Master CSI 2 — 2013-2014

Cryptographie avancée : Examen du 16 décembre 2013

Durée : 3h. Sans document. Les exercices sont indépendants.

– EXERCICE 1. Soient g et h deux entiers d'ordre $q|p-1$ modulo un premier p publics.

Alice s'engage auprès de Bob en lui fournissant l'entier $E \bmod p$. Elle souhaite convaincre Bob qu'elle connaît deux entiers r et x tels que

$$E = g^r h^x \bmod p.$$

Proposer un protocole en trois passes de la forme :
- Alice fournit à Bob un entier z modulo p,
- Bob fournit à Bob un bit $\varepsilon = 0, 1$,
- Alice révèle à Bob deux entiers u et v modulo q.

Montrer que votre protocole démontre la connaissance de r et x et est complet, valide, et sans divulgation.

– EXERCICE 2. Soient g_1, g_2, g_3 trois générateurs d'un sous-groupe multiplicatif G de $\mathbb{Z}/p\mathbb{Z}$ d'ordre q premier. Soit donné un triplet (y_1, y_2, y_3) d'éléments de G. Proposer un protocole sans divulgation qui démontre l'existence d'un entier x modulo q tel que l'on ait simultanément :

$$y_1 = g_1^x \bmod p, \quad y_2 = g_2^x \bmod p, \quad y_3 = g_3^x \bmod p.$$

Montrer que votre protocole est bien complet, valide et sans divulgation.

– EXERCICE 3. Soient g et h deux générateurs d'un sous-groupe multiplicatif G de $\mathbb{Z}/p\mathbb{Z}$ d'ordre q premier. Soit donné un triplet (y, z_1, z_2), d'éléments de G. Le protocole suivant est destiné à démontrer qu'il existe un entier x modulo q tel que $y = g^x \bmod p$ et
- soit $z_1 = h^x \bmod p$,

– soit $z_2 = h^x \bmod p$.

Le protocole se déroule ainsi :

– le prouveur P envoie au vérificateur V quatre éléments de G, soient u_1, v_1, u_2, v_2,
– le vérificateur renvoie un entier c modulo q,
– le prouveur envoie quatre entiers c_1, c_2, w_1, w_2 modulo q tels que
  – $c_1 + c_2 = c \bmod q$,
  – $g^{w_1} = u_1 y^{c_1}$ et $h^{w_1} = v_1 z_1^{c_1}$,
  – $g^{w_2} = u_2 y^{c_2}$ et $h^{w_2} = v_2 z_2^{c_2}$.

a) Montrer que le protocole est complet. On montrera par exemple que si $h^x = z_1$, alors le prouveur peut avoir préparé u_2 et v_2 sous la forme $u_2 = g^{w_2} y^{-c_2}$ et $v_2 = h^{w_2} z_2^{-c_2}$.

b) Montrer que le protocole est valide. On montrera que si le prouveur est capable de répondre à deux défis distincts c et c' par deux réponses satisfaisantes (c_1, c_2, w_1, w_2) et (c'_1, c'_2, w'_1, w'_2), alors
  – soit $c_1 \neq c'_1$, et dans ce cas on doit avoir $y = g^x$ et $h^x = z_1$ pour un même x,
  – soit $c_2 \neq c'_2$, et dans ce cas on doit avoir $y = g^x$ et $h^x = z_2$.

c) Montrer que le protocole est sans divulgation. En particulier, le vérificateur ne sait pas lequel des deux entiers, z_1 ou z_2, est égal à h^x avec $y = g^x$.

– EXERCICE 4. Soit p un nombre premier et g un élément d'ordre q dans $(\mathbb{Z}/p\mathbb{Z})^*$, pour un diviseur q de $p-1$ donné. Soit G le sous-groupe multiplicatif de $(\mathbb{Z}/p\mathbb{Z})^*$ engendré par g. On rappelle que le problème de Diffie-Hellman décisionnel consiste à savoir décider si, étant donnés g^a et g^b, un troisième élément z du groupe G est ou non égal à $g^{ab} \bmod p$.

