Compte-rendu :
Le chiffre ADFGVX

BROZZONI Vincent

JUGAND Théo

LESAGE Olivier

I - Le chiffre ADFGVX

Introduit à la fin de la Première Guerre mondiale par le lieutenant allemand Fritz Nebel, le chiffre ADFGVX a été inventé afin de sécuriser les communications radiophoniques lors de l'offensive sur le territoire français. Il est le successeur amélioré du chiffre ADFGX qui ne permettait pas de chiffrer l'entièreté de l'alphabet ni les 10 chiffres.

Son fonctionnement est l'union d'une substitution inspirée du carré de Polybe et d'une transposition.

	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

Carré de Polybe simple

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

Carré de Polybe ADFGVX

Chaque lettre est d'abord remplacée par un couple de lettres parmi A,D,F,G,V, X. Par exemple, ci-dessus on remplace B par le couple DX.
Le message alors obtenu était ensuite mélangé en utilisant une clé (dite de transposition).
On envoie alors un message en n'utilisant que 6 lettres distinctes. Ces 6 lettres, A,D,F,G,V, X ayant un code morse très différents sont impossible à confondre

On a alors un procédé extrêmement sûr , et aussi extrêmement pratique pour les messages radio.

II - Contexte historique

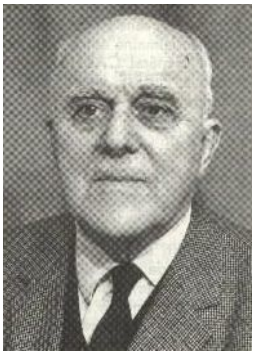
Création d'ADFGX

Mars 1918, les armées sont épuisées par une guerre de position qui dure depuis plus de 3 ans. Chacun sent que la guerre de mouvement va reprendre. L'Allemagne vient de signer l'armistice avec la Russie et n'a plus à se préoccuper du front est et elle doit rendre sa victoire irréversible avant l'arrivée des renforts des États-Unis sur le sol français.

L'armée allemande a décidé de retenir les leçons de 1914, quand ses transmissions radio avaient été catastrophiques :

- radiogrammes transmis avec retard
- radiogrammes souvent indéchiffrables
- demandes de la réémission de message

Tout cela constituait une aubaine pour le service du chiffre français, qui perça successivement tous les chiffres allemands (Ubchi, ABC, KRU,…).



Cette fois l'armée allemande consacre du temps à choisir son algorithme de chiffrement. C'est le système proposé par le colonel Fritz Nebel qui est retenu. Il comporte les deux éléments essentiels des algorithmes de chiffrement:
substitution et *transposition*.

Ce chiffre est baptisé *ADFGX* par les français, alors que son nom côté allemand est *GEDEFU 18* (GEheimschrift DEr FUnker 18, chiffre des télégraphistes 18).

L’entrée en guerre du chiffre ADFGX

Les premiers messages chiffrés à l'aide du chiffre ADFGX sont transmis par l'armée allemande au début du mois de mars 1918. Interceptés par les français, ils parviennent sur les bureaux du service du chiffre français, où l'on est affolé par cette nouvelle méthode. Elle ne ressemble en rien aux précédentes, et le trafic en ce mois de mars est trop faible pour comprendre comment elle fonctionne.

Le 21 mars, les allemands lancent une offensive en Picardie, dans le but de séparer les armées françaises et anglaises. Le nombre de radiogrammes chiffrés augmente subitement, mais l'ADFGX reste un mystère pour le service du chiffre français.

Georges Painvin

Le capitaine Georges Painvin est un polytechnicien et paléontologue de son état. Initialement mobilisé comme officier d'ordonnance, il avait très vite fait des avancées importantes sur les premiers systèmes cryptographiques allemands et, presque contre son gré, il avait intégré le "cabinet noir" du chiffre français.
Il est devenu le meilleur des cryptologues de cette Première Guerre mondiale, faisant tomber tour à tour chacun des chiffres ennemis.

La contre offensive

Painvin décide de se concentrer sur les messages envoyés le 1er avril. Parmi eux, deux messages de même longueur et qui se ressemblent beaucoup.

Le 5 avril, il comprend la méthode et trouve les clés de chiffrement des messages du 1er avril. C'est un véritable exploit sachant que la première clé comporte 25 caractères et la seconde une vingtaine. Malheureusement, ces clés changent chaque jour et tout le travail est à refaire. Enfin, presque, car la méthode est désormais comprise.

Peu à peu, le service du chiffre français perfectionne ses méthodes, et il ne lui faut plus que de quelques heures à quelques jours pour déchiffrer les messages allemands. Pendant ce temps, l'offensive des allemands continue. Ils franchissent la Marne à Château-Thierry, et Paris est désormais à portée d'obus.

Fin mai, après une nouvelle offensive sur l'Aisne, l'avance allemande menace directement Paris. Plusieurs axes paraissent possibles pour une ultime offensive, et il est vital pour les français de choisir le bon afin de placer les rares divisions de réserve disponibles.

