Procédures pour les messages (tiré du Manuel du Simulateur Enigma de Dirk Rijmenants)

Procédure de la Wehrmacht [1]

Chaque jour, les opérateurs de la Heer (Armée) et de la Luftwaffe (Armée de l'Air) installent la machine selon la fiche de clés secrète quotidienne. Cette feuille contenait le jour (Tag), la sélection et l'ordre du rotor (Walzenlage), le réglage des anneaux (Ringstellung), les connexions enfichables (Steckerverbindungen) et les groupes d'identification (Kenngruppen). Les jours étaient imprimés dans l'ordre inversé afin que l'opérateur puisse couper chaque paramètre expiré en bas.

```
├-------------------------------------------------------------------------
Tag  Walzenlage  Ringstellung     Steckerverbindungen          Kenngruppen
-------------------------------------------------------------------------
31   I   II   V    06 22 14   PO ML IU KJ NH YT GB VF RE DC   EXS TGY IKJ LOP
30   III IV  II    17 04 26   BN VC XS WQ AZ GT YH JU IK PM   KIJ TFR BVC ZAE
29   V   I  III    15 02 09   ML KJ HG FD SQ TR EZ IU BV XC   QZE TRF IOU TGB
```

Pour identifier la clé, utilisée pour un message particulier, l'opérateur devait insérer un groupe d'identification de cinq lettres, généralement comme premier groupe du message. Ce soi-disant Buchstabenkenngruppe est composé de deux lettres sélectionnées au hasard et de l'un des quatre Kenngruppen à trois lettres possibles sur la feuille de clés de ce jour. Dans notre cas, quelques exemples d'un Buchstabenkenngruppe correct pour le jour 31 sont TVEXS TGYZA ou LOPXY. Ce groupe de cinq lettres, généralement au début du message, devait être ignoré lors du cryptage et du déchiffrement.

Si un message était divisé en plusieurs parties, l'opérateur devait insérer un nouveau Buchstabenkenngruppe pour chaque partie du message. Ce groupe d'identification de clé a été inclus dans le nombre de lettres pour l'en-tête du message. En regardant ce premier groupe, le destinataire a immédiatement reconnu quelle clé était utilisée pour ce message particulier, ce qui était important lorsque les messages arrivaient des jours précédents. Pour chiffrer un message, l'opérateur devait sélectionner une position de départ aléatoire pour les rotors, appelée clé de message, qui devait être unique pour chaque message. Cette procédure évitait une utilisation excessive des mêmes paramètres secrets pour une journée donnée. La clé du message devant être gardée secrète, ils ont utilisé la procédure suivante :

L'opérateur a sélectionné une position de base aléatoire (Grundstellung) et une clé de message aléatoire (Spruchschlussel). Dans notre exemple, l'opérateur sélectionne EHZ et XWB. Il place les rotors dans la position de base EHZ et saisit la clé de message aléatoire XWB. Le TBS résultant est la clé de message chiffrée. Ensuite, il crypte le message à l'aide de la machine avec la clé de message aléatoire XWB comme position de départ des rotors. Enfin, il envoie la position de départ EHZ et la clé de message cryptée TBS ainsi que le message crypté au destinataire.

Au jour 31, le message suivant est transmis, de C à U6Z, envoyé à 15h10 et contenant 49 lettres.

```
U6Z DE C 1510 = 49 = EHZ TBS =

TVEXS QBLTW LDAHH YEOEF
PTWYB LENDP MKOXL DFAMU
DWIJD XRJZ=
```

Pour décrypter le message nous procédons comme suit :

- Sélectionnez le Wehrmacht Enigma I avec réflecteur B.
- Sélectionnez les rotors, ajustez leur réglage de bague et réglez les bouchons selon la fiche technique jour 31.
- Réglez les positions de démarrage du rotor sur EHZ, le premier trigramme du message
- Tapez le deuxième trigramme TBS pour récupérer la clé du message d'origine. Le résultat devrait être XWB
- Définissez la clé de message décryptée XWB comme position de départ pour les trois rotors.
- Décryptez maintenant le message réel, mais assurez-vous d'ignorer le groupe d'identification de clé TVEXS.

Ceci pourrait bien être votre premier message décrypté, Bonne Chance !