On souhaite construire un protocole de transfert inconscient. Alice dispose de deux secrets s_1 et s_2, éléments de $(\mathbb{Z}/p\mathbb{Z})$. Bob souhaite acquérir un des deux, disons s_i, sans qu'Alice découvre la valeur de i. On procède ainsi :

– Bob choisit deux entiers modulo q aléatoires a et b, puis il communique à Alice quatre entiers modulo p,

$$(g^a, g^b, Z_1, Z_2).$$

– Alice *vérifie que* $Z_1 \neq Z_2 \bmod p$ (si $Z_1 = Z_2$ elle interrompt le protocole) puis choisit deux entiers modulo q aléatoires u et v et communique à Bob trois entiers modulo p, soit w, $s_1 + x_1$ et $s_2 + x_2$, où :

$$w = (g^a)^u g^v$$
$$x_1 = Z_1^u (g^b)^v$$
$$x_2 = Z_2^u (g^b)^v.$$

a) Trouver une valeur de Z_1 (respectivement Z_2) qui permet à Bob d'obtenir x_1 (resp. x_2) et par conséquent s_1 (resp. s_2).

b) Montrer que si Bob a utilisé cette valeur pour Z_1 (par exemple) alors, quelle que soit la valeur de Z_2, il n'a aucune information sur x_2 (et donc sur l'autre secret s_2), ceci même si Bob est suffisamment puissant pour savoir calculer des logarithmes modulo p. On montrera donc que toutes les valeurs possibles de x_2 sont compatibles avec toutes les données dont dispose Bob.

c) Montrer que si Alice sait quel est le secret que Bob obtient par ce procédé, alors elle sait résoudre le problème de Diffie-Hellman décisionnel.

d) Montrer que le protocole de l'exercice 3 permet de contraindre Bob à suivre le présent protocole sans possibilité de tricher, c'est-à-dire en obtenant exactement un des deux secrets et rien sur l'autre.

– EXERCICE 5. On suppose que l'on dispose d'un protocole $\mathcal{P}$ de transfert inconscient d'un secret de $\{0,1\}^\ell$ parmi deux. On souhaite réaliser le transfert inconscient d'un secret parmi trois secrets appelés a, b, c et également dans $\{0,1\}^\ell$.

a) Montrer, comment en appliquant deux fois le protocole $\mathcal{P}$ à deux paires de secrets, x, y d'une part et z, t d'autre part, et en ayant décomposé a, b, c en sommes bien choisies d'éléments de $\{x, y, z, t\}$, on peut réaliser le transfert inconscient d'un secret de $\{a, b, c\}$. On montrera notamment que le récepteur n'a aucune information sur au moins deux des trois secrets.

b) Pouvez-vous généraliser votre protocole à un transfert inconscient d'un secret parmi $n > 3$? Montrer comment réaliser un transfert inconscient d'un secret parmi sept en trois applications du protocole $\mathcal{P}$.

– EXERCICE 6. Soit p un nombre premier et g un élément d'ordre q dans $(\mathbb{Z}/p\mathbb{Z})^*$, pour un diviseur q de $p-1$ donné. Soit G le sous-groupe multiplicatif de $(\mathbb{Z}/p\mathbb{Z})^*$ engendré par g. On rappelle que le problème de Diffie-Hellman décisionnel consiste à savoir décider si, étant donnés g^a et g^b, un troisième élément z du groupe G est ou non égal à $g^{ab} \bmod p$.

Soit $h : (\mathbb{Z}/p\mathbb{Z})^* \to \{0,1\}^n$ une fonction de hachage. Soit s un entier modulo q et soit $P = g^s \in \mathbb{Z}/p\mathbb{Z}$. Les données (p, q, g, P) sont publiques et s est une donnée secrète.

À un message clair $M \in \{0,1\}^n$ on associe le message chiffré dans $G \times \mathbb{Z}/p\mathbb{Z} \times \{0,1\}^n$

$$C = (g^r, xP^r, M + h(x))$$

où r et x sont des quantités choisies aléatoirement, respectivement dans $\mathbb{Z}/q\mathbb{Z}$ et dans $\mathbb{Z}/p\mathbb{Z}$, et où $+$ désigne l'addition bit à bit de n-uples binaires.

a) Montrer comment le détenteur du secret s déchiffre le cryptogramme C.

b) Montrer pourquoi, dans le modèle de l'oracle aléatoire, décrypter C est aussi difficile que de résoudre le problème de Diffie-Hellman décisionnel. On montrera que s'il existe un attaquant qui distingue si un chiffré est le chiffré de M_0 ou de M_1, alors on peut l'utiliser comme sous-programme pour construire un algorithme qui résoud le problème de Diffie-Hellman décisionnel. On supposera que l'attaquant mène une attaque à clair choisis (CPA).