Fiche de Td No 2

Exercice No 6 chiffrement par bloc

Mode ECB

On considère un chiffrement par permutation travaillant sur des blocs de 4 bits. On utilise la clef suivante :

1	2	3	4
3	1	2	4

Le 1er bit du résultat est le 3e de la source, ...

Chiffrez m=100100101001111 en utilisant le mot de ECB.

Déchiffrez ensuite le résultat.

Mode CBC:

faite de même en utilisant le mode CBC en utilisant Vi=1010 comme vecteur d'initialisation.

Exercice No 7 amélioration de la méthode ECB

Citez les forces et les faiblesses du mode ECB.

Proposez une méthode pour améliorer sa sécurité.

Exercice No 8 méthodes de chiffrement par bloc

On considère les méthodes de chiffrement par bloc ECB, CBC et OFB vues en cours. Montrer que si un bloc chiffré est vérolé lors du transfert, il y aura au plus deux blocs déchiffrés vérolés.

Exercice No 9 double DES

Considérant que la taille des clefs de DES est trop petite, on se propose de combiner deux chiffrement DES avec deux clefs différentes K1 et K2. Ainsi, C=E(K1,(E(K2,M)).

Question 1 donner le procédé de déchiffrement associé.

Question 2 Quelle est la taille de l'espace des clefs de ce double DES.

Question 3 on suppose que l'on connaît un couple (M,C). Comment cela peut-il nous aider à trouver la clef correspondante ? Quel est la complexité de votre attaque ?

On partira du principe qu'on est techniquement capable de stocker 2^{56} blocs de 64 bits.

Exercice No 10 chiffrement de petits message par clef publiques

Une banque utilisse un procédé de chiffrement à clef publique pour communiquer avec ses clients.

L'une des applications consiste à faire envoyer un code secret de 4 chiffres par les clients à la banque. Nous supposerons que le message ne contient que le code secret.

- Que peux-faire un espion pour déchiffrer le code secret chiffré ?
- Comment s'en protéger ?

Exercice No 11 masque jetable (One Time Pad)

Pour chiffrer un message en clair $M=m1m2m3...m_l$ (avec m_i valant 0 ou 1), Ahmed applique la méthode suivante :

- générer un nombre aléatoire K de l bits : $k1k2k3...k_l$
- $C=E_k(M)=M \oplus K$ où $\oplus$ est le ou exclusif.
- Elle envoie C à Benjamin

Pour le déchiffrer, Benjamin applique la méthode suivante :

- $D_k(C)= C \oplus K$ (on suppose que Benjamin connait K)

Question 1 montrer que si a,b et c sont 3 bits, on a :

- $(a \oplus b) \oplus b=a \oplus (b \oplus b)=a$
- $(a \oplus b) \oplus c=a \oplus (b \oplus c)$

Question 2 Donner un exemple de chiffrement et de déchifrrement du message en clair M=0111001111110010

Question 3 Montrer que pour tour message M et toute clef K, on a $D_k(E_k(M))=M$

Question 4 Montrer qu'il existe A tel que 10101111= 10101010⊕A.

Généraliser ce résultat en montrant que quelque soit P et C, il existe A tel que $P=C \oplus A$.

Que peut-on en déduire sur la sécurité du procédé de chiffrement ? Les attaques de type « force brute » ou statisque ont-elles un intérêt ?

Question 5 Que permet la connaissance d'une partie de la clef K ?

Question 6 Alice envoit un courrier M1 anodin chiffré avec une clef K à Ahmed. Charles intercepte le courrier et en connait la version en clair (c'est un bulletin météo). Alice envoit un courrier M2 à Ahmed et, par flemme, le chiffre avec la même clef K. Charles intercepte le courrier C2. Peut-il retrouver M2 ? Comment ?

Question 7 Le fait que la clef soit aléatoire est-il important pour la sécurité de la méthode ? Comment Arthur peut-il faire pour générer une clef aléatoire ? Donnez les avantages et faiblesses de votre méthode de génération de clef aléatoire.

Question 8 Donnez les avantages et inconvénients du procédé OTP.

Exercice No 12 signature en aveugle

Question 1 rappeler le fonctionnement de RSA en tant qu'algorithme de chiffrement. On rappellera :

- les éléments constituant la clef publique
- les éléments constituant la clef privée
- les relations qui les lient
- le procédé mathématique de chiffrement
- le procédé mathématique de déchiffrement

Question 2

RSA peut aussi être utilisé en tant qu'algorithme de signature. Décrivez le processus et expliquez quelles propriété de RSA permet cela.

Question 3

Barack utilise un système de signature RSA. Le travail de Barack est de signer les messages de toutes les Abigaël de l'entreprise. On ne souhaite pas que Barack puisse lire la version en clair des message qu'il signe. Voici le processus que l'on vous demande de compléter :

- Abigaël crée un message M en clair
- de M, Abigaël déduit M' selon un procédé à préciser
- Abigaël envoie M' à Barack
- Barack applique un procédé à préciser à M' et obtient S'
- Barack envoie S' à Abigaël
- Abigaël déduit S, version signée de S, de S' selon un procédé à préciser