Zeitschrift: Pionier : Zeitschrift für die Übermittlungstruppen
Herausgeber: Eidg. Verband der Übermittlungstruppen; Vereinigung Schweiz. Feld-Telegraphen-Offiziere und -Unteroffiziere
Band: 27 (1954)
Heft: 3

Artikel: La cryptographie [suite]
Autor: [s.n.]
DOI: https://doi.org/10.5169/seals-561095

halbzerfallenen Hüttlein einrichteten. Schön ist es, wie einmal ein Telegraphist der Gegenstation nach Durchgabe seiner Meldung vergisst, den Sender auszuschalten und wir unter allgemeiner Heiterkeit die Korrekturen des Langnauer Kursleiters mitanhören konnten. Eine Warnung für später!

Ein chiffriertes Telegramm, das von einem Schüler an Hand einer Tabelle entziffert wird, macht uns auf die vorgerückte Zeit aufmerksam. Der Verkehr wird ordnungsgemäss beendigt, die Geräte verladen und nach einer fröhlichen Schneeballschlacht die Rückkehr nach Grünenmatt angetreten. Dort treffen wir im «Löwen» mit den Langnauern zusammen. Die Übung wird durchbesprochen, die Kritik fällt zur allgemeinen Zufriedenheit aus. Anschliessend wird der Parkdienst erledigt und die Stationen per Bahn ans Zeughaus zurückgeschoben. Nach kurzem aber gemütlichem Beisammensein aller Teilnehmer führt uns der Ramseier Express nach Hause. Wir sind zwar müde, aber doch voller Befriedigung über den gelungenen Sonntag.

Mit herzlichem Gruss!

Dein Hansjörg.

La cryptographie

(suite du no 2)

Les transpositions par tableau

Les grilles

Nous ne saurions avoir, dans ce bref exposé, la prétention d'analyser tous les procédés de déchiffrement et toutes les méthodes de décryptement. Mentionnons seulement que les procédés de transposition peuvent être variés à l'infini grâce à l'emploi de clefs.

Par exemple, on prendra une clef de 5 lettres: MARNE, sous lesquelles on écrira leur ordre de succession dans l'alphabet, 31542, et on disposera le texte en un tableau rectangulaire à cinq colonnes. Puis on prendra les lettres par colonne non plus dans l'ordre 31542, mais dans l'ordre 12345. Le décrypteur écrira le cryptogramme sur plusieurs bandes qu'il fera patiemment glisser les unes en face des autres pour faire apparaître les mots clairs. La méthode du mot probable lui sera d'un grand secours dans cette recherche.

Les grilles sont des feuilles de papier ajourées qui masquent une partie d'un quadrillage. On écrit le message dans les fenêtres de la grille et on complète le quadrillage par des lettres indifférentes. Dans d'autres cas on fait tourner la grille pour découvrir de nouvelles fenêtres. L'inconvénient des grilles est leur matérialité, on n'est jamais sûr que l'ennemi n'en possède pas un exemplaire ou une copie.

Les codes

Si on veut faire un code sous forme de tableau, les lettres, syllables, mots, signes de ponctuation, chiffres à représenter sont rangés dans les cases du tableau, dont les lignes et les colonnes sont numérotés. Chaque élément est alors représenté par le rang de la ligne et le rang de la colonne où il se trouve.

Un mot pourra se trouver tout entier dans une case, mais on pourra également le former syllabe par syllabe ou lettre par lettre, ce qui fournit, à moins que le chiffreur ne soit paresseux, une variété assez grande de représentation du même texte.

Mais si l'on veut retrouver les éléments qu'on cherche, il faut les placer dans un ordre méthodique: les chiffres avec les chiffres, les signes de ponctuation avec les signes de ponctuation, etc., et c'est cette nécessité, combinée avec certaines négligences du chiffreur et du rédacteur du message (messages commençant toujours de la même façon: Général de division à...) qui permettront au décrypteur de trouver le principe de la classification pour la constitution du répertoire.

Les machines à chiffrer et à déchiffrer

Pour peu qu'on y réfléchisse un moment, on verra qu'un grand nombre des procédés que nous avons décrits et, en particulier, le procédé de Vigenère, font appel à des opérations intellectuelles qui peuvent être aussi facilement mécanisées que l'addition ou la multiplication dans une machine à calculer. De nombreuses et ingénieuses machines à chiffrer ont donc été inventées, qui fournissent un ou deux cryptogrammes d'un texte tapé en clair sur un clavier. Elles permettent de chiffrer rapidement et sans erreur, avec des clefs pratiquement indéfinies.

Une machine ingénieuse avait été inventée par Belin avant la guerre: elle consistait à brouiller la transmission normale des images par des variations de vitesses de rotation et le décentrement de certains organes du belinographe, appareil à reproduire les images à distance. Il en résultait sur un récepteur normal un ensemble de points sans rapports entre eux, alors que sur un récepteur « accordé », l'image redevenait claire.

Une lutte jamais terminée

Au terme de cette étude élémentaire, nous voyons quelles sont les armes du décrypteur devant un message qui lui est soumis: il connaît en principe tous les procédés qui, à un moment donné, ont été inventés, et il arrive parfois à diagnostiquer quel est celui qui a été employé. Il connaît souvent l'expéditeur et le destinataire, et dans ses grandes lignes le thème du message. Enfin, il peut parfois compter sur la maladresse de l'adversaire: qu'une erreur s'introduise au chiffrement, le message sera retransmis. Certains chiffreurs maladroits vont même jusqu'à donner en clair les mots mal compris, imprudence dont Napoléon était coutumier, ce qui lui valait d'avoir tous ses messages immédiatement décryptés par l'ennemi. La manière dont on utilise un système de chiffrement intervient pour en accroître ou en réduire la sûreté: un chiffreur routinier et sans imagination donnera beaucoup plus d'indices au décrypteur qu'un opérateur qui comprend ce qu'il fait. Enfin, le chiffrement doit être employé à bon escient: c'est un procédé lent, qu'il ne faut pas surcharger, et souvent on a intérêt à parler en clair quand la situation est mouvante et que les messages doivent être utilisés immédiatement. D'ailleurs, la radio a cessé, avec les progrès de l'électronique, d'être un procédé de transmission indiscret: la modulation en impulsions des ondes ultra-courtes est un procédé qui suppose entre émetteur et récepteur un accord qui est pratiquement impossible à réaliser sans convention spéciale entre les correspondants. Le secret est ici dans la technique de transmission, et la conversation peut avoir lieu en clair, sans risque d'indiscrétion.