TD - Construction d'une fonction de hachage

Une fonction de hachage h est une fonction de $E \subset \{0,1\}^*$ dans $F \subset \{0,1\}^m$:

$$h : E \subset \{0,1\}^* \longrightarrow F \subset \{0,1\}^m$$

où m est un entier fixé (par exemple $m = 128$ pour $h = \text{MD5}$).

Une fonction de hachage est dite **résistante aux collisions** si il est difficile (i.e. extrêmement coûteux) de trouver $(x, y) \in E^2$ avec $x \neq y$ tels que: $h(x) = h(y)$.
Cet exercice construit une telle fonction de hachage à partir d'une fonction à sens unique (ici le logarithme discret).

I. Construction d'une fonction de hachage : $\{0,1\}^{2m} \longrightarrow \{0,1\}^m$

Soit p un grand nombre premier tel que $q = \frac{p-1}{2}$ soit aussi premier. On note $\mathbb{F}_p = \mathbb{Z}/p.\mathbb{Z}$ et $\mathbb{F}_p^*$ le groupe multiplicatif $(\{1, 2, \ldots, p-1\}, \times_{\bmod p})$. On définit de même $\mathbb{F}_q$ et $\mathbb{F}_q^*$.

Soient α et β deux éléments **primitifs** (i.e. *générateurs*) de $\mathbb{F}_p^*$. On suppose que α, β et p sont publics (connus de tout le monde) et on définit h_1 par :

$$\begin{array}{rccl} h_1 : & \mathbb{F}_q \times \mathbb{F}_q & \to & F_p \\ & (x_1, x_2) & \mapsto & \alpha^{x_1}.\beta^{x_2} \mod p \end{array}$$

Soit λ l'entier de $\mathbb{F}_q^*$ égal au logarithme discret de β en base α : $\alpha^\lambda = \beta \mod p$.
Dans toute cette question, on suppose que λ n'est pas connu et extrêmement coûteux à calculer.

Pour montrer que h_1 est résistante aux collisions, on procède comme suit:

- On suppose que l'on connaît une collision pour h_1, i.e.
  $\exists (x_1, x_2, x_3, x_4) \in \{0, 1, \ldots, q-1\}^4$ tels que $(x_1, x_2) \neq (x_3, x_4)$ et $h_1(x_1, x_2) = h_1(x_3, x_4)$
- et on montre qu'on peut alors facilement calculer λ. Pour cela, on définit

$$d = \text{pgcd}(x_4 - x_2, p - 1).$$

Nota Bene. On rappelle que p et q sont premiers et que $p = 2q + 1$.

1. Quels sont les diviseurs de $p-1$? En déduire $d \in \{1, 2, q, p-1\}$.

2. Justifier $-(q-1) \leq x_4 - x_2 \leq q-1$; en déduire que $d \neq q$ et $d \neq p-1$.

3. Montrer que $\alpha^{(x_1-x_3)} \equiv \beta^{(x_4-x_2)} \mod p$.

4. On suppose ici $d = 1$; montrer qu'alors $\lambda = (x_1 - x_3).(x_4 - x_2)^{-1} \mod (p-1)$.

5. On suppose ici $d = 2$ et on pose $u = (x_4 - x_2)^{-1} \mod q$.
5.a. Justifier que $\beta^q = -1 \mod p$; en déduire $\beta^{u.(x_4-x_2)} = \pm\beta \mod p$.
5.b. Montrer qu'on a : $\lambda = u.(x_1 - x_3) \mod p-1$ ou bien $\lambda = u.(x_1 - x_3) + q \mod p-1$.

6. Conclure en donnant un algorithme qui prend en entrée une collision $(x_1, x_2) \neq (x_3, x_4)$ et qui retourne λ.
Majorer le coût de cet algorithme et en déduire que h_1 est résistante aux collisions.

II. Extension à une fonction de hachage : $\{0,1\}^* \longrightarrow \{0,1\}^m$

On suppose donnée une fonction de hachage $h_1 : \{0,1\}^{2m} \to \{0,1\}^m$ résistante aux collisions (comme celle de la partie I par exemple) :

$$\begin{array}{rccc} h_1 : & \{0,1\}^m \times \{0,1\}^m & \to & \{0,1\}^m \\ & (x_1, x_2) & \mapsto & h_1(x_1, x_2) \end{array}$$

A partir de h_1, on définit de manière récursive $h_i : \{0,1\}^{2^i m} \longrightarrow \{0,1\}^m$ par:

$$\begin{array}{rccc} h_i : & \left(\{0,1\}^{2^{i-1}m}\right)^2 & \longrightarrow & \{0,1\}^m \\ & (x_1, x_2) & \mapsto & h_1(h_{i-1}(x_1), h_{i-1}(x_2)) \end{array}$$

7. Soient $(x_1, x_2, x_3, x_4) \in \mathbb{F}_q^4$; expliciter $h_2(x_1, x_2, x_3, x_4)$ en fonction de h_1.

8. Montrer que h_2 est résistante aux collisions. **Indication :** *on pourra procéder par l'absurde en montrant que si l'on connaît une collision pour h_2 alors on peut facilement calculer une collision pour h_1.*

9. Généraliser en justifiant que h_i est résistante aux collisions.

10. Combien d'appels à la fonction h_1 sont effectués lors d'un appel à h_i ?
En déduire que le calcul du hachage d'une séquence de n bits a un coût $O(n)$.

11. Comment peut-on étendre cette méthode pour construire une fonction de hachage sans collision de $\{0,1\}^* \longrightarrow \{0,1\}^m$?