École normale supérieure **2019-2020**
Département d'informatique

Introduction à la cryptologie
TD n° 7 : Correction.

Exercice 1 (Échauffement)**.**

1. Si les deux propriétés sont vraies pour tout générateur, trivialement il existe un générateur tel qu'elles sont vraies (on suppose $\mathbb{G}$ non vide). Réciproquement, supposons qu'il existe un générateur g tel que les deux propriétés sont vraies. Soit $h = g^x$ un générateur de $\mathbb{G}$. On a :
   - $e(h,h) = e(g,g)^{x^2} \neq 1$; en effet $e(g,g) \neq 1$, donc comme $\mathbb{G}_T$ est cyclique, $e(g,g)$ est générateur, et d'autre part $x \neq 0$ puisque g^x est générateur, donc $e(g,g)^{x^2} \neq 1$.
   - $e(h^a, h^b) = e(g,g)^{x^2ab} = e(h,h)^{ab}$.
2. Soit un triplet (g^a, g^b, g^c). On veut vérifier si $c = ab$ (modulo p). Pour cela, il suffit de vérifier :

$$e(g^a, g^b) \stackrel{?}{=} e(g^c, g).$$

   En effet, l'égalité est vraie ssi $e(g,g)^{ab} = e(g,g)^c$, ssi $ab = c \bmod p$ parce que $e(g,g) \neq 1$ et le groupe est cyclique, ce qui implique que $e(g,g)$ est générateur donc l'égalité $e(g,g)^{ab} = e(g,g)^c$ ne peut avoir lieu que si les exposants sont égaux mod p.

Exercice 2 (Échange de clef sans interaction à trois participants)**.**

1. A, B, C tirent respectivement une valeur uniformément aléatoire a, b, c, et publient respectivement g^a, g^b, g^c. Pour trouver le secret commun A, B, C calculent respectivement $e(g^b, g^c)^a$, $e(g^a, g^c)^b$, $e(g^a, g^b)^c$. Les propriétés du couplage e garantissent que ces trois valeurs sont égales à $e(g,g)^{abc}$, les trois parties obtiennent donc bien une valeur commune. D'autre part, un adversaire qui observe les communications obtient g^a, g^b, g^c. Retrouver le secret commun $e(g,g)^{abc}$ est difficile pour lui, puisqu'il s'agit exactement d'une instance du problème de Diffie-Hellman bilinéaire.
2. Supposons qu'on a $n+1$ participants $A_1, \ldots, A_{n+1}$. Le participant A_k tire a_k uniformément aléatoirement et publie g^{a_k}. Après avoir reçu g^{a_i} pour $i \neq k$ des autres participants, il calcule le secret commun :

$$e_n(g_1^a, \ldots, g^{a_{k-1}}, g^{a_{k+1}}, \ldots, g^{a_{n+1}})^{a_k} = e_n(g, \ldots, g)^{a_1 \cdots\cdots a_{n+1}}.$$

   La sécurité de ce protocole repose sur une variante « multilinéaire » du problème de Diffie-Hellman : calculer $e(g, \ldots, g)^{a_1 \cdots\cdots a_{n+1}}$ à partir de g^{a_1}, …, $g^{a_{n+1}}$.

Exercice 3 (Poignées de main secrètes)**.**

1. Soient a, b tels que $\mathsf{id}_A = g^a$, $\mathsf{id}_B = g^b$. Alors $e(\mathsf{id}_A^s, \mathsf{id}_B) = e(g,g)^{abs} = e(\mathsf{id}_A, \mathsf{id}_B^s)$, donc les deux participants peuvent calculer cette valeur, ce qui leur permet de vérifier ce qu'a envoyé l'autre.
2. Sans les nonces, on suppôt de l'état qui écoute la conversation peut retenir par exemple tout ce que A envoie à B, et le répéter plus tard pour se faire passer pour A auprès de B, et en particulier lui faire croire qu'il fait partie de la société secrète. C'est une attaque dont l'application est très générale en sécurité informatique, appelée attaque par rejeu.
3. Les deux participants peuvent calculer $H(e(\mathsf{id}_A, \mathsf{id}_B^s) \parallel n_A \parallel n_B \parallel 2)$ et l'utiliser comme secret commun. Le vil attaquant qui écoute la conversation ne peut pas plus calculer cette valeur que les précédentes.

