

WAR DEPARTMENT
OFFICE OF THE CHIEF SIGNAL OFFICER
WASHINGTON

January 29, 1934

Mr. David A. Salmon,
Chief, Division of Communications
and Records,
Department of State,
Washington, D. C.

Dear Mr. Salmon:

In accordance with the Chief Signal Officer's reply to your letter of January 16, I am sending you a permutation table and instructions pertaining thereto. This table is constructed according to our latest principles and will provide a set of 150,000 five-letter code groups embodying the two-letter difference and nontransposability features throughout.

Very truly yours,

William F. Friedman,
Chief of Signal Intelligence Section.

Attached:
Table and
instructions.

Section 2. - Second Letter

Section 1. - First Letter

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

26

210

29
607
574
607

560 - 40

520

500

78x2

560
40
520

(2)

$$6 \times 520 = 3120 \times 3 = 9360$$

$$7 \times 520 = 3640 \times 8 = 29120$$

$$8 \times 520 = 4160 \times 8 = 33280$$

$$9 \times 520 = 4680 \times 4 = 18720$$

$$10 \times 520 = 5200 \times 1 = 5200$$

$$11 \times 520 = 5720 \times 4 = 22880$$

$$12 \times 520 = 6240 \times 1 = 6240$$

$$29 \times 124800$$

$$6 \times 500 = 3000 \times 111 = 9000$$

$$7 \times 500 = 3500 \times 111 = 24500$$

$$8 \times 500 = 4000 \times 111 = 28000$$

$$9 \times 500 = 4500 \times 111 = 13500$$

$$10 \times 500 = 5000 \times 1 = 5000$$

$$11 \times 500 = 5500 \times 111 = 22000$$

$$12 \times 500 = 6000 \times 1 = 6000$$

$$108000$$

$$12480$$

$$120480$$

$$7 \times 520 = 3640 \checkmark$$

$$8 \times 520 = 4160 \checkmark$$

$$9 \times 520 = 4680 \checkmark$$

$$12480$$

$$\begin{array}{r}
 607 \\
 \underline{18} \\
 4856 \\
 \underline{607} \\
 10926 \\
 \underline{1214} \\
 12140 \\
 \\
 10926 \\
 \underline{607} \\
 11533
 \end{array}$$

$$\begin{array}{r}
 11514 \\
 \underline{606} \\
 10908
 \end{array}$$

$$\begin{array}{r}
 10926 \\
 \underline{607} \\
 10313
 \end{array}$$

$$\begin{array}{r}
 604 \\
 \underline{18} \\
 4832 \\
 \underline{604} \\
 10872
 \end{array}$$

$$\begin{array}{r}
 603 \\
 \underline{17} \\
 4221 \\
 \underline{603} \\
 10251
 \end{array}$$

$$\begin{array}{r}
 10872 \\
 \underline{604} \\
 10268
 \end{array}$$

$$\begin{array}{r}
 10872 \\
 \underline{604} \\
 10268
 \end{array}$$

$$17 \times 607 = 10319$$

$$18 \times 607 = 10926$$

$$17 \times 607 = 10319$$

$$18 \times 607 = 10926$$

$$17 \times 605 = 11461$$

$$18 \times 607 = 10926$$

$$17 \times 607 = 10319$$

$$18 \times 607 = 10926$$

$$17 \times 604 = 10268$$

$$18 \times 606 = 10908$$

$$17 \times 607 = 10319$$

$$19 \times 607 = 11533$$

$$17 \times 607 = 10319$$

$$19 \times 604 = 11476$$

$$24 \times 26 = 624$$

$$25 \times 22 = 550$$

$$24 \times 23 = 552$$

$$23 \times 24 = 552$$

$$25 \times$$

$$\begin{array}{r} 676 \\ 640 \\ \hline 27040 \\ 4056 \\ \hline 432640 \end{array}$$

