PRINCIPLES OF SOLVING M[illegible] CRYPTOGRAMS

Produced by the

[illegible] MACHINE

Technical Paper
of the
Signal Intelligence Section,
War Plans and Training Division,
Office of the Chief Signal Officer,
War Department

[illegible]shington
December, 1931

PRINCIPLES OF SOLUTION OF CRYPTOGRAMS

Produced by the

I. T. & T. CIPHER MACHINE

1. Introduction. - a. The I. T. & T. Cipher Machine is composed of three essentially distinct units:

(1) A teletype transmitter

(2) A mixer

(3) A teletype receiver

From a cryptographic standpoint, the second of these three elements is the only one in which we are interested. It applies a running key to the individual letters of the plain text in a manner which will be fully discussed in what follows. The first and third of the foregoing elements are merely the ordinary teletype machines. It is assumed that the reader has a general understanding of the construction and principles underlying these printing telegraph devices. For convenience, the Baudot or 5-unit code employed by them is shown herein as Fig. 1. The explanation of the numerical designations 2, 3, ... 7, will follow.

b. Attached hereto is a blueprint of the connection diagram of the cipher printer unit.

c. Also attached hereto are the cipher-operating instructions as prepared by the I. T. & T. Company (Appendix A.).

2. Description of the mixer. - a. The mixer contains ten toothed wheels, mounted on a common shaft, in such a manner that they move forward simultaneously one step at a time. The first wheel has 26 teeth and

BAUDOT CODE

Upper Case	Lower Case						
-	A	+	+	-	-	-	
?	B	+	-	-	+	+	
:	C	-	+	+	+	-	
$	D	+	-	-	+	-	
3	E	+	-	-	-	-	
!	F	+	-	+	+	-	
&	G	-	+	-	+	+	
£	H	-	-	+	-	+	
8	I	-	+	+	-	-	
'	J	+	+	-	+	-	
(	K	+	+	+	+	-	
)	L	-	+	-	-	+	
.	M	-	-	+	+	+	
,	N	-	-	+	+	-	
9	O	-	-	-	+	+	
0	P	-	+	+	-	+	
1	Q	+	+	+	-	+	
4	R	-	+	-	+	-	
'	S	+	-	+	-	-	
5	T	-	-	-	-	+	
7	U	+	+	+	-	-	
;	V	-	+	+	+	+	
2	W	+	+	-	-	+	
/	X	+	-	+	+	+	
6	Y	+	-	+	-	+	
"	Z	+	-	-	-	+	

2	+ + - + +	(Figures)
3	- - + - -	(Space)
4	+ + + + +	(Letters)
5	- + - - -	(Line Feed)
6	- - - - -	(Blank)
7	- - - + -	(Car. ret.)

Fig. 1

thereafter each wheel has one tooth more than the preceding one, so that the tenth one has 105 teeth. After the proper switch has been closed to set the mixer into operation, the depression of any key on the transmitter keyboard actuates the mechanism which moves the wheels in the mixer. Corresponding to each wheel is a switch which is mounted immediately behind it and which is acted upon by an irregular arrangement of notchings (that is, elevations and depressions) on the periphery of the wheel. (These switches are shown at the left in the accompanying blueprint, marked 1 to 10.)

b. Alongside the elevations and depressions on the periphery is a smooth band upon which are engraved the letters of the alphabet in their normal order. This permits the wheels to be set in initial positions according to a pre-arranged keyword which is visible only through a series of 10 narrow slits arranged horizontally in a plate immediately in front of the series of cipher wheels. Unless otherwise stated, it will be assumed that a dictionary word

is used as the initial setting of the 10 wheels.

