Zeitschrift: Schweizer Soldat : Monatszeitschrift für Armee und Kader mit FHD-Zeitung

Herausgeber: Verlagsgenossenschaft Schweizer Soldat

Band: 9 (1933-1934)

Heft: 13

Artikel: La cryptographie au service de l'armée [Schluss]

Autor: [s.n.]

DOI: https://doi.org/10.5169/seals-708943

Nutzungsbedingungen

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Mehr erfahren

Conditions d'utilisation

L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. En savoir plus

Terms of use

The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. Find out more

Download PDF: 11.08.2025

ETH-Bibliothek Zürich, E-Periodica, https://www.e-periodica.ch

La cryptographie au service de l'armée

En la recevant, le destinataire compte les lettres, les divise en groupe de 49 lettres, puis, dans chaque groupe, écrit les lettres en 7 rangées horizontales qu'il numérote dans l'ordre des chiffres de la clef; il les rétablit par interposition dans l'ordre naturel des nombres, numérote à leur tour les colonnes verticales dans l'ordre des chiffres de la clef, les rétablit dans l'ordre naturel, efface la colonne 4 et les rangées 2 et 6, et lit la dépêche.

Ce procédé, malgré la complication qu'il présente et le temps nécessaire pour transcrire une dépêche, peut être utilement employé, car il défie presque complètement les recherches des déchiffreurs les plus exercés.

Il peut d'ailleurs être simplifié en n'intervertissant que les colonnes ou que les rangées de lettres, et en ne réservant pas de colonnes ou de rangées pour l'inscription de lettres nulles; mais ce serait alors au détriment de la sécurité. Dans ce cas, en effet, un déchiffreur sagace et patient essaiera d'abord, d'après le nombre des lettres de la dépêche interceptée, de déterminer le nombre des cases de chaque tableau; cela fait, il répartira les lettres par rangées et, en étudiant attentivement celles-ci ou les colonnes verticales, il cherchera la loi de leur interposition par le rapprochement des lettres qui, dans la langue dans laquelle est présumée écrite la dépêche, se trouvent fréquemment ou toujours accolées.

Ainsi, dans l'exemple précédent, si l'on n'avait interverti que les colonnes verticales, et qu'après des recherches et des essais répétés, le déchiffreur soit arrivé à reconstituer les deux seconds tableaux, il remarquera, dans la dernière rangée, les lettres *u* et *q;* or, en français, la lettre *q* est toujours suivie de *u*; cette indication permet de replacer dans leur ordre les deux colonnes qui les contiennent; d'autre part, la première ligne contient les lettres du mot *l'ennemi* qui, dans n'importe quel ordre soient-elles, frapperont les regards et permettront de rétablir l'ordre dans les colonnes verticales et, par conséquent, feront découvrir l'ordre de la clef. Ce n'est donc qu'avec la double interposition des colonnes et des rangées et de l'introduction des lettres nulles que ce procédé présente une réelle sécurité.

2° *Chiffrement par interversion des lettres et à double clef.* — Ce procédé cryptographique consiste dans l'emploi combiné d'une clef donnée par une phrase, un mot, convenus d'avance, et une table ou damier de lettres ayant 27 cases de côté. Dans les cases de la 1e rangée horizontale sont écrites les 26 lettres de l'alphabet dans leur ordre alphabétique, en commençant par *a*, et en reproduisant l'*a* après le *z* pour remplir la 27e case. Dans la colonne verticale de gauche, on écrit le même alphabet avec reproduction de l'*a* pour la 27e case inférieure. La 2e rangée horizontale commence alors par un *b*, à partir duquel on suit l'ordre alphabétique; après le z il reste deux cases à remplir, dans lesquelles on inscrit *a, b*. La 5e rangée commence par *e*, on écrit ensuite: *f, g... z*, puis on reprend: *a, b, c, d, e*. On obtient ainsi une table dont, faute de place, nous ne pouvons reproduire qu'une partie:

a	b	c	d	...	...	x	y	z	a
b	c	d	e	...	...	y	z	a	b
c	d	e	f	...	...	z	a	b	c
d	e	f	g	...	...	a	b	c	d
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
x	y	z	a	...	...	u	v	w	x
y	z	a	b	...	...	v	w	x	y
z	a	b	c	...	...	w	x	y	z
a	b	c	d	...	...	x	y	z	a

Supposons qu'on prenne pour clef le mot: *Paris,* et qu'on ait à transmettre la même dépêche que précédemment. On écrit d'abord celle-ci, et on répète au-dessous autant de fois le mot *Paris* qu'il est nécessaire, en ayant soin que les lettres se couvrent bien verticalement:

lenne	miest	a Mire	court	Attaq	uezle	defro	nt ...
paris	paris	paris	paris	paris	paris	paris	pa ...

