IN REPLY REFER TO

_____ DIVISION

WAR DEPARTMENT

OFFICE OF THE CHIEF SIGNAL OFFICER

WASHINGTON

September 12, 1921.

MEMORANDUM for Major Bender:

1. As requested by Colonel Russell, I have set forth in brief my ideas on the modifications proposed for making the Printing Telegraph Cipher safe for the use of the Army. I transmit them herewith.

2. Two of the modifications involve but little change in the present apparatus. The third requires the insertion of a fourth transmitter and certain changes in types of relays.

3. These recommendations as submitted are the result of experimental tests and trials made with the machines as they are arranged at present. While I feel satisfied that the modifications proposed are practicable, I think they should be thoroughly tested out on properly equipped machines before they are adopted.

W. F. Friedman

Code Compilation Section.

PROPOSED MODIFICATIONS FOR THE PRINTING TELEGRAPH CIPHER

Patentable material begins with 913

1. The Printing Telegraph Cipher System, as developed by the American Telegraph and Telephone Company is, in a final analysis, a substitution cipher involving a series of 32 mixed, reciprocal alphabets which are employed in a random manner determined by a non-repeating, unintelligible running key. The running key is produced by the interaction of two unintelligible revolving keys of different lengths. The characters on these keys, which are in the form of tapes, are numbered, and the relative positions in which these two tapes were placed at the beginning of the encipherment of each message are given in the form of a pair of numbers called key indicators. These indicators appear in plain text in the preamble to each message, so that at the receiving end the operator may set his duplicate pair of key tapes in the proper positions for decipherment. The processes of encipherment and decipherment are entirely automatic, and of an electrical nature.

2. Any attempts to render this cipher system insoluble, without an understanding and comprehensive grasp of the principles by means of which it was solved, would seem to be useless. Furthermore, it is necessary to know all the details of the practical application of the system in order that any improvements or modifications proposed may be within the limits of practicability. It is not within the scope of this description to do more than summarize these principles.

3. The first condition which is imposed by military necessity is that all stations on one circuit must use the same key tapes each day. To do otherwise would cause confusion. This condition thus automatically eliminates all modifications proposing different pairs of keys for each station.

4. The second condition which must be realised is the impossibility of using a single, very long tape. The reasons for this opinion are given below under paragraph 10 . The principle of two revolving, relatively short tapes is of sufficient worth to warrant

exhaustive study with a view to modifying the system so as to render it safe.

5. With these two conditions in mind, let us proceed first to review very briefly the principles of solution and then to consider various modifications which may be employed. The solution of the Printing Telegraph cipher, as demonstrated in a paper by the author written when at the Riverbank Laboratories, is achieved by the principles to be described briefly below.

6. Determination of the length of the two key tapes is the first step in the analysis. This is made possible by the fact that the key indicators for each message are given in plain text at the beginning of each message. The determination is accomplished by a mathematical analysis of the key indicators for the various messages of the day's activity. The lengths of the two keys, according to the original method as developed by the A. T. & T. Co., differ by but one unit. The lengths of the two keys, according to the modified method as adopted later by the Signal Corps, differ by more than one unit, and in no case are the two lengths to possess a common factor, nor is one to be an exact multiple of the other. It was shown that regardless of which method was used, the lengths of the two key tapes could readily be determined. It was proposed to prevent the determination of these key indicators by the enemy by enciphering and encoding them, and a method for this purpose was devised by the M. I. D. This method was submitted and demonstrated to be of little advantage, for the key indicators could still be read by the enemy.

7. The method of employing two revolving key tapes results in the production of distinct cyclic phenomena, which are not difficult of analysis by superimposition. The determination of the lengths of the two key tapes enables the cryptanalyst to allocate each message to a particular cycle. When the two key tapes differ by one and only one unit, these cycles are produced successively with consecutive revolutions of the

tapes, Cycles 1, 2, 3, 4 ..., being produced in regular order. When the two tapes differ by more than one unit, the cycles are not produced successively with consecutive revolutions of the tapes; Cycle 1 may be followed by Cycle 71, then by Cycle 141, and so on.

8. Solution is dependent upon the correct superimposition and subsequent analysis of at least three cycles, two of which I have called the EXPERIMENTAL CYCLES, the third, the CONFIRMATIVE CYCLE. The closer together these cycles are, the easier is the analysis. The easiest case is when all three cycles are directly sequent; such as, for example, Cycles 10, 11, 12, or Cycles 41, 42, 43, etc.

