Solution Fiche TD N° 01

Questions de cours

1. L'objectif du chiffrement c'est de rendre le message illisible, par contre l'objectif de la stéganographie c'est de dissumuler un message secret dans un message anodin.

2. Dansla stéganographie classique,on traite des données textuelles,par contre dans la stéganographie moderne,on traite d'autres types de données (son, viédo, etc)

3. Non, il n'est pas nécessaire de cacher l'algorithme de chiffrement car la confidentialité d'un système de chiffrement est difficile à garantir, il est en général mis à la disposition de tous les utilisateurs dont il est souvent diffusé dans les logiciels ou des dispositifs matériels. A partir de ce principe on constate que la sécurité d'un système de chiffrement repose uniquement sur la protection de la clé.

4. Si on cherche, on trouvera du texte paraissant aléatoire, donc aucun moyen de savoir si on a trouvé quelque chose.

Exercice N°1

1. Chiffrement du message "MESSAGE" avec la clé "C"

Lettre en clair	M	E	S	S	A	G	E
Rang de L_i	12	4	18	18	0	6	4
k	2	14	18	10	2	2	8
Rang de C_i	14	18	10	2	2	8	12
lettre chiffré	O	S	K	C	C	I	M

   Le cryptogramme obtenu est **C="OSKCCIM"**

2. Déchiffrement du cryptogramme "PNAAMUKEI" avec la clé "M"

   Les fonctions de déchiffrement du cryptosystème de césar récursif sont:

   $l_1 = C_1 - k$
   $l_i = C_i - C_{i-1}$ pour i>= 2

Lettre chiffrée	P	N	A	A	M	U	K	E	i
Rang de C_i	15	13	0	0	12	20	10	4	8
k	12	15	13	0	0	12	20	10	4
Rang de C_i	3	24	13	0	12	8	16	20	4
lettre chiffré	D	Y	N	A	M	I	Q	U	E

   Le message en claire **M= "DYNAMIQUE"**

3. L'ensemble des clés possibles est celui des 26 lettres de l'alphabet, donc de taille insuffisante pour assurer la moindre sécurité. De plus, on peut décrypter toutes les lettres d'un message crypté, sauf la première sans connaître la clé, juste en faisant la soustraction avec la lettre précédente.

Exercice N°2

1. Chiffrement du message "BONE" pour (a,b)=(2,5)

Lettre en clair	B	O	N	E
Rang de L_i	1	14	13	4
k= (2,5)	12	15	13	0
$(a * L_i + b) \bmod 26$	7	7	5	13
lettre chiffré	H	H	F	N

Conclusion: La substitution n'est pas unique (plusieurs lettres correspondent à une même autre - voir la table de décodage). Ceci est dû au fait que le coefficient a n'est pas premier avec 26;

2. Deux équations permettront de trouver la clé (a,b)

$F(R) = F(17) = 9 \equiv J \Rightarrow (17 * a + b) mod 26 = 9$
$F(A) = F(0) = 20 \equiv U \Rightarrow (0 * a + b) mod 26 = 20$

Exercice N°3

1. Chiffrement vigenère avec la clé k= "SECRET"

Lettre en clair	E	N	C	O	R	E	P	L	U	S	E	T	O	N	N	A	N	T	C	E	L	A
Rang de L_i	4	13	2	14	17	4	15	11	20	18	4	19	14	13	13	0	13	19	2	4	11	0
k	S	E	C	R	E	T	E	N	C	O	R	E	P	L	U	S	E	T	O	N	N	A
$Rang_k$	18	4	2	17	4	19	4	13	2	14	17	4	15	11	20	18	4	19	14	13	13	0
$(L_i + K_i) \bmod 26$	22	17	4	5	21	23	19	24	22	6	21	23	3	24	7	18	17	12	16	17	24	0
lettre chiffré	W	R	E	F	V	X	T	Y	W	G	V	X	D	Y	H	S	R	M	Q	R	Y	A

le crtptogramme c="**WREFVXTYWGVXDYHSRMQRYA**"