Remarque : dans la procédure d'avant-guerre de la Wehrmacht, chaque clé de message était cryptée deux fois (pour exclure les erreurs) par une position de base secrète fixe, valable toute la journée. Par exemple, avec le paramètre de base ABC, la touche de message XYZ a été saisie deux fois, ce qui a donné JKL MNO. Seule la clé de message doublement cryptée JKL MNO a été envoyée avec le message. Cependant, cela a créé une relation mathématique entre J et M, K et N, et L et O, une faille qui a été exploitée par les décrypteurs polonais. Les cryptologues allemands ont compris cette faille et ont abandonné la clé de message à double cryptage en 1939, la remplaçant par une position de base aléatoire, envoyée avec une clé de message cryptée une fois.

[1] *Le terme Wehrmacht est utilisé à tort. En fait, il ne s'agit que de la Heer et de la Luftwaffe mais pas de la Kriegsmarine. La Wehrmacht englobait ces trois armées !*

Message Procedures (from Enigma Sim Manual - Dirk Rijmenants)

Wehrmacht Procedure

Each day, the Heer (Army) and Luftwaffe (Airforce) operators set up the machine according to the secret daily key sheet. This sheet contained the day (Tag), rotor selection and order (Walzenlage), ring setting (Ringstellung), plug connections (Steckerverbindungen) and identification groups (Kenngruppen). The days were printed in reversed order so that the operator could cut off each expired setting at the bottom.

```
├-------------------------------------------------------------------------
Tag  Walzenlage  Ringstellung     Steckerverbindungen           Kenngruppen
-------------------------------------------------------------------------
31   I   II   V    06 22 14   PO ML IU KJ NH YT GB VF RE DC   EXS TGY IKJ LOP
30   III IV  II    17 04 26   BN VC XS WQ AZ GT YH JU IK PM   KIJ TFR BVC ZAE
29   V   I  III    15 02 09   ML KJ HG FD SQ TR EZ IU BV XC   QZE TRF IOU TGB
```

To identify the key, used for a particular message, the operator had to insert a five-letter identification group, usually as first group of the message. This so-called Buchstabenkenngruppe is composed of two randomly selected letters and one of the four possible three-letter Kenngruppen on the key sheet for that day. In our case, some examples of a correct Buchstabenkenngruppe for day 31 are TVEXS TGYZA or LOPXY. This five letter group, usually at the start of the message, had to be skipped during encryption and decryption.

If a message was divided into several parts, the operator had to insert a new Buchstabenkenngruppe for each part of the message. This key identification group was included in the letters count for the message header. By looking at this first group, the recipient immediately recognized which key was used for that particular message, which was important when messages arrived from previous days. To encrypt a message, the operator had to select a random start position for the rotors, the so-called message key, which had to be unique for each message. This procedure avoided excessive use of the same secret settings for a given day. Since the message key must be kept secret, they used the following procedure:

The operator selected a random basic position (Grundstellung) and a random message key (Spruchschlussel). In our example, the operator selects EHZ and XWB. He sets the rotors in the basic position EHZ and keys in the random message key XWB. The resulting TBS is the encrypted message key. Next, he encrypts the message with the random message key XWB as start position of the rotors. Finally, he sends the start position EHZ and encrypted message key TBS along with the encrypted message to the recipient.

On day 31 the following message is transmitted, from C to U6Z, sent at 1510 hrs and containing 49 letters.

```
U6Z DE C 1510 = 49 = EHZ TBS =

TVEXS QBLTW LDAHH YEOEF
PTWYB LENDP MKOXL DFAMU
DWIJD XRJZ=
```

To decrypt the message we proceed as follows:

- Select the Wehrmacht Enigma I with B reflector.
- Select the rotors, adjust their ring setting and set the plugs according to key sheet day 31
- Set the rotor start positions to EHZ, the first trigram of the message
- Type in the second trigram TBS to retrieve the original message key. The result should be XWB
- Set the decrypted message key XWB as start position for the three rotors.
- Now decrypt the actual message, but make sure to skip the key identification group TVEXS.

This may well be your first decrypted message, Good Luck!

Note: in the pre-war Wehrmacht procedure, each message key was encrypted twice (to exclude errors) by a fixed secret basic position, valid for the whole day. For instance, with basic setting ABC, the message key XYZ was keyed in twice, resulting in JKL MNO. Only the double encrypted message key JKL MNO was sent along with the message. However, this created a mathematical relation between J and M, K and N, and L and O, a flaw that was exploited by the Polish codebreakers. German cryptologists understood this flaw and dropped the double encrypted message key in 1939, replacing it with a random basic position, sent along with a once encrypted message key.