Initiation à l'histoire de la cryptographie

par Saint-Erulo

CHAPITRES

PRÉSENTATION ET PLAN DES FICHES

1. PRÉSENTATION DES FICHES :

Ces fiches ont été rédigées spécialement pour vous *initier à la cryptographie* et vous donner l'envie de vous amuser à déchiffrer des messages secrets. Au début, ce sera un jeu, puis si vous y prenez goût, cela deviendra une passion. Éventuellement cela pourra devenir votre métier.

Cette initiation aura un aspect principalement historique : nous étudierons les deux principales méthodes de chiffrement, *la substitution* (remplacement des lettres par d'autres lettres, par des chiffres ou par des symboles) et *la transposition* (mélange des lettres selon une méthode prédéfinie). Nous verrons également *les systèmes de codage et les dictionnaires.*

Cet aspect historique est fondamental. Pour bien débuter dans le monde de la cryptographie, il est indispensable d'apprendre comment, au cours des siècles, ont évolué les méthodes pour cacher aux ennemis ou aux simples tiers les messages que l'on adresse à ses alliés ou à ses amis. Cela permet de s'initier au jargon bizarre de la cryptographie : chiffrement, clé, analyse fréquentielle, casser un code, système RSA... (ces mots seront définis au fur et à mesure). Mais surtout, cette histoire permet de comprendre l'extraordinaire révolution de la cryptographie moderne, la rupture brutale qui s'est effectuée au cours des années 1970-1980, rupture qui a balayé tous les anciens concepts, et les nouveautés qui en ont résulté : protection des données dans les ordinateurs, communications dans les réseaux sociaux, utilisation privée dans les cartes bancaires etc.

Le système de *« fiches » écrites* a été volontairement choisi. En effet, il existe de nombreuses vidéos sur YouTube, bien réalisées, attrayantes, qui proposent des cours de cryptographie. Mais au départ, pour vraiment comprendre et progresser dans ce domaine, il faut avoir devant soi un papier et un crayon, écrire, chercher et finalement trouver la solution. C'est comme l'histoire-géo, les maths ou le sport , ça ne vient pas tout seul : il faut bosser, faire des exercices, s'entraîner. Des sites Internet vous proposent de déchiffrer automatiquement des messages secrets. Ces sites sont très bien réalisés, mais encore faut-il savoir comment les utiliser, et déterminer à quel type de message on a affaire. Et là, seule la pratique concrète des recherches avec un papier, un crayon, une simple calculatrice vous permettra d'utiliser efficacement ces sites. On peut aussi se servir d'Excel ou créer des programmes Python, mais là encore il faut connaître et comprendre les modes de chiffrement de base. Les énigmes du Club Alkindi sont là pour vous amuser, mais aussi pour vous y entraîner. Et vous découvrirez le plaisir de trouver la solution, de déchiffrer un message secret.

Ces fiches sont évolutives : elles sont éditées en fichiers pdf, et on peut facilement les modifier, supprimer une ancienne fiche, y substituer une nouvelle. Bien entendu vous pouvez les télécharger.

N’hésitez pas à poser des questions et à signaler des erreurs ou des améliorations possibles, les échanges nous permettront de progresser.

Il existe sur le sujet quelques livres très bien faits, et d’autres un peu moins bons. Nous les évoquerons. Il existe également de nombreux sites Internet, et quelques films. Là aussi nous pourrons tous échanger sur ces sujets.

2. PLAN DES FICHES :

Ce plan est donné à titre indicatif. Il donne une structure générale, avec quelques données incontournables, et suit une évolution historique. Il essaye également d’être le plus pédagogique possible. Mais il n’est pas figé et est modifiable : l’auteur peut faire des erreurs, il apportera des améliorations, et les lecteurs pourront demander à approfondir tel ou tel point.

Fiche 1 : Présentation et plan des fiches

Fiche 2 : A quoi sert la cryptographie ?

- Jusqu’au milieu du XXe siècle, le secret des messages concerne principalement les militaires et les diplomates. Le problème de fond : communiquer en sécurité, c’est à dire donner une information à un ami en cachant cette information à tous les autres.

- Lutte constante entre les chiffreurs et les déchiffreurs : créer une méthode secrète, la découvrir.

- Les deux méthodes de base du chiffrement : substitution et transposition.

- *Substitution* = remplacement d’une lettre par une autre lettre, un nombre ou un symbole - -
- *Transposition* = mélange des lettres selon une méthode prédéfinie.
  Exemples : substitution simple lettre à lettre, transposition par une grille rectangulaire.

- Il existe aussi *les codes et les dictionnaires.*

Fiche 3 : Les chiffrements par substitution

Définition des termes **:** clair, cryptogramme, clef, algorithme...

- Le chiffrement par substitution simple

- Le chiffre de Jules César (1er siècle avant J-C)
- Inversion de l’alphabet : l’Atbash dans la Bible hébraïque
- Méthodes basiques de substitution : une lettre, un nombre ou un symbole remplacent une lettre.

- Le chiffrement par bigrammes **:** Le carré de Polybe (150 avant J-C)

- Les méthodes classiques de substitution simple

- Comment décrypter ? : l’analyse de fréquence, AlKindi (IXe siècle)

- Neutraliser l’analyse de fréquence : Le chiffre de Vigenère (XVIe siècle) :

- Le chiffre inviolable **:** le concept de clé aléatoire utilisée une seule fois.

- Inconvénient des clés aléatoires utilisées « une fois » : lourdeur de la méthode, difficulté et risque dans la communication des clefs aux amis.

- Le principe de *Kerckhoffs* (1883)

Fiche 4 : Les codes, les dictionnaires : une forme de substitution

- Les codes : le Morse, le système binaire, l'ASCII, l'alphabet radio international : ce sont des façons de coder, *mais ce n'est pas de la cryptographie*, il n'y a rien de caché.

- Les codes et les dictionnaires : Exemples : le chiffre des Templiers, le chiffre des francs-maçons, Marie Stuart, le Grand Chiffre de Louis XIV etc.

Fiche 5 : Les chiffrements par transposition :

- Très utilisé par les militaires, surtout au XIXe siècle et jusqu'à la Seconde Guerre mondiale. Très efficace et redoutable. Mais aussi quelques inconvénients.

- la scytale spartiate ou bâton de Plutarque (- 600 av. J-C)
- le chiffre *rail fence* ou zig zag
- les grilles rectangulaires
- le chiffre Übchi
- le chiffre ADFGX : *substitution,* puis *surchiffrement* au moyen d'une *transposition*

Fiche 6 : L' entre-deux guerres : Enigma

On reste dans la substitution, mais ça se complique : c'est l'ère des machines électromécaniques, ancêtres des ordinateurs (la « bombe » d'Alan Turing pour déchiffrer Enigma), Dans le concours Alkindi, il y a des énigmes avec des machines (figurées !)

Fiche 7 : Une rupture radicale : le système RSA (1975)

Petits rappels simples d'arithmétique : les nombres premiers, les fonctions à sens unique (fonction modulo), les puissances.

Les précurseurs : Le système Diffie, Hellmann, Merke

Le système RSA : Ronald Rivest, Adi Shamir et Leonard Adleman

Révolution complète dans les méthodes de chiffrement : aucune clef n'est échangée avec le destinataire. Concepts de clef symétrique et asymétrique, clef publique et clef privée.

Fiche 8 : Que faire face à une énigme ?

- Des chiffres ? Des lettres ? On est face à quel type de chiffrement ?
- Exemples
- Trouver l'algorithme, la clef ?
- L'environnement, les indices, les mots probables
- L'importance de travailler en équipe : des littéraires et des matheux
- La question de la vitesse

Fiche 9 : Résolution d'une énigme complexe

Exemple de la résolution de l'exercice n° 7 posé à la finale du concours Alkindi en 2019.

Fiche 10 : Les livres, les sites Internet, les films, les séries

Quelques bons livres en français, des grands classiques.
Des sites Internet, un grand film, une très bonne série, une belle pièce de théâtre.

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

A QUOI SERT LA CRYPTOGRAPHIE ?

De tous temps, les échanges d'informations entre les hommes (ou les femmes) ont eu besoin, souvent, d'être secrets. Dans les domaines politiques, diplomatiques, militaires, mais aussi dans des sphères plus privées telles que les relations amoureuses, par exemple.

Le secret des communications entre les personnes, ou aujourd'hui entre les ordinateurs, repose donc sur l'emploi de méthodes qui assurent cette confidentialité des messages échangés : c'est l'objet de la cryptographie.

L'Histoire nous montre de multiples exemples de messages secrets qui ont décidé de la victoire ou de la défaite d'une bataille, ou causé des drames personnels : ainsi par exemple la triste histoire de Marie Stuart :

Marie Stuart était reine d'Écosse. A la suite de longues aventures, à l'âge de 26 ans, Marie fût emprisonnée au château de Chartley, au nord de l'Angleterre. Elle était retenue prisonnière par Elisabeth I^{re}, reine d'Angleterre. Ses contacts avec le monde extérieur s'effectuaient par des lettres chiffrées par son secrétaire et sorties clandestinement de sa prison. Or le messager qui transportait les lettres était un traître à la cause de Marie, un agent double qui les transmettait à un ministre d'Élizabeth I^{re}. Ce ministre employait un excellent linguiste, Thomas Phelippes, qui parlait 5 langues et était l'un des meilleurs cryptanalystes d'Europe.

Marie était en prison depuis de nombreuses années lorsque des nobles écossais préparèrent un complot pour la faire évader et assassiner Élizabeth ! L'auteur du complot communiqua avec Marie et dans une lettre lui demanda son accord. Marie répondit affirmativement. Le messager agent double confia comme à son habitude cette lettre au ministre d'Élizabeth et ce dernier eut une idée machiavélique : après avoir fait décrypter cette lettre de Marie Stuart adressée au chef des nobles écossais, il la fit recopier par Phelippes avec le même code secret et en plus, demanda au destinataire le nom de tous les comploteurs ! Le chef des nobles répondit et livra ainsi, malgré lui, tous ses complices, qui furent exécutés. Face aux preuves écrites, Marie Stuart eut un procès et périt également sur l'échafaud.

Il est certain que le procédé de chiffrement employé par Marie Stuart devait comporter quelques faiblesses... Cette malheureuse histoire est emblématique de la lutte constante que se livrent les concepteurs de codes secrets et ceux qui cherchent à percer ces secrets, les « briseurs de codes ». Les livres sur la cryptographie racontent de nombreuses histoires de ce type, depuis l'Antiquité jusqu'à aujourd'hui : rappelez-vous l'affaire Edward Snowden, avec ses publications des documents secrets de la CIA et de la NSA (National Security Agency).

Tout au long de ces fiches, nous étudierons quelques méthodes (parmi de nombreuses autres) pour créer des codes secrets, et dans chaque cas, nous verrons les techniques pour essayer de les « décrypter » comme on dit dans le jargon de la cryptographie. Ces fiches vous apprendront en partie l'histoire de la cryptographie, histoire nécessaire à connaître pour bien comprendre les

différentes évolutions de ce domaine d'activité. Par ailleurs, elles vous permettront de mieux résoudre les énigmes présentées sur ce site, en vous amusant, espérons-le.

Les méthodes de base de chiffrement :

Il existe principalement deux méthodes pour chiffrer un texte, la substitution et la transposition.

1) ***La substitution,*** qui consiste à remplacer les lettres du message clair par d'autres lettres, ou par des nombres. Exemple de substitution de lettres par des nombres :

On remplace les 26 lettres de l'alphabet par les 26 premiers nombres écrits en sens inverse, comme suit :

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1

La lettre A est remplacée par 26, B par 25, C par 24 etc.

Le message : ***Demain dès l'aube, à l'heure où blanchit la campagne,***

sera chiffré par : 23 22 14 26 18 13 23 22 8 15 26 6 25 22 26 15 19 22 6 9 22 etc...

2) ***La transposition***, qui consiste à mélanger les lettres du message clair selon un ordre prédéfini.

Exemple de transposition classique : on écrit le message dans un carré de 6 x6, en ligne, puis on relève les lettres en colonne.

Le message : ***Je partirai. Vois-tu, je sais que tu m'attends.*** s'écrit dans le carré

J	E	P	A	R	T
I	R	A	I	V	O
I	S	T	U	J	E
S	A	I	S	Q	U
E	T	U	M	A	T
T	E	N	D	S	

Puis on écrit le message en lisant par colonnes de haut en bas et de gauche à droite :

JIISETERSATERATIUNAIUSMDRVJQASTOEUT

On peut laisser les cases vides comme telles ou y placer une lettre.

Le déchiffrement est souvent complexe. Si l'on ne connaît pas les dimensions du carré et que la transposition suit un ordre compliqué, il est très difficile de reconstituer le message clair.

3) ***Les codes et les dictionnaires***

Dans un code, une lettre souvent est remplacée par un signe ou par un symbole. On pourra citer par exemple le chiffre des Templiers ou le chiffre des francs-maçons.

Dans un « dictionnaire », ce sont des mots et non pas simplement des lettres qui sont remplacés par des nombres. Le Grand Chiffre de Louis XIV en est un bon exemple. En France, le dictionnaire chiffré le plus connu fut celui de F. -J. Sittler.

Les codes et les dictionnaires sont en fait des formes de chiffrements par substitution, et ils seront donc étudiés comme tels dans ces fiches.

Il est également important de ne pas confondre les « codes » ordinaires, publiques, et les codes qui permettent d'effectuer un chiffrement. Ainsi par exemple l'alphabet Morse, le système de numération binaire ou le code ASCII sont des codes. Ils sont parfois employés en cryptographie, mais ce ne sont pas des codes secrets. Ce sont des moyens d'écrire des lettres ou des chiffres d'une façon codée connue du monde entier.

Tout ceci sera expliqué avec de nombreux exemples dans la fiche n° 4.

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

LES CHIFFREMENTS PAR SUBSTITUTION

Quelques définitions pour bien se comprendre :

Clair : message d'origine à transmettre. On le désigne par le « clair »

Chiffrer, crypter, coder : transformer le message d'origine en message secret et incompréhensible pour n'importe qui d'autre que son destinataire.

Cryptogramme : message chiffré. On le désigne aussi par le « crypto ».

Algorithme de chiffrement : Méthode utilisée pour chiffrer. C'est une suite d'opérations à effectuer pour parvenir à chiffrer un texte. On effectue les opérations inverses pour déchiffrer.

Clef : un algorithme de chiffrement nécessite généralement une clef, qui peut être un mot, une phrase, une suite de chiffres connus seulement par l'expéditeur et le destinataire du message.

Déchiffrer : reconstituer le message clair en connaissant le mode de chiffrement et la clef.

Décrypter : trouver le message clair sans connaître le mode de chiffrement ni la clé.

1. Le chiffrement par substitution simple

C'est le système le plus courant : chaque lettre du message clair est remplacée par une autre lettre dans le message chiffré. Commençons par un peu d'Histoire :

1. 1 Le chiffre de Jules César

C'est l'un des plus simples : chaque lettre de l'alphabet est décalée de 3 lettres, ce qui donne :

Clair : A B C D E F G H ...
Crypto : D E F G H I J K

Ainsi le message : VENI VIDI VICI sera chiffré par : YHQL YLGL YLFL

On peut également décaler les lettres de 3, 4, 5… positions, dans un sens ou dans un autre. Dans ce cas général où la longueur du décalage est inconnue, le déchiffrement s'effectue en testant des positions de lettres jusqu'à obtenir un message qui ait un sens.
En fait ce code était utilisé par Jules César pour sa correspondance privée. (Suétone, Vie des 12 Césars, Livre 1, paragraphe 56).

Sur le plan militaire, avec ses généraux, il employait un autre procédé : il écrivait en grec (Guerre des Gaules, Livre 5, paragraphe 48).

1.2 Inversion de l'alphabet

On peut chiffrer en inversant l'ordre des lettres dans l'alphabet, comme suit :

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

Dans la Bible hébraïque, il existe un mode de cryptage appelé l'*Atbash.* Dans ce système, chaque lettre de l'alphabet est remplacée par la lettre qui occupe la même place en partant de la fin de l'alphabet, comme ci-dessus. A= Z, B=Y, etc. Le mot « atbash » est formé par la première lettre de l'alphabet hébreu, aleph, puis tav, la dernière, puis la seconde, beth, et l'avant dernière, shin.
Dans Jérémie, chapitre 25, verset 26, la ville de Babel (Babylone) est appelée Shéshakh,

2. Substitution par bigrammes : le carré de Polybe

Pour rester dans l'Antiquité, citons *le carré de Polybe* (général grec, 200-155 avant J-C,). Les lettres de l'alphabet sont placées dans un carré de 5 x5, comme suit :

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

Chaque lettre est repérée par un couple de nombres. Par exemple, S sera chiffré 43, puisqu'il se trouve ligne 4 et colonne 3. Le J est supprimé pour avoir 25 lettres.

Pour le rendre plus difficile à déchiffrer, on peut convenir d'un mot que l'on commence à écrire dans la grille, en supprimant les doublons, puis on écrit les lettre manquantes.

Exemple avec le mot Polybe :

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

L'énigme n°24 repose sur le principe d'un carré de Polybe, avec une légère variante.

3. Les méthodes classiques de substitution simple

Outre ces méthodes très anciennes et historiquement intéressantes, la méthode de chiffrement par substitution la plus classique consiste tout simplement à remplacer une lettre de l'alphabet par n'importe quelle autre lettre. Mais une même lettre du cryptogramme correspond toujours à la même lettre du message clair et réciproquement.

L'énigme n° 3 est un parfait exemple de ce mode de chiffrement. Voici la première phrase :

PT F'LWOL HAL R'WFT ZTAWMT LWHKTDT DAOL YAWM HAL L'YOTK A ET JW'GF XGOM PT XTWV ZOTF DT DAFUTK DGO-DTDT LO XGWL MKGWXTN HSWL DASOF JW'DGO

L'auteur de l'énigme a conservé les séparations entre les mots ainsi que la ponctuation, sans doute du fait du style très original, ce qui rend cette énigme un peu moins difficile à déchiffrer.

4. Comment déchiffrer ce type de texte ? L'analyse de fréquence

Au IXe siècle, un philosophe et mathématicien arabe, *AlKindi*, a mis au point une technique pour déchiffrer ce type de message : *l'analyse de fréquence.*

Dans une langue donnée, il y a des lettres qui reviennent plus fréquemment que d'autres. En français, par exemple, le E est la lettre la plus répandue, suivie par le A, puis le S, le I etc.
Sur des milliers de pages de texte, la fréquence des lettres est la suivante : 17 ,3 % de E, 8,4 % de A, 8,1 % de S , 7,3 % de I, 7,1 % de N et de T, etc. Vous trouverez partout sur Internet des tables de fréquence des lettres, et elles ne sont pas toutes d'accord entre elles sur les statistiques. Mais peu importe.

L'idée d'AlKindi est donc la suivante (en adaptant de l'arabe au français) : dans le cryptogramme, on compte le nombre de fois où l'on trouve chaque lettre. Si la lettre la plus fréquente est par exemple un M, on supposera qu'il est mis pour le E. Si la 2ème lettre la plus fréquente est le P, elle représentera sans doute le A ou le S, et ainsi de suite pour les 10 premières lettres (E, S, A, I, N, T, R, U, L, O). Bien sûr, on ne tombe pas juste au premier coup, il faut chercher un peu.

Pour continuer le décryptage, on travaille sur les *bigrammes*, c'est à dire sur les couples de lettres. Les bigrammes les plus fréquents en français sont ES, LE, DE, RE… Donc on essaye d'identifier, dans le cryptogramme, des couples de lettres qui pourraient représenter ces bigrammes en clair. On observe également les *répétitions de lettres* : SS, LL, TT … Même travail sur les trigramme : LES, le verbe être à la 3ème personne du singulier EST…

Tout ceci permet, petit à petit, de reconstituer des fragments du texte, et d'attribuer à chaque lettre du crypto une lettre du clair. C'est parfois assez long et fastidieux. Actuellement, certains sites Internet permettent de faire automatiquement ce travail.

