Addendum to "A Cryptologic Fairy Tale"

BY BRIGADIER JOHN H. TILTMAN

~~Top Secret Umbra~~

(Insert after page 28 of *NSA Technical Journal*, VII. 2. Spring 1962.)

EO 1.4.(b)
EO 1.4.(c)
EO 1.4.(d)

More recently I have seen an extremely ingenious development on these lines. In this system a book containing a considerable number of grilles of varying width was employed, numbered consecutively. [redacted] of which in each column 3 were forbidden. The width of the grilles varied from 8 to 15 columns. A transposition key of at least 15 letters was provided for each day. The grilles were used in succession, [redacted] rigorously throughout each message and from message to message. If, for example, the next grille to be used was 11 columns wide, the user formed a top key by numbering the first 11 letters of the key for the day alpha-numerically and a side key by numbering the first 8 letters of the key for the day. He then wrote the text to be enciphered letter by letter from left to right into the permitted squares from line to line in the order of the side key. He repeated this process for the rest of his text, using as many successive grilles as necessary. I do not remember how he dealt with the end of his text when it did not completely fill the last grille, but suggest that the most practical way (to avoid awkwardness) is to add nulls at the end of the P/L text to complete the number of letters to a multiple of 5 and fill only as many columns of the final grille as necessary. Having written the whole text into the successive grilles, the user took out the columns of 5-letter groups from the first grille in the order of the top key, then from the second grille, etc., writing them straight into the message form. [redacted] An example showing the working of this system is attached.

The practical advantages of the use of such a system as a field cipher are evident, if you consider that it combines grille and double transposition and yet is virtually a single process. Presumably, transparent or semi-transparent paper is laid over the appropriate grille by the encipherer and decipherer. The latter writes his horizontal and vertical keys in the appropriate places, writes the 5-letter groups as received column by column over the permitted squares of the successive grilles according to the keys and reads off the plain text line by line according to the side key.

[redacted]

[redacted]

EO 1.4.(b)
EO 1.4.(c)
EO 1.4.(d)

[redacted]

```
     Grille 24          Grille 25
    |F L O W E R S O F|F L O W E R S O F T H E F O R|
    |2 4 5 9 1 7 8 6 3|3 7 8 15 1 11 13 9 4 14 6 2 5 10 12|
F 2 |- N - F I - N E D|E - H E - N S I - - - V E - S|
L 3 |T - O M - A - N -|- T - O P - - - T H E - - O -|
O 4 |U A - L - - C I -|B J - E C - T I - S T O - S T|
W 8 |- - E N T - I S F|- L Y - - S - T A - - F - E -|
E 1 |I T - I S C - - O|- A R - F - R O M C O - M P R|
R 6 |A - N - - D - T H|T - E R - E S T - A - N D - -|
S 7 |E T R - E A T - M|T O G - I V E - T H E - A N A|
O 5 |- P H - E R S - -|I - - M U L - - A - T E I - N|
```

```
   Grille 26        Grille 27                Grille 28
  |F L O W E R S O|F L O W E R S O F T H E|F L O W E R S O F T
  |2 3 4 8 1 6 7 5|3 6 7 12 1 9 10 8 4 11 5 2|2 4 5 10 1 7 8 6 3 9
2 |T - H - E S U -|T - - R - O D - U - C T|- A - C|
3 |B - J E - - - -|I O N - T - O D - I A -|T - I -|
4 |- C - T X - X T|G - N O - S - - - I - S|C - A L|
8 |N T - E - N - D|H R - E - E - Y E A - R|C E - -|
1 |- E L - - F O R|E - D - A S A - N I N -|- S P R|
6 |T T - L E P A P|- A N A L - Y S T - W I|P E - R|
7 |E - R I S - I -|- T H - T W O O - R - T|I - E N|
5 |- H I - S L - I|- F - O R - - T H - E -|- E X -|
```

Fig. 2—Daily Transposition Key: FLOWERS OF THE FOREST

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

Fig. 3—Completed Cipher Text of 240 Letters