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 1. - First Letter

| 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 |
| 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 |

Section 2. - Second Letter

| 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 |
| 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 |

REF ID:A67392
<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>$6 \times 570$</td>
<td>$= 3420 \times 3$</td>
<td>$= 9260$</td>
</tr>
<tr>
<td>$7 \times 570$</td>
<td>$= 3990 \times 8$</td>
<td>$= 29120$</td>
</tr>
<tr>
<td>$8 \times 570$</td>
<td>$= 4560 \times 8$</td>
<td>$= 36280$</td>
</tr>
<tr>
<td>$9 \times 570$</td>
<td>$= 4500 \times 4$</td>
<td>$= 18720$</td>
</tr>
<tr>
<td>$10$</td>
<td>$= 5000 \times 1$</td>
<td>$= 5000$</td>
</tr>
<tr>
<td>$11$</td>
<td>$= 5700 \times 4$</td>
<td>$= 22880$</td>
</tr>
<tr>
<td>$12$</td>
<td>$= 6240 \times 1$</td>
<td>$= 6240$</td>
</tr>
<tr>
<td>$9$</td>
<td>$= 174800$</td>
<td></td>
</tr>
<tr>
<td>$6 \times 500$</td>
<td>$= 3000 \times 111$</td>
<td>$= 99300$</td>
</tr>
<tr>
<td>$7 \times 500$</td>
<td>$= 3500 \times 111$</td>
<td>$= 245500$</td>
</tr>
<tr>
<td>$8 \times 500$</td>
<td>$= 4000 \times 111$</td>
<td>$= 280000$</td>
</tr>
<tr>
<td>$9 \times 500$</td>
<td>$= 4500 \times 111$</td>
<td>$= 135000$</td>
</tr>
<tr>
<td>$10 \times 500$</td>
<td>$= 5000 \times 1$</td>
<td>$= 50000$</td>
</tr>
<tr>
<td>$11 \times 500$</td>
<td>$= 5500 \times 111$</td>
<td>$= 22000$</td>
</tr>
<tr>
<td>$12 \times 500$</td>
<td>$= 6000 \times 1$</td>
<td>$= 60000$</td>
</tr>
<tr>
<td>$108000$</td>
<td>$= 12480$</td>
<td>$= 120480$</td>
</tr>
</tbody>
</table>
\[
\begin{align*}
24 \times 24 &= 576 \\
55 \times 2 &= 110 \\
24 \times 3 &= 72 \\
13 \times 24 &= 312 \\
\end{align*}
\]

\[
\begin{align*}
676 \\
640 \\
27040 \\
4056 \\
13216 \\
\end{align*}
\]
<table>
<thead>
<tr>
<th>Calculation</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>$7 \times 60 = 420$</td>
<td>$420$</td>
</tr>
<tr>
<td>$7 \times 6 = 42$</td>
<td>$42$</td>
</tr>
<tr>
<td>$11 \times 6 = 66$</td>
<td>$66$</td>
</tr>
<tr>
<td>$10 \times 6 = 60$</td>
<td>$60$</td>
</tr>
<tr>
<td>$7 \times 6 = 42$</td>
<td>$42$</td>
</tr>
<tr>
<td>$8 \times 6 = 48$</td>
<td>$48$</td>
</tr>
<tr>
<td>$8 \times 6 = 48$</td>
<td>$48$</td>
</tr>
<tr>
<td>$11 \times 6 = 66$</td>
<td>$66$</td>
</tr>
<tr>
<td>$6 \times 4 = 24$</td>
<td>$24$</td>
</tr>
<tr>
<td>$7 \times 6 = 42$</td>
<td>$42$</td>
</tr>
<tr>
<td>$11 \times 6 = 66$</td>
<td>$66$</td>
</tr>
<tr>
<td>$6 \times 4 = 24$</td>
<td>$24$</td>
</tr>
<tr>
<td>$9 \times 6 = 54$</td>
<td>$54$</td>
</tr>
<tr>
<td>$9 \times 6 = 54$</td>
<td>$54$</td>
</tr>
<tr>
<td>$6 \times 4 = 24$</td>
<td>$24$</td>
</tr>
<tr>
<td>$11 \times 4 = 44$</td>
<td>$44$</td>
</tr>
<tr>
<td>$8 \times 6 = 48$</td>
<td>$48$</td>
</tr>
<tr>
<td>$9 \times 6 = 54$</td>
<td>$54$</td>
</tr>
<tr>
<td>$6 \times 4 = 24$</td>
<td>$24$</td>
</tr>
<tr>
<td>$11 \times 4 = 44$</td>
<td>$44$</td>
</tr>
<tr>
<td>$8 \times 6 = 48$</td>
<td>$48$</td>
</tr>
<tr>
<td>$9 \times 6 = 54$</td>
<td>$54$</td>
</tr>
<tr>
<td>$6 \times 4 = 24$</td>
<td>$24$</td>
</tr>
<tr>
<td>$11 \times 4 = 44$</td>
<td>$44$</td>
</tr>
</tbody>
</table>

**Total:** $1457$
CORRECTION OF ERRORS

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

2. Errors made in encoding, or deciphering, or copying. — These errors are avoided by the exercise of great care on the part of those preparing dispatches which is the best safeguard against most of the more 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 decipher 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 addressess 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.

3. 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.

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 difference. - 3. 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 in-
structions 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.

4. 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.

5. 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 AFOC. 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 this letter is E, giving the
complete group AFOCE.

4. With AFO as the initial trigraph we may construct, besides AFOCE, a
series of 22 code groups all differing from one another in the last two letters,
for example, AFOL, AFONE, AFOOC, etc. Or, with OCE as the final trigraph we
may have, besides AFOCE, a series of 8 code groups all differing from one
another in the first two letters, for example ENJO, IVOM, MAJO. 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.

tions 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) DOSCU
(2) DSCU
(3) DSCU
(4) DSCU
(5) DSCU
```

(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 E, giving the group DOSGU as a possibility.

(2) Assuming the second letter, O, to be wrong, the procedure in finding
the missing letter in D-SGU 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 filling in 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 U 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 DOSGU 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 the letter in Section 3 which lies at the
intersection of the vertical line determined by following the
O letters D and 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 DOSCU as a third possibility.

(4) Assuming the fourth letter, C, to be wrong, the procedure in cor-
recting 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 deter-
mined, 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 DOSGU 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 DOSZU as a possibility.

9. The meaning of each of the possibilities is then found and that one is
selected which best fits the context. Thus:
(1) \(-\text{OSC} = \text{BOSCU}\) =
(2) \(-\text{DSCU} = \text{(No group possible)}\)
\(\text{DOSCU} = \text{(3) \text{DSCU = DOKCU}}\) =
(4) \(-\text{DOSU} = \text{(No group possible)}\)
(5) \(-\text{DOSC} = \text{DOSCZ} =

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

```
* * *
* * *
* * *
* * *
```

4. 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 ex-
plained 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 bona fide 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 will fit the context, it may be assumed to be correct.

2. An example may serve to make the procedure more clear. Suppose the group RICOK 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:

IRK RIKC CKIR KROC ROCIK KRCIO KCOIR CIRKO KORCI

One and only one of the foregoing ten groups will be found on reference to the error corrector table, viz., the group RIKOC. 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.

3. Correcting other types of errors. 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.

4. 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 thirty-fourth and fifty 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 sequent; 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.

9. 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 make 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.