Un très bon exemple d'analyse de fréquence est donné dans *Le Scarabée d'or*, la célèbre nouvelle d'Edgar Poe publiée dans le recueil des *Histoires extraordinaires.* L'histoire est écrite à l'origine en anglais, et la traduction de Charles Baudelaire explicite parfaitement tous les raisonnements du narrateur pour parvenir à décrypter un mystérieux parchemin.

Après l'étude de lettres, des bigrammes et des trigrammes, au fur et à mesure que l'on trouve des fragments de mots, on peut faire des hypothèses sur des *mots courants* ou sur des *mots probables* à partir d'indices que l'on possède sur le message : d'où vient-il, quel est son *environnement* ?

Un point important : pour réaliser une analyse de fréquence valable, il faut que le message soit assez long, ou bien il faut avoir plusieurs messages du même auteur. C'est par exemple le cas de l'énigme n° 3, déjà citée. Mais certaines énigmes, qui ne comportent que quelques mots, voire un seul, sont totalement réfractaires à cette méthode.

Face aux tentatives et aux réussites en matière de déchiffrement par l'analyse de fréquence, une parade a été mise au point par un cryptographe, Blaise de Vigenère, au cours du XVIe siècle :

5. Neutraliser la fréquence des lettres : le Chiffre de Vigenère (XVIe siècle)

La méthode de chiffrement inventée par Blaise de Vigenère vers les années 1580 présente quelque complications inhérentes à toute nouveauté. Il utilisait des substitutions mono-alphabétiques, confondait (volontairement) le I, le J et le Y ainsi que le V et le W. On ne s'attardera pas sur la création de cette méthode. Elle a été rapidement simplifié, et est devenue un mode de chiffrement très utilisé jusqu'au XXe siècle. Elle fait partie des bases de la cryptographie.

Le chiffre de Vigenère repose sur une idée simple : l'utilisation d'une clef. La clef est un mot ou une phrase, connue seulement de l'expéditeur et du destinataire du message. Le principe repose sur un décalage des lettres, comme dans le Chiffre de César, mais ce décalage varie à chaque lettre en fonction de la clef.

Pour chiffrer, on utilise une *table de Vigenère*, sorte de table de Pythagore, comme celle utilisée pour l'addition. *Voir le grand tableau page suivante*.

On appelle le message d'origine le « clair » , le message crypté le « crypto ». On procède comme suit : chaque lettre du message clair est repérée sur la 1ère ligne horizontale. Puis on va descendre sur la colonne verticale de cette lettre, jusqu'à la ligne horizontale de la lettre de la clé. La lettre à l' intersection de la lettre « claire » en colonne et de la lettre « clef » en ligne est la lettre cryptée.

Exemple sur le tableau de Vigenère page suivante (suivre les lettres en jaune) : la lettre du clair M avec la lettre de la clef J donnera ==> lettre cryptée V.

Exemple sur un texte : Message clair : **Les sanglots longs des violons de l'automne**
Clef : **Verlaine**
On aura le chiffrement suivant :

Clair	L	**E**	**S**		**S**	**A**	**N**	**G**	**L**	**O**	**T**	**S**		**L**	**O**	**N**	**G**	**S**		**D**	**E**	**S**
Clef	**V**	**E**	**R**		**L**	**A**	**I**	**N**	**E**	**V**	**E**	**R**		**L**	**A**	**I**	**N**	**E**		**V**	**E**	**R**
Crypto	**G**	**I**	**J**		**D**	**A**	**V**	**T**	**P**	**J**	**X**	**J**		**W**	**O**	**V**	**T**	**W**		**Y**	**I**	**J**

Clair	**V**	**I**	**O**	**L**	**O**	**N**	**S**		**D**	**E**		**L**	**A**	**U**	**T**	**O**	**M**	**N**	**E**
Clef	**L**	**A**	**I**	**N**	**E**	**V**	**E**		**R**	**L**		**A**	**I**	**N**	**E**	**V**	**E**	**R**	**L**
Crypto	**G**	**I**	**W**	**Y**	**S**	**I**	**W**		**U**	**P**		**L**	**I**	**H**	**X**	**J**	**Q**	**E**	**P**

Table de Vigenère

Lettres de la clef	Lettres du message clair																									
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

L'importance de ce type de chiffrement est capitale : chaque lettre claire est combinée avec une lettre différente de la clef. Une même lettre est donc chiffrée de différentes manières. L'analyse de la fréquence des lettres dans le message chiffré n'est plus possible.

On vient de voir que les lettres du message clair sont généralement remplacées par d'autres lettres. Mais on peut les remplacer par des chiffres (Énigme n° 1), par d'autres caractères, voire par des symboles. La fiche n° 3, qui traitera des *Codes et des dictionnaires*, en donnera quelques exemples.

Pour introduire la notion *d'algorithme*, on peut écrire que l'algorithme du chiffre de Vigenère est

Clair + Clef = Crypto

Pour déchiffrer ce type de messages, on effectue l'opération inverse à l'aide du tableau de Vigenère :

Crypto - Clef = Clair

On présente souvent le crypto par blocs de 5 lettres, ce qui complique l'analyse des mots probables dans le déchiffrement.

Ce chiffrement avec une clef est-il indéchiffrable ?

A vrai dire, non. En effet, Charles Babbage, vers 1854, a mis au point une méthode qui permet, malgré la clé, de casser ce type de chiffrement. Voici le principe de cette méthode :

Il faut d'abord essayer de trouver la longueur de la clef. Pour se faire, Babbage recherche dans le message chiffré les répétitions de 2 lettres ou 3 lettres. Il suppose que dans ces cas, la même partie de texte clair a été chiffrée avec la même partie de la clef. A partir de là, et en comptant le nombre de lettres entre chaque occurrence de répétitions de lettres identiques, il en déduit la longueur de la clef (avec plusieurs possibilités). Ayant fait une hypothèse sur la longueur de la clef, par exemple une clef de 7 lettres, il divise le message en blocs de 7 lettres et écrit ces blocs les uns en dessous des autres, formant ainsi 7 colonnes. Ainsi, dans une même colonne, les lettres ont toutes été chiffrées par la même lettre de la clef. Enfin, il effectue une analyse de fréquence sur les lettres de ces colonnes en appliquant la méthode expliquée au paragraphe 4. Toutes ces analyses supposent que le crypto soit assez long pour pouvoir être effectuées.

La méthode est assez complexe et dépasse un peu le cadre de ce « cours » qui se veut être une initiation. Si l'on veut bien la comprendre et la travailler, on trouvera aisément des livres ou des sites sur Internet consacrés à la cryptographie qui développent le sujet. (Voir la fiche n° 10).

Pour éviter cette tentative de déchiffrement en utilisant la longueur de la clef, l'idée est venue d'utiliser des clef aussi longues que le message clair, par exemple chiffrer un texte en clair par une clef qui est un texte aussi long que le message clair. Cela complique les choses pour le décrypteur, qui ne peux s'appuyer sur aucune fréquence de lettres. Dans ce cas, il faut travailler à partir de mots probables et supposés dans le texte : mots fréquents, vocabulaire usuel ou vocabulaire technique relatif au sujet du message (militaire, diplomatique…).

En combinant les lettres d'un mot clair supposé avec les lettre du cypto, on peut en déduire un fragment de clef qui a un sens (Crypto moins clair = clef).

Le carré de Vigenère est constitué de lettres, mais on peut travailler sur des chiffres. En posant A=1, B=2, C=3…, le chiffrement peut s'effectuer mathématiquement. On remplace chaque lettre du clair et de la clé par son rang dans l'alphabet, on additionne et on retire 26 si le nombre est supérieur à 26. Le résultat donne le rang de la lettre cryptée.. On peut donc travailler directement avec des nombres, ce qui est plus facile. Faites-le avec un papier et un crayon, vous verrez.

6. Le chiffre inviolable : la clé aléatoire utilisée une fois

Avec l'utilisation d'un algorithme de chiffrement (ici une simple addition) et d'une clef, une idée s'est rapidement imposée : si le clef est composée de lettres au hasard , *aléatoires* comme on dit, une lettre du clair est chiffrée avec n'importe quelle lettre de la clé. Exemple :

Clair : **B L E S S E N T M O N C O E U R D' U N E L A N G U E U R M O N O T O N E**

Clé : **H N T F S M P K D C B Z M etc. n'importe quelle lettre...**

Le résultat sera indéchiffrable, car on n'a aucune idée de la lettre employée pour chiffrer. De plus, il faut que la clef ne soit utilisée *qu'une seule fois*. Si elle est réutilisée, il y a le risque que l'analyse de deux cryptos permette le déchiffrement. On parle donc de « *clef aléatoire une fois* » (elle n'est pas belge.)

Le système est parfait, ce type de message chiffré est indéchiffrable.

Dans les années 1970 / 1980, les transmissions entre les bâtiments de la Marine nationale et entre les bâtiments et le continent étaient fondées sur ce principe. Concrètement, il y avait un téléscripteur (une grosse machine) sur laquelle défilaient deux bandes de papier, larges d'environ 2 cm. Une bande avec le clair, une bande avec la clef. Les deux bandes étaient calées au départ pour être synchronisées puis défilaient côte à côte dans le téléscripteur. La machine faisait l'addition des lettres, obtenait le crypto et le transmettait par radio au destinataire.

Les navires français étaient souvent accompagnés par des « chalutiers» soviétiques, bardés d'antennes et de radars, qui ne pêchaient pas beaucoup et suivaient tous les exercices en mer. Ils interceptaient les communications, mais ne parvenaient pas à les déchiffrer.

Cette méthode présente un inconvénient. L'échange de clefs entre l'émetteur et le destinataire est long et délicat. Le système est un peu lourd et suppose des conditions de communications des clefs en toute sécurité. Elle est encore utilisée de nos jours par certaines ambassades qui peuvent transmettre leurs clefs par la valise diplomatique.

7. Le principe de Kerckhoffs

Nous avons vu en détail le mécanisme de l'utilisation d'un algorithme de chiffrement et d'une clef, jusqu'à la méthode de la *clé aléatoire une fois.*

L'importance de la clef par rapport à l'algorithme est un principe de base de la cryptographie. Ce principe a été fixé en 1883 par le linguiste hollandais Auguste Kerckhoffs Van Nieuwenhoff dans son traité « *La cryptographie militaire* ». Principe de Kerckhoffs :

« La sécurité d'un système de chiffrement ne doit reposer que sur le secret de la clef et non pas sur le secret de l'algorithme de chiffrement, qui peut être connu de l'ennemi. »

Ce principe est fondamental. Nous le trouverons constamment tout au long de ces fiches.

*****
***
*

LES CODES ET LES DICTIONNAIRES

1. Les codes qui ne sont pas secrets

Il existe des codes qui ne sont pas secrets et qui sont utilisés par tous. Ces codes sont souvent des moyens de communication ou des systèmes de numération. Ce sont des méthodes pour coder, mais ce n'est pas à proprement parler de la cryptographie puisque tout le monde les connaît et les utilise. Citons quelques grands classiques :

- ***Le code Morse international***, ou alphabet Morse international, dans lequel chaque lettre est représentée par un système de points et de traits. Il permet de transmettre des textes à l'aide de séries d'impulsions courtes et longues. Il est utilisé entre autres pour des émissions à caractère automatique : radiobalises en aviation, indicatif d'appel des stations maritimes, signalisation maritime par des transpondeurs radar.

-***L'alphabet phonétique de l'OTAN*** est un alphabet radio international qui a été normalisé par l'Union internationale des télécommunications. On connaît les célèbres « Alpha, Bravo, Charlie, Delta... » que l'on entend dans les films. Chaque mot désigne une lettre et ces mots ont été spécialement choisis pour qu'ils soient biens distincts les uns des autres quand on les prononce à la radio et qu'il n'y ait aucune ambiguïté sur la lettre considérée.

- ***Le système de numération binaire***
C'est un système de numération, c'est à dire une façon de compter. Mais au lieu d'utiliser le système décimal, c'est à dire les 10 chiffres de 0 à 9, on n'utilise que le 0 et le 1. Les tables de correspondance avec le système décimal se trouvent partout.

Ces chiffres 0 et 1, chiffres de la numération binaire positionnelle, sont appelés communément « *bits* », abréviation de l'anglais *binary digit*, soit « chiffre binaire ». Les bits sont le système de calcul utilisés par les ordinateurs : les 0 et les 1 sont déterminés par la présence ou non d'un courant électrique.

- ***Le système de numération hexadécimal***
est un système de numération en base 16. Il utilise 16 symboles, les chiffres arabes pour les 10 premiers chiffres (de 0 à 9), , puis les lettres A à F pour les 5 suivants. Le nombre 15 (décimal) s'écrit donc F, le nombre 16 s'écrit 10, c'est à dire (1 x 16) + 0 unités, le nombre 17 s'écrit 11, soit (1 x 16) + 1 unité, le nombre 18 s'écrit 12, soit (1 x 16) + 2 unités et ainsi de suite.

Le système de numération hexadécimal est très utilisé en informatique car il permet une conversion sans aucun calcul avec le système binaire, système employé par les ordinateurs, du fait que 16 est une puissance de 2. Un chiffre en base 16 correspond exactement à 4 chiffres en base 2. Recherchez sur Internet si le sujet vous intéresse et si vous souhaitez approfondir ces notions.

Pour visualiser concrètement, le tableau page suivante met en parallèle les premiers nombres écrits dans chaque système.

Décimal	Héxadécimal	Binaire
0	0	0
1	1	1
2	2	10
3	3	11
4	4	100
5	5	101
6	6	110
7	7	111
8	8	1000
9	9	1001
10	A	1010
11	B	1011
12	C	1100
13	D	1101
14	E	1110
15	F	1111
16	10	10000
17	11	10001
18	12	10010

- Le code ASCII (American Standard Code for Information Interchange)

La mémoire d'un ordinateur conserve toutes les données sous forme numérique. Il n'existe pas de méthode pour stocker directement les caractères. Chaque caractère du clavier possède donc son équivalent en code numérique : c'est le code ASCII.

Le code ASCII permet de représenter les chiffre de 0 à 9, les lettres majuscules et minuscules ainsi que des symboles comme %, *, #, § , les symboles de ponctuation, l'espace, en fait tous les chiffres, lettres et symboles que l'on trouve sur un clavier d'ordinateur. Ce code comporte 128 nombres représentés par 7 bits, de 0 à 127 (7 bit permettent d'écrire les nombres de 0 à 127, puisqu'en numération binaire 127 = 1111111, soit 7 caractères).

L'ASCII suffit pour représenter les textes en anglais, mais il est trop limité pour les autres langues, dont le français et ses lettres avec des accents. Les limitations du jeu de caractères ASCII sont encore sensibles actuellement, par exemple dans le choix restreint de caractères généralement offerts pour composer une adresse électronique.

Pour être clair, *voir le tableau page suivante*. On y trouve les 128 caractères du code ASCII représentés par un nombre en système décimal ou hexadécimal. La 1re colonne est le codage en nombres décimaux, la 2ème le codage en hexadécimal, et la 3ème marquée « Char » (caractère) est le symbole qui est à représenter.

Par exemple, le chiffre 4 est codé 52 (en décimal), < est codé 60, @ est codé 64, P majuscule est codé 80, k minuscule est codé 107 etc.
Plusieurs énigmes de ce site utilisent un codage ASCII.

Decimal	Hex	Char	Decimal	Hex	Char	Decimal	Hex	Char	Decimal	Hex	Char
0	0	[NULL]	32	20	[SPACE]	64	40	@	96	60	`
1	1	[START OF HEADING]	33	21	!	65	41	A	97	61	a
2	2	[START OF TEXT]	34	22	"	66	42	B	98	62	b
3	3	[END OF TEXT]	35	23	#	67	43	C	99	63	c
4	4	[END OF TRANSMISSION]	36	24	$	68	44	D	100	64	d
5	5	[ENQUIRY]	37	25	%	69	45	E	101	65	e
6	6	[ACKNOWLEDGE]	38	26	&	70	46	F	102	66	f
7	7	[BELL]	39	27	'	71	47	G	103	67	g
8	8	[BACKSPACE]	40	28	(	72	48	H	104	68	h
9	9	[HORIZONTAL TAB]	41	29	)	73	49	I	105	69	i
10	A	[LINE FEED]	42	2A	*	74	4A	J	106	6A	j
11	B	[VERTICAL TAB]	43	2B	+	75	4B	K	107	6B	k
12	C	[FORM FEED]	44	2C	,	76	4C	L	108	6C	l
13	D	[CARRIAGE RETURN]	45	2D	-	77	4D	M	109	6D	m
14	E	[SHIFT OUT]	46	2E	.	78	4E	N	110	6E	n
15	F	[SHIFT IN]	47	2F	/	79	4F	O	111	6F	o
16	10	[DATA LINK ESCAPE]	48	30	0	80	50	P	112	70	p
17	11	[DEVICE CONTROL 1]	49	31	1	81	51	Q	113	71	q
18	12	[DEVICE CONTROL 2]	50	32	2	82	52	R	114	72	r
19	13	[DEVICE CONTROL 3]	51	33	3	83	53	S	115	73	s
20	14	[DEVICE CONTROL 4]	52	34	4	84	54	T	116	74	t
21	15	[NEGATIVE ACKNOWLEDGE]	53	35	5	85	55	U	117	75	u
22	16	[SYNCHRONOUS IDLE]	54	36	6	86	56	V	118	76	v
23	17	[ENG OF TRANS. BLOCK]	55	37	7	87	57	W	119	77	w
24	18	[CANCEL]	56	38	8	88	58	X	120	78	x
25	19	[END OF MEDIUM]	57	39	9	89	59	Y	121	79	y
26	1A	[SUBSTITUTE]	58	3A	:	90	5A	Z	122	7A	z
27	1B	[ESCAPE]	59	3B	;	91	5B	[	123	7B	{
28	1C	[FILE SEPARATOR]	60	3C	<	92	5C	\	124	7C	|
29	1D	[GROUP SEPARATOR]	61	3D	=	93	5D	]	125	7D	}
30	1E	[RECORD SEPARATOR]	62	3E	>	94	5E	^	126	7E	~
31	1F	[UNIT SEPARATOR]	63	3F	?	95	5F	_	127	7F	[DEL]

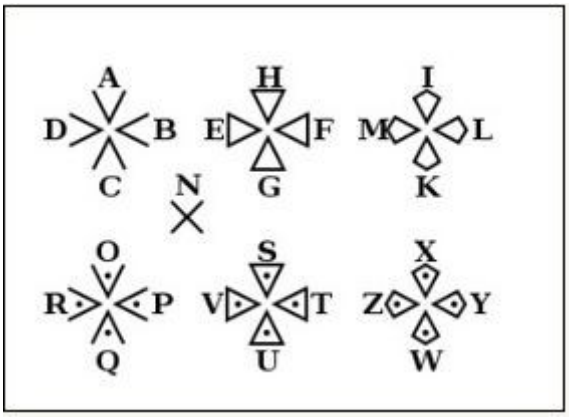
- Comme il a été expliqué en introduction, tous ces types de codage ne sont pas de la cryptographie à proprement parler. Cependant, de nombreuses énigmes de ce site comportent des codages en numérotation binaire, ASCII ou autres. *Il est important de se familiariser avec ceux-ci. Ils sont d'un usage courant en informatique et sont présents dans certaines énigmes du concours Alkindi.* Leur pratique permet de mieux maîtriser d'autres types de codages réellement cryptographiques et de faire marcher ses neurones.

2. Les « vrais » codes secrets

Une rapide promenade dans l'Histoire permettra de juger de l'imagination des hommes pour créer des codes secrets. Citons par exemple :

- Le chiffre des Templiers

Le codage des lettres est le suivant :



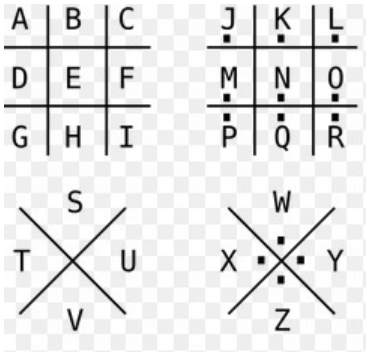
Ces symboles on été créés à partir de la croix des templiers

elle-même issue probablement de la croix de l'Ordre de Saint-Jean de Jérusalem.