$$\begin{array}{r} (18 \times 676) \\ 60 \\ \hline 607 \\ 676 \end{array}$$

$$18 \times 607 = 10926$$

$$20 \times 607 = 12140$$

$$19 \times 607 = 11533$$

$$19 \times 606 = 11514$$

$$19 \times 605 = 11495$$

$$18 \times 606 = 10908$$

$$19 \times 606 = 11514$$

$$17 \times 606 = 10302$$

$$18 \times 604 = 10872$$

$$17 \times 603 = 10251$$

$$19 \times 607 = 11533$$

$$17 \times 607 = 10319$$

$$18 \times 607 = 10926$$

$$17 \times 603 = 10251$$

$$18 \times 604 = 10872$$

with 20 envelopes

7X607 = 4249	7.493 3451	6X607 = 3642	6.493 2958
7X607 = 4249	7.493 3451	9X607 = 5463	9.493 4437
11X607 = 6677	11.493 5423	12X604 = 7248	12.490 5880
10X607 = 6070	10.493-4930	7X606 = 4242	7.492 3494
7X605 = 4235	7.491-3437	8X607 = 4856	8.493 3944
8X606 = 4848	8.492-3936	7X607 = 4249	7.493 3451
8X606 = 4848	8.492-3936	8X607 = 4856	8.493 3944
11X606 = 6666	11.4925412	9X604 = 5463	9.490 4910
6X604 = 3624	6.490-2940		
7X607 = 4221	7.489. 3423		
7X607 = 4249	7.493. 3451		
11X607 = 6677	11.493. 5423		
8X607 = 4856	8.493. 3944		
8X603 = 4824	8.489. 3912		
7X604 = 4228	7.490 3430		
9X607 = 5463	9.493 4437		
8X607 = 4856	8.493 3944		
9X607 = 5463	9.493 4437		
6X604 = 3624	6.490 2940		
11X605 = 6655	11.491 5401		
8X607 = 4856	8.493 3944		

145,457

603 ||
604 ###
605 ||
606 ||||
607 ####

Handwritten calculations on lined paper:

Top left:
$$\begin{array}{r} 21 \\ 20 \\ \hline 580 \\ 87 \\ \hline 493 \end{array}$$

Top right:
$$\begin{array}{r} 29 \\ 29 \\ \hline 580 \\ 87 \\ \hline 1160 \\ 4640 \\ \hline 51360 \end{array}$$

Middle left:
$$\begin{array}{r} 39 \\ 60 \\ \hline 3944 \end{array}$$

Middle right:
$$\begin{array}{r} 106 \\ 106 \\ \hline 3642 \\ 607 \\ \hline 9712 \\ 2424 \\ \hline 1210 \\ 3020 \\ \hline 1206 \end{array}$$

Bottom left:
$$\begin{array}{r} 2940 \\ 604 \\ \hline 3544 \end{array}$$

Bottom right:
$$\begin{array}{r} 29 \\ 17572 \\ \hline 174 \end{array} \quad (606)$$

6 III 18 240 60 39 4
 7 III 56
 8 III 64
 9 III 36 2940 604 354 6 3 8 2
 10 I 10
 11 III 44
 12 I 12
 29) 240 (82
 8 23 ~
 80
 49 1
 49 1
 49 1
 540 1

CORRECTION OF ERRORS

	Paragraph
Sources of errors	1
Types of garbles	2
The error corrector table and the two-letter difference	3
Types of errors	-
Correcting errors of the substitution type	4
Correcting errors of the transposition type	5
Correcting other types of errors	6
Service messages	7

1. Sources of errors. - Garbles or mutilations in the text of cryptograms come from two sources:

a. Errors made in encoding, or enciphering, or copying. - These errors are avoidable by the exercise of great care on the part of those preparing dispatches which is the best safeguard against most of the most serious errors made in communication - those made at the source. Where time permits, every dispatch should be verified; that is, deciphered and decoded from the final typed copy by someone other than the person who originally prepared the message, before it is filed for transmission. It is not a reliable check merely to encode or encipher a second time, because the same error is very likely to be repeated; the reverse process, complete decoding, is certain to disclose any errors and will insure that the final dispatch is correct. When this is impracticable, the dispatch should be verified after it has been filed, and any errors noted should be corrected and the addressee notified. If the errors merely involve a very limited number of single letters, a correction message may be sent; but if the error is of a serious nature, such as the use of the wrong code or cipher, the entire dispatch should be carefully paraphrased by the originator of the dispatch; if this is impossible, then the paraphrasing should be done by the commanding officer of the transmitting message center, and prepared anew.

b. Errors made in transmission or reception. - These are unavoidable so far as the person who prepared the dispatch is concerned, and constitute by far the greatest proportion of simple errors encountered.

2. Types of garbles. - a. Garbled or mutilated letters in a code message are of three types:

- (1) Substitutions of incorrect letters for the correct ones.
- (2) Transpositions of the members of a pair of correct letters.
- (3) Omissions and additions of letters.

b. By far the most common errors are of the first type, and it is fortunately true that it is unusual for an operator to make more than a single such error in a group of five letters.

