Master CSI 1 — 2011-2012

Cryptologie, MA8W01 : Examen du 16 avril 2012

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 4 modulo 67 ?

b) Alice et Bob décident d'utiliser le protocole de Diffie-Hellman dans le sous-groupe de $(\mathbb{Z}/67\mathbb{Z})^*$ engendré par $\alpha = 4$. Alice choisit l'exposant secret $a = 7$ et Bob l'exposant secret $b = 10$. Que s'échangent-ils sur le canal et quel est leur secret partagé à l'issue du protocole ?

– **Solution.** L'ordre multiplicatif de 4 modulo 67 est 33. Alice et Bob échangent $4^7 = 36 \bmod 67$ et $4^{10} = 26 \bmod 67$. Leur secret partagé est $S = 4^{7\times 10} = 4^4 = 55 \bmod 67$.

– Exercice 2. Les paramètres publics d'un système d'El Gamal sont $(p, \alpha, P = \alpha^s \bmod p)$, où s est la clé secrète. Le système est utilisé pour signer des messages. Dans le cas où $p = 83$, $\alpha = 2$, $P = 11$, on est confronté à trois messages successifs, $10, 12, 17$, de signatures respectives $(45, 58)$, $(66, 10)$, $(47, 23)$.

a) Vérifier que $(45, 58)$ est bien une signature El Gamal du message $M = 10$.

b) On apprend que le générateur pseudo-aléatoire qui produit le premier terme u d'une signature (u, v) a pour effet de multiplier u par une constante a lorsqu'il s'agit de fabriquer la signature (u', v') du message suivant. Dans notre exemple on peut constater que $66 = 7\times 45 \bmod p$ et $47 = 7\times 66 \bmod p$. Montrer comment dans ce cas la connaissance de trois messages signés successifs permet de découvrir la clé secrète s.

c) Appliquer la méthode pour trouver la clé s correspondant à $P = 11$ de l'exemple.

– **Solution.**

a) Il s'agit de vérifier que $2^M = P^{45}45^{58} = 28 \bmod 83$.

b) Si on appelle M, M', M'' les trois messages consécutifs et (u, v), (u', v'), (u'', v'') leurs signatures respectives, on a :

$$M = us + kv$$
$$M' = u's + k'v'$$
$$M'' = u''s + k''v''$$

où $u = \alpha^k \bmod p$, et $u' = \alpha^{k'}, u'' = \alpha^{k''}$ respectivement. On fait l'hypothèse que $u'' = au' = a^2u$: écrivons $a = \alpha^x \bmod p$, on peut donc écrire $k' = k + x$ et $k'' = k + 2x$ pour obtenir le système :

$$\begin{aligned} M &= us + kv \\ M' &= u's + (k+x)v' \\ M'' &= u''s + (k+2x)v'' \end{aligned}$$

toutes ces égalités ayant lieu modulo l'ordre de α. Il s'agit d'un système de trois équations à trois inconnues, soit s, k et x. Sa résolution doit permetre de trouver s.

c) Dans ce cas particulier, le système ci-dessus devient, modulo 82 :

$$\begin{aligned} 10 &= 45s + k58 \\ 12 &= 66s + (k+x)10 \\ 17 &= 47s + (k+2x)23. \end{aligned}$$

En retranchant la première équation multipliée par $5 = 10/2$ à la deuxième multipliée par $29 = 58/2$, on obtient :

$$52 = 49s + 44x \tag{1}$$

puis en retranchant la première équation multipliée par 23 à la troisième multipliée par 58 on obtient :

$$18 = 51s + 44x. \tag{2}$$

Enfin, la différence de (1) et (2) donne le résultat, soit $s = 24 \bmod 82$.

– Exercice 3. On suppose que p est premier et que 2 est primitif modulo p.

a) Montrer que $2^{(p-3)/2} = (p-1)/2 \bmod p$.

b) Montrer que si $p = 1 \bmod 4$ alors $(p-3)/2$ est toujours inversible modulo $p - 1$.

c) On suppose la condition précédente réalisée. Soit $P = 2^s \bmod p$ la clé publique d'un utilisateur qui s'en sert pour réaliser des signatures El Gamal. En supposant que s est pair, montrer comment réaliser une signature valide (u, v) d'un message quelconque M, *sans connaître la clé secrète* s, en prenant $u = (p-1)/2$.

d) Adapter la méthode du cas précédent dans le cas où s est impair.

e) Application numérique : on prend $p = 61$ et $P = 2^s = 27 \bmod p$. Proposer une signature (u, v) valide du message $M = 5$ sans chercher à retrouver la clé secrète s.

