Correction for imperfect lower key	3	P	L	Z	6	U	. . .
Plain text	P	E	A	T	E	D	. . .

Having found intelligible plain text for Washington 25, perfect keys are constructed in the normal manner and the decipherment continued.

The process described above has been carried out in full detail to demonstrate its mechanics. It may be summarized below:

Upper key loci	186
Lower key loci	272
Base	S Y F 2 Y 6
Correction for assumed plain text of Cycle -76	T G B Y T Q Z D S E 3
First resultant	L H V V E K
Correction for assumed plain text of Cycle -75	A K 5 6 E 3 P L Z 6 U
Plain text for Cycle -86	P E A T E D

(TRANSPORTATION3S...)
(TGBYTIVH3UQZDSE3...)

(ADJUT/ANT3GENERAL3ARMY)
AK56E7NFU3PLZ6UL)

This process takes longer to describe than to perform, naturally, and compared with the time it would take to try out all possible combinations of beginnings by constructing perfect keys in each case, it is several hundred times more rapid. The progressive values for all possible beginnings, once having been determined, can be kept on file so that with all the data at hand the process is extremely rapid.

B. (Case 2)--Experimental and confirmative cycles equidistant.

Given three cycles which are equidistant, with two of them beginning near the same locus, a solution is possible, provided that the assumed text contains three or four more letters than the distance between the cycles.

<u>Example</u>

Message 1 - Key indicators 300 * 309 (Cycle -9)

X B C P R A Q 4 O K P 6 N O X V Z A K D N X Z . . .

Message 2 - Key indicators 303 * 316 (Cycle -13)

W L L O 2 A K D Y R J 2 W S P O U 4 H J O Q . . . .

Message 3 - Key indicators 100 * 117 (Cycle -17)

The section beginning with 303 * 320 is as follows:

. . . G D A C I W S U U U P 2 T Y 5 K C 6 . . .

These messages are arranged as follows:

```
                       300  303                 313
                       309  312                 322
Message 1 (Cycle -9)    X B C P R A Q 4 O K P 6 N O X V Z A K D N X Z . . .

                            303                 313
                            316                 326
Message 2 (Cycle -13)         W L L O 2 A K D Y R J 2 W S P O U 4 H J . . .

                            303                 313
                            320                 330
Message 3 (Cycle -17)   . . . G D A C I W S U U U P 2 T Y 5 K C 6 6 0 . . .
```

We must first prepare these cipher letters properly so as to be able to make trials quickly. The reconstruction of the two imperfect keys is first carried out. Inasmuch as the steps are somewhat different from the ordinary ones in constructing keys from sequent cycles, we will show them somewhat in detail.

```
                    303
                    312
Cycle -9        X B C P R A Q 4 O K P 6 N O X V Z A K D N X Z . . .

                    303
                    316
Cycle -13             W L L O 2 A K D Y R J 2 W S P O U 4 H J . . .

                    303
                    320
Cycle -17       . . . G D A C I W S U U U P 2 T Y 5 K C 6 6 6 . . .
```

These cycles are four apart. Let us divide up the three lines into sections of four letters, beginning with the letters falling beneath upper key 303. Thus:

```
                      303     |307     |311     |315     |319     |
                      312     |316     |320     |324     |328     |
Cycle -9    X B C P R A Q|4 O K F|6 N O X|V Z A K|D N X Z|. . .
                      303     |307     |311     |315     |319     |
                      316     |320     |324     |328     |332     |
Cycle -13         W L L O|2 A K D|Y R J 2|W S P O|U 4 H J|. . .
                      303     |307     |311     |315     |319     |
                      320     |324     |328     |332     |336     |
Cycle -17       . G D A C|I W S U|U U P 2|T Y 5 K|C 6 6 0|. . .
```

Since these cycles are four apart, then the construction of the two keys from Cycles -9 and -13 must be carried out in intervals or <u>periods of four</u>. That is, if we assume the upper key for the first of Cycle -13 to be 7, then the lower key would be W. This letter W, the 316th letter of the lower key must then be placed above the letter 4 in Cycle -9, that is in the locus designated as {307/316} in Cycle -9. The resultant of W and 4, viz, 6, is then 307th upper key letter. Applying 6 to locus {307/320} in Cycle -13, we get B for the 320th letter in the lower key. This letter applied to the locus {311/320} in Cycle -9 gives 2 as the 311th upper key letter, etc. The result is as follows:

```
                  |303      |307      |311      |315      |319      |
                  |312      |316      |320      |324      |328      |
                  |         |6        |2        |D        |W        |
                  |         |W        |B        |Q        |G        |
Cycle -9    X B C |P R A Q  |4 O K F  |6 N O X  |V Z A K  |D N X Z  |. . .
                  |303      |307      |311      |315      |319      |
                  |316      |320      |324      |328      |332      |
                  |7        |6        |2        |D        |W        |
                  |W        |B        |Q        |G        |H        |
Cycle -13         |W L L O  |2 A K D  |Y R J 2  |W S P O  |U 4 H J  |. . .
                  |303      |307      |311      |315      |319      |
                  |320      |324      |328      |332      |336      |
Cycle -17   . . . |G D A C  |I W S U  |U U P 2  |T Y 5 K  |C 6 6 0  |. . .
```

We have been dealing so far with the first position letters in these sections of four letters, or as we shall term them the <u>first elements of the periods</u>. Let us now take up the second, third, and fourth elements of the periods, beginning, as before, with 7 as a base, that is, as the upper key letter in loci {304/317}, {305/318}, and {306/319} in Cycle -13. Each set or series of letters is entirely independent of any other set, and that is why it is absolutely immaterial with what letter as a base each series is begun: the ultimate result, viz, the interaction of certain letters in Cycle -17 will be the same regardless of the initial letter in each set of elements. The four reconstructed, and independent series are as shown below, and the manner in which they interact in the third message is also indicated. The result of applying the keys to the cipher letters is marked BASE. Of course, no plain text appears as yet.

```
          ⎧ Upper key loci     303     307     311     315     319
          ⎪ Lower key loci     312     316     320     324     328
Cycle -9  ⎨
          ⎪ Upper key loci                6 R X C 2 S R G D V 2 Q W Q D V . .
          ⎪ Lower key loci                W L L O B D L U Q K E O G 6 H K . .
          ⎩ Cipher          X B C P R A Q 4 O K P 6 N O X V Z A K D N X Z . .

          ⎧ Upper key loci     303     307     311     315     319
          ⎪ Lower key loci     316     320     324     328     332
Cycle -13 ⎨
          ⎪ Upper key loci     7 7 7 7 6 R X C 2 S R G D V 2 Q W Q D V . .
          ⎪ Lower key loci     W L L O B D L U Q K E O G 6 H K H 5 X Y . .
          ⎩ Cipher             W L L O 2 A K D Y R J 2 W S P O U 4 H J . .

          ⎧ Upper key loci     303     307     311     315     319
          ⎪ Lower key loci     320     324     328     332     336
Cycle -17 ⎨
          ⎪ Upper key loci     7 7 7 7 6 R X C 2 S R G D V 2 Q W Q D V . .
          ⎪ Lower key loci     B D L U Q K E O G 6 H K H 5 X Y
          ⎩ Cipher             G D A C I W S U U U P 2 T Y 5 K C 6 6 O . .
            BASE               A 7 Z D|R P B Z|5 B 4 Q|F H 7 F|
                                 (1)     (2)     (3)     (4)
```

