Université Lyon I

"Cryptographie et Sécurité des Systèmes Informatiques" (MIF30)

Partiel du 27 mars 2006. Durée: 2H.
Notes de cours/TD autorisées.
Calculatrice interdite, rédaction du détail des calculs exigée.

Exercice I

Pour $x \in \mathbb{Z}$, résoudre

$$x^2 \equiv 7 \pmod{991}$$

Exercice II

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

$$\begin{cases} x^2 \equiv -3 \pmod{7} \\ 2x \equiv 1 \pmod{9} \end{cases}$$

Exercice III

Soient p et q deux entiers impairs tels que

$$p \equiv 1 \pmod{3}$$

$$q \equiv 1 \pmod{3}$$

1. Montrer
$$p + q - 2 \equiv pq - 1 \pmod{4}$$
2. Montrer que 3 est inversible modulo pq
3. On suppose, de plus, que
$$pq \equiv 3 \pmod{4}$$

Parmi les trois équations suivantes

$$x^2 \equiv 3 \pmod{p} \quad (1)$$

$$x^2 \equiv 3 \pmod{q} \quad (2)$$

$$x^2 \equiv 3 \pmod{pq} \quad (3)$$

combien ne possèdent pas de solution et peut-on dire lesquelles?

Exercice IV. Méthode RSA

Alice choisit les deux entiers premiers $p = 47$, $q = 59$ et publie sa clef publique (n=pq= 2773, e=17).

1. Alice ayant calculé la valeur $\phi(n) = 2668$, montrer qu'elle a obtenu comme clef privée: $d = 157$

2. Dans la suite, on admettra les résultats suivants

$$2005^{156} \equiv 1653 \pmod{2773}$$

$$121^2 \equiv 776 \pmod{2773}$$

$$435^2 \equiv 661 \pmod{2773}$$

$$2668 = 16 * 157 + 156$$

$$2300^{16} = 1771 \pmod{2773}$$

$$776^2 \equiv 435 \pmod{2773}$$

$$661 * 11 \equiv 1725 \pmod{2773}$$

$$2300 * 2005 = 1 \pmod{2773}$$

   (a) Crypter le message $M = 11$ avec la clef publique d'Alice.

   (b) Alice reçoit de la part de Bob le message crypté $MC = 1771$. Quelle est la valeur du message M décrypté par Alice?

Exercice V. La Genèse revisitée par RSA

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

   Pour qu'une clef cassée ne permette pas de décrypter trop de messages précédant une telle compromission ("forward secrecy"), les personnes de la liste changent régulierement leur clef, de manière synchrone selon une courte période fixe.
   Cette mesure protocolaire affectera-t-elle la lecture de certains messages et, si oui, que proposez-vous pour y remédier ?

2. Oscar conçoit un logiciel contenant un générateur de clefs de type RSA qui fonctionne selon le principe suivant:

   Récupération de la clef publique actuelle (n, e_1) d'Adam et recherche aléatoire d'un entier e_2 premier avec e_1 tel que (n, e_2) soit une clef publique valide à renvoyer par le programme.

   En cas d'insuccès au bout d'un nombre d'étapes fixé, la clef privée est un nombre aléatoire et la clef publique générée, non valide, est de la forme (n, e_2) avec pour seule condition e_2 premier avec e_1.
   Donner un exemple d'une telle clef publique non valide.

3. Oscar concocte une belle interface spécialement conçue pour Eve. Il offre son logiciel à Eve qui, heureuse, décide dorénavant de l'utiliser systématiquement.

   (a) Alice peut-elle vérifier qu'une clef publique d'une personne de sa liste de diffusion est bien valide?

   (b) Montrer qu'Oscar peut maintenant, de manière passive en lisant les messages cryptés validement ou non à destination d'Adam et Eve, sauf cas de désynchronisation, décrypter tous les messages envoyés par Alice à sa liste de diffusion.

Exercice VI. Authentification

1. On considère le protocole suivant:

   1. $A \rightarrow B : A$

   2. $B \rightarrow A : n_B$

   3. $A \rightarrow B : \{n_B\}_{K_{AT}}$

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

   5. $T \rightarrow B : \{n_B\}_{K_{BT}}$

   où B propose un challenge à base du nomus ("nonce") n_B et où T est une tierce partie de confiance qui partage une clef secrète K_{AT} avec A et une clef secrète K_{BT} avec B.

2. Dire pourquoi c'est un protocole d'authentification. Est-ce une authentification mutuelle ou bien, de A et B, qui authentifie qui?

3. Avec pour but de prouver que l'authentification n'est pas forte, "Oscar joue et gagne en 4 coups"; pour cela, il engage, sous deux identités différentes, deux sessions de ce même protocole en direction de B et organise son attaque selon le schéma suivant

   1. ... $\rightarrow B : ...$

   1'. ... $\rightarrow B : ...$

   2. ...

   2'. ...

   3. ...

   3'. ...

   4. ...

   4'. ...

   5. $T \rightarrow B : \{n_B\}_{K_{BT}}$

   Compléter ce schéma en écrivant complètement les passes 1, 1', 2, 2', 3, 3', 4 et 4' pour montrer qu'une telle attaque existe.