TD Cryptographie à Clé Publique

Collisions & fonctions de hachage

Sebastien.Varrette@imag.