We are ready now to try out various beginnings. As before, we will assume one beginning, keeping it constant, and trying all other beginnings with it. Let us assume Cycle -13 begins with ADJUTANT3 GENERAL, and proceed to apply corrections for imperfect keys for Cycle -13 first. The upper keys for the first period of Cycle -17 are unaffected by the plain text assumed. The lower keys are affected by the letters ADJUTANT. In the preceding section we corrected the keys by adding the progressive value of the plain text, and this value was determined by adding the letters of the plain text in their direct sequence. But in this case, since the four elements of the periods are independent, we cannot apply merely the progressive value but must apply what shall be termed the PERIODIC PROGRESSIVE VALUE, found by adding in progressive manner every <u>n</u>th letter of the assumed plain text, <u>n</u> being the period. Or, put in the form of an expression, the sign $\int/4$ is understood to indicate that the progressive value of every fourth letter of the series is to be taken. For the first period of Cycle -17 the correction for imperfect lower keys will therefore be the following:

```
              1st period
      ⎧       A D J U
 ∫/4  ⎨       T A N T
      ⎩       W R U Q
```

This correction applied to the first period of the base gives the following:

	1st period	2nd period	3rd period
Base	A 7 Z D	R P B Z	5 B 4 Q
Correction for imperfect upper key	- - - -		
Correction for imperfect lower key }	W R U Q		
First resultant	T R P V		

The corrections for imperfect upper and lower keys for the second and third periods are as follows:

2nd period		3rd period	
Upper key	Lower key	Upper key	Lower key
A D J U	∫4 A D J U T A N T 3 G E N Q T I 6	∫4 A D J U T A N T W R U Q	∫4 A D J U T A N T 3 G E N E R A L P G S D

These corrections are applied to the respective periods as follows:

	1st period	2nd period	3rd period
Base	A 7 Z D	R P B Z	5 B 4 Q
Correction for imperfect upper key	– – – –	A D J U	W R U Q
Correction for imperfect lower key	W R U Q	Q T I 6	P G S D
First resultant	T R P V	V K H F	G D R D

Having determined the first resultant we are now ready to test all possible beginnings for Cycle -9. Let us proceed at once to the correct one, viz, COMMANDING3GENERAL. The periodic progressive corrections are found as before, beginning with the letter I of COMMANDING since it is the first one to enter into the calculations, that is ∫/4 ING3GENERAL is to be taken.

1st period		2nd period		3rd period	
Upper key	Lower key	Upper key	Lower key	Upper key	Lower key
No correction necessary	I N G 3	I N G 3	∫4 I N G 3 G E N E M F P S	∫4 I N G 3 G E N E M F P S	∫4 I N G 3 G E N E R A L 6 P C 3 V

These corrections are applied to the second resultant and yield intelligible plain text. Thus:

	1st period	2nd period	3rd period
First resultant	T R P V	V K H F	G D R D
Correction for imperfect upper key	– – – –	I N G 3	M F P S
Correction for imperfect lower key	I N G 3	M F P S	P C 3 V
Plain text	- P I N G	3 C O N	T R O L

All these steps may be simplified and summarized as shown below. It was necessary to go through all the steps above in order to show the mechanics of the process in detail. But if these steps be analyzed carefully, it will become apparent that certain repetitions of plain text periods cancel out, being duplicates, so that the final result is achieved just as well by going through only the following steps:

	1st period	2nd period	3rd period
Base	A 7 Z D	R P B Z	5 B 4 Q
Correction for plain text of Cycle -13	A D J U T A N T	T A N T 3 G E N	3 G E N E R A L
First resultant	T R P V	V K H F	G D R D
Correction for plain text of Cycle -9	I N G 3	G E N E	R A L 6
Plain text for Cycle -17	P I N G	3 C O N	T R O L

No further comment is necessary in regard to the rapidity of the process. Once intelligible text is found, new keys are constructed employing the deciphered plain text and taking into account the fact that the periods consist of four independent elements. The reconstructed keys will not be perfect keys, but they will operate in every case where the cycle involved is four or a multiple of four intervals away from any of the cycles which entered into their reconstruction.

C. (Case 3)--The distance between the confirmative cycle and the nearer experimental cycle is a multiple of the distance between the two experimental cycles.

In the case just discussed, the cycles were equidistant. The process can be applied likewise to those cases in which the distance between the confirmative and the nearer experimental cycle is a multiple of that between the two experimental cycles. The practical application of the method is dependent upon the same two factors as before, viz, the distance between the cycles, and the length of the plain text assumed. An example taken from the series of test messages will serve our purposes. The messages have been arranged for decipherment:

Messages

```
Upper key loci                         014
Lower key loci                         623
N.Y. 20 (Cycle -609)                ...VQVY43VG36...   Confirmative

Upper key loci              *  002     014
Lower key loci                 623     635
HOB. 32 (Cycle -621)        NT4SJOVVCK73RSOFEY2HI07VPB...  Experimental

Upper key loci              *  002     014
Lower key loci                 626     638
WASH. 13 (Cycle -624)         VCCSGUPWMUDY2NR02GHPIB...  Experimental
```

Hoboken 32, and Washington 13, the experimental cycles, are three cycles apart; while New York 20, the confirmative cycle, and Hoboken 32, the nearer experimental cycle, are twelve cycles apart; in other words, the distance between the first and second cycles is the fourth multiple of that between the second and third.

Let us reconstruct imperfect keys employing the principles of periodicity just elucidated. The period, being the distance between the experimental cycles, is three. The keys, using X, Y, and Z as bases, are as follows:

N.Y. 20 Cycle -609	Upper key loci		014
	Lower key loci		623
	Cipher		...VQVY43VG36

HOB. 32 Cycle -621	Upper key loci	002	014
	Lower key loci	* 623	635
	Upper key loci	XYZXYTOJXJ7NFM66PDARS	
	Lower key loci	PFKA650KQCOENDBKTZAHW	
	Cipher	NT4SJOVVCK73RSOFEY2HIO7VPB	

WASH. 13 Cycle -624	Upper key loci	002	014
	Lower key loci	626	638
	Upper key loci	XYZXYTOJXJ7NFM66PD	
	Lower key loci	A650KQCOENDBKTZAHW	
	Cipher	VCCSGUPWMUDY2NRO2GHPIB	

Applying to New York 20 upper keys 014 ... and lower keys 623 ... we have the following:

N. Y. 20 Cycle -609	Upper key loci	014	020
	Lower key loci	623	629
	Upper key loci	F M 6 6 P D A R S . . .	
	Lower key loci	P F K A 6 5 0 K Q . . .	
	Cipher	V Q V Y 4 3 V G 3 . . .	
	Base	S I R F S L S 5 P . . .	