3. Action of the mixer. - a. The action of the wheels is in pairs -- 1 with 2, 3 with 4, etc. If two elevations or two depressions should occur simultaneously on each of the two member wheels of a pair of wheels, and should thus cause identical positionings of the respective switches controlled by them, the combined effect is one of nullification; that is, the resultant of similar settings of the two members of a pair of switches is negative, and will hereafter be denoted by -. Should, however, an elevation and a depression occur simultaneously, the resultant action is of the opposite type and is denoted by +. This resultant action affects the individual impulses or units of the Baudot permutation representing the message character. Here again the interaction of two like elements results in a -, that of two unlike elements, in a +. As a consequence, the five Baudot units representing each plain-text character are independently affected, giving a new set of five units in the Baudot code which corresponds to the cipher letter. This cipher letter is the one which is printed at the receiver.

b. The electrical principles underlying the cryptographic treatment in this system are such that any one of the set of 32 permutations may be brought about by the encipherment of any letter, depending, of course, upon the keying character. This being the case it is obvious that the cipher text will be composed of heterogeneous sequences of 32 elements. Since the normal alphabet contains only 26 letters, it follows that 6 of the 32 permutations produced cryptographically by this machine will have to be represented by arbitrarily selected characters other than letters. These 6 permutations are the ones designated in Fig. 1 by the numerals 2 to 7, inclusive, which designations were assigned these permutations by the I. T. & T. Co. It is therefore obvious that the printed cipher text will consist of intermixtures of letters and figures, a serious disadvantage from the practical point of view of economy in cost of transmission.

4. Principles of analysis involved.- a. The construction of the mixer is such as to preclude the possibility of either interchanging the wheels or of changing their notchings. For this reason we may consider the sequence of cipher wheels and the series of elevations and depressions on each wheel as fixed elements, the exact nature of which can be ascertained by the enemy. This information can be obtained quite readily by examining one of the mixers and following out the procedure set forth in subparagraph b.

b. The method of ascertaining the notchings on the wheels of the mixer was kindly furnished by the I. T. & T. Co., and reads as follows:

(1) Set the mixer to AAAAAAAAA.

(2) Remove the top cover so that the movement of the switch operating levers can be seen.

(3) Prepare a record sheet with 20 columns and a maximum of 105 lines, which should be numbered on the right hand margin.

(4) Note down by some symbolization in the odd-numbered columns whether the operating levers are in or out, and in the corresponding even-numbered columns the letters which show up in the windows. For the initial setting the operating levers will all be in.

(5) Throw the machine into cipher and operate the space bar or any other key, noting on the record sheet the positions of the 10 operating levers. Thus, after the first operation of the space bar, all the operating levers will be pushed out and should be so recorded. At the next operation of the space bar a variation will begin to show. After 105 operations of the space bar with the corresponding recording, the record sheet will show the actual notching of all the wheels and the proper relation of the key word letters to that notching.

c. As regards the notchings on the cipher wheels, if an elevation is denoted by - and a depression by +, it is possible to set up ten slidable strips which will correspond to the wheels.[1] (See attached Fig. 2)

d. The solution of a cryptogram enciphered by the machine therefore reduces itself to discovering merely the initial settings of the wheels, or their equivalent sliding strips.

5. Determination of the key for a single message when a portion of the plain text is known.- a. The construction of the machine is such that the

[1] The arrangements are such that when an elevation presents itself to the switch lever, the contact is opened.