Exercice N°4

1. Grille de chiffrement Playfair correspondante à "WORSHIP"

W	O	R	S	H
I/J	P	A	B	C
D	E	F	G	K
L	M	N	Q	T
U	V	X	Y	Z

2. Chiffrement du messaga M="you can do it just try"

Bloc en clair	YO	UC	AN	DO	IT	JU	ST	TR	YX
Bloc chiffré	VS	ZI/ZJ	FX	EW	CL	DW	HQ	NH	ZY

Le crytogramme C="**VSZIFXEWCLDWHQNHZY**"

3. Grille de chiffrement Playfair corréspondante à la clé "COVID"

C	O	V	I	D
A	B	E	F	G
H	J	K	L	M
N	P	Q	R	S
T	U	X	Y	Z

4. Chiffrement du message M="Pandemie"

Bloc en clair	PA	ND	EM	IE
Bloc chiffré	NB	SC	GK	VF

Le crytogramme C="**NBSCGKVF**"

Exercice N°5

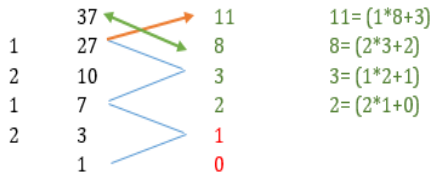
1. Peut-on apliquer le chiffrement de Hill avec la clé k= $\begin{pmatrix} 7 & 10 \\ 3 & 6 \end{pmatrix}$

   $det(k) = 7 * 6 - 3 * 10 = 12$

   PGCD (det(k), 26) $\neq 1$ d'ou nous pouvons pas appliquer le chiffrement de Hill avec la clé $k = \begin{pmatrix} 7 & 10 \\ 3 & 6 \end{pmatrix}$

2. Résolution de l'éuqation diophantienne $37x - 27y = 1$ Nous avons l'éqaution diophantienne

$$37x - 27y = 1 \tag{1}$$



   En utilisant la division éuclidienne nous obtenons

$$27 * 11 - 37 * 8 = 1 \tag{2}$$

   d'ou $\begin{cases} x = & -8 \\ y = & -11 \end{cases}$ ..

3. Chiffrement du message en clair M="EXAM"
   det(k)= (9*8-5*7)=37 mod 26= 11
   PGCD(det(k),26) =PGCD(37,26)=1 d'ou la matrice K est une matrice valide.

$$\begin{pmatrix} C_E \\ C_X \end{pmatrix} = \begin{pmatrix} 9 & 5 \\ 7 & 8 \end{pmatrix} * \begin{pmatrix} 4 \\ 23 \end{pmatrix} \bmod 26 = \begin{pmatrix} 21 \\ 4 \end{pmatrix} \equiv \begin{pmatrix} V \\ E \end{pmatrix}$$

$$\begin{pmatrix} C_A \\ C_M \end{pmatrix} = \begin{pmatrix} 9 & 5 \\ 7 & 8 \end{pmatrix} * \begin{pmatrix} 0 \\ 12 \end{pmatrix} \bmod 26 = \begin{pmatrix} 8 \\ 18 \end{pmatrix} \equiv \begin{pmatrix} I \\ S \end{pmatrix}$$

   Le cryptogramme C= "**VEIS**"

4. Déchiffrement du cryptogramme C="KWVB"

$\begin{pmatrix} L_K \\ L_W \end{pmatrix} = \begin{pmatrix} 9 & 5 \\ 7 & 8 \end{pmatrix}^{-1} * \begin{pmatrix} 10 \\ 22 \end{pmatrix} \bmod 26$

$\begin{pmatrix} 9 & 5 \\ 7 & 8 \end{pmatrix}^{-1} = dek(k)^{-1} * \begin{pmatrix} 8 & -5 \\ -7 & 9 \end{pmatrix}$

D'apres le théorèm vu en cours:

$det(k) * det(k)^{-1} mod 26 = 1 \equiv det(k) * det(k)^{-1} * 26y = 1$ d'ou on résoudra l'équation diophantienne $37 * det(k)^{-1} + 26y = 1$ en utilisant la division eucludienne.

