Excerpt of TM 11-380 (M-209 Manual) – May 1947

REASON FOR use OF RANDOM INDICATORS

I. Danger of a Repeated Indicator

a. The most serious fault occurring in use of Converter M-209 - (*) is the re-use of indicators, either for two encipherments of the same message or for two different messages. The chances of this fault occurring are negligible *if each operator selects a random message indicator each time he enciphers a message or message part*. When the same indicators are used for two different messages enciphered in the same pin and lug setting, those messages may be read by the enemy. The process by which they are read is illustrated below. By the same procedure, a message which is re-enciphered with the same indicators (and the same pin and lug setting) as used for its first version may be read.

b. Suppose an operator has enciphered the following two messages with the same indicators:

```
Message 1 TTHVL UIHVC OESRM IUDPG
          HTPVS VXWPE TLMIV YDSCV . . .
Message 2 TTHVL UIHVC HOUWG AMAUK
          TIAGR HHBBN SJDGF LUOOW . . .
```

(1) The rotors were alined exactly the same for the first letter of message 1 and the first letter of message 2; therefore, Whatever number of spaces the tvpe-wheel assembly turned to encipher the first letter of message 1, it turned an equal number of spaces to encipher the first letter of message 2. Likewise the rotors were alined exactly the same for enciphering the second letter of message 1 as for the second letter of message 2, and therefore the type-wheel assembly turned the same number of spaces for one of those letters as for the other. This same condition is true for the third letters of the text, the fourth letters, etc.

(2) The machine enciphers on the following principle:

(a) The plain-text alphabet is on the indicating disk and the cipher-text alphabet is on the type wheel. The two alphabets have a fixed relationship, shown below.

```
      Indicating index
             ↓
Plain text   AZYXWVUTSRQPONMLKJIHGFEDCB
Cipher text  STUVWXYZABCDEFGHIJKLMNOPQR
                    ↑
               Print hammer

  ←―――――――――――――――――――――――――――――
Direction alphabets move during operation
```

It will be noted that when a letter of the plain-text (upper) alphabet is alined at the indicating index, a letter seven positions to the right in the cipher (lower) alphabet is at the print hammer. This relationship is always true at the start of the encipherment of a letter. Then the type-wheel assembly is moved a number of positions, or perhaps none, when the drive knob is turned, and whatever letter of the cipher alphabet is in position against the print hammer is printed.

(b) Suppose the letter A is set at the indicating index to be enciphered; its cipher equivalent will depend entirely upon the number of spaces which the type-wheel assembly turns before printing. If the type-wheel assembly does not turn at all, Z on the type wheel will be against the print hammer and will therefore be printed as the cipher letter. (*The letter at the print hammer is the same as the first letter showing on the reproducing disk.*) If, on the other hand, the type-wheel assembly, is made to move one space, A will be at the print hammer and will therefore be the cipher letter; or if A is to be enciphered and the type-wheel assembly turns seven spaces, the letter G will have moved to the print hammer and will be printed as the cipher letter.

Note. The operator should follow the explanation with a converter at hand.

(c) As another example, if the operator will set R at the indicating index, he will find that the letter I on the type wheel is at the print hammer (as indicated by the I showing on that reproducing disk). It can be seen therefore that if the type-wheel assemblv does not move, an l will print as the Cipher letter ; (it turns toward the operator), the letter L is at the print hammer and will therefore be the cipher letter.

(3) It will be seen that if both the plain-text letter and its cipher letter are known, the exact number of spaces turned by the type-wheel can be determined. For example, if it is known that R was set at the Indicating index and N was printed as the cipher letter, then the type-wheel assembly has turned five spaces. Also, if it is known exactly how far the type-wheel assembly has moved, and the cipher letter is known, the cipher letter on the type-wheel can be set against the print hammer and the plain-text letter found by reversing the type-wheel assembly (turning it toward the rear of the machine) the proper number of spaces. For example, if the cipher letter is K and the type-wheel assembly is known to have turned 8 spaces, K is set at the print hammer by making K the first letter showing on the reproducing disk, then the type-wheel is turned back eight spaces and X is found to have been at the indicating index as the plain-text letter.

