FACULTÉ DES SCIENCES ET TECHNIQUES
LIMOGES

2010-2011

Master I

Introduction à la cryptologie

Contrôle du 04 janvier 2011

durée : 2 h

Sans documents, calculatrice autorisée

Exercice 1 :
On considère que les lettres de A à Z sont représentées respectivement par les entiers de 0 à 25. On considère l'algorithme de Vigenère avec la clef `EXAM`.

1. Chiffrer à l'aide de ce procédé le message suivant : `CRYPTOGRAPHIE`.
2. Déchiffrer le message : `XOAHEFLEIOIQYU`.

Exercice 2 : Dans cet exercice, nous étudions l'algorithme DES (Data Encryption Standard).

1. Vérifier et corriger si nécessaire la parité de la clef D.E.S. suivante : `BF4C57E520AD1183`
2. Rappeler les longueurs des paramètres d'entrée (message, clef) ainsi que sa sécurité théorique (c'est-à-dire l'ordre de grandeur ou le nombre de tests à effectuer pour lancer une attaque exhaustive sur la clé).
3. Proposez diverses solutions (vues en cours) pour augmenter cette taille de clef sans changer de structure d'algorithme.

Une des solutions est le double chiffrement. Supposons qu'Alice envoie à Bob le message M en utilisant le double DES. Elle transmet C après avoir calculé DES pour la clé K_1 puis DES pour la clé K_2 à partir d'un message M.

3. Faire un schéma de ce double chiffrement et préciser la sécurité théorique de ce schéma.
4. Supposons que Charlie intercepte la communication et récupère M et C. Il établit deux listes de messages :
$$L_1 = \bigcup_K \{DES_K(M) : K \text{ clé}\}, \quad L_2 = \bigcup_{K'} \{DES^{-1}_{K'}(C); K' \text{ clé}\}.$$
5. Déterminer comment Charlie peut retrouver K_1 et K_2.
6. Nous cherchons à déterminer le coût de cette attaque. On rappelle que lorsque l'on a deux listes de n éléments, il faut en moyenne $O(n \log_2 n)$ opérations pour trouver un élément en commun (ou affirmer qu'il n'y en a pas). Déterminer le coût de cette attaque (appelée attaque par le milieu) et le comparer à la sécurité théorique espérée.
7. En déduire la sécurité d'un triple DES à 3 clés. Rappeler à l'aide d'un schéma la version à deux clés et comparer sa sécurité avec la précédente. Conclure.

Problème : Exponentiation RSA

Alice utilise le système cryptographique RSA pour communiquer avec Bob. Charlie récupère une feuille de calcul qui a permis à Alice de déchiffrer ce que lui avait écrit Bob.

1. Rappeler le système RSA.
2. Ici, quelle est la clef privée d'Alice ? Quel est le message de Bob ?
3. Charlie n'a pas réussi à retrouver la clef publique d'Alice sur Internet. Peut-il le faire à l'aide de la feuille de calcul ?
   [pour la conclusion finale de cette question, on pourra s'aider en vérifiant que 101 est un diviseur de n]
4. Quelle est la valeur de la clef publique e utilisée par Alice ?
   [Si la question précédente est négative, on pourra supposer que $\varphi(n) = 11200$]
5. Expliquer pourquoi la valeur de e trouvée à la question précédente ne doit être divisible par aucun des entiers 2, 5, ou 7.
6. En général, si n et $\varphi(n)$ sont connus, comment peut-on trouver les deux facteurs premiers p et q de n ?
7. Qu'est-ce qu'Alice doit faire pour signer une empreinte d'une message. Donner la signature de $h = 9726$.
8. Que doit faire Charlie pour chiffrer le message $M = 2$ à destination d'Alice ? Quelle sera la valeur transmise à Alice ?
9. Est-ce que Charlie peut se faire passer pour Bob auprès d'Alice ? Et inversement peut-il se faire passer pour Alice auprès de Bob ? Que faut-il mettre en place ?

i	d_i	z
11	1	$1^2 \times 9726 = 9726$
10	1	$9726^2 \times 9726 \equiv 2659$
9	0	$2659^2 \equiv 5634$
8	1	$5634^2 \times 9726 \equiv 9167$
7	1	$9167^2 \times 9726 \equiv 4958$
6	1	$4958^2 \times 9726 \equiv 7783$
5	0	$7783^2 \equiv 6298$
4	0	$6298^2 \equiv 4629$
3	1	$4629^2 \times 9726 \equiv 10185$
2	1	$10185^2 \times 9726 \equiv 105$
1	0	$105^2 = 11025$
0	1	$11025^2 \times 9726 \equiv 5761$