Let us assume for the plain text of Hoboken 32, SURGEON3GENERAL6 N52WASHINGTON, and determine the first resultant. We must begin with the E of SURGEON, since that is the first letter which enters into relations.

New York 20

1st period Upper key	1st period Lower key	2nd period Upper key	2nd period Lower key	3rd period Upper key	3rd period Lower key
3 G E	E O N	3 G E	No correction necessary	3 G E	3 G E
N E R		N E R		N E R	
A L 6		A L 6		A L 6	
N 5 2		N 5 2		N 5 2	
U P L		W A 5		W A 5	
		H Y F		5 5 S	
				J R 4	

	1st period	2nd period	3rd period
Base	S I R	P S L	S 5 P
Correction for imperfect upper key	U P L	H Y F	U R 4
Correction for imperfect lower key	E O N	- - -	3 G E
First resultant	A 4 H	B T 5	R K 5

Let us now try as the assumed plain text of Washington 13 the correct beginning, DEPARTMENT3AIR3SERVICE.

New York 20

1st period Upper key	1st period Lower key	2nd period Upper key	2nd period Lower key	3rd period Upper key	3rd period Lower key
D E P	No correction necessary	D E P	D E P	D E P	D E P
A R T		A R T		A R T	A R T
M E N		M E N		M E N	R J I
T 3 A		T 3 A		T 3 A	
I C D		I R 3		I R 3	
		7 3 F		S E R	
				S S U	

	1st period	2nd period	3rd period
First resultant	A 4 H	B T 5	R K 5
Correction for imperfect upper key	I C D	7 3 F	S S U
Correction for imperfect lower key	- - -	D E P	R J I
Plain text	S I X	T Y 3	S E V

The appearance of the words SIXTY3SEV ... gives the beginning of excellent plain text. The keys are reconstructed and the decipherment continued.

The short-cut, eliminating all details, for this process is summarized below. The plain text letters are the summations of the letters in the columns.

New York 20

	1st period	2nd period	3rd period
Base	S I R	F S L	S 5 P
Assumed plain text for Hoboken 32	E O N	3 G E	N E R
	3 G E	N E R	A L 6
	N E R	A L 6	N 5 2
	A L 6	N 5 2	W A 5
	N 5 2	W A 5	5 5 S
Assumed plain text for Washington 13	D E P	A R T	M E N
	A R T	M E N	T 3 A
	M E N	T 3 A	I R 3
	T 3 A	I R 3	S E R
Plain text for New York 20	S I X	T Y 3	S E V

D. (Case 4)--The three cycles at irregular intervals.

We have been leading up, step by step, to the solution of the most important case of all, viz, that in which no sequent cycles, or cycles at any regular distances apart are available. This case is, of course, the most valuable from the practical standpoint, and warrants restatement. It means that given two messages separated by 2, 3, 4, ... up to say 15 cycles, plain text may be assumed and tested upon any other cycle that may be available, providing only that the keys applying to this third cycle fall within the sections of assumed plain text.

Let us study an actual example taken from the series of test messages. We shall choose as the experimental cycles Hoboken 32 and Washington 13, which are three cycles apart. For the confirmative cycle we shall take Washington 39. In the diagram below the messages have been arranged for decipherment; imperfect keys have been constructed and applied to Washington 39.

```
     Hoboken 32
     Cycle -621
Upper key loci        785      002                        012                               022
Lower key loci        619      623                        633                               004
Imperfect upper key           |X Y Z|X Y T|O J X|J 7 N|F M 6|6 P D|A R S|C T
Imperfect lower key           |P F K|A 6 5|O K Q|C O E|N D B|K T Z|A H W|Q M
Cipher              ||N T 4 S|J O V|V C K|7 3 R|S O F|E Y 2|H I O|7 V P|B N

    Washington 13
     Cycle -621
Upper key loci                 002                        012                               022
Lower key loci                 626                        636                               007
Imperfect upper key           |X Y Z|X Y T|O J X|J 7 N|F M 6|6 P D|A R S|C T
Imperfect lower key           |A 6 5|O K Q|C O E|N D B|K T Z|A H W|Q M A|Q Z
Cipher                       ||V C C|S G U|P W M|U D Y|2 N R|O 2 G|H P I|B E

    Washington 39 ((Conf.)
     Cycle -631
Upper key loci                 002                        012                               022
Lower key loci                 633                        004                               014
Imperfect upper key           |X Y Z|X Y T|O J X|J 7 N|F M 6|6 P D|A R S|C T
Imperfect lower key           |O E N|D B K|T Z A|H W Q|M A Q|Z
Cipher                     ...|U D L|6 5 K|D X R|A G 7|F L 6|A H P|4 5 T|7 .

Base                          |2 X K|K W T|E U H|M D 6|M F Q|     |     |
```

Before we can proceed, it will be necessary to introduce into the discussion a feature which presents itself here for the first time.

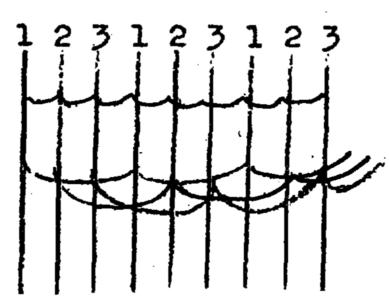
The distance between the two experimental cycles determines the period and the periodic length is simply the sum of the number of its constituent elements. As regards the upper key, the periods, and therefore all their constituent elements, for all cycles, coincide, since all of our analysis is based upon the fiction of a stationary longer (= upper) key. But as regards the lower key, which in our analysis is regarded as the moving key, any period in one experimental cycle has a homologous period in the other experimental cycle, both periods being composed naturally of the same elements and in the same order. In other words, the first, second, third ... elements of a given period of one experimental cycle coincide with the first, second, third ... elements of a homologous period of the other experimental cycle. The case is somewhat analogous to that in wave motion, when two waves of similar period reach their maximum magnitude simultaneously, the two waves being in a condition termed as "in phase."

