Chiffrement et déchiffrement

Procédure de la Heer et de la Luftwaffe

La méthode de chiffrement courante pendant la Seconde Guerre Mondiale utilisait **un double trigramme**, contenant une **position de départ aléatoire** et une **clé de message aléatoire**. La **position de départ** est la position externe des rotors vus dans les petites fenêtres des rotors sur le panneau avant, à ne pas confondre avec le réglage de la bague ou Ringstellung, qui est le réglage interne du câblage du rotor. La **clé du message** est la position de départ du rotor au début du chiffrement du message.

Pour communiquer, l'expéditeur **et** le destinataire doivent avoir les mêmes paramètres de machine Enigma prévus pour ce jour-là, comme prescrit dans le livre de codes. Dans notre exemple, nous utilisons les paramètres machine suivants sur une Enigma à 3 rotors :

UKW	B
Walzenlage	II IV III
Ringstellung	U N F
Steckerverbindungen	AL CF DU HP RX
Kenngruppen	EDX KFU FGM NBQ

Message: THIS X IS X A X MESSAGE

Tout d'abord, nous sélectionnons une clé de message aléatoire, disons **RHC**. Ensuite, nous sélectionnons une position de départ aléatoire, disons **VTK**. Avec l'Enigma maintenant en position de départ **VTK**, nous chiffrons la clé de message **RHC**. Avec les réglages de la machine ci-dessus, cela donne **ZIW**.

Nous définissons maintenant la clé de message **RHC** comme position de départ et chiffrons le message. Nous complétons le message en chiffrant trois X, pour remplir un groupe complet de cinq lettres :

```
ALNRI HWKVS BSGZK FDUMK
```

Les Kenngruppen sont utilisés pour identifier la clé quotidienne utilisée sur un message particulier. L'opérateur doit insérer un groupe d'identification de cinq lettres comme premier groupe du message. Le groupe est composé de deux lettres sélectionnées au hasard et d'un des quatre Kenngruppen à trois lettres possibles. Si les Kenngruppen pour ce jour sont EDX, KFU, FGM, NBQ, quelques exemples d'un groupe d'identification correct sont SVEDX, CMKFU ou USNBQ. Ce groupe de cinq lettres au début du message ne doit pas être chiffré avec le reste du message ! Si un message est divisé en plusieurs parties (max 250 caractères par partie), l'opérateur doit insérer un autre groupe d'identification pour chaque partie du message. Lors du comptage des lettres pour l'en-tête du message, les cinq lettres du groupe d'identification doivent être incluses. L'opérateur destinataire sait immédiatement quelle clé doit être appliquée en regardant les trois dernières lettres du premier groupe.

Enfin, nous transmettons la destination, l'expéditeur, l'heure, le nombre de groupes, le trigramme de départ aléatoire VTK et la clé du message chiffré ZIW, le groupe d'identification CMKFU et le message chiffré :

```
U47 DE U112 1800 = 4 = VTK ZIW =

CMKFU ALNRI HWKVS BSGZK FDUMK
```

Le récepteur place sa machine en position de départ VTK, déchiffre la clé de message ZIW en RHC et utilise finalement la clé de message récupérée RHC comme position de départ pour déchiffrer le message. Notez que le premier groupe du message est le groupe d'identification et doit être ignoré lors du déchiffrement !

Enciphering and Deciphering

Heer and Luftwaffe Procedure

The common method of enciphering during the Second World War used a **double trigram**, containing a **random start position** and **random message key**. The **start position** is the external position of the rotors as viewed in the little rotor windows on the front panel, not to be confused with the ring setting or Ringstellung, which is the internal setting of the rotor wiring. The **message key** is the start position of the rotor at the start of the message enciphering.

To communicate, both sender and receiver must have identical Enigma machine settings for that day, as prescribed in the codebook. In our example, we use the following machine settings on a 3-rotor Enigma:

UKW	B
Walzenlage	II IV III
Ringstellung	U N F
Steckerverbindungen	AL CF DU HP RX
Kenngruppen	EDX KFU FGM NBQ

Message: THIS X IS X A X MESSAGE

First, we select a random message key, let's say **RHC**. Next, we select a random start position, let's say **VTK**. With the Enigma now in the **VTK** start position, we encipher message key **RHC**. With the machine settings from above, this results in **ZIW**.

We now set the message key **RHC** as start position and encipher the message. We complete the message by enciphering three X's, to fill a complete group of five:

```
ALNRI HWKVS BSGZK FDUMK
```

The Kenngruppen are used to identify the daily key that is used on a particular message. The operator must insert a five letter identification group as the first group of the message. The group is composed of two randomly selected letters and one of the four possible three-letter Kenngruppen. If the Kenngruppen for that day are EDX, KFU, FGM, NBQ, some examples of a correct identification group are SVEDX, CMKFU or USNBQ. This five letter group at the start of the message should not be encrypted with the rest of the message! If a message is divided into several parts (max 250 characters per part), the operator must insert another identification group for each part of the message. When counting the letters for the message header, the five letters of the identification group must be included. The receiving operator immediately knows which key should be applied by looking at the last three letters of the first group.

Finally, we transmit destination, sender, time, number of groups, the random start trigram VTK and the enciphered message key ZIW, the identification group CMKFU and the encrypted message:

```
U47 DE U112 1800 = 4 = VTK ZIW =

CMKFU ALNRI HWKVS BSGZK FDUMK
```

The receiver sets his machine in start position VTK, deciphers the message key ZIW back into RHC, and finally uses the retrieved message key RHC as start position to decipher the message. Note that the first group of the message if the identification group and should be skipped when deciphering!