On rappelle qu'on utilise la notation $x \leftarrow U(\mathcal{X})$ pour signifier que x est tiré uniformément au hasard dans $\mathcal{X}$. La difficulté des questions posées ci-dessous est, elle, non uniforme. Le barême final en tiendra compte.

Résistance aux collisions

Soit G un groupe cyclique d'ordre q premier et g un générateur. On considère une famille de fonctions de hachage définie par exponentiation dans le groupe G, dont on va prouver la résistance aux collisions en supposant la difficulté du problème du logarithme discret. On rappelle qu'une *collision* est une paire d'entrées *distinctes* ayant la même sortie.

On considère le jeu suivant $\mathcal{G}$ entre un challenger $\mathcal{C}$ et un adversaire $\mathcal{A}$:

- Le challenger $\mathcal{C}$ choisit $a \leftarrow U(\mathbb{Z}_q)$ et envoie $h := g^a$ à $\mathcal{A}$
- La valeur h définit une fonction de hachage $H : \mathbb{Z}_q^2 \to G$ par $H(x, y) := g^x h^y$
- $\mathcal{A}$ renvoie $(x, y), (x', y')$ et gagne le jeu s'il s'agit d'une collision de H

L'avantage de $\mathcal{A}$ est simplement défini par sa probabilité de gagner au jeu.

Question 1. *Soit $(x, y), (x', y')$ une collision de H. Montrer qu'on peut en déduire a efficacement.*

Question 2. *Écrire un jeu de sécurité $\mathcal{G}'$, joué entre un adversaire et un challenger, correspondant au problème du logarithme discret, et définir l'avantage de l'adversaire dans ce jeu.*

Question 3. *Soit $\mathcal{A}$ un adversaire dans le jeu $\mathcal{G}$. Construire un adversaire $\mathcal{B}$ jouant au jeu $\mathcal{G}'$ et exprimer son avantage en fonction de celui de $\mathcal{A}$. Conclure.*

Auto-réducibilité aléatoire

Soit G un groupe cyclique d'ordre q premier et g un générateur. On suppose qu'il existe un algorithme $\mathcal{A}$ prenant en entrée un élément de G et renvoyant son logarithme discret, qui réussit avec probabilité ε :

$$\Pr_{u \leftarrow U(G)} [\mathcal{A}(u) = DL(u)] = \varepsilon \ .$$

Où cette probabilité est sur le choix uniforme de u et les choix aléatoires dans $\mathcal{A}$.

Question 4. *Soit $F \subseteq G$ l'ensemble des u tels que $\Pr[\mathcal{A}(u) = DL(u)] = 0$, c'est-à-dire que $\mathcal{A}$ échoue totalement sur l'entrée u. Quelle est la taille maximale de F ?*

Question 5. *Soit $u \in G$ fixé. On tire $\sigma \leftarrow U(\mathbb{Z}_q)$. Justifier rapidement que $u \cdot g^\sigma$ est distribué uniformément au hasard dans G.*

Question 6. *En déduire un algorithme $\mathcal{B}$ tel que, pour tout $u \in G$:*

$$\Pr[\mathcal{B}(u) = DL(u)] = \varepsilon$$

où la probabilité est prise sur les choix aléatoires dans $\mathcal{B}$ uniquement.

On a ainsi démontré une réduction du *pire cas* au *cas moyen* pour le problème du logarithme discret.

Problème de domaine dans ElGamal

Soient p, q des nombres premiers tels que $q := (p-1)/2$. On sait que $\mathbb{Z}_p^*$ est d'ordre $p-1 = 2q$ et contient donc un unique sous-groupe d'ordre q noté G. On admet que ce sous-groupe est l'ensemble des éléments de $\mathbb{Z}_p^*$ qui sont des carrés modulo p, i.e., de la forme g^a où g est un générateur de $\mathbb{Z}_p^*$ et a est pair.

On considère la version suivante du cryptosystème ElGamal.

Cryptosystème ElGamal dans $\mathbb{Z}_p^*$

KeyGen :

- Choisir $a \leftarrow U(\mathbb{Z}_p^*)$ (différent de 1) et calculer $g = a^2 \bmod p$ un générateur de G
- Choisir $x \leftarrow U(\mathbb{Z}_q)$ et calculer $h = g^x \bmod p$
- $\mathsf{pk} = h$, $\mathsf{sk} = x$

$\mathsf{Enc}(\mathsf{pk}, m)$ où $m \in \mathbb{Z}_p$:

- Choisir $r \in \mathbb{Z}_q$
- Renvoyer $(g^r \bmod p, m \cdot h^r \bmod p)$

Question 7. *Montrer qu'il existe un algorithme efficace qui, étant donné un élément de $\mathbb{Z}_p^*$, détermine si celui-ci est un carré modulo p.*

Indice : utiliser une exponentiation.

