UNIVERSITÉ MOHAMMED V AGDAL
FACULTÉ DES SCIENCES
LABORATOIRE DE MATHÉMATIQUES, INFORMATIQUE ET APPLICATIONS

Année 2009-10
Master CSI
Introduction à la cryptographie
Contrôle final

Exercice 1. Une recherche exhaustive de la clé dans le cas du système de Vernam a-t-elle un sens ? Expliquez votre réponse.

Exercice 2. On considère l'AES-128 et la clé

`2c 7f 16 17 28 ae d2 a6 ab f7 15 88 09 cf 4f 3c`

Calculer w_i, $i = 0, \cdots, 7$.
Utilisez cette clé pour donner le résultat de la première ronde , du chiffrement de

`32 43 f6 a8 88 5a 30 8d 31 31 98 a2 e0 37 07 34`

On donne le résultat sous forme matricielle.

Exercice 3. Soit $f : \mathbb{F}_2^{2m} \longrightarrow \mathbb{F}_2^m$ une fonction de hachage et h une deuxième fonction de hachage définie par :

$$\begin{array}{rccc} h: & \mathbb{F}_2^{4m} & \longrightarrow & \mathbb{F}_2^m \\ & x_1||x_2 & \longrightarrow & f(f(x_1)||f(x_2)) \end{array}$$

où $||$ désigne l'opération de concaténation. Montrez que si f est résistante aux collisions, alors h est aussi résistante aux collisions.

Exercice 4. A public key cryptosystem was used to encrypt x, and you have the corresponding ciphertext y. The owner of the private key is willing to decrypt exactly one ciphertext y' that you can choose and send to him, as long as $y' \neq y$. How can you use this to find x, if
a) RSA is used ?
b) ElGamal is used ?

Exercice 5. Assume that Alice randomly selected two prime numbers p = 73 and q = 101. Alice randomly selected a random number $e_1 = 113$ as her public key (for encryption). Assume that Bob also selected $p = 73$ and $q = 101$ for his RSA system and Bob selected a random number $e_2 = 127$ as his public key. Alice published her public key $e_1 = 113$ and $n = 7373$. Bob published his public key $e_2 = 127$ and n = 7373. Charlie wants to send a message $m = 2009$ to both Alice and Bob using their public key for encryption. Answer the following questions. For all computations, you need to show the details (step by step) of your calculation. You cannot just list the number directly computed by using some code as your answer.
a) What is the ciphertext C_1 Charlie sent to Alice ?
b) What is the ciphertext C_2 Charlie sent to Bob ?
c) What is the decryption key d_1 used by Alice based on RSA system ?
d) Show the process Alice decrypts the ciphertext using only the procedure $C_1^{d_1} = 1 \ mod \ n$?
e) Assume that Bob uses the Chinese Remainder Theorem approach instead for decryption. Show all the computations done by Bob to decrypt the ciphertext C_2.
f) Assume that an attacker Oscar intercepted both the ciphertext C_1 and the ciphertext C_2. Oscar only knows n, e_1, e_2. Is it possible that Oscar can recover the original message m (assuming the Oscar cannot do factoring of n now) ? If possible, show the computing procedure Oscar can use to find m.