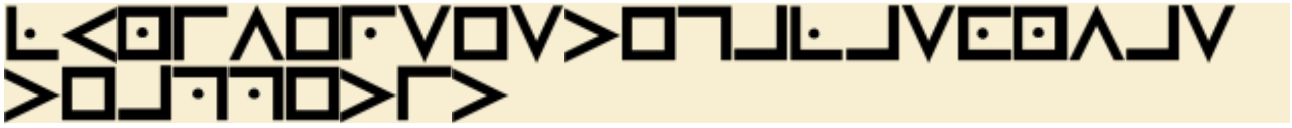
Ainsi le texte : **« Pour l'enfant, amoureux de cartes et d'estampes »** sera chiffré :

- Le chiffre des francs-maçons

Ce mode de chiffrement est inspiré du chiffre des Templiers. Il se présente ainsi



Le texte **« L'univers est égal à son vaste appétit »** deviendra



Les francs-maçons britannique surnommaient ce chiffre Pig-Ben, l'« enclos aux cochons » en anglais, sans doute du fait des lignes régulières et géométriques qui le composait. Il y a également un jeu de mot avec Big Ben, la grosse cloche de l'horloge du palais de Westminster à Londres.

- Le chiffre de Marie Stuart

La fin de la vie de la reine Marie Stuart a été évoquée rapidement dans la fiche n° 2, *A quoi sert la cryptographie ?* Dans le cas de cette malheureuse reine, son chiffre, ou plutôt une mauvaise utilisation de celui-ci, l'a conduite à la mort.
Le chiffre de Marie Stuart peut aussi être appelé une *nomenclature*. Il est en effet constitué d'un alphabet chiffré, de symboles indiquant que la lettre suivante est nulle ou doublée, ainsi que de symboles exprimant les mots les plus courants. Le voici :

Tous ces codes sont des chiffrements par substitution. Ils ne résistent pas à une attaque par l'analyse de fréquence, surtout si les émetteurs des messages commettent les erreurs classiques qui font le bonheur des décrypteurs : nombreux messages codé avec le même système de chiffrement, erreurs de chiffrement, présence de mots probables répétés en début ou en fin de messages. Nous ne reviendrons pas sur l'importance d'une clef, le lecteur se lasserait...

Certaines énigmes de ce site sont constituées à partir de ces types de code.

- Les polices de caractères

Il existe également des énigmes qui sont codées tout simplement par une *police de caractères* que l'on trouve dans Word. Ainsi par exemple l'étrange message :

✌♒·🖉 ✈◆♏ ●♏ ❍❑■♎♏ ♏♦♦ ♑❒♋■♎ → ●♋ ♍●♋❒♦🡅 ♎♏♦ ●♋❍❑♏♦·🖉

est écrit en police Wingdings et signifie : « **Ah! Que le monde est grand à la clarté des lampes** !»

Pour conclure sur les codes, un exemple amusant de codage par symboles est donné par Arthur Conan Doyle dans *Les hommes dansants*, une aventure de Sherlock Holmes. Le célèbre détective fait une très belle démonstration d'analyse de fréquence (difficile en anglais) et de recherche de mots probables pour décrypter des messages constitués par des petits dessins :

3. Les dictionnaires

Les dictionnaires chiffrés reposent sur le principe de faire correspondre un mot, et non pas seulement une lettre, à un nombre.

Continuons notre approche historique avec :

- Le Grand Chiffre de Louis XIV

C'était un dictionnaire où les mots courants étaient codés. Les mots rares étaient découpés en syllabes. Pour résister à une analyse de fréquence, une même syllabe pouvait être codée par plusieurs nombres différents. C'était donc beaucoup plus subtil qu'un simple chiffrement par substitution. Il comportait au total 587 nombres.

Ce chiffre fut élaboré par le célèbre cryptologue Antoine Rossignol qui avait été au service de Richelieu, Louis XIII et Mazarin. Son nom est resté dans l'Histoire puisque dans le langage courant un *rossignol* désigne un outil qui permet de forcer les serrures. Ce chiffre tomba en désuétude après la mort d'Antoine Rossignol et de son fils, et rapidement plus personne ne sut l'employer. De ce fait, il résista aux briseurs de code pendant 300 ans ! Jusqu'à la fin du XIXe siècle, personne n'était capable de le lire.

En 1890, une nouvelle correspondance de Louis XIV utilisant ce Grand Chiffre fut découverte par un historien. Il la confia à Étienne Bazeries, un spécialiste du service cryptographique de l'armée. Celui-ci mit trois ans à le décrypter entièrement !

Ce déchiffrement permit entre autre la découverte de l'identité d'un personnage rendu célèbre par Alexandre Dumas dans son roman *Le Vicomte de Bragelonne* : l'homme au Masque de fer. Ainsi un nom fut mit sur ce mystérieux personnage : c'était le général de Bulonde. Mais est-ce vraiment la vérité ? Ces lettres cryptées étaient peut-être destinées à être déchiffrées pour orienter les générations suivantes sur une fausse piste et cacher la véritable identité de l'homme au Masque de fer... En tout cas certains l'ont imaginé. Nous sommes dans le monde du secret…

- Le dictionnaire de Sittler

En France, la loi du 13 juin 1866 sur les usages commerciaux autorisa le chiffrement des dépêches privées par télégrammes. A cette époque, tout le monde correspondait par télégrammes envoyés par la Poste, un peu comme les SMS aujourd'hui. Aussitôt, de nombreux codes basés sur des dictionnaires virent le jour.

Un des premiers codes commerciaux fut le code Sittler de 1868. Le dictionnaire fonctionne ainsi : les mots et les expressions courantes sont rangés dans l'ordre alphabétique sur les 100 lignes d'une page. Le dictionnaire comporte 100 pages. L'utilisateur détermine lui-même la numérotation de chaque page de son dictionnaire, dans n'importe quel ordre.
Chaque mot du message est chiffré par un nombre qui commence par le numéro de la page, puis le numéro de la ligne où se trouve le mot. Bien entendu le destinataire des messages possède un dictionnaire identique pour déchiffrer. On peut ajouter un codage supplémentaire au chiffre initial. Cela s'appelle un surchiffrement.
Avec 100 mots par page et un dictionnaire de 100 pages, on peut coder 10 000 mots, ce qui est largement suffisant pour une utilisation courante.

Ce dictionnaire fut très utilisé entre 1890 et 1920 par des particuliers, des entreprises ou par l'État.

Ce système de codage présentait des faiblesses. Mais tout le monde l'utilisait et en particulier les autorités diplomatiques et militaires italiennes et allemandes.

En août 1914, un croiseur allemand, le Magdeburg, s'est échoué près d'une île en mer Baltique. Il fallut évacuer le navire et un officier prit les livres de codes pour les jeter au fond la mer. Mais les bâtiments russes tirèrent au canon sur le navire allemand et firent de nombreuses victimes. Ils repêchèrent l'officier, mort, qui tenait les livres de codes serrés dans ses bras.

Les codes furent donnés aux Britanniques qui les étudièrent et jusqu'en 1916, ceux-ci décryptèrent tous les messages de la Marine allemande. Cette histoire est un peu comparable à celle d'Énigma pendant la Seconde Guerre mondiale.

4. Les codes mystérieux et non-déchiffrés

Il existe des codes célèbres qui n'ont jamais été décryptés, comme le manuscrit de Voynich, le disque de Phaistos ou les chiffres de Beale, un étrange personnage qui a caché un fabuleux trésor. Et bien d'autres codes ou chiffres mystérieux Mais ces histoires appartiennent aux mythes de la cryptographie et sortent largement du cadre d'une initiation. Vous les trouverez sur Internet si elles vous intéressent. Mais de toute façon, on ne les proposera jamais comme énigmes sur le site de Club Akindi !

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

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 :

et

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

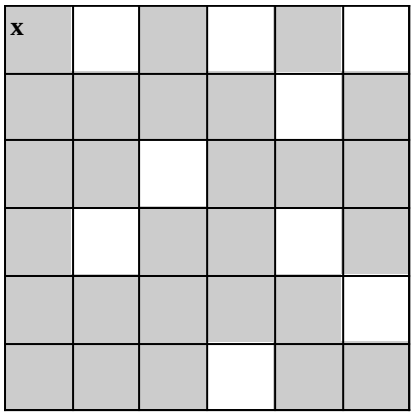
sera chiffré : **RAEMDLI BULDRER UAMDOUV**
L'énigme 15 est construite sur ce thème.

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.

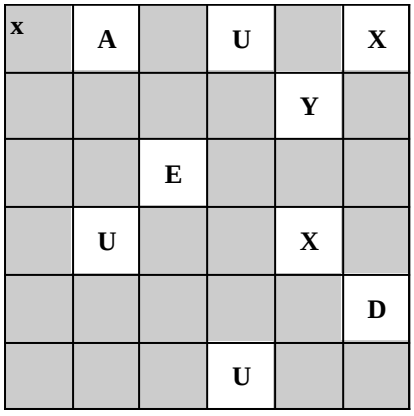
Dessin :



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.

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

L'ENTRE-DEUX GUERRES : 1920 - 1945

Si l'on considère l'histoire des Transmissions, on constate qu'au cours de la seconde moitié du XIXe siècle, le télégraphe et les communications en alphabet Morse se sont généralisés dans le monde entier. Puis, au début du XXe siècle, l'invention de la radio a permis de développer considérablement le volume et surtout la vitesse de ces communications. A cette époque,les messages radio vont donc devenir le moyen de transmission par excellence. Inconvénient : ils peuvent se faire intercepter !

Du fait des interceptions massives de messages et du fantastique travail des cryptanalystes, les messages chiffrés par transposition, très utilisés fin XIXe et début XXe, ont été souvent décryptés (chiffre ADFGVX en 1918, voir Fiche n° 5). La fin de la Première Guerre mondiale va marquer la fin de l'utilisation de ces types de chiffrements. Puis, à partir de 1920, les militaires vont ressentir la nécessité d'utiliser des machines.

1. Enigma

En 1926, l'ingénieur allemand Arthur Scherbius breveta une machine conçue pour faciliter les communications sécurisées : *Enigma.* Au départ, Enigma fut conçue pour protéger le secret des communications commerciales. Mais cette version commerciale fut un échec. Dès 1926, en raison de sa facilité d'utilisation et de la complexité du chiffrement qu'elle permet, Enigma fut choisie par le gouvernement allemand pour coder les communications militaires. L'armée allemande fut dotée d' environ 100 000 machines entre 1926 et 1945.

En fait il existait une série de machines : chacun des trois corps de l'armée hitlérienne, la Luftwaffe (aviation), la Wehrmacht (armée de terre) et la Kriegsmarine (marine) avait la sienne.

La machine Enigma se présente comme une ancienne machine à écrire. Elle est constituée d'un clavier, d'un tableau lumineux de 26 lettres, de trois rotors et d'un réflecteur. La position des connexions entre les 3 rotors, qui sont modifiables, ainsi que la position de ces rotors, constituent la clef de chiffrement.

L'utilisation d'Enigma est relativement simple : l'émetteur dispose les connexions et les rotors en position de sortie, tels que spécifié par le livre des clefs pour ce jour-là. Puis il tape les lettres du message qui se trouve automatiquement chiffré. A chaque frappe d'une nouvelle lettre, un rotor tourne, modifiant le chiffrement. A la réception, le destinataire tape le message chiffré et la machine restitue les lettres en clair sur le clavier lumineux. Le système des rotors permettait plus de 10 millions de milliards de combinaisons, donc autant de clefs différentes. En pratique, la clef était changée chaque jour.

Si vous êtes intéressés, vous trouverez le fonctionnement détaillé d'Enigma dans les principaux livres cités dans la fiche n° 10 et sur de nombreux sites Internet. Expliquer ce fonctionnement dans le détail serait un peu fastidieux et sortirait du cadre de ces fiches, d'autant que ces livres et ces sites Internet l'expliquent parfaitement bien.
Ce fonctionnement d'Enigma est également expliqué dans la vidéo suivante (très courte) sur YouTube ainsi que sur d'autres vidéo.

https://www.youtube.com/watch?v=dTiqXrrH-oQ

On peut voir une Enigma au Musée de l'Armée à Paris, au Musée des Transmissions de Cesson-Sévigné (près de Rennes) ainsi qu'au Musée de la ville de Bletchley en Grande-Bretagne.

2. Casser Enigma

L'histoire de la cryptanalyse d'Enigma est un véritable roman d'espionnage.

En 1931, un fonctionnaire allemand du Bureau du Chiffre, Hans-Thilo Schmidt, trahit son pays pour de l'argent et fournit aux Français les tables de chiffrement et les manuels d'utilisation d'Enigma. Cet espion, Schmidt, fut traité par un officier français , le capitaine Gustave Bertrand. (« traiter» un agent signifie assurer la liaison avec un agent étranger qui est source de renseignements).

Gustave Bertrand remit la précieuse documentation sur Enigma à ses collègues français de la Section du Chiffre, mais ils ne parvinrent pas à briser le cryptage de la machine. Sur ordre de sa hiérarchie, le capitaine Bertrand remit alors les mêmes documents au Bureau du Chiffre britannique, également sans succès. En décembre 1932, ll s'adressa alors au Bureau du Chiffre polonais et communiqua certains éléments au colonel Gwido Langer, le chef du Biuro Szyfrów (Bureau du chiffre polonais).

Dans ce Bureau du chiffre polonais travaillait une équipe de mathématiciens de très haut niveau. Parmi eux se trouvait *Marian Rejewski*, qui, grâce aux documents remis par Gustave Bertrand concentra les efforts des équipes sur le problème des clefs. Après quelques mois d'un dur labeur, il parvint à dégager 105 456 clefs, parmi les 10 millions de milliards de clés initiales possibles. Pour cela, les mathématiciens polonais construisirent une machine appelée « Bomba », qui générait toutes les positions possibles des rotors pour rechercher la clé du jour. En 1934, le Bureau de cryptanalyse polonais avait réussi à casser Enigma et pouvait déchiffrer un message en quelques heures.

Les Allemands ne savaient pas que les Polonais étaient parvenus à briser la sécurité d'Enigma. Pourtant, ils amélioraient constamment le système et en 1938, ils ajoutèrent deux rotors supplémentaires à la machine. Le nombre de clés possibles fut multiplié par 10. Ceci posa quelques problèmes aux cryptanalystes polonais.

Après la déclaration de guerre et la défaite de la Pologne face à l'Allemagne nazie, certains membres du Bureau du Chiffre polonais vinrent en France grâce à Gustave Bertrand. Ils échangèrent beaucoup d'informations avec les Anglais et leur permirent de travailler efficacement sur Enigma. En 1942, dans la France de Vichy, les Français et les Polonais poursuivirent conjointement leurs efforts de déchiffrement. Mais leur histoire devint dramatique : la Gestapo les traquait et le MI 6 (Military Intelligence section 6) tenta de les exfiltrer. Sur le point de passer en Espagne en 1943, ils furent arrêtés par une patrouille allemande et ne purent jamais se rendre en Angleterre.

3. Enigma vaincue : Alan Turing

Alan Turing naquit le 23 juin 1912. Après ses études secondaires, il fut admis en 1931 au King's College de Cambrige, haut-lieu de l'enseignement des mathématiques en Grande-Bretagne. Pendant ses études, en 1937, il publia son célèbre article *« On computable Numbers »*, article de logique mathématique sur la difficulté de discerner le vrai du faux. Dans cet article, il décrit une machine imaginaire capable d'enchaîner des opérations de calcul (un algorithme) : l'ancêtre de l'ordinateur.

Il existe différentes branches dans les mathématiques : la théorie des nombres, l'algèbre, l'analyse, la géométrie, la logique etc. Alan Turing est un logicien. Une petite histoire permettra de comprendre la notion de logicien :

Un biologiste, un physicien et un mathématicien sont dans un train en Écosse. Tout à coup, ils aperçoivent un mouton noir dans un pré qui borde la voie.
– Le biologiste dit : « Tiens, en Écosse, les moutons sont noirs.»
– Le physicien le corrige et dit : «Il faut s'en tenir à ce que l'on a observé : on peut dire qu'en Écosse, il existe au moins un mouton noir.»
– « Non, dit le mathématicien, on peut seulement dire qu'en Écosse il existe un mouton dont au moins un côté est noir.»

Revenons à nos propres moutons :

Au début de la Seconde Guerre mondiale, l'interception et le déchiffrement des messages de l'ennemi sont fondamentaux. Les sous-marins allemands règnent en maîtres sur l'océan atlantique et le ravitaillement de la Grande-Bretagne en nourriture et en armes est compromis. C'est la célèbre Bataille de l'Atlantique.
Les communications entre la terre et les sous-marins s'effectuaient avec Enigma. Décrypter ces transmissions est un enjeu vital. Connaître les positions des U-boots est fondamental pour que les bâtiments de ravitaillement les évitent et que ceux de la Royal Navy puissent les attaquer.
Des équipes de spécialistes en cryptographie furent réunies au début de la guerre à Bletchley Park, un grand manoir situé à 80 km au nord de Londres. A la déclaration de guerre en septembre 1939, Alan Turing fut invité à rejoindre Bletchley Park pour y diriger le service chargé de décrypter les messages de la Marine allemande. À cette époque, les Enigma de la Kriegsmarine ont 4 ou 5 rotors. Dans les premières années de la guerre, les Anglais posséderont une ou deux Enigma, récupérées difficilement sur des sous-marins en perdition.

Ces Enigma vont être étudiées par les experts de Bletchley Park et Alan Turing, dans la logique de son article de 1937 sur une machine qui calcule, fit construire un premier appareil de décodage automatique appelé « la Bombe ». Quinze bombes furent construites dans les huit mois suivants pour apporter des améliorations.

Enigma était utilisée par les armées, mais les communications entre les états-majors et la chancellerie d'Hitler étaient chiffrées par une machine appelée machine de Lorenz. Pour parvenir à la décrypter une machine de décodage plus puissante fut nécessaire. Ce nouvel outil découla lui aussi des travaux de Turing. Il s'agit d'un calculateur électronique de grande taille, appelé pour cette raison Colossus. Alimenté par câbles, Colossus effectue les opérations de déchiffrement en suivant une logique abstraite et universelle ; il est également capable de programmer d'autres machines et de s'arrêter lui-même après avoir inscrit ses résultats sur un ruban de papier. L'ordinateur est né.

La vie et les actions d'Alan Turing à Bletchley Park ainsi que sa fin tragique en 1954 appartiennent à l'Histoire avec un grand H. Là encore, nous laisserons les livres, les sites Internet et un très beau film (*Imitation Game*) raconter tout cela en détail.

Remarquons simplement quelques points importants ou méconnus :

- De nombreux historiens estiment que la cryptanalyse d'Enigma a permis d'écourter la durée de la Seconde Guerre mondiale d'environ deux ans.

- Toutes les activités de décryptage réalisées à Betchley Park pendant la Seconde Guerre mondiale ont été tenues secrètes jusque dans les années 1975 / 1980. Elles étaient classifiées « Top Secret », le plus haut niveau de classification (correspondant au « Très Secret - Défense » français) par les autorités britanniques. Tout s'est passé comme si ces événements n'avaient jamais existé. Colossus a été détruit après la guerre sur ordre de Winston Churchill.

- On a commencé à entendre parler d'Alan Turing dans les années 80. David Kahn évoque Enigma et Alan Turing dans son livre extraordinairement bien documenté « La guerre des codes secrets », publié en France en 1980. La première biographie qui lui a été consacrée, *Alan Turing : the enigma* d'Andrew Hodges, fut publiée en 1983. Ce livre a été édité en France en 1988 et réimprimé en 2014 et 2015 à la suite du succès de la sortie du film *Imitation Game*.

- En 1945, les Anglais ont récupéré de nombreuses machines Enigma dans les unités combattantes allemandes, dans les états-majors, les ministères etc. Très généreusement, ils en ont offert un grand nombre à des pays amis et en particulier aux pays du Commonwealth pour un usage diplomatique ou militaire. Il se trouve que par un malencontreux oubli, ils ne les ont pas informés qu'il savaient décrypter les messages…

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

LE CHIFFREMENT RSA

Dans la fiche n° 3 sur les procédés de chiffrement par substitution, nous avons vu qu'il existait un mode de chiffrement inviolable, qui ne pouvait pas être décrypté : le chiffrement à l'aide d'un tableau de Vigenère avec une *clef aléatoire utilisée une seule fois*.

