LES FICHES DU CLUB ALKINDI **juillet 2021**
FICHE N° 5

LES CHIFFREMENTS PAR TRANSPOSITION

Le chiffrement par transposition constitue le deuxième grand moyen utilisé pour chiffrer. Il consiste simplement à mélanger toutes les lettres du message clair dans un ordre prédéfini, ordre qui sera inversé par le destinataire pour le déchiffrement. On pourrait presque considérer le message chiffré comme un anagramme composé de toutes les lettres du message clair.

Voyons les principales techniques de transposition :

1. La scytale (Grèce antique)

C'est un bâton ou un cylindre en bois autour duquel on enroulait une lanière de cuir. On écrivait sur cette lanière le message clair, normalement, de gauche à droite. Puis la lanière était déroulée et le messager la portait comme une ceinture. La lanière une fois déroulée, les lettres écrites ne forment aucune suite logique de mots.

Il suffisait au destinataire d'enrouler la lanière sur un cylindre de même diamètre pour lire le message.

Plutarque raconte son utilisation par Lysandre, général de Sparte, en 404 avant J-C.

La scytale est aussi appelée « *bâton de Plutarque* ». Une BD des aventures de Blake et Mortimer, sortie en 2014, par Yves Sente et André Juillard, porte le titre « Le bâton de Plutarque ».

2. Le chiffre *rail fence* ou zigzag

Le chiffre *rail fence* est une méthode de transposition simple, qui a été employée pendant la guerre de Sécession aux États Unis (1861 - 1865). Elle consiste à écrire les chiffres en zig-zag, sur deux ou trois lignes, et à relever le texte en ligne.

Exemple : Message clair : **Rimbaud Le dormeur du val** sera écrit comme ceci :

R				**A**				**E**				**M**				**D**				**L**
	I		**B**		**U**		**L**		**D**		**R**		**E**		**R**		**U**		**A**	
		M				**D**				**O**				**U**				**V**		

et sera chiffré : **RAEMDLI BULDRER UAMDOUV**

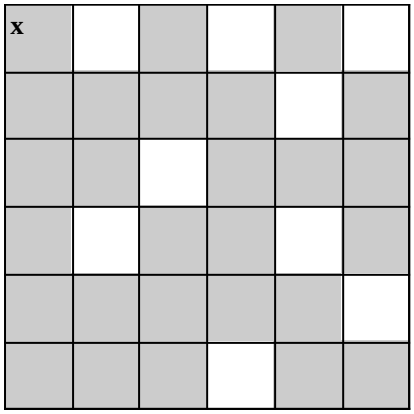
L’énigme 15 est construite sur ce thème.

3. Les grilles tournantes

Merci à M. Hervé Lehning à qui je me suis permis d’emprunter son modèle de grille tournante dans son remarquable livre *La Bible des codes secrets* (voir fiche n° 10).

On prend un carré en carton de 6 cm sur 6 cm. On dessine sur ce carton 36 petits carré de 1 cm de côté qui forment 6 x 6 cases. Puis 9 de ces petits carrés sont ajourés.

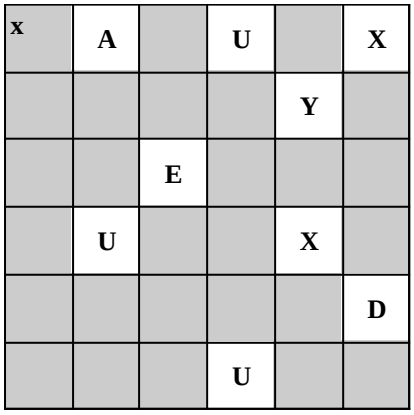
Dessin :



Les 9 cases blanches sont ajourées. La petite croix en haut à gauche permet de repérer la position initiale du carré.