9. The method of analysis is to assume plain text at definite locations in the experimental cycles, reconstruct the hypothetical key tapes, and if the plain text that has been assumed is correct not only as regards the actual words assumed, but also the exact location at which they are assumed to occur, the application of the reconstructed keys will yield intelligible text in the confirmative cycle. Once a small portion of intelligible text has been found in this way, reconstruction of the key tapes goes forward rapidly until with their complete reconstruction the cryptanalyst is in a position to decipher any message enciphered by them, by placing the two keys in correct juxtaposition according to the key indicators for the various messages.

10. There are several methods of modifying the system so as to render it more safe, and several precautions, which a proper comprehension of the principles of solution indicates, that should be observed. It has been proposed by Major Mauborgne to use only a single, long key tape. This was, in fact, the very first method experimentally adopted by the A.T. & T. Co., and soon discarded on account of its impracticability. The preparation of a single tape 999,999 units in length is a matter requiring much time, and labor. It would be equivalent to the making of a tape of 150,000 words each day, and numbering the units in groups of tens, a long drawn out piece of labor in itself. Furthermore, at least three duplicates of this long tape are required,

if four stations are operative on the same circuit and the labor in preparing the necessary duplicates would also be very great. The handling of such a long tape would entail the use of a reel to wind and unwind the tape, and the latter would wear and tear very easily. The equivalent length of tape may be obtained by two comparatively short endless tapes, one 999 characters in length, the other 1000. The machines have been arranged for the latter method, and it appears to me to be unwise to discard the labor-saving features which the method of two revolving, endless key tapes provides. It remains, therefore, to modify the present method and mechanism so as to render the use of two continuous key tapes safe for military use. The methods which have suggested themselves to me will now be considered in detail.

11. The modifications of method may be divided into two types or classes. One type has for its purpose the interruption or elimination of the cyclic phenomena produced by the revolutions of the key tapes. The other type does not attempt to interfere with the cyclic phenomena but makes the reconstruction of the two key tapes impossible, and thus renders the resultant cipher insoluble.

12. It is possible to break up the cyclic phenomena in the system, by interposing an interruptor in the nature of a character which automatically stops and starts one of the key tapes. This character may be any arbitrarily determined letter in either one of the key tapes, or any arbitrarily determined letter which is the resultant of the interaction of two letters which are passing through the key tape transmitters simultaneously. This would effectually break up the regularity in the sequence of cycles, but it would introduce the grave danger of the production of "overlaps", i.e., the condition wherein two or more messages or parts of them have been enciphered by the same resultant single key and thus very easily solvable. This danger would be all the greater due to the fact that four stations are operating with the same pair of key tapes each day. Furthermore, even granting that no overlaps would be produced, it would still not obviate the possibility of the correct superimpo-

sition of a few cycles which may eventually lead to solution in the manner described above.

13. It is, however, possible to bring into play an interruptor of a different nature, which would achieve the same purpose but without the dangers mentioned in paragraph 12. This method involves the insertion of a third, or auxiliary, key tape, and corresponding transmitter, the operation of which would be intermittent and determined by any arbitrarily determined resultant of the two principal key tapes. The effect of this would be quite far reaching.

14. In the first place, it would add a third key to the cipher without entailing any additional time in the encipherment or decipherment. The only additional time that would be necessary would be that involved in the preparation of a third key tape of 200 to 900 units in length, which would miltiply the length of the resultant of the two principal key tapes by an equivalent number of times. But its main function is not that in particular, for theoretically, the insertion of a third key tape, or even more, would not complicate the solution very greatly because the solution is not at all dependent upon any analysis of the resultant single key but upon the analysis of superimposed cycles, which is a totally different process.

15. The main function of the auxiliary key would be to break up the cyclic phenomena of the system by introducing a key which is intermittent and irregular. The resultant of the two principal tapes would still be cyclic in nature, but the resultant of the application of the auxiliary tape to that of the two principal tapes would not be cyclic. No indication of the intermittency of this auxiliary key would be given in the final cipher messages. The enemy cryptanalysts would never know when they were dealing with two keys, and when with three. Each message would be a composite of the interaction of two keys at one interval and of three keys at another interval; the lengths of the intervals, and their exact moments of introduction and withdrawal would likewise be unknown, and externally indeterminate.

16. Furthermore, the danger of the production of "overlaps" is entirely eliminated because the two principal keys do not undergo any displacements other than those normally produced by their own cyclic movements. Hence, no two messages emanating from any of the four stations could possibly use the same resultant single key, and thus no overlaps can be produced.