Cependant, ce procédé présente des inconvénients pratiques majeurs : la communication des clés en toute sécurité et de façon simple entre les expéditeurs et les destinataires des messages est assez difficile. De plus, si le volume des messages est important, il nécessite un nombre considérable de clés, ce qui complique encore plus leur communication. Lorsque le destinataire est une unité militaire sur le terrain ou un sous-marin, on voit bien le problème logistique qui est posé avec en plus le risque de l'interception des clefs lors de leur communication aux destinataires.
En résumé, c'est le problème bien connu en cryptographie de *la distribution de la clef.*

1. Les précurseurs : l'algorithme d'échange de clés Diffie-Hellman-Merkle

Dans les exemples donnés sur le fonctionnement de ces chiffrements, il y a trois personnages imaginaires : Alice, Bob et Ève. Alice envoie des messages à Bob et Ève les espionne.

Whitley Diffie et Martin Hellman et Ralph Merkle sont des cryptographes américains. En 1976, ils ont inventé un système fonctionnant de la façon suivante :

Alice veut envoyer un message à Bob. Elle met ce message dans un coffret en fer, met un cadenas et l'envoie à Bob. Lorsqu'il reçoit le coffret, Bob ajoute son propre cadenas et le renvoie à Alice. Alice reçoit donc le coffret muni de deux cadenas. Elle retire le sien, en ne laissant que le cadenas de Bob. Enfin elle le retourne à Bob, qui peut ouvrir son propre cadenas avec sa propre clef.

On a bien compris l'analogie : les cadenas sont un procédé de chiffrement. Alice chiffre son message avec sa clé et l'envoie à Bob. Bob le chiffre et le renvoi à Alice. Alice le déchiffre et le renvoie à Bob qui le déchiffre. Mais il y a un problème : si ça fonctionne en théorie, en pratique ce n'est pas possible car l'ordre dans lequel intervient les chiffrement et les déchiffrements a son importance. Il doit obéir à la loi : *« dernier mis, premier enlevé »*.Autrement dit , le dernier chiffrement effectué doit être le premier à être enlevé. Si la chronologie des chiffrements avec la clef n'est pas respectée, ce qui est le cas dans le schéma proposé, ça ne fonctionne pas.

Comme ce système à deux cadenas ne pouvait pas s'appliquer, Diffie et Hellmann passèrent des mois à essayer trouver une solution pour contourner le problème. Ils concentrèrent leurs efforts sur diverses fonctions mathématiques, en particulier les fonctions à sens unique.

Si l'on considère une fonction classique y = 2x + 3, il est facile de calculer y avec une valeur de x donnée. Si l'on veut inverser la fonction, c'est à dire trouver x avec une valeur donnée de y, la fonction devient x = (y-3) / 2. Il n'est pas difficile de l'inverser.

Ce qui intéressait Diffie et Hellman, c'était *les fonctions à sens unique,* c'est à dire une fonction qu'il est impossible d'inverser : une fonction non-réversible. Une fonction modulo, par exemple, est une fonction à sens unique. Ils travaillèrent donc sur les fonctions modulo.

L'arithmétique modulo est relativement simple : le résultat d'une fonction modulo est le reste de la division de 2 nombres entiers.

Exemple : 17 modulo 6 est égal à 5, parce que 17 divisé par 6 = 2 , que 6 x 2 = 12 et 17 - 12 =5. Donc le reste de la division de 17 par 6 est égal à 5.

Autre exemple : 99 (mod 13) = 8 puisque 99 divisé par 13 = 7, et 7 x 13 = 91. Donc le reste de la division est égal à 99 – 91 = 8.

Considérons maintenant la fonction $f(x) = 3^x \pmod 7$ et calculons sa valeur pour x = 1, 2, 3 etc.

Le tableau suivant nous donne la valeur de f(x) :

X	1	2	3	4	5	6	7	8	9	10	11	12
3^x	3	9	27	81	243	729	2 187	6 561	19 683	59 049	177 147	531 441
$3^x \bmod 7$	3	2	6	4	5	1	3	2	6	4	5	1

Essayons maintenant de calculer la valeur de la fonction réciproque, c'est à dire la valeur de x à partir d'une valeur de f(x).

Si l'on suppose f(x) = 2, c'est à dire 3^x (modulo 7) = 2, on voit qu'il y a plusieurs solutions : x = 2, x = 8 etc. Si l'on travaille sur des petits nombres, il est relativement facile trouver x, même si le calcul est un peu fastidieux.

Mais si au lieu de $f(x) = 3^x \pmod 7$ on prend la fonction

$$f(x) = 453^x \pmod{21\,997}$$

les choses se compliquent un peu : on voit qu'il est relativement facile d'attribuer une valeur à x et de calculer f(x), mais si l'on attribue une valeur à f(x), par exemple 5 787, et que l'on écrit :

$$f(x) = 453^x \pmod{21\,997} = 5\,787$$

il sera quasi impossible de trouver la valeur de x. On ne peut pas inverser cette fonction, c'est une fonction à sens unique.

Au printemps 1976, après deux ans de travail sur ces fonctions, Hellman parvint à résoudre le problème de l'échange de clefs. Il prouva qu'en utilisant les propriétés des fonctions à sens unique, *Alice et Bob pouvaient établir une clef secrète, sans se rencontrer*. A partir de 2 nombres échangés entre eux, plus un nombre choisi par Alice et un nombre choisi par Bob, chacun gardant secret son nombre. Alice et Bob peuvent définir une même clef qu'ils peuvent utiliser pour chiffrer un message.

Si Ève, la méchante, intercepte les messages, elle aura connaissance des nombres échangés, mais pas des deux nombres secrets, et il lui sera impossible de déchiffrer ces messages.

Cette découverte est fondamentale, car elle est totalement *contraire à l'intuition scientifique.* Elle obligea les cryptographes à réviser complètement les règles du chiffrement.

Pour ne pas alourdir cette fiche qui est une initiation, nous ne décrirons pas mathématiquement ce procédé de calcul que l'on trouve par ailleurs facilement sur Internet ou dans le livre *Histoire des codes secrets* de Simon Singh. Il est plus important de comprendre les concepts qui régissent ces types de chiffrement. Par contre, nous verrons en détail l'aspect mathématique du procédé de chiffrement RSA, qui en est dérivé, dans le paragraphe suivant.

Hellman a renversé un des piliers fondamentaux de la cryptographie et prouvé qu'Alice et Bob n'avaient pas besoin d'échanger une clef commune. Ensuite, il suffisait de trouver un schéma un petit peu plus efficace pour que le problème de la distribution des clefs soit totalement surmonté. Ce fut Whitfield Diffie qui le trouva.

Whitfield Diffie eut l'idée géniale d'un nouveau type de chiffre, qui utilisait *une clef asymétrique.*

Voici le principe :

Le destinataire du message créé une clé publique et une clé privée. La personne qui veut lui adresser un message le chiffre avec la clé publique que tout le monde connaît et envoie le message. A la réception, le destinataire déchiffre avec sa clé privée connue de lui seul.

Soyons encore plus clair : dans un système de chiffrement traditionnel, l'expéditeur chiffre le message avec une clef et l'adresse au destinataire. Ce destinataire connaît la clef de chiffrement, qui a été échangée avec l'expéditeur, et déchiffre le message. Dans le chiffrement RSA, ce n'est pas l'expéditeur qui chiffre avec sa clé : il chiffre avec une clef donnée par le destinataire et connue de tous.

Prenons une analogie avec une boite et des cadenas :

N'importe qui peut fermer un cadenas en appuyant dessus. Mais seule la personne qui a la clé du cadenas peut l'ouvrir. Tout le monde peut verrouiller (chiffrement), mais seul le possesseur de la clé peut déverrouiller (déchiffrement).

L'idée de Diffie est que la clé qui sert à chiffrer n'a aucune raison d'être semblable à la clé qui sert à déchiffrer. De ce fait la clé qui sert à chiffrer peut-être connue de tous, et même le message chiffré. Seule la clef privée permettra de déchiffrer.
Cela dit, s'il avait conçu le concept général de chiffre asymétrique, Diffie n'avait aucun exemple concret à proposer. Le concept était génial, mais personne ne savait comment le mettre en musique.

Il fallait trouver une fonction mathématique qui fasse le même travail et qui puisse être intégrée dans un système opérationnel de chiffrement.

Diffie publia les grandes lignes de son idée au cours de l'été 1975. D'autres mathématiciens se mirent à la recherche de la fonction requise pour créer un chiffrement asymétrique. Diffie, Helman et Merkle poursuivirent leurs recherches à l'université de Stanford (Californie). Ils ne réussirent pas à trouver de solution. Ce furent trois autres chercheurs qui y parvinrent : Ron Rivest, Adi Shamir et Leonard Adleman.

2. Le chiffrement RSA

Ron Rivest, Adi Shamir et Leonard Adleman étaient chercheurs et travaillaient tous les trois au Laboratoire d'informatique du MIT (Massachusetts Institute of Technology) près de Boston.

Ronald **R**ivest, Adi **S**hamir et Leonard **A**dleman

Les initiales de leurs noms ont formé le nom du mode de chiffrement.

Ils travaillèrent plusieurs années à la recherche d'une fonction à sens unique pour résoudre le problème d'une clef asymétrique. En avril 1977, Rivest, à la fin d'une soirée bien arrosée*, (ne l'imitez pas ! Quoique...), eut une inspiration sur la façon de générer un chiffre asymétrique. Il passa la fin de la nuit à formaliser son idée et le matin il avait rédigé un texte. C'était Rivest qui a fait la découverte, mais comme ils travaillaient ensemble depuis plus d'un an sur le problème, Rivest insista pour signer l'article de leurs trois noms.

* Source : Simon Singh, Histoire des codes secrets

Le concept du chiffrement RSA :

Dans tous les systèmes de chiffrement classiques, on utilise la même clef pour chiffrer et déchiffrer un message. C'est un chiffrement dit « symétrique ».

Le chiffrement RSA repose sur le principe suivant :

Reprenons nos trois personnages : on convient que Alice est destinataire des messages et souhaite en recevoir de la part de Bob et d'autres personnes. Il y a toujours Ève, la méchante, qui veut intercepter le message.

Alice souhaite recevoir des messages : elle va fabriquer des centaines de cadenas tous identiques, mais seule sa clef pourra les ouvrir. Alice envoie ces cadenas dans des bureaux de postes partout à travers le monde. Bob veut envoyer un message à Alice. Il le met dans une boîte, va à son bureau de poste, demande un cadenas d'Alice et verrouille la boite avec la cadenas. Il expédie la boite. A sa réception, seule Alice peut ouvrir la boite. Si Ève intercepte la boîte, elle ne peut pas l'ouvrir, elle n'a pas la clé.

On a bien compris l'analogie : les cadenas distribués partout sont la clé publique d'Alice et la clé du cadenas est sa clé privée.

Reste à trouver l'algorithme, c'est à dire les opérations mathématiques qui vont réaliser la chose ! C'est ce que réalisa Ron Rivest.

3. Concrètement, les mathématiques du chiffrement RSA :

Création de clefs par Alice

Afin de pouvoir recevoir des messages, Alice va donc créer une *clé publique*.
Pour se faire, elle choisit deux nombres entiers et premiers, p et q. Elle effectue leur produit pour déterminer un nombre N tel que :

$$N = p \times q$$

Pour illustrer, nous allons prendre par exemple p = 17 et q = 11, soit N = 17 x 11 = 187.

L'essentiel de la méthode est déjà présent : il repose sur le fait que connaissant N, il est très difficile et très long de calculer p et q. Dans l'exemple, c'est facile. Mais dans la réalité, p et q sont des nombres de 100 chiffres, donc N fait 200 chiffres. Et là, il faut un temps quasi infini à un ordinateur pour décomposer N en deux facteurs premiers.

Alice va ensuite choisir un autre nombre, **e**, **qui est un entier compris entre 2 et (p-1)(q-1) -1 et qui est premier avec p-1 et q-1**. C'est à dire tel que le PGCD de **e** et de (p-1)(q-1) soit égal à 1. Prenons par exemple **e = 7.**
Dans l'exemple, on calcule aisément (p-1)(q-1) = 16 x 10 = 160

Ces deux nombres, N et e, constituent la clef publique d'Alice. Alice peut publier sa clé sur un annuaire, par exemple Internet. Dans l'exemple, elle va publier : **RSA, 187, 7.**

Ensuite, Alice va calculer sa clef secrète, **d**. Ce nombre d est tel que

$$\mathbf{e*d \equiv 1 \bmod (p-1)(q-1)}$$

C'est à dire dans notre exemple (7 x d) mod (160) = 1. L'opération s'appelle une inversion modulaire.

En fait il existe un entier d et un seul qui satisfait la relation à partir d'une valeur de e choisie.

Ce nombre d est la clef privée d'Alice et elle la garde secrète.

Dans l'exemple, on aura **d = 23.** On a en effet 23 x 7 = 161 et 161 (mod 160) = 1. Calculer la valeur de **d** n'est pas immédiat, mais l'algorithme d'Euclide permet à Alice de trouver **d** facilement et sûrement. **L'important est, puisque p et q sont inconnus de tous, qu'il n'y a qu'Alice qui puisse calculer le produit (p-1)(q-1) et donc sa clef secrète d.**

2. Chiffrement et envoi du message par Bob

Bob veut envoyer un message à Alice. Supposons le message

Clair : VIVE LES VACANCES

Il le transforme en nombres en remplaçant chaque lettre par son rang dans l'alphabet :

Clair : 22 09 22 05 12 05 19 22 01 03 01 14 03 05 19

Désignons par « blocs B» ces nombres de 2 chiffres dont chacun représente une lettre. Bob va chiffrer chaque nombre B à l'aide du nombre N et du nombre e d'Alice (qui sont publiques) en le transformant en un nombre C selon la relation :

$$C = B^{e} \pmod N \quad \text{c'est à dire} \quad C = B^{7} \pmod{187}$$

Le message clair est donc chiffré ainsi :

Chiffré : 044 070 044 146 177 146 145 044 001 130 001 108 130 146 145

Bob adresse ce message chiffré à Alice

3. Réception et déchiffrement du message par Alice

A la réception du message, Alice va inverser le processus à l'aide de sa clé secrète d.

A partir de chaque nombre chiffré C, elle va calculer B selon la formule :

$$B = C^{d} \pmod N \quad \text{c'est à dire} \quad B = C^{23} \pmod{187}$$

Avec ce calcul, le message chiffré : 44 70 44 146 177 146 145 044 001 130 001 108 130 146 145

redevient : 22 09 22 05 12 05 19 22 01 03 01 14 03 05 19 , c'est à dire :

V I V E L E S VACANCES

Une calculatrice ordinaire peut difficilement calculer 145^{23} (mod 187). Si l'on est intéressé, on pourra aisément effectuer les calculs sur le site dcode.fr : https://www.dcode.fr/chiffre-rsa

Remarquons que dans l'exemple précédent, on a chiffré de la même façon les 3 V, les 3 E et les 2 S et les 2 A de « Vive les vacances ». Dans la pratique, pour casser une éventuelle analyse de fréquence, on crée des blocs de taille différente des nombres à chiffrer, par exemple les nombres de 2 chiffres sont regroupé par blocs de 3 et chiffrés comme tels. De plus, les blocs sont des très grands nombres.

On voit que cette méthode de chiffrement évite totalement un échange de clefs entre Alice et Bob.
Le chiffrement repose pour l'instant sur l'impossibilité actuelle de factoriser un très grand nombre (plus de 200 chiffres) en deux nombres premiers eux aussi très grands, ainsi que sur la non-réversibilité des fonctions modulo.

Remarque cryptograhique :

Pour l'instant, on ne sait pas factoriser, c'est à dire décomposer en facteurs, un très grand nombre qui est le produit de 2 nombres premiers. Mais il est possible que quelqu'un dans un organisme de cryptographie, à la NSA ou en Russie par exemple, y soit parvenu et que le secret soit bien gardé pour pouvoir espionner les petits camarades. Le secret du déchiffrement d'Enigma a été gardé pendant 40 ans. C'est le monde de la cryptographie.

Remarque mathématique :

Si l'on pose la question sur Google : combien y a-t-il d'atomes dans tout l'Univers visible ? on obtient une réponse, selon les sites Internet consultés, qui est un nombre de l'ordre de 10^{80} atomes. Pourtant le nombre 80 ne paraît pas très grand… Ceci pour dire qu'avec des nombres de l'ordre de 10^{100} ou 10^{200} , on est totalement en dehors du réel, ou du moins d'un réel physique quantifiable qui ait un sens concret. C'est juste une remarque au passage.

Conclusion

45 ans après sa création, le chiffrement RSA est toujours très utilisé, pour les paiements par cartes bancaires entre autres.

Pour une utilisation grand public, les chiffrements modernes concernent principalement les problèmes de signature électronique. On utilise pour cela des fonctions de hachage, qui réalisent des résumés d'un message, sous forme d'une suite de bits, généralement en numérotation hexadécimale.

Pour chiffrer, il existe aussi la méthode de chiffrement par blocs et de chiffrement par flots, en cryptographie symétrique (clé identique pour l'expéditeur et le destinataire)

Actuellement, la recherche en cryptographie s'oriente vers des chiffrements du type RSA, mais encore plus subtils. Il existe par exemple des chiffrements effectués à partir des courbes elliptiques : à partir de points sur la courbe, on détermine une clé secrète et une clé publique. On estime qu'une clef de 200 bits pour les courbes elliptiques est plus sûre qu'une clef de 1024 bits pour le chiffrement RSA. Cette technologie est utilisées pour les cartes à puces et a fait l'objet de nombreux dépôts de brevets à travers le monde.

Si vous êtes passionnés par le Chiffre et que vous souhaitez écrire sur ce site Internet quelques pages à propos de l'un de ces sujets, vous serez le bienvenu. Et si vous persévérez loin dans cette voie, c'est peut être vous qui écrirez les prochains chapitres de l' Histoire de la Cryptographie à travers votre métier.

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

COMMENT RÉSOUDRE UNE ÉNIGME ?

Il est conseillé d'avoir un aperçu, même succinct, des principaux modes de chiffrement avant d'aborder cette fiche. Si vous êtes débutant, la lecture des fiches n° 3, 4, et 5 vous sera utile.

Voici donc quelques pistes pour aborder une énigme :

Tout d'abord, il convient de la lire soigneusement, deux ou trois fois. Est ce que ça me fait penser à quelque chose de connu, que j'ai déjà vu ? Puis il faut bien lire le titre et les indices donnés pour essayer de capter le thème de l'énigme et son environnement.

1. Au départ :

Souvent, l'énigme vous « parle » immédiatement, simplement en la regardant, ou avec le titre et les indices : on reconnaît du binaire, du Morse, de l'alphabet phonétique…

Dans sa résolution de l'énigme n° 8 de la finale 2020 du Concours Alkindi donnée sur Internet (https://concours-alkindi.fr/docs/resolution_enigme_dgse_2020.pdf), Julien, le cryptanalyste de la DGSE, écrit :

La première étape lorsque l'on cherche à résoudre une énigme est d'y trouver des points d'accroche, des choses qui attirent l'œil , qui interpellent ou qui rappellent un mécanisme déjà vu.

Exemple : Vous lisez :

- une suite de nombres croissants de façon bizarre : vous pensez à la suite de Fibonacci.
- une suite de nombres inférieurs à 100 et il y a le mot « éléments » en sous-titre : vous pensez au tableau des éléments périodiques de Mendeleïev .

Au moins deux énigmes du site sont bâties sur ces 2 thèmes.

Ce sont des points de départ. Ensuite l'énigme peut présenter plus ou moins de difficultés, et il faut un peu chercher.

2. Pour continuer :

Il se peut que le texte ne vous dise rien au premier abord. Il y a alors plusieurs cas de figures :

- L'énigme est constituée de lettres

Il peut y avoir y avoir une astuce dans la présentation : texte clair mais écrit à l'envers, ou sur deux colonnes de bas en haut, la première ou la dernière lettre de chaque mot, une charade, le rapport avec le cadran d'un vieux téléphone, etc...