	37	10	10=(1*7+3)
1	26	7	7=(2*3+1)
2	11	3	3=(2*1+1)
2	4	1	1=(1*1+0)
1	3	1	
	1	0	

Nous obtenons l'équation suivante $26 * 10 - 37 * 7 = 1$ d'ou $\begin{cases} det(k)^{-1} = & -7 = 19 \\ y = & 10 \end{cases}$

$\begin{pmatrix} L_K \\ L_W \end{pmatrix} = 19 * \begin{pmatrix} 8 & -5 \\ -7 & 9 \end{pmatrix} * \begin{pmatrix} 10 \\ 22 \end{pmatrix} \bmod 26 = \begin{pmatrix} 2 \\ 14 \end{pmatrix} \equiv \begin{pmatrix} C \\ O \end{pmatrix}$

$\begin{pmatrix} L_V \\ L_B \end{pmatrix} = 19 * \begin{pmatrix} 8 & -5 \\ -7 & 9 \end{pmatrix} * \begin{pmatrix} 21 \\ 1 \end{pmatrix} \bmod 26 = \begin{pmatrix} 3 \\ 4 \end{pmatrix} \equiv \begin{pmatrix} D \\ E \end{pmatrix}$

Le message en clair obtenu M="**CODE**"

Exercice N°6

1. Cryptanalyse par force brute

   Pour $k = 9$, le message en clair obtenu M="**A stitch in time saves nine**" ("Un point à temps en vaut cent" autrement dit l'entretien consciencieux permet d'éviterle gaspillage).

2. Cryptanalyse par analyse de fréquences

   Pour décrypter la phrase suivante: "LHLZ HFQ BC HFFPZ WH YOUPFH MUPZH". On compte les apparitions des lettres comme suit:

Lettre	H	F	P	Z
Nombre apparitions	6	4	3	3

   On suppose donc que le H crypte la lettre E, le F la lettre S, ce qui donne:

*E** ES* ** ESS** *E ***SE ****E

   D'après les statistiques P et Z devraient se décrypter en A et I (ou I et A). Le quatrième mot "HFFPZ", pour l'instant décrypté en "ESS**", se complète donc en "ESSAI" ou "ESSIA". La première solution semble correcte ! Ainsi P crypte A, et Z crypte I. La phrase est maintenant :

*E*I ES* ** ESSAI *E ***ASE **AIE

En réfléchissant un petit peu, on décrypte le message : M= "**CECI EST UN ESSAI DE PHRASE VRAIE**"

3. Dans le premier sous-message, la lettre la plus fréquente est **R** avec **5** apparitions. Après, on trouve **H** et **X** avec chacune **4** apparitions.
   Dans le deuxième sous-message, la lettre la plus fréquente est **S** avec **7** occurences, ensuite on a **F** avec **6** occurences.
   En posant **R** comme codage de **E** par la première lettre C1 de la clé et S comme codage de E par la deuxième lettre C2, on obtient que:

   C1 = R - E = N et C2 = S - E = O

   On essait de décoder le début du message, on obtient BESROP.. Ce qui ne semble pas à un texte en français. On essaie d'autres possibilités. Par exemple, en supposant que le codage de E + C1 = H. On trouve alors que C1 = H - E = D. Le décodage du début du message avec la clé **DO** donne
   LECRYPTOGRAMMEDEVIGENERENESTPLUSCON
   SIDEREDENOSJOURSCOMMEUNPROTOCOLESUR

Exercice N°7

1. Chiffrement du message M="cryptographie par transposition"
   Nous avons le nombre de lettres du message en clair $m = 29$ et $n = 6$
   $m \bmod n = 5$ d'ou les 5 premiéres colonnes aurant $(m/n) + 1 = 5$ lignes

6	5	4	3	2	1
C	R	Y	P	T	O
G	R	A	P	H	I
E	P	A	R	T	R
A	N	S	P	O	S
I	T	I	O	N	

   Le cryptogramme C="**OIRSTHTONPPRPOYAASIRRPNTCGEAI**"

2. Déchiffrement avec le mot clé "WATER"

   Nous avons le nombre de lettres du cryptogramme $m = 23$ et n =5
   $m \bmod n = 3$ d'ou les 3 premiéres colonnes aurant $(m/n) + 1 + 5$ lignes

W 5	A 1	T 4	E 2	R 3
L	A	S	T	E
G	A	N	O	G
R	A	P	H	I
E	M	O	D	E
R	N	E	*	*

   Le message en clair obtenu M='**La stéganographie moderne**'