CRYPTOGRAPHIE
ou comment coder et décoder un message secret

La cryptographie est l'ensemble des techniques qui permettent de chiffrer et de déchiffrer un message, dont le contenu ne doit être connu que de son expéditeur et de son destinataire.
Son déchiffrement par un tiers n'est pourtant pas impossible. Il nécessite la connaissance d'un certain nombre de données fondamentales.
Au cours des siècles, de nombreux systèmes cryptographiques ont été mis au point, de plus en plus perfectionnés, de plus en plus astucieux!
De grands chercheurs associés à la naissance de l'informatique étaient aussi des spécialistes de cryptographie : Charles Babbage (1894), Alan Turing (il s'est illustré pendant la seconde guerre mondiale, en décodant les messages que la marine allemande chiffrait avec la machine Enigma, dont un exemplaire a été envoyé en Angleterre par des résistants)

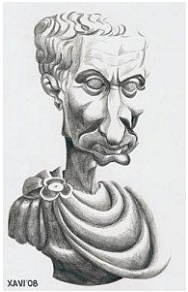
Les méthodes de codage sont nombreuses. Il existe deux grands types de cryptographie : la substitution et la transposition.
Nous allons nous concentrer sur quelques exemples de méthodes de substitution.

La substitution simple ou substitution monoalphabétique

La substitution monoalphabétique consiste à remplacer chaque lettre du texte clair par une lettre, un signe ou un nombre. La méthode la plus connue est le Chiffre de César.

1- Le Chiffre de César (ou chiffrement par décalage)

Le Chiffre de César est la méthode de cryptographie la plus ancienne communément admise par l'histoire. Il consiste en une substitution mono-alphabétique, où la substitution est définie par un décalage fixe dans l'alphabet.



On peut fabriquer une Roue pour déchiffrer les cryptographes.

On découpe d'abord deux cercles dans du bristol, un légèrement plus petit que l'autre. Avec un rapporteur, on divise chaque cercle en 26 sections de 13,8 degrés.
On écrit une lettre de l'alphabet dans chaque division de chaque roue.
On attache ensuite les deux roues en leur centre au moyen d'une attache parisienne de façon à ce que l'on puisse les faire tourner séparément. Désormais, si on veut transcrire un cryptographe où l'alphabet a glissé de 19 rangs, il suffit de mettre le A et le T en face l'un de l'autre et on peut traduire le message !(fig 1)

On peut aussi réaliser une figure avec Geogebra !!!

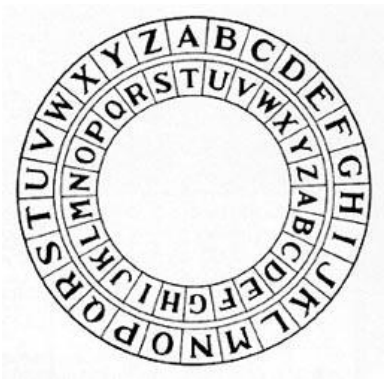


fig1

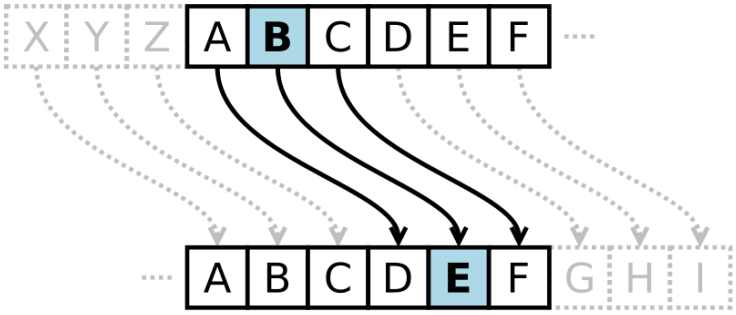


fig2

a)Par exemple, avec une clé de cryptage égale à 3(fig 2) le mot CHAMPION est codé par FKDPSLRQ

Avec la même clé de cryptage, crypter votre prénom et décrypter le mot WURXYH.

b)Décrypter le texte suivant sachant que la clé de codage est 10 : ebqoxd ovswsxob vk mslvo.

c)Sachant que le texte en clair suivant : rendez vous rue de la paix

donne : mziyzu qjpn mpz yz gv kvds déterminer la clé de cryptage.

d) Décrypter le texte suivant en supposant que le mot "ennemi" y figure :

stywj jssjrn ij ytzotzwx jxy ij wjytzw

e) Le mot AJMQAPA a été crypté mais on ignore la clé de cryptage. Saurez-vous la trouver et décrypter ce mot ?

f) Expliquer les faiblesses d'un tel système de chiffrement.

2- Le 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.

Les nombres a et b sont des entiers naturels qui forment la clé du cryptage.

Exemple avec la clé (a ; b) = (3 ; 7)

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									37		
Rang y		10									11		
En crypté		K									L		

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											76		
Rang y											24		
En crypté											Y		

a) Coder votre prénom avec la clé (3;7)

b) Décrypter la phrase RXF HPJJF avec la clé (3;7)

c)On prend maintenant pour clé (2;13) .Coder alors le mot ENTIER . Quel problème apparaît dans ce codage ?

