BUREAU OF SECURITY AND SIGNALS INTELLIGENCE (BOSS)

DEPARTMENT OF STANDARDS AND PRACTICES

REPORT SP-013

METHODS OF MIXING KEYS

There are several ways to mix a key alphabet by use of a keyword. It is, of course, necessary that both sender and receiver of an encrypted message agree on the method. Both also must agree on the placement of special characters in the unmixed alphabet, in cases where the alphabet has more than twenty-six characters. Typically, space comes before letters, and digits and other character after letters.

1. RANDOM MIXING

Key alphabets can be deranged randomly. In this case, cipher operators must carry a code book.

2. CLASSICAL METHODS

Classically, we write the keyword and follow it by the remainder of the alphabet. However, there are many options.

- The keyword can be placed at the beginning:

  KEYWORD*ABCFGHIJLMNPQSTUVXZ

- The keyword can be placed at the end. We do not recommend this option for simple substitution ciphers, since the letters at the beginning of the alphabet are used more frequently than those at the end; this option introduces a weakness into the cipher.

  ABCFGHIJLMNPQSTUVXZ*KEYWORD

- The remaining letters are in forward order:

  KEYWORD*ABCFGHIJLMNPQSTUVXZ

- The remaining letters are in reverse order:

  KEYWORD*ZXVUTSQPNMLJIHGFCBA

- The remaining letters are written beginning from the start (or end if reversed):

  KEYWORD*ABCFGHIJLMNPQSTUVXZ

- The remaining letters are written beginning from the letter that is alphabetically next after the last letter of the keyword:

  KEYWORD*FGHIJLMNPQSTUVXZABC

- The remaining letters are written beginning from the letter that is alphabetically next after the alphabetically last letter of the keyword. In our example, the last letter of KEYWORD is Y.

  KEYWORD*ZABCFGHIJLMNPQSTUVX

3. WHEATSTONE'S PRESCRIPTION

Here is Wheatstone's recipe, abstracted from his instructions for using his Cryptograph:

A. Write down the keyword.

SECRETKEY

B. Write down the alphabet.

ABCDEFGHIJKLMNOPQRSTUVWXYZ*#

C. Remove from the alphabet all letters that appear in the keyword.

ABCDEFGHIJKLMNOPQRSTUVWXYZ*#

ABDFGHIJLMNOPQUVWXZ*#

D. Write the remainder of the alphabet under the keyword, in rows so that a letter of the keyword is at the top of each column.

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

E. Delete all but the first occurrence of any duplicate letters in the keyword.

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

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

F. Read the mixed alphabet off in columns, starting on the left.

SAMZ EBN* CDO# RFP GQ THU KIV JW YLX

SAMZEBN*CDO#RFPGQTHUKIVJWYLX

4. BAZERIES'S PRESCRIPTION

First, write down as many copies of the keyword needed to have as many characters as in the alphabet. This example uses twenty-nine characters.

SECRETKEY SECRETKEY SECRETKEY SE

SECRETKEYSECRETKEYSECRETKEYSE

Then, look for the alphabetically first letter of the keyword and begin placing, in order, characters from the alphabet under it, from left to right. In our example, that letter is C.

```
SECRETKEYSECRETKEYSECRETKEYSE
  A         B         C
```

Move on to the alphabetically next letter in the keyword; in our case, E.

```
SECRETKEYSECRETKEYSECRETKEYSE
 DA  E   F   GB H   I   JC  K   L   M
```

Continue with the next letter and the next, until all are used.

```
SECRETKEYSECRETKEYSECRETKEYSE
 DA E  NF   GB H OI   JC  K PL   M

SECRETKEYSECRETKEYSECRETKEYSE
 DAQE NF   GBRH OI   JCSK  PL   M

SECRETKEYSECRETKEYSECRETKEYSE
TDAQE NF UGBRH OI  VJCSK PL WM

SECRETKEYSECRETKEYSECRETKEYSE
TDAQEXNF UGBRHYOI  VJCSKZPL WM

SECRETKEYSECRETKEYSECRETKEYSE
TDAQEXNF*UGBRHYOI#VJCSKZPL&WM
```

The result is the mixed alphabet.

```
TDAQEXNF*UGBRHYOI#VJCSKZPL&WM
```

5. ANYTHING ELSE

Any other method will suffice, so long as all parties agree on it.