Master CSI 2 2018-2019

Cryptologie Avancée — 4TCY903U

Responsables : G. Castagnos – G. Zémor

Devoir Surveillé — 22 octobre 2018

Documents non autorisés

Partie G. Castagnos

– **Exercice 1.** Soit k un paramètre de sécurité. Soit Gen un algorithme polynomial probabiliste qui prend en entrée 1^k et retourne $(p, n, q_0, q_1, g_0, g_1)$ avec $n = q_0 q_1$, $p = 2n + 1$, q_0, q_1 étant deux premiers distincts de k bits, p un nombre premier et g_0, g_1 deux éléments de $(\mathbf{Z}/p\mathbf{Z})^\times$ d'ordres respectifs q_0 et q_1.

Dans la suite, on notera $G_0 = \langle g_0 \rangle, G_1 = \langle g_1 \rangle, G$ les sous groupes de $(\mathbf{Z}/p\mathbf{Z})^\times$ d'ordres respectifs q_0, q_1 et n.

(a) Montrer que pour tout élément $x \in G$, il existe un unique couple $(x_0, x_1) \in G_0 \times G_1$ tel de $x = x_0 x_1$.

Étant donné une sortie de Gen, on considère le schéma de chiffrement asymétrique suivant. La clef publique est $pk = (p, n, g_0, g_1)$. Pour chiffrer $m \in G$, on tire deux entiers r_0 et r_1 uniformément dans $\{0, \ldots, n-1\}$, et on pose $c := (c_0, c_1) := (mg_0^{r_0}, mg_1^{r_1}) \in G \times G$.

(b) Donner une clef secrète et un algorithme de déchiffrement.

(c) On fait l'hypothèse suivante : étant donné (p, n, g_0, g_1) retourné par Gen, il est difficile de distinguer des couples d'éléments tirés uniformément dans $G_0 \times G_1$ de couples d'éléments tirés uniformément dans $G \times G$. Donner une formulation précise de cette hypothèse et montrer que ce schéma de chiffrement est sûr au sens IND – CPA (indistinguable pour des attaques à clairs choisis) sous cette hypothèse.

(d) On considère maintenant l'hypothèse suivante : étant donné (p, n, g_0, g_1) retourné par Gen et x un élément tiré uniformément dans G il est difficile de trouver $(x_0, x_1) \in G_0 \times G_1$ tel que $x = x_0 x_1$. Montrer que le schéma est sûr au sens OW – CPA (sens unique pour des attaques à clairs choisis) sous cette hypothèse.

– **Exercice 2.** Soit $N = pq$ un entier RSA et e premier avec $\varphi(N)$. Soit $\mathcal{A}$ un algorithme polynomial probabiliste ayant un succès $1/100$ pour résoudre le problème RSA : c'est à dire que si y est tiré uniformément dans $(\mathbf{Z}/N\mathbf{Z})^\times$, la probabilité que $\mathcal{A}$ sous l'entrée (N, e, y) retourne $x \in (\mathbf{Z}/N\mathbf{Z})^\times$ tel que $x^e = y$ est $1/100$.

Construire un algorithme polynomial probabiliste $\mathcal{B}$ utilisant $\mathcal{A}$, ayant un succès supérieur à $1 - e^{-5} \approx 0,99$ pour résoudre le problème RSA. Pour l'analyse de la probabilité de succès, on pourra utiliser le fait que pour tout réel z, $1 - z \leqslant e^{-z}$.

Partie G. Zémor

– **Exercice 3.** Soit n un entier et soient A et B deux entiers modulo n. Proposer un protocole en trois passes qui démontre simultanément que A et B sont des carrés modulo n. Le prouveur soumettra deux entiers modulo n, et le vérificateur renverra un défi constitué de deux bits. Montrer que le protocole est complet, valide, et sans divulgation.

– **Exercice 4.** Soit p un nombre premier et q un diviseur premier de $p - 1$. Soient g et h deux générateurs du sous-groupe multiplicatif d'ordre q de $\mathbf{Z}/p\mathbf{Z}$. Ces données sont considérées publiques, ainsi qu'un entier C modulo p . Un prouveur P souhaite démontrer qu'il est en possession d'un triplet (x, s, t) d'entiers modulo q tel que

$$\begin{aligned} C &= g^x h^s \mod p \\ C &= C^x h^t \mod p. \end{aligned}$$

On considère le protocole dont suit une description partielle. Son but est de démontrer l'existence et la possession par P d'un tel triplet.

- Le prouveur communique au vérificateur V trois entiers modulo p notés a, b, c.
- Le vérificateur renvoie un bit aléatoire $\varepsilon = 0, 1$.
- Le prouveur envoie trois entiers modulo q, soit α, β, γ. Si $\varepsilon = 0$, alors V vérifie que
$$g^\alpha = a, h^\beta = b, h^\gamma = c \mod p.$$

(a) Décrire la fin du protocole. Que vérifie V lorsque $\varepsilon = 1$?

(b) Montrer que ce protocole est complet, valide, et sans divulgation.

(c) On fait l'hypothèse qu'il est algorithmiquement difficile d'être en possession de deux couples distincts (u, v) et (u', v') d'entiers modulo q tels que $g^u h^v = g^{u'} h^{v'} \mod p$. Le prouveur prétend que son triplet (x, s, t) est tel que $x = 0$ ou $x = 1$. Pourquoi V le croit-il (après execution satisfaisante du protocole) ?

(d) Question bonus : comment peut-on justifier l'hypothèse précédente en supposant qu'il est difficile de trouver un entier e tel que $g^e = h \mod p$?