3. The error corrector table and two-letter differences. - 1. The code groups employed in this code were constructed by means of the chart shown as an insert at the end of the book. Such a chart is often called a "permutation table", "code word construction table", "a garble table", etc. In these instructions it will be referred to as the ERROR CORRECTOR TABLE because it has been included in the code in order to assist in the correction of errors.

b. The error corrector table for this code consists of five sections:

Section 1. A single column of 26 letters, from which the initial letters are taken.

Sections 2, 3, and 4. Three intermediate squares of letters (with certain blank spaces), from which the second, third, and fourth letters, respectively, are taken in turn.

Section 5. A single row of 26 letters, from which the final letters are taken.

c. The basic principle in using this table to construct code words in composing a code is that each of its five sections contributes one and only one letter to the formation of the word and that in selecting the successive letters one always proceeds in straight lines. For example, suppose the initial letter selected is A, the first letter in Section 1. We may then select any one of the letters on the same line with A but in Section 2; suppose we select F, giving AF as the initial pair of letters of the code group being constructed. We then proceed down the column in which F is located, directly into Section 3 and select the third letter, for example O, giving AFO as the initial trigraph of the code group. We then go to the right into Section 4, straight along the line in which the O we selected is located and select a

fourth letter. Suppose we select C, giving the four letters AFQC. We then have available as the fifth letter only one letter, namely, that which, in Section 5 is directly above the C we selected. In this case the letter is E, giving the complete group AFQCE.

d. With AFO as the initial trigraph we may construct, besides AFQCE, a series of 22 code groups all differing from one another in the last two letters, for example, AFQHA, AFQNB, AFQCC, etc. Or, with QCE as the final trigraph we may have, besides AFQCE, a series of 81 code groups all differing from one another in the first two letters, for example ENJCE, IVQCE, MAJCE. Consideration of this method of construction will show that when the letters are combined in the manner indicated, the resulting code groups must all differ from one another in at least two letters. This is referred to as the "two-letter differential", and it is of great assistance in correcting errors when they occur as the result of mistakes in writing, copying, transmission, or reception.

4. Correcting errors of the substitution type. - a. Single-letter substitutions are by far the most usual of all types of errors, and their correction is quite simple when the code groups are constructed upon the two-letter difference principle. The method will be illustrated by an example.

b. Suppose the code groups DOSCU appears in a dispatch in the position shown below and is not found listed in the decoding volume:

...

DOSCU

...

?

The error may be in any one of the five letters of DOSCU, and by changing them one at a time, a maximum of five possibilities for the correct group will be found. The group is written down five times, leaving a blank space for the letter that is assumed to be incorrect in each case. Thus:

	(1)	- O S C U
	(2)	D - S C U
DOSCU	(3)	D O - C U
	(4)	D O S - U
	(5)	D O S C -

- (1) Assuming the first letter, D, to be wrong, the process consists in finding the correct letter to be inserted in the group -OSCU. Refer

to the error corrector table and in Section 5, beginning with U, we find, by following the successive letters C, S, and O, in Sections 4, 3, and 2, respectively, that the first letter should be B, giving the group BOSCU as a possibility.

- (2) Assuming the second letter, O, to be wrong, the procedure in finding the missing letter in D-SCU is exactly the same as under (1) above except that we now must locate the second letter of the group, given the first, third, fourth and fifth. By following U, C and S, in Sections 5, 4, and 3, respectively, and then finding the letter in Section 2 which is at the intersection of the horizontal line in which D is located in Section 1 and the vertical column in which the S is located in Section 3, we find a blank in the table which indicates that if only one letter in the group DOSCU is wrong, it is not the second.
- (3) Assuming the third letter, S, to be wrong, the procedure in correcting DO-CU consists in finding that letter in Section 3 which lies at the intersection of the vertical line determined by following the letters D and ^O in Sections 1 and 2, respectively, and the horizontal line determined by following the letters U and C in Sections 5 and 4, respectively. This letter is K, giving DOKCU as a third possibility.
- (4) Assuming the fourth letter, C, to be wrong, the procedure in correcting DOS-U is obvious. We follow the letters D, O, and S in Sections 1, 2, and 3 respectively, then find the letter in Section 4 which lies at the intersection of the horizontal line thus determined, with the vertical column in which U is located in Section 5. In this case, we find a blank in the table, which indicates that if only one letter in the group, DOSCU is wrong, it is not the fourth.
- (5) Assuming the fifth letter, U, to be wrong, the procedure shows that it should be Z, giving DOSCZ as a possibility.

g. The meaning of each of the possibilities is then found and that one is selected which best fits the context. Thus:

- (1) - O S C U = B O S C U =
 (2) D - S C U = (No group possible)
 D O S C U = (3) D O - C U = D O K C U =
 (4) D O S - U = (No group possible)
 (5) D O S C - = D O S C Z =

Here it is seen that the requirements of the context are met by selecting as the correct group, yielding the following:

...

