

DU « CARRÉ DE POLYBE » AU « RADIOGRAMME DE LA VICTOIRE » DE JUIN 1918

par François DROUIN

Dans un carré 5×5, je place les vingt-six lettres de notre alphabet latin. Il n'y a que vingt-cinq cases, I et J sont regroupés.

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I / J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

A chaque lettre correspond un couple formé d'un nombre rouge et d'un nombre noir. « APMEP » va être codé 11 53 23 51 53 et pourrait être transmis sous sa forme chiffrée ou en utilisant des signaux différents pour les nombres rouges et les nombres noirs (le « P » pourrait correspondre à cinq signaux d'une couleur suivis de trois signaux d'une autre couleur).

Cette méthode de codage est celle du « carré de Polybe » : Polybe a vécu en Grèce vers -200, mais son carré était encore utilisé par les nihilistes russes vers 1900 : ils communiquaient entre eux dans leurs prisons à l'aide de coups brefs et de coups longs sur les tuyaux de leurs cellules, il n'est donc pas surprenant que plus tard l'alphabet morse ait été utilisé par la suite pour ce codage.

Nous retrouvons l'utilisation d'un « carré de Polybe » à la page 53 du récit des aventures de Blake et Mortimer, « Le bâton de Plutarque » paru fin 2014. Les nombres en tête de ligne et de colonne indiquent des flashes vus à droite et des flashes vus à gauche. Il n'est cependant pas précisé comment le Professeur Mortimer a compris que ces éclairs lumineux avaient pour source un codage à l'aide d'un tel carré.

Cette méthode de codage a ensuite été améliorée pour pouvoir coder des chiffres. Vingt-six lettres et dix chiffres amènent à l'utilisation d'un carré 6×6. Par ailleurs, pour le codage des lignes et des colonnes les lettres A, D, F, G, V, X ont été utilisées pour leurs codes en morse très différents les uns des autres, permettant d'éviter les erreurs de transmission radio.

A	D	F	G	V	X
· –	– · ·	· · – ·	– – ·	· · · –	– – · · –

Les vingt-six lettres et les dix chiffres sont disposés selon notre envie dans le carré 6×6 .

	A	D	F	G	V	X
A	A	6	E	O	D	Y
D	H	U	3	L	X	I
F	Z	9	B	5	M	4
G	N	J	Q	F	7	T
V	C	P	2	G	K	1
X	V	R	8	W	S	0

« L'APMEP LORRAINE EN 2018 » se code « GD AA DV VF FA DV FA AG FV XX XV FX ».
Je choisis le mot « CUBE » qui va me servir de clé de codage. J'écris le message obtenu dans un rectangle 4×6. Je repère chaque colonne par une des lettres de mon mot clé.

C	U	B	E		B	C	E	U
G	D	A	A		A	G	A	D
D	V	V	F		V	D	F	V
F	A	D	V		D	F	V	A
F	A	A	G		A	F	G	A
F	V	X	X		X	F	X	V
X	V	F	X		F	X	X	V

J'ai réordonné les colonnes du tableau selon l'ordre alphabétique des lettres de mon mot clé. « AGADVDFVDFVAAFVFXVFXV » est le message que je transmettrai. Sans connaître mon mot clé et mon tableau de départ, le déchiffrement sera ardu...

Et pourtant...

Le 1^{er} juin 1918, les services du chiffre de l'armée française recevaient le message
FGAXA XAXFF FAFVA AVDFA GAXFX FAFAG DXGGX AGXFD XGAGX GAXGX AGXVF
VXXAG XDDAX GGAAF DGGAF FXGGX XDFAX GXAXV AGXGG DFAGG GXVAX VFXGV
FFGGA XDGAX FDVGG A

Le lieutenant Georges-Jean Painvin réussit à retrouver la clé (un ensemble de 21 lettres...) ainsi que la grille de départ et décode le message.

Munitionierung beschleunigen Punkt soweit nicht eingesehen auch bei Tag (« hâter l'approvisionnement en munitions, le faire même de jour tant qu'on n'est pas vu »).

L'attaque se produisit le 10 juin 1918, mais l'État Major français prévenu a pu prendre ses dispositions. Au vu de l'importance qu'a eu ce message, il est actuellement appelé « Radiogramme de la Victoire ».

Le système utilisé par l'armée allemande et repris en début de cet article était nommé GEDEFU 18 (*GEheimschrift DEr FUnker 18*, « chiffre des radiotélégraphistes 18 ») et avait été conçu en 1918 par le colonel Fritz Nebel. Il fallut attendre les années soixante pour que soit connu ce qu'avait fait le lieutenant Georges-Jean Painvin, Fritz Nebel lui-même ne l'apprit que quelques années plus tard... Les secrets militaires sont bien gardés.

Éléments de sitograhie

<http://www.bibmath.net/crypto/index.php?action=affiche&quoi=substi/polybe> Pour en savoir plus à propos des « carrés de Polybe ». Le site fournit de quoi coder et décoder vos messages.

<http://www.bibmath.net/crypto/index.php?action=affiche&quoi=debvingt/radiogramme> Pour en savoir plus sur le radiogramme de la Victoire.

<http://www.bibmath.net/crypto/index.php?action=affiche&quoi=debvingt/adfgvx> Pour en savoir plus à propos du code « ADFGVX ». Le site fournit de quoi coder et décoder vos messages.

<http://www.annales.org/archives/x/painvin.html> Pour en savoir plus à propos de Georges-Jean Painvin.