Message clair : **Aux yeux du souvenir que le monde est petit**

On commence par écrire les lettre du clair en remplissant les trous dans l’ordre normal de l’écriture, de gauche à droite et de haut en bas. On va donc écrire les 9 premières lettres ainsi :



Puis on tourne le carré en carton d' 1/4 de tour dans le sens des aiguilles d'une montre et on écrit les 9 lettres suivantes dans les cases ajourées. On recommence de la même façon une 2ème et 3ème fois. A la fin, on obtient ceci :

T	**A**	**E**	**U**	**T**	**X**
D	**P**	**N**	**I**	**Y**	**S**
S	**N**	**E**	**E**	**Q**	**X**
Q	**U**	**E**	**M**	**X**	**O**
E	**E**	**I**	**T**	**V**	**D**
L	**R**	**E**	**U**	**U**	**U**

Le message comportant 35 lettres, il reste une case vide (en jaune) que l'on remplit par un X par exemple. Les cases ajourées ont été conçues de telle sorte qu'en tournant 3 fois le carré en carton, elles couvrent tous les petits carrés de ce carton. On a positionné 9 x 4 lettres, autrement dit 6 x6.

Le destinataire déchiffre en faisant les opérations en sens inverse avec le même modèle de carré ajouré. Si l'on écrit le message crypté sans espace, le déchiffrement n'est pas évident :

TAEUTXDPNIYSSNEEQXQUEMXOEEITVDLREUUU

L'énigme 40 est une forme de grille tournante. Dans son roman *Mathias Sandorf*, Jules Verne nous fait une très belle démonstration de déchiffrement d'un message crypté selon cette méthode. Un message secret chiffré par transposition apparaît également dans le célèbre *Voyage au centre de la Terre.*

4. Les transpositions rectangulaires

- Une première méthode, basique, consiste à écrire le clair en lignes et à le relever en colonnes.

Ainsi le clair « **Une tortue était, à la tête légère »**

s'écrira par exemple dans un rectangle de 9 X 3 :

U	**N**	**E**	**T**	**O**	**R**	**T**	**U**	**E**
E	**T**	**A**	**I**	**T**	**A**	**L**	**A**	**T**
E	**T**	**E**	**L**	**E**	**G**	**E**	**R**	**E**

et sera relevé en colonnes, de gauche à droite et de haut en bas :

UEENTTEAETILOTERAGTLEUARETE

Pour décrypter, il faut commencer par essayer de déterminer les dimensions du rectangle, puis tenter des essais en positionnant les lettres. Il faut se munir d'un bon crayon et d'une bonne gomme.

- Mais bien sûr on peut compliquer le chiffrement en appliquant *une clef :*

5. Transposition rectangulaire avec clef :

Commençons par créer un tableau simple : Exemple :

Clair : « **Qui lasse de son trou voulut voir le pays »**

Le texte comporte 33 lettres. On rajoute 2 lettres factices à la fin, par exemple M et G, pour obtenir un tableau de 7 colonnes sur 5 lignes. Ce qui donne :

Q	**U**	**I**	**L**	**A**	**S**	**S**
E	**D**	**E**	**S**	**O**	**N**	**T**
R	**O**	**U**	**V**	**O**	**U**	**L**
U	**T**	**V**	**O**	**I**	**R**	**L**
E	**P**	**A**	**Y**	**S**	**M**	**G**

On choisit ensuite une clef, par exemple : **VERLAINE**
On écrit les lettres de la clef dans l'ordre alphabétique en retirant les doublons : **A E I L N R V**

Et on les numérote : **A E I L N R V**
1 2 3 4 5 6 7

Enfin on réécrit la clef normalement, ce qui nous donne :

V E R L A I N E
7 2 6 4 1 3 5

C'est presque terminé. Il suffit de numéroter les colonnes du tableau avec les chiffres de la clé :

7	**2**	**6**	**4**	**1**	**3**	**5**
Q	**U**	**I**	**L**	**A**	**S**	**S**
E	**D**	**E**	**S**	**O**	**N**	**T**
R	**O**	**U**	**V**	**O**	**U**	**L**
U	**T**	**V**	**O**	**I**	**R**	**L**
E	**P**	**A**	**Y**	**S**	**M**	**G**

et de reclasser ces colonnes dans l'ordre croissant des chiffres :

1	2	3	4	5	6	7
A	U	S	L	S	I	Q
O	D	N	S	T	E	E
O	O	U	V	L	U	R
I	T	R	O	L	V	U
S	P	M	Y	G	A	E

En lisant les colonnes de haut en bas, le message chiffré sera donc

AOOISUDOTPSNURMLSVOYSTLLGIEUVAQERUE

Le destinataire, avec la clef, pourra reconstituer l'ordre des colonnes et déchiffrer le message. Ce type de chiffrement est extrêmement difficile à casser.