Exercice 4 (Sécurité des signatures de Boneh-Boyen)**.**

1. Pour une signature légitime on a :
$$e(\sigma, ug^m) = e(g^{(x+m)^{-1}}, g^{x+m}) = e(g,g) = g_T.$$
La signature est donc acceptée.

2. Soit $(h_0, \ldots, h_q) \in \mathbb{G}^{q+1}$. Pour vérifier qu'il s'agit d'une instance de q-SDH, on procède par récurrence. Si $q = 0$, il suffit de vérifier que h_0 est générateur, donc simplement vérifier $h_0 \neq 1$ puisqu'on est dans un groupe cyclique. Pour $q > 0$, supposons qu'on a vérifié par récurrence que $(h_0, \ldots, h_{q-1})$ est une instance de $(q-1)$-SDH. Alors il suffit de vérifier $e(h_0, h_q) = e(h_1, h_{q-1})$. En effet, posons $h_0 = g$, $h_1 = g^x$, $h_{q-1} = g^y$, $h_q = g^z$. Alors l'égalité précédente est vraie ssi $z = xy \bmod p$. Or par récurrence on sait que $y = x^{q-1}$. On déduit $z = g^x$, CQFD.
Supposons maintenant qu'on a une solution prétendue à une instance q-SDH $(g, g^x, g^{x^2}, \ldots, g^{x^q})$. On a donc une paire (m, h) et on souhaite vérifier $h = g^{(x+m)^{-1}}$. Pour cela, il suffit de vérifier $e(h, g^x g^m) = e(g,g)$. Noter que h, g^x, g, m sont connus.

3. (a) En tirant plein parti de notre connaissance magique de x, lorsque l'adversaire demande la signature de m_k, nous pouvons lui renvoyer :
$$\sigma_i = h^{(x+m_k)^{-1}} = g^{\prod_{i \neq k}(x+m_i)}.$$
En fin de compte, l'adversaire forge une signature (m^*, σ^*) pour $m^* \notin \{m_i\}$. On a $\sigma^* = h^{(x+m^*)^{-1}}$. Pour répondre à l'instance q-SDH, on voudrait connaître $g^{(x+m^*)^{-1}}$ plutôt que $h^{(x+m^*)^{-1}}$. Pour cela, il suffit d'observer :
$$g^{(x+m^*)^{-1}} = \left(h^{(x+m^*)^{-1}}\right)^{\prod (x+m_i)^{-1}}.$$
La réponse à l'instance q-SDH est $(m^*, g^{(x+m^*)^{-1}})$.
Remarque. Bien sûr avec notre connaissance magique de x on aurait pu calculer cela directement. Mais on souhaite quand même utiliser la sortie de l'adversaire, pour mieux se préparer au raisonnement qui suit, où on ne connaît plus x.

   (b) Une observation critique est la suivante : l'instance q-SDH $(g, g^x, g^{x^2}, \ldots, g^{x^q})$ nous permet de calculer $g^{P(x)}$ pour n'importe quel polynôme P de degré au plus q à coefficients connus. En effet, si $P(X) = \sum_{i \leq q} a_i X^i$, alors
$$g^{P(x)} = \prod_{i \leq q} (g^{x^i})^{a_i}.$$
En particulier, même sans connaître x, l'instance q-SDH nous permet de calculer $h = g^{\prod(x+m_i)}$: en effet, en développant $\prod(X + m_i)$ on obtient un polynôme de degré q, dont on peut calculer les coefficients explicitement (puisque les m_i sont connus).