17. The operation of the auxiliary key tape will now be described. Each day this operation will be determined by a different character, which will be arbitrarily selected by the central station. The character chosen will be the resultant of the interaction of any one of 32 different pairs of characters passing through the two principal key tape transmitters at the same moment. Let us suppose this resultant to be the letter K on a given day, and let us set down a few characters of two hypothetical principal keys, designated as the "A" and "B" tapes, and also of the hypothetical auxiliary key, designated as the "C" tape. We will then proceed to find the successive resultants of the interaction of the respective units during one cycle, by referring to the cipher square, applying to the system (Fig. 1)

Fig. 2.

	1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20
Trans. #1 - A tape	R P Q N V O X Z K V T P F C H T Q O R S
Trans #2 - B tape	D N S O Z W D I V T X B B L M 4 O G L Y
Primary Resultants	A G L H (K) J H Q Z C F (K) M M 4 O (K) 2 O T
Trans. #3 C tape	V R O S P N T P X S Q
Secondary Resultants	A G L H Z E N L U 2 X K M M 4 O B 5 A U

The first four letters of the message would be enciphered by the resultants of the interaction of the two principal keys only. Now the fifth combination of key letters yields the letter K, which determines the introduction of the auxiliary key tape. Immediately, the auxiliary key is entered into the reaction, and it will continue to interact with the two principal keys until the same combination, K, is again produced by the interaction of another pair of

units of the principal keys. In this case, the auxiliary key is in effect for seven letters of the message, viz; letters 5 to 11, inclusive. Immediately thereafter, the auxiliary key is withdrawn from the interaction, and only the two principal keys are operative. The number of times this process of inserting the auxiliary key and withdrawing it, and the lengths of the intervals each process is in effect, is determined only by the letters of the two principal keys, and this determination will be totally different for each cycle of the principal keys, since different pairs of letters are brought into interaction with each cycle. Thus, for example, in Cycle 2, with the same principal keys as above, the introduction and withdrawal of the auxiliary key would be determined at these points;

Fig. 3

Cycle 2

	1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20
A tape	R P Q N V O X Z K V T P F C H T Q O R S
B tape	N S O Z W D I V T X B B L M 4 O G L Y R
Primary Resultants	I W (K) X F Q 6 (K) 5 A D (K) 5 L M 4 F R 5 (K)
C tape	P V S Q R E K W O V R Q P
Secondary Resultants	I W B A 4 I Z K 5 A D I T V 3 P U X D K

18. Letters 1 and 2 would be enciphered by the interaction of only the two principal keys. With the production of the letter K as the resultant of the interaction of letters Q and O, the auxiliary key is immediately introduced, to be operative for five letters. From the eighth to the eleventh letters, the auxiliary key is not in effect, from the twelfth to the nineteenth it is again in effect. These intervals and lengths of introduction and withdrawal of the auxiliary key are entirely different from those produced by the first cycle, and would be different from those in any other cycle, for at no time is the same pair of characters of the two principal keys again brought into interaction until the entire potential length of the resultant single key has been employed.

19. At the receiving end, the introduction and withdrawal of the auxiliary tape would be determined in exactly the same manner and by exactly the same resultants of the two principal keys as at the sending end. The process would be automatically reversed, and no special treatment of cipher messages or key tapes would be involved, since the machine automatically takes care of all steps in the process.

20. The wiring diagram for the changes necessary to insert the third key tape transmitter and to effect its operation in the manner described above is shown in Plate 1. (To be prepared)

¶s 21 to 31 deal with a method — no new apparatus necessary.

21. We shall now consider a proposed modification in which the purpose is not to interfere in any way with the cyclic phenomena of the two principal key tapes but to make the reconstruction of the keys exceedingly difficult, if not impossible.

22. It is feasible to provide a means of automatically stopping the plain text tape at a given point, but allowing the two key tapes and the machine perforator to continue uninterruptedly until the plain text tape is again started. This stopping and starting of the plain text tape can be done by hand at random and absolutely irregularly. No indication of the interruption will show in the cipher message, and no correction or automatically operated interruptor is necessary at the receiving end. This is a most remarkable phenomenon in cryptographic methods, and is the only case known to me where an irregularly operative interruptor does not have to be counteracted at the receiving end by an identical reversal of the operations at the sending end. This modification would not eliminate the cyclic phenomena produced by the revolutions of the key tapes, but would render the analysis of superimposed cycles more difficult because of considerations requiring too detailed an explanation to set forth in this brief. In a few words, it would increase the difficulty of reconstructing the two key tapes

from any assumptions of plain text in the experimental cycles, and the application of the thus reconstructed portions to the confirmative cycle.

