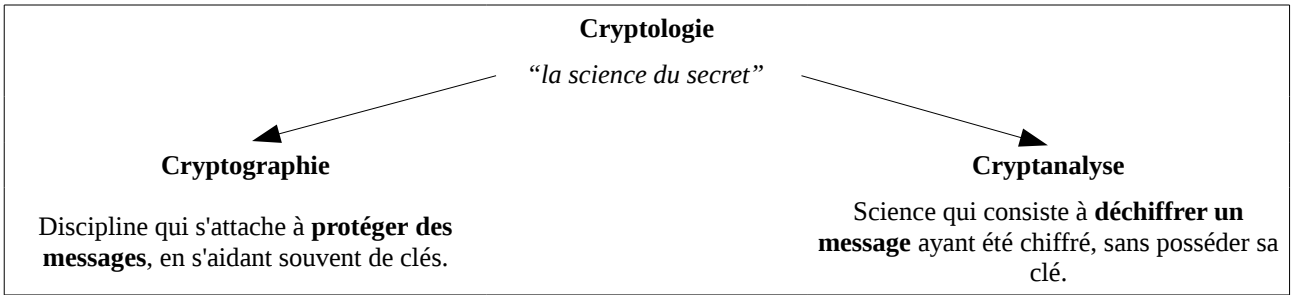
CRYPTOLOGIE

Taller de Talento Matemático

04 / 04 / 2014

INTRODUCTION

Dans le domaine militaire, commercial, judiciaire, criminel, et même privé, l'usage de messages codés existe depuis bien longtemps. En effet, le plus ancien document chiffré connu à ce jour remonte au XVIe siècle av. J.-C. : il s'agit d'une tablette en argile sur laquelle un potier avait gravé sa recette secrète de poterie en supprimant des consonnes et en modifiant l'orthographe des mots.
La cryptologie a très longtemps été considérée comme un art, et n'est devenue une science qu'au XXIe siècle ! Il s'agit d'une discipline qui fait appel à la logique, à la rigueur, à la méthode et... à l'imagination.



Un peu de vocabulaire...

- **Chiffrement :** transformation à l'aide d'une clé d'un message en clair – *texte clair* – en un message incompréhensible - *texte chiffré* - pour celui qui ne dispose pas de la clé de déchiffrement.
- **Cryptogramme :** message chiffré.
- **Décrypter :** retrouver le message clair correspondant à un message chiffré *sans posséder la clé de déchiffrement.*
- **Attaque :** processus par lequel on essaye de comprendre un message chiffré.
- **Clé :** c'est le "secret" du message !

Un peu d'histoire...

- **La technique grecque (Xe – VIIIe siècle av. J.-C.) :** technique de chiffrement par transposition qui utilisait un bâton et une lanière de cuir.
- **La technique des Hébreux (Ve siècle av. J.-C.) :** l'une des premières techniques de chiffrement, utilisée dans des textes religieux. La méthode la plus connue est la méthode Atbash, une méthode de *substitution alphabétique* inversée, qui consistait à remplacer chaque lettre du texte en clair par une autre lettre : A → Z, B → Y, etc.

- **Nabuchodonosor, roi de Babylone (-600) :** il écrivait sur le crâne rasé de ses esclaves, attendait que leurs cheveux repoussent, puis les envoyait à ses généraux. Il suffisait ainsi de raser à nouveau le messager pour pouvoir lire le message. *(Mais il ne s'agit pas réellement de cryptographie, car le message n'est pas chiffré mais seulement caché.)*
- **A partir de -200 :** apparaissent les premiers vrais systèmes de cryptographie (chiffre de César, carré de Polybe...).
- **Gabriele de Lavinde (1379) :** publication d'un recueil de codes et de clés, utilisé par la suite par les diplomates européens et américains pendant des siècles.
- **Blaise de Vigenère (1586) :** présentation d'une technique de chiffrement par substitution polyalphabétique. Son chiffrement ne sera décrypté qu'en... 1854 !
- **Première et Seconde Guerres Mondiales :** à partir de cette époque, l'essentiel des communications se firent par radio, c'est entre autres la raison pour laquelle cette guerre marque un tournant dans l'histoire et l'évolution de la cryptologie (cf machine Enigma).Par ailleurs, les exploits des alliés en matière de cryptologie auraient permis d'écourter la guerre (de un à deux ans, selon certains spécialistes). Churchill citait la cryptographie comme l'un des facteurs clefs de la victoire...
- **Cryptographie et informatique :** créée en 1919 mais utilisée pendant la seconde Guerre Mondiale, la machine Enigma (une machine à chiffrer et déchiffrer offrant un nombre de clés énorme) était un ancêtre de nos ordinateurs. Peu de temps après, un code utilisé par la haute hiérarchie allemande (le code Lorenz) intriguait les alliés qui souhaitaient le déchiffrer, et qui créèrent, pour cela, une nouvelle machine : Colossus. C'est ainsi que le premier ordinateur fut construit !