Now, in the case of three equidistant cycles, the lower key periods of the confirmative cycle are in phase with those of the experimental cycles. The same is true of the case where the distance between the confirmative cycle and the nearer experimental cycle is a multiple of the distance between the two experimental cycles. But in the case which conforms to neither of these cases, that is, where the distance between the confirmative cycle and the nearer experimental cycle is neither equal to nor a multiple of the distance between the two experimental cycles, the lower key periods of the confirmative cycle are not in phase with those of the experimental cycles. The condition, to continue the analogy with wave motion, exhibits a "difference in phase"; and in this case, with a period of three, the difference is either 1/3 or 2/3 of a period. That is, the periods of the confirmative cycle are either advanced or retarded 1/3 or 2/3 of a period. When this is the case, the application of imperfect keys derived from the two experimental cycles will not result in the production of intelligible text in the confirmative cycle unless a correction for the difference in phase is applied. The reason for this phenomenon is obvious when one considers the origin of imperfect keys as contrasted with that of perfect keys. In reconstructed perfect keys, adjacent letters of both the upper and the lower key bear a definite relation to one another--they are the individual successive links of a continuous single chain which has been made, link by link, from the plain text-cipher text relations. But imperfect keys that have been constructed from experimental cycles not directly sequent consist of several independent chains which "dovetail" in such a manner as to produce intelligible text only where the periods of the confirmative cycle are in phase with those of the experimental cycle. These chains are independent because they are generated by independent, unrelated base letters.

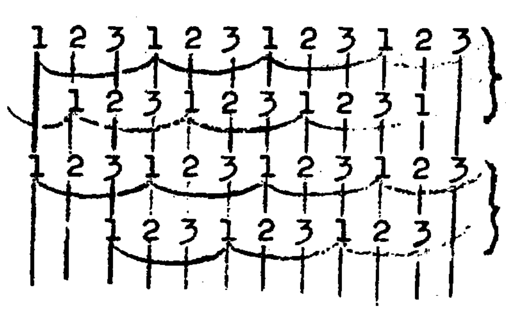
The difference between keys of these two types is comparable to that between a single phase and a polyphase alternating current of electricity, and we have termed a key of the first type a MONOPHASE KEY, and one of the second type a POLYPHASE KEY. The difference between them may be shown diagrammatically in the following sketch:

Monophase

Polyphase



Difference in phase in a polyphase key may be shown likewise in diagrammatic manner:



1/3 phase difference (120°)

2/3 phase difference (240°)

If, after a polyphase key has been constructed, we can establish a relationship between the letters or elements of its period (= the phases of the period), then the independent chains of the polyphase key may be merged and converted into one continuous chain which will then constitute a perfect monophase key.

Let us proceed now to decipher the messages. For the beginning of Hoboken 32, one experimental cycle, we will assume SURGEON3 GENERAL6N52WASHINGTON. The corrections to be applied are shown below. The upper keys being constant, its periods are in phase throughout all cycles. The lower key periods of Washington 39 are out of phase with those of the experimental cycles, being retarded 1/3 of a period. The elements of the periods of Washington 39 are in the order 2-3-1, instead of 1-2-3 because the first elements of the periods of Washington 39 are the second elements of those of the experimental cycles. For this reason the correction to be applied to Washington 39 takes the following form:

Washington 39

1st period		2nd period		3rd period	
Upper key	Lower key	Upper key	Lower key	Upper key	Lower key
No correction necessary	2-3-1	1-2-3	2-3-1	1-2-3	2-3-1
	. . 3	3 G E	. . 3	3 G E	. . 3
	G E N		G E N	N E R	G E N
	E R A		E R A	4 6 J	E R A
	6 J J		L 6 N		L 6 N
			D T U		5 2 W
					P L H

4th period		5th period	
Upper key	Lower key	Upper key	Lower key
1-2-3	2-3-1	1-2-3	2-3-1
3 G E	. . 3	3 G E	. . 3
N E R	G E N	N E R	G E N
A L 6	E R A	A L 6	E R A
J D T	L 6 N	N 5 2	L 6 N
	5 2 W	U P L	5 2 W
	A 5 5		A 5 5
	Y F J		5 S H
			R 4 5

	1st Per.	2nd Per.	3rd Per.	4th Per.	5th Per.
Base	2 X K	K W T	E U H	M D 6	M F Q
Correction for imp. upper key	- - -	3 G E	4 6 J	J D T	U P L
Correction for imp. lower key	6 J J	D T U	P L H	Y F J	R 4 5
1st resultant	B P 3	2 B P	5 C J	2 F 7	Z W G

Let us assume for the beginning of Washington 13 the phrase DEPARTMENT3AIR3SERVICE. The corrections are as follows:

1st period		2nd period		3rd period	
Upper key	Lower key	Upper key	Lower key	Upper key	Lower key
No correction necessary	2-1-3 . . D E P A R T M E N T R R I	1-2-3 D E P	2-1-3 . . D E P A R T M E N T 3 A I C D 7	1-2-3 D E P A R T R J I	2-1-3 . . D E P A R T M E N T 3 A I R 3 S 3 F S

4th period		5th period	
Upper key	Lower key	Upper key	Lower key
1-2-3 D E P A R T M E N P R R	2-1-3 . . D E P A R T M E N T 3 A I R 3 S E R V S U 6	1-2-3 D E P A R T M E N T 3 A I C D	2-1-3 . . D E P A R T M E N T 3 A I R 3 S E R V I C D A D G

Let us now apply these corrections to the first resultant:

	1st Per.	2nd Per.	3rd Per.	4th Per.	5th Per.
1st resultant	B P 3	2 B P	5 C J	2 F 7	Z W G
Correction for imp. upper key	- - -	D E P	R J I	P R R	I C D
Correction for imp. lower key	R R I	C D 7	3 F S	S U 6	A D G
2nd resultant	W M 2	S Z 7	Z 4 4	Z 7 Z	H H D

We are ready now to apply the correction for difference in phase. Our imperfect polyphase keys consist of three independent chains, generated by the initial letters X, Y, and Z. Let us designate by the letters k_1, k_2, and k_3 those letters in perfect monophase keys which occupy the positions of X, Y, and Z of our imperfect polyphase keys. Now k_2 and k_1 are related insofar as k_2 is derived from k_1 by means of the plain text-cipher relations which intervene; and k_3 is related to k_2 in the same manner. If we could convert X into k_1, Y into k_2 and Z into k_3, our imperfect polyphase keys could be converted into perfect monophase keys. Now X plus an unknown letter c_1 would equal k_1; Y plus an unknown letter c_2, would equal k_2; and Z plus an unknown letter c_3, would equal k_3. These three unknown letters c_1, c_2, and c_3, which would constitute the corrections for phase difference, would repeat themselves periodically throughout the imperfect keys. We can transfer these relations directly to the second resultant.

