Exercices sur : Sécurité des réseaux
Sécurité informatique

Auteur : omar cheikhrouhou
Omar.cheikhrouhou@isetsf.rnu.tn

Ch2_Cryptographie

1. Dressez un tableau comparatif entre la cryptographie symétrique et la cryptographie asymétrique ?
2. citez trois algorithmes de chiffrement symétriques ? quelle est l'algorithme le plus utilisé actuellement ? (4 points)
3. citez trois algorithmes de chiffrement asymétriques ? quelle est l'algorithme le plus utilisé actuellement ? (4 points)
4. Dans la cryptographie asymétriques chaque entité possède une paire de clés (Kpub_i/ Kpriv_i) avec i : identité de l'entité i.
    a. Expliquez la différence entre ces deux clés ?
    b. Quelle clé j'utilise pour chiffrer un message destiné à R ? Qui peut lire ce message ?
    c. Quelle clé j'utilise pour signer un message destiné à R ? Qui peut vérifier la signature du message ?
5. Expliquez la différence entre : Le **chiffrement de flux** ou **chiffrement par flot** (en anglais *stream cipher*) et Le **chiffrement par bloc** (en anglais *block cipher*) ?

Le **chiffrement par bloc** : découpage des données en blocs de taille généralement fixe. Les blocs sont ensuite chiffrés les uns après les autres.
Le **chiffrement de flux** ou **chiffrement par flot** (en anglais *stream cipher*) traite les données de longueur quelconque et n'a pas besoin de les découper.

6. Pour chiffrer nos communications effectuées par les téléphones mobiles de type GSM on utilise l'algorithme de chiffrement A5/1. A votre avis (Expliquez) c'est un algorithme :
    a. symétrique ou asymétrique ?
    b. de chiffrement de flux ou de chiffrement par bloc ?

7. Le protocole WEP utilisé pour la sécurité des réseaux sans fil (Wi-Fi) utilise l'algorithme de chiffrement RC5. A votre avis (Expliquez) c'est un algorithme :
    a. symétrique ou asymétrique ?
    b. de chiffrement de flux ou de chiffrement par bloc ?
8. Parmi les algorithmes de chiffrement suivants indiquez ceux qui sont symétriques et ceux qui sont asymétriques ?
    a. DES
    b. RSA
    c. AES
    d. RC5

Ch3_Algorithmes Cryptographique Symétriques

Exercice : Chiffrement symétrique et asymétrique
Un groupe de n personnes souhaite utiliser un système cryptographique pour s'échanger deux à deux des informations confidentielles. Les informations échangées entre deux membres du groupe ne devront pas pouvoir être lues par un autre membre.
Le groupe décide d'utiliser un système symétrique de chiffrement.
1. Quel est le nombre minimal de clefs symétriques nécessaires ?
2. Donner le nom d'un algorithme de chiffrement symétrique reconnu.
Le groupe décide ensuite de remplacer ce système par un système asymétrique.
1. Quel est le nombre minimal de couples de clés asymétriques nécessaires pour que chaque membre puisse envoyer et recevoir des informations chiffrées et/ou signées ?
2. Alice souhaite envoyer des informations chiffrées et signées à Bob (Alice et Bob
appartiennent tous les deux au groupe). Quelle(s) clef(s) Bob doit-il utiliser ?
3. Donner le nom d'un algorithme de chiffrement asymétrique reconnu.
Le groupe décide finalement d'utiliser un système hybride pour le chiffrement (i.e. qui utilise à la
fois le cryptographie symétrique et asymétrique)

1. Donner les raisons qui ont poussées le groupe à utiliser un tel système.

Exercice N° :

On souhaite réaliser un système de messagerie sécurisée à l'intérieur d'une société. Pour cela, on utilise des « messages électroniques » et et un système à clés publiques (chiffrement asymétrique). Un tel message comporte une information M qui contient le nom *A* de l'expéditeur et le nom *B* du destinataire et les données secrètes D à partager.