23. This method may be used for the interior of messages, but it is intended primarily to disguise the beginnings and ends of the messages. The reason for this differentiation in treatment is the fact that the beginnings and endings of these messages are particularly susceptible to attack because they contain addresses and signatures which are always the easiest points of attack by the cryptanalyst. Especially is this the case here because the messages are confined to communications between large headquarters where such relatively long addresses as "Quartermaster General", "Chief of Ordnance", "Surgeon General", etc., are very common. In fact, the solution of the test case submitted by the Signal Corps was based upon the assumptions of these very addresses, and it turned out that the assumption of "Quartermaster General" in one of the experimental cycles and "Chief Signal Officer" in the other immediately yielded intelligible text in the confirmative cycle. If, now, a random, irregular interruption of the plain text tape occurs at the beginning and endings of messages, the enemy cannot proceed to assume entire addresses or names, for they will be interrupted irregularly in somewhat this fashion:

Q -- U A R - - - - - - - T E - - R - - - M A S T - - - - E R

24. Here the dashes represent blanks which are inserted in an irregular manner between the letters of the plain text. The enemy may know that such interruptions occur, but their location and length would be unknown. Their exact location would be unknown even to the encipherer and the decipherer, because it is done in an absolutely random manner during the enciphering process by the operator himself.

25. What actually happens during these interruptions is that the machine perforator is punching the resultants of those pairs of characters

on the key tapes which are interacting during the interruption. These resultants will not be differentiated in any manner whatsoever, externally, from those cipher letters which are the resultants of the interaction of all three tapes, viz., the two key tapes and the plain text tape. In the deciphering process, when a portion of cipher tape which is the result of the interaction of only the two keys is passing through the transmitter, the cipher letters are exactly neutralized by the same resultants of the key tapes as were involved in the encipherment. The result is that the printer merely stops printing for a corresponding number of units, until such a time as the cipher letters which were the resultants of all three tapes are going through the transmitter. Then the printer immediately continues printing.

26. As stated before, this method may also be applied to the interior of messages, but its employment for a considerable portion of the messages would soon exhaust the potential length of the resultant single key, so that a station would be going beyond the limits set by the allotment before it had enciphered all its messages, unless considerably longer key tapes are employed. This would be a disadvantage, for, normally, key tapes not exceeding 999 units in length are sufficient for the traffic of four stations.

27. It may be well to give a diagrammatic representation of the results of this method as applied to the beginning of a message. Let the message be addressed as follows:

QUARTERMASTER3GENERAL6N542WASHINGTON6N53D6M53C6M542222.

(Note: The meaning of the figures are these:
2 - Line Feed
3 - Space
4 - Carriage Return
5 - Letters
6 - Figures)

28. The encipherment may be in this manner:

Fig. 4.

A tape-O V N K T P R X S T A P Q W V N C T P O I N V Q K B D N C Q R I V L T M O X P

B tape-B Q V C R I L A M X Z P L K T P O P V N C D P O L Y C I Q R N T P A B L M S Q

Plain-text Q U A - - - - R T E R M - - - - A S T E - - - R 3 G E - - N E - - R A L 6 N 5

Cipher-P C Z E G T O H D N O M S M C G Y A O Y 4 S 4 S B P I R B Q U P 4 6 R M 5 H V

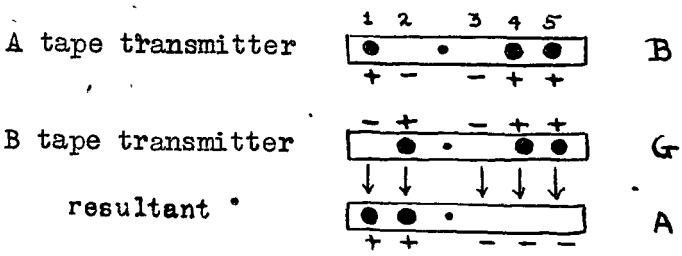
29. If now the enemy should try to assume a plain text beginning for this message, even if he did assume the correct address, he would not know how the letters are interrupted, and unless he knows this too, his attempts to reconstruct the keys will be of no avail.

30. This modification may be applied in conjunction with that involving the third or auxiliary key tape, the two being independent of each other. If the plain text tape is stopped while the auxiliary transmitter is in operation, the cipher letters will merely be the resultants of the three key tapes, instead of only two, as would otherwise be the case.

31. The actual method of stopping and starting the plain text transmitter is most simple, and requires absolutely no changes in apparatus. It consists merely in throwing the start-stop lever arm of this transmitter to the right or left; to the right when the transmitter is to be stopped; to the left, when it is to be started.

