Université Lyon I

"Cryptographie et Sécurité des Systèmes Informatiques" (MIF30)

Partiel du 14 avril 2008. Durée: 2H.
Notes de cours/TD autorisées.
Calculatrice interdite, rédaction du détail des calculs exigée.

Exercice I

Pour $x \in \mathbb{Z}$, résoudre le système de congruences:

$$\begin{cases} 2x^2 \equiv 8 \pmod{11} \\ 5x \equiv 1 \pmod{9} \end{cases}$$

Exercice II

Soit un entier naturel n impair et différent de 1.

Pour quelles valeurs de n l'équation

1.

$$x^2 \equiv 5 \pmod{n}$$

a-t-elle des solutions?

2. Même question pour l'équation

$$x^2 \equiv 13 \pmod{n}$$

Exercice III. Hachage

Soit l un entier fixé et un e un cryptosystème qui, pour toute clef $K \in {\mathbb{F}_2}^{2l}$ de longueur $2l$, définit une application par blocs

$$e_K : {\mathbb{F}_2}^l \to {\mathbb{F}_2}^l$$

i.e. associe à un bloc M binaire de longueur l, un bloc binaire $e_K(M)$ de même longueur.

On définit alors une fonction de hachage h qui,
à un message binaire M de longueur quelconque,
associe un haché $h(M)$ de longueur $2l$

$$h : {\mathbb{F}_2}^* \to {\mathbb{F}_2}^{2l}$$

h est définie de la manière suivante.
On fixe un vecteur d'initialisation

$$IV = (h_{0,1}, h_{0,2}) \in {\mathbb{F}_2}^l \times {\mathbb{F}_2}^l$$

Quitte à faire du bourrage,
on considère M de longueur nl en l'écrivant en blocs de longueur constante l ($m_i \in {\mathbb{F}_2}^l$)

$$M = m_1 \,||\, m_2 \,||\, ... \,||\, m_n$$

Puis, pour $i \in [1, n]$, on pose

$$\begin{cases} h_{i,1} = (e_{h_{i-1,2}||m_i}(h_{i-1,1}) \oplus m_i) + h_{i-1,2} \mod 2^l \\ h_{i,2} = e_{h_{i-1,2}||m_i}(h_{i-1,1}) \oplus h_{i-1,1} \end{cases}$$

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

Le haché de M est enfin défini par

$$h(M) = (h_{n,1}, h_{n,2})$$

1. Décrire un algorithme $\mathcal{A}$ qui donne en sortie une (première) préimage m d'un haché $H \in \text{Im } h$ en complétant le schema suivant

   Entrée IV, H

   Faire

   1 choisir aléatoirement: $n, m_1, m_2, ...m_{n-1}$

   2 calculer $h_{n-1,1}, h_{n-1,2}$

   3 trouver m_n tel que ...

   Jusqu'à ...

   Sortie $m = m_1 \,||\, m_2 \,||\, ... \,||\, m_n$

2. Votre algorithme fournit-il toujours une préimage au bout d'un nombre fini d'itérations de la boucle "faire"?
   Sinon, quelles modifications de l'algorithme proposez-vous?

3. On suppose que h est une fonction de hachage parfaitement aléatoire (distribution uniforme des valeurs de h). Pour une itération de la boucle "faire" donnée, qu'elle est la probabilté pour que le test de la fin de la boucle soit vrai?

4. On note l'ensemble des événements élémentaires $\mathcal{E}$ formés des exécutions de l'algorithme $\mathcal{A}$ qui donnent en sortie une préimage au bout d'un nombre fini d'itérations.
   On définit la variable aléatoire $\mathcal{C} : \mathcal{E} \to \mathbb{N}^*$ en notant $\mathcal{C}(a)$ le nombre d'itérations de boucle dans l'exécution de $a \in \mathcal{E}$.
   En fonction de l, calculer l'espérance de $\mathcal{C}$

$$E(\mathcal{C}) = \sum_{1}^{\infty} n.\mathcal{P}(\mathcal{C} = n)$$

Exercice IV. Authentification

On considère le protocole d'authentification et d'établissement de clef suivant

1. $A \rightarrow B : A, n_A$

2. $B \rightarrow T : B, n_B, \{A, n_A\}_{K_{BT}}$

3. $T \rightarrow A : n_B, \{B, K_{AB}, n_A\}_{K_{AT}}, \{A, K_{AB}, n_B\}_{K_{BT}}$

4. $A \rightarrow B : \{A, K_{AB}, n_B\}_{K_{BT}}, \{n_B\}_{K_{AB}}$

où

- n_A (resp. n_B) est un nomus ("nonce") engendré ("aléatoirement") par A (resp. B)
- K_{AT} (resp. K_{BT}) est une clef symétrique privée, connue seulement de A (resp. de B) et d'une tierce partie de confiance T (clef définie hors protocole et non attaquable dans ce protocole)

A la fin de ce protocole, la clef de session symétrique commune entre A et B est K_{AB}.

1. Analyser chaque passe en terme d'authentification d'identité en utilisant précisément les définitions du cours.
2. Exhiber une attaque dans laquelle A n'authentifie pas B. On pourra chercher une attaque dans laquelle Oscar, "l'homme du milieu" noté O (ou O_I sous l'identité I), "joue et gagne en 3 coups" en interceptant tous les messages destinés à B.
3. Analyser chaque passe en terme d'établissement de clef (toujours en utilisant précisément les définitions du cours).
4. Exhiber une attaque par "polysémie" dans laquelle la clef K_{AB} de B pour A n'est pas exclusive. On pourra chercher une attaque dans laquelle Oscar, "l'homme du milieu", "joue et gagne en 3 coups".