(4) Now consider the two cipher-text messages. By guessing the correct plain-text letter for the first

letter of message 1, the number of spaces the type-wheel was turned to produce the first clpher-text letter of message 1 (and also, therefore, the first cipher-text letter of message 2), can be determined. By setting the first cipher-text of message 2 at the print hammer and turning the type-wheel assembly back the same number of spaces, the first plain-text letter of message 2 can be determined. Similarly, by the second plain-text letter of message 2 may be found, etc. Now, if instead of guessing a single plain-text letter, a full correct word is guessed for message 1, the correct letters will be determined for each corresponding cipher letter of message 2.

(a) Suppose the first plain-text word of message 1 to be TWOZ (the letter Z represents an enciphered space). If this is correct, the letter T was set at the indicating index for the first letter of message 1. Setting T at the indicating index, G is found to be at the print hammer. The type-wheel assembly must have moved eight spaces for O to come to the print hammer. As has already been noted, the type-wheel assembly moved the same number of spaces for the first letter of message 2; the type-wheel assembly then has moved eight spaces and stopped with H at the print hammer. By setting H at the print hammer and reversing the type-wheel assembly eight spaces, it will be seen that A on the indicating disk is at the indicating index and was the first plain-text letter.

```
Message 1 OESRM IUDPG ...
          TWOZ
Message 2 HOUWG AMAUK ...
          A???
```

(b) For the second letter of message 1 W was set at the indicating index, which would put D at the print hammer. Since E was printed, the tvpe-wheel assembl must have turned 1 space. For message 2 the letter O was printed at that point, and since the type-wheel assembly turned 1 space the print hammer must have started at N, and the letter at the indicating index therefore was M.

(c) By applying the same procedure to the third and fourth letters, it is found that the text of message 2 begins with AMMU, if message 1 begins with TWOZ. AMMU suggests AMMUNITION, and that word is filled in as the suspected first word of message 2.

(d) By the same reasoning as before, if the fifth plain-text letter of message 2 is N, the print hammer started at M, and the type-wheel assembly moved 20 spaces to G. Then for message 1 the type-wheel assembly is known to have stopped with M at the print hammer, after moving 20 spaces. The plain-text letter must therefore have been H. Continuation of this process proves that AMMUNlTlON is correct for message 2, since it yields logical plain text for message 1.

```
Message 1 TTHVL UIHVC OESRM IUDPG
                      TWOZH ALFTR
          HTPVS VXWPE TLMIV YDSCV ...
          ACKS
Message 2 TTHVL UIHVC HOUWG AMAUK
                      AMMUN ITION
          TIAGR HHBBN SJDGF LUOOW ...
```

(e) This process is followed until the complete text is read for both messages:

TWO HALFTRACKS NEEDED ASREPLA . . .
AMMUNITION ON HAND SUFFICIENT . . .

c. In the above illustration it is supposed that the first word of one message has been “guessed.” In actual practice this “guessing” means that the cryptanalyst tries several words and discards each one which when placed in the message yields meaningless letters as “plain text” of the other message. Only the right word, when placed in the right message, yields a “good” word for the other message. Guessing a correct word is easier than may appear at first glance, and there are several short cuts in the method of completing solutions which are too detailed to be explained here. Any word which is known to be somewhere in one of the messages will serve the same purpose as a beginning word, although an hour or two may be required in finding its exact position.

d. IT SHOULD BE EMPHASIZED THAT THE ABOVE PROCEDURE CAN BE APPLIED ONLY WHEN A MESSAGE INDICATOR IS RE-USED It is therefore important that operators follow the rules regarding selection of indicators.