32. There is one more modification which is well worth considering. As developed by the A. T. & T. Co., the printing telegraph cipher system employs a cipher square or quadricular table involving 32 mixed, reciprocal alphabets which are constant in nature, and are not intended to be changed. The electrical circuit is so designed that when homologous selecting pins in the two key tape transmitters are kept down by the tapes, or when both pins are allowed to come through the tapes, no impulse is sent through the winding of the corresponding relay, because no circuit has been established. However, when a pin in one key tape transmitter is kept down and its homologous pin in the other key tape transmitter is allowed to come through the tape, a circuit

is at once established through the winding of the relay involved, and the relay operates. This arrangement is the same with respect to all five of the key tape transmitter relays, and an understanding of the phenomenon leads to a comprehension of the manner in which the enciphering process is accomplished and the nature of the cipher square. (Fig 1) For example, when the letters B and G interact, we have the letter A as the resultant



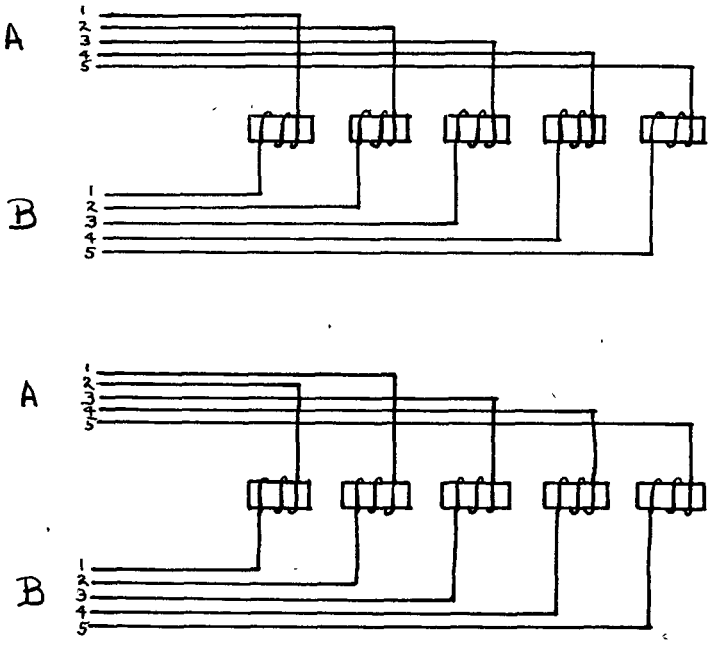
33. Here the first selecting pin of the A tape transmitter is making contact to + battery, and the homologous pin of the B tape transmitter is making contact to - battery, thus resulting in establishing a circuit through the winding of relay 1, and operating the relay. The same is true with respect to the second pair of homologous selecting pins, with reversed signs in effect, and relay 2 is operated. In the case of the third pair of selecting pins, both pins are making contact to - battery, so that no circuit is established; in the cases of the fourth and fifth pairs, all pins are making contacts to + battery, and no circuit is established. Hence relays 3, 4, and 5 remain inoperative, only relays 1 and 2 being operated, and the printer will print the letter A, or if the machine perforator is operating, only magnets 1 and 2 will be operated so that holes 1 and 2 are punched in the tape.

34. Now if we change the wiring of the key tape transmitters, we may effectually break up the relations established by the present connections. There are 120 different combinations of connections possible between the five selecting contact terminals of one key tape transmitter and the five homologous terminals of the other transmitter. Terminal 1 of the A tape transmitter may be connected with terminal 1, 2, 3, 4 or 5 of the B tape transmitter. The same holds true with respect to the other four terminals of the A tape transmitter. The number of possible combinations of connections which can be made is

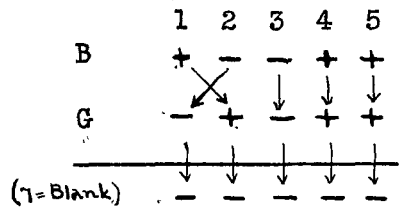
5 x 4 x 3 x 2 = 120 combinations.

35. For example, let us connect terminal 1 of the A tape transmitter with terminal 2 of the B tape transmitter; and terminal 2 of the A transmitter with terminal 1 of the B transmitter. The difference in the circuits is shown in Figure 5.

