

Le décryptement du système ADFGX

Au printemps 1918, libéré du front est, les Allemands reprennent l'offensive à l'ouest. Le haut commandement allemand ayant compris que ses chiffres n'étaient guère secrets décida d'en changer avant le jour de la grande offensive. **Le nouveau chiffre fut appelé ADFGX par les Français** car il n'utilisait que ces lettres.

Pour éviter les confusions à la réception, le nouveau chiffre allemand n'utilisait que cinq lettres, très éloignées en code morse : A, D, F, G et X. En disposant les 25 lettres de l'alphabet (en confondant le I et le J) dans un carré de côté 5, on peut les désigner par un couple de ces cinq lettres. Ce carré constitue la clef d'une substitution alphabétique et peut être rempli à l'aide d'une phrase, en n'utilisant qu'une seule fois chaque lettre. Ici : **Geheimschrift der Funker**.

	A	D	F	G	X
A	G	E	H	I	M
D	S	C	R	F	T
F	D	U	N	K	A
G	B	L	O	P	Q
X	V	W	X	Y	Z

Ainsi, A est codé FX (ligne et colonne de A dans le carré). Pour « *Attaquez demain à quatre heures* », nous obtenons :

FX DX DX FX GX FD AD XX FA AD AX FX AG FF FX GX FD FX DX DF AD AF AD FD DF AD DA.

On opère alors une transposition dont la clef est un mot, comme par exemple ici « nébuleux », comme dans le Chiffre Übchi :

N	E	B	U	L	E	U	X
5	2	1	6	4	3	7	8
F	X	D	X	D	X	F	X
G	X	F	D	A	D	X	X
F	A	A	D	A	X	F	X
A	G	F	F	F	X	G	X
F	D	F	X	D	X	D	F
A	D	A	F	A	D	F	D
D	F	A	D	D	A	G	X

Nous écrivons alors les colonnes dans l'ordre donné par la seconde ligne du tableau et groupons les lettres par cinq pour obtenir le message chiffré :

**DFAFF AAXXA GDDFX DXXXD ADAAF DADFG FAFAD XDDFX FDFXF GDFGX
XXXFD X**

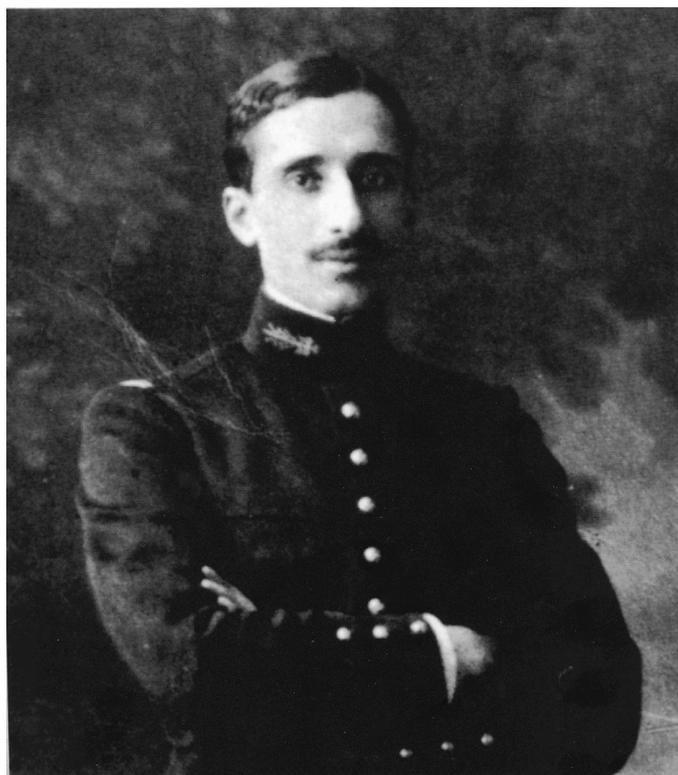
Nous écrivons alors les colonnes dans l'ordre donné par la seconde ligne du tableau et groupons les lettres par cinq pour obtenir le message chiffré :

**DFAFF AAXXA GDDFX DXXXD ADAAF DADFG FAFAD XDDFX FDFXF GDFGX
XXXFD X**

Le décryptement du système ADFGX

Le système ADFGX a été utilisé à partir du 5 mars 1918. Les messages allemands sont alors devenus indécryptables pour les Français. Même s'il était évident que les Allemands allaient attaquer, l'état-major ne savait pas où. L'offensive du 21 mars fut donc une surprise, suivie par plusieurs attaques qui, progressivement, asséchaient les réserves françaises. Alors qu'au départ, elles étaient échelonnées à l'arrière dans tous les endroits probables d'attaques allemandes, il fallait maintenant choisir où les disposer.