Usant alors de la table, l'expéditeur cherche dans la colonne verticale de gauche la lettre *l,* 1re lettre de la dépêche; il suit la rangée horizontale de *l* jusqu'à ce qu'il rencontre la lettre *p,* lettre correspondante de la clef, descend la colonne verticale contenant cette lettre *p,* et trouve à la dernière rangée de la table la lettre *e* qu'il inscrit et qui sera la 1re lettre de la dépêche chiffrée à transmettre. En procédant ainsi pour toutes les lettres, on obtiendra:

Dépêche								
en clair:	lenne	miest	àMire	court	attaq	uezle	defro	nt
clef:	paris	paris	paris	paris	paris	paris	paris	pa
chiffre:	ewevo	dsnqz	pojro	nmxrz	phyic	vwsxo	mwmre	ch

Pour mettre en clair la dépêche chiffrée, le destinataire procède de façon identique. Au-dessous de chacune des lettres de la dépêche chiffrée, il écrit les lettres de la clef en observant les mêmes précautions que précédemment; puis, cherchant la lettre *e,* 1re lettre de la dépêche chiffrée, dans la colonne verticale de gauche de la table, il suit la rangée horizontale jusqu'à ce qu'il rencontre la lettre *p,* lettre correspondante de la clef; il descend la colonne verticale et trouve au bas la lettre *l,* 1re lettre de la dépêche en clair.

On remarque qu'avec ce système, une même lettre peut être représentée de vingt-six façons différentes, autant qu'il y a de lettres dans l'alphabet; c'est une garantie de secret absolue. Il est impossible, sans connaître la clef, de déchiffrer une dépêche ainsi traduite; c'est ce qui doit faire préférer ce système à tous les autres, malgré le temps qu'il exige pour chiffrer. On peut d'ailleurs, à l'aide d'alphabets mobiles sur réglettes et d'autres artifices de ce genre, diminuer notablement les lenteurs inhérentes à ce système.

Nous avons pris, pour expliquer ce procédé de cryptographie, une table ne contenant que les lettres simples de l'alphabet; avec elle, les dépêches sont transmises sans ponctuation, sans accents, et les nombres devraient être écrits en toutes lettres. C'est là une cause d'obscurité et de lenteur qu'il est facile de faire disparaître; il suffit pour cela d'introduire dans la table, en l'agrandissant, les signes de ponctuation, les lettres accentuées et les chiffres que donne par exemple l'alphabet Morse. Il faut avoir soin, après avoir constitué l'alphabet général, dans un ordre déterminé, par adjonction des signes et chiffres, d'observer rigoureusement, dans la construction de la table, le principe que nous avons expliqué pour l'établissement de la table simple.

L'introduction de ces chiffres et signes, sans rendre l'emploi de la table plus long ou plus difficile, fournit un moyen de rendre la correspondance encore plus secrète; ces chiffres et signes peuvent, en effet, dans l'alphabet général à former, être disposés d'une façon quelconque, qui est, bien entendu, la même dans les tables des deux correspondants. Cette table devient à son tour une clef, que les correspondants peuvent modifier périodiquement par convention, comme le mot formant clef.

Il nous reste à formuler quelques prescriptions générales concernant l'emploi de la cryptographie dans la correspondance militaire.

Avec des procédés de cryptographie élémentaire, il serait dangereux de laisser des parties en clair dans

une dépêche chiffrée; elles peuvent aider à traduire les parties chiffrées et par conséquent à trouver la clef; avec le dernier système étudié, ce danger n'est pas à craindre. Il faut avoir soin, si on chiffre seulement des parties de la dépêche, de chiffrer des phrases entières, mais jamais des mots isolés.

Quand on a chiffré une dépêche, il est de bonne précaution, avant de l'expédier, de la déchiffrer ou de la faire déchiffrer, afin de s'assurer qu'on n'a pas commis d'erreurs.

Les brouillons qui ont servi aux opérations de chiffrement doivent toujours être brûlés; la traduction littérale de ces dépêches ne doit jamais figurer dans un document destiné à être publié. Ces précautions ont pour but de ne fournir à l'ennemi, qui aurait intercepté une dépêche chiffrée, aucun indice pouvant, par rapprochement de textes ou correspondance de signes, le mettre sur la voie de la découverte du procédé de cryptographie employé et même de la clef. (Fin.)

Fin de manœuvres

D'une voix éraillée par la laryngite, le lieutenant hurlait des ordres que personne n'entendait. Les genoux crottés, une molletière à demi déroulée, les jumelles brinbalant sur sa poitrine où les boutons de cuivre luisaient comme des pissenlits, il courait devant les groupes éparpillés qui le suivaient dans un tintamarre infernal de gamelles, de baïonnettes et de crosses entre-choquées. Poussé par une ardeur que les approches de midi rendaient incompréhensible, la première section de la III/8 avait maintenant dépassé dangereusement la ligne de front d'au moins trois cent mètres. Ce zèle excessif s'expliquait pourtant. A cinquante pas devant elle, caché derrière les arbres d'un verger qui tendaient en riant leurs bras chargés de pommes mûres, un hameau soulevait au-dessus des frondaisons ses toits rouges d'où — c'est Bavolet, vannier ambulant au civil, qui l'avait vu le premier — montaient vers le ciel, gonflé comme une voile bleue, de paisibles fumées blanches.