...

...

...

d. If all attempts to correct an error assumed to be of the single-letter substitution type have resulted in failure or doubt, the next step is to assume that an error of the transposition type is involved. This is explained in detail in paragraph 5.

5. Correcting errors of the transposition type. - a. A rather common error, usually made in copying, is to transpose the members of a pair of letters; that is, two letters, both correct, exchange positions in the group. Ten such transpositions are possible in a 5-letter group, as follows:

- Type (1) - 1st and 2d
 (2) - 2d and 3d
 (3) - 3d and 4th
 (4) - 4th and 5th
 (5) - 1st and 3d
 (6) - 2d and 4th
 (7) - 3d and 5th
 (8) - 1st and 4th
 (9) - 2d and 5th
 (10) - 1st and 5th

b. The table from which the code words of this code have been constructed is of such character that even if two letters in a group become transposed, the resulting code group will not be a bonafide group and hence will not be found in the decoding section. On the other hand, if a code group as received

does contain an error of this sort, transposing the proper letters will uncover it. The procedure is quite simple. The first step in correcting an error is to assume that a single-letter error of the substitution type is involved and proceed as shown under paragraph 4. If this results in failure, or gives a correction of doubtful validity, the next step is to assume that a transposition is involved, make the proper transposition of each type shown above, and see if any of the resulting groups are in the decoding section. If one is found so listed, with a meaning that well fits the context, it may be assumed to be correct.

g. An example may serve to make the procedure more clear. Suppose the group RICKK has been received, found to be incorrect, and tests for a single-letter error have given no good results. The ten possible transpositions are written down, thus:

IRCKK RICKK CIRCK RIKCK RIKCI RCIKK RICKO RCKIK OICCK KICOR

One and only one of the foregoing ten groups will be found on reference to the error corrector table, viz., the group RIKCK. The meaning of this group is then sought in the decoding section, and if it fits well with the context, may be taken to be correct.

6. Correcting other types of errors. - a. Since all the code groups contain five letters, the omission or addition of a letter is at once noted. This type of error is most often due to the false grouping of the characters of the Morse telegraph code by the receiving operator. By reference to the error corrector tables and to the table of most common telegraphic errors, shown on page 000 of the decoding section, the majority of such garbles can be corrected.

b. Occasionally attempts to correct a garbled group by assuming a single error of the substitution type or an error of the transposition type result in failure to find a suitable group. In such cases, if the situation is urgent, and it would delay action to wait for a service message (par. 7), attempt should be made to correct an apparent error by assuming that two letters have been garbled in transmission. The most natural assumption is to consider that two sequent letters have been changed by a false grouping of Morse signals. Assuming the first three letters to be correct, the last two can be found by reference to

the error corrector table; or, assuming the third, fourth, and fifth letters to be correct, the first and second can be found. It is not usual that a 2-letter mutilation should involve letters that are not adjacent; however, as a last resort, in the absence of success in other directions, one may assume errors of the substitution type involving two separated letters. In every case, however, the corrections involving two letters should be regarded as tentative, until servicing of the message in question verifies the corrections made.

g. When cipher tables are employed to give added cryptographic security, errors of a different nature are likely to be introduced, such as those occasioned by the incorrect substitution of letters, by the use of incorrect alphabets and incorrect indicators, by failure to show changes in alphabet sequences when necessary, etc. A proper understanding of the mechanics of the cipher system employed is necessary for the correction of errors introduced from this source.

7. Service messages. - In a difficult case, where a dispatch is so badly mutilated that neither the error corrector table nor the table of telegraphic errors gives an unmistakable meaning to the mutilated dispatch, or when doubt still exists as to the accuracy of a dispatch, several groups of which have had to be corrected, a service message should be requested. This is, in effect, a request that the mutilated group or groups be repeated from the point of origin, which should result in disclosing errors made in the previous transmission.