Universite Badji Mokhtar-Annaba
Faculté des Sciences de l'Ingenieur
Département d'Informatique

جامعة باجي مختار – عنابـــــــــة
كلية علـــــــوم الهندســـــة
قسم الإعـــــــلام الآلـــــــــي

Exercice1 :

Il existe 6 types génériques d'attaques cryptanalytiques donnez le principe de chaque attaque.

Exercice2 :

Définir la cryptographie symétrique. Quels sont ses avantages/désavantages par rapport à la cryptographie asymétrique ?

Exercice 3 :

1- Appliquer la méthode César pour chiffrer le message suivant :
Je suis à Londres dans un des rues les plus misérables de la ville. K=17
Un enfant a dit je sais des poèmes. K=12

2- Décrypter le texte suivant qui a été obtenu en appliquant le chiffrement de César sur un texte en langue française dans lequel les espaces ont été supprimées :

vcfgrwqwfsbhfsntowbsobgfsbhfsnqvsnjcigsghqsoixcif
rviwtshseicwbsgojsnjcigdogeisjcigoihfsgofhwgobgjc
igbsrsjsnqwfqizsfrobgzsgfisgzsgxcifgcijfopzsgeioj
sqzsggwubsgrsjchfsdfctsggwcbdofzseiszsghhcbashwsf

3- Le message suivant a été codé avec un code de César, décodez-le par analyse de fréquence.

JTVMNKKTVLDEVVTLWTWITKTXUTLWJERUTVTWTHDXATLIUNEWV.
JTVIEVWELOWENLVVNOEDJJTVLTPTXYTLWTWUT
SNLITTVQXTVXUJXWEJEWTONKKXLT

Exercice 4 :

1- Rappelez la définition du cryptosystème de Hill défini modulo un entier n.
2- Supposons la taille m*m de la matrice clé connue. Montrer comment le chiffrement de Hill peut être cryptanalysé à l'aide d'un texte (succession de blocs) clair/chiffré bien choisi.
3- Supposons que le texte FRIDAY est chiffré en utilisant le cryptosystème de Hill (modulo 26) avec une taille de blocs m = 2 en le texte PQCFKU. Trouvez la clé K.

4- Chiffrez le message suivant « Rendez-vous ce soir » avec le chiffrement de Hill en utilisant la matrice $\begin{bmatrix} 3 & 2 \\ 1 & 3 \end{bmatrix}$

5- ELECTION avec la clé (ou matrice) de chiffrement $\begin{bmatrix} 3 & 5 \\ 1 & 2 \end{bmatrix}$
6- MATHEMATIQUE avec la clé $\begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix}$
7- Sachant que le message a été chiffré par la méthode de Hill, en utilisant la matrice $\begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix}$, quel est le message en clair obtenu en déchiffrant le cryptogramme suivant: « FGXGE DSPGV »

Exercice 5 :

1- Chiffré par la méthode de Vigenère le message suivant:

M= Ce système de codage n'est pas sûr, mais plus que le code de César si la clé est longue.
En utilisant le mot-clef : n1 = 3, n2 = 14, n3 = 7, n4 = 22, n5 = 19

2- Trouver le chiffrement de message LA MAISON BLANCHE avec un chiffrement de Vigenère avec la clé XYZ.
3- key: monarchie
plaintext: au secours nous sommes decouverts
4- Texte clair : un ami qui vous veut du bien
Mot_clé : VIGENERE
5- Sachant que le message a été chiffré par la méthode de Vigenère, en utilisant le mot-clef VICTOR HUGO, quel est le message en clair obtenu en déchiffrant le cryptogramme suivant:
GMPYO EAUBO DBTXQ LKYAL WINES JKUTG GIVXH VSYRC BQUXH RPNVF JXTXV LTVRS KIKLW SSYNC IVGMS FUPUM VQVNB IHGKO PJGGW KZOXI

Exercice 06 :

On veut envoyer le message suivant:
RENDEZ VOUS DEMAIN MIDI VILLETANEUSE
L'expéditeur et le destinataire du message se mettent d'accord sur une grille de largeur fixée à l'avance (ici une grille de 6 cases de large).
L'expéditeur écrit le message dans la grille en remplaçant les espaces entre les mots par le symbole ■. Il obtient:

R	E	N	D	E	Z
□	V	O	U	S	□
D	E	M	A	I	N
□	M	I	D	I	□
V	I	L	L	E	T
A	N	E	U	S	E

Il lit le texte en colonne et obtient ainsi le message crypté:

R□D□VAEVEMINNOMILEDUADLUESIIESZ□N□TEC

Pour pouvoir modifier le code rapidement sans toucher à son principe et pouvoir ainsi augmenter la sécurité les deux interlocuteurs peuvent décider l'ajout d'une clé secrète constituée par l'ordre de lecture des colonnes.

1- On choisit la clé: CAPTER crypter le message précédent.
2- Combien de code peut-on avoir ?
3- Déchiffrer le message précédent ?