– **Solution.**

a) Notons que $2^{(p-1)/2}$ est une racine carrée de 1 d'après le petit théorème de Fermat. Dire que 2 est primitif c'est dire que son ordre est $p-1$, donc $2^{(p-1)/2} \neq 1 \bmod p$, donc $2^{(p-1)/2} = -1 \bmod p$. On en déduit les égalités suivantes dans $\mathbb{Z}/p\mathbb{Z}$:

$$\begin{aligned} 2^{(p-3)/2} &= 2^{(p-1)/2}2^{-1} \\ &= -2^{-1} \\ &= (p-1)2^{-1} \\ &= \frac{p-1}{2}. \end{aligned}$$

b) On a $(p-1) - 2 \times (p-3)/2 = 2$. Donc le pgcd de $p-1$ et de $(p-3)/2$ divise 2. Mais si $p = 1 \bmod 4$ alors $(p-3)/2$ est impair et le pgcd de $p-1$ et de $(p-3)/2$ ne peut être que 1.

c) Il s'agit de trouver un couple (u, v) vérifiant

$$2^M = P^u u^v \bmod p.$$

En prenant $u = (p-1)/2$ l'équation devient

$$\begin{aligned} 2^M &= 2^{s(p-1)/2}\left(\frac{p-1}{2}\right)^v \\ &= \left(2^{(p-1)/2}\right)^s \left(2^{(p-3)/2}\right)^v \\ &= (-1)^s 2^{v(p-3)/2} = 2^{v(p-3)/2}. \end{aligned}$$

Il suffit donc de poser

$$v = M\left(\frac{p-3}{2}\right)^{-1} \bmod (p-1)$$

ce qui est toujours possible d'après la question précédente.

d) Dans ce cas il s'agit d'obtenir

$$\begin{aligned} 2^M &= (-1)^s 2^{v(p-3)/2} = -2^{v(p-3)/2} \\ &= 2^{(p-1)/2}2^{v(p-3)/2}. \end{aligned}$$

Il suffit donc de poser

$$v = \left(M - \frac{p-1}{2}\right)\left(\frac{p-3}{2}\right)^{-1} \bmod (p-1)$$

e) On ne sait pas si s est pair ou impair, mais on peut toujours essayer chacun des cas et tester s'ils marchent. Ici, si on suppose pour commencer que s est pair, on prend $u = 30$, et

$$v = 5(29^{-1}) = 25 \bmod 60$$

et on constate que $(30, 25)$ est une signature valide de $M = 5$.

– Exercice 4. On considère un système à clé publique de type El Gamal où les données publiques sont (p, α, P) avec $P = \alpha^s \bmod p$ où s est la clé secrète.

a) En choisissant u de la forme $P^x\alpha^y$, montrer comment fabriquer, sans connaître la clé secrète s, un triplet (M, u, v) tel que (u, v) soit une signature valide du message M.

b) Le faire avec $p = 53, \alpha = 2, P = 48$. On évitera le message $M = 0$.

– **Solution.**

a) Il s'agit de trouver un triplet (M, u, v) qui vérifie

$$\alpha^M = P^u u^v \bmod p.$$

En choisissant x, y arbitrairement et en posant $u = P^x\alpha^y \bmod p$, l'équation de vérification s'écrit :

$$\begin{aligned}\alpha^M &= P^u \left(P^x\alpha^y\right)^v \\ &= P^{u+xv}\alpha^{yv}.\end{aligned}$$

Il suffit donc de poser $v = -ux^{-1} \bmod (p-1)$ (ce qui veut dire que l'on a choisi x inversible modulo $(p-1)$) pour que l'on ait $P^{u+xv} = 1$ puis enfin on choisit tout simplement

$$M = yv \bmod (p-1)$$

et le couple (u, v) est une signature valide de M.

b) En prenant $x = 1, y = 2$, on trouve que $(33, 19)$ est une signature valide de $M = 38$.

– Exercice 5.

a) Soit $n = 3 \times 5 \times 7 = 105$. Utiliser le théorème chinois pour trouver toutes les racines carrées de 1.

b) Plus généralement, si $n = pqr$ où p, q, r sont des nombres premiers, combien y a-t-il de carrés dans $(\mathbb{Z}/n\mathbb{Z})^*$?

c) Combien y a-t-il dans $(\mathbb{Z}/n\mathbb{Z})^*$ de non carrés x de symbole de Jacobi $\left(\frac{x}{n}\right) = 1$?

– **Solution.**

a) On calcule $70x + 21y + 15z \bmod 105$ pour tous les huit $(x, y, z) \in \{1, -1\}^3$. On trouve $1, 76, 64, 34, 71, 41, 29, 104$.

b) Comme chaque carré a huit racines, il y en a $\phi(n)/8 = (p-1)(q-1)(r-1)/8$.

c) L'ensemble se partitionne en trois parties : les carrés mod p qui sont des non-carrés mod q, r, les carrés mod q qui sont des non-carrés mod p, r, les carrés mod r qui sont des non-carrés mod p, q. Il y en a donc en tout

$$3\frac{p-1}{2}\frac{q-1}{2}\frac{r-1}{2} = \frac{3}{8}(p-1)(q-1)(r-1).$$

– EXERCICE 6. Soient p et q deux nombres premiers tels que que $p' = (p-1)/2$ et $q' = (q-1)/2$ soient encore des nombres premiers. Soit $n = pq$. Soit n une clé publique et (p,q) la clé secrète associée. On considère la variante suivante de signature RSA : une signature S d'un message M, $1 \leqslant M \leqslant n-1$, est valide si

$$S^M = M \bmod n.$$

a) Montrer que si M est impair et premier avec p' et q' alors M admet une signature valide : expliquer comment on la construit grâce à la clé secrète.

b) Soient $p = 23$ et $q = 47$, $n = pq = 1081$. Trouver une signature valide de $M = 5$.

c) Montrer que si l'on obtient la signature d'un message x ainsi que la signature d'un message $y = Mx$, alors on sait trouver la signature du message M sans connaître la clé secrète.