A cette vue, quelque chose avait craqué dans l'âme trop tendue des soldats et, comme ils arrivaient sous les arbres, ils sentirent qu'il était vain d'aller plus loin. D'ailleurs, furieux comme un Robinson dérangé dans son île, un arbitre était apparu sur le seuil d'une maison. Sa bouche ouverte avait fait un trou dans son visage rouge:

« Lieutenant! ... »

Le jeune officier courait, collait sa main au casque, et, les lèvres sèches, s'annonçait en bredouillant pendant qu'une harde de poules, le cou tendu déguerpissaient à toutes pattes. La conversation fut brève et quand le lieutenant revint, il était aussi rouge que le gros major qui se retirait à petits furibonds.

La subdivision avait déjà *compris* et, prévenant avec intelligence les ordres probables, s'était débarrassée des sacs qui gisaient dans l'herbe comme un troupeau paissant de bêtes à croupetons.

— « La section .... anéantie par un feu meurtrier .... attend ici jusqu'à .... »

C'était la supposition du major arbitre que le lieutenant exposait ainsi à ses hommes, sans divulguer pourtant les appréciations qu'avaient obtenues ses initiatives tactiques. Mais déjà on n'écoutait plus. Et, à ce moment, Bavolet, l'oreille tournée vers le lointain, la face extasiée, annonça qu'il entendait une sonnerie de trompettes. En écho, il répéta un taratata fallacieux. Tous avaient aussi .... *entendu* .... quelque chose. Alors, tout en ne s'éloignant pas trop des sacs et des faisceaux de fusils, après que le chef de section eut accordé un repos déjà pris à moitié, on décida que la fin des manœuvres avait sonné.

*

Le hameau paraissait désert. Seule, au bord de la route, une fontaine racontait avec ennui une histoire interminable, et des ombres bleues se blotissaient derrière les murs et sous les arbres. C'était midi, l'heure charmante entre toutes au service militaire.

Le verger n'était plus qu'un grouillement et qu'un éclat de rire. Dans un coin, le lieutenant parlait avec abandon à ses sous-officiers qui mouraient d'envie de se jeter à plat ventre dans l'herbe moelleuse. Mais l'heure de la détente n'était pas encore venue.

En un tournemain, les soldats avaient déballé leurs sacs. Le couteau, ouvert au poing, au risque de s'éborgner à chaque bouchée, ils s'étaient mis à manger en coupant au niveau des lèvres d'épaisses rouelles dans des saucissons que le jeune chef considérait avec mélancolie.

Une demi-heure plus tard, la tête appuyée au tronc des pommiers, la plupart des soldats fumaient, d'autres dormaient, leurs touchantes figures de petits hommes fatigués criblées de taches claires par le soleil qui filtrait au travers des feuillages. Quelques hommes avaient été tout de suite happés par les portes ouvertes des maisons, qui ne reparaîtraient qu'au dernier moment, impertubables et souriants. Ses chaussures à la main, un malchanceux s'en revenait cahin-caha de la fontaine où il avait baigné ses orteils bleuis et tuméfiés.

Lorsque la petite armée fut au trois quarts assoupie, le lieutenant s'assit à son tour, déboutonna sa tunique et ôta son casque qui libéra un tourbillon de boucles enfantines. Il tira de sa sabretache un reste de chocolat qu'il fourra tout entier dans sa bouche. C'était midi partout.

Quelque part — où cela pouvait-il bien être? — un dernier coup de fusil fit un trou dans le cristal de l'air.

*

Alors, au milieu du silence fragile, s'éleva le vagissement d'un marmot dans une maison. D'abord, ce fut un geignement léger. Puis le cri devint une sorte de hululement coupé d'arrêts prolongés pendant lesquels le nourrisson reprenait sans doute haleine. Après ces moments d'accalmie, la clameur recommençait avec plus de vigueur, ressemblant tantôt aux modulations enamourées d'un matou, tantôt à des glapissements aigus.

Déjà, quelques dormeurs avaient soulevé une paupière lourde de sommeil et maugréaient.

— « Ben, mon vieux, il a du souffle, le môme! » fit une voix qui bâillait.

Et comme les aboiements du moutard continuaient avec une force renouvelée, Mordau, qui était employé chez Foetisch, se mit sur son séant et exprima l'ire qui le soulevait:

— « Change de disque, nom d'une pipe! » Mais loin d'obtempérer, le gosse poussa de tels hurlements que l'appointé sanitaire Tscheppen, de l'Armée du Salut, se sentit appelé .... à se mêler de quelque chose. Il s'approcha d'une fenêtre, regarda en collant son œil contre la vitre et fit un signe pour appeler ses camarades.

Lié au châlit par des courroies, un bébé de huit à dix mois gigotait désespérément en montrant son petit derrière nu. La chambre était dans un désordre répugnant: des vêtements d'homme et de femme traînaient dans tous les coins comme des cocons abandonnés, et des ustensiles de cuisine fraternisaient avec d'humbles objets de toilette.

Le petit homme, quand il vit tous ces visages bru-