Utilisation du tableur Excel **pour le cryptage affine**

But du TP : On souhaite crypter puis décrypter un message de façon automatique à l'aide du tableur EXCEL. On considère que le message ne comporte que les lettres de A à Z écrites en majuscules. De plus tous les espaces entre les mots ont été supprimés.

1 Préliminaire :

On commence par attribuer son rang x à chacune des lettres de l'alphabet. On appellera cette étape la **numérisation du message**.

En informatique, les caractères sont codés à l'aide du code ASCII, consistant à attribuer à chaque caractère un entier entre 0 et 255. Par exemple, le code ASCII de @ vaut 64, celui de A vaut 65, celui de B vaut 66 etc. Connaissant le code ASCII d'une lettre, il suffit donc de retirer 65 pour obtenir le numéro de celle-ci dans l'ordre alphabétique.

Questions de syntaxe : Dans EXCEL, la fonction qui donne le code ASCII d'un caractère est = CODE(). Dans ces conditions, la formule =CODE(caractère) - 65 renvoie un entier compris entre 0 et 25 représentant le numéro du caractère dans l'ordre alphabétique.

2 Cryptage du message

2.1 Numérisation du message

En utilisant le principe décrit ci-dessus, numériser le message suivant : BONJOURATOUS.

On écrira le message en ligne, avec une lettre par cellule. Le titre de la ligne sera Message en clair.

Ligne suivante, le titre sera Message numérisé.

2.2 Cryptage du message

On va crypter le message avec la clé (7;0) c'est-à-dire au moyen de la fonction C qui à tout entier x compris entre 0 et 25 associe le reste y de la division euclidienne de 7x par 26. On obtient ainsi un entier compris entre 0 et 25. Dans EXCEL, la fonction donnant le reste de la division euclidienne d'un nombre par 26 est =MOD(nombre ; 26).

Mettre pour titre de la ligne suivante : Message numérisé crypté, puis réaliser le cryptage.

Pour revenir à un message alphabétique, on utilise la fonction EXCEL =CAR(code ASCII) qui retourne le caractère associé à son code ASCII. Il suffira donc d'appliquer à chaque cellule de la ligne du Message numérisé crypté, la formule =CAR(code + 65).

Mettre pour titre de la ligne suivante : Message crypté, et réaliser l'association code- caractère.

2.3 Décryptage du message

Notons D la fonction qui à tout entier x compris entre 0 et 25 associe le reste de la division euclidienne de 15x par 26.

Commencer par numériser le message crypté obtenu précédemment, puis retrouver le message originel en utilisant la fonction D de décryptage.

2.4 Amélioration

Le codage proposé ci-dessus est rudimentaire, notamment parce que la lettre N est invariante. On modifie donc la fonction de cryptage C ainsi : C(x) = reste de la division euclidienne de 7x + 8 par 26. Comment faut-il alors modifier la fonction de décryptage D ?

Refaire le cryptage et le décryptage du message précédent en utilisant les nouvelles fonctions de cryptage et de décryptage.

3- Codage et statistiques : la méthode d'Al-kindi

Les possibilités de codage sont très nombreuses mais le déchiffrement d'un texte chiffré par une méthode de substitution monoalphabétique n'est pourtant pas impossible, **à condition que le texte soit assez long.**
Les savants arabes sont les inventeurs de la cryptanalyse. C'est une méthode permettant de décrypter les messages codés. Les lettres du texte à coder sont remplacées par d'autres lettres de la façon suivante :

1. deux lettres différentes sont codées de façons différentes.
2. la même lettre est toujours codée de la même façon.

Le premier traité exposant une procédure pour décrypter un texte codé de cette à été écrit par Al Kindi au neuvième siècle après J.C. Sa théorie repose sur le fait que dans un texte, les lettres ont des fréquences différentes. Par exemple, en français, la fréquence de la lettre E est, selon le texte, presque toujours supérieure aux fréquences des autres lettres. Selon sa théorie, il y a donc de fortes chances pour que, dans un texte codé, la lettre qui apparaît le plus fréquemment représente un E. Les lettres les moins fréquentes représentent probablement un W, un K ou un X...

Le tableau ci-dessous exprime, en pourcentage, les fréquences moyennes , des lettres utilisées dans les textes écrits en français.

A	B	C	D	E	F	G	H	I	J	K	L	M
7,68	0,8	3,32	3,6	17,76	1,06	1,1	0,64	7,23	0,19	0	5,89	2,72

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
7,61	5,34	3,24	1,34	6,81	8,23	7,3	6,05	1,27	0	0,54	0,21	0,07

Calculer, dans un autre tableau, les fréquences , de chaque lettre du message codé ci-dessous. En observant les correspondances entre les deux tableaux , décoder le message .

Message français à décoder

BKSMAMZCZMTFY KF OKATOCFZ ZHKY CYZIAMKIYKUKFZ AK UKYYCLK ATOK RTIY CRKP BHCFADM IF XCY OKAMYMB RKHY SC YTSIZMTF BMFCSK OCFY AKZZK CAZMRMZK UCZDKUCZMGIK CI SCX

Pour vous aider, vous pouvez utiliser le lien suivant qui permet de faire l'analyse fréquentielle d'un texte simple : http://www.cryptage.org/outil-crypto-frequences.html