Master CSI 1 2009-2010

Cryptologie, MHT 811 : Examen du 19 avril 2010

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.

a) Quel est l'ordre multiplicatif de 2 modulo $p = 67$?

b) Alice et Bob décident d'utiliser le protocole de Diffie-Hellman dans le sous-groupe de $(\mathbb{Z}/59\mathbb{Z})^*$ engendré par $\alpha = 2$. Alice choisit l'exposant secret $\alpha = 5$ et Bob l'exposant secret 11. Que s'échangent-ils sur le canal et quel est leur secret partagé à l'issue du protocole ?

c) Notons m_A la quantité envoyée par Alice à Bob et m_B la quantité envoyée par Bob à Alice. Soit $q = (p-1)/3 = 22$. Une observatrice malintentionnée Eve intercepte m_A, l'élève à la puissance q, et remplace le message m_A à destination de Bob par m_A^q. De même il remplace le message m_B à destination d'Alice par m_B^q. Quel est le nouveau «secret» commun à Alice et Bob ?

d) Montrer que, quelles que soient les valeurs secrètes α et β choisies par Alice et Bob, le «secret» partagé ainsi arrangé par Eve ne peut prendre que trois valeurs : lesquelles ?

– Exercice 2. On considère un système de signature d'El Gamal associé au nombre premier $p = 59$, et dont une clé publique est $P = 2^s = 33 \mod p$ pour un exposant secret s.

a) Vérifier que $(u, v) = (47, 54)$ est une signature El Gamal valide du message $M = 11$, et que $(u', v') = (47, 4)$ est une signature valide du message $M' = 21$.

b) Constater que $u = u'$ et utiliser cette propriété pour retrouver le secret s (sans utiliser de recherche exhaustive).

– Exercice 3. Soient les nombres premiers $p = 23$ et $q = 31$ et soit $n = pq = 713$.

a) Montrer que l'entier 98 est un carré modulo n

b) Trouver la racine carrée modulo n de 98 qui est elle-même un carré modulo n.

– Exercice 4. Vous êtes confronté à un cryptogramme RSA $C = M^e \mod n$ avec un exposant public $e = 7$. Un espion vous indique que le message en clair inconnu vérifie la propriété $M^{12345} = 1 \mod n$. Trouvez un entier u tel que $C^u = M \mod n$. Cet entier u ne sera pas forcément l'exposant secret d de déchiffrement RSA associé à la clé publique (n, e), mais il doit convenir pour ce cryptogramme particulier.

– Exercice 5. deux utilisateurs A et B utilisent le système RSA avec le même modulo $n = 1333$ et des exposants différents. Soit $a = 3$ l'exposant public de A et $b = 5$ l'exposant public de B.

a) Chiffrer le message $M = 701$ à destination de A et B, c'est-à-dire calculer C_A le cryptogramme pour A et C_B le cryptogramme pour B.

b) Un adversaire intercepte C_A et C_B, puis effectue les calculs suivants :
- $x = a^{-1} \mod b$
- $y = \frac{xa-1}{b}$
- $z = C_A^x (C_B^y)^{-1} \mod n$.

c) Effectuer ces calculs dans l'exemple précédent. Que remarquez-vous ?

d) Montrer que le même phénomène se produit pour a et b des exposants quelconques et un entier n quelconque. Que faut-il en conclure pour la sécurité du système RSA ?

– Exercice 6. Soit $n = pq$ un entier RSA. On note λ le plus petit commun multiple de $p-1$ et de $q-1$.

a) Démontrer que pour tout $x \in (\mathbb{Z}/n\mathbb{Z})^*$ on a $x^\lambda = 1 \mod n$ et que la moitié des éléments de $(\mathbb{Z}/n\mathbb{Z})^*$ vérifient $x^{\lambda/2} \neq \pm 1 \mod n$. On pourra utiliser le théorème chinois.

b) Soit e un exposant de chiffrement RSA, c'est-à-dire un entier premier avec $p-1$ et $q-1$. Soit d un exposant de déchiffrement, c'est-à-dire tel que $M^{ed} = M \mod n$ pour tout entier M. Montrer que $ed-1$ est un multiple de λ.

c) Montrer que si $u = 2^i k \lambda$ où k est un entier impair, alors pour tout $x \in (\mathbb{Z}/n\mathbb{Z})^*$ on a $x^{u/2^{i+1}} = x^{\lambda/2}$.

d) En déduire qu'il existe une puissance de 2, soit 2^j, qui divise $ed-1$ et telle que $x^{(ed-1)/2^j}$ a une probabilité très proche de $1/2$ d'être une racine carrée de 1 différente de 1 ou de -1, ceci lorsque x est choisi aléatoirement et uniformément entre 1 et $n-1$.

e) En déduire un algorithme probabiliste qui permet, lorsqu'on dispose des deux exposants de chiffrement et de déchiffrement RSA, de factoriser n.

– Exercice 7.

a) Vérifier que 2 est primitif dans $\mathbb{Z}/11\mathbb{Z}$. Combien y a-t-il d'éléments dans $(\mathbb{Z}/121\mathbb{Z})^* = (\mathbb{Z}/(11^2)\mathbb{Z})^*$? Montrer que l'ordre multiplicatif de 2 dans $(\mathbb{Z}/121\mathbb{Z})^*$ est un multiple de 10 et un diviseur de 110 : calculer 2^{10} modulo 121 et en déduire que 2 est primitif dans $\mathbb{Z}/121\mathbb{Z}$ (c'est-à-dire que 2 engendre $(\mathbb{Z}/121\mathbb{Z})^*$).

b) Plus généralement, si p est premier, montrer que si g est un élément primitif de $\mathbb{Z}/p\mathbb{Z}$ alors soit g, soit $g+p$ est un élément primitif de $\mathbb{Z}/p^2\mathbb{Z}$.

c) Soit $\Gamma = \{x \in \mathbb{Z}/p^2\mathbb{Z},\ x = 1 \bmod p\}$. Montrer que Γ est un sous-groupe multiplicatif de $(\mathbb{Z}/p^2\mathbb{Z})^*$ de cardinal p, et que si $g \neq 1$ dans $\mathbb{Z}/p^2\mathbb{Z}$ alors, pour tout entier x, $0 \leqslant x \leqslant p-1$, si $y = g^x \bmod p^2$, on a la formule :

$$x = \frac{y-1}{g-1}.$$

d) Soit $n = p^2 q$ où q est un deuxième nombre premier. On rend public n ainsi qu'un entier $m < p$ et entier g primitif de $\mathbb{Z}/p^2\mathbb{Z}$. On considère la fonction de chiffrement définie par :

$$\begin{array}{rcl} \{0,1,\ldots,m\} & \to & \mathbb{Z}/n\mathbb{Z} \\ M & \mapsto & C = g^{M+nr} \end{array}$$

où r est un entier aléatoire. Montrer que le calcul de

$$\frac{C^{p-1}-1}{g^{p-1}-1}$$

dans $\mathbb{Z}/p^2\mathbb{Z}$ permet de déchiffrer et de retrouver M. Ce système de chiffrement est dû à Okamoto et Uchiyama (1998).