Sécurité - Master Ingénierie Informatique - Examen 2011-2012

Durée 2h. L'utilisation de notes de cours est autorisée, l'utilisation de livres et de dispositifs électroniques est interdite. Les points associés à chaque question sont donnés à titre indicatif.

Exercice 1 (carré latin, 6 points) *Soit $n \geq 1$ un nombre naturel. Un carré latin d'ordre n est une matrice L de dimension $n \times n$ à coefficients dans $\mathbf{Z}_n = \{0, \ldots, n-1\}$ tel que chaque élément de $\mathbf{Z}_n$ apparaît exactement une fois dans chaque ligne et chaque colonne.*

Étant donné un carré latin L de dimension n, on prend $\mathbf{Z}_n$ comme espace des textes clairs, des textes chiffrés et des clefs. Le chiffrement $E_k(x)$ avec la clef k du texte clair x correspond au coefficient $L[k, x]$ (ligne k, colonne x) de la matrice. A noter qu'on compte les lignes et les colonnes de 0 à $(n-1)$.

1. *Expliquez comment calculer la fonction de déchiffrement $D_k(y)$.*
2. *Montrez que pour tout $n \geq 1$ on peut construire un carré latin L de dimension $n \times n$.*
3. *Construisez un carré latin de dimension 4 et utilisez-le pour chiffrer le texte clair $x = 3$ et pour déchiffrer le texte chiffré $y = 2$ avec la clef $k = 2$.*
4. *Si n est très grand, il n'est pas pratique de construire explicitement le carré latin de dimension n. Pouvez-vous calculer directement les fonctions de chiffrement et déchiffrement associées au carré latin que vous avez construit ? Le système obtenu est-il équivalent à un système de chiffrement étudié dans le cours ?*
5. *Expliquez comment appliquer le résultat sur la sécurité parfaite présenté dans le cours pour conclure que le système de chiffrement décrit est* parfaitement sûr *à condition que la clef est choisie de façon uniforme et est utilisée une seule fois.*

Exercice 2 (variante de Diffie-Hellman, 6 points) *Soient p, q nombres premiers avec $p = 2q + 1$ et soit g un élément du groupe multiplicatif $(Z_p)^*$ d'ordre q. En d'autres termes, q est le plus petit nombre positif tel que $(g^q \equiv 1) \bmod p$.*

Un ensemble d'utilisateurs $U = \{1, \ldots, n\}$ se mettent d'accord sur un triplet (p, q, g). Chaque utilisateur $i \in U$ génère :

- *Une clef secrète $x_i \in \mathbf{Z}_q$.*
- *Une clef publique $y_i \in \mathbf{Z}_p$ telle que $y_i = (g^{x_i}) \bmod p$.*

Chaque clef publique est authentifiée à l'aide, par exemple, d'un tiers de confiance.

Un utilisateur i établit une clef commune K avec l'utilisateur j par le protocole suivant :

$$\begin{array}{ll} i \to j : & (i,\ \nu a_i \in \mathbf{Z}_q\ (g^{a_i}) \bmod p\ ) \\ j \to i : & (j,\ \nu a_j \in \mathbf{Z}_q\ (g^{a_j}) \bmod p\ ) \end{array}$$

où on utilise la notation $\nu x \in X$ pour dire qu'on choisit un élément x dans l'ensemble X de façon uniforme (cette notation est celle utilisée à plusieurs reprises dans le cours).

1. *A la fin du protocole, i et j calculent une clef $K = (g^{a_i x_j + a_j x_i}) \bmod p$ (attention aux indices !). Expliquez comment i peut calculer K.*
2. *Supposons que j choisit toujours un petit a_j, par exemple $a_j < 10^{10}$. Expliquez comment un utilisateur $k \neq i$ peut établir une clef avec j que j utilisera pour communiquer avec i.*

Exercice 3 (Signature RSA à anneau, 8 points) *On décrit une version simplifiée d'un système de signature qui permet à un ensemble d'utilisateurs* $U = \{1, \ldots, m\}$, $m \geq 2$ *de signer un message de façon telle que :*

- *le récepteur du message peut vérifier que le message a bien été signé par un des utilisateurs sans savoir lequel et*
- *chaque utilisateur peut signer sans la coopération des autres utilisateurs.*

Ce qui est demandé est simplement que chaque utilisateur ait une clef publique authentifiée.

Hypothèses

- *Chaque utilisateur* $i \in U$ *a une clef publique RSA* (e_i, n_i) *et une clef privée RSA* d_i *où* n_i *est un modulo sur au plus* s *bits. On écrit* $E_i(x)$ *pour* $(x^{e_i}) \bmod n_i$ *et* $D_i(y)$ *pour* $(y^{d_i}) \bmod n_i$.
- *On fixe une fonction de hachage* $h : 2^* \to 2^s$.
- *Soit* $t = 2^s$. *On définit* $E'_i : \mathbf{Z}_t \to \mathbf{Z}_t$ *par*

$$E'_i(x) = \begin{cases} n_i q + E_i(r) & \text{si } x = n_i q + r, 0 \leq r < n_i, n_i(q+1) \leq t \\ x & \text{autrement} \end{cases}$$

Signature pour $m = 2$ *L'utilisateur* $i = 1$ *signe un message* msg *comme suit :*

- *Il choisit* $x_2 \in \mathbf{Z}_t$.
- *Il calcule* $y_2 = E'_2(x_2)$.
- *Il calcule* $x_1 = D'_1(h(msg) \oplus y_2)$.
- *La signature est* $(\{1, 2\}, x_1, x_2)$.