Second resultant - W M 2 S Z 7 Z 4 4 Z 7 Z H H D

W plus the unknown letter c_1 would give the correct plain text for that locus; M plus c_2 would give the correct plain text letter for the second locus; and 2 plus c_3 would give the correct plain text letter for the third locus. The cycle would repeat itself throughout the second resultant.

W
S
Z } + c_1 = correct plain text for 1st letters of periods
Z
H

M
Z
4 } + c_2 = correct plain text for 2nd letters of periods
7
H

2
7
4 } + c_3 = correct plain text for 3rd letters of periods
Z
D

The correction being constant for the three elements of the periods, we may set up the respective elements of these periods on the ordinary sliding alphabets, whereupon the correct plain text for each set of elements will appear on one generatrix which can be selected from all others by inspection, since it will be the one which contains the best assortment of high-frequency letters.

The correct generatrix will be different for each set of elements, of course, but by selecting the most likely generatrices, the corrected elements will now form intelligible plain text. Thus:

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

Note that in the set-up of the first elements the Y generatrix is composed entirely of high-frequency letters, I T 3 3 E. In the set-up of the second elements the T generatrix is composed of high-frequency letters, N E O T 3. Uniting the first and second elements in the third resultant we have the following:

	1	2	3	4	5
	1 2 3	1 2 3	1 2 3	1 2 3	1 2 3
Third resultant:	W M 2	S Z 7	Z 4 4	Z 7 Z	H H D
Plain text;	I N	T E	3 0	3 T	E 3

In the set-up of the third elements the 3 generatrix is composed entirely of high-frequency letters, but they do not combine well with the plain text found thus far. This generatrix when combined with the other two gives:

1	2	3	4	5
1 2 3	1 2 3	1 2 3	1 2 3	1 2 3
W M 2	S Z 7	Z 4 4	Z 7 Z	H H D
I N I	T E 3	3 0 N	3 T Y	E 3 F

The correct generatrix is the S generatrix. It gives the following:

1	2	3	4	5
1 2 3	1 2 3	1 2 3	1 2 3	1 2 3
W M 2	S Z 7	Z 4 4	Z 7 Z	H H D
I N U	T E S	3 0 F	3 T H	E 3 N

In all subsequent cycles the correction for the difference in phase is the period indicated by the generatrices determined above, viz, Y T S. In other words $c_1 = Y$; $c_2 = T$; $c_3 = S$.

For example, in Washington 68 the steps without going through the explanation above give the base shown below:

Hoboken 32
Cycle -621 Exp.

Upper key loci		002			012		019	022	
Lower key loci		623			633		001	004	
Imp. upper key		X Y Z	X Y T	O J X	J 7 N	F M 6	6 P D	A R S	C T
Imp. lower key		P F K	A 6 5	O K Q	C O E	N D B	K T Z	A H W	Q M
Cipher	N T 4 S	J O V	V C K	7 3 R	S O F	E Y 2	H I O	7 V P	B N

Washington 13
Cycle -624 Exp.

Upper key loci	002			012	016		022	
Lower key loci	626			636	001		007	
Imp. upper key	X Y Z	X Y T	O J X	J 7 N	F M 6	6 P D	A R S	C T
Imp. lower key	A 6 5	O K Q	C O E	N D B	K T Z	A H W	Q M A	Q Z
Cipher	V C C	S G U	P W M	U D Y	2 N R	O 2 G	H P I	B E

Washington 68
Cycle -638 Conf.

Upper key loci	002			012			022	
Lower key loci	001			011			021	
Imp. upper key	X Y Z	X Y T	O J X	J 7 N	F M 6	6 P D	A R S	C T
Imp. lower key	Z A H	W Q M	A Q Z					
Cipher	L M X	T 7 E	Y H O	5 U 4	S 4 F	2 6 Y	Z D T	R
Base	V R O	V 2 F	C 4 H					

Assuming for the beginnings of Hoboken 32 and Washington 13 the same addresses as before, viz, SURGEON3GENERAL6N52WA555SHINGTON and DEPARTMENT3AIR3SERVICE, respectively, we apply the proper corrections to the base derived above.

Since the first period of the lower key of Washington 68 is affected by the assumed plain text for the 2nd, 3rd, 4th, 5th, and 6th periods of Hoboken 32, and also by that for the 1st, 2nd, 3rd, 4th, and 5th periods of Washington 13, we must be guided accordingly in making the corrections for imperfect keys. Again, since the first element of the 1st period of Washington 68 is the third element of the 5th period of Washington 13, then the relative order of the elements of the periods of Washington 68 is 3-1-2, as compared with their order, 1-2-3, in Washington 13 and Hoboken 32, the experimental cycles. The order of the elements of the upper key is the same for all cycles. The corrections for the first three periods of Washington 68 take the following form:

Correction for assumed plain text for Hoboken 32, SURGEON/3 GENERAL6N52WA555SHINGTON =

For Upper Key

```
                    Period
         1                 2         3
   No correc-            1-2-3     1-2-3
   tion neces-           3 G E     N E R
   sary                  3 G E ->  3 G E
                                   4 6 J
```

For Lower Key

```
                                   Period
  2        3        4        5        6        7        8
3-1-2    3-1-2    3-1-2    3-1-2    3-1-2    3-1-2    3-1-2
. 3 G    E N E    R A L    6 N 5    2 W A    5 5 5    S H I
. 3 G -> . 3 G
         E 4 6 -> E 4 6
                  J J D -> J J D
                           T U P -> T U P
                                    L H Y -> L H Y
                                             F J R -> F J R
                                                      4 5 N
```

	Period 1	Period 2	Period 3
Base	V R O	V 2 F	C 4 H
Correction for imperfect upper key	- - -	3 G E	4 6 J
Correction for imperfect lower key	L H Y	F J R	4 5 N
First resultant	N V F	Q W I	C N W

Correction for assumed plain text for Washington 13, ∫/3DEPART MENT3AIR3SERVICE =

For Upper Key

```
                 Period
      1               2          3
No correc-          1-2-3      1-2-3
tion neces-         D E P      A R T
sary                D E P  ->  D E P
                               R J I
```

For Lower Key

```
                                   Period
  1       2        3        4        5        6        7        8
3-1-2   3-1-2    3-1-2    3-1-2    3-1-2    3-1-2    3-1-2    3-1-2
. D E   P A R    T M E    N T 3    A I R    3 S E    R V I    C E 3
. D E ->. D E
        P R J -> P R J
                 I P R -> I P R
                          R I C -> R I C
                                   D 7 3 -> D 7 3
                                            F S S -> F S S
                                                     U 6 A -> U 6 A
                                                              D G U
```

	Period 1	Period 2	Period 3
First resultant	N V P	Q W I	C N W
Correction for imperfect upper key	- - -	D E P	R J I
Correction for imperfect lower key	F S S	U 6 A	D G U
Second resultant	E 6 4	B D W	F X L

We are ready now to apply the correction for the difference in phase. We have found that $c_1 = Y$; $c_2 = T$; and $c_3 = S$. Since in this case the third element of a period of the experimental cycle becomes the first element of that of the confirmative cycle, then the correction to be applied becomes S Y T to correspond with the order 3-1-2 of the letters of the confirmative cycle periods.

