République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université Abderrahmane Mira de Béjaia
Faculté des Sciences Exactes

Département d'Informatique
Module : Sécurité 1
Niveau : Master1

Série de TD N°3

Exercice1

Dans un système de chiffrement par flot RC4, quel est le problème de sécurité qu'on peut avoir, si on chiffre plusieurs messages avec une même clé **k**.

Exercice 2

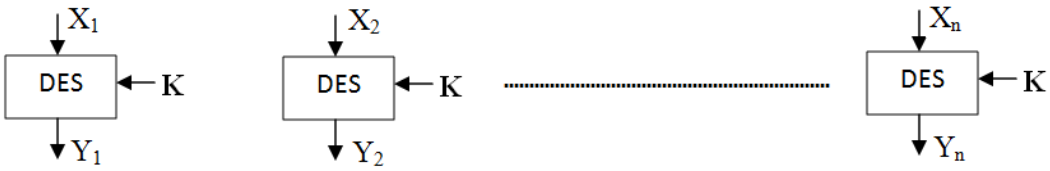
1-Montrer que le processus de Déchiffrement DES consiste à appliquer le même algorithme avec l'ordre des clés inversé (k16 au premier tour, k15 au deuxième tour,….k1 au dernier tour) .

2-Sachant que la machine spécialisée DES-cracker met en moyenne 4.5 jours pour retrouver par recherche exhaustive une clé DES de 56 bits, combien de temps mettrait-elle pour retrouver une clé de 40bits ? 112 bits (3DES) ?
3-Soit K = 133457799BBCDFF1 une clé (en hexadécimal).Trouver la clé K1 générée par le DES.

Exercice3

Les algorithmes de chiffrement symétrique, dits par blocs, tels que DES, 3DES ou AES, peuvent être vus comme des boîtes noires prenant en entrée un bloc de données possédant une taille fixe (64 bits pour le DES) ainsi qu'une clé et retournant un bloc de données chiffrées ayant la même taille qu'en entrée.

En pratique ces algorithmes de chiffrement sont utilisés par des méthodes de chiffrement (modes de chiffrement). Le mode le plus basique est appelé ECB (Electronic Code Book). Le mode ECB, illustré sur la figure 1 avec DES, consiste simplement à découper les données à chiffrer en ***n*** blocs X_1 , X_2 , X_3…..X_n possédant la longueur du bloc de l'algorithme de chiffrement utilisé (64 bits pour DES) et à chiffrer chaque bloc au moyen de la même clé K, obtenant ainsi les blocs chiffrés Y_1 , Y_2 , Y_3…..Y_n .



Mode ECB avec DES

Question : Expliquer pourquoi ce mode de chiffrement peut fournir certaines informations sur les données chiffrées (à travers un exemple).

Exercice4

Un groupe de **n** étudiants souhaite utiliser un système cryptographique pour s'échanger deux à deux des informations confidentielles. Les informations échangées entre deux membres ne doivent pas être lues par un autre membre.

Le groupe décide d'utiliser un système de chiffrement Symétrique.

1. Quel est le nombre minimal de clés Symétriques nécessaires ? Donner un nom d'un système Symétrique connu.

Le groupe décide après d'utiliser un Système de chiffrement Asymétrique.

2. Quel est le nombre minimal de couples de clés Asymétriques nécessaires pour que chaque membre puisse envoyer et recevoir des informations chiffrées ?

Le groupe décide finalement d'utiliser un système hybride pour le chiffrement (combinaison entre systèmes Symétrique et Asymétrique).

3. Donner les raisons qui ont poussées ce groupe à utiliser un tel système ; illustrer sous forme d'un schéma un tel système Hybride.

Exercice5

1-Effectuer les calculs suivants en utilisant l'algorithme de calcul (Square-and-multiply)
$2^{79} \mod(101)$; $3^{197} \mod(101)$.
2-Calculer les coefficients u et v satisfaisant au+bv=PGCD(a,b), tel que : a=6711 et b=831, sur Z.

Exercice6

1-Rappeler le principe de RSA.
2-Montrer que la fonction de chiffrement est bien l'inverse de la fonction de déchiffrement (D(E(x))=x).
3-On considère un module RSA avec **n=pq**, où **p** et **q** sont les inconnues. Une des méthodes de cryptanalyse de tel système et la factorisation de **n**. Montrer simplement que la connaissance de **Φ(n)** permet de remonter à la factorisation de **n**.