Ces hypothèses une fois éliminées, il faut se poser la question basique : quel est ce type d'énigme : une substitution, une transposition, un code, un mélange d'un peu tout ça ?

a) ***Les lettres du message chiffré sont des lettres peu utilisées en français***

et le texte ressemble à des phrases. Dans ce cas, il y a de fortes chances que l'on soit en face de mots codées directement tels qu'ils sont. Il faut effectuer une analyse de fréquence et compter chaque lettre (voir fiche n° 3, analyse de fréquence).

- Si on est face à une belle distribution de lettres du type A= 15 %, B, C et D = 8 %, etc. un chiffrement en *substitution simple* est probable. Il peut s'agir tout simplement d'un code Jules César, mais aussi d'un codage lettres par lettres, donc il faut effectuer un travail d'analyse de chaque lettre et rechercher dans le crypto quelle est la lettre qui remplace le E, le S, les voyelles (voir fiche n° 3 paragraphe 3 , la substitution simple). Il faut de préférence que le texte soit assez long pour procéder à une analyse de fréquence, sinon c'est quasi mission impossible.

- Si l'analyse de fréquence révèle que chaque lettre est répartie à peu près uniformément dans le texte, il s'agit sans doute d'*une substitution avec clef*, du type tableau de Vigenère (fiche n° 3).
Il faut donc écrire le crypto sur une ligne, et ensuite tester des clefs.

C'est là où le contexte de l'énigme intervient : quel est son titre, qu'est-il écrit pour présenter cette énigme, y a-t-il un dessin (énigme 19) ? Ce sont des indices pour la clef. Les indices, le contexte de l'énigme, la personne qui l'a écrite, déterminent des clefs ou des mots probables.

Notons l'importance de *l'attaque* : il est souvent plus facile de travailler sur les premiers mots ou sur les derniers mots d'un message. Un message peut commencer par « bonjour, « salut », « le code », « cette énigme » ou se terminer par « la solution est », le code est » ou par une signature ... qui sont des indications précieuses de mots probables.

On n'insistera jamais assez sur l'importance de la recherche de mots probables et des mot courants dans un crypto. C'est une attaque de la sorte qui permit (entre autres) de déchiffrer les messages codés avec la machine Enigma et envoyés par les autorités allemandes à leurs sous-marins : dans les bulletins météo, ce sont souvent les mêmes mots que l'on retrouve.

Une astuce : nous avons vu dans la fiche n° 3, à propos du tableau de Vigenère, que pour chiffrer un texte nous avons la relation fondamentale :

Clair + Clef = Crypto

qui peut s'écrire : **Crypto – Clef = Clair**

On peut donc écrire le crypto, puis en utilisant un tableau de Vigenère, effectuer des hypothèses de clef qui feraient apparaître dans le clair un mot ayant du sens.

On a aussi la relation :

Crypto – Clair = Clef

cela signifie que l'on peut fonctionner à l'inverse et faire des hypothèses sur des mots probables du message permettant de trouver une clef qui soit un mot qui ait un sens en français. Le système fonctionne dans les deux sens.

b) ***Les lettres du message chiffré sont fréquentes en français***

(présence de E, de voyelles, de S, N, T, R, L ...) et surtout elles sont collées les unes aux autres : il y a de fortes chances que l'on se trouve face à un chiffrement par transposition, avec une grille rectangulaire de transposition (énigmes 14 , 15, 29).

Il faut alors trouver le bon ordre des lettres (voir fiche n° 5). D'abord, il convient de les compter. Le nombre de lettres est souvent le produit du nombre de lignes par le nombre de colonnes du carré ou du rectangle à partir duquel la transposition a été effectuée. Par exemple si l'on trouve 48 lettres, il est possible que le message ait été écrit sur 8 lignes et 6 colonnes (ou 6 lignes sur 8 colonnes). Bien sûr, des lettres nulles ont pu être ajoutées pour compléter le tableau. On écrit le texte en lignes et on essaye de faire apparaître des mots qui ont un sens en lisant en colonnes, ou inversement. Là encore on fonctionne par mots probables ou noms qui pourraient exister dans le message clair.

Si en plus les colonnes ont subi des permutations à partir d'une clef, les choses se compliquent fortement. (voir fiche n° 5).

Les chiffrements par transposition sont assez, voire très difficiles à décrypter (énigmes n° 29, 30 ,31). Elles demandent souvent de longues recherches, il faut faire de nombreuses hypothèses.

- ***L'énigme est constituée de chiffres***

Il faut tout d'abord examiner si l'on est face à un type de codage connu : ASCII, numération binaire, hexadécimale etc.

Si rien d'évident n'apparaît, plusieurs pistes :

- ces nombres sont compris entre 1 et 26, ou 1 et 36 : il faut bien sûr remplacer chaque nombre par une lettre. On raisonne plus facilement sur des lettres que sur des chiffres.

- ils sont plus grands : on peut essayer de les rectifier en modulo 26 ou autre modulo (énigme 32).

- est ce que ces nombres sont divisibles ou sont premiers ?

- est-ce que chaque nombre est constitué de 2 chiffres ? : il peut s'agir de la numérotation de lignes et de colonnes comme dans un carré de Polybe.

Il peut s'agir de nombres et de chiffres : sur l'une des énigmes de ce site, par exemple, les nombres correspondent aux nombres de jours terrestres nécessaires à une planète du système solaire pour effectuer sa révolution autour du soleil et les lettres ne sont pas chiffrées. Une fois la planète trouvée, on prend simplement la 1re lettre de son nom. Astucieux...

En résumé, il convient de faire correspondre ces chiffres à des lettres et avec un peu d'imagination, on trouve des solutions. Quand on a trouvé une série de lettres, on est alors ramené au problème précédent, comme on dit en mathématiques.

- ***L'énigme est constituée de symboles***

Il est vraisemblablement que nous sommes face à une substitution et que ces symboles représentent des lettres. Si ces symboles ne vous sont absolument pas connu (Templiers, Francs-maçons), un copié-collé du texte sur Google peut faciliter les choses. Vous ferez parfois des découvertes !

Comme pour les cas des nombres, *on peut remplacer les symboles par les lettres de l'alphabet* : on réfléchit plus facilement face à des lettres, dans un environnement connu et familier.

Enfin, mais non des moindres, si l'on ne trouve rien, il convient évidemment de consulter ***le forum*** relatif à l'énigme. On y trouve de précieux indices.

3. Le travail en équipe

Le travail en équipe est essentiel. Le concours Alkindi se fait par équipe et si l'on peut s'entraîner en groupe, c'est mieux. C'est une évidence.

Bien sûr, une équipe est fondée sur la complémentarité de ces membres. A ce sujet, vous avez vu à travers les fiches que pour résoudre une énigme, il faut parfois faire un peu de maths, mais qu'il faut également avoir des qualités en matière littéraire. C'est pourquoi il est important d'avoir dans une équipe **des matheux et des littéraire**s : ils sont complémentaires, chacun(e) fera progresser l'équipe grâce à ses compétences dans son domaine.

A Bletchley Park, près de Londres, pendant la Seconde Guerre mondiale, se trouvait le célèbre *Government Code and Cypher School* au sein duquel travaillaient des mathématiciens, des linguistes, un champion de jeu d'échec, des cruciverbistes etc. On y a recruté du personnel à partir de concours de mots croisés publiés dans le quotidien *Daily Telegraph*.

La résolution d'une énigme nécessite également des qualités d'analyse et de synthèse : analyse pour creuser à fond toutes les possibilités, synthèse pour de temps en temps prendre de la hauteur de vue, regarder de façon globale, revenir à l'essentiel. Ces qualités se trouvent plus ou moins développées en chacun(e) d'entre nous, et là encore la complémentarité des participant(e)s à l'équipe sera importante.

4. La question de la vitesse

La vitesse est également essentielle. Bien sûr, elle se travaille et s'acquiert par la pratique. Prenons par exemple ce message fréquent dans les livres traitant de codes secrets :

« Attaquez demain à 5 heures. Signé général Foch »

Si le message est décrypté par l'ennemi le jour de l'attaque vers quinze heures, cela n'a pas beaucoup d' importance. S'il est décrypté à 3 heures du matin, c'est plus ennuyeux…

Les épreuves de la finale du concours Alkindi se déroulent dans un temps très limité et sur ce site, pour s'entraîner, un bonus est donné au premier qui découvre l'énigme.

La vitesse de résolution d'une énigme est très importante. En équipe, on travaille beaucoup plus vite, on parle, on échange, les idées fusent, chacun apporte aux autres et on progresse beaucoup mieux.

5. Conclusion

Axel, l'administrateur principal de ce site, est allé deux fois en finale du Concours Alkindi avec son équipe. Il nous fait part de son expérience dans cette conclusion qu'il a tout spécialement écrite :

Pour résoudre une énigme, il faut se poser un millier de questions qui ont bien été détaillées dans cette fiche. Il faut chercher, se creuser la tête et ça passe souvent par l'utilisation d'un papier et un crayon.

Pour celles et ceux, futurs candidat(e)s du concours Alkindi qui liront cette fiche, il est important de beaucoup s'exercer. Une chose très importante a été dite dans la présentation des fiches : on pourrait comparer la crypto à des maths dans le sens où ça ne vient pas tout seul.

A moins d'être un(e) véritable génie, les mécanismes que vous devrez acquérir pour résoudre les énigmes si vous arrivez à accéder à la finale du concours Alkindi passent par l'entraînement et la répétition. Ça peut paraître difficile au premier abord mais une fois que vous avez franchi ce cap, ça devient génial ;-).

Une dernière chose à ne pas négliger est qu'il y a une grande différence entre décrypter seul et décrypter en équipe. Si vous participez au concours Alkindi en équipe, entraînez-vous évidemment seul pour progresser mais programmez-vous également des séances d'entraînement ensemble, cela est important pour pouvoir vous faire confiance, apprendre à vous dispatcher les tâches et ne pas paniquer le jour de la finale. Croyez-moi, c'est essentiel…

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

RÉSOLUTION D'UNE ÉNIGME COMPLEXE

Cette énigme est l'exercice n° 7 de l'épreuve finale du Concours Alkindi de 2019. Elle se présente comme suit :

451956011031688349628038305790411254240318196291822346635584477275573923684763329704365784231252305233440950145583905896406215202688278749095325592563004280026540515538790996345413323017454484314017000503759595145468454709293262223331026094476181190651745098779651750988910975597519

Bon courage !

Aucune équipe n'a pu terminer cet exercice. Lors de l'épreuve finale du concours 2020, un exercice identique, l'exercice n° 8, a été proposé. Personne n'a pu le résoudre non plus.

Un an après, au printemps 2021, surprise ! La solution de l'énigme n°8 de la finale 2020 est donnée sur le site officiel du Concours AlKindi. Il suffit simplement de se rendre sur le site :

https://www.concours-alkindi.fr/docs/resolution_enigme_dgse_2020.pdf

pour lire la solution de l'énigme. Elle avait été proposée par la DGSE, partenaire du concours AlKindi, et la solution est signée par « Julien, cryptanalyste à la DGSE ».

Sa lecture est très édifiante, car non seulement elle donne la solution, mais elle explique aussi avec clarté et avec humour quelles sont les questions à se poser devant une énigme et comment réfléchir. Avant de lire cette solution, il faut peut-être faire un bref détour mathématique par les nombres premiers, concept fondamental de l'énigme.

Rappel mathématique : qu’est ce qu’un nombre premier ?

Un nombre premier est un nombre qui « n’est divisible que par 1 et par lui-même », comme disent les mathématiciens. Dit autrement, un nombre premier est un nombre qui n’est divisible par aucun autre nombre. La liste des nombres premiers est 2, 3, 5, 7, 13, 17, 19, 23, 29, 31, 37 ….
Il existe une infinité de nombres premiers.

Si l’on décompose un nombre quelconque en facteurs, c’est à dire si l’on recherche les diviseurs de ce nombre, ces diviseurs sont des nombres premiers. Ils sont appelés facteurs premiers. Par exemple 546 = 2 x 3 x 7 x 13. Le nombre 546 est constitué de 4 facteurs : 2, 3, 7 et 13, qui sont des nombres premiers.

La lecture de la solution de l’exercice n° 8 de la finale 2020, telle que donnée sur le site Internet mentionné ci-dessus, est vivement conseillée pour le compréhension de la suite. En effet, cette énigme se déchiffre exactement de la même manière.

Rappelons donc le texte de l’ énigme :

Énigme :

4519560110316883496280
3830579041125424031819
6291822346635584477275
5739236847633297043657
8423125230523344095014
5583905896406215202688
2787490953255925630042
800265405155387909963
454133230174544843140
170005037595951454684
547092932622233310260
9447618119065174509877
965175098891097559751

Bon courage !

En suivant la méthodologie indiquée pour l’exercice n°8, sur le site déjà mentionné :

https://www.concours-alkindi.fr/docs/resolution_enigme_dgse_2020.pdf,

la solution s’établit comme suit :

1) Il faut considérer cet ensemble de chiffres comme un nombre, les lignes se suivent :

45195601103168834962803830579041125424031819629182234663558447727557392368476332970436578423125230523344095014558390589640621520268827874909532559256300428002654051553879099634541332301745448431401700050375959514546845470929326222333102609447618119065174509877965175098891097559751

Ce nombre est donc constitué de 281 chiffres ! Appelons le X.

2) Il faut diviser ce nombre en facteurs premiers. Cette opération est réalisable sur le site *dcode.fr*,

sur sa page https://www.dcode.fr/decomposition-nombres-premiers

Le résultat de la décomposition en facteurs premiers nous donne X =

```
3 × 719 × 983 × 1283 × 1543 × 1867 × 2137 × 2711 × 3533 × 4397 × 4663 × 5347 × 6287 ×
7253 × 8191 × 9209 × 10133 × 11239 × 11699 × 12109 × 12527 × 13219 × 14243 × 15307 ×
15607 × 16741 × 17683 × 18773 × 19843 × 20921 × 21997 × 23099 × 24223 × 24611 × 25747 ×
26861 × 28001 × 29033 × 30271 × 30649 × 31663 × 32693 × 33811 × 34211 × 35419 × 36563 ×
37649 × 38873 × 40037 × 41231 × 42397 × 42701 × 43801 × 44893 × 45281 × 46489 × 46877 ×
47947 × 49201 × 50417 × 51637 × 52861 × 54037 × 55163 × 55681 × 56149 × 56633
```

Le nombre X est donc constitué de 67 facteurs premiers.

3) Il faut ensuite calculer la position de chacun de ces nombres dans la liste des nombres premiers.

Le site *dcode.fr* va nous y aider. La page https://www.dcode.fr/fonction-compte-nombre-premier nous indique le rang de chacun de ces nombres dans la suite des nombres premiers. Le chiffre 3 est au 2ème rang, 719 au 128ème, 983 est 166ème, 1283 au 208ème, etc. jusqu'à 56 633 qui est le 5743ème nombre premier. Ce qui nous donne la suite de nombres suivants :

2 128 166 208 243 285 322 395 494 599 631 707 818 928 1 028 1 142 etc..

Encore une fois, cet exposé est très résumé, il faut suivre le raisonnement publié sur Internet.

4) On calcule ensuite la différence entre chaque nombre et le précédent. On obtient la suite :

126 38 42 35 42 37 73 99 105 32 76 111 110 100 114 101 15 46 46 46 76 101 115 etc.

5) Enfin, l'examen de ces nombres, tous inférieurs à 128, permet de découvrir que nous sommes en présence d'un code ASCII. Une table de ce code prise sur Internet nous fournit la solution, ainsi que notre ami *dcode.fr* sur sa page https://www.dcode.fr/code-ascii

Et la solution est : **~&*#*% Ici Londres...Les sanglots longs des violons de l'automne…**

On notera la présence de symboles et non de lettres en début de message pour induire le décrypteur en erreur et lui faire croire qu'il part sur une fausse piste. Astucieux...

Conclusion (très importante) :

Cette énigme, petite merveille de complexité, présente également l'intérêt d'être une parfaite illustration du ***Principe de Kerckhoffs*** :

« La sécurité d'un système de chiffrement ne doit reposer que sur le secret de la clef et non pas sur le secret de l'algorithme de chiffrement, qui peut être connu de l'ennemi. »

En effet, l'algorithme de chiffrement de cette énigme est extrêmement compliqué. Pourtant, l'explication du décryptage de l'exercice n° 8 de la finale 2020 a permis de résoudre assez facilement cet exercice n° 7 de la finale 2019 en appliquant les mêmes opérations de déchiffrement.

Pourquoi ? ***Parce qu'il n'y a pas de clef dans cette énigme***. Il n'y a qu'un algorithme, c'est à dire une suite d'opérations à effectuer. Si cette méthode, aussi complexe soit-elle, est appliquée à plusieurs messages et que l'ennemi la connaît, il pourra décrypter facilement tous les messages. L'énigme a bien entendu été construite dans cet esprit.

Il était évidemment impossible pour les candidats participants à la finale de résoudre cette dernière énigme dans le temps imparti pour l'épreuve et munis seulement d'un papier et d'un crayon. D'ailleurs il est même quasi-impossible de la résoudre chez soi avec son ordinateur si on ne connaît pas la méthode de calcul. L'analyste de la DGSE qui l'a conçue a sans doute voulu montrer un exemple de l'utilisation des concepts de la cryptographie moderne, comme par exemple dans le chiffrement RSA : nombre immensément grand de 281 chiffres, nombres premiers, code ASCII...

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

LIVRES, SITES INTERNET, FILMS ET SÉRIES

Si vous avez lu un livre de cryptographie ou découvert un site Internet intéressant, n'hésitez pas à partager votre opinion sur ce site afin que cela profite à tous.

1. DES LIVRES

***Histoires des codes secrets,* Simon Singh, Le Livre de Poche**

Ce livre est sans doute l'un des meilleurs, sinon le meilleur livre sur le sujet. Si vous n'achetez qu'un seul livre, achetez celui-là. Il présente une approche très historique et permet de bien comprendre les techniques de chiffrement et de déchiffrement de l'Antiquité jusqu'à notre époque moderne (le système RSA). L'auteur, Simon Singh, est docteur en physique nucléaire et journaliste scientifique en Grande-Bretagne. L'ouvrage est extrêmement clair, bien documenté, facile à lire, avec une approche très pédagogique. Autre avantage, c'est un Livre de Poche et il n'est pas cher .
Ce livre est un peu ancien (paru en 1999), mais reste une valeur très sûre.

***La Bible des codes secrets*, Hervé Lehning, Flammarion**

Un excellent livre également. L'auteur est professeur agrégé de mathématiques et il a une excellente pédagogie. Le récit est historique, comme il se doit, tout est très clair, bien expliqué, avec humour et avec des petits exercices (corrigés) qui permettent de bien comprendre et de s'entraîner à pratiquer. Ce livre est très complet et comme il est récent (novembre 2019), il aborde également dans ses derniers chapitres des sujets plus modernes : la protection du Wi-Fi, la sécurité des téléphones portables, les fonctions de hachage, la confidentialité des objets connectés etc.
Ce livre est ressorti en poche en octobre 2022 dans la collection Champs science (Flammarion).

Cryptographie classique, de la préparation du concours Alkindi aux épreuves du bac.
Arnaud Henry-Labordère, Éditions Ellipses

Un livre intéressant dont le titre annonce clairement l'objet. L'auteur explique bien la nécessité de connaître les méthodes de cryptographie classiques et en donne de très nombreux exemples de l'Antiquité à la Première Guerre mondiale. Il traite également des machines cryptographiques et des chiffrements modernes : le RSA, le chiffrement symétrique par bloc (DES) ou d'autres modes de chiffrements modernes assez complexes. Le livre est très dense, certains sujets sont traités de façon un peu résumée, mais ils peuvent être approfondis par ailleurs sur Internet. Un bon livre.

À noter : ce livre fournit également une « boîte à outils » de *petits programmes classiques en Python,* pour chiffrer et déchiffrer, niveau Bac scientifique, ainsi que *les Annales et corrigés de tous les exercices des épreuves finale du concours Alkindi de 2016 à 2020.*

La Cryptologie, L'art des codes secrets, **Philippe Guillot, éditeur edp sciences**

Philippe Guillot est maître de conférence à l'Université Paris 8, en charge du cours de cryptologie, d'histoire de la cryptologie et d'algorithmique algébrique dans le master « Mathématiques fondamentales et protection de l'information ». Auparavant, il a travaillé dans le domaine de la sécurité informatique chez Thomson CSF, Thales et Canal-Plus Technologies.