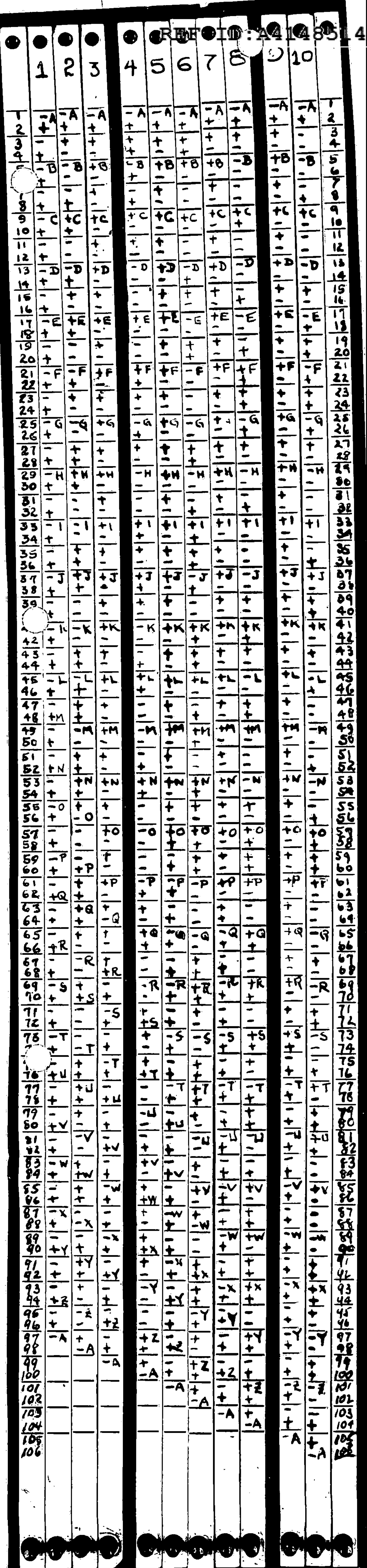


FIG. 2

last three characters of every cipher message represent the same plain-text elements, viz., "Figure Shift", "J", "Letter Shift". (See par. 5 of Appendix A.) These three characters correspond to the action of taking the machine out of cipher; in other words, stopping the movement and the action of the mixer. In addition, it may safely be assumed that the three characters immediately preceding those just mentioned are "Figure Shift", "X", "Letter Shift", which correspond to the "period" at the end of the message. Although the presence of this group of three characters is not invariable, and is not absolutely essential to solution, its existence will be assumed in what follows for the sake of simplicity.

b. Each character element of the cipher text is the resultant of the interaction of fifteen elements; namely, five elements of the plain text (in Baudot code), and ten mixer wheels arranged in five sets. Let attention be directed for the present to the first unit of the cipher text, the first unit of the plain text, and mixer wheels 1 and 2. The following diagram makes this clear. If the first element of a letter of the cipher text is denoted by C_1, the first element of the plain-text letter by P_1, the partial keys (introduced by mixer wheels 1 and 2) by K_1 and K_2, and the resultant of K_1 and K_2 by K_{r1}, the following graphical representation of the interaction of these elements can be drawn up:

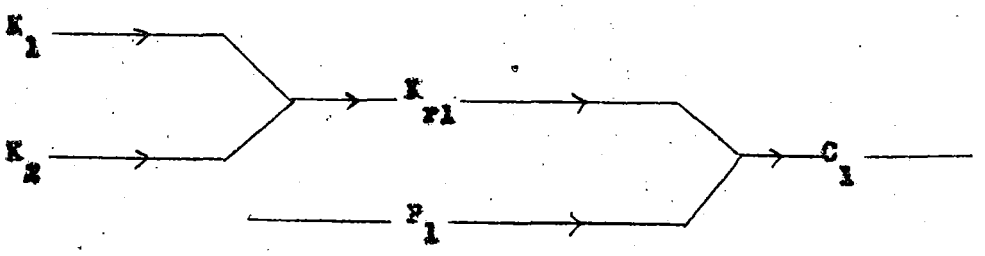


Fig. 3

A consideration of the foregoing representation will show that if any two of the final three elements are known, the third can be derived. For, if K_{r1} is - and P_1 +, then C_1 is + since - and + combine to give +. On the other hand, if C_1 is known to be + and P_1 to be +, then a - is obtained for K_{r1}.

To appreciate more clearly the various steps involved in the enciphering process, it would be wise to carry it out step by step.

c. The following graphical representation of encipherment (Fig. 4) by means of the strips is equivalent to what the machine does electrically. Let the message be ADVANCE AT ... to be enciphered with the initial setting ARBITRATE. Since the machine also enciphers the spaces between words (represented by the numeral "3"), the plain-text elements in the line designated P in the figure, are ADVANCE 3 AT 3.