Cependant, les télégrammes envoyés le 1er juin révèlent à Painvin et au service du chiffre une terrible surprise. Ils ne sont plus codés à l'aide des cinq lettres A,D,F,G,X, mais désormais à l'aide de six lettres, A,D,F,G,V et X.

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

Immédiatement, Painvin a la bonne idée :

- Avec 5 lettres, on peut former 25 bigrammes et donc coder 25 symboles, soit toutes les lettres de l'alphabet sauf une.
- Avec 6 lettres, on peut former 36 bigrammes et coder les 26 lettres de l'alphabet et les 10 chiffres.

C'est effectivement la différence entre les systèmes ADFGX et ADFGVX.

Le 2 juin, après deux jours et une nuit de travail sans relâche, il parvient à déterminer les clés utilisées la veille. Les messages sont alors déchiffrés et l'un d'entre eux révèle une information vitale :

“Hâtez l'approvisionnement en munitions, le faire même de jour tant que l'on n'est pas vu.”


TÉLÉGRAMME CHIFFRE

Général Commandant en Chef

Etat-Major Bacon

Picardie

Le radiogramme suivant, [illegible] un poste situé près de Rémaugis, le 1er Juin, est donné comme Guillemots. Hâtez l'approvisionnement en munitions, le faire même de jour tant qu'on n'est pas vu - Guillemots.

CHIFFRE

Ce télégramme provient du Haut Commandement allemand et est envoyé à une grande unité dans la région de Rémaugis, probablement à Tilloloy. La future attaque allemande avait donc pour objectif Compiègne, lui ouvrant ainsi la voie directe de Paris. Elle a eu lieu le 9 juin mais fut repoussée par une contre-offensive du général Mangin, préparée en partie grâce à l'information obtenue par Painvin.

Radiogramme de la Victoire

L’histoire de ce déchiffrement fut gardée secrète pendant 50 ans. Painvin, qui fit ensuite une grande carrière dans l'industrie, ne la révéla pas avant 1968. Une vitrine du musée de l'armée, à l'Hôtel des Invalides de Paris, retrace l'histoire de ce déchiffrement. On peut y lire le texte suivant :

"Le Radiogramme de la Victoire"

En 1918, les offensives allemandes sur le front britannique, le 21 mars, puis sur le front français de l'Aisne, le 27 mai, menaçaient directement Paris. Nul ne savait alors où se produirait la prochaine offensive ennemie. Le travail de nos cryptologues devait permettre de le savoir avec exactitude.

Le nouveau chiffre allemand mis en service en mars 1918 n'utilisait que cinq lettres: A, D, F, G, X. Ce système très compliqué nécessitait l'emploi de deux clés, changées chaque jour. Dès le 5 avril, le capitaine G.-J. PAINVIN avait découvert, par l'étude des messages chiffrés du 1er avril, les deux clés utilisées et reconstitué le système de chiffrement.

Mais le 1er juin, en pleine crise de l'offensive sur l'Aisne, les Allemands ajoutèrent une sixième lettre, le V , mettant nos services aux prises avec une difficulté nouvelle. Le 2 juin, le capitaine PAINVIN avait résolu le problème et restitué les deux clés. Elles permirent le décryptage de tous les messages chiffrés captés le 1er juin. Parmi ceux-ci figurait un radiogramme adressé par le Haut Commandement allemand à un Etat-Major d'Armée repéré par la radiogoniométrie dans la région de Rémaugis, à l'est de Montdidier.

"Accélérer la montée des munitions. Point. Même pendant le jour partout où l'on n'est pas vu."

Les Divisions du Général MANGIN furent donc concentrées dès les premiers jours de juin face au point précis où se déclencha, le 9 juin, l'offensive allemande. Celle-ci échoua. La porte de Paris était définitivement fermée à l'ennemi. Pour nous, celle de la victoire allait s'ouvrir.

III - Comment ADFGVX marche

Chiffrer

Le chiffrement ADFGVX utilise une grille de substitution de 36 caractères (composée des 26 lettres de l'alphabet latin et des 10 chiffres). Les lignes et les colonnes sont nommées, de haut en bas et de gauche à droite, par les lettres ADFGVX. Chaque lettre du message claire doit exister dans la grille afin de pouvoir être retranscrit sous la forme de coordonnées.

Le chiffrement se décompose en deux parties. La première partie consiste à substituer les lettres du message claire par le coordonnées dans la grille de substitution.

Exemple

	A	D	F	G	V	X
A	8	t	b	w	r	q
D	p	4	c	g	2	9
F	3	o	5	m	x	e
G	d	a	z	j	s	y
V	l	h	7	u	v	0
X	n	1	k	6	i	f

Le message clair “lancer assaut” deviendra : AV DG AX FD XF VA DG VG VG DG GV DA.

La seconde partie consiste en une transposition par permutation basée sur un mot clé. Le message doit être écrit dans un tableau de largeur n (n étant la largeur du mot clé). Ensuite les colonnes sont permutées de manière à être ordonnées de manière alphabétique. Cette étape nécessite que le mot clé ne contiennent pas de doublon et que le message remplisse entièrement la dernière ligne du tableau (si ce n’est pas le cas il faut ajouter des lettres à la fin du message afin de combler le vide).