Washington 68

	1st Period	2nd Period	3rd Period
Second resultant	E 6 4	B D W	F X L
Correction for phase difference	S Y T	S Y T	S Y T
Plain text	3 C O	M M A	4 4 2

It is desirable, of course, to construct perfect monophase keys, in order to eliminate the corrections for differences in phase in subsequent work. The method is as follows:

Take the first three letters upon which the reconstruction of the imperfect keys was based. In this case they are X Y Z.

Take any pair of equivalents for Y, the first letter of the corrective period, such as U L. Place these two equivalents beneath X Y Z and find the resultant. Thus:

```
Basic letters          X Y Z
Equivalents of Y       U L
Resultant              G U
```

Take the resultant of L (the second member of the pair of equivalents of Y) and T (the second letter of the corrective period), which is 2; add this letter to Z, the third basic letter. Thus:

```
X Y Z
U L 2
G U W
```

These three letters used as a base in connection with the correct plain text for the two experimental cycles will give two perfect monophase keys such as will apply to any cycles produced through their interaction, without the intervention of a correction for phase differences. The steps diagrammatically for the conversion of polyphase keys to monophase are as follows:

```
Corrective period            Y T S
Base for polyphase keys      U L 2
Base for monophase keys      X Y Z
                             G U W
```

Beginning with these letters as a base for the construction of perfect keys from the two experimental cycles we have the following:

```
                    002
                    623
                    G U W Q M S X D L
                    T U E F 4 J Z N L
Hoboken 32 || N T 4 S J O V V C K 7 3 R S O F E Y 2 H I O 7 V P B N
           || S U R G E O N 3 G E N E R A L 6 N 5 2 W A 5 5 5 S H I

             002
             626
             G U W Q M S X D L
             F 4 J Z N L Q 6 2
Washington 13 || V C C S G U P W M U D Y 2 N R O 2 G H P I B E
              || D E P A R T M E N T 3 A I R 3 S E R V I C E 3
```

Comparison of these keys with those given on pages , shows that they are identical with the monophase keys and will therefore apply to any message enciphered by their means.[1]

[1] I was unable to find, in my manuscript, where these monophase keys had been reconstructed. Evidently some page or pages must be missing and we will have to take it for granted that the statement made is correct.--W.F.F. ('48)

RÉSUMÉ

In the original brochure the basic principles for the analysis of this cipher were set forth. The analysis was based upon a careful study of the method of encipherment in which two key tapes differing in length by but one letter were used. In this method sequent revolutions of the key tapes produce what we have termed sequent cycles, the analysis of any three of which is sufficient for a complete solution to be achieved. It was also shown, first, how the slightest carelessness in the operation of the machine would produce messages enciphered by means of the same single key letters, and second, how such messages, termed overlaps, are particularly easy to solve.

In Addendum 1 it was shown how the same principles of solution apply to the system when the two key tapes differ in length by more than one letter. The dangers of using two keys whose lengths possess a factor in common were also demonstrated therein.

In Addendum 2 the correctness of the principles set forth, and the truth of the statements and claims made were demonstrated by the actual solution of the series of test messages submitted. The method of determining the lengths of the key tapes was elucidated. The mathematical relations existing between various lengths of key tapes and the resultant cycles were demonstrated, and the untrustworthiness of the adopted method of allotment of the key tapes indicated. The various types of solution were given, and their feasibility discussed. It was then shown how solution was no longer dependent upon the finding of three sequent cycles, a discovery which completed the demonstration of the vulnerability of the system.

William F. Friedman

ADDENDUM 3.

One of the prerequisites to the solution of this cipher being the knowledge of the key indicators for the various messages, there was submitted for our consideration a method of encoding and enciphering the indicators.

The result of investigation shows that (1) the method as submitted does not, to an appreciable degree, add to the safety of the system; (2) the possession of the code book is not essential to solution.

A list of encoded and enciphered key indicators for 80 messages was drawn up by one set of operators and submitted to another. Within ten minutes after certain tables had been made, the exact length of the two keys were determined; and within three hours the key indicators in the form of numbers for any message could be read at will. This list follows:

Message	Length	Indicators	Message	Length	Indicators
1	278	IDH - EJJ	41	392	AGJ - CAG
2	690	JEE - AID	42	156	HEC - BGE
3	81	FGC - IEJ	43	721	FGI - GAD
4	201	AFF - CBC	44	890	JHI - IFC
5	949	JCG - EEF	45	312	EAA - CFC
6	152	BDH - IDE	46	260	DBE - HBJ
7	275	JDJ - AJH	47	89	CHH - JAB
8	501	JDG - ABJ	48	121	AAE - DGC
9	370	GEJ - DEF	49	363	FJA - HHC
10	1108	FHE - JID	50	405	DJF - DEI
11	473	CIG - EAE	51	560	AIA - BDD
12	191	CIJ - EEJ	52	703	GGG - JJC
13	312	JEI - CII	53	1009	DDJ - BHA
14	297	FAD - CIH	54	804	AAJ - BDJ
15	451	CIJ - GIH	55	462	BIA - GIA
16	902	CFF - BCJ	56	791	FIC - HEC
17	79	JCE - HGJ	57	920	GGJ - IGD
18	210	CDE - JFJ	58	201	GCI - CJG
19	506	CGG - BFC	59	527	DCE - FDC
20	787	DCB - CGA	60	386	EJF - FFC
21	380	EJJ - DAJ	61	747	FCE - IIA
22	170	GEB - DJE	62	920	CIH - GFA
23	542	DID - GHF	63	1780	JHB - JJJ
24	1083	CEI - GFA	64	309	DHA - HJH
25	167	CEB - GHJ	65	187	HHH - GFC
26	392	GJE - HDI	66	99	EFB - DHF
27	468	JGH - IGI	67	209	ADG - BIG
28	554	DHC - EGH	68	867	FED - JBE
29	920	FFC - IHF	69	729	EFI - GGJ
30	387	FBE - DBG	70	372	CDC - EJF
31	542	HJH - GBB	71	221	FDF - HAF
32	659	CJB - DFF	72	183	FCD - CAG
33	365	FDA - EBE	73	149	JEE - BDB
34	1162	BBH - AIC	74	540	IAA - JAD
35	293	AED - GED	75	274	JED - AEA
36	180	BAA - EBE	76	963	JEI - LAJ
37	297	ACB - JCF	77	582	JGG - BAE
38	326	BEA - CDI	78	91	JHH - GJC
39	860	BJH - JIJ	79	355	HAG - ACE
40	471	GGI - GEG	80	79	CFD - JIA

The method of analyzing the encoded and enciphered indicators was as follows:

The system of encoding and enciphering the indicators is such that any key indicator which is repeated will have the same final form. For example, suppose one message has the key indicators 050 * 281. The plain code group for 050 is GJJ. Now, inasmuch as only 3 enciphering alphabets are used, one for each letter of the three code letters, whatever be the cipher equivalents for G^1, J^2, and J^3, both messages will show as the long key indicator the same combinations of letters, for example, using the tables given in the code book, FEC.

