CHAPITRE 1 : Cryptographie classique

1 Définitions

Crypto : est issu du grec kryptos qui signifie caché.

Chiffrement : Le chiffrement consiste à transformer une donnée (texte, message, ...) afin de la rendre incompréhensible par une personne autre que celui qui a créé le message et celui qui en est le destinataire. La fonction permettant de retrouver le texte clair à partir du texte chiffré porte le nom de déchiffrement.

Texte chiffré : Appelé également cryptogramme, le texte chiffré est le résultat de l'application d'un chiffrement à un texte clair.

Clef : Il s'agit du paramètre impliqué et autorisant des opérations de chiffrement et/ou déchiffrement. Dans le cas d'un algorithme symétrique, la clef est identique lors des deux opérations. Dans le cas d'algorithmes asymétriques, elle diffère pour les deux opérations.

Cryptographie : La cryptographie est l'étude des méthodes donnant la possibilité d'envoyer des données de manière confidentielle sur un support donné.

Cryptanalyse : Opposée à la cryptographie, elle a pour but de retrouver le texte clair à partir de textes chiffrés en déterminant les failles des algorithmes utilisés.

2. Le chiffrement de Jules Cesar

Le chiffre de Cesar est une substitution à alphabet régulier. Son principe est un décalage des lettres de l'alphabet, chaque lettre est décalée d'une position allant de 1 à 25. Le chiffre de Cesar est très simple à mettre en œuvre, on choisit le décalage et on l'applique sur chaque lettre ; si on dépasse Z on repasse à A.

Dans les formules ci-dessous, p est l'indice de la lettre de l'aphabet, k est le décalage.

a b c d e … m n p … x y z

0 1 2 3 4 12 13 14 23 24 25

La règle de correspondance est comme suit :

$$E_k(x) = (x + k) \bmod 26$$

La fonction inverse est :

$$D_k(y) = (y - k) \bmod 26$$

Exemple :

Supposons qu'Ali et Redha utilisent une clé k=10 avec le chiffre de Cesar. Quand Ali veut envoyer le message : iwanttomeetyou

Ali convertit le texte en chaine d'entiers :

8 22 0 13 19 19 14 12 4 4 19 24 14 20

Ensuite il rajoute 10 à chaque valeur modulo 26, il obtient :

18 6 10 23 3 3 24 22 14 14 3 8 24 4

Alors le message codé est le suivant :

SGKXDDYWOODIYE

Pour décrypter ce message Redha convertit le message en chaine d'entiers et soustrait 10 à chaque valeur. Ensuite, il convertit cette chaine d'entiers en caractères équivalents.

Remarque : il suffit de décoder une lettre pour déduire le reste.

3. Le chiffrement monoalphabétique à alphabet désordonné :

Le chiffrement de Cesar est particulièrement simple à décrypter. Du fait que l'identitfication d'un seul couple (lettre claire, lettre chiffrée) révèle la substitution. Cette méthode peut être vue comme une généralisation du chiffre de Cesar.
En plus de la correspondance entre les lettres et les chiffres, on utilisera une permutation $\Pi(x)=x'$ si et seulement si $\Pi^{-1}(x')=x$.
Soit la permutation suivante :

Π = 0 1 2 3 4 5 6 7 8
2 5 1 4 3 6 0 8 7

$E_\Pi(x) = \Pi(x)$
$D_\Pi(y) = \Pi^{-1}(y)$ où Π^{-1} est la permutation inverse de Π

Π^{-1} = 0 1 2 3 4 5 6 7 8
6 2 0 4 3 1 5 8 7

En pratique on peut éliminer les entiers, on utilisera directement la permutation des 26 caractères.

Exemple : Ali et Redha choisissent une permutation aléatoire comme suite :
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
C G H W Z Q T N M L S X V R Y E O F D J I K U P B A

iwanttomeetyou message en clair
MUCRJJYVZZJBYI message crypté
Il y a 26 ! permutations sur un alphabet de 26 caractères. Afin d'attaquer ce code, on utilise les propriétés statistiques de la langue (anglais dans notre exemple)

caractère	probabilité	caractère	probabilité	caractère	probabilité	caractère	probabilité
A	.0.082	G	0.020	M	0.024	S	0.063
B	0.015	H	0.061	N	0.067	T	0.091
C	0.028	I	0.070	O	0.075	U	0.028
D	0.043	J	0.002	P	0.019	V	0.010
E	0.127	K	0.008	Q	0.001	W	0.023
F	0.022	L	0.040	R	0.060	X	0.001
						Y	0.020
						Z	0.001

