A Method of Reconstructing the Primary Alphabet From a Single One of the Series of Secondary Alphabets

William F. Friedman

Publication No. 15

RIVERBANK LABORATORIES
DEPARTMENT OF CIPHERS
RIVERBANK
GENEVA, ILL.
1917

A Method of Reconstructing the Primary Alphabet From a Single One of the Series of Secondary Alphabets

In a modified Vigenère table, that is, one in which a key-word followed by the rest of the unused letters of the alphabet is employed instead of the straight direct alphabet, it is possible to derive a series of twenty-five mixed alphabets. We will designate the "masterkey" alphabet, that is, the one containing the key-word and on which the table is based, as the *primary alphabet*, and the alphabets resulting from the table as the *secondary alphabets*.

The following is an example of such a table and its method of use, employing the key-word "Stenography":

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

To encipher the words "General Pershing has" etc., using the key-word CARGO, in accordance with the well-known original Vigenère method, viz. finding at the top the key letter, at the left side the text letter, and taking the letter at the intersection of the vertical and horizontal columns as the cipher letter, we have:[1]

```
key letter .... C A R G O   C A R G O   C A R G O   C A R
plain text .... G E N E R   A L P E R   S H I N G   H A S
cipher ........ K H H A Y   M Z F A Y   C J U P H   U F R
```

Now for each different key letter in the encipherment of a message a different one of the series of the twenty-five alphabets is employed; e.g., in the case of the above key-word CARGO, in the C alphabet, T is enciphered by D, E is enciphered by F, G by K, etc.; the next key letter being A, T is enciphered by P, E by H, N by Y, etc.

Considering the primary alphabet as partaking of the nature of a disk or wheel, each line of the table, consisting of exactly the same sequence of letters, is a repetition of the preceding line, removed one place to the left. It is therefore possible to produce every one of the secondary alphabets by the use of two strips of paper upon which the

[1] It is possible, of course, to use a square table in several other ways, but whatever the method, any cipher message enciphered by the use of a key-word and square table, may be deciphered by a multi-alphabet system, and therefore, the present principles of finding the primary alphabet are applicable to all.

same primary alphabet appears, sliding one beneath the other, one place at a time, thus producing consecutively the twenty-five secondary alphabets. For example, using the same primary alphabet as above, placed on two strips of cross-section paper, and sliding S of the lower strip one space to the left, we have:[2]

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

Considering the lower strip to represent the plain text, the entire Z secondary alphabet of the table can be produced from the above relative positions of the sliding alphabets, and is as follows, for enciphering:

```
(1) 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
    R Y B C T D O P F I J K L E N A M G Z S Q U V W H X
```

For deciphering however, this alphabet would be written thus:

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

Given this secondary alphabet it is possible to recover the primary by the following method:

Write the numerical sequence from 1 to 26, using, preferably, cross-section paper so as to have the spaces between the letters the same. Starting with the letter A, which equals P, place P under the space No. 1; under space No. 2, place the equivalent of P, which is H; under space No. 3 place the equivalent of H, which is Y; under space No. 4, place the equivalent of Y, which is B, etc., thus:

```
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26
P H Y B
```

This procedure results in the reconstruction of the primary alphabet, thus:

```
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26
P H Y B C D F I J  K  L  M  Q  U  V  W  X  Z  S  T  E  N  O  G  R  A
```

In working out this example we placed the equivalent of each letter right next to the letter itself as each was determined in order. This was because the cipher letters and the plain text letters were one space removed from each other in the sliding strips when the Z secondary alphabet is used. In other words, the alphabets were one place removed from each other. If they had been removed two places from each other, then we should have every time to leave *one* space between a letter and its equivalent; when three places removed, then *two* spaces should have to be left; when four places removed, *three* spaces etc., in short when n places removed, then $n - 1$ spaces should be left. Thus given the enciphering alphabet as follows:

```
(3) 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
    G N Y B S C N A D F I J K T E R L O X Z M Q U V P W
```

and the resulting deciphering alphabet:

