Université Abderrahmane Mira de Bejaia
Faculté des Sciences Exactes
Département d'Informatique

جامعة بجاية
Tasdawit n Bgayet
Université de Béjaïa

Module : Cryptographie
Niveau : L3 RN option RS
2023 - 2024

Fiche TD N° 2
Cryptographie Moderne

Question de cours

1. Citer quelques exemples d'algorithmes de chiffrement symétrique.
2. Citer quelques exemples d'algorithmes de chiffrement asymétrique.
3. Proposer un algorithme de chiffrement symétrique.
4. Selon la cryptographie symétrique, proposer un protocole d'authentification entre deux entités A et B qui partagent une clé KAB.
5. De quel problème mathématique le système de chiffrement RSA tire sa sécurité ?
6. Quels sont les éléments généraux présents dans tous les algorithmes déchiffrement asymétriques ?
7. Pour quels usages utilise-t-on la cryptographie symétrique ? Asymétrique ?

Exercice 1.

1. En utilisant l'algorithme d'exponentiation rapide, calculer :

   $351^{17} \bmod 437$ $41247^{21} \bmod 17$ $353^{611} \bmod 18$

2. Résoudre les équations diophantiennes suivantes :

   $144x+625y=1$ $37x-27y=1$ $323x-391y=1$

Exercice 2. Protocole de Diffie-Hellman

a. Quel est le secret commun k qu'établissent A et B en utilisant le protocole Diffie-Hellman avec n=17 et g=3 si les nombres aléatoires qu'ils ont choisis sont $x_a= 7$ et $x_b= 4$?

b. A quoi va servir cette clé k ? quel est l'avantage de l'utiliser ?

c. Décrire une attaque pour ce protocole dans laquelle un attaquant actif (i.e. qui peut modifier les données) peut ensuite intercepter, déchiffrer et modifier toutes les communications que l'entité A ou B chiffrerait avec sa clé. Expliquer quelles sont les faiblesses Diffie-Hellman dans ce contexte.

d. Dix-sept personnes veulent pouvoir s'échanger des messages deux à deux. Si elles choisissent un système à clé secrète, combien de clés faut-il en tout ? Même question pour un système à clé publique. Quels sont les avantages de chaque système ?

Exercice 3. Chiffrement de RSA

Deux entités A et B choisissent comme nombre premier p =17 et q=19, comme exposant e=5. Les deux entités se fixent un protocole RSA dans lequel les messages sont des nombres en base 10 que l'on code par bloc de 2 chiffres. A veut envoyer le message « 462739 » à B.

a. Donner la clé publique de B.

b. Donner la clé secrète de B.
c. Ecrire le message chiffré qu'A envoie à B.
d. Déchiffrer le message qu'a reçu B et vérifier que c'est bien celui qu'a envoyé par A.

Exercice 4. Chiffrement d'El Gamal

On s'intéresse à l'algorithme cryptographique d'ElGamal.

1. Peut-on avoir pour un même message clair plusieurs messages chiffrés ? justifier votre.

2. Afin d'utiliser l'algorithme ElGamal, deux entités « A » et « B » s'entendent sur les valeurs de p=7 ; g=3 Et a = 4 la clé secrète de l'entité A, donner la clé publique de « A».

3. Supposons que « B » veut envoyer le message m=2 à « A » avec b =5 ; quel est le message chiffré correspondant à envoyer à « A » ?

4. Montrer comment Alice retrouve le message m à partir du message chiffré reçu.

Exercice 5. Chiffrement de Rabin

1. Peut-on créer une paire de clés à partir de p=191 et q=199 ? Expliquer.
2. Calculer la paire de clés.
3. Chiffrer le message M=457, ensuite déchiffrer le résultat.

Exercice 6. Chiffrement de Merkel-Hellman

Soit la clé privée (A= {1, 3, 5, 10, 25, 53, 101, 205, 512}, n=143, m=960).

1. Calculer la clé publique correspondante.
2. Chiffrer le message M=457, ensuite déchiffrer le résultat.

Exercices supplémentaires

Exercice 1

1. Exécuter le protocole de Diffie-Hellman pour les utilisateurs A et B qui possèdent, respectivement les clés privées x=113 et y=97 pour g=20 et n=43. Vérifier la validité de la clé partagée.
2. Ré-exécuter le protocole pour trois utilisateurs A, B et C sachant que l'utilisateur C possède la clé privée z=13. Vérifier la validité de la clé partagée.

Exercice 2

On souhaite générer une paire de clé RSA à partir de n=1073 et $\phi(n)$=1008.

1. Calculer les paramètres p et q.
2. Calculer la clé privée correspondante à e=17.
3. Chiffrer le message M=976, ensuite déchiffrer le résultat.

Exercice 3 Chiffrement d'El Gamal

1. Calculer une paire de clés pour p=97, g=13, et a=45.
2. Chiffrer M=81 pour b=35, ensuite déchiffrer le résultat.