What has been said as regards the long key indicators applies likewise to the short key indicators.

Two sets of tables were therefore drawn up in the form of indexes of the letter indicators, one set applying to the long key indicators, the other set, to the short key indicators.

* * * * * * * * * * * * * * * *

Now note that in a series of only 80 messages there are several instances in which the letter indicators are identical as regards both the long key and the short key indexes. For example, the long key indicator for messages 12 and 15 are identical, CIJ.

Now there is only one circumstance under which two messages in the same series, that is, from the same station, can have the same long or the same short key indicator, and that is when the number of letters intervening between the two messages is equal to or is an exact multiple of the length of the long key or the short key respectively.

Refer to the series of test messages submitted and note the key indicators for Washington 42 and Washington 53. They are 020 * 160 and 020 * 261 respectively. Now the total number of letters from the beginning of Washington 42 to the beginning of Washington 53 is as follows:

WASHINGTON	42	275
	43	374
	44	206
	45	378
	46	421
	47	319
	48	359
	49	400
	50	326
	51	582
	52	273
Total		3913

Now there are eleven messages from Washington 42 to Washington 53. Since the slip is consistently 2, we must add 11 x 2 or 22 letters to the total. This gives 3935 as the grand total. The factors of this number are 5 x 787. The length of the long key is clearly 787. The correctness of this number can be corroborated from several more instances. In the same manner, taking the distance between messages 12 and 15 in this series we have the following:

Message	12	191
	13	312
	14	297
Total		800

Now it is clear that the length of the long key is at least 800 letters. We have yet to take into account the slip between messages. If we assume the slip to be 1, then the length of the long key would be 803; if 2, it would be 806; if 3, it would be 809, if 4, it would be 812, etc. Let us refer to another repetition viz., that between messages 42 and 81, indicator EEC. The total number of letters intervening is as follows:

Message			
	51 - 560	61 - 747	71 - 221
42 - 156	52 - 703	62 - 920	72 - 183
43 - 721	53 -1009	63 -1780	73 - 149
44 - 890	54 - 804	64 - 309	74 - 540
45 - 312	55 - 462	65 - 187	75 - 274
46 - 260	56 - 791	66 - 99	76 - 963
47 - 89	57 - 920	67 - 209	77 - 582
48 - 121	58 - 201	68 - 867	78 - 91
49 - 363	59 - 529	69 - 725	79 - 355
50 - 405	60 - 386	70 - 372	80 - 79
		Total - - - -	19332

Total no. of message = 39.

Since the long key is at least 800 letters in length, the number of revolutions it has made between messages 42 and 81 is 24 (19332 - 800). Trial of a slip of 1,2,3,4 letters is then made. If the slip be 1, then we must add 39 x 1 to 19332 and see if the total is exactly divisible by 803. If the slip be 2, then we must add 39 x 2, or 78 to 19332 and see if the total is exactly divisible by 806, etc. When we try a slip of 4, and add 39 x 4 = 156 to 19332 we have 19488. A slip of 4 would mean a key of 812 letters and calculation shows that 812 is the 24th multiple of 19488, and indicates 24 complete revolutions between messages 42 and 81.

The length of the short key was ascertained by exactly the same principles, except that the amount to be added for slip was not known. The length of the short key was found to be 693. Thus, messages 41 and 72 showed repetitions of the short key indicators, CAG. The calculations are as follows:

Message	41 - 392	51 - 560	61 - 747
	42 - 156	52 - 703	62 - 920
	43 - 721	53 -1009	63 -1780
	44 - 890	54 - 805	64 - 309
	45 - 312	55 - 462	65 - 187
	46 - 260	56 - 791	66 - 99
	47 - 89	57 - 920	67 - 209
	48 - 121	58 - 201	68 - 867
	49 - 363	59 - 529	69 - 725
	50 - 405	60 - 386	70 - 372
			71 - 221
		Total - -	16506
Total no. of messages 31.		Slip - - -	124
			16632

16632 ÷ 24 = 693 = length of short key.

As far as the solution of the messages is concerned we need have nothing more to do with the encoded and enciphered indicators, for we can proceed to find the indicators for the series of messages, assuming as the beginning points any pair of indicators we please, because solution is based upon the relative positions of cycles, not their absolute number. For example, the cycle number of any two cycles may be 72 and 75, or 133 and 136, or 2 and 5: the distance between the two cycles is the same, viz., 3. Another way of pointing out the relativity of the calculations is this: the two key tapes are continuous endless chains. It is therefore of no importance whether we call a given locus on one of the tapes 001 or 201, so long as we are consistent throughout in designating the other loci. Thus, the locus immediately following 001 would be called 002. If we designate locus 001 as 201, then the next one is 202, etc. We may start in therefore, to find the relative key indicators for our series of messages by basing the calculations upon the indicators 001 * 101 for message 1. These calculations are as follows:

Solution may now be achieved by exactly the same principles as those given in the preceding brochures. It is apparent, therefore, from a consideration of the preceding paragraphs that the possession of the code book is not essential to solution.

However, if we desire we can determine the absolute key indicators. The method is simple and is as follows:

From the relative calculations above, tables are made of the long key indicators and the short key indicators similar to those made at the beginning of the problem, with the letter indicators. This index is as follows:

* * * * * * * *

We look in these tables for an unbroken sequence of indicators in which the intervals between sucessive key indicator numbers are small. In the index for the short key indicators we have a sequence 488...491, 492...506, applying to messages 9, 15,55,36. Let us set down the short key letter indicators for these messages, and their relative positions. Thus:

Message 9 - DEF - 488
* * * * * * * *
15 - GIH - 491
55 - GIA - 492
* * * * * * * *
36 - EBE - 506

The only repetitions of letters in the letter indicators are the pair of letters G, and I. This means that in the code list of equivalents for indicator numbers there are two sequent numbers the first two letters of whose code equivalents are the same. There are many such cases in the code book, so we must find some further points of contact to enable us to pick out the correct pair. For example, we find that the short key indicator for message 11 is EAE, value 588. Let us add this to the table. Thus:

Message 9 - DEF - 488
* * * * * * * *
15 - GIH - 491
55 - GIA - 492
* * * * * * * *
36 - EBE - 506
* * * * * * * *
11 - EAE - 588

We have now two more points of contact. The absolute equivalents of the relative positions 506 and 588 must agree in the first and third letters, and they must be 82 intervals apart, since 588 - 506 = 82.