Ce livre est d'un niveau assez élevé. Le 1er chapitre retrace l'histoire des méthodes traditionnelles. Les 2 chapitres suivants traitent de la cryptologie symétrique moderne et de la cryptologie à clé publique (asymétrique). Puis les chapitres suivants donnent de nombreux exemples de l'utilisation de la cryptographie au quotidien : cartes bancaires, Internet, téléphone mobile, télévision à péage. Le chapitre 7 présente les éléments de la théorie cryptologique (très ardu), et le dernier chapitre traite de cryptologie quantique.

Ce livre vous intéressera si vous souhaitez entreprendre des études dans le domaine informatique et dans la cybersécurité.

Une BD *: « Qui a cassé Enigma ?* **de Fabien Tillon (scénario), et Lelio Bonaccorso((dessin),**

Cette BD a été réalisée d'après l'œuvre de Dermot Turing, « ***Enigma, où comment les Alliés ont réussi a casser le code nazi*** ». Dermot Turing, neveu d'Alan Turing, a écrit un livre pour raconter les débuts des recherches pour décrypter Enigma, de 1931 à 1940, et le rôle très important joué par les mathématiciens polonais avant les travaux définitifs de son oncle.

2. DES SITES INTERNET

- dcode.fr

Ce site vous permet de gagner énormément de temps, puisqu'il décrypte un message secret chiffré par un tableau de Vigenère ou par le code ADFGX en quelques dixièmes de seconde. Encore faut-il savoir, face à un message, de quel type de chiffrement il s'agit ?
D'où la nécessité de connaître un peu les principaux types de chiffrement. Le sujet a été évoqué dans la fiche de présentation (fiche n° 1).

Par aileurs, **dcode.fr** présente des articles forts intéressants qui traitent de nombreux sujets de cryptographie, de l'Antiquité à nos jours.

- cryptoprograms.com

Site à peu près semblable à dcode.fr qui permet de chiffrer et de déchiffrer en anglais, en français et dans de nombreuses autres langues.
Il existe de nombreux sites Internet consacrés à a cryptographie, il suffit de taper « code secret » ou « cryptographie » sur Google. Laissez-vous le plaisir de les découvrir et n'hésitez pas à nous en parler.

3. APPLICATION Android pour téléphone mobile

Cryptography – Collection of cyphers and hashes

Cette application est assez impressionnante. Elle propose un très grand nombre de modes de chiffrements et de déchiffrements, ainsi que des cours théoriques ! Elle a été créée à l'origine en anglais, mais s'adapte à la langue du téléphone, en l'occurrence le français pour nous.

Une application très sympa, à télécharger sur son téléphone sur Google Play Store ou sur :

https://play.google.com/store/apps/details?id=com.nitramite.cryptography

4. UN FILM

The Imitation Game (2014, de Morten Tyldum)

The Imitation Game raconte la vie du mathématicien anglais Alan Turing qui avec son équipe de collaborateurs est parvenu à décrypter les messages de la machine Enigma à Bletchley Park, près de Londres, durant la Seconde Guerre mondiale (voir fiche n° 6).

L'acteur britannique Benedict Cumberbatch est remarquable dans le rôle du célèbre mathématicien. Il faut l'écouter bafouiller en interprétant ce personnage, timide, introverti, mal à l'aise en société, mais extrêmement intelligent. Bien sûr, le film est un peu romancé : Alan Turing n'était pas en opposition permanente avec ses supérieurs ni avec les membres de son équipe. Mais il faut bien pimenter un peu le récit, et la scène où le héros réalise par quel moyen il peut « casser » Enigma ne suffirait pas à elle toute seule à remplir le film, même si c'est l'un des moment fort et émouvant. De nombreux flash-backs permettent de mieux comprendre la vie d'Alan Turing et sa fin tragique.

Un très beau film, passionnant et agréable à voir.

5. UNE SÉRIE

Le Bureau des Légendes

Une série que ne traite pas spécifiquement de cryptographie, mais plutôt de certains aspects du travail de la DGSE. Elle comporte 5 saisons de 10 épisodes, et raconte la vie quotidienne d'agents de renseignement français à l'étranger et sur le territoire national.

Réalisée par Eric Rochant, cette série a été unanimement saluée par la critique française et internationale. Les scénarios des différentes saisons collent remarquablement bien à la réalité géopolitique des périodes concernées (2015 à 2020), comme par exemple la question de l'armement atomique de l'Iran, du ver informatique Stuxnet ou de la lutte contre l'État Islamique en Syrie et en Irak.

A certains moments, et spécialement dans la saison 4, on y découvre le travail des spécialistes des cyberattaques, qui nécessitent une très grande technicité. Les séquences de piratage de téléphones portables en Russie sont assez jubilatoires.

Attention : les scènes d'ouvertures de certains épisodes de la saison 5 sont un peu délicates pour des jeunes de moins de 13 / 14 ans.

6. UNE PIÈCE DE THÉÂTRE

La Machine de Turing

Cette pièce de théâtre a été créée en 2018 par Benoit Solès, qui interprète le rôle d'Alan Turing. En une quinzaine de scènes sont évoqués les moments forts de la vie du grand mathématicien : son enfance, son amitié avec Christopher, la vie à Cambridge, la recherche en mathématiques : est ce qu'une machine peut penser ? Et bien sûr les secrets dans lesquels il lui a fallu vivre : secret sur le décryptage d'Enigma, secret de son homosexualité.

C'est une pièce très forte et très émouvante, qui souvent bouleverse le spectateur. Elle a obtenu 4 Molière en 2019. Bien que très récente, elle est déjà publiée dans les classiques Nathan et peut être étudiée au collège ou au lycée. Elle est toujours jouée à Paris et tourne parfois dans toute la France et à l'étranger.

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

LE CHIFFREMENT AES

1. Le contexte d'AES

En 1977, un chiffrement appelé DES fut créé par IBM. Il scindait les messages en blocs de 64 bits, pour les chiffrer avec une clé de 64 bits également. On s'aperçut qu'il comportait quelques faiblesses et il fut triplé, c'est-à-dire que les opérations de chiffrement furent appliquées 3 fois de suite : ce fut le triple DES. Puis il fut remplacé par un nouvel algorithme : l'AES.

L'AES fut adopté par le National Institute of Standards and Technology en 2000.

2. Principe de fonctionnement de l'AES

AES est un algorithme de chiffrement symétrique : il utilise la même clé pour le chiffrement et le déchiffrement des données. Il repose sur une combinaison d'opérations de substitutions et d'opérations de permutations.

Les données du message à chiffrer sont réparties en **blocs,** qui sont des carrés de 16 cases (4x4) dans lesquels ces données sont placées. On applique ensuite sur ces blocs un certain nombre d'opérations de chiffrement appelées **tours.**

Chaque tour suit une série d'étapes bien définies.

3. La structure de l'algorithme AES

Voici les étapes d'un chiffrement AES (l'exemple concret expliquera en détail les opérations) :

- Avant le premier tour, **un premier chiffrement** est effectué avec une **clé initiale**. Puis viennent les tours qui comportent les opérations suivantes :

- **SubBytes** (Substitution des octets)

Dans cette étape, chaque octet du bloc de données chiffrées est remplacé par un autre octet selon une table de substitution appelée **S-box** (voir cette table en annexe 1)

- **ShiftRows** (Permutation des lignes)

Dans cette étape, les octets de chaque ligne du bloc de données (considéré comme une matrice de 4x4) sont déplacés de manière cyclique. La première ligne n'est pas modifiée, la seconde est décalée

d'un octet vers la gauche, la troisième de deux octets, et la quatrième de trois octets. Cela permet de brouiller les positions des données dans le bloc.

- **MixColumns** (Mélange des colonnes)

Dans cette étape, chaque colonne du bloc est mélangée avec une ligne d'un autre bloc en effectuant un produit matriciel, l'un des blocs étant constituée de chiffres et l'autre contenant les données.

- **AddRoundKey** (Ajout de la clé de tour)

Enfin, une opération XOR (voir la définition dans l'exemple ci-dessous) est effectuée entre le bloc de données et une sous-clé dérivée de la clé initiale. La sous-clé change à chaque tour, elle est obtenue à l'aide d'un processus appelé **Key Expansion**. Donc à chaque round, les blocs ont une nouvelle sous-clé spécifique.

4. Le processus de Key Expansion (Expansion de la clé)

Dans AES, la clé initiale est étendue pour générer une sous-clé unique pour chaque tour. L'algorithme AES inclut **un processus d'expansion de la clé qui utilise la clé initiale et la transforme en une série de sous-clés.** Chaque sous-clé dépend de la sous-clé du round précédent : la clé du round 2 est calculé par un algorithme à partir de la clé du round 1.

5. Processus complet de chiffrement

1. **Initialisation** : La première étape est un **AddRoundKey**, où le bloc de données d'entrée est chiffré avec la clé initiale.

2. **Tours principaux** : Ensuite, chaque tour (excepté le dernier) applique les quatre étapes mentionnées plus haut : SubBytes, ShiftRows, MixColumns, et AddRoundKey.

3. **Dernier tour** : Lors du dernier tour, l'étape **MixColumns** est omise, ne laissant que SubBytes, ShiftRows, et AddRoundKey.

6. Exemple concret de chiffrement :

6.1 Initialisation : AddRoundKey

Soit le message clair :

L	**e**	**s**		**R**	**o**	**i**	**s**		**M**	**a**	**u**	**d**	**i**	**t**	**s**

et la clé :

c	**r**	**y**	**p**	**t**	**o**	**g**	**r**	**a**	**p**	**h**	**i**	**q**	**u**	**e**	**s**

Ici, la clé est un mot pour une meilleure compréhension, mais dans la réalité c'est une clé aléatoire.

On code le message et la clé en numération hexadécimale. Si vous le souhaitez, consultez la fiche n°4 « Les codes et les dictionnaires » pour voir le codage ASCII et la numération hexadécimale.

Vous trouverez également en annexe 2 une table ASCII pour une meilleure compréhension.

Cela nous donne donc en hexadécimal :

L	**e**	**s**		**R**	**o**	**i**	**s**		**M**	**a**	**u**	**d**	**i**	**t**	**s**
4C	**65**	**73**	**20**	**52**	**6F**	**69**	**73**	**20**	**4D**	**61**	**75**	**64**	**69**	**74**	**73**

et pour la clé :

c	**r**	**y**	**p**	**t**	**o**	**g**	**r**	**a**	**p**	**h**	**i**	**q**	**u**	**e**	**s**
63	**72**	**79**	**70**	**74**	**6F**	**67**	**72**	**61**	**70**	**68**	**69**	**71**	**75**	**65**	**73**

Les données en hexadécimal sont ensuite réparties dans des carrés de 4 x 4 cases, appelés blocs. Chaque bloc comporte donc 16 cases, et dans chaque case se trouve un nombre hexadécimal de 2 chiffres qui en binaire égale un octet (8 bits). On a donc au total des blocs de 128 bits (16 x8).

On écrit les données verticalement dans la colonne 1, puis colonne 2, colonne 3 etc. , ce qui donne pour le message clair:

4C	**52**	**20**	**64**
65	**6F**	**4D**	**69**
73	**69**	**61**	**74**
20	**73**	**75**	**73**

Message clair

et pour la clé :

63	**74**	**61**	**71**
72	**6F**	**70**	**75**
79	**67**	**68**	**65**
70	**72**	**69**	**73**

Clé

Comme dans un chiffrement de type Vigenère, on va additionner le message clair et la clé.
Ceci va s'effectuer en additionnant chaque nombre du bloc du message clair avec le nombre de la case correspondante du bloc de la clé.

Pour cela, l'ordinateur convertit les nombres hexadécimaux en nombres binaires, effectue les additions en binaire, puis reconvertit le résultat des additions en hexadécimal.

Les calculs sont effectués en « chiffrement XOR » (en anglais eXclusive OR, c'est-à-dire « ou exclusif »).

L'addition XOR , en binaire, est notée $\oplus$. Les règles de calcul sont très spécifiques et reposent sur l'addition des 0 et des 1. Elles sont les suivantes :

Addition en XOR		
A	**B**	**R = A ⊕ B**
0	0	0
0	1	1
1	0	1
1	1	0

On trouvera en annexe 3 le détail des opérations d'addition en XOR. Dans notre exemple on effectue le calcul : 01001100 ⊕ 0110001 = 00101111, et donc = 2F en hexadécimal.

On a donc 4C ⊕ 63 = 2F

4C	**52**	**20**	**64**
65	**6F**	**4D**	**69**
73	**69**	**61**	**74**
20	**73**	**75**	**73**

Clair

+

63	**74**	**61**	**71**
72	**6F**	**70**	**75**
79	**67**	**68**	**65**
70	**72**	**69**	**73**

Clé

=

2F			

Chiffré

6.2 SubBytes :

Dans cette étape, chaque octet du bloc de données est remplacé par un autre octet selon une table de substitution appelée **S-box** (voir cette table en annexe 1). Cette table de substitution est conçue pour être non-linéaire, ce qui permet de rendre le chiffrement plus résistant aux attaques.

6.3 ShiftRows (permutation des lignes) :

Dans cette étape, les octets de chaque ligne du bloc de données (considéré comme une matrice de 4x4) sont déplacés de manière cyclique. La première ligne n'est pas modifiée, la seconde est décalée d'un octet vers la gauche, la troisième de deux octets, et la quatrième de trois octets. Cela permet de brouiller les positions des données dans le bloc.

En supposant les données dans un bloc de 16 cases, le tableau d'origine est ainsi modifié :

1	**2**	**3**	**4**
5	**6**	**7**	**8**
9	**10**	**11**	**12**
13	**14**	**15**	**16**

→

1	**2**	**3**	**4**
6	**7**	**8**	**5**
11	**12**	**9**	**10**
16	**13**	**14**	**15**

6.4 Mix Columns (Mélange des colonnes)

On effectue un produit matriciel : on multiplie chaque donnée d'une colonne par une ligne d'une matrice prédéfinie par l'algorithme AES.

Voici un exemple :

Pour la 1ère ligne, on calcule :

i_0	i_1	i_2	i_3
i_4	i_5	i_6	i_7
i_8	i_9	i_{10}	i_{11}
i_{12}	i_{13}	i_{14}	i_{15}

x

1	**2**	**3**	**4**
6	**7**	**8**	**5**
11	**12**	**9**	**10**
16	**13**	**14**	**15**

=

		c	**d**
			e
			f
			g

$(4xi_0)$

$+ (5xi_1) + (10xi_2) + (15xi_3)$ qui est égal à **d**

Puis pour la 2ème ligne : = $(4xi_4) + (5xi_5) + (10xi_6) + (15xi_7)$ = **e**

On continue pour la 3ème ligne : $(4xi_8) + (5xi_9) + (10xi_{10}) + (15xi_{11})$ = **f**

Et on calcule enfin la valeur g de la 4ème ligne = **g**.

On recommence le processus sur la colonne 3 :

$(3xi_0) + (8xi_1) + (9xi_2) + (14xi_3)$ qui est égal à **c**, 1ère donnée de la colonne 3.
Et ainsi de suite sur les 3 autres données de la 3éme colonne, puis les colonnes 2 et 1.

Les multiplications sont également effectuées **en numération binaire** , par l'intermédiaire de calculs sur des polynômes. Le processus mathématique est un peu complexe, on trouvera si on le souhaite le détail des calculs en annexe 3.

On obtient au final un nouveau bloc qui est résultat de ce produit matriciel.

6.5 AddRoundKey

Enfin, une nouvelle opération d'addition est effectuée entre le bloc de données et une sous-clé dérivée de la clé initiale, pour préparer les opérations sur le bloc suivant. La sous-clé change à chaque tour, provenant du processus appelé **Key Expansion** (voir paragraphe 4).

On répète toutes ces opérations 9 à 13 fois avec les sous-clés dérivées de la clé principale, et on ne fait pas de **MixColumn** sur la dernière opération pour réduire le temps de chiffrement de AES.

7. Déchiffrement

Le processus de déchiffrement est une inversion des étapes de chiffrement, avec quelques différences spécifiques :

- **Inverse SubBytes** : Utilisation d'une table de substitution inverse (Inverse S-box).
- **Inverse ShiftRows** : Les lignes sont décalées dans l'autre sens.

- **Inverse MixColumns** : Application inverse du mélange des colonnes.
- **AddRoundKey** reste inchangé, puisqu' une opération XOR est son propre inverse.

8. Conclusion : sécurité d'AES

Comme toujours dans un mode de chiffrement, il faut faire un compromis entre sécurité et temps de calcul. L'étape **MixColumn**, qui est un produit matriciel, est longue en temps de calcul.

On considère actuellement qu'avec un minimum de 10 tours et avec une clé suffisamment longue d'au moins 256 bits, AES est bien sécurisé. Aucune attaque pratique ne remet en cause la sécurité d'AES lorsqu'il est correctement utilisé. (Un nombre de 256 bits représente un nombre d'environ 77 chiffres en décimal)

AES est largement utilisé dans de nombreuses applications (VPN, https, chiffrement des fichiers, etc.). Il a été conçu pour être efficace aussi bien sur le matériel que sur le logiciel, ce qui le rend adapté pour un large éventail de systèmes, des serveurs puissants aux dispositifs embarqués.

9. Remerciements :

Pour réaliser cette fiche, j'ai utilisé, parmi d'autres sources d'information, une **vidéo réalisée par Mickaël Dupont**, publiée sur YouTube (et citée avec l'autorisation de l'auteur) :

https://www.youtube.com/@MickaDupont?app=desktop

Je vous la recommande vivement, elle est extrêmement claire et pédagogique.