Sur la base de ces probabilités, on partitionneles 26 lettres en 5 groupes :
1 : E sa probablité est de 0.123
2 : T,A,O,I,N,S,H,R ont leur probabilité entre 0.09 et 0.06
3 : D,L ont une probabilité autour de 0.04
4 : C,U,M,W,F,G,Y,P,F,B ont une probabilité entre 0.028 et 0.015
5 : V,K,J,X,Q,Z ont une probabilité inférieure à 0.01
Il est aussi utile de considérer la fréquence de deux ou trois lettres consécutives (diagramme ou trigramme). Les 30 plus communs digrammes dans l'ordre décroissant sont :
TH, HE, IN, ER, AN, RE, ED, ON, ES, ST, EN, AT, TO, NT, HA, ND, OU, EA, NG, AS, OR, TI, IS, ET, IT, AR, TE, SE, HI, OF
Les 12 plus communs trigrammes dans l'odre décroissant sont:

THE, ING, AND, HER, ERE, ENT, THA, NTH, WAS, ETH, FOR, DTH
Analyser le texte chiffré, la letter qui apparait le plus est considérée comme le code de e. La lettre qui apparait moins fait partie du $2^{ème}$ groupe, on choisit la lettre en analysabt les digrammes pour décoder et ainsi de suite, on arrive à décoder le message.

4. Chiffrement par permutation de bloc :

$E_\Pi(x_1,x_2, \ldots,x_n)=(y_{\Pi(1)},y_{\Pi(2)}, \ldots,y_{\Pi(n)})$
$D_\Pi(y_1,y_2, \ldots,y_n)=(y_{\Pi^{-1}(1)},y_{\Pi^{-1}(2)}, \ldots,y_{\Pi^{-1}(n)})$

Exemple :
Supposons que Ali et redha choisissent des blocs de 6 –n=6) et utilisent la permutation suivante

$$\Pi = \begin{matrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 1 & 6 & 2 & 5 \end{matrix}$$

Ali veut envoyer le texte suivant
he walked up down the passage two or three times
Ali divise le texte en groups de 6
hewalk edupan ddownt hepass agetwo orthre etimes
ensuite realize la permutation de chaque groupe et obtient le message code suivant
WLEHKAUADENPONDDTWPSEHSAEWGAOTTRROEHIETESM
Quand Redha recoit le mesage codé, il le divise en blocs de 6 et pour chaque bloc, il applique la permutation inverse

$$\Pi^{-1} = \begin{matrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 2 & 1 & 6 & 4 \end{matrix}$$

Il obtiendra le message en clair

Remarque : on voit que le premier e est codé en L, le second e est codé en U et le troisième est codé en S. Dans ce cas, la probabilité n'est pas d'une grande utilité.

5. Chiffrement de Vigénère :

On le définit comme suit :
$K=(k_1,k_2,\ldots..k_m)$
$E_k=(x_1,x_2,\ldots,x_m)=(x_1+k_1,x_2+k_2,\ldots,x_m+k_m)$
$D_k=(y_1,y_2,\ldots,y_m)=(y_1-k_1,y_2-k_2,\ldots,y_m-k_m)$
Les opérations sont effectuées modulo 26
Ali et redha choisissent la valeur de m, ensuite ils choisissent une chaine de longueur m comme clé pour coder le message. Ali divise le texte en blocs de taille m, et code le bloc en utilisant la clé.
Exemple :
m=5 et la clé secrète est ONWAR, supposons que le texte est le suivant
the art of war teaches us to rely
on obtiendra le message chiffré suivant
HUAAIHBBWRFGAATVROUJHBNECM

6. Chiffrement de Hill :

On utilise une matrice inversible.
$E_K(x) =x.K$ K matrice mxm

$D_K(y) =y.K^{-1}$

La correction de ce chiffrement est facile à vérifier

$y.K^{-1} = x.K.\ K^{-1} = x.I = x$

Exemple :

Ali et redha choisissent m=2 et utilise la clé

$$K = \begin{matrix} 11 & 8 \\ 3 & 7 \end{matrix}$$

Quand Ali veut envoyer le message letusfly à Redha, le message en clair est mis comme suite :

(11,4), (19,20),(18,5),(11,24)

Ensuite, il calcule le message codé comme suite

(11.4) K =(3.12)
(19.20)K=(9.6)
(18.5)K=(5.23)
(11.24)K=(11.22)

Alors le message codé sera DMJGFXLW

Redha peut trouver à partir de K que

$$K^{-1} = \begin{matrix} 7 & 18 \\ 23 & 11 \end{matrix}$$

Il peut décoder le message chiffré.