Search is made throughout the code book to find all the cases. Examine the following:

	Enc. Code	Relative position	Plain Code	Absolute Position
Message 9	DEF	488	GFJ	388
15	GIH	491	AGD	391
55	GIA	492	AGB	392
36	EBE	506	CDH	406
11	EAE	588	CBH	488

The agreement is good. By refering to other numbers as given by the index, if the letters of the encoded and enciphered indicators fit in with the set already drawn up, we may assume that we have struck the correct absolute positions of the indicators. For example, if, according to the above $C^1_p = E^1_c$; $F^2_p = E^2_c$, and $J^3_p = F^3_c$, then in message 5, short key indicator EEF = CFJ plain code = 574 absolute position. The interval between 488 and 574, absolute, must be the same as that between the relative equivalents. We find that 488 absolute = 588 relative and that the short key indicator for message 5 as calculated relatively is 674. The proof is complete.

Once a short section like the above is determined, the rest follows very easily.

To illustrate how careful the officer in charge must be, note the relative positions of the key tapes at the end of message 2, viz., 648--623. His next message contains approximately 70 words, he notes, and he figures that 350 letters will be enciphered, or, including functions, approximately 400 characters will be necessary for the message. He then finds that the addition of 400 characters to the point where message 2 left off will throw him "out of bounds." Thus:

```
 648 - 623 (a)
 400 - 400 (c)
1048 - 1023
 700 -  670
 348    353  Difference equals - 5.
```

In other words, he will be encroaching upon a region reserved for Station 4. He must therefore shift his key tapes back a long distance, and he moves them into the position 418 - 362, or a difference of 56, and then proceeds to encipher. He has had to do this several times during the course of the day, and the greater the difference in length between the key tapes, the more often will such shifting back be necessary.

Now note that in this series of only 17 messages we have five sequent cycles. Using message 2 as a base, because it shows the greatest difference in the series of 5 messages in the sequent cycles, the arrangement is as follows:

Cycle 1 - Message 2 Key Indicators 442 - 417, Difference 25

Cycle 2 - Message 12 Key Indicators 260 - 236, Difference 24

Cycle 3 - Message 17 Key Indicators 225 202, Difference 23

Cycle 4 - Message 4 Key Indicators 090 - 068, Difference 22

Cycle 5 - Message 1 Key Indicators 076 - 055, Difference 21

These messages have been arranged graphically in Fig. 19, and are now ready to be attacked in the manner described before, using the beginnings and taking advantage of the fact that encipherment begins with name and address. The fact that messages carry in plain text the place from which the message emanates, limits the number of possibilities for assumption of a signature, granting that the enemy has a good intelligence system and a close liaison exists between the cipher office and the intelligence bureau. Unless all messages passing over the line are enciphered, addresses and signatures in plain text in ordinary messages would form a valuable body of information for the basis of assumptions of plain text.

Once a start is made toward decipherment, the rest follows quickly because the key indicators for other messages will enable the decipherer to shift the keys already partially reconstructed into other positions and by building up sections of the key tapes the sections can be united in the proper manner and thus the complete keys result. For example, note the key indicators for message 3. viz., 418 - 362. Granting that we have reconstructed the longer key from 418 to say 450, and the shorter key from 362 to say 395, in one of these five cycles, it is only necessary to bring together these series of longer and shorter key letters from 418 to 450 on the one, and from 362 to 395 on the other to produce the decipherment of the beginning of message 3. By continuing such procedure, the entire keys may be pieced together and completely reconstructed.

It should be noted that an excessive difference in length between the two key tapes is likely to cause great difficulties, for the greater this difference the sooner does one station become "out of bounds," for the range of the key tapes becomes more limited as the difference between them increases. For example, we have given two tapes, 700 and 600 letters, a difference of 100 letters. The displacement is therefore 100 letters per revolution of the longer tape. This means that after only seven revolutions of the longer tape one has returned to the starting point, and further encipherment without resetting the tapes would mean an overlap. Compare this with the case where the tapes differ by only one letter, for example, tapes of 700 and 699 letters. Here, only after the longer tape has made 700 revolutions does one get back to the starting point. In other words, one can encipher 700 x 699 or 489, 300 letters before an overlap would be produced.

* * * * *

It is clear, therefore, that the modified method of using the machine affords no better protection against decipherment than the original method, and it is also patent that the principles for the solution of this cipher as first laid down according to our original understanding of the method of using the machine apply with equal validity to the modified method as submitted.

* * * * *

It may be thought that the occurrence of sequent cycles can be avoided by strict supervision. There are some things to be said on that point.

Supervision could undoubtedly be exercised in each of the offices involved in a quad, but it would of necessity have to be supervision of the most careful nature by officers specially qualified. Granting this, there might be two methods of eliminating the possibility of the occurrence of sequent cycles. One would be to have an absolutely random choice of key indicagors (within the limits of the region assigned for the station) but with the restriction that no two messages are to be in sequent cycles. The other method would be to devise some system whereby 2, 3 or more cycles are skipped regularly in all traffic.

After considering these alternatives, we may say that the solution of cases in which one or two intervening cycles are missing can be achieved with no great difficulty. The solution of cases in which say five intervening cycles are missing may be more difficult to achieve, but the necessity of skipping any number of cycles above five in the case of random choice of indicators, and say five regularly in a systematic choice of indicators is so involved with practical difficulties that the entire system would be weak. For, if at least five cycles must intervene, and if a station be allotted 200 cycles for its day's traffic, then the greatest number of cycles actually available would be 40, or in the case of a longer tape of 700 letters in length, a limit of 28,000 letters would be imposed upon the day's activity for that station. In the case of a station that must transact a large volume of business every day this would never be sufficient and the tapes would have to be increased very greatly in length. All of this is aside from the danger of a misunderstanding of the rules and of carelessness in operation.

Furthermore, in the case of a single very long message, unless the message be broken up into parts, the encipherment of such a message is bound to extend into two or more sequent cycles. Of course, without a knowledge of the lengths of the tapes this would afford no clues to the decipherer. But the decipherer can tell approximately the lengths of the tapes by studying the indicators for no messages pass beyond 695 for the longer tape and 690 for the shorter, he can feel reasonably certain that the tapes are in the neighborhood of 700 letters in length. It would take considerable experimentation to determine their exact length, but it could be done within a practicable length of time by a corps of decipherers if the results to be expected would warrant the expenditure of the time and labor.

* * * * * *

August 19, 1919.