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

[redacted]

Non - Responsive

A Cryptologic Fairy Tale

BY BRIGADIER JOHN H. TILTMAN

~~*Top Secret Dinar*~~

The paper describes the diagnosis and solution in 1939 of a German Transposition field cipher and traces the derivation from it of a British field cipher and further development therefrom of the main German Army field cipher of 1944-1945, the "Rasterschluessel". The principles of the security of transposition systems are discussed.

I am afraid that the title of this paper gives you very little idea of its subject. The title, however, is not as unreasonable as it sounds. In the first place the subject is definitely "cryptologic" as it has both cryptographic and cryptanalytic aspects. Further, it can be called a "Fairy Tale" for two reasons:

(1) It departs somewhat from the truth because the workings of the cryptanalytic solution which forms the first part of the lecture have not survived and I have had to construct an example exhibiting features as close to the original as I could from memory, and

(2) The story has a reasonably happy ending.

I couldn't think of a title that would express the essence of the subject less cumbersome than the following:

"Cross-pollination of cryptographic ideas between enemies."

The naval, military and air sections of GCHQ moved to their war station, Bletchley Park, on 15th August 1939 a couple of weeks before the Germans invaded Poland. I was in charge of the military section. About the middle of September we received some intercepts presumed to emanate from German Panzer units in action in Poland, which showed the following superficial characteristics. No message exceeded 138 letters in length, of which the first 8 letters clearly constituted a non-textual indicator of some kind, the first digraph being repeated as the second and the third repeated as the fourth. The remaining letters of the message conformed to German literal frequency. The system employed could therefore be assumed to be some form of transposition.

[redacted]

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

[redacted]

[redacted]

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

[redacted]

[redacted]

[redacted]

There is not sufficient information in my fabricated example to derive the indicating systems completely but the general lines can be deduced. In the original German system, called by them the *Heftschluessel*, the 26 letters of the alphabet were rearranged at random and written in two lines of 13 letters each at the top of the grille and again at the left hand side, giving two alternative letters in each position. The two transposition keys were written at the top and bottom of the grille respectively. The first digraph (repeated for check purposes as the second) gives column and line coordinates for the starting point of the plain text within the grille. The third digraph (repeated as the fourth) gives the starting points within the two keys used cyclically.

In the German usage of this system the transposition keys were changed daily, also presumably the two alphabets used for the indicators. I don't remember how often the grille was changed but it certainly was not constant for all key-areas or for long periods. Shortly after the solution of the messages intercepted during the invasion of Poland, the same system became heavily used for a totally different purpose. An Army transmitter somewhere in western Germany began broadcasting at 4-hour intervals [redacted] messages known as *Barbarameldungen*. These proved on solution to be corrections for weather conditions to artillery range-tables. Regularly 2 hours later than each of these [redacted] messages the same station sent out long general weather forecasts and these were enciphered in the *Heftschluessel*, and, owing to the limitation of textual message-lengths to 130 letters, each of them was enciphered and transmitted in 5 or 6 (sometimes even 7) parts. This meant that we received between 30 and 40 messages a day. [redacted]

However, after we had managed to recover the daily changes for rather more than a month, the system was changed. The successor cipher had a similar indicating system and was clearly a transposition cipher but the number of textual letters in a message was limited to 120 instead of 130. The weather forecasts continued to come in in several parts 6 times daily in the new cipher and [redacted]

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

[redacted]

On 1st February 1940 this new system went out of use and was replaced by the first German Military Double Playfair System which I managed to break into in about 2 weeks, thereafter reading more or less currently for about two months.

During 1940 and 1941 I was under continuous pressure to give attention to the cryptographic security of transposition systems. There were three reasons for this:

(1) The German police were using Double Transposition [redacted] [redacted] for each day for the first and second processes respectively.

