Exercice 1 : Algorithme de Shanks

Considérons un groupe multiplicatif $\mathbb{G}$ et plaçons-nous dans le sous-groupe $\langle g \rangle$ d'ordre connu q engendré par $g \in \mathbb{G}$ (autrement dit, nous avons $\langle g \rangle = \{1, g, g^2, \ldots, g^{q-1}\}$). Proposer un algorithme de résolution de logarithme discret par compromis temps-mémoire de complexité $O(\sqrt{q})$ opérations de groupe en temps et $O(\sqrt{q})$ éléments de groupe en mémoire.

Indication. On pourra remarquer que pour tout élément $h = g^x \in \langle g \rangle$, l'entier x s'écrit sous la forme $x = x_1 T + x_0$ avec $0 \leq x_0 < T$ et $0 \leq x_1 < T$ pour $T = \lceil \sqrt{q} \rceil + 1$.

Exercice 2 : Auto-réducibilité du logarithme discret

Soit $\mathbb{G}$ un groupe, et considérons le groupe cyclique d'ordre q engendré par $g \in \mathbb{G}$. Considérons enfin un algorithme $\mathcal{A}$ qui prend en entrée un élément de $\langle g \rangle$ et retourne un élément de $\mathbb{Z}_q$, en temps τ (dans le pire des cas). Supposons qu'il existe un sous-ensemble E de $\langle g \rangle$ avec $|E| \geq \epsilon q$ et $\epsilon \in]0, 1]$ pour lequel lorsque $\mathcal{A}$ est exécuté sur un élément $y \in E$, l'élément x retourné par $\mathcal{A}$ vérifie $g^x = y$.

Montrer qu'il existe un algorithme $\mathcal{B}$ qui résout le problème du logarithme discret dans $\langle g \rangle$ en un temps espéré $O(\tau/\epsilon)$.

Exercice 3 : Notions de sécurité

3.a] Supposons qu'on ait un système de chiffrement à clef publique qui soit sémantiquement sûr (IND-CPA). Démontrez qu'il n'existe pas d'algorithme polynomial capable de calculer la clef secrète à partir de la clef publique.

Un algorithme de chiffrement asymétrique est *sémantiquement sûr face aux attaques adaptatives à chiffré choisi* (≪ INDistinguishability under Adaptive Chosen Ciphertext Attack ≫ — IND-CCA2) si tout adversaire $\mathcal{A}$ fonctionnant en temps polynomial n'a qu'un avantage négligeable au jeu suivant, paramétré par un bit b :

1. Le challenger fabrique une paire de clefs (pk, sk) et transmet pk à $\mathcal{A}$.
2. $\mathcal{A}$ peut faire des calculs, et peut faire déchiffrer les messages de son choix par le challenger.
3. $\mathcal{A}$ envoie deux messages $M_0 \neq M_1$ au challenger.
4. Le challenger calcule $C \leftarrow \{M_b\}_{pk}$ puis envoie le chiffré C à $\mathcal{A}$.
5. $\mathcal{A}$ peut faire déchiffrer les messages de son choix par le challenger, tant qu'ils sont différents de C.
6. $\mathcal{A}$ renvoie un bit $\hat{b}$. Il ≪ gagne ≫ si $b = \hat{b}$.

3.b] Montrez que le chiffrement Elgamal n'est pas IND-CCA2 (il est pourtant sémantiquement sûr face à des *clairs* choisis).

Exercice 4 : Chiffrement commutatif et protocole à 3 passes

Un algorithme de chiffrement (symmétrique) est *commutatif* si $E(K_1, E(K_2, x)) = E(K_2, E(K_1, x))$. On suppose que tout le monde partage un grand nombre premier p. Chaque participant se choisit une clef secrète k au hasard dans l'ensemble $2, 3, \ldots, p-1$. La définition du chiffrement est :

$$E(k, x) = x^k \mod p \qquad (0 \leq x < p)$$

4.a] Le chiffrement est-il commutatif ?

4.b] Vous connaissez un autre mécanisme de chiffrement qui est commutatif. Lequel ?

4.c] Quelle est la complexité du chiffrement, en fonction de la taille de p ?

4.d] Comment peut-on faire pour déchiffrer ?

4.e] Pourquoi est-il difficile de récupérer la clef à partir d'*une* paire clair-chiffré *connue* ? Et de *deux* ?

Le ≪ protocole à 3 passes ≫de Shamir (inventé vers 1980) est le suivant. Les deux participants nommés A et B ont chacun une clef symétrique K_a et K_b, respectivement, qu'ils ne connaissent pas mutuellement. Avec un algortihme de chiffrement commutatif, A transmet un message chiffré à B :

— $A \to B : \{M\}_{K_a}$
— $B \to A : \{\{M\}_{K_a}\}_{K_b}$
— $A \to B : \{M\}_{K_b}$

4.f] Comment A calcule le 3ème message ? Comment B récupère M à la fin ?

4.g] Ce protocole est-il sûr face à des adversaires actifs ?

Exercice 5 : Sécurité sémantique du chiffrement Elgamal

Considérons le groupe $\mathbb{Z}_p^\times$ (il est cyclique) muni d'un de ses générateurs g (une ≪ racine primitive modulo p ≫).

5.a] g peut-il être un résidu quadratique ? (supposer que c'est vrai ; qu'est-ce qui se passe ?)

5.b] A quelle condition sur x est-ce que g^x est un résidu quadratique ?

5.c] Considérons un triplet Diffie-Hellman (u, v, w). Si w est un résidu quadratique, que peut-on dire de u et v ?

5.d] Même question si w n'est pas un résidu quadratique ?

5.e] Déduisez-en un algorithme qui obtient un avantage non-négligeable pour résoudre le problème DDH sur le groupe.

5.f] Quelles sont les conséquences sur le chiffrement Elgamal ?

5.g] Pour éviter ce problème, on peut faire le chiffrement Elgamal en remplaçant g par g^2. Qu'est-ce que ça change ?

Exercice 6 : Signature de Schnorr en présence de *nonce-reuse*

Montrez qu'un adversaire qui dispose de la clef publique et deux signatures σ_1 et σ_2 de deux messages $M_1 \neq M_2$ peut aisément calculer la clef secrète du signataire.