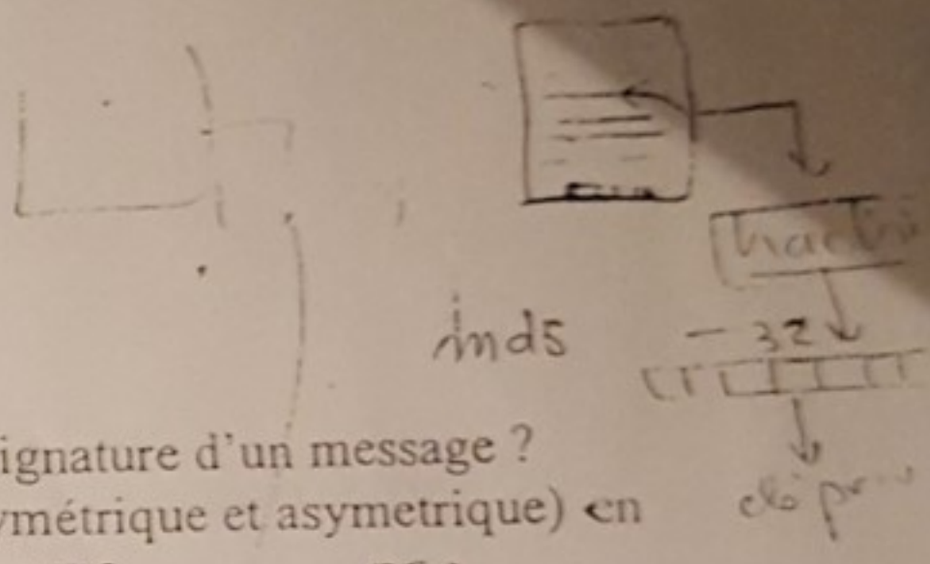
Département d'informatique
Faculté des sciences
Université de Batna

Master 1 CS S2

Introduction à la cryptographie

Contrôle final
11 septembre 2012
Durée : 1H30



Questions de cours :

1. C'est quoi la différence entre le hachage d'un message et la signature d'un message ?
2. Faites une comparaison des deux types de cryptosystèmes (symétrique et asymetrique) en citant deux exemples de chaque type.
3. Expliquer le principe d'échange de clef Deffie-Hellman.

Exercice 1 :

Supposons que Bob_1 et Bob_2 ont pour clef publique RSA (n, b_1) et (n, b_2) respectivement, avec b_1 et b_2 premiers entre eux. Supposons aussi qu'Alice envoi le même message m à Bob_1 et Bob_2 en le cryptant avec leurs clefs publiques RSA respectives. Est-ce que Eve qui intercepte les deux messages crypiés peut découvrir le texte en claire correspondant ? Justifiez votre réponse.

Exercice 2 :

1- Calculer le module n et l'entier $\varphi(n)$ associés aux nombres premiers p = 19 et q = 23.
2- Quels sont les exposants privés (secrets) associés aux exposants publics : b = 9, b = 14 et b = 17 (on vous demande de donner les détails des calculs).

Exercice 3 :

1- Numériser le message « UNE » en utilisant la correspondance A → 0, B → 1, …, Z → 25.
2- Chiffrer le message numérisé précédent avec le chiffrement affine et la clef (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'Euclid 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 le message (18,10, 21).