	P	A	D	V	A	N	C	E	3	A	T	3
	P_1	✦	✦	-	✦	-	-	✦	-	✦	-	-
A	K_1	-	✦	-	✦	-	✦	-	✦	-	✦	-
R	K_2	-	-	✦	✦	-	-	-	-	✦	✦	✦
	K_{r1}	-	✦	✦	-	-	✦	-	✦	✦	-	✦
	C_1	✦	-	✦	✦	-	✦	✦	✦	-	-	✦
	P_2	✦	-	✦	✦	-	✦	-	-	✦	-	-
B	K_3	✦	-	✦	-	✦	-	✦	-	✦	-	✦
I	K_4	✦	✦	✦	-	✦	✦	✦	-	-	-	-
	K_{r2}	-	✦	-	-	-	✦	-	-	✦	-	✦
	C_2	✦	✦	✦	✦	-	-	-	-	-	-	✦
	P_3	-	-	✦	-	✦	✦	-	✦	-	-	✦
T	K_5	-	✦	-	✦	-	✦	-	✦	-	✦	-
R	K_6	✦	✦	✦	-	-	-	✦	✦	✦	✦	✦
	K_{r3}	✦	-	✦	✦	-	✦	✦	-	✦	-	✦
	C_3	✦	-	-	✦	✦	-	✦	✦	✦	-	-
	P_4	-	✦	✦	-	✦	✦	-	-	-	-	-
A	K_7	-	✦	✦	-	✦	-	✦	-	✦	-	✦
T	K_8	-	✦	✦	✦	-	-	✦	✦	-	✦	
	K_{r4}	-	-	-	✦	✦	-	✦	✦	-	-	-
	C_4	-	✦	✦	✦	-	✦	✦	✦	-	-	-
	P_5	-	-	✦	-	-	-	-	-	✦	-	
H	K_9	✦	-	✦	-	✦	-	✦	-	✦	-	✦
S	K_{10}	-	-	-	✦	✦	-	✦	✦	✦	✦	-
	K_{r5}	✦	-	✦	✦	-	-	✦	-	✦	✦	
	C_5	✦	-	-	✦	-	-	✦	-	-	✦	
	C	C	R	J	4	3	D	F	X	3	6	W

Fig. 4

d. In the foregoing figure:

(1) P_1, P_2, P_3, P_4, P_5 are the successive Baudot components of the corresponding plain-text letters in the line designated P.

(2) K_1, K_2, K_3, K_4, ... K_{10} are the electrically represented effects of the projections on the wheels, 1, 2, 3, 4, ... 10.

(3) K_{r1}, K_{r2}, K_{r3}, K_{r4}, K_{r5} are the electrically represented resultants of combining K_1 and K_2, K_3 and K_4, K_5 and K_6, K_7 and K_8, K_9 and K_{10}.

(4) C_1, C_2, C_3, C_4, C_5 are the resultants of combining P_1 and K_{r1}, P_2 and K_{r2}, P_3 and K_{r3}, P_4 and K_{r4}, P_5 and K_{r5} and are

(5) The Baudot components of the cipher letters which are seen in the last line of the figure, designated by the letter C.

(6) The sequence of +'s and -'s for K_1, K_2, K_3, etc., are obtained from the strips by reading the sequence of signs on strip 1 starting with A; on strip 2 starting with B; on strip 3 starting with B, etc.

(7) Consider now what takes place in the mixer. The striking of Key "L" in the transmitter sends the five impulses $\begin{matrix} P_1 & P_2 & P_3 & P_4 & P_5 \\ + & + & - & - & - \end{matrix}$.

Wheels 1 and 2 interact to give $(-)(-) \equiv (-)K_{r1}$

Wheels 3 and 4 interact to give $(+)(+) \equiv (-)K_{r2}$

Wheels 5 and 6 interact to give $(-)(+) \equiv (+)K_{r3}$

Wheels 7 and 8 interact to give $(-)(-) \equiv (-)K_{r4}$

Wheels 9 and 10 interact to give $(+)(-) \equiv (+)K_{r5}$

(8) The resultant keys now interact with the elements of the plain-text letter to give the elements of the cipher letter as follows:

$P_1\ (+)\ K_{r1}\ (-) \equiv (+)C_1$

$P_2\ (+)\ K_{r2}\ (-) \equiv (+)C_2$

$P_3\ (-)\ K_{r3}\ (+) \equiv (+)C_3$

$P_4\ (-)\ K_{r4}\ (-) \equiv (-)C_4$

$P_5\ (-)\ K_{r5}\ (+) \equiv (+)C_5$

(9) The five cipher impulses + + + - + leave the mixer and the letter Q appears on the receiving machine as the first cipher letter. Carrying out all these steps in order, the second plain-text letter D becomes cipher R. The reader is advised to carry out all these steps in detail in order to gain a clearer understanding of what follows.

e. Since the last six characters of the plain text and of the cipher text are known (Figure Shift-H-Letter Shift/Figure Shift-J-Letter Shift), the resultant K_r used to encipher the last six characters of the plain text can be derived. One gets as a result five sets of six characters each corresponding to six impulses of K_{r1}, K_{r2}, ... K_{r5}, respectively. The problem now is to find the settings of the wheels which will give these sequences of six known characters in each K_r. The reasoning is applied to one pair of wheels at a time.

f. The application of the theory outlined above is exemplified in the solution of the following message[1]:

(1) The message:

7 D P E 5 C A P 4 R N D Y C 6
Z L Y 5 C A C C D O . . . . . L B 2 J Y
5 W Y N B P C I S 3 I V X C E N T N F C

Total length of enciphered text is exactly 175 characters.

(2) The last six characters are written out with their Baudot code equivalents and their assumed plain-text equivalents, as follows:

Cipher text:	N	K	T	L	W	O
	-	-	-	+	+	-
	-	-	-	+	+	-
	+	+	-	+	-	-
	+	+	-	-	-	+
	-	+	+	+	+	+
Plain text:	Fig. Sh.	L	Let. Sh.	Fig. Sh.	J	Let. Sh.
	+	-	+	+	+	+
	+	-	+	+	+	+
	-	+	+	-	-	+
	+	+	+	+	+	+
	+	+	+	+	-	+

[1] This was Message No. 7, Set A, of the test messages submitted by the Department of State in connection with the study made for them to determine the degree of cryptographic security afforded by the machine. The complete message will be found in Appendix B.

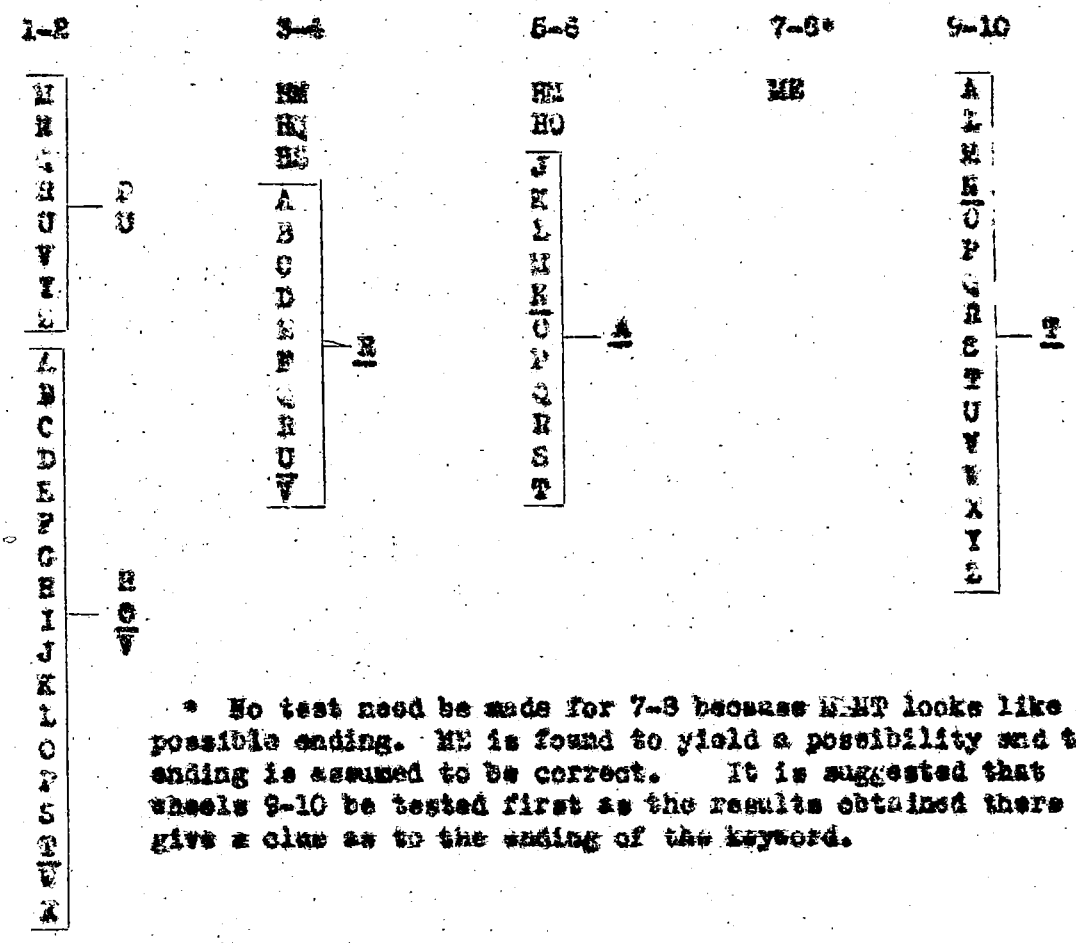
Corresponding portions of the resultant keys obtained by combining the foregoing two sets of symbols:

1-2	+	-	+	-	-	+
3-4	+	-	+	-	-	+
5-6	+	-	+	+	-	+
7-8	-	-	+	+	+	-
9-10	+	-	-	-	+	-

(3) An experiment is now instituted to find a setting of mixer wheels 1 and 2 which will yield a resultant key composed of the sequence + - + - - +, such that, when a retrogression of 175-6 or 169 steps on each wheel is made, the two letters marking the initial positions of the first and second cipher wheels will give two letters which might form the initial digraph of a probable 10-letter keyword. If the position thus found for each of these two wheels is not such as to bring their designating letters <u>exactly</u> in front of the slit through which they were visible as keying letters at the beginning of the encipherment of this message, it is automatically excluded. Furthermore, only 26 different initial settings need be considered at the maximum. The detailed reasoning on which this reduction in number of possible initial settings to a maximum of 26 is based is as follows: Since the cipher wheels of the mixer are set up according to a keyword at the beginning of the encipherment of a message, it is obvious that in this method of use no advantage is taken of the maximum initial positioning possibilities of the cipher wheels. For example, the periphery of the first wheel has 96 teeth; this does not mean, however, that there are 96 possible initial settings of this wheel to be considered in this phase of the cryptanalysis of the system. For, on setting up the wheels according to a keyword which is visible only through the narrow slit referred to under paragraph 2b, only 26 different initial settings are brought into play. Thus, the series of 96 potential initial settings become reduced to but 26.

(4) The foregoing procedure is followed for each pair of wheels. The experiment proceeds more rapidly if letter combinations are set up first and the resulting K_r at a distance of 169 letters is compared with the desired K_r.

(5) For this particular example, the following possibilities for the corresponding wheels are found:



* No test need be made for 7-8 because NEHT looks like a possible ending. ME is found to yield a possibility and this ending is assumed to be correct. It is suggested that wheels 9-10 be tested first as the results obtained there may give a clue as to the ending of the keyword.

The reason for the relatively great number of letters on the odd wheels is due to their regularity. Inspection will show that these wheels are almost exclusively composed of an alternation of + and -. Given any possible combination, such as M' on wheels 1 and 2, all the combinations ending in P can be written down at once without any difficulty.

(6) From these combinations of letters a study of possible and probable keywords is made. As a matter of interest, the keyword TOU[illegible]NT was guessed in this case, and proved to be the correct one. The beginning of the message reads:

I N S T A L L A T I O N S O F 3 . . .

(7) In general, it is not necessary to have the correct setting for all ten wheels before text can be found. If the proper positions of but two pairs of wheels are found, it is possible to limit each letter of the plain text to one of eight possibilities and a part of the text may be guessed. This method will be fully illustrated later.