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

To find the primary alphabet, place the equivalent of A, which is H, in space No. 1; then place the equivalent of H, which is B, one space removed from H, that is, in space No. 3; place the equivalent of B, which is D, in space No. 5, etc., thus:

```
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26
H   B   D   I   K    M    U    W    Z    T    N    G    A
```

When we have reached the point G equals A, we find that our determined sequence begins to repeat itself, since A equals H. To continue the procedure, we assume that a

[2] In actual practice one of the alphabets on the sliding strips should be double in length in order to secure coincidence of plain text and cipher-equivalent letters no matter where set.

sequence such as FG, JK, PQ, VWXYZ is not interrupted by the key-word in the primary alphabet. We then experiment on this basis by placing, for example in the case above, the letter J in the space No. 8 and continue as before, placing the equivalent of J, which is L, in space No. 10, etc. Thus the primary alphabet is again reproduced completely.

```
 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26
 H Y B C D F I J K  L  M  Q  U  V  W  X  Z  S  T  E  N  O  G  R  A  P
```

It follows then that to recover the primary alphabet from any one of the secondary alphabets, it will be necessary to leave as many spaces between each cipher letter of the secondary alphabet and its equivalent plain text letter, as the number of places the primary alphabets have been removed from each other. In other words, if n represents the number of places the primary alphabets were shifted, then in recovering the primary from any secondary alphabet, the primary alphabet will appear when the equivalent of each letter of that particular secondary alphabet has been put in the $n-1$ place from the letter itself. Reduced to the form of an equation:

If $n =$ the number of places the primary alphabet has been shifted;
then $n-1 =$ the number of spaces which should be left between each letter of a secondary alphabet and its equivalent;
or $n-1 =$ the number of the place into which is put the equivalent of any letter counting from that letter.

Now in actual practice two things are true with respect to the above:

1. no secondary alphabet will carry in itself any indication whatever as to its position in the table, that is, the number of spaces the primary alphabets have been shifted (with one exception to be discussed later);
2. hardly ever will any secondary alphabet be complete except in deciphering a very long message.

In practice therefore, the recovery of a primary alphabet will not be so simple as in the above cases, but will necessitate considerable experiment, for which the following two principles may serve as guiding points:

1. A sequence of determined letters must be either a pronounceable combination, thus being part of the key-word; or
2. A sequence of determined letters must follow the normal straight alphabetical sequence interrupted by those letters which have been incorporated in the key-word. That is, a sequence such as GHKLN is entirely possible and indicates that I, J and M are present in the key-word, while the sequence such as HGKNL is impossible and indicates that we have not left the proper number of spaces between letters and their equivalents.

In order to illustrate the above points we will work out an example. Given the deciphering alphabet:

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

The tabulated results are as follows:

```
           1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26
1st trial: N Q B
2nd trial: N   Q   B   T
3rd trial: N D   Q V   B     T       R       O       C       U       L
4th trial: N   U   Q       B           T           R           O           C
5th trial: N         Q           B             T             R
6th trial: N       O   Q         C     B           U     T           L     R
7th trial: N   R         Q    O             B     C             T
8th trial: N           R   Q                 O     B               C     T
9th trial: N T C D             Q  R  U  V                 B  O  L  I
```

At the ninth trial we are beginning to see a possible portion of a key-word, together with two other normal sequences save for interruptions. A continuation of this leads to the completion of the primary alphabet which is as follows:

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

and the key-word is ABOLISHMENT.