On note KA_{Pub} la clé publique *de A et* $_{KAPri}$ *la* $_{clé\ privée}$ de A

On note aussi KB_{Pub} la clé publique *de B et* $_{KBPri}$ *la* $_{clé\ privée}$ de B

1. Comment assurer la confidentialité d'une information M envoyée par l'expéditeur A au destinataire B ?
2. Comment assurer l'intégrité d'une information M envoyée par l'expéditeur A ?
3. Expliquer comment le destinataire B vérifie l'authenticité de A et l'intégrité du message ?
4. On suppose qu'à un instant t1 un message M1 chiffré a été envoyé par A à B. Ce même message peut être renvoyé tel qu'il est dans un deuxième temps t2 (t2>t1) pour tromper le destinataire. Quelle technique peut-on utiliser pour éviter ce rejoue de message ?

Exercice N° : cryptographie symétrique

Soit le cryptogramme suivant : **H A W U D R U G L Q D L U H**

1. En utilisant l'algorithme de césar, le cryptanalyste teste l'ensemble des clés possibles pour essayer de déchiffrer le cryptogramme.

   Au bout de combien d'essai, le cryptanalyste parvient à identifier la bonne clé ? Justifier votre réponse ?
2. Utiliser l'algorithme de César (clé = 3) pour déchiffrer le cryptogramme ci dessus.
3. Peut-on dire alors la valeur 3 est la clé qui a été utilisée par l'algorithme de césar pour obtenir le cryptogramme ci dessus ? Justifier votre réponse ?
4. L'algorithme de César est un crypto-système mono alphabétique ou poly-alphabétique ? Justifier votre réponse ?
5. Quels sont les inconvénients du crypto-système de César ?
6. Soit **F** la fonction de cryptage suivante :

lettre	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
F(lettre)	**I**	**P**	**A**	**R**	**J**	**Q**	**B**	**V**	**K**	**C**	**L**	**D**	**U**	**E**	**W**	**S**	**T**	**N**	**Z**	**M**	**F**	**G**	**Y**	**O**	**H**	**X**

   a. Trouver la fonction $\mathbf{F^{-1}}$ de décryptage ?
   b. Crypter le texte « ***resource reservation in fourth generation wireless networks***» avec la fonction **F** et avec l'algorithme de césar (clé=3)
   c. Quel est l'avantage de cet algorithme (**F**) par rapport à celui de césar ?
   d. L'algorithme **F** est un crypto-système mono alphabétique ou poly-alphabétique ? Justifier votre réponse ?
   e. Décrire alors dans ce cas une technique utilisée par le cryptanalyse pour essayer de déchiffrer le cryptogramme ?
7. Utiliser la clé « ABCD » (1234) pour déchiffrer avec le crypto système de Vignère le cryptogramme suivant : **D T B T U C Q E M A V I**
8. Déduire à partir de la question précédente si le crypto-système de Vignère est poly-alphabétique ou non ? Justifier votre réponse ?

Exercice N°

Pour réaliser un système de paiement électronique, on utilise des "chèques électroniques" et un système à clés publiques (chiffrement asymétrique). Un tel chèque comporte une information *M qui* contient le nom *N* du titulaire du compte, le nom *B* de la banque et la

somme S. On suppose que la clé publique de N, K_{PN}, est accessible à tous. Une personne recevant un chèque en paiement l'envoie à la banque.

5. Comment assurer la confidentialité d'une information M envoyée par le client à la banque ?
6. Comment assurer l'intégrité d'une information M envoyée par le client à la banque ?
7. Expliquer comment la banque vérifie l'authenticité du client et l'intégrité du chèque.
8. La solution cheque électronique permet à une personne de faire une copie du chèque et de l'envoyer à la banque pour se faire payer deux fois. Proposez une modification simple pour éviter cela.