A noter que si l'on y regarde bien, le chiffrement avec la scytale est une transposition rectangulaire. La clef est le diamètre du rouleau.

6. Le chiffre Übchi

Ce chiffrement était utilisé par l'armée allemande au début de la Première Guerre mondiale. Il consiste en une double transposition de lignes et de colonnes et utilise également une clef. C'est un grand classique. Exemple :

Message clair : **Deux canards à qui la commère**
Communiqua ce beau dessein

Clef **: BAUDELAIRE**

Comme dans le cas du paragraphe 5, on numérote les lettres de la clef, puis on copie le texte :

B A U D E L A I R E
3 1 10 4 5 8 2 7 9 6

3	1	10	4	5	8	2	7	9	6
D	E	U	X	C	A	N	A	R	D
S	A	Q	U	I	L	A	C	O	M
M	E	R	E	C	O	M	M	U	N
I	Q	U	A	C	E	B	E	A	U
D	E	S	S	E	I	N	C	I	A

En relevant *les colonnes* dans l'ordre de la clef, nous avons donc :

EAEQE NAMBN DSMID XUEAS CICCE DMNUA ACMEC ALOEI ROUAI UQRUS

On recopie ce texte *en lignes* dans le tableau, ce qui donne :

3	1	10	4	5	8	2	7	9	6
E	A	E	Q	E	N	A	M	B	N
D	S	M	I	D	X	U	E	A	S
C	I	C	C	E	D	M	N	U	A
A	C	M	E	C	A	L	O	E	I
R	O	U	A	I	U	O	R	U	S

et on recopie de nouveau le texte pris en colonnes, toujours dans l'ordre des colonnes indiqué par la clef. Nous avons alors le message chiffré définitif :

Crypto : ASICO AUMLQ EDCAR QICEA EDECI NSAIS MENOR NDAU BAUEU EMCMU

Ce double chiffrement avec clef était extrêmement complexe. La clef était changée toutes les semaines. En 1914, le mode de chiffrement (l'algorithme) était connu par les cryptanalystes de l'armée française. Grâce à des messages de longueur égale et avec un énorme travail, ils parvenaient souvent à décrypter, ce qui prenait quand même parfois quelques jours.

L'énigme 29 est un chiffrement Übchi. La clef est donnée, les utilisateurs qui proposent des énigmes sur ce site sont trop bons. Bon courage quand même.

7. Le chiffre ADFGX

Nous allons terminer cette revue des principaux modes de chiffrement par transposition avec un chiffre également utilisé par l'armée allemande tout à la fin de la Première Guerre mondiale, **le chiffre ADFGX.** Pourquoi ce nom bizarre ? Parce que dans une transmission en alphabet Morse, les lettre A,D,F,G,X sont très distinctes et ne peuvent pas être confondues.

Au départ, ce chiffre utilise un carré de Polybe bien connu (voir fiche n° 3). Ce carré de Polybe est rempli avec une clef qui est changée chaque jour. On inscrit la clef dans les premières cases du carré. Le J et le I sont confondus pour pouvoir inscrire les 25 lettres. On supprime les doublons et après avoir écrit les lettres de la clef, on écrit les lettres manquantes (voir Fiche n° 3 paragraphe 2, le carré de Polybe avec une clef).

Exemple : Clef : **JEAN DE LA FONTAINE**

Nous obtenons le carré suivant, le J se transformant en I :

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

soit à chiffrer le message clair : **La tortue et les deux canards**

Le codage du clair avec ce carré de Polybe s'établit ainsi :

DA AF DG DF GF DG GX AD AD DG DA AD GG AX AD GX XF FA AF AG AF GF AX GG

Ce chiffrement est une *substitution* simple. Nous allons maintenant effectuer une *transposition*. Cette 2ème opération se nomme un ***surchiffrement,*** car on chiffre une deuxième fois le message déjà chiffré. Pour ce faire, on choisit une 2ème clef et on numérote les lettres de cette clef de la même façon que dans le chiffre Übchi (paragraphe 6).

