Département d'informatique
Faculté des sciences
Université de Batna

Master I SRI S2

Cryptographie

Examen final
29 Mai 2014
Durée : 1h30

Questions de cours :

1. C'est quoi la différence entre le hachage d'un message et le MAC ?
2. Citer les applications de la cryptographie asymétrique ?
3. Calculer le nombre de clefs possibles pour le chiffrement affine.

Exercice 1 :

Considérons un LSFR à cinq états $(x_0, x_1, x_2, x_3, x_4)$ dont l'état initial est 01110 et la fonction linéaire est définie par $f(x_0, x_1, x_2, x_3, x_4) = \sum_{i=0}^{n} c_i x_i$, avec $c = (c_0, c_1, c_2, c_3, c_4) = (1,0,1,0,0)$.

1- Donner les seize premiers bits générés par ce LSFR et crypter la séquence de bits 1001111010101100.
2- En utilisant la structure de Feistel à deux rondes et deux clefs $K_1 = 11011100$ et $K_2 = K_1$ décalée de deux bits vers la gauche, crypter la séquence de bits résultante de la question 1. (la fonction à utiliser est le XOR).
3- Quel est le type du cryptage résultant des deux questions ?

Exercice 2 :

Considérons le chiffrement RSA dont le module n est égal à 253.

1- Donner la factorisation de n et le plus petit exposant de chiffrement.
2- Calculer le chiffrement du message m = 165.
3- Que faut-t-il faire pour pouvoir déchiffrer un message crypté c.

Exercice 3 :

Chiffrer le message «MAI» avec le chiffrement affine ayant pour clef le couple (7, 3).

1- Calculer pgcd(7, 26) et déterminer deux entiers u et v tels que $7u+26v = pgcd(7,26)$ en utilisant l'algorithme d'Euclid étendu (on vous demande de donner les détails des calculs).
2- Donner l'expression de la fonction de déchiffrement correspondante à la fonction de chiffrement de la question (1), montrer que ces fonctions sont valables et déchiffrer le message (0, 23, 6).

Interrogation (30 minutes)

Ecrire un programme en langage C qui réalise le chiffrement et déchiffrement avec l'algorithme ElGamel. Votre programme doit obligatoirement faire appel à aux trois fonctions : `generateur` `crypter` et `decrypter`.