6. Determination of the initial key applicable to a series of messages. - a. The foregoing analysis is based upon the method of use of the machine in which the cipher wheels of the mixer are reset to a new keyword for each message to be enciphered. Another method of use is that in which the wheels are brought to an initial setting as determined by a keyword and messages are then enciphered sequentially without resetting the mixer wheels.

b. Given such a set of such messages, the procedure of analysis is more simple inasmuch as the endings of all the messages become available for study. Thus, suppose there are four sequent messages; instead of having but a single set of six characters available for study, four sets of six characters spaced at intervals corresponding to the lengths of the various messages are now at hand. The number of possible initial settings for the mixer wheels is thus greatly reduced, for generally only one can be found which will yield the requisite four sets of six characters properly spaced in the text.

c. If the group of messages studied does not begin with the initial one of the series, the procedure differs only in that a keyword can no longer be sought and used as a basis for eliminating possibilities. Even in such a case, however, the number of possibilities is very small; an actual test on four messages yielded but one possible setting for each pair of wheels. By proceeding backwards from the initial setting for this group of messages, the original keyword setting was found, even though the initial message of the sequence was not furnished.

7. Solution without the knowledge of any plain text. - a. It is possible to solve messages enciphered by this machine without making any assumptions about the plain text. The solution in this case rests on a frequency basis. It happens that the weighted frequencies of + and - units in the Baudot code are not equal. Thus, consider the first unit of each permutation in the code; 16 are + and 16 are -. If each of these +'s and -'s be weighted with the frequency of the character it represents, a relative frequency of .56 for + and .64 for - is obtained showing quite a discrepancy between the two. The same kind of calculation can be made for the other positions of the Baudot impulses. Figure 5 shows the complete tabulation. In every case but the third, the -'s predominate. This fact forms the basis of the solution.

Relative Frequency of + and - in Elements of Baudot Code
Based on 120,000 letters reduced to 1200 -- A.T.&T. Text.

1st		2nd		3rd		4th		5th	
+	-	+	-	+	-	+	-	+	-
A 72	C 55	A 72	B 11	C 55	A 72	B 11	A 72	B 11	A 72
B 11	G 16	C 55	D 40	F 30	B 11	G 55	E 126	G 16	C 55
D 40	H 33	G 16	E 126	H 33	D 40	D 40	H 33	H 33	D 40
E 126	I 76	I 76	F 30	I 76	E 126	F 30	I 76	L 36	E 126
F 30	L 36	J 2	H 33	K 3	G 16	G 16	L 36	M 25	F 30
J 2	M 25	K 3	M 25	M 25	J 2	J 2	P 27	O 74	I 76
K 3	N 76	L 36	N 76	N 76	L 36	K 3	Q 3	P 27	J 2
Q 3	O 74	P 27	O 74	P 27	O 74	M 25	S 58	Q 3	K 3
S 58	P 27	Q 3	S 58	Q 3	R 65	N 76	T 90	T 90	N 76
U 30	R 65	R 65	T 90	S 58	T 90	O 74	U 30	V 13	R 65
W 14	T 90	U 30	X 5	U 30	W 14	R 65	W 14	W 14	S 58
X 5	V 13	V 13	Y 21	V 13	Z 1	V 13	Y 21	X 5	U 30
Y 21	Z 180	W 14	Z 1	X 5	Z 10	X 5	Z 1	Y 21	S 180
Z 1	5 0	Z 10	S 180	Y 21	5 0	Z 10	S 180	Z 1	5 0
R 10	6 0	4 10	6 0	S 180	6 0	4 10	6 0	2 10	6 0
4 10	7 0	5 0	7 0	4 10	7 0	7 0	6 0	4 10	7 0
436	764	430	770	623	577	433	767	391	809
36.3%	63.7%	35.8%	64.2%	51.8%	48.2%	36.0%	64.0%	32.6%	67.4%

Fig. 5

b. Consider the following message[1]:

4 6 2 7 C 3 N 5 6 P K M I D Y 6 Q N 6 X A D K I W

I U T C E C I 5 J O 5 6 C N I Q F E Q 4 C 2 T I 5 . . . . .

