Master CSI 1 — 2010-2011

Cryptologie, MHT 811 : Examen du 11 avril 2011

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 le nombre premier $p = 61$.

a) Montrer que 2 est primitif modulo p.

b) Dans un système de chiffrement El Gamal, Bob a pour clé secrète 7 et comme clé publique associée $6 = 2^7 \bmod 61$. Alice envoie à Bob le message chiffré $(20, 25)$. Quel est le clair associé ? 22

– Exercice 2. A et B souhaitent partager un secret commun S afin de l'utiliser comme clé dans un système de chiffrement à clé secrète.

a) Rappeler comment fonctionne le protocole de Diffie-Hellman pour l'établissement de S.

b) Montrer comment une tierce partie C qui peut communiquer avec A et B et intercepter les connexions entre A et B peut se faire passer pour B auprès de A et pour A auprès de B, puis peut ensuite décrypter les communications entre A et B sans qu'elles s'en aperçoivent.

c) Afin d'éviter le problème ci-dessus on propose le protocole suivant : On suppose que tout le monde a accès à une base de données publique où à chaque utilisateur U est associée une clé publique Y_U de la forme $Y_U = g^{X_U} \bmod p$ pour des quantités g et p fixes et publiques. Chaque quantité X_U est secrète et détenue par le seul utilisateur U. Décrire un protocole permettant à A et à B de partager une quantité secrète S de la forme $S = g^{aX_A + bX_B} \bmod p$.

d) Expliquer pourquoi C ne peut plus monter la même attaque que précédemment contre le protocole de Diffie-Hellman.

– Exercice 3. Dans une variante du système de Rabin, la clé publique est un couple (n, b) et la clé privée est la factorisation $n = pq$, où p et q sont deux nombres premiers. Pour un message $M \in \mathbb{Z}/n\mathbb{Z}$, le cryptogramme est

$$C = M(M + b) \mod n.$$

a) Décrire un algorithme et/ou une formule pour déchiffrer le cryptogramme C.

b) On suppose que $p = 23$, $q = 47$ et $b = 60$.
- Calculer toutes les racines carrées de 1 modulo n.
- Calculer le cryptogramme associé au message en clair $M = 111$.
- Quels sont tous les clairs possibles pour le cryptogramme trouvé précédemment ?

– EXERCICE 4. Les paramètres publics d'un système de signature d'El Gamal sont $p = 83$, $\alpha = 2$, $P = (\alpha^s \mod p) = 15$.

a) Montrer que 2 est primitif modulo 83.

b) Vérifier que $(u, v) = (47, 62)$ est une signature valide du message $M = 11$.

c) On suppose maintenant que l'on a affaire à un algorithme de vérification de signature buggé (bogué) qui accepte des signatures (u, v) même si $u > p$. On cherche à fabriquer une signature «valide» d'un nouveau message μ sans connaître la clé secrète. On prendra $\mu = 17$.
On forme $M^* = M^{-1} \mod (p - 1)$, et

$$\begin{aligned} M^* &= M^{-1} \mod (p-1) \\ u' &= u + p(u\mu M^* - u) \\ v' &= v\mu M^* \mod (p-1) \end{aligned}$$

Calculer le couple (u', v') et montrer qu'il constitue une signature reconnue comme valide du message μ.

d) Expliquer pourquoi la méthode précédente donne toujours une signature reconnue comme valide pour tout message μ.

– EXERCICE 5. On considère la variante suivante du système de chiffrement RSA. On considère un entier $n = pq$ où p est un grand nombre premier de s bits, c'est-à-dire que $2^{s-1} - 1 \leqslant p \leqslant 2^s - 1$, mais l'entier q est un entier de st bits, où t est petit ($t \approx 10$) : l'entier q est quelconque, il peut être choisi aléatoirement, et n'a comme seule propriété d'être sensiblement plus grand que p.

La clé publique du système est un couple (n, e) où e est un entier. La clé secrète du système est l'entier p. L'ensemble des messages en clair est l'ensemble des entiers de (strictement) moins de s bits, soit $\mathcal{M} = \{0, 1, \ldots, 2^{s-1} - 1\}$. Le chiffrement d'un message $M \in \mathcal{M}$ se fait par la fonction :

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

a) Montrer que l'application ci-dessus est injective si et seulement si e est premier avec $p - 1$.

b) Sous l'hypothèse ci-dessus, donner un algorithme de déchiffrement.

c) Montrer que si l'on a accès à l'algorithme de déchiffrement ci-dessus, alors en lui soumettant une entrée bien choisie on peut découvrir la clé secrète.

d) Montrer que si $e < t$, alors il devient facile de décrypter avec la seule connaissance de la clé publique.

– EXERCICE 6. Soit $n = pq$ un entier RSA et soient e et d des exposants de chiffrement et de déchiffrement associés. On considère le système de chiffrement suivant qui transforme des messages en clair dans $\mathbb{Z}/n\mathbb{Z}$ en des messages chiffrés dans $\mathbb{Z}/n^2\mathbb{Z}$. Le clair $M \in \{0, 1, \dots, n-1\}$ est transformé en le cryptogramme :

$$C = r^e(1 + Mn) \mod n^2$$

où r est un élément de $(\mathbb{Z}/n\mathbb{Z})^*$ aléatoire.

a) Trouver et expliquer comment marche l'algorithme de déchiffrement.

b) Montrer que si C_1 et C_2 sont deux chiffrés de deux messages M_1 et M_2 alors $C_1C_2 \mod n^2$ est un chiffré du message $M_1 + M_2 \mod n$.

– EXERCICE 7. Soit p un nombre premier et soit α un élément primitif modulo p. Soit $y = \cancel{g}\alpha^x \bmod p$ où $x \in \{0, 1, \dots, p-1\}$. On suppose y connu et l'on s'intéresse à la détermination de x. Soit $x_{\ell-1} \dots x_1 x_0$ l'écriture en base 2 de x, soit $x = \sum_{i=0}^{\ell-1} x_i 2^i$.

a) Montrer qu'il est facile de déterminer (c'est-à-dire qu'il est possible de trouver en un temps de calcul raisonnable) la parité de x, c'est-à-dire le bit x_0.

b) On suppose maintenant que $p = 3 \mod 4$. Montrer que si $x_0 = 0$ et que si vous disposez d'un algorithme qui vous calcule efficacement la valeur de x_1, alors vous pouvez calculer efficacement la valeur de $\alpha^{x/2}$.

c) En déduire que si vous disposez d'un algorithme efficace qui, étant donné tout $z = \alpha^a \bmod p$ où $a \in \{0, 1, \dots, p-1\}$, vous donne le deuxième bit a_1 de a dans son écriture binaire ($a = \sum_{i=0}^{\ell-1} a_i 2^i$), alors vous pouvez construire un algorithme efficace qui calcule a à partir de z. Décrire l'algorithme.