Exemple

B(1)	**R(2)**	**A(3)**	**V(4)**	**O(5)**
A	V	D	G	A
X	F	D	X	F
V	A	D	C	V
G	V	G	D	G
G	V	D	A	**X**

deviendra :

A(3)	**B(1)**	**O(5)**	**R(2)**	**V(4)**
D	A	A	V	G
D	X	F	F	X
D	V	V	A	C
G	G	G	V	D
D	G	**X**	V	A

Le message chiffré final est : DA AV GD XF FX DV VA CG GG VD DG XV A

Déchiffrer

Le déchiffrement nécessite de connaître la grille de substitution ainsi que la clé de transposition.
Un tableau de **n** colonnes où **n** est la taille de la clé contient le message chiffré qui est transcrit verticalement (i.e de haut en bas et de gauche à droite).

Exemple

A (3)	B (1)	O (5)	R (2)	V (4)
D	A	A	V	G
D	X	F	F	X
D	V	V	A	C
G	G	G	V	D
D	G	**X**	V	A

Le tableau subit ensuite une permutation inverse des colonnes. Afin de retrouver l'ordre original des lettres, il faut permuter les colonnes en fonction de l'ordre des lettres de la clé.

Exemple

B(1)	R(2)	A(3)	V(4)	O(5)
A	V	D	G	A
X	F	D	X	F
V	A	D	C	V
G	V	G	D	G
G	V	D	A	**X**

Il faut ensuite récupérer le message intermédiaire chiffré qui est constitué des lettres du tableau lu en lignes.

Message intermédiaire : AV DG AX FD XF VA DG VG VG DG GV DA

Enfin, il faut remplacer chaque bigramme du message intermédiaire par la lettre de la grille de substitution qui correspond. On obtient donc le message déchiffré.

Message déchiffré : lancer assaut

IV - Comment décrypter

Pour décrypter un texte chiffré à l'aide du chiffre ADFGVX, il faut dans un premier temps déterminer la longueur de la clé et remettre les colonnes dans le bon ordre. Pour cela il faut tester toutes les possibilités afin d'obtenir un indice de coïncidence convenable.

L'indice de coïncidence est un indice mesurant la distribution des lettres dans un texte. Il vaut environ 0,0746 dans un texte en français. Si les lettres sont uniformément distribuées (contenu aléatoire sans biais) alors l'indice vaut 0,0385.

Il se calcul avec la formule suivante :

$IC = \sum_{q=A}^{q=Z} \frac{n_q(n_q-1)}{n(n-1)}$ avec n le nombre de lettres total du message, n_A le nombre de A, n_B le nombre de B, etc.

Dans le cas d'un texte chiffré à l'aide du chiffre ADFGVX, l'alphabet sera composé des bigramme AA, AD, AF, …, DA, DD, …, XX.

Pour trouver le bon ordre de colonne, il faut donc essayer de les transposer en essayant toutes les possibilités jusqu'à obtenir un indice de coïncidence convenable. Si la clés est de 7 caractères, cela revient à faire $\sum_{n=2}^{n=7} n!$ soit 5 040 essais.

Une fois cette étape finie, on suppose que le texte est dans le bon ordre et que seulement une substitution est appliquée aux lettres. Pour retrouver le texte original, il faut regarder la fréquence de chaque bigramme et le comparer à la fréquence de lettres de l'alphabet dans la langue du texte. Par exemple en français, la lettre la plus utilisée est le e avec une fréquence d'apparition de 12.10% (viens ensuite le a, le i puis le s). Afin d'automatiser ce processus, il est possible d'utiliser un dictionnaire afin de comparer les mots obtenus (certaines lettres ayant des fréquences très proches, il est difficile de les différencier).

V - Sources

Le chiffre ADFGVX

- Chiffre ADFGVX — Wikipédia (wikipedia.org)
- Carré de Polybe — Wikipédia (wikipedia.org)
- ADFGVX Cipher - Crypto Corner (interactive-maths.com)

Contexte historique :

- Le radiogramme de la victoire (bibmath.net)
- La Première Guerre mondiale 1914-1918 - Le Point
- Colonel Fritz Nebel (1891–1967) - Le blog crypto (over-blog.fr)
- Georges Painvin — Wikipédia (wikipedia.org)
- A Brief History of Cryptological Systems – Aircamp Games
- Le chiffre ADFGVX - Le blog crypto (over-blog.fr)

Comment ADFGVX marche:

- Chiffre ADFGVX (wikipedia.org)
- ADFGVX cipher (wikipedia.org)
- Chiffre ADFGVX (dcode.fr)

Comment décrypter:

- Breaking ADFGVX (lilxam.tuxfamily.org)
- Décryptez les secrets les mieux gardes (zestedesavoir.com)
- Indice de coïncidence (https://fr.wikipedia.org)
- Fréquence d'apparition des lettres en français (wikipedia.org)