*****

***

*

Annexe 1

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

Annexe 2

Table ASCII (0 - 127)

Binaire	Hex.	Déc.	Caractères ASCII	Explications	Groupe
		0-31			Caractère de contrôle
0100000	20	32	SP	Espace (*Space*)	Caractère spécial
0100001	21	33	!	Point d’exclamation	Caractère spécial
0100010	22	34	"	Guillemets droits en haut	Caractère spécial
0100011	23	35	#	Dièse	Caractère spécial
0100100	24	36	$	Signe dollar	Caractère spécial
0100101	25	37	%	Signe pourcentage	Caractère spécial
0100110	26	38	&	Esperluette	Caractère spécial
0100111	27	39	‘	Apostrophe	Caractère spécial
0101000	28	40	(	Parenthèse gauche	Caractère spécial
0101001	29	41	)	Parenthèse droite	Caractère spécial
0101010	2A	42	*	Astérisque	Caractère spécial
0101011	2B	43	+	Signe plus	Caractère spécial
0101100	2C	44	,	Virgule	Caractère spécial
0101101	2D	45	-	Trait d’union	Caractère spécial
0101110	2E	46	.	Point (fin de phrase)	Caractère spécial
0101111	2F	47	/	Barre oblique (« slash »)	Caractère spécial
0110000	30	48	0		Chiffre
0110001	31	49	1		Chiffre
0110010	32	50	2		Chiffre
0110011	33	51	3		Chiffre
0110100	34	52	4		Chiffre
0110101	35	53	5		Chiffre
0110110	36	54	6		Chiffre
0110111	37	55	7		Chiffre
0111000	38	56	8		Chiffre
0111001	39	57	9		Chiffre
0111010	3A	58	:	Deux points	Caractère spécial
0111011	3B	59	;	Point-virgule	Caractère spécial
0111100	3C	60	<	Inférieur à	Caractère spécial
0111101	3D	61	=	Signe égal	Caractère spécial
0111110	3E	62	>	Plus grand que	Caractère spécial
0111111	3F	63	?	Point d’interrogation	Caractère spécial

1000000	40	64	@	Arobase	Caractère spécial
1000001	41	65	A		Lettre majuscule
1000010	42	66	B		Lettre majuscule
1000011	43	67	C		Lettre majuscule
1000100	44	68	D		Lettre majuscule
1000101	45	69	E		Lettre majuscule
1000110	46	70	F		Lettre majuscule
1000111	47	71	G		Lettre majuscule
1001000	48	72	H		Lettre majuscule
1001001	49	73	I		Lettre majuscule
1001010	4A	74	J		Lettre majuscule
1001011	4B	75	K		Lettre majuscule
1001100	4C	76	L		Lettre majuscule
1001101	4D	77	M		Lettre majuscule
1001110	4E	78	N		Lettre majuscule
1001111	4F	79	O		Lettre majuscule
1010000	50	80	P		Lettre majuscule
1010001	51	81	Q		Lettre majuscule
1010010	52	82	R		Lettre majuscule
1010011	53	83	S		Lettre majuscule
1010100	54	84	T		Lettre majuscule
1010101	55	85	U		Lettre majuscule
1010110	56	86	V		Lettre majuscule
1010111	57	87	W		Lettre majuscule
1011000	58	88	X		Lettre majuscule
1011001	59	89	Y		Lettre majuscule
1011010	5A	90	Z		Lettre majuscule
1011011	5B	91	[	Crochet gauche	Caractère spécial
1011100	5C	92	\	Barre oblique inversée (*backslash*)	Caractère spécial
1011101	5D	93	]	Crochet droit	Caractère spécial
1011110	5E	94	^	Accent circonflexe	Caractère spécial
1011111	5F	95	_	Tiret bas	Caractère spécial
1100000	60	96	`	Accent grave	Caractère spécial
1100001	61	97	a		Lettre minuscule
1100010	62	98	b		Lettre minuscule
1100011	63	99	c		Lettre minuscule
1100100	64	100	d		Lettre minuscule
1100101	65	101	e		Lettre minuscule
1100110	66	102	f		Lettre minuscule
1100111	67	103	g		Lettre minuscule
1101000	68	104	h		Lettre minuscule
1101001	69	105	i		Lettre minuscule
1101010	6A	106	j		Lettre minuscule
1101011	6B	107	k		Lettre minuscule

1101100	6C	108	l		Lettre minuscule
1101101	6D	109	m		Lettre minuscule
1101110	6E	110	n		Lettre minuscule
1101111	6F	111	o		Lettre minuscule
1110000	70	112	p		Lettre minuscule
1110001	71	113	q		Lettre minuscule
1110010	72	114	r		Lettre minuscule
1110011	73	115	s		Lettre minuscule
1110100	74	116	t		Lettre minuscule
1110101	75	117	u		Lettre minuscule
1110110	76	118	v		Lettre minuscule
1110111	77	119	w		Lettre minuscule
1111000	78	120	x		Lettre minuscule
1111001	79	121	y		Lettre minuscule
1111010	7A	122	z		Lettre minuscule
1111011	7B	123	{	Accolade gauche	Caractère spécial
1111100	7C	124	|	Trait vertical (*pipe*)	Caractère spécial
1111101	7D	125	}	Accolade droite	Caractère spécial
1111110	7E	126	~	Tilde	Caractère spécial
111111	7F	127	DEL	Delete	Caractère spécial

Annexe 3

Les opérations en numération binaire et hexadécimale

1. Les systèmes de numération décimale, binaire et hexadécimale :

Un ordinateur calcule beaucoup plus vite en système binaire qu'en système décimal. C'est pourquoi en informatique on effectue les calculs en système binaire.

La relation entre les 3 systèmes de numération est la suivante :

Numération décimale : le nombre 523, par exemple, est constitué ainsi :

Position	10^2	10^1	10^0
Nombre	5	2	3

On a donc $523 = (5x10^2) + (2x10^1) + (3x10^0)$

$= (5x100) + (2x10) + (3x1)$

$= 500 + 20 + 3$

$= 523$

Numération hexadécimale :

Soit le nombre hexadécimal 5C. Comme pour le décimal, on a :

Position	16^1	16^0
Nombre	5	C

De la même façon que pour le décimal, on a :

$5C = (5x16^1) + (Cx16^0)$

$= (5x16) + (12x1)$ en décimal

$= 80 + 12 = 92$

Numération binaire

Soit le nombre 203 qui s'écrit en binaire binaire 11001011 :

Position du bit	7	6	5	4	3	2	1	0
Nombre	1	1	0	0	1	0	1	1

En décimal, il se calcule comme suit :

$= 2^7 + 2^6 + 2^3 + 2^1 + 2^0$

$= 128 + 64 + 8 + 2 + 1 = 203$

Relation entre le binaire et l'hexadécimal :

Si l'on considère un octet, c'est à dire 8 bits, on peut constater qu'un nombre binaire de 8 bits est constitué de 4 bits de rang 7 à 4 et de 4 bits de rang 3 à 0. Le nombre décimal 203 va donc s'écrire

Rang du bit	**7 6 5 4**	**3 2 1 0**
Binaire	1 1 0 0	1 0 1 1
Hexadécimal	C	B

On a séparé en deux groupes de 4 pour plus de clarté, mais bien sûr c'est un seul et même chiffre d'un octet. Les 4 derniers bits sont 1011 qui est égal à B et les 4 premiers bits sont 1100 qui est égal à C. On a donc CB = en décimal (12 x16) +11 = 192 + 11 = 203 que l'on retrouve bien.

Autre exemple :

Rang du bit	**7 6 5 4**	**3 2 1 0**
Binaire	0 1 1 0	1 0 0 1
Hexadécimal	6	9

Et 69 en hexadécimal = (6 x 16) + 9 =105 en décimal

Dans le code ASCII , on peut ainsi avoir 256 caractères (de 0 à 255) représentés chacun par un octet en binaire ou un nombre de 2 chiffres en hexadécimal.

On a ainsi de 0 à 255 :

	Décimal	**Binaire**	**Hexadécimal**
de	0	00000000	00
	15	00001111	0F
	16	00010000	10
	127	01111111	7F
	128	10000000	80
à	255	11111111	FF

2. L'addition XOR en binaire :

L'addition XOR , en binaire, est notée ⊕. En XOR, les règles de calcul sont les suivantes:

Addition en XOR		
A	**B**	**R = A ⊕ B**
0	0	0
0	1	1
1	0	1
1	1	0

Notons qu' il n'y a pas de retenues, contrairement à une addition classique de 2 nombres binaires.

Ce qui nous donne par exemple :

	Hexa		**Binaire**
	4C	--->	01001100
⊕	63	--->	⊕ 01100011
	-----		----------
	2F	←---	**00101111**

3. La multiplication en binaire

Dans l'opération **Mix Columns ,** il faut effectuer un produit entre les deux tableaux. Mathématiquement, c'est un produit de matrices. Voici le détail du calcul :

On effectue ce que l'on appelle un produit matriciel : on multiplie chaque donnée d'une colonne par une ligne d'une matrice prédéfinie par l'algorithme AES.

Exemple : Soit à multiplier les deux tableaux :

03	02	01	01
01	02	03	01
03	01	02	01
02	01	01	03

Matrice prédéfinie

x

FA		**31**	**C7**
C5	**2F**	**3F**	**36**
31	**12**	**9**	**10**
6D	**13**	**14**	**15**

Message

=

d		
e		
f		
g		

Résultat crypté

Pour effectuer ce produit matriciel, il faut calculer dans la case d:

d = (03xFA) + (02xC5) + ((01x31) + 01x6D)

Calcul du premier facteur

On travaille en binaire. On a : 03 x FA = 11 x 11111010
hexa binaire

Pour effectuer ce calcul, on introduit un polynôme f(x) dont les exposants de x vont être déterminés par la position des 1 dans le nombre binaire. Les exposants de x varient de 7 à 0 :

--→ 11 correspond à un polynôme : $(x^1 + x^0)$ c'est à dire (x + 1)

— > 11111010 correspond à un polynôme : $(x^7 + x^6 + x^5 + x^4 + x^3 + x)$

On voit que les exposants de x correspondent aux position des 1 dans l'octet. Il y a dans le chiffre binaire 11111010 des zéros en position 3 et en position 1, c'est à dire $x^2 + x^0$, donc ces 2 termes sont supprimés dans le polynôme.

On va donc effectuer la multiplication :

$$(x + 1)(x^7 + x^6 + x^5 + x^4 + x^3 + x)$$

Ce qui nous donne :

$x(x^7 + x^6 + x^5 + x^4 + x^3 + x) + (x^7 + x^6 + x^5 + x^4 + x^3 + x)$

$= x^8 + x^7 + x^6 + x^5 + x^4 + x^2 + x^7 + x^6 + x^5 + x^4 + x^3 + x$

Là, on supprime les valeurs de x qui sont en double, c'est à dire qui ont le même exposant. En effet, l'addition est un XOR, et donc l'addition de deux nombres identique = 0. (Règle 1 + 1 = 0). Il reste

03 x FA = $x^8 + x^3 + x^2 + x$

Afin de supprimer les termes en x^8, on soustrait le polynôme irréductible $(x^8 + x^4 + x^3 + x + 1)$

Ce qui nous donne :

03 x FA = $x^8 + x^3 + x^2 + x - (x^8 + x^4 + x^3 + x + 1)$

03 x FA = $x^4 + x^2 + 1$

Soit en résultat binaire 03 x FA = 00010101

On effectue le même type de calcul pour 02xC5, soit en binaire = 10 x 11000101

Pour la 2ème multiplication, le même type de calcul avec les polynômes, que nous ne détaillerons pas de nouveau, nous donne le résultat :

02 x C5 = $x^7 + x^4 + 1$ soit en binaire = 10010001

Pour les 3ème et 4ème termes, c'est plus facile puisque 01 x 31 = 31 et 01 x 6D = 6D.

01 x 31 = 00110001
01 x 6D= 01101101

En définitive, le calcul de d est le suivant (en XOR)

```
    03 x FA  = 00010101
⊕   02 x C5  = 10010001
⊕   01 x 31  =  00110001
⊕   01 x 6D =  01101101
                ----------
          d =    11011000
```

Soit d = D8 en hexadécimal, c'est ce nombre qui est reporté dans le tableau du résultat chiffré.

L'algorithme effectue le même calcul de multiplication de matrices sur chacune des 16 cases du tableau.

*****
***
*

LE CHIFFREMENT PAR COURBES ELLIPTIQUES

1. **Qu'est ce qu'une courbe elliptique ?**

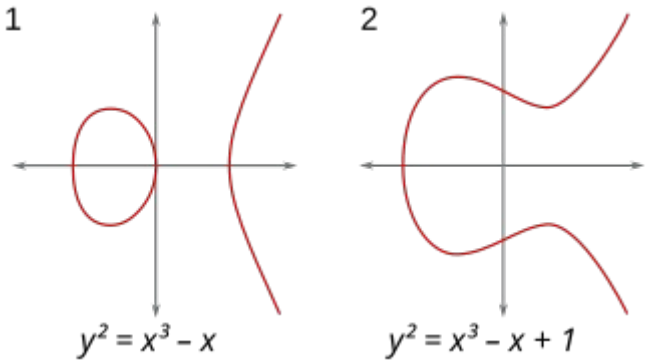
Les courbes elliptiques sont des fonctions de type : $y^2 = f(x)$ où f(x) est un polynôme en x^3

En cryptographie, on utilise des courbes elliptiques de la forme :

$$y^2 = x^3 + ax + b$$

Remarquons qu'il n'y a pas de x^2 . Les coefficients a et b sont des nombres réels. Selon le choix de ces coefficients, les graphes peuvent avoir deux formes possibles.

Exemples :



On voit que dans le graphe 1, l'équation a trois racines réelles distinctes (-1, 0, et +1) et que dans le graphe 2, elle n'a qu'une seule racine réelle.

2. **Utilisation des courbes elliptiques en cryptographie :**

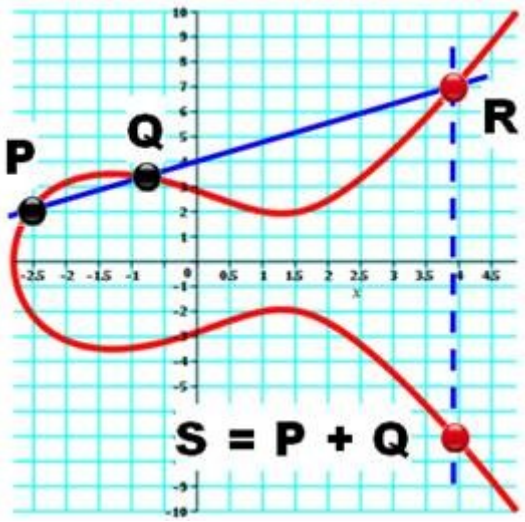
Cette fiche a pour but de présenter de façon simple le chiffrement par courbes elliptiques. Nous resterons dans un contexte général et ne tiendrons pas compte des nombreux cas particuliers présentés par ces courbes. Nous essaierons de rester au niveau de mathématiques du lycée.

2.1 Addition de deux points sur une courbe elliptique :

Pour commencer, on définit l'addition de deux points de la courbe. L'addition s'effectue de la manière suivante : on choisit deux points P et Q sur une courbe elliptique. Ces deux points sont définis par leurs coordonnées $P(x_1, y_1)$ et $Q(x_2,y_2)$.

Deux points P et Q sur une courbe elliptique forment une droite qui coupe toujours la courbe en un troisième point. Soit R ce point. Le symétrique du point R par rapport à l'axe des x, appelons-le S, **est défini comme la somme des points P et Q**. Les points sont définis par leurs coordonnées.

Cette définition peut paraître un peu étrange, regardons un graphe :



On a donc $S(x_3, y_3) = P(x_1, y_1) + Q(x_2,y_2)$

Pour ne pas alourdir cette présentation, nous verrons en détail l'aspect mathématique de cette addition dans l'annexe 1. Pour l'instant prenons cette addition telle qu'elle est.

Sur une courbe elliptique, de même que l'on peut additionner deux points, on peut également multiplier un point par un nombre entier.

2.2 Multiplication d'un point par un entier :

Puisque l'on a défini l'addition, continuons et définissons la multiplication d'un point par un nombre entier d.

Si P est un point sur la courbe, on peut calculer 2P, 3P, 4P etc. en utilisant ce qu'on appelle la *multiplication scalaire*. Concrètement **on répète le principe de l'addition** : P + P = 2P, puis 2P + P = 3P, puis 3P + P = 4P et ainsi de suite…

Le résultat de cette multiplication est un point S. Là encore nous verrons tout cela en détail en annexe avec des exemples chiffrés et des graphes. Le but ici est de comprendre les principes.

En résumé, nous avons donc un point **P** sur une courbe elliptique, un nombre entier **d** et un point **S** sur cette courbe tel que :

$$\mathbf{S = d \times P}$$

Et nous en arrivons enfin au principe de chiffrement :

3. Principe de chiffrement :

Le chiffrement repose sur le fait que si l'on connaît un point P sur une courbe elliptique et un autre point S tel que S = dP, il est extrêmement difficile de trouver d à partir des coordonnées de P et de S.

Ce chiffrement, qui est **asymétrique**, s'effectue donc comme suit :

- Alice et Bob se mettent d'accord, publiquement, sur une courbe elliptique ainsi que sur un point P (x_1, y_1) situé sur la courbe, ce point P étant également connu publiquement.

- Alice choisit secrètement un nombre entier d_A et envoie à Bob les coordonnées du point d_AP.

- Bob choisit secrètement un nombre entier d_B et envoie à Alice les coordonnées du point d_BP.

- Alice peut calculer $d_A(d_BP)$ et Bob peut calculer $d_B(d_AP)$, **c'est à dire $((d_Ad_B)P)$ qui est leur clé commune.**

Si Ève, qui espionne Alice et Bob, a intercepté les échanges, elle connaît l'équation de la courbe, le point P, d_AP et d_BP. Mais elle ne peut pas calculer d_A et d_B, et donc le produit $(d_Ad_B)P$ qui est la clé commune.

Le calcul de d_A en connaissant P et le produit d_AP s'appelle résoudre le *logarithme discret* sur une courbe elliptique. Si les nombres d_A et d_B sont suffisamment grands, on ne peut pas les calculer avec les performances actuelles des ordinateurs.

Ce mode de chiffrement asymétrique, comme le RSA, repose sur une difficulté arithmétique non calculable actuellement par les ordinateurs.

ANNEXE 1

NOMBRES RÉELS ET CORPS FINIS

1. Courbes elliptiques sur les nombres réels (définition mathématique générale)

Les courbes elliptiques ont d'abord été étudiées dans le cadre des mathématiques pures, sur des corps tels que les **nombres réels R**. Ce sont des objets géométriques qui possèdent une structure algébrique particulière, souvent définis par une équation de la forme :

$$y^2 = x^3 + ax + b$$

Dans ce cadre, les courbes elliptiques sont représentées comme des objets continus, avec une courbe lisse qui peut être visualisée graphiquement. Travailler sur les nombres réels ou complexes permet d'étudier les propriétés géométriques et algébriques de ces courbes (points d'inflexion, tangentes, symétries, etc.).

Cependant, en matière de cryptographie, **travailler avec des nombres réels n'est pas sécurisé ni pratique** pour plusieurs raisons :

- Les nombres réels impliquent une précision infinie, ce qui est impossible à gérer en informatique.
- Les algorithmes de chiffrement nécessitent des opérations discrètes pour éviter les attaques basées sur des approximations ou des erreurs de calcul.

Ainsi, bien que la définition mathématique des courbes elliptiques soit souvent donnée dans le contexte des nombres réels, **ce n'est pas un cadre approprié pour les applications cryptographiques**.

2. Courbes elliptiques sur un corps fini $\mathbf{F_p}$

En cryptographie, pour rendre les courbes elliptiques utilisables et sécurisées, on les utilise sur un **corps fini,** souvent noté $\mathbf{F_p}$ (F pour Field = champ fini en anglais) et où p est un nombre premier. Travailler sur un corps fini signifie que toutes les opérations (addition, multiplication, etc.) se font avec des entiers **modulo p**.

Par exemple, l'équation de la courbe elliptique devient :

$$y^2 \equiv x^3 + ax + b \pmod p$$

Ce passage des nombres réels à un corps fini présente plusieurs avantages :

1. **Sécurité** : Les courbes elliptiques sur les corps finis offrent une grande difficulté à résoudre certains problèmes mathématiques sous-jacents (comme le problème du logarithme discret elliptique), ce qui les rend particulièrement adaptées pour la cryptographie. Les solutions aux problèmes cryptographiques dans un corps fini sont beaucoup plus difficiles à calculer que dans $\mathbb{R}$ surtout avec des nombres très grands.
2. **Calculs discrets** : Dans un corps fini, tous les calculs sont discrets et bornés. Cela permet d'éviter les problèmes d'approximation liés aux nombres réels et d'utiliser des algorithmes efficaces pour les opérations de chiffrement et de déchiffrement.
3. **Efficacité** : Les opérations sur les corps finis peuvent être implémentées efficacement sur des ordinateurs, car elles se réduisent à des opérations arithmétiques simples (addition, multiplication) modulo un nombre premier p. Cela est particulièrement important dans les systèmes cryptographiques modernes, où la vitesse et la précision des calculs sont critiques.

3. Exemple concret d'utilisation d'un corps fini

Si on utilise la courbe elliptique définie par l'équation :

$$y^2 = x^3 + ax + b$$

et que l'on choisit de travailler sur le corps fini $\mathbb{F}_p$, cela signifie que l'on va "restreindre" les valeurs possibles de x et y aux nombres entiers compris entre 0 et $p-1$, en appliquant des opérations modulo p. Par exemple, si $p=17$, alors x et y seront des entiers entre 0 et 16, et toutes les additions, multiplications et divisions seront effectuées modulo 17. Cet exemple sera traité en détail dans l'annexe 2.

Pourquoi cette distinction est-elle importante ?

- **Contexte mathématique général** : Les courbes elliptiques définies sur les nombres réels servent surtout à étudier les propriétés générales des courbes et à comprendre leur structure géométrique. C'est un contexte important pour la recherche théorique en mathématiques.
- **Contexte cryptographique** : En cryptographie, on travaille sur des **corps finis** pour garantir que les opérations soient discrètes, efficaces et sécurisées. Les courbes sur les corps finis sont celles qui résistent aux attaques cryptographiques.

