Université Abdalhafid Boussouf Mila
Institut des sciences et technologies
3ème Année informatique
Module: Sécurité informatique

Série TD N° 04

Exercice 1 :

1. L'utilisateur A choisi les facteurs premiers p = 3 et q = 11.
   - Déterminez une clé privée et une clé publique du cryptosystème RSA utilisant p et q.
2. Les utilisateurs A et B décident d'un protocole RSA dans lequel les lettres d'un message sont codées par leur position dans l'alphabet (en base 10), et le message est découpé en blocs de 2 chiffres (en base 10). B veut envoyer le message « CALCUL ».
   - Donnez le message chiffré que B envoie à A.
   - Donnez le message déchiffré par A, du message reçu de B, et vérifiez qu'il correspond bien à celui envoyé par B.
3. Si on découpe le message en blocs de 3 chiffres (en base 10).
   - Donnez le message chiffré que B envoie à A.
   - Donnez le message déchiffré par A, du message reçu de B, et vérifiez qu'il correspond bien à celui envoyé par B.

Exercice 2 :

Un professeur envoie ses notes au secrétariat de l'École par mail. La clé publique du secrétariat de l'Ecole est (e = 3, n = 33).
1- Déterminer la clé privée du secrétariat de l'Ecole.
2- Pour assurer la confidentialité de ses messages, le professeur chiffre les notes avec la clé RSA du secrétariat.

- Quel message chiffré correspond à la note 14?
- Quelle note correspond au message chiffré 29?

Exercice 3:

Soit l'utilisateur A qui possède la clé privée (3, 55) et la clé publique (27, 55) RSA.
Soit l'utilisateur B qui possède la clé privée (7, 187) et la clé publique (23, 187) RSA.

1. Pour assurer la confidentialité de ses messages, l'utilisateur A chiffre le message m = 2 avec la clé RSA de B. Donnez le message chiffré.
2. Pour assurer l'authenticité de ses messages, l'utilisateur A signe le message m en utilisant la signature RSA et chiffre le résultat avec la clé RSA de B. Donnez le message signé et chiffré c.
3. L'utilisateur B reçoit le message c. Vérifiez la signature.