Master CSI 1 2012-2013

Cryptologie, MA8W01 : Examen du 22 avril 2013

Master Sciences et Technologies, mention Mathématiques ou Informatique, spécialité Cryptologie et Sécurité informatique

Responsable : Gilles Zémor

Durée : 3h. Sans document. Les exercices sont indépendants.

– EXERCICE 1. Soit un nombre premier p de la forme $p = 2q + 1$ où q est lui même un nombre premier.

a) Montrer que 2 est primitif modulo p si et seulement si $2^q = -1 \mod p$.

b) Montrer que 2 est primitif modulo 83.

c) Si Alice est Bob utilisent 2 et $p = 83$ pour mettre en œuvre un protocole de Diffie-Hellman, et choisissent les exposants secrets 5 et 9, quel est leur secret partagé ?

d) Soit $P = 2^s = 22 \mod 83$ une clé publique El Gamal dont on ne connaît pas la clé secrète associée. Montrer que le couple $(56, 60)$ est une signature valide du message 10 modulo 83.

– EXERCICE 2. Deux utilisateurs A et B utilisent le système RSA avec le même modulo n mais avec des exposants publics e_A et e_B distincts. On supposera que e_A et e_B sont premiers entre eux. On suppose qu'un même message M est envoyé à A et B sous forme chiffrée, et qu'un observateur O intercepte les deux cryptogrammes C_A et C_B.

a) Montrer comment on peut retrouver facilement M à partir de C_A et C_B.

b) Le faire explicitement, sans factoriser n, pour les valeurs $n = 11021$, $e_A = 7$, $e_B = 13$, $C_A = 5342$, $C_B = 348$.

– EXERCICE 3. Soit $n = 97 \times 101 = 9797$. Soit $e = 449$. On constate que la fonction de chiffrement RSA

$$\begin{aligned} f : \mathbb{Z}/n\mathbb{Z} &\to \mathbb{Z}/n\mathbb{Z} \\ M &\mapsto M^e \end{aligned}$$

est involutive, c'est-à-dire vérifie $f(f(M)) = M$ pour tout M. Montrer qu'il existe toujours de tels exposants non-triviaux e pour tout entier RSA $n = pq$. Pour $n = 9797$, à l'aide du théorème chinois, trouver un autre exposant $e' \neq \pm 449$ et non-trivial tel que $f(f(M)) = M$.

– EXERCICE 4.

a) Soit p un nombre premier et soit α un entier primitif modulo p. Soit $y = \alpha^x \mod p$. Montrer comment on peut, à partir de la seule connaissance de α, p et y, trouver efficacement le dernier bit (le moins significatif) de x dans son écriture binaire.

b) On suppose maintenant que $p = 5 \mod 8$. Montrer que -1 est un carré modulo p et que 2 n'est pas un carré modulo p.

c) Soit a un carré modulo p. Montrer que $a^{(p-1)/4} = \pm 1 \mod p$.

d) Si $a^{(p-1)/4} = 1 \mod p$, montrer que $a^{(p+3)/8} \mod p$ est une racine carrée de a modulo p.

e) Si $a^{(p-1)/4} = -1 \mod p$, montrer que $2^{-1}(4a)^{(p+3)/8} \mod p$ est une racine carrée de a modulo p.

f) Soient $p = 5 \mod 8$, α un entier primitif modulo p, et $y = \alpha^x \mod p$. Montrer comment on peut, à partir de la seule connaissance de α, p et y, trouver efficacement le *deuxième* bit le moins significatif de x, c'est-à-dire x_1 dans l'écriture

$$x = x_0 + x_1 2 + \cdots + x_i 2^i + \cdots$$

– EXERCICE 5. On rappelle que le chiffrement de Blum-Micali a pour clé secrète deux entiers premiers p et q, pour clé publique le produit $n = pq$ ainsi qu'un non-carré modulo n de symbole de Jacobi 1, et qu'un symbole binaire m est chiffré par un carré aléatoire si $m = 0$ et un non-carré aléatoire si $m = 1$. On pose $n = 107 \times 127 = 13589$ et on donne le chiffré du message $M = (M_1, M_2, M_3, M_4)$ suivant :

$$C = (1281, 6373, 245, 2135).$$

a) En remarquant que 107 et 127 sont des entiers de Blum, i.e. égaux à 3 modulo 4, déduire très simplement de C un cryptogramme qui chiffre le message complémentaire $\overline{M} = (\overline{M_1}, \overline{M_2}, \overline{M_3}, \overline{M_4})$ de M.

b) Déchiffrer C pour trouver le message en clair M dans $\{0, 1\}^4$.

– EXERCICE 6. Soit α un élément d'ordre q premier dans un groupe G (par exemple $\mathbb{Z}/p\mathbb{Z}$). Les données α, q, G sont publiques. Une autorité choisit deux entiers s et t modulo q et publie les quantités

$$P = \alpha^s \qquad Q = \alpha^t \quad \text{dans } G.$$

L'autorité délivre ensuite de manière confidentielle à un ensemble $\mathcal{U}$ d'utilisateurs un couple d'entiers de la forme $(u, s + tu)$ où l'entier u est variable et est différent pour chaque utilisateur U de $\mathcal{U}$. Les opérations d'addition et de multiplication permettant de former $s + tu$ sont effectuées modulo le nombre premier q.

Une troisième entité souhaite maintenant établir un secret S commun avec toute la communauté $\mathcal{U}$. Elle procède ainsi : elle choisit deux entiers aléatoires r et x modulo q, puis diffuse publiquement le triplet $(x, \alpha^r, P^r \times Q^{rx})$.

a) Montrer comment les utilisateurs U de $\mathfrak{U}$ peuvent calculer la quantité $S = P^r$.

b) Que se passe-t-il si $x = u$ pour un certain utilisateur U ? Montrer que l'on peut ainsi *révoquer* l'utilisateur U, en l'excluant du groupe d'utilisateurs qui ont accès au secret commun S.

c) Discuter la difficulté d'obtenir S à partir uniquement de données publiques (si on ne fait pas partie de la communauté $\mathfrak{U}$).

d) Application : le groupe G est le groupe multiplicatif de $\mathbb{Z}/107\mathbb{Z}$. le nombre premier q est 53 et $\alpha = 4$. On a $P = 83$, $Q = 9$. Vous êtes un utilisateur U disposant de $u = 5$ et $s + tu = 42$. Vous recevez le triplet $(8, 34, 105)$. Calculer le secret S. (Cette question est un peu longue : séparez bien les différentes étapes).