[1] This was Message No. 4 of Set A. See footnote 1 to Page 8. The complete message will be found in Appendix B.

(1) Assign to each character of the message its Baudot equivalent, arranging the impulses in five columns to correspond to the five impulses of the Baudot code. Since the greatest difference in the relative frequencies exists in the fourth and fifth positions, let these two positions be considered first. Let a setting of wheels 9 and 10 be assumed such as will give a frequent digraph ending. Apply the resultant key thus obtained to the last elements of the Baudot equivalents using the laws of combination already described. The result is a series of ǂ's and -'s; find their relative frequency. If the relative frequency of -'s does not approximate the theoretical frequency, the setting is discarded and another tested. It was found by actual trial that the amount of text required for a definite result is not very great. In some cases sixty letters were found to be sufficient. Let the test message be followed in some detail.

4 6 2 7 0	[illegible]	K Z I D Y	6 Q Z 6 X	. . . . .
ǂ - ǂ - -	ǂ - ǂ - -	ǂ - - ǂ ǂ	- ǂ - - ǂ	
ǂ - - - ǂ	- - - - ǂ	ǂ - ǂ - -	- ǂ - - -	
ǂ - - - -	- ǂ ǂ - ǂ	ǂ ǂ ǂ - ǂ	- ǂ ǂ - ǂ	
ǂ - - ǂ ǂ	- ǂ - - -	ǂ ǂ - ǂ -	- - ǂ - ǂ	
ǂ - ǂ - ǂ	- - - - ǂ	- ǂ - - ǂ	- ǂ - - ǂ	

If the keyword is assumed to end in ZK, there results:

$0 - K_9$ ǂ - ǂ - ǂ - ǂ - ǂ - ǂ - ǂ - ǂ . . . etc.

$K - K_{10}$ - - - ǂ ǂ ǂ ǂ ǂ - - - - - ǂ . . . etc.

K_{r5} ǂ - ǂ ǂ - ǂ - ǂ - - ǂ - ǂ - - . . . etc.

The interaction of K_{r5} with C_5 yields:

K_{r5} ǂ - ǂ ǂ - ǂ - ǂ - - ǂ - ǂ - - . . . etc.

C_5 ǂ - ǂ - ǂ - - - ǂ - ǂ - - ǂ . . . etc.

P_5 - - - ǂ ǂ ǂ - ǂ - ǂ ǂ ǂ ǂ - ǂ . . . etc.

After sixty letters had been used, it was found that there were thirty ǂ's and thirty -'s. This seemed to be sufficient indication that ZK was wrong.

(2) The following table gives the frequencies obtained for the various endings tested:

	-	+	Total	Relative Frequency of Minus
OW	30	30	60	.50
NT	57	93	150	.38
ST	64	56	120	.53
HS	28	32	60	.47
AT	46	44	90	.50+
OR	28	32	60	.47
LE	46	44	90	.50+
SS	27	33	60	.45
ES	105	45	150	.70

Note how small an amount of text is needed to give reliable results.

(3) ES is obviously an excellent possibility. Assume it to be correct and proceed similarly with mixer-wheel pair 7-8. The number of possibilities is further limited in that now a good tetragraph ending is desired. The digraph TI is tried first:

	-	+	Total	Relative Frequency of Minus
TI	65	25	90	.72

(4) TIES is obviously an excellent possibility. Instead of carrying through this process now for the remaining wheels, the work can be shortened as follows:

(5) The key . . . TIES is applied to the last two elements of the Baudot equivalents obtaining for the first fifteen characters:

4 - + - - + + - + + - - - - - + ...

5 - - - + + - - + - - + + - - - . . . . .

(6) Only eight letters can correspond in each case to the combination obtained.

(7) Write these sets in their proper order.

4 - + - - + + - + + - - - - - + ...

5 - - - + + - - + - - + + - - - . . . . .

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

(8) After some search it was found that the message began EDITORSOFSTATE ... . Now the first method outlined under Paragraph 5 is applied to find the complete keyword, which is found to be PRINTING.

c. The procedure is similar for a series of messages.