(2) The British Army was using a Grille Transposition System known as the Army Stencil Cipher whose security I had criticized on the grounds that the stencil carried too many holes, c.s. permitted squares. The *Heftschluessel* whose solution I described earlier is an example of this, the proportion of 3 forbidden to 10 permitted squares [redacted]

(3) I had to provide a cryptanalytic training course at short notice to test the capability of new recruits to GCHQ before they were accepted and placed in the organization.

[redacted]

Here is a special case you may not all have seen. This is not part of the fairy-tale—it really happened. During the first course of the Cryptanalytic School I started in Bedford in 1941, the Chief Instructor, Major Masters, was giving a first description of the process of Double Transposition on the blackboard. He chose a short key at random and wrote it on the board—53142. He then wrote a short message under it

```
53142
ARRIV
INGTO
DAY
```

He then wrote the key down again and wrote under it horizontally the columns of his earlier diagram in numerical order:

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

```
53142
RGYVO
RNAIT
AID
```

He then took out the columns in numerical order and wrote them horizontally: YADOT GNIVI RRA, this being his original text written backwards.

[redacted]

Sometime later in 1941 I produced the "Cysquare" which was accepted by the War Office as a low-echelon cipher to replace the "Stencil" cipher and issued to the Eighth Army in North Africa. Figures 8 and 9 give photographs of two pages of the printed instructions. The grille has 676 (26 x 26) squares. Each column and each line contains 10 white (permitted) squares, with the exception of 3 "plus" lines containing 20 white squares each and 3 "minus" lines which contain no white squares at all. The key for the day consists of 26 letters of the alphabet in random order with the numbers from 1 to 26 written under them also in random order. For each message the operator selects a 4-letter indicator from a random list of such groups provided him for use in turn. The indicator in the case of the example given is GMBX. The numbers corresponding to this indicator are 11 19 20 7, *i.e.*, position 11, line 19, column 20, taking out number 7. The grille could be used with any of its sides at the top. Position II indicates that the grille is used as shown with numbers 8 to 13 at the top. The numerical key for the day is written from left to right at the top of the grille and from the bottom upwards on the left hand side. The plain text is written into the grille starting at the next white square after the square described by the line coordinate 19 and the column coordinate 20, using the elements of the key to define the corresponding lines and columns. If and when the operator reaches the last white square in the grille he

proceeds from the top left-hand corner. He then takes out the columns of letters starting at the top of the grille and in the column designated by the taking out number, *i.e.*, in this case 7. The message is written out in 4-letter groups preceded by the 4 letter indicator and followed by the number of letters, the indicator repeated, and the time and date. No message of more than 220 letters was permitted. If a message handed in for transmission exceeded this length it had to be divided into parts, none of them exceeding 200 letters in length.

The cipher was originally designed to be used in one of two forms:

(1) *Stencil form*, in which holes were punched through a card to correspond to white squares. This form allowed both sides to be used, giving 8 "positions" instead of 4.

(2) *Pad form*. Here the grilles were issued in pads of 50 pages each printed with identical grilles. I note from the instructions (which I did *not* write) that the operator was encouraged to use each sheet as many times as possible by rubbing out the letters of each message after use!

Everyone who has had the responsibility of designing a cipher knows that a cryptographic system has to be a compromise between security and practicability. I consider my Cysquare to have been strong on security!

At this point I may as well confess that the cipher was a complete flop. It must have been issued to the Eighth Army in pad form as it was apparent very shortly after its introduction that the code clerks refused to use it on the grounds that after a very little desert weather and use of indiarubber the permitted squares were indistinguishable from the forbidden ones. The failure of the cipher created a temporary communication vacuum which had to be filled in another way, but, in the meantime, whenever Rommel overran British armoured and infantry units he captured the Cysquare with its instructions and the German cryptographic experts apparently thought it was wonderful.

[redacted]

[redacted]

[redacted]

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

[redacted]

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

Fig. 1.

[redacted]

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

Fig. 3.

[redacted]

Fig. 4.

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

[redacted]

Fig. 5.

[redacted]

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

[redacted]

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

Fig. 9.