SUBSTITUTION SIMPLE ou MONOALPHABETIQUE

La substitution simple consiste à remplacer chaque lettre du texte clair par une lettre, un signe ou un nombre, identique du début à la fin du cryptage.

Le chiffre de César

Le chiffre de César est une méthode de chiffrement basée sur un décalage fixe des lettres du message dans l'alphabet. Elle consiste à remplacer chaque lettre par une autre, déphasée d'une quantité constante (en suivant l'ordre cyclique des lettres). La clé de chiffrement *n* - secrète - de cette méthode est un nombre compris entre 0 et 25 qui représente **la valeur du décalage**. Pour décrypter le message, on applique le même algorithme, mais à l'envers.

Applications

1. Avec la clé 3 (celle de Jules César), coder le mot **MATHEMATIQUES** et décrypter le mot **FHVDU**.
2. Décrypter le texte **UL ALUAL YPLU JVUAYL AVU LUULTP PS ZL CLUNLYH** sachant que le mot "ennemi" y figure.

Le carré de Polybe

Cette méthode consiste à remplacer chaque lettre par ses coordonnées dans un carré 5 x 5. *Cette technique fut utilisée pour transmettre des messages à distance, en utilisant des lampes : celles de droites indiquaient la première coordonnée et celles de gauche indiquaient la seconde.*

Le principe de base est simple, mais il se complique lorsque l'on utilise une clé : un mot qui s'écrit au début du carré. Les cases suivantes sont remplies par ordre alphabétique.

Application

Construire le carré de Polybe avec la clé MATES (enlever la lettre K), et déchiffrer ce message : **14 34 31 41 11 21 44 14 14 15 45 35 12 35 32 11 12 34 44 12 22 32 41 35 12 34**.

Le code des républicains

Cette technique fut utilisée pendant la guerre civile d'Espagne. Le principe est le même que celui du carré de Polybe, mais le tableau est constitué de 10 colonnes et 3 lignes (seules les 8 premières cases de la première ligne sont remplies).

Application

Avec la clé TALENT, décoder le message suivant : **20 17 7 6 6 7 29 7 20 0 3 7 4 13 28 20 17 20 17 8 10 9 28 0 12 9 20 0 17 20 9 12 13 17 6 0**.

Cryptage affine

Un cryptage affine consiste à chiffrer chaque lettre de l'alphabet, puis à remplacer le nombre initial x par le nombre y qui est le reste de la division euclidienne de $ax+b$ par 26, a et b étant des entiers naturels.

La clé de chiffrement – secrète – d'un tel cryptage correspond aux **valeurs des nombres *a* et *b***.

Application :

Avec la clé $(a,b)=(3,7)$, remplir le tableau suivant puis décoder le message **O TGGTPG U TJM AHJ NGFRT**.

