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

جامعة باجي مختار – عنابـــــــــة
كلية علـــــــــوم الهندســـــــة
قسم الإعـــــــــلام الآلـــــــــي

Série TD

Exercice 1 :

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

Exercice 2 :

1- Appliquer la méthode César pour chiffrer les messages 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

Exercice 3 :

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 cryptanalyse 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 $\begin{matrix} 3 & 2 \\ 1 & 3 \end{matrix}$

Exercice 4:

Appliquer la méthode playfair pour chiffrer les messages suivant :

1- Mot clé : victor hugo

-Texte clair : Sa bouche, pale, s'ouvrait ; la mort noyait son œil farouche, ses bras pendants semblaient demander des appuis.

2- Texte clair : un ami qui vous veut du bien.

- Mot_clé : PLAYFAIR

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.

Exercice 6:

A- Considère le système RSA avec P = 19 et Q = 23.

Q1 : Calculer N et Q(N).

Q2 : Calculer l'exposant d associé à e=9, puis e=14.

Q3 : Calculer l'exposant d associé à e=17.

B- Effectuer le chiffrement et le déchiffrement en utilisant l'algorithme RSA pour les valeurs suivantes : P = 3 ; Q = 11 ; e = 7 ; M = 9 ;

C- Étant donné un système RSA de clé publique (35,11). Quelle est la clé secrète d ?