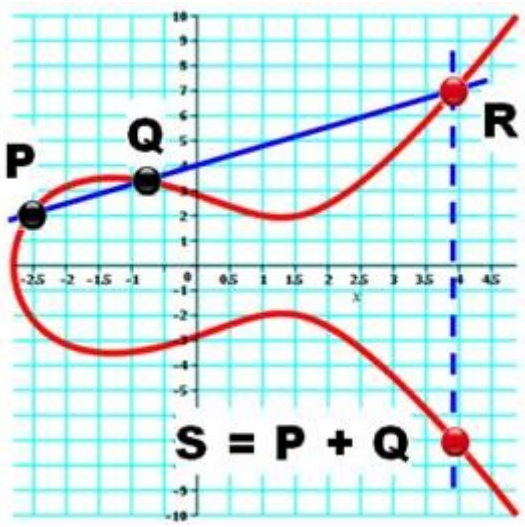
ANNEXE 2

LES OPÉRATIONS D'ADDITION ET DE MULTIPLICATION DE POINTS SUR UNE COURBE ELLIPTIQUE

Nous allons d'abord travailler sur les nombres réels. Nous avons vu que sur une courbe elliptique, on peut additionner deux points ou multiplier un point par un nombre entier. Commençons par l'addition de deux points :

1. Addition de deux points :

Voici un graphe pour visualiser :



Pour additionner deux points P + Q, on considère le point R qui est le point d'intersection de la droite passant par P et Q avec la courbe elliptique. Puis on prend le symétrique de R par rapport à l'axe des x, ce qui détermine le point S. On démontre que S = P +Q.

Nous allons expliquer dans ce paragraphe **l'aspect mathématique théorique** (voir annexe 1)**.** Puis, dans le paragraphe 2, qui présente la multiplication d'un point par un nombre, nous prendrons un exemple chiffré. Nous avons donc comme données :

- une courbe elliptique $y^2 = x^3 + ax + b$

- une droite $y = kx + m$ qui coupe la courbe en 3 points, P, Q et R

Les nombres a, b, k et m sont connus. On a défini les coordonnées de P et Q, et nous cherchons celles du point R et du point S.

On pose P = (x_1, y_1) , Q = (x_2, y_2) , R = (x_3, y_3) et S = (x_4, y_4)

et la pente de la droite est $k = \frac{y2-y1}{x2-x1}$

Le point R (x_3, y_3) étant à une intersection de la courbe et de la droite, on commence par déterminer la valeur de x_3 à partir des coordonnées connues des points P et Q qui se trouvent sur la courbe et sur la droite. Après un calcul assez long, on obtient :

$$\mathbf{x_3 = k^2 - x_1 - x_2}$$

Nous avons donc déterminé la valeur de x_3 à partir des données connues k, x_1 et x_2

Puis on calcule la valeur de y_3 :

La pente k de la droite peut s'écrire également $k = \frac{y3-y1}{x3-x1}$

On a donc $k (x_3 - x_1) = y_3 - y_1$

Soit $\mathbf{y_3 = k (x_3 - x_1) + y_1}$

Pour terminer, nous obtenons donc les coordonnées du point S = P + Q, sachant que par définition le point S (x_4, y_4) est le symétrique de R par rapport à l'axe des abscisses.

Nous avons donc $\mathbf{x_4 = x_3}$ et $\mathbf{y_4 = - y_3 = k (x_1 - x_3) - y_1}$

En conclusion, on peut écrire le résultat de l'addition :

$$\mathbf{P (x_1,y_1) + Q (x_2,y_2) = S(x_4,y_4)}$$

Nous verrons dans le paragraphe suivant un exemple concret avec des chiffres.

2. Multiplication d'un point P par un nombre entier

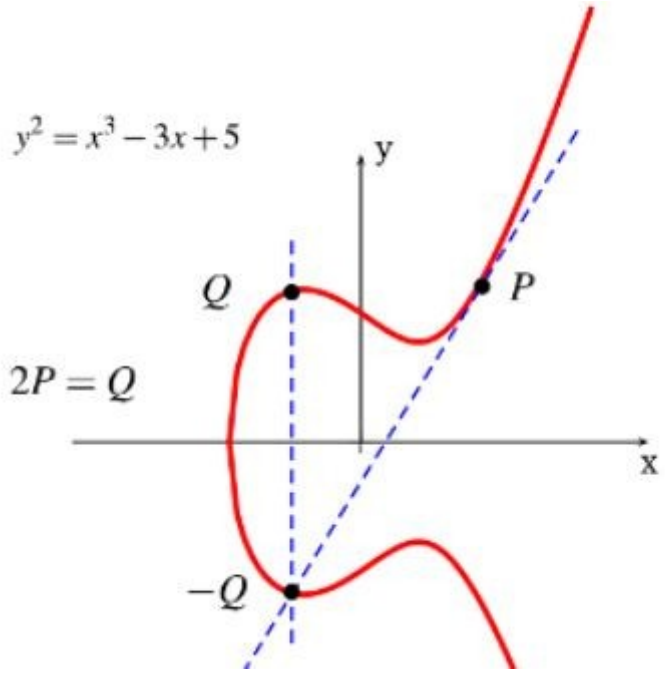
Nous allons maintenant voir **un exemple sur un corps fini** (voir annexe 1) avec des petits nombres.

Nous allons donc multiplier le point P par un nombre. Cette multiplication s'effectue selon le principe de l'addition : on additionne P + P = 2.P, puis 2P + P = 3.P, puis 3 P + P = 4.P etc.

Dans l'addition, on additionne deux points P et Q. Mais ici, on n'a qu'un seul point P. Comment faire ?

Pour ajouter P à lui-même , on trace la tangente à la courbe en P, et on considère que cette tangente touche deux fois la courbe au point P. On calcule les coordonnées de la troisième intersection, puis celles du point symétrique, comme dans l'addition. On obtient ainsi P + P = 2P.

Graphe :



Sur ce graphe, on a tracé la tangente en P à la courbe. Elle recoupe la courbe en un point – Q. Le symétrique de ce point – Q par rapport à l'axe des abscisses est le point Q. On a donc Q = 2.P.

L'équation de la courbe dans l'exemple chiffré n'est pas celle du graphe. Le graphe est simplement là pour visualiser les calculs.

Exemple chiffré en travaillant sur un corps fini:

Les données sont :

- une courbe elliptique $\mathbf{y^2 = x^3 + 2x + 2 \bmod 17}$, donc **a = 2 et b = 2**
- un point générateur **P = (5,1)**
- on effectue les calculs modulo p, avec p nombre premier, et on choisit **p = 17**

2.1 Doublement du point P :

On commence par doubler P (5,1). Comme dans le cas de l'addition, il faut déterminer le pente de la droite. La pente k de la tangente en P est donnée par :

$$k = \frac{3x2+a}{2y1} \quad \text{modulo p}$$

Il faut lire $(3 x_1^2 + a) / (2y_1)$, où x_1 et y_1 sont les coordonnées du point P (5,1)

On effectue le calcul : $k = (3*5^2 + 2) / (2*1) \bmod 17 = \frac{77}{2} \bmod 17$

Ici il faut calculer l'inverse modulaire de 2 mod 17, et on trouve 9.

Si l'on est peu familier avec la notion d'inverse modulaire, voir la fiche sur le chiffrement RSA.
Par ailleurs, le site dcode.fr permet de calculer l'inverse modulaire rapidement sur des grands nombres : https://www.dcode.fr/inverse-modulaire

On a donc k = 77*9 mod 17 = 693 mod 17 = 13

La pente de la tangente est **k = 13 mod 17**

On calcule ensuite les coordonnées du nouveau point avec les mêmes formules que l'addition :

$x_2 = k^2 - 2x_1 \bmod 17$, soit

$x_2 = 13^2 - 2*5 \bmod 17 = (169 - 10) \bmod 17 = 159 \bmod 17 = 6 \bmod 17$

x_2 = 6 mod 17

Puis on calcule y_2 toujours de la même façon que dans l'addition :

$y_2 = k(x_1 - x_2) - y_1 \pmod{17}$, soit

$y_2 = 13*(5-6) - 1 \pmod{17}$

$= -14 \pmod{17}$

y_2 = 3 mod p soit en définitive **Q = 2.P = (6, 3)**

2. 2 Suite de la multiplication : calcul de 3.P

On veut continuer le processus de multiplication, c'est-à-dire calculer 3P. Pour ce faire, on applique les règles de l'addition de deux points, c'est à dire dire que P + 2P = 3P. On va donc définir un point S tel que S = P + Q = P + 2P = 3P

On effectue donc l'addition des 2 points P (5,1) et Q (6,3)

La pente de la droite P, Q est donnée par

$$k = \frac{1-3}{5-6} \bmod 17, \text{ soit}$$

Or (1-3) = -2 et (5 -6) = -1 , soit $\frac{-2}{-1} = 2 \bmod 17$

$k = 2 \bmod 17$

À partir de k, on calcule $x_3 = k^2 - x_1 - x_2 \bmod 17$

x_3 = (2^2 -5 -6) mod 17 = (- 7) mod 17 = **10 mod 17**

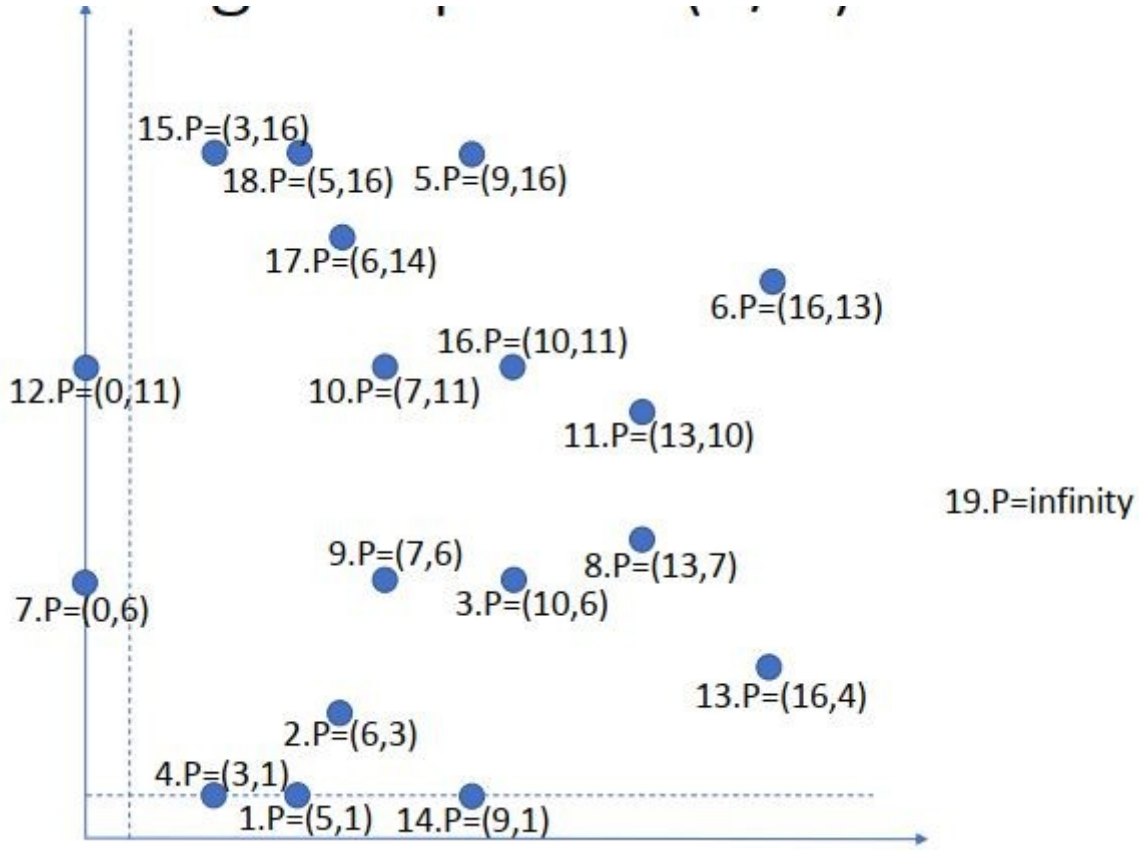
Puis on calcule $y_3 = k(x_1 - x_3) - y_1$ (mod 17)

y_3 = 2(5-10) – 1 mod 10 soit (-11) mod 17 = **6 mod 17**

Au final on a S = 3.P = (10,6)

On a vu dans le corps principal de la fiche que d'une façon générale, on avait S = dP. Dans la réalité, le chiffre d est très grand et la difficulté pour casser ce chiffre réside donc dans la difficulté de calculer d en connaissant P et S. De plus, il y a deux nombres d, celui d'Alice et celui de Bob.

Le tableau suivant permet de visualiser la position des points 4.P, 5.P, 6.P , etc. jusqu'à 18.P à partir de P (5,1), 2.P (6,3) et 3.P (10,6) :



Ce tableau est tiré du cours du professeur Alexandre Guitton, qui est téléchargeable librement sur Internet :

https://perso.isima.fr/~alguitto/index.html (voir support de cours, courbes elliptiques V2).

Le point 19.P = l'infini correspond à une droite verticale, parallèle à l'axe des y et qui coupe donc la courbe en 2 points. Le 3ème point est renvoyé à l'infini. Ce cas particulier n' a pas été traité pour ne pas alourdir la fiche.

On pourra également si on le souhaite effectuer des calculs sur le site :

https://andrea.corbellini.name/ecc/interactive/modk-add.html

Ce site permet d'effectuer des additions et des multiplications de points sur l'ensemble R des nombres réels ou sur un champ fini F_p en choisissant la courbe elliptique, le nombre premier p et les coordonnées du point P. Bien qu'en anglais, son utilisation est très simple et les graphiques qui s'affichent instantanément permettent de bien comprendre et de voir la différence entre un calcul avec les nombres réels et un calcul avec un corps fini.

3. Conclusion :

Dans les chiffrements par courbes elliptiques, il faut bien voir que dans la réalité, la clé privée d_A d'Alice et la clé privée d_B de Bob sont des nombres entiers qui ont généralement une taille d'environ 256 bits.

Comme on l'a vu au début de la fiche et dans cette annexe, le principe de chiffrement repose sur le fait qu'après l'échange de leurs clés d_A et d_B, Alice et Bob ont pu calculer une clé commune :

$$K = d_A * d_B * P$$

K est donc un point sur la courbe elliptique représenté par ses coordonnées x_K et y_K. Chacune de ces coordonnées est un entier de 256 bits. Le total des deux coordonnées représente donc 512 bits.

En pratique, souvent, seules les coordonnées x_K ou des dérivés de x_K sont utilisées afin de produire une clé symétrique plus petite. Par exemple, Alice et Bob peuvent utiliser une clé de chiffrement AES de 256 bits en utilisant x_K comme clé initiale pour dériver des clés, puisque AES utilise des clés dérivées à partir de la clé initiale (voir fiche sur le chiffrement AES).

Pour se faire une idée de la taille de ces clés, rappelons qu'un nombre de 256 bits en binaire représente un nombre entier d'environ 77 chiffres en décimal et de 64 chiffres en hexadécimal.

*****
***
*

LE CHIFFREMENT HYBRIDE :

1. Le chiffrement hybride :

Le chiffrement hybride consiste à associer deux types de chiffrement : un chiffrement symétrique (type AES) et un chiffrement asymétrique (type RSA). Rappelons la nature de ces deux types de chiffrement ;

- **Le chiffrement symétrique** : Une seule et même clé sert à chiffrer et à déchiffrer les données (exemple : AES). Ce mode de chiffrement est très rapide et efficace pour chiffrer de grandes quantités de données, mais pose un problème de distribution sécurisée de la clé.

- **Le chiffrement asymétrique** : Il utilise une paire de clés, une publique pour chiffrer et une privée pour déchiffrer (exemple : RSA). Il résout le problème de distribution des clés, mais il est beaucoup plus lent, surtout pour chiffrer des volumes importants de données.

Le chiffrement RSA a été abordé dans la fiche n° 7 d'initiation à la cryptographie et le chiffrement AES dans l'une des fiches sur la cryptographie moderne.

2. Principe de fonctionnement du chiffrement hybride

Le chiffrement hybride combine ces deux méthodes pour tirer parti de leurs forces tout en minimisant leurs inconvénients. Le principe général de fonctionnement est le suivant :

- **Génération d'une clé de session symétrique** :

Le chiffreur génère une clé symétrique aléatoire (appelée **clé de session**), souvent à l'aide d'un algorithme. Cette clé est temporaire et utilisée uniquement pour une session spécifique.

- **Chiffrement des données avec la clé symétrique** :

La clé symétrique est utilisée pour chiffrer les données du message clair avec un algorithme de chiffrement symétrique rapide et efficace.

- **Chiffrement de la clé symétrique avec un algorithme asymétrique** :

La clé symétrique est ensuite chiffrée à l'aide d'un algorithme asymétrique (comme RSA) et de la clé publique du destinataire. Cette étape garantit que seule la personne possédant la clé privée correspondante peut déchiffrer la clé symétrique.

- **Transmission** :

Les données chiffrées du message et la clé symétrique chiffrée sont envoyées au destinataire.

- **Déchiffrement** :

Le destinataire déchiffre d'abord la clé symétrique avec sa clé privée de chiffrement asymétrique.

Il utilise ensuite cette clé symétrique pour déchiffrer le message.

3. Illustration pratique du chiffrement hybride avec Alice et Bob :

- Bob veut adresser un message à Alice

- Alice dispose d'une clé pour le chiffrement en RSA. Elle a donc diffusé publiquement N et son exposant public e. Bien entendu, elle garde toujours secret son exposant privé d.

Opérations à effectuer par Bob :

- Créer le message en clair.

- Créer une clé symétrique, appelée « clé de session ». Cette clé est généralement plus courte que le message clair.

- Chiffrer le message clair avec cette clé symétrique, par exemple avec un chiffrement AES.

- Chiffrer ensuite la clé symétrique par un chiffrement RSA avec la clé publique N et e d'Alice.

- Adresser à Alice en un seul fichier le message chiffré avec la clé symétrique et cette clé symétrique chiffrée en RSA avec la clé publique.

Opérations à effectuer par Alice :

Lorsqu'elle reçoit ce fichier, Alice déchiffre la clé symétrique grâce à sa clé privée d, puis déchiffre le message original avec cette clé symétrique.

4. Les avantages du chiffrement hybride

- **Efficacité :** L'algorithme symétrique est utilisé pour chiffrer les données volumineuses de manière rapide, tandis que l'algorithme asymétrique est utilisé uniquement pour protéger la clé de session, ce qui minimise l'impact de sa lenteur.

- **Sécurité de la clé :** L'utilisation d'un chiffrement asymétrique garantit que la clé symétrique ne peut être déchiffrée que par le destinataire prévu, ce qui résout le problème de distribution de clé dans le chiffrement symétrique.

- **Confidentialité :** Même si quelqu'un intercepte les données, il ne peut pas les déchiffrer sans la clé de session, qui elle-même est protégée par le chiffrement asymétrique

5. Les limites de ce type chiffrement

Bien que très efficace, le chiffrement hybride n'est pas exempt d’incertitudes :

Gestion des clés : Si une clé privée est compromise, toutes les sessions passées et futures pourraient être déchiffrées.

Attaques : Les attaques sur les algorithmes RSA ou d'autres algorithmes asymétriques peuvent compromettre la sécurité globale du chiffrement hybride. Cependant, en utilisant des tailles de clés suffisamment grandes et des protocoles de chiffrement modernes (comme les courbes elliptiques), ces attaques sont atténuées.

Un chiffre hybride actuel utilise le plus souvent un algorithme symétrique de type AES avec une clé de session de 128 symboles binaires (bits) qui permet de chiffrer de longs messages de manière sûre, associé à un RSA qui utilise des clés de 1024 à 2048 bits.

6. Les applications courantes du chiffrement hybride

Le chiffrement hybride est la méthode de base dans de nombreuses applications de sécurité, telles que :

- **SSL/TLS** : Utilisé pour sécuriser les connexions Internet entre un navigateur et un serveur web (par exemple, HTTPS).

- **PGP (Pretty Good Privacy)** : Utilisé pour le chiffrement des e-mails.

- **Messagerie sécurisée** : Des applications comme Signal ou WhatsApp utilisent le mode hybride pour échanger des messages.

*****

***

*