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, Marie était 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.

Des nobles écossais préparèrent un complot pour faire évader Marie 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 partirais. 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.

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