TD4 – Fonctions de hachage

Exercice 1. *Concaténations*

Soit $\mathcal{H}_1 = (\mathsf{Gen}_1, H_1)$ et $\mathcal{H}_2 = (\mathsf{Gen}_2, H_2)$ deux fonctions de hachage. On définit $\mathcal{H} = (\mathsf{Gen}, H)$ où $\mathsf{Gen}(1^n)$ renvoie $(s_1, s_2) = (\mathsf{Gen}_1(1^n), \mathsf{Gen}_2(1^n))$, et $H^{s_1,s_2}(x) = H_1^{s_1}(x) \| H_2^{s_2}(x)$.

✎ Montrer que si au moins l'une des deux fonctions de hachage $\mathcal{H}_1$ ou $\mathcal{H}_2$ est résistante aux collisions, alors $\mathcal{H}$ également.

Exercice 2. *Notions de sécurité*

Dans tout l'exercice, on considère des fonctions de compression $H : \{0,1\}^{2n} \to \{0,1\}^n$.

Une fonction de hachage (Gen, H) est *résistante à la seconde préimage* si étant donné s et x tiré uniformément, un algorithme polynomial probabiliste n'a qu'une probabilité négligeable de produire x' tel que $H^s(x) = H^s(x')$.

1. **i.** Définir une expérience de sécurité pour la résistance à la seconde préimage, et définir formellement cette notion de sécurité.
   ii. Montrer qu'une fonction de hachage résistante aux collisions est résistante à la seconde préimage. *Montrer que si on dispose d'un attaquant pour la seconde préimage, on peut en construire un pour les collisions.*

Une fonction de hachage (Gen, H) est *résistante à la préimage* si étant donné s et $y = H^s(x)$ où x est tiré uniformément, un algorithme polynomial probabiliste n'a qu'une probabilité négligeable de produire x' tel que $H^s(x') = y$.

2. **i.** Pourquoi demande-t-on à l'attaquant de renvoyer x' tel que $H^s(x') = y$, et pas x ?
   ii. Définir une expérience de sécurité pour la résistance à la préimage, et définir formellement cette notion de sécurité.

   On cherche à montrer qu'une fonction de hachage résistante à la seconde préimage est résistante à la préimage. Pour cela, on considère un attaquant A pour la préimage, et on construit un attaquant A' pour la seconde préimage : sur l'entrée s et x, A' calcule $y \leftarrow H^s(x)$, et $x' \leftarrow A(s, y)$, puis renvoie x'.

   iii. Soit $x \in \{0,1\}^{2n}$, tiré uniformément. Montrer que la probabilité pour que x soit la seule préimage de $H^s(x)$ est $< 1/2^n$.
   iv. Montrer que si x n'est pas la seule préimage de $H^s(x)$, A renvoie $x' = x$ avec probabilité $\leq \frac{1}{2}$.
   v. Montrer qu'une fonction de hachage résistante à la seconde préimage est résistante à la préimage.

Exercice 3. *Anniversaires*

1. Supposons que votre téléphone possède $3\,500$ chansons en mémoire, et que vous décidiez au hasard les chansons que vous écoutez. Combien de chansons devez-vous écouter avant d'écouter deux fois la même chansons, avec probabilité au moins 50% ?
2. Adapter la preuve du paradoxe des anniversaires pour prouver le résultat suivant : *si on tire $y_1, \ldots, y_q \in \{0,1\}^\ell$ et $z_1, \ldots, z_q \in \{0,1\}^\ell$, uniformément et indépendamment, la probabilité qu'il existe i et j tels que $y_i = z_j$ est comprise entre $q^2/2^{\ell+1}$ et $q^2/2^\ell$.*
3. Soit $H : \{0,1\}^n \to \{0,1\}^{2n}$ une fonction aléatoire. On définit la fonction $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^{2n}$ par $F_k(x) = H(k \oplus x)$. Montrer qu'un attaquant ayant accès à des oracles pour H et F_k peut retrouver la clef k de n bits avec probabilité constante en temps environ $2^{n/2}$.