Heureusement, le 5 avril, Georges Painvin réussit à décrypter le système.



Georges Painvin

Malgré la méfiance allemande, la chance lui sourit le 4 avril, quand il reçut deux messages ayant de fortes similarités, qui lui permirent d'accéder à la longueur de la seconde clef.

Le système ADFGVX

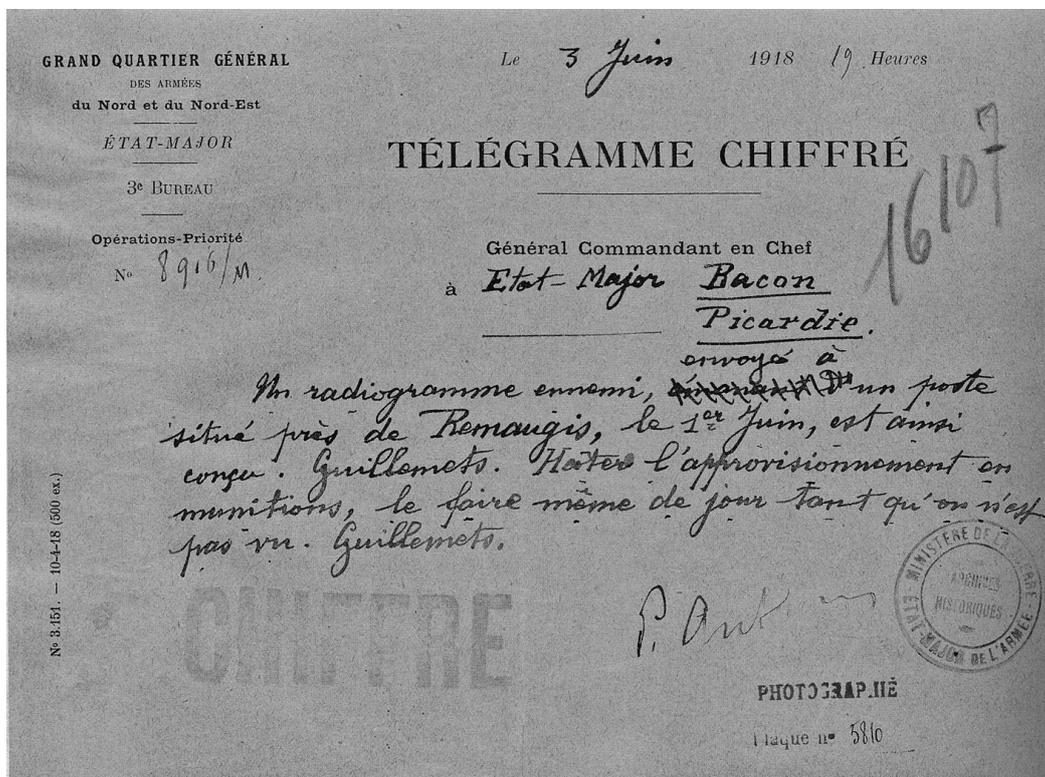
Le premier juin 1918, les Allemands changèrent à nouveau de chiffre, ajoutant un V aux cinq lettres ADFGX. Le capitaine Georges Painvin, d'abord officier d'ordonnance devenu le meilleur cryptologue de la première guerre mondiale, comprit rapidement que le système n'avait pas réellement changé, que le carré avait seulement un côté de six. Cela faisait 36 symboles au total. L'hypothèse qui lui parut naturelle était qu'ils chiffraient ainsi les 26 lettres de l'alphabet plus les dix chiffres. Cette apparente complication précipita la perte des Allemands.

En effet, ils commençaient leurs messages par leur adresse comme « 15^e division d'infanterie » ou « 25^e division d'infanterie ». En toutes lettres, cela donnait des messages commençant par « quinze » ou « vingt-cinq », qui différaient énormément. Avec le nouveau système, entre « 15 » et « 25 », seule la première lettre différait.

Le lieu de la future offensive décrypté

Deux communications ayant les particularités que nous venons d'étudier furent interceptées le premier juin. Polytechnicien et paléontologue, Georges Painvin les décrypta dès le lendemain. Tous les messages furent alors déchiffrés et **le lieu de la future offensive allemande se dévoila**. Les réserves françaises purent ainsi se placer exactement où il fallait. Ce fut la victoire de Méry, qui allait changer le cours de la guerre en cette fin de printemps 1918.

Grâce à un décrypteur de génie, les Allemands ne purent plus prendre les Français par surprise.



Télégramme de la victoire