It is possible to reconstruct completely by the exercise of some ingenuity, a primary alphabet from a partial secondary in which as many as ten or twelve letters are missing. Given the following partial deciphering alphabet:

```
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
V R   P A M O   U S B F G H   T I   E   D   L N
```

the following letters are missing: C J K Q W X Y Z. The first thing to do is to find the longest sequence of equivalents, which in this case begins with Q. Going through all the steps as before, we get no good results until we have left about 19 or 20 spaces between letters and equivalents, when the sequence in the primary alphabet begins to assume a nearly normal appearance. At 20 spaces interval the sequence of some of the letters is such as to make us certain that we are on the right track at last.

```
              1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26
 1st trial: Q I U D P T
10th trial: Q       D             I           P                U           T
18th trial: Q   D                 U     T                 I     P
20th trial: Q T         P             D             U              I
```

This is as far as we can get with our first unbroken sequence. Our next longest sequence of equivalents begins with J. Now if in the primary alphabet the sequence IJ is unbroken, then J would follow I in the last of the above trials and the letters determined from this start should agree with those already placed.

```
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26
Q T V       P A           D  E           U  S           I  J
```

The next longest sequence of equivalents begins with W, and we will assume that the VW sequence is unbroken in the primary alphabet, which means that we should place W after V in the tentative primary alphabet.

```
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26
Q T V W     P A    H     D  E     M     U  S     F     I  J     L
```

The next sequence of equivalents begins with X, which we will place after W.

```
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26
Q T V W X   P A    H     D  E     M  O  U  S     F  G  I  J     L  N
```

The remaining letters are easily placed and the whole sequence is now completed.

```
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26
Q T V W X Z P A C  H  Y  D  E  R  M  O  U  S  B  F  G  I  J  K  L  N
```

The key-word is PACHYDERMOUS.

Sometimes a continuance of the sequence may be found by going backward instead of forward. Many possibilities will suggest themselves to the ingenious decipherer.

One and only one of the series of twenty-five secondary alphabets carries with it a number which indicates its position in the table, viz., the 13th, which is what may be called a *reciprocal* alphabet, in which for example plain text letter A equals R and plain text letter R equals A. In working out the primary alphabet from this particular secondary

alphabet, it is necessary to assume parts of unbroken sequences such as BC, FG, JK, PQ, VWXYZ, and remove their equivalents 13 spaces right from the start, since in a table such as is being discussed the 13th secondary alphabet is *always* a reciprocal alphabet. The following is an example:

```
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
N   G   T         O M R   A   X D L U E S H I P
```

The first step would be to fill in as many of the missing values as possible. If J is O, then O is J; if V is H, then H is V, etc. The alphabet, as nearly complete from the values given as possible, is as follows:

```
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
N   G Q T   C V W O M R K A J X D L U E S H I P
```

We first assume that the UVWXYZ sequence is unbroken and what is probably a portion of the key-word SHIP, are 13 spaces apart. Thus:

```
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26
            S H I P     F G J                 U V W X Y Z
```

If our key-word ends in SHIP and if B is not a part of it, then B would be likely to follow P, and 13 spaces in advance would bring Y as its equivalent, which is very good. The only unfilled letters are Z and F. Placing F next to B brings Z in proper position. After F may come G, which would give C as the first letter of the key-word; after G must come J, which gives O as the second letter of the key-word; since H and I are already a part of the key-word. Thus, step by step the whole primary alphabet is reconstructed.

```
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26
C O M R A D E S H  I  P  B  F  G  J  K  L  N  Q  T  U  V  W  X  Y  Z
```

It has been shown repeatedly that the method of enciphering by means of the Vigenère table, the so-called "Chiffre indeschiffrable", is easily attacked by the ordinary principles and rules of deciphering. The above method of recovering or reconstructing the primary alphabet is an addition to deciphering methods which will not only save months of labor, but will also furnish a means whereby enemy messages may be deciphered exactly as rapidly as by the intended recipient himself.

Exercises

Solve the following examples:

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

(2) 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  English
      P R U Y C K X W H S E A T D F   I   B Q L V M N O

(3) 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  German
    J Z   M O A N   E R L Q U K S T B P   Y V C I   G H

(4) 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  French
    G A   C F   L   N P   S T V U   Y     B H O R I D E

(5) 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  Spanish
    U   T M P E   I R   A N L     O S B Y D   G   Q
```