Question 8. *Montrer que ce schéma n'est pas IND-CPA, et expliquer pourquoi la preuve de sécurité de ElGamal (vue en cours) ne fonctionne pas ici.*

Question 9. *On suppose maintenant que m est encodé comme une chaîne de bits de même taille que p : $m \in \{0,1\}^{|p|}$. On modifie la fonction de chiffrement en :*

$$\mathsf{Enc}(\mathsf{pk}, m) = (g^r \bmod p, m \oplus (h^r \bmod p))$$

où $\oplus$ est un XOR de représentations binaires. Le schéma est-il IND-CPA ?

Chiffrement à clé publique anonyme

Soit G un groupe cyclique d'ordre q premier et g un générateur. On suppose que le problème DDH est difficile dans G.

On considère les trois jeux de sécurité suivants $\mathcal{G}_0, \mathcal{G}_1, \mathcal{G}_2$ joués entre un challenger et un distingueur $\mathcal{D}$. Dans les trois jeux, le challenger tire $r, x, y, t \leftarrow U(\mathbb{Z}_q)$.

- Dans $\mathcal{G}_0$, il envoie (g^r, g^x, g^y, g^{xr})
- Dans $\mathcal{G}_1$, il envoie (g^r, g^x, g^y, g^t)
- Dans $\mathcal{G}_2$, il envoie (g^r, g^x, g^y, g^{yr})

Le distingueur renvoie ensuite un bit b.

Question 10. *Montrer que, sous l'hypothèse DDH dans G, les paires de jeux $(\mathcal{G}_0, \mathcal{G}_1)$ et $(\mathcal{G}_1, \mathcal{G}_2)$ sont indistinguables. Qu'en est-il de $(\mathcal{G}_0, \mathcal{G}_2)$?*

On considère le jeu suivant $\mathcal{G}$ joué entre un challenger $\mathcal{C}$ et un adversaire $\mathcal{A}$.

1. Le challenger tire $r, x, y \leftarrow U(\mathbb{Z}_q)$ et un bit $b \in \{0,1\}$

2. Si $b = 0$, le challenger envoie (g^r, g^x, g^y, g^{xr}), sinon il envoie (g^r, g^x, g^y, g^{yr})
3. L'adversaire renvoie un bit b' et gagne si $b = b'$

Question 11. *Déduire de la question précédente que, sous l'hypothèse DDH, tout adversaire PPT a un avantage négligeable dans le jeu $\mathcal{G}$.*

On considère le cryptosystème ElGamal (vu en cours). Plusieurs utilisateurs ont publié leur clé publique. Alice veut envoyer un message sans qu'il soit possible de déterminer à quelle personne il a été envoyé. On formalise cette propriété d'*anonymité* par le jeu de sécurité suivant entre un challenger $\mathcal{C}$ et un adversaire $\mathcal{A}$.

- $\mathcal{C}$ produit deux paires de clés $(\mathsf{pk}_0, \mathsf{sk}_0)$ et $(\mathsf{pk}_1, \mathsf{sk}_1)$, et un bit $b \in \{0, 1\}$
- $\mathcal{A}$ sélectionne un message m et l'envoie à $\mathcal{C}$
- $\mathcal{C}$ renvoie $\mathsf{Enc}(\mathsf{pk}_b, m)$
- $\mathcal{A}$ renvoie un bit b' et gagne si $b = b'$

Question 12. *En utilisant la question précédente, montrer que le chiffrement ElGamal est anonyme.*

Question 13. *On considère le cryptosystème* padded RSA *vu en cours, avec une génération de clés utilisant deux nombres premiers aléatoires de ℓ bits exactement (c'est-à-dire $2^{\ell-1} \leq P, Q < 2^\ell$), et un chiffrement de la forme $\mathsf{Enc}(x) = (r\|x)^e \bmod N$ où $\|$ indique une concaténation de bit-strings entre le clair x et la valeur aléatoire r.*

Justifier que padded RSA n'est pas anonyme.

Un peu de cryptographie symétrique

On considère un chiffrement symétrique (un « chiffrement à bloc », que nous verrons en cours) utilisant une clé k de n bits, une permutation *publique* $\Pi : \{0,1\}^n \to \{0,1\}^n$, et avec des clairs / chiffrés de n bits. La construction est :

$$E_k(x) = \Pi(k \oplus x) \oplus k \ .$$

On essaie de récupérer la clé k dans une attaque à *clair choisi* où l'attaquant peut obtenir le chiffré sur toute entrée de son choix.

Question 14. *Montrer comment attaquer efficacement le chiffrement si :*

- *On enlève le premier XOR de clé ;*
- *On enlève le deuxième XOR de clé ;*
- *On utilise comme permutation une fonction linéaire, de la forme : $\Pi(y) = My$ où M est une matrice Booléenne inversible aléatoire de dimensions $n \times n$.*