Département d'informatique
Faculté des sciences
Université de Batna

Master I CS S2

Introduction à la cryptographie
11 juin 2013

Contrôle final
Durée : 1H30

Questions de cours :

1. Expliquez le principe de l'algorithme 3DES est dites, en justifiant votre réponse, s'il est plus avantageux ou non que l'algorithme DES avec des clés de 128 bits.
2. Quels sont les inconvénients de l'algorithme AES par rapport à l'algorithme DES ?
3. Expliquez l'utilité et le principe de l'algorithme d'échange de clés Deffie-Hellman.
4. Quelle est la principale différence entre le hachage et le MAC (Message Authentification Code).

vérification de clés

Exercice 1 :

1- Numériser le message « MAIS » en utilisant la correspondance A → 0, B → 1, …, Z → 25.
2- Chiffrer le message numérisé précédent avec le chiffrement affine et la clé (15,8).
3- On considère l'entier $a = 15$, calculer $pgcd(15,26)$ et déterminer deux entiers u et v tels que $15u+26v = pgcd(15,26)$ en utilisant l'algorithme d'Euclide étendu (on vous demande de donner les détails des calculs).
4- Donner l'expression de la fonction de déchiffrement correspondante à la fonction de chiffrement de la question (2). Et déchiffrer, en utilisant cette dernière, le message (Q, I, W).

Exercice 2 : Soit le scénario suivant :

Une personne A souhaite envoyer le message 17, en le chiffrant par l'algorithme ELGamal, à une personne B qui va déchiffrer le message reçu. Pour cela, B choisie un nombre premier $p = 19$, un générateur $a = 10$ et un nombre secret $a = 5$, et A choisie un nombre entier $k = 6$.

Expliquer le reste du protocole qui se déroule entre A et B en détaillant les calculs effectués par chacun d'entre eux jusqu'à ce que B obtienne la valeur 17.