   (c) Avec la question précédente, on sait fournir à l'adversaire une signature valide des messages m_i. L'adversaire nous renvoie alors une signature $\sigma^* = h^{(x+m^*)^{-1}}$ d'un message $m^* \notin \{m_i\}$. Comme plus haut, il nous reste à déduire $g^{(x+m^*)^{-1}}$ pour avoir une solution $(m^*, g^{(x+m^*)^{-1}})$ à l'instance q-SDH. Pour calculer cette valeur, l'idée générale est la même que dans la question précédente, mais avec quelques étapes supplémentaires. On a
$$\begin{aligned} h^{(x+m^*)^{-1}} &= g^{\frac{\prod(x+m_i)}{x+m^*}} \\ &= g^{\frac{P_1(x+m^*)}{x+m^*}} && \text{pour un certain polynôme } P_1 \text{ connu de degré } q \\ &= g^{P_2(x+m^*)+\frac{c}{x+m^*}} && \text{pour } P_2 \text{ connu de degré } q-1 \text{ et une constante } c. \end{aligned}$$
Par la question précédente, nous savons calculer $g^{P_2(x+m^*)}$ (noter que m^* est connu), donc on trouve :
$$g^{(x+m^*)^{-1}} = \left(h^{(x+m^*)^{-1}} g^{-P_2(x+m^*)}\right)^{c^{-1}}.$$

Exercice 5 (Chiffrement basé sur l'identité sans couplage)**.**

1. Par le théorème des restes chinois, $\mathbb{Z}_N \sim \mathbb{Z}_p \times \mathbb{Z}_q$, en particulier x est un résidu quadratique modulo N ssi c'est un résidu modulo p et q. Supposons $\left(\frac{a}{N}\right) = 1$. On a $\left(\frac{a}{N}\right) = \left(\frac{a}{p}\right)\left(\frac{a}{q}\right)$ donc soit $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right) = 1$, soit $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right) = -1$. Dans le premier cas, a est un résidu quadratique modulo p et q, donc c'est un résidu quadratique modulo N. Dans le second cas, a n'est pas un résidu modulo p, ni modulo q. Montrons que dans ce cas, $-a$ est un résidu quadratique modulo p et q. Par hypothèse, $p \equiv q \equiv 3 \bmod 4$, donc $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = -1$, donc -1 n'est pas un résidu quadratique. D'autre part $\mathbb{Z}_p$ est un corps donc $\mathbb{Z}_p^*$ est un groupe cyclique, et $x \mapsto -x$ est une bijection entre les résidus et non-résidus quadratiques de $\mathbb{Z}_p^*$. On déduit que $-a$ est bien un résidu quadratique modulo p, de même modulo q, donc c'est un résidu quadratique modulo N.
2. Comme $\left(\frac{a}{N}\right) = 1$, a est dans $\mathbb{Z}_N^*$. On peut donc poser $r^2 = \epsilon a$ pour un certain ϵ. Notre but est de montrer $\epsilon = \pm 1$. On a
$$\epsilon = r^2/a = a^{(\phi(N)+4)/4-1} = a^{\phi(N)/4}.$$
En particulier, modulo p on obtient :
$$\epsilon = a^{\phi(N)/4} = \left(a^{(p-1)/2}\right)^{(q-1)/2} = \left(\frac{a}{p}\right)^{(q-1)/2} = \left(\frac{a}{p}\right) \bmod p$$
où la dernière égalité utilise $\left(\frac{a}{p}\right) = \pm 1$, et $q \equiv 3 \bmod 4$. De même par symétrie on a $\epsilon = \left(\frac{a}{q}\right) \bmod q$. Par ailleurs, comme $\left(\frac{a}{N}\right) = 1$, on a $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$, donc on déduit $\epsilon \bmod p = \epsilon \bmod q = \pm 1$, donc $\epsilon = \pm 1 \bmod N$, comme voulu.
3. On suppose $r^2 = a \bmod N$; l'autre cas est similaire. En suivant l'indication, on a
$$c_1 + 2r = t_1 + a t_1^{-1} + 2r = \frac{1}{t_1}(t_1^2 + 2rt_1 + a) = \frac{1}{t_1}(t_1 + r)^2.$$
On déduit $m = \left(\frac{t_1}{N}\right) = \left(\frac{c_1+2r}{N}\right)$. L'algorithme de déchiffrement consiste simplement à calculer cette dernière valeur. C'est possible puisqu'il suffit de calculer $c_1 + 2r$, puis un symbole de Jacobi. Noter que calculer efficacement un symbole de Jacobi ne nécessite pas d'information secrète (en particulier, pas besoin de la factorisation de N).