ATTIA Adam, CANAQUE Alan, GADY Antoine & HUYNH Christian Département Informatique G4S1

CRYPTOGRAPHIE

L'Eveil de l'Humanité

Au 3ème millénaire avant Jésus-Christ, on peut parler de cryptographie dès lors que l'Homme eut appris à lire et à écrire. En effet, un analphabète ne peut déchiffrer un message écrit, de même que la langue est une contrainte de cryptage.

Evolution de la cryptographie

Substitution mono-alphabétique

M	O	T
P	R	W

Cela consiste à **décaler** toutes les lettres d'un message par rapport à un même **nombre donné**. Ce fut le code utilisé par Jules César pour communiquer secrètement.

Ex : décaler toutes les lettres de 3 rangs.

Ainsi MOT devient PRW, cependant ce code est très peu sûr puisqu'il n'y a **que 25 combinaisons** possibles pour crypter un message.

	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

Substitution polyalphabétique

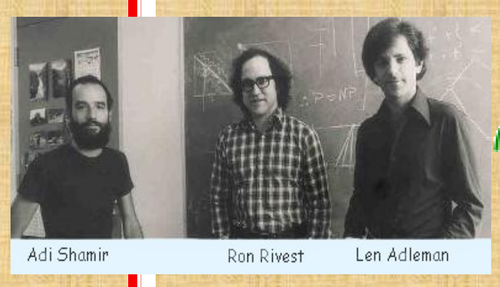
C	R	Y	P	T	A	G	E
M	O	T	M	O	T	M	O
O	F	A vous de trouver la suite					

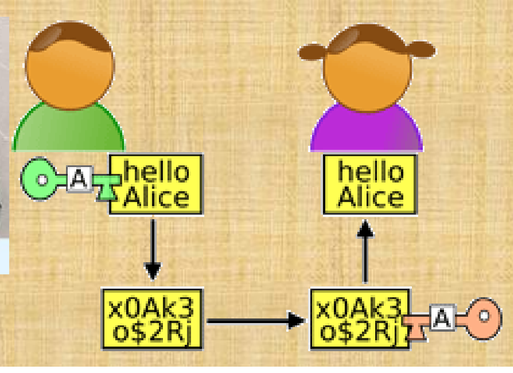
Cette méthode consiste à choisir un mot servant de clé et à crypter le message selon ce mot clé. Cette méthode a été établie bien longtemps après le chiffre de César, par Vigenère au 16ème siècle. Il fallu plus de **trois siècles** pour briser ce code.

Dans l'exemple ci-dessus, on cherche à crypter « cryptage » avec la clé « mot ».

NB : Il existe également une méthode de cryptage appelée cryptage par surchiffrement qui consiste à utiliser plusieurs méthodes de cryptage successivement

Asymétrique à clé publique + clé privée (RSA):





On utilise une **paire de clés**, une publique qui sert à crypter les messages et une autre privée qui sert à les décrypter.

Ex : Alice veut communiquer avec Bob. Celui-ci crypte le message avec la clé publique donnée par Alice qui possède une clé privée unique différente de la clé publique permettant de décrypter le message de Bob.

Alice peut signer le message qu'elle envoie à Bob via la clé privée, la clé publique que détient Bob permet en effet de vérifier la signature.

Applications/Importance de nos jours

Le protocole de sécurité **SSL** (Secure Sockets Layers) utilisés par les navigateurs repose sur un cryptage RSA

Les **cartes bancaires** utilisent la signature RSA pour authentifier la carte lorsqu'on l'introduit dans un terminal. En effet, lors de la création de la carte, les données du propriétaire ainsi que les clés publique et privée sont inscrites dans la puce.

Une **authentification en ligne** de la carte peut aussi être effectuée lorsque l'on veut retirer de plus grosses sommes par exemple, cela demande un temps assez long. Le terminal interroge alors un centre de contrôle à distance qui envoie un nombre aléatoire à la carte. Celle-ci renvoie une valeur calculée grâce à une clé secrète contenue dans une partie illisible de la puce ainsi qu'à un algorithme de cryptage (DES, AES). Si la valeur est reconnue par le centre, ce-dernier émet une autorisation d'opération à la carte.

La plupart des systèmes de sécurité de nos jours utilisent un cryptage à clés asymétriques dont RSA

Perspective d'avenir

Récemment, nous avons découvert que les **ordinateurs quantiques** pourraient mettre en **péril** tous nos systèmes de cryptographie actuels puisqu'ils sont incomparablement plus puissants que nos machines actuelles, le décryptage leur est facile.

C'est pour cela que l'on cherche à développer une **cryptographie quantique**.