Université Lyon I

"Cryptographie et Sécurité des Systèmes Informatiques" (MIF30)

Partiel du 26 mars 2007. Durée: 2H.
Notes de cours/TD autorisées.
Calculatrice interdite, rédaction du détail des calculs exigée.

**Exercice I**

Pour $x \in \mathbb{Z}$, résoudre

$$x^2 \equiv 125 \pmod{627}$$

**Exercice II. (Méthode RSA)**

Les questions dans cet exercice II sont indépendantes.

1. Par analogie avec le triple DES, sous quelles hypothèses pourrait-on définir le triple RSA et quel en serait l'intérêt?

2. Alice a publié sa clef publique (n=35, e=17). De la part de Bob, elle reçoit le message crypté

$$MC = 32 \mod 35$$

   (a) Calculer la clef privée $d$ d'Alice ainsi que $MC^{-1} \mod 35$.

   (b) Retrouver le message en clair $M$ envoyé par Bob.

3. Alice a choisi une clef publique RSA $(n, e)$ telle que

$$e = \frac{\phi(n)}{2} + 1$$

   A-t-elle fait un bon choix?

4. Alice possède une liste de diffusion à laquelle Adam et Eve appartiennent. Elle crypte à l'aide du protocole RSA chacun de ses messages $M$ à destination des personnes de sa liste.

   Oscar constate ou obtient que la clef publique d'Adam soit de la forme $(n_1 = p_1 * q_1, e_1 = 2)$ et celle d'Eve de la forme $(n_2 = p_2 * q_2, e_2 = 2)$, $n_1$ et $n_2$ étant étrangers.

   Oscar conçoit alors un logiciel qui découpe, avant d'être cryptés, les messages d'Alice en blocs formant des entiers $M_i$ à crypter par RSA, tels que $M_i < n_1$ et $M_i < n_2$

   Oscar offre son logiciel à Eve qui l'utilise alors.

   (a) Dire quels calculs Oscar peut faire maintenant pour décrypter tous les messages cryptés $MC$ envoyés par Alice à sa liste de diffusion.

   (b) Avec les valeurs $n_1 = 7$ et $n_2 = 11$ faire ces calculs pour retrouver $M$ dont le cryptogramme envoyé à Adam est $MC_1 = 4 \mod 7$ et celui envoyé à Eve est $MC_2 = 3 \mod 11$

## Exercice III. Hachage

Oscar offre à Alice un logiciel contenant une fonction de hachage $h$ s'appliquant à un message binaire de longueur pair:

$$M = (M_1, M_2) \in \mathbb{F}_2^n \times \mathbb{F}_2^n, \quad long(M_1) = long(M_2) = n$$

Le début de l'algorithme de ce logiciel commence par produire un message

$$f(M) = (m_1, m_2) \in \mathbb{F}_2^n \times \mathbb{F}_2^n$$

$f : \mathbb{F}_2^{2n} \to \mathbb{F}_2^{2n}$ étant définie par

$$m_1 = g(g(M_1) \oplus M_2) \oplus M_1$$

$$m_2 = g(M_1) \oplus M_2$$

($\oplus$: addition ("xor") dans $\mathbb{F}_2^n$)

où $g$ est l'application

$$M_i \mapsto \sigma(M_i) \oplus \sigma^{-1}(M_i)$$

et $\sigma$ est la permutation circulaire de décalage à gauche

$$(x_n, x_{n-1}, \ldots, x_2, x_1) \mapsto (x_{n-1}, , \ldots, x_2, x_1, x_n)$$

($\sigma^{-1}$ étant un décalage à droite).

Le hachage $h$ est enfin défini par

$$h(M) = f(M) \oplus M \oplus (1, 1, 0, 0, \ldots, , 0, 0, 1, 1)$$

Montrer qu'Oscar a offert à Alice une fonction de hachage qui n'est pas cryptographique.

**Exercice IV. Authentification**

On considère le protocole d'établissement de clef de session:

**1.** $A \rightarrow B : K_A$

**2.** $B \rightarrow A : K_B, K'_B$

**3.** $A \rightarrow B : e_{K'_B}(n_A, A)$

**4.** $B \rightarrow A : e_{K_A}(n_B)$

**5.** $B \rightarrow A : e_{K_A}(sign_B(n_A))$

**6.** $A \rightarrow B : e_{K'_B}(h(n_B))$

où

- $n_A$ (resp. $n_B$) est un nomus ("nonce") engendré ("aléatoirement") par $A$ (resp. $B$)
- $K_A$ (resp. $K_B$) est la clef publique de $A$ (resp. de $B$) (dont la validité dépasse largement la durée de la session en cours d'établissement)
- $K'_B$ est une autre clef publique de $B$ éphémère, ne durant que le temps de la session en cours d'établissement
- $sign_B$ désigne une fonction de signature de $B$
- $e_K$ désigne une fonction d'encryptage avec la clef publique $K$
- $h$ désigne une fonction de hachage cryptographique

1. A la fin de ce protocole, la clef de session commune entre $A$ et $B$ est $K_{AB} = n_A \oplus n_B$ (ou une fonction de $K_{AB}$, connue de $A$ et $B$ ou bien définie hors du protocole d'établissement de session). Le but du protocole est d'obtenir une croyance mutuelle en une clef commune entre $A$ et $B$. Si le protocole s'est déroulé correctement uniquement avec les 6 passes précitées, le but est-il atteint: la clef est-elle fraîche, bonne, confirmée, de qui pour qui?
2. Quelle est l'utilité de la clef publique de $B$ éphémère $K'_B$?

3. Oscar, noté $O$, peut jouer "l'homme du milieu" de telle sorte qu'à la fin de son attaque la session se déroule entre $A$ et $O$, bien que $A$ croie communiquer avec $B$. Décrire dans un schema (de forme analogue à celui décrivant le protocole ci-supra) et expliciter une telle attaque dans laquelle Oscar "joue et gagne en 5 coups" en interceptant tous les messages de $A$ pour $B$ et de $B$ pour $A$.