Master CSI 1 2014-2015

Cryptologie, MA8W01 : Examen du 21 avril 2015

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 $p = 83$.

a) Montrer que dans $\mathbb{Z}/p\mathbb{Z}$, tous les carrés non nuls et différents de 1 sont d'ordre multiplicatif égal à 41.

b) Montrer que 2 n'est pas un carré modulo p.

c) Alice et Bob décident d'utiliser le protocole de Diffie-Hellman dans le sous-groupe de $(\mathbb{Z}/p\mathbb{Z})^*$ engendré par engendré par $\alpha = 4$. Alice choisit l'exposant secret $a = 5$ et Bob l'exposant secret $b = 8$. Que s'échangent-ils sur le canal et quel est leur secret partagé à l'issue du protocole ?

d) Soit $P = 4^s = 65 \bmod 83$ une clé publique El Gamal dont on ne connaît pas la clé secrète associée s. Montrer que le couple $(44, 14)$ est une signature valide du message $M = 10 \bmod 83$.

– Exercice 2. Soit p un nombre premier, $p = 3 \bmod 4$. Soit Q l'ensemble des carrés de $\mathbb{Z}/p\mathbb{Z}$. Montrer que l'application $x \mapsto x^2$ est une bijection de Q dans Q et que son application réciproque est l'application $y \mapsto y^{(p+1)/4}$.

– Exercice 3. On considère le système RSA associé au modulo $n = pq$. Soit e l'exposant public. Soit d_1 l'inverse de e modulo $p-1$ et soit d_2 l'inverse de e modulo $q-1$. Soit C le chiffré RSA du message en clair M.

a) Comment peut-on calculer M à partir de $C^{d_1} \bmod p$ et $C^{d_2} \bmod q$? Il y a-t-il une économie de calcul par rapport au déchiffrement RSA standard ?

b) Supposons qu'une machine, par exemple une carte à puce, soit programmée pour déchiffrer de cette manière. Supposons qu'il soit possible de demander à la machine le déchiffrement de cryptogrammes C arbitraires. Supposons enfin, qu'on puisse provoquer une erreur dans le calcul de $C^{d_1} \bmod p$: montrer alors comment en déduire les facteurs premiers p, q de n.

– Exercice 4. Soient p et q deux nombres premiers que l'on suppose tels que $p = 3 \bmod 4$ et $q = 3 \bmod 4$. Soit $n = pq$. Soit λ le plus petit commun multiple de $p-1$ et $q-1$.

a) Démontrer que pour tout $x \in (\mathbb{Z}/n\mathbb{Z})^*$ on a $x^\lambda = 1 \mod n$.

b) Montrer que si le symbole de Jacobi $\left(\frac{x}{n}\right) = -1$, alors $x^{\lambda/2}$ est une racine carrée de 1, différente de 1 et de -1.

c) Soient e et d des exposants RSA, publics et secrets respectivement. Montrer que $ed - 1$ est un multiple de λ.

d) Supposons que 2^j divise $ed-1$ et que $(ed-1)/2^j$ soit impair : alors montrer que $(ed-1)/2^j$ est un multiple de $\lambda/2$ mais pas de λ.

e) En déduire que si $\left(\frac{x}{n}\right) = -1$, alors $x^{(ed-1)/2^j}$ est une racine carrée de 1 modulo n, différente de 1 et de -1.

f) En déduire un procédé pour trouver les facteurs premiers p et q à partir de n, e, d.

– EXERCICE 5. Soit α un élément primitif modulo un premier p. Soit f la fonction :

$$\begin{aligned} \{1,\dots,p-1\} &\rightarrow \{1,\dots,p-1\} \\ x &\mapsto \alpha^x \bmod p. \end{aligned}$$

Soit y un entier modulo p, non nul, fixé. Soit maintenant $\mathcal{N} = \{0,1\}^n$ l'ensemble des chaînes de n bits consécutifs. On va définir une application F, de $\mathcal{N}$ dans $\{1,\dots,p-1\}$ de la manière suivante. Soit $\varepsilon = (\varepsilon_1,\dots,\varepsilon_n) \in \mathcal{N}$. Soit $z_1, z_2, \dots, z_n$ la suite d'entiers calculée ainsi :

$$\begin{aligned} z_1 &= y^{\varepsilon_1}\alpha \bmod p \\ z_2 &= y^{\varepsilon_2}\alpha^{z_1} \bmod p \\ &\vdots \\ z_{i+1} &= y^{\varepsilon_{i+1}}\alpha^{z_i} \bmod p \\ &\vdots \\ z_n &= y^{\varepsilon_n}\alpha^{z_{n-1}} \bmod p. \end{aligned}$$

L'image de ε par la fonction F est maintenant définie comme :

$$F(\varepsilon) = z_n.$$

On dit que deux éléments $\varepsilon, \varepsilon'$ de $\mathcal{N}$ constituent une *collision* pour F si $F(\varepsilon) = F(\varepsilon')$. Noter que si n est choisi suffisamment grand, des collisions existent forcément.

Montrer que si un algorithme $\mathcal{A}$ permet de trouver une collision pour la fonction F, alors on peut en déduire un logarithme modulo p en base α de y.

– EXERCICE 6. Le chiffrement de Blum-Micali est un chiffrement à clé publique qui a pour clé secrète deux entiers premiers p et q, pour clé publique le produit $n = pq$ ansi qu'un non-carré y modulo n de symbole de Jacobi 1. Pour chiffrer un symbole binaire m, on choisit un entier modulo n aléatoire uniforme x, puis on chiffre m par $x^2 \bmod n$ si $m = 0$ et par $yx^2 \bmod n$ si $m = 1$.

On pose $n = 71 \times 83 = 5893$.

a) Trouver un y convenable : on pourra remarquer que 71 et 83 sont des entiers de Blum, i.e. égaux à 3 modulo 4.

b) Soit $M = (m_0, m_1, m_2, m_3)$ un message de 4 bits. On donne son chiffré $C = (4716, 764, 1123, 366)$. Comment obtenir le chiffré de $M + (1, 0, 0, 0)$?

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

– Exercice 7. On propose de construire le système de signature suivant : n est un entier de type RSA, produit de deux premiers, $n = pq$. Soit α un entier modulo n, d'ordre s premier. La clé publique d'Alice est le couple (n, α). La clé secrète est l'entier premier s. Pour signer un message M, Alice calcule $x = M^{-1} \bmod s$, puis calcule $S = \alpha^x \bmod n$. S est la signature du message M.

a) Montrer comment on peut vérifier l'authenticité de la signature S.

b) Montrer que s doit diviser $p - 1$ ou $q - 1$: si s divise $p - 1$ mais pas $q - 1$, montrer comment on peut factoriser n uniquement à partir de la clé publique.