Université Djilali Bounaâma - Khemis-Miliana
Département : Mathématiques et Informatique
3ème Année Licence - informatique
Matière : Sécurité informatique et Cryptographie

Série d'exercices N° 02

Exercice n° 01 :

On souhaite chiffrer le message en clair « **EYE** » avec la clé « **S** » par un Xoring :
Sachant que les valeurs décimales des lettres claires dans la table ASCII sont : E=69, Y=89, S=83.
Donner le message chiffré en décimal ?

Exercice n° 02 :

Un système est protégé par un mot de passe. Après un essai infructueux le système attend un moment avant de redemander le mot de passe (le temps total d'une tentative est 3 secondes). Combien de temps (en secondes) faudra-t-il pour pénétrer le système sachant que le mot de passe est composé de 4 chiffres ?

Exercice n° 03 :

- Que veut dire "une clé" dans le chiffrement moderne ?
- Citez quelques opérations concernant la gestion des clés ?
- Expliquez brièvement le principe du chiffrement dans le mode ECB ?

Exercice n° 04 :

- Expliquez à travers un schéma le principe de chiffrement CBC ?
- On souhaite chiffrer la suite binaire **"1100110101110111010111101"** par le mode CBC avec des blocs de 8 bits sachant que :

Le vecteur aléatoire **IV = "10010101"**
La clé **K** = **"11101101"**
La fonction de chiffrement sert à inverser le bloc à chiffrer
Ecrire alors la suite binaire chiffrée ?

Exercice n° 05 : Bijection de Feistel

On souhaite chiffrer le message suivant avec une bijection de Feistel répétée deux fois :
M = 11011110001010011101110010110101
La fonction aléatoire **f** est une transposition simple et dont la clé est : **2413**

- Dessiner le schéma de Feistel (standard) ensuite écrire les formules de chiffrement et de déchiffrement ?
- Schématiser la procédure de chiffrement de M, ensuite écrire le message chiffré ?

Exercice n° 06 : Chiffrement RSA

On souhaite chiffrer un message M avec RSA, on suit les étapes suivantes :

1- On choisit deux nombres premiers distincts **p** et **q**, leur produit est **n**

Exemple : **p=11**, **q=17**

2- On choisit **e** premier avec **φ(n)** c-à-d **pgcd(e,φ(n))=1**

Exemple : **e=7**

3- On calcule **d** tel que **e×d ≡ 1 (mod φ(n))**

Exemple : **d=23**

- Calculer **φ(n)**, ensuite déduire les valeurs de la clé publique et privée ?
- Ecrire les formules de chiffrement et de déchiffrement d'un message **M** ?
- Calculer **X**, le message chiffré de **M=88** en utilisant la méthode de calcul de la puissance modulaire ?
- Schématiser la procédure de chiffrement/déchiffrement ?