Fig. 5

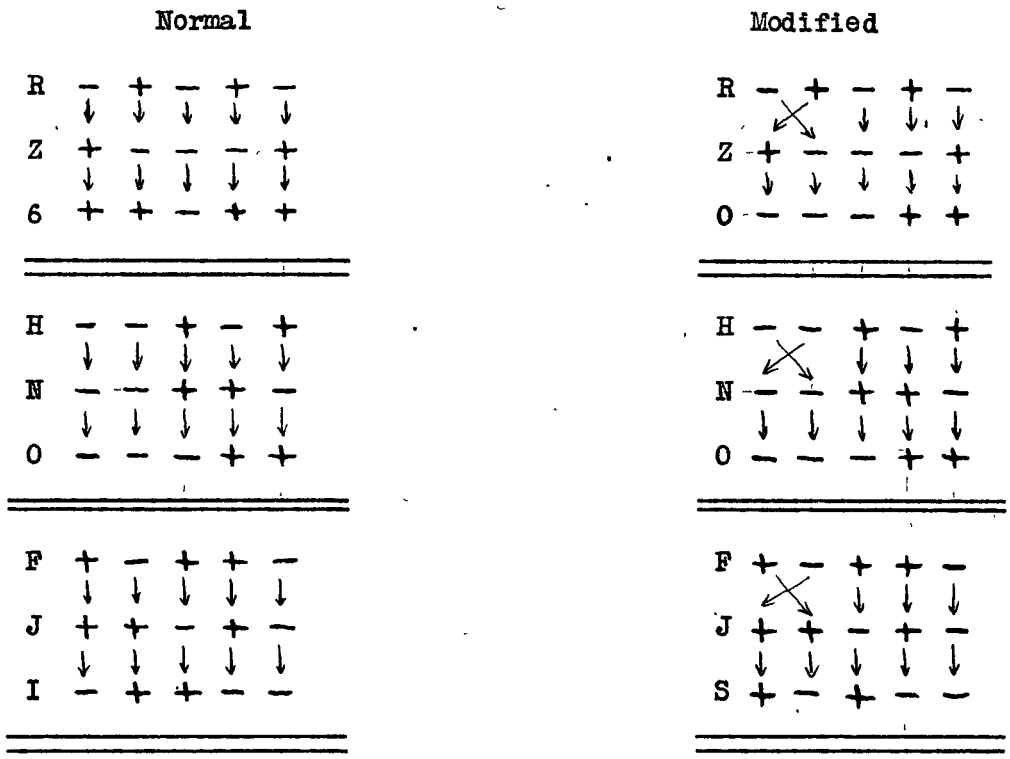


36. Now let us see what the resultant of letters B and G are:



37. It is seen that the resultant should be a blank. This is, indeed, what the actual resultant is, when the indicated change is made in the connections. The resultant of several other pairs of letters are given herewith to illustrate the nature of the changes from the normal.

Fig. 6

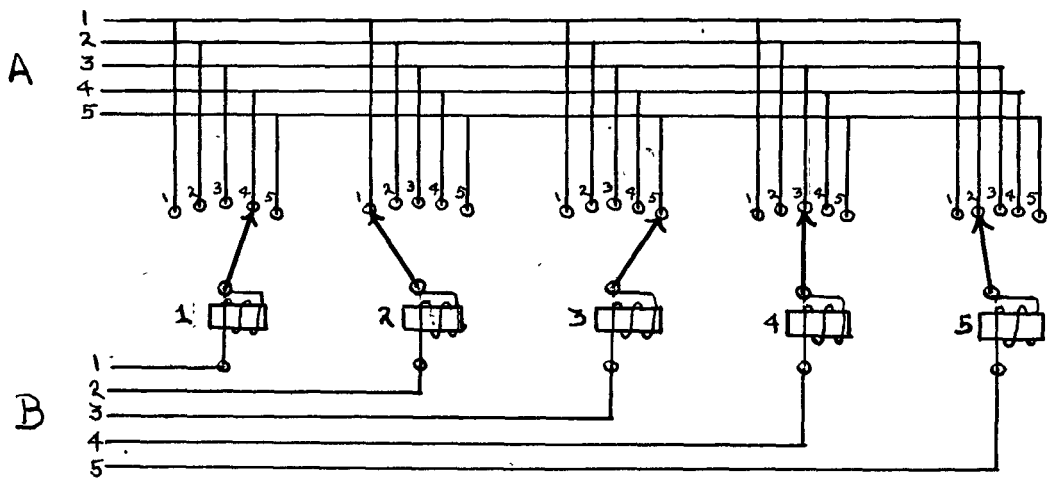


38. With another change in connections, an entirely different series of resultants will be produced. This would mean an entirely different cipher square for each possible set of connections. Since there are 120 different combinations possible, the number of different cipher squares would be 120, and the number of alphabets involved in the system would no longer be only 32, but 120 x 32, or 3,840.

39. The result of the foregoing then is: the reconstruction of key tapes from assumptions of plain text in the experimental cycles would be rendered highly improbable, if not absolutely impossible. It is difficult enough now, with only one cipher square involved; but with 120 different possible squares, the exact one which is being used on a given day is unknown to the enemy and manifests itself in absolutely no way in the cipher messages, the problem of solution may be considered to be practicably impossible.