– **Solution.**

a) Si M est impair et premier avec p' et q' alors M est premier avec $p-1 = 2p'$ et $q-1 = 2q'$ et est donc inversible modulo $\phi(n) = (p-1)(q-1) = 4p'q'$. En posant $X = M^{-1} \bmod \phi(n)$ et $S = M^X \bmod n$ on obtient une signature valide car $S^M = M^{MX} = M$ d'après le théorème de Fermat-Euler $M^{\phi(n)} = 1 \bmod n$.

Ou encore : pour avoir $S^M = M \bmod n$ il suffit d'avoir S' et S'' tels que $S'^M = M \bmod p$ et $S''^M = M \bmod q$ et $S = S' \bmod p$ et $S = S'' \bmod q$. On calcule $S' = M^{X'} \bmod p$ et $S'' = M^{X''} \bmod q$ où $X' = M^{-1} \bmod (p-1)$ et $X'' = M^{-1} \bmod (q-1)$ puis on reconstitue S grâce au théorème chinois.

b) Le calcul donne $X' = 9 \bmod 22$, $X'' = 37 \bmod 46$ puis $S' = 11$ et $S'' = 20$. Enfin l'identité de Bézout $47 - 2.23 = 1$ nous donne $S = 11.47 - 46.20 = 678 \bmod n$

– EXERCICE 7. Soient p et q deux nombres premiers et $n = pq$. On considère encore une variante de signature RSA, où la clé publique est un couple (n, g), g étant un entier de $(\mathbb{Z}/n\mathbb{Z})^*$ d'ordre r secret. La clé secrète est l'entier r. La signature d'un message $M \in \mathbb{Z}/n\mathbb{Z}$ est un entier S tel que :

$$S^M = g \bmod n.$$

Il peut y avoir des entiers M qui n'admettent pas de signature mais on choisit les paramètres de telle sorte que ces cas soient suffisamment rares.

a) Expliquer comment la connaissance de la clé secrète r permet de signer des messages.

b) On suppose r premier. Montrer que r doit être un diviseur, soit de $p-1$, soit de $q-1$.

c) Toujours dans le cas où r est premier, on suppose que r est un diviseur de $p-1$, mais pas de $q-1$. Montrer comment on peut retrouver les facteurs p et q grâce à un calcul de pgcd.

d) Montrer que si r est un diviseur de $p-1$ et de $q-1$, alors r est un diviseur de $n-1$.

e) On suppose toujours que r est premier, et cette fois que r est un diviseur de $p-1$ *et* de $q-1$. Montrer que si a est l'inverse de M modulo $(n-1)$, alors $\sigma = g^a \bmod n$ est une signature valide de M.

f) Comment l'entier r doit-il être choisi pour espérer avoir un procédé de signature solide ? Qu'est-ce que cela implique sur le choix des nombres premiers p et q ?

– **Solution.**

a) Il suffit de calculer $X = M^{-1} \bmod r$ et $S = g^X$ est une signature valide.

b) On sait que $g^{\phi(n)} = g^{(p-1)(q-1)} = 1$. L'ordre r de g doit donc être un diviseur de $(p-1)(q-1)$. Si r est premier r doit donc diviser $(p-1)$ ou $(q-1)$.

c) On a $n = pq = q+(p-1)q = q \bmod r$. Donc $g^n = g^q \bmod n$ et par conséquent $g^n = g^q = g \bmod q$. Donc $g^n - g$ est un multiple de q. Par ailleurs si $g^n - g$ était aussi un multiple de p, on aurait $g^n - g = 0 \bmod n$ et $g^{n-1} = 1 \bmod n$. Ceci impliquerait $r|(n-1)$ et donc $n-1 = q-1+(p-1)q = 0 \bmod r$, donc $q-1 = 0 \bmod r$ ce qui est contraire à l'hypothèse sur r. Donc le calcul du pgcd de n et de $g^n - g \bmod n$ doit donner q.

d) $n-1 = (p-1)(q-1)+(p-1)+(q-1)$.

e) Si r divise $p-1$ et $q-1$ alors r divise $n-1$. En remarquant que si $aM = 1 \bmod (n-1)$ alors $aM = 1 \bmod r$ on obtient que $\sigma^M = g^{aM \bmod r} = g \bmod n$

f) On a vu que si r est premier, toutes les configurations possibles mènent à des faiblesses. L'entier r doit donc être composé. De plus, r ne peut diviser $p-1$ (ou $q-1$), donc certains de ses facteurs doivent être des diviseurs de $p-1$ et d'autres de $q-1$.