Vérification pour $m = 2$ *On vérifie que :*

$$h(msg) = E'_1(x_1) \oplus E'_2(x_2)$$

1. *Expliquez pourquoi* E'_i, $i = 1, \ldots, m$, *est une permutation sur* $\mathbf{Z}_t$ *et définissez la permutation inverse* D'_i.
2. *Expliquez pourquoi un message correctement signé passe la vérification.*
3. *Montrez que si* $h(msg) = h(msg')$ *alors toute signature pour* msg *est aussi une signature valide pour* msg'.
4. *Généralisez le schéma de signature et de vérification à* $m > 2$ *utilisateurs.*

Solutions

Exercice 1

1. On cherche à la ligne k l'unique colonne x tel $L[k][x] = y$.
2. On peut définir :
$$L[k][x] = (x + k)\ mod\ n$$
3. On obtient, pour $n = 4$:
$$L = \begin{bmatrix} 0 & 1 & 2 & 3 \\ 1 & 2 & 3 & 0 \\ 2 & 3 & 0 & 1 \\ 3 & 0 & 1 & 2 \end{bmatrix}$$
et donc $E_2(3) = 1$ et $D_2(2) = 0$.
4. On a :
$$E_k(x) = L[k][x] = (x + k)\ mod\ n$$
et
$$D_k(y) = (y - k)\ mod\ n$$
Ce qui correspond au système de chiffrement par décalage de dimension 1 (ou de César).
5. D'après le résultat présenté dans le cours il suffit de vérifier que pour tout texte clair x et texte chiffré y il existe unique une clef k tel que $E_k(x) = y$. En effet on doit avoir $((x + k) \equiv y)\ mod\ n$ qui a comme seule solution modulo n :
$$(k \equiv (y - x))\ mod\ n$$

Exercice 2

1. On observe :
$$\begin{aligned} K &= (g^{a_i x_j} g^{a_j x_i})\ mod\ p \\ &= (g^{x_j})^{a_i} (g^{a_j})^{x_i}\ mod\ p \\ &= ((y_j)^{a_i} (g^{a_j})^{x_i})\ mod\ p \end{aligned}$$
L'utilisateur i connaît :
– y_j la clef publique de j.
– a_i : cette valeur est calculée par i.
– $(g^{a_j})\ mod\ p$: cette valeur est transmise par j.
– x_i la clef privée de i.
et peut donc calculer K.
2. On a l'échange de messages suivant :
$$\begin{aligned} k(i) \to j : &\quad (i,\ \nu a_k \in \mathbf{Z}_q\ (g^{a_k})\ mod\ p\ ) \\ j \to k(i) : &\quad (j,\ \nu a_j \in \mathbf{Z}_q\ (g^{a_j})\ mod\ p\ ) \end{aligned}$$
Pour retrouver la clef K sans connaître les clefs secrètes des autres participants, l'utilisateur k procède de la façon suivante :
– Il calcule $(g^a)\ mod\ p$ pour $a = 0, 1, \ldots, 10^{10}$ jusqu'à tomber sur $(g^{a_j})\ mod\ p$. Il apprend ainsi a_j.

– Maintenant il observe :

$$\begin{aligned} K &= (g^{a_k x_j} g^{a_j x_i}) \, mod \, p \\ &= (g^{x_j})^{a_k} (g^{x_i})^{a_j} \, mod \, p \\ &= ((y_j)^{a_k} (y_i)^{a_j}) \, mod \, p \end{aligned}$$

Donc à partir des clefs publiques y_i et y_j et des exposants a_k et a_j, il peut calculer la clef K que j croit partager avec i.

Exercice 3

1. On définit $D'_i : \mathbf{Z}_t \to \mathbf{Z}_t$ par :

$$D'_i(y) = \begin{cases} qn_i + D_i(y - qn_i) & \text{si } y = qn_i + r, 0 \leq r < n_i, (q+1)n_i \leq t \\ y & \text{autrement} \end{cases}$$

Si $x = qn_i + r$, $0 \leq r < n_i$ et $(q+1)n_i \leq t$ alors :

$$\begin{aligned} D'_i(E'_i(x)) &= D'_i(qn_i + E_i(r)) \qquad (\text{avec } 0 \leq E_i(r) < n_i) \\ &= qn_i + D_i(E_i(r)) \\ &= qn_i + r \\ &= x \end{aligned}$$

Autrement, $D'_i(E'_i(x)) = D'_i(x) = x$.
Donc E'_i a une inverse gauche sur $\mathbf{Z}_t$ ce qui suffit a conclure que E'_i est injective et doit donc être une permutation sur $\mathbf{Z}_t$ avec inverse D'_i.

2. Si par exemple $i = 1$ a signé le message on a :

$$\begin{aligned} E'_1(x_1) \oplus E'_2(x_2) &= E'_1(D'_1(h(m) \oplus E'_2(x_2))) \oplus E'_2(x_2) \\ &= h(m) \oplus E'_2(x_2) \oplus E'_2(x_2) \\ &= h(m) \end{aligned}$$

3. On a

$$E'_1(D'_1(h(msg) \oplus E'_2(x_2))) \oplus E'_2(x_2) \quad = E'_1(D'_1(h(msg') \oplus E'_2(x_2))) \oplus E'_2(x_2)$$

4. Par exemple, l'utilisateur $i = 1$ signe un message msg comme suit :
   – Il choisit $x_i \in \mathbf{Z}_t$ pour $i = 2, \ldots, m$.
   – Il calcule $y_i = E'_i(x_i)$ pour $i = 2, \ldots, m$.
   – Il calcule $x_1 = (D'_1(h(m) \oplus y_2 \oplus \cdots \oplus y_m)$.
   – La signature est $(\{1, \ldots, m\}, x_1, \ldots, x_m)$.

   Vérification On vérifie que :

$$h(m) = E'_1(x_1) \oplus \cdots \oplus E'_m(x_m)$$