Master I

Initiation à la Cryptographie

Contrôle du 05 janvier 2006

durée : 2 h

Sans documents, calculatrice autorisée

Exercices Rapides

1) Donner les schémas de chiffrement et déchiffrement pour le mode CFB du D.E.S. On rappelle ce mode de chaînage :
$$\begin{cases} c_0 = IV \\ c_i = m_i \oplus \ \mathrm{DES}_K(c_{i-1}) \end{cases}$$
2) Dans la question précédente, quelle est la taille en bits de IV ? Que peut-on déchiffrer si on a perdu IV ?
3) Sur quelles propriétés/assurances repose la sécurité du chiffrement de Vernam (Masque jetable) ?
4) Les algorithmes de hachage sont parfois utilisés pour l'authentification par mot de passe. On stocke l'empreinte h(mot_de_passe). Comment vérifier que le mot de passe est correct ? Pourquoi ne pas stocker directement le mot de passe dans le fichier contenant tous les mots de passe ?
5) Chiffrer EXAMJANVIER à l'aide du système de chiffrement de **VIGENÈRE** et du mot-clef CRYTO.

Problème : R.S.A

Une manière d'accélérer un déchiffrement RSA est d'utiliser le théorème chinois.
Supposons que le déchiffrement classique est donné par le calcul

$$\mathrm{Dechiffre\_RSA}(y) = y^d \bmod n \quad \text{avec } n = pq.$$

Soit $d_p = d \bmod (p-1)$ et $d_q = d \bmod (q-1)$.
Soit $M_p = q^{-1} \bmod p$ et $M_q = p^{-1} \bmod q$.
Considérons l'algorithme suivant :

Déchiffrement RSA-CRT

$x_p \leftarrow y^{d_p} \bmod p$
$x_q \leftarrow y^{d_q} \bmod q$
$x \leftarrow M_p\, q\, x_p + M_q\, p\, x_q \bmod n$
Retourner(x)

a) Rappeler les avantages, inconvénients et utilisations du système RSA.

b) Montrer que le résultat x retourné par l'algorithme proposé est en fait $y^d \bmod n$.

c) Calcul de complexité : On suppose que le temps de calcul d'une exponentiation modulaire est proportionnelle au cube de la taille de la représentation binaire du modulus. Ainsi si un modulus est représenté sur m bits, la durée du calcul sera d'un temps proportionnel à m^3. Déterminer le temps de calcul pour le RSA-CRT en supposant que p et q se représentent avec m bits et que d_p, d_q, M_p et M_q sont précalculés et que l'addition est négligeable. Déterminer la taille de la représentation de n puis déterminer le coût en temps de calcul d'un déchiffrement RSA classique. Déterminer le rapport (ratio) entre les deux méthodes.

d) Si $d = 2003$, $p = 1511$ et $q = 2003$, calculer d_p, d_q, M_p et M_q.

e) A l'aide des calculs précédents, déchiffrer la valeur $y = 152702$.