Série de révision
Module Sécurité Informatique
Master IPS 2021-2022

Exercice 1

Alice change sa clé RSA tous les 25 jours. Bob lui change sa clé tous les 31 jours. Sachant qu'Alice change sa clé aujourd'hui et que Bob a changé sa clé il y a trois jours, déterminer quand sera la prochaine fois qu'Alice et Bob changeront leur clé le même jour.

Exercice 2

On suppose que Bob a envoyé un message m à la fois à Alice, Aline et Anna qu'il a auparavant chiffré avec leur cryptosystème RSA respectif

- Alice a choisi un modulus RSA $N_1 = 2773$ et la clef publique $k = 3$,
- Aline a choisi le modulus $N_2 = 2257$ et la clef publique $k = 3$,
- Anna a choisi le modulus $N_3 = 2173$ et la clef publique $k = 3$.

Les messages chiffrés correspondant sont

$$\begin{array}{l} m^3 \mod N_1 \equiv 1673, \text{ pour Alice,} \\ m^3 \mod N_2 \equiv 1525, \text{ pour Aline,} \\ m^3 \mod N_3 \equiv 1032, \text{ pour Anna.} \end{array}$$

(a) Trouver un entier $0 \leq x < (N_1 N_2 N_3)$ tel que

$$\begin{array}{rcl} x & = & 1673 \mod N_1, \\ x & = & 1525 \mod N_2, \\ x & = & 1032 \mod N_3. \end{array}$$

(b) En utilisant le résultat de la question précédente, retrouvez d'abord le cube du message clair qu'a envoyé Bob à Aline, Alice et Anna, puis déduisez-en le message clair m.

(c) Sachant que les entiers $s = 1020$ et $t = 691$ vérifient $s^2 \equiv t^2 \mod N_1$, factorisez N_1 et déduisez en la clef privée d'Alice.

Exercice 3

Soit g un fonction de hachage résistante aux collisions. On définit la fonction h de hachage :

$$h(x) = \begin{array}{l} 1 // x \\ 0 // g(x) \end{array}$$

a. Montrer que h est résistante aux collisions.

b. Montrer que pour toute fonction h résistante aux collisions, h est résistante aux secondes pré-images.

Exercice 4

Le schéma ElGamal en signature utilise un générateur g de Z^*_p et une clé publique $y = g^x \bmod p$, ou` x est la clé privée.

a. Dans quel ensemble est choisi x ?

b. Pour signer un message m, le signataire tire un aléa k et calcule $r = g^k \bmod p$ et $s = k^{-1} (H(m)-xr)$: la signature est (r, s).

Décrire une attaque contre ce schéma de signature si le même aléa k est utilisé pour signer deux messages distincts. De quel type d'attaque s'agit-il ?