40. For practical purposes, the establishing of a given combination could be facilitated by a panel of the nature shown in Figure 7.

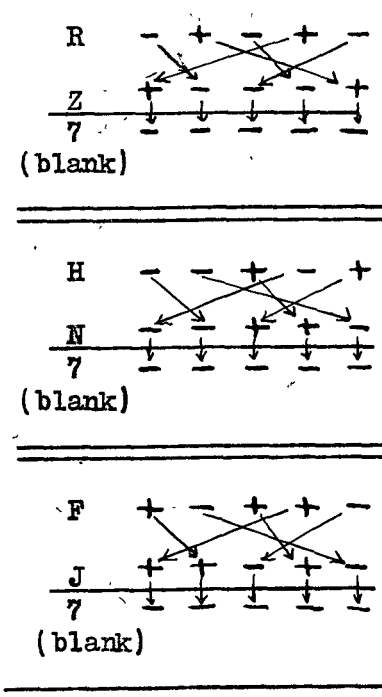
Fig. 7



41. Here the combination is 4 - 1 - 5 - 3 - 2; i.e., the winding of relay 1 is connected to selecting pin contacts 4 of the A transmitter and 1 of the B transmitter; the winding of relay 2 is connected to selecting pin contacts 1 of the A transmitter and 2 of the B transmitter; that of relay 3, to 5 and 3, respectively, etc.

42. Let us see what the resultants of the letters R and Z, H and N, F and J will now be.

Fig. 8.



43. It is seen that blanks result from each of these pairs of interacting letters. Other pairs would give different resultants.

44. The changing of the connections between the key tape transmitters would have no effect upon the normal operation of the machine so far as the transmission and reception of plain text is concerned.

45. It is submitted that the insertion of the third or auxiliary key tape transmitter, the changing of the connections between the two principal key tape transmitters and the use of the interruptor as described in paragraphs 22 to 31 will make the printing telegraph cipher insoluble, without impairing its practicability in the slightest degree.

46. The subsequent pages of this paper will deal with a phase of the normal method of encipherment which entails precautions not observed heretofore, and which should be observed in the future. It deals with the method of allotting definite sections of the key tapes to the four stations on a single circuit.

¶s 46-66 deal with methods for allotting the cipher tapes to various stations.

47. The purpose of allotting definite sections of the key tapes to the four stations is to preclude the possibility of two stations employing identical portions of the theoretical resultant single key. If this condition is not prevented, overlaps will be produced, i.e., two or more messages, or

parts of them, will be enciphered by the same resultant single key, and the messages are rendered very easily solvable.

48. The method heretofore has been to divide up the length of the longer key into four equal or nearly equal parts, and assign each station a given pair of initial indicators for its messages. For example, let us suppose that two key lengths 800 and 763 are chosen. Each station would then be assigned 800 ÷ 4 = 200 units of the long key; the initial short key indicators for all four stations would be the same, for example, 001. The initial key indicators for the four stations would be assigned as follows:

Station A	Station B	Station C	Station D
001 - 001	201 - 001	401 - 001	601 - 001

49. In this case, no overlaps could be produced, providing the traffic for no station exceeded its allotted number of resultant single key units, in this specific instance $\frac{(800)(763)}{4}$, or 152,600 units. The reason for this is that the length of the longer key is exactly divisible by 4, and hence the allotment can be made in four exactly equal sections. However, when the length of the longer key is not an exact multiple of 4, the case is slightly different. It has been assumed, heretofore, that if the nearest fourth part of the length be allotted to each station, no overlaps can be produced. For example, in the test case which was submitted and solved, the lengths of the two keys were 787 and 639 units respectively. The initial indicators for the four stations were these:

Washington	Hoboken	Norfolk	New York
126-001	322 - 001	518 - 001	714 - 001

50. These initial indicators were derived by adding the nearest integral fourth part of 787 to the initial long key indicator for Washington. Thus:

787 ÷ 4 = 196 +

Washington	-	126	(Initial long key indicator)
Hoboken	-	196 322	(" " " ")
Norfolk	-	196 518	(" " " ")
New York	-	196 714	(" " " ")

51. It will now be demonstrated that this method is not mathematically strictly correct and that if followed consistently will lead to the production of overlaps. Let us suppose that these two key lengths have been selected: 917 and 723. These two lengths are strictly legitimate, since they do not possess a common factor, nor is one an exact multiple of the other, two conditions which must be met. The nearest integral fourth part of 917 is 229. Assuming that the initial key indicators for Station A would be arbitrarily selected as 125 - 001, the indicators for the four stations would be as follows:

Station A	Station B	Station C	Station D
125 - 001	354 - 001	583 - 001	812 - 001

52. Let us now determine what the indicators for Station A are after exactly 9399 letters have been enciphered.

Station A

Initial indicators	- 125	- 001
Length of messages	9399	9399
	9524 -	9400

53. From these two totals we should now deduct the greatest exact multiples of the respective key lengths such as will leave positive remainders. Hence:

	9524 -	9400
Deduct (917 x 10)	9170 -	9399 Deduct (723 x 13)
	354 -	001

54. The longer key will have completed 10 whole revolutions, the shorter one, 13. Immediately thereafter, it will be noted that the indicators become 354 - 001, which coincide exactly with the initial indicators for Station B. In other words, after 9399 letters have been enciphered at

Station A, all subsequent traffic of Station A would be enciphered in the same resultant single key as the traffic of Station B.

55. The same phenomenon is true of the traffic of Station B with respect to that of Station C, and that of Station C with respect to that of Station D.

Station B	Station C	Station D
354 - 001	583 - 001	812 - 001
9399 -9399	9399 - 9399	
9753 -9400	9982 - 9400	
9170 -9399	9170 - 9399	
583 - 001	812 - 001	

56. Furthermore, it is obvious that after Station A has enciphered 9399 x 3 = 28197 letters, Station B 9399 x 2 = 18798 letters, and Station C 9399 letters, the traffic of all four stations is enciphered by the same resultant single key, or in other words, a four-fold overlap would result.

57. The conclusion is obvious, therefore, that this method of allotment is not correct, and must be modified.

58. There are two methods of allotment which are accurate, and can therefore never involve the danger of overlaps. One is to base the allotment upon a correct distribution of complete cycles; the other is to base it upon an exact division of the theoretical resultant single key.

59. The former method is explained in detail in an unpublished paper by the author, entitled "The Mechanics of Differential Primary Keys". The explanation is too long to be incorporated in this paper, but in brief it may be said that it depends upon the solution of two indeterminate or Diophantine equations in which the lengths of the two keys and their relative displacements in consecutive revolutions play the major part. This method is possibly too complicated for practical purposes, and we shall proceed to explain the second method, which is considerably easier to apply. The steps are as follows:

60. First, determine the length of the theoretical resultant single key. Let us take the two lengths given above, viz., 917 and 723.

$$917 \times 723 = 662{,}991 \text{ units}$$

Second, divide this length by 4

$$622{,}991 \div 4 = 165{,}747\tfrac{3}{4}$$

61. This quotient represents the single key allotment length for each station; or, in other words, each of four stations may encipher 165,747 letters without causing any overlap with the traffic of the other stations.

62. Third, add this length to the initial key indicators for Station A, and deduct the greatest exact multiples of the two key lengths such as will leave positive remainders. Let the initial indicators for Station A be the same as before:

	Station A	
	125 - 001	
	165747 -165747	
	165872 -165748	
Deduct (917 x 180)	165060 -165567	Deduct (723 x 229)
Key indicators for Station B	812 - 181	

63. The initial key indicators for Station C are derived in exactly the same manner from those of Station B; and those for Station D from those of Station C. They are all as follows:

Station A	Station B	Station C	Station D
125 - 001	812 181	582 361	352 541
165747 165747	165747 165747	165747 165747	165147 165747
165872 165748	166559 165928	166329 166108	166099 166288
165060 165567	165060 165567	165060 165567	165060 165567
812 - 181	1499 361	1269 541	1039 721
	917	917	917
	582 - 361	352 - 541	122 - 721

64. It will be noted that the final pair of indicators for Station D are 122 - 721. If now we add 3 units (which are represented by

the $\frac{3}{4}$ of a unit dropped by each station due to the fact that the resultant single key is not exactly divisible by 4), we have this

$$\begin{array}{r} 122 - 721 \\ \underline{3 \quad\quad 3} \\ 125 - 724 \end{array}$$

65. Now unit 724 of the short key is really the same as unit 001, since it is 723 units in length. Hence we have 125 - 001, which are the initial key indicators for Station A, proving that the allotment lengths and key indicators for the four stations are correct.

66. The practice has heretofore been to slip the two key tapes forward two units at the end of messages. The purpose of this has apparently been to try to increase the difficulty of determining the lengths of the two keys by the enemy. This, however, fails in its purpose, unless the slip be different for each message, ranging from 1 to 25 units. However, great care must be observed that both keys are slipped exactly the same amounts in every case, otherwise the production of overlaps will result. In fact, the danger is so great, and the advantages to be gained by slipping the tapes so slight, that it is recommended the practice be discontinued in the future.

September 12, 1921

W. F. Friedman