Soit la clef : **FLAUBERT** qui est donc numérotée dans l'ordre des lettres

F	**L**	**A**	**U**	**B**	**E**	**R**	**T**
4	**5**	**1**	**8**	**2**	**3**	**6**	**7**

Puis on écrit le message codé ci-dessus en ADFGX dans un tableau de 8 colonnes, en numérotant les colonnes selon la clef « *Flaubert* ». Ce qui nous donne :

4	**5**	**1**	**8**	**2**	**3**	**6**	**7**
D	**A**	**A**	**F**	**D**	**G**	**D**	**F**
G	**F**	**D**	**G**	**G**	**X**	**A**	**D**
A	**D**	**D**	**G**	**D**	**A**	**A**	**D**
G	**G**	**A**	**X**	**A**	**D**	**G**	**X**
X	**F**	**F**	**A**	**A**	**F**	**A**	**G**
A	**F**	**G**	**F**	**A**	**X**	**G**	**G**

Pour terminer, on relève les lettres par colonnes dans l'ordre défini par la clef « *Flaubert* » c'est à dire 4 5 1 8 2 3 6 7 . Nous obtenons ainsi le message chiffré définitif :

Crypto : ADDAFG DGDAAA GXADFX DGAGXA AFDGFF DAAGAG FDDXGG FGGXAF

que l'on peut écrire par groupe de 5 lettres pour ne laisser aucun indice sur la longueur des colonnes du tableau. Tant qu'à brouiller les pistes …

Remarquons que le message clair comportait 24 lettres. La transposition des lettres dans ce tableau s'est effectuée dans 48 cases. On a donc séparé les groupes de 2 lettres du code ADFGX, ce qui rend la reconstitution du 1er message chiffré quasi impossible sans la clef.

Remarquons également que ce type de chiffrement utilise 2 clefs : l'une pour la substitution dans le carré de Polybe, l'autre dans la transposition pour écrire les colonnes dans l'ordre. Toujours l'importance d'une clef !

Ce dernier mode de chiffrement est particulièrement complexe, et félicitations si vous avez lu cette fiche jusqu'au bout ! Le chiffre ADFGX, utilisé par l'armée allemande, représente l'un des sommet de la cryptographie du début du XXe siècle.

8. Conclusion : un peu d'Histoire

Le chiffre ADFGX fut utilisé par les Allemands à partir du 5 mars 1918. Un mois plus tard, après des semaines de travail jour et nuit, un cryptanalyste français génial, Georges Painvin, parvint à le décrypter.

Trois mois après sa création, le 1er juin 1918, ce code fut modifié et devint ADFGVX. L'ajout de la lettre V permettait de créer un carré de 6 x 6, c'est à dire de crypter les 26 lettres et les 10 chiffres. En comparant des messages envoyés par des mêmes unités et comportant des débuts identiques, Georges Painvain décrypta ce nouveau code très rapidement. Les Services de Renseignements français furent ainsi informés des offensives allemandes et les troupes purent les contrer favorablement, ce qui pesa fortement sur les derniers mois de la Grande Guerre.

Après la Première Guerre mondiale, nous entrons dans l'ère des machines électro-mécaniques qui trouvera son apogée avec la célèbre machine Enigma inventée au début de la période de l'entre-deux guerres. Puis viendront les ordinateurs et de nouveaux modes de chiffrement sans échange de clefs, comme le système RSA, construit sur d'étranges fonctions mathématiques.

Nous verrons tout cela dans les deux fiches suivantes. Mais vous pouvez maintenant laisser de côté les feuilles de papier, le crayon et la gomme. Ce sera simplement pour la culture générale et le plaisir d'en parler avec vos parents et vos amis.

****
*****
***
*