En clair	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**
Rang x	0	1	2	3	4	5	6	7	8	9	10	11	12
$ax+b$		10			19					34			
Rang y		10			19					8			
En chiffré		K			T					I			
En clair	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
Rang x	13	14	15	16	17	18	19	20	21	22	23	24	25
$ax+b$			52								76		
Rang y			0								24		
En chiffré			A								Y		

Cryptage par substitution monoalphabétique aléatoire

On peut aussi coder un texte en substituant les lettres de façon aléatoire. Dans ce cas, les possibilités de chiffrement sont très grandes mais il n'existe pas de clé : pour déchiffrer le message, il est nécessaire d'avoir toutes les correspondances entre les lettres. Pour faciliter le décryptage par le destinataire du message, on peut définir une clé représentée par un mot de passe, dont les lettres correspondront aux premiers caractères de l'alphabet, puis terminer le codage par ordre alphabétique.

Casser un code

Le déchiffrement d'un texte chiffré par substitution simple n'est pas impossible, à condition que le texte soit assez long. Les statistiques révèlent que, dans un texte rédigé en français, les lettres les plus fréquentes sont les suivantes :

Lettre	E	S	A	N	T	I
Fréquence	17,76 %	8,23 %	7,68 %	7,61 %	7,30 %	7,23 %

On peut aussi repérer les lettres doublées, qui se répartissent ainsi (sur 10 000 bigrammes) :

ss	ee	ll	tt	nn	mm	rr	pp	ff	cc	aa	uu	ii	gg
73	66	66	29	24	20	17	16	10	8	3	3	2	1

- Une consonne doublée est toujours précédée d'une voyelle. Elle est suivie soit d'une voyelle, soit de l'une des lettres R ou L (attroupement, application).
- La voyelle E est pratiquement la seule qui se redouble fréquemment. Elle est alors souvent suivie de S (féminin pluriel).

LE CHIFFRE ADFGVX

Histoire

Utilisé par les allemands lors de la 1ère Guerre Mondiale et déchiffré par un cryptologue français (Georges Painvin). Ce dernier permit d'arrêter les allemands à l'entrée de Paris et marqua ainsi un tournant dans cette guerre.

Méthode

Cette méthode de chiffrement mélange la substitution et la **transposition** (mélanger l'ordre des lettres du message).

SUBSTITUTION : Elle est au départ basée sur un carré de Polybe 6 x 6, mais les intitulés des lignes/colonnes sont les lettres ADFGVX. Les lettres de l'alphabet sont alors écrites dans ce tableau, dans un ordre qui changeait chaque jour (d'où la difficulté du déchiffrement!), cet ordre est la 1ère clé du chiffre.

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

Comme dans le carré de Polybe, chaque lettre est alors codée par le couple de lettres qui constituent ses coordonnées.
Le message **RENFORT COMPIEGNE 16H10** devient donc après cette première étape :

TRANSPOSITION : On choisit ensuite, pour faire la transposition, une clé qui est un mot courant, par exemple DEMAIN. On écrit cette clé dans un tableau, et on recopie le texte intermédiaire dans le tableau comme ci-dessous. On numérote chaque colonne suivant l'ordre alphabétique des lettres de la clé :

D	E	M	A	I	N
2	3	5	1	4	6
D	F	A	X	V	V
F	A	F	D	D	F
G	F	D	D	F	D
F	G	V	A	G	D
A	X	G	G	V	V
A	X	X	A	V	F
D	V	X	A	D	X

Le message chiffré est obtenu en lisant d'abord la colonne numérotée 1, puis la colonne numérotée 2, etc. On obtient donc, après cette deuxième étape :

Déchiffrement

- On écrit le texte chiffré dans le tableau contenant la clé de transposition, en le remplissant non pas en lignes mais en colonnes.
- On recopie ce texte cette fois en le lisant en lignes, en regroupant les caractères par binômes.
- Enfin, on utilise ces binômes comme coordonnées pour retrouver la lettre de départ dans le tableau de substitution.

Voir http://www.bibmath.net/crypto/index.php?action=affiche&quoi=debvingt/adfgvx

SUBSTITUTION POLYALPHABETIQUE – la méthode de Vigenère

Malgré les faiblesses -connues- de la cryptographie par substitution simple, jusqu'au XVIe siècle, aucun véritable nouveau procédé cryptographique étant à la fois sûr et facile à utiliser n'a su remplacer la méthode du chiffre de César. Ce n'était pas sans compter sur un diplomate français, Blaise de Vigenère (1523-1598), qui fut l'initiateur d'une nouvelle méthode de chiffrement qui domina durant plus de 3 siècles...

Présentation

Vigenère était un personnage très hétéroclite : alchimiste, écrivain, historien... mais aussi diplomate, au service des ducs de Nevers et des rois de France. En 1586, il publia son *Traicté des chiffres ou Secrètes manières d'écrire*, texte dans lequel il explique son idée.

Le principe de sa méthode est en fait basé sur le chiffre de César, sauf que le décalage utilisé change de lettre en lettre. Afin de s'y retrouver, on utilise une table composée de plusieurs alphabets, tous écrits dans l'ordre, mais ayant chacun son rôle particulier.

Utilisation de la table (cf. annexe)

CRYPTAGE :

- Il est d'abord nécessaire de choisir **une clé** qui sera un mot, au choix du rédacteur.
- On écrit ensuite cette clé sous le message à coder, en la répétant autant de fois que nécessaire pour que, sous chaque lettre du message, on trouve une lettre de la clé.
- Pour coder une lettre, on cherche dans **(1)** la lettre du message clair, dans **(2)** la lettre de la clé lui correspondant, puis on détermine dans la table **(3)**, à leur intersection, la lettre chiffrée.

		Lettre en clair					
		A	**B**	**C**	**D**	**E**	**F**
Clé utilisée	**A**	A	B	C	D	E	F
	B	B	C	D	E	F	G
	C	C	D	E	F	G	H
	D	D	E	F	G	H	I
	E	E	F	G	H	I	J

Lettre chiffrée

(1) **(2)** **(3)**

DECRYPTAGE :

- Il suffit de chercher dans **(2)** la ligne correspondant à la lettre de la clé, puis de trouver la lettre codée dans cette ligne **(3)**. En remontant, on retrouve dans **(1)** la lettre décodée.

Exemple :

1. Cryptage du mot FANTASTIQUE avec la clé CAROLE :

Mot clair (1)	**F**	**A**	**N**	**T**	**A**	**S**	**T**	**I**	**Q**	**U**	**E**
Clé **(2)**	C	A	R	O	L	E	C	A	R	O	L
***Mot codé* (3)**											

2. Décryptage du mot avec la clé CAROLE :

***Mot codé* (3)**	***O***	***E***	***I***	***J***	***P***	***M***	***N***	***L***	***V***	***I***	***D***	***I***
Clé (2)												
Mot clair (1)												

Application

1. Avec la clé COLUCHE, coder le message suivant *(début d'une citation d'un humoriste français qui nous sert de clé...)* : DES IDEES, TOUT LE MONDE EN A
2. Avec la même clé, décoder le message suivant *(fin de la citation)* : QP KW PP HOFN E

Puissance de la méthode

Avec la méthode de Vigenère, chaque lettre peut être codée par de nombreuses lettres différentes au sein d'un même message n'utilisant pourtant qu'une seule clé ! Il s'agit d'un **système de substitution poly-alphabétique**. Il est donc impossible de décoder ce message par analyse fréquentielle, comme il était fait pour le chiffre de César. Cette technique s'avère ainsi considérablement plus solide que toutes celles qui existaient jusqu'alors !

De plus, il est très facile de convenir d'une clé avec son (ou ses) destinataire(s). On peut alors produire une infinité de clés, et ainsi, une infinité de cryptages.

Malgré son apparence au départ compliquée, le chiffre de Vigenère est très simple à utiliser, tant dans le codage que dans le décodage. D'où son succès...

Casser Vigenère

Le londonien Charles Babbage en 1854, et le prussien Friedrich Wilhelm Kasiski vers la même époque, réussirent à casser Vigenère. On peut remarquer que tous les lettres espacées de k (ou k est la longueur de la clé) sont décalées de la même constante. Il suffit donc de réaliser une analyse des fréquences pour chacun des sous-textes.
La difficulté est de trouver la longueur de la clé, sans celle-ci, impossible de décrypter.

Leur méthode consista à chercher des répétitions dans le texte chiffré (généralement, des répétitions de minimum 3 lettres). L'idée c'est qu'une même séquence de lettres du texte clair a été chiffrée avec la même partie de la clef et donc la meme séquence de lettres a été répétée dans le texte chiffré. En notant le nombre de lettres qui séparent les séquences redondantes, on peut obtenir un multiple de la longueur de la clé.

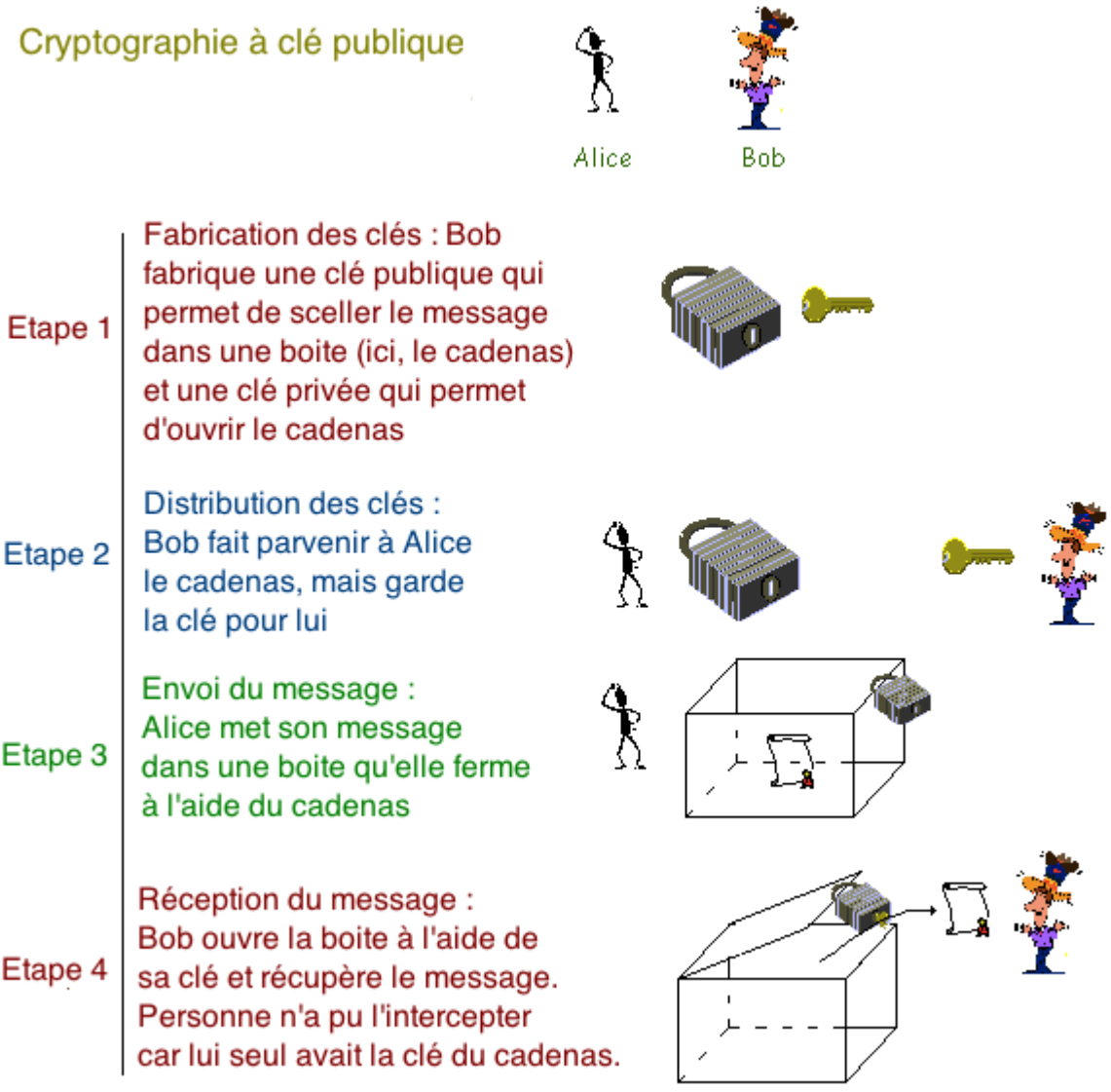
Par exemple, on repère un motif qui se répète séparé par 24 caractères et un autre motif séparé par 16 caractères. On recherche les diviseurs communs, la clé peut être de longueur 1, 2, 4 ou 8.

CHIFFRAGE A CLÉ PUBLIQUE

Pour commencer : chiffrage à clé secrète

Les méthodes vues précédemment sont des méthodes dites « symétriques » : l'algorithme de chiffrement et l'algorithme de déchiffrement sont inverses l'un de l'autre, et dépendent d'une unique clé (ou d'un unique couple de clé, comme pour le chiffre ADGFVX par exemple), connue par l'expéditeur et par le destinataire. Le principe de ces chiffrements est souvent simple, mais ils sont pourtant très sûrs **tant que le secret de la clé est bien gardé !!!** Là est le point faible de ces systèmes.

Principe du chiffrage à clé publique



Sécurité du système

Un chiffrage à clé publique est donc **asymétrique** : ce n'est pas la même fonction qui permet de chiffrer que de déchiffrer. Il faut donc trouver, pour un système à clé publique, deux fonctions P et S qui permettent de chiffrer / déchiffrer un message tout en assurant la sécurité de ce dernier, ce qui n'est pas si évident ! Le système le plus utilisé aujourd'hui est le chiffre RSA (1977) dont la sécurité est basée sur la difficulté de factoriser des nombres entiers.

Exemple : http://www.cryptage.org/rsa.html

Authentification des diffuseurs de clé publique

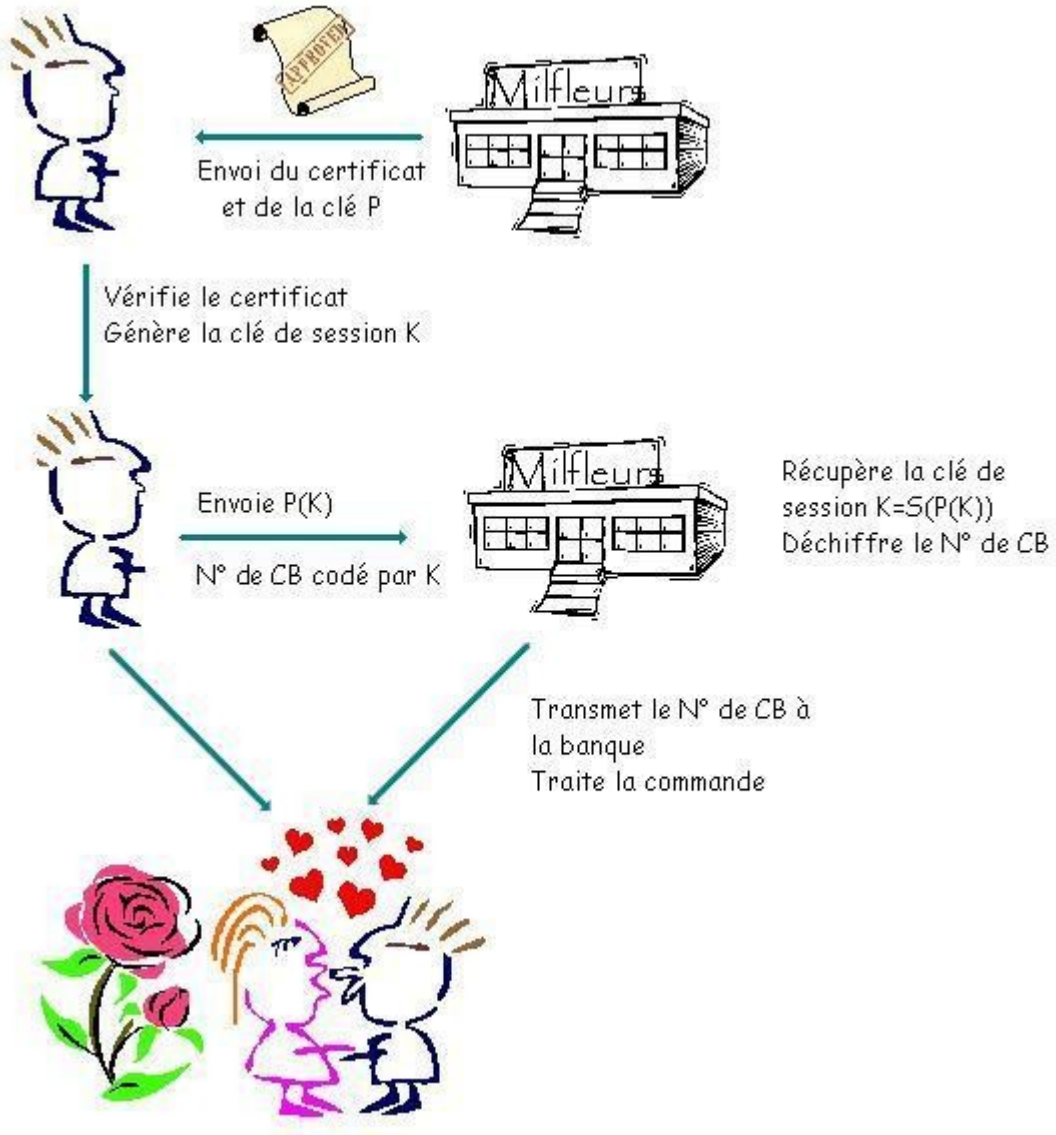
Avec ce système, on code un message en fonction de la clé que nous a transmis la personne à qui on souhaite écrire. Il faut donc être certain que cette clé est bien celle de la personne en question ! D'où l'existence de certificats d'authenticité.

ET AUJOURD'HUI ?

Depuis la Seconde Guerre Mondiale, les techniques cryptographiques ont explosé : en effet, les méthodes n'ont maintenant plus besoin d'être utilisables à la main entre deux tirs de baïonnette, mais sont utilisées et attaquées par des machines extrèmement puissantes (mais encore limitées... d'où la puissance du système RSA!!!).

La nature des besoins a elle aussi changé. Longtemps, la cryptographie était l'apanage des militaires ou des politiques (ou des amoureux). Désormais, l'**usage civil** (banque, commerce électronique, téléphonie mobile,…) est très nettement prédominant. Et si la cryptographie doit encore assurer la confidentialité des échanges, ce n'est plus son seul usage, on l'utilise surtout :

- pour authentifier des expéditeurs
- pour identifier des personnes
- pour assurer la validité des votes électroniques
- sécurité du commerce électronique



POUR ALLER PLUS LOIN... LA STEGANOGRAPHIE

Histoire

L'apparition de la stéganographie, l'art de cacher des informations, est très ancienne, et à peu près contemporaine de celle de la cryptographie. La première trace écrite se trouve dans les *Histoires* de Hérodote (biographie), parues vers 445 av J.-C, à travers deux récits. Le premier relate l'histoire d'Histiée, ancien tyran de Milet, et gendre d'Aristagoras, le nouveau tyran de Milet. Conseiller du roi Darius à la cour de Perse, il voulut organiser une révolte contre les Perses vers 500 av J-.C.. Pour transmettre son message à Aristagoras, il eut l'idée de raser la tête de son esclave le plus fidèle, de lui tatouer son message sur le crâne et d'attendre que les cheveux repoussent avant d'envoyer l'esclave pour Milet, avec pour consigne de se faire raser les cheveux. Bien sûr, il ne fallait pas être trop pressé pour transmettre le message!

Stéganographie et informatique

Avec l'avénement de l'informatique, et plus particulièrement avec la multiplication des transferts de fichiers sur les réseaux, la stéganographie est redevenue un sujet à la mode avec de nombreuses innovations. Quoi de plus facile, en effet, que de glisser quelques bits discrets au milieu d'un flot d'images, de textes et de programmes. Les moyens de cacher sont innombrables, des plus rudimentaires aux plus sophistiqués.

Table de Vigenère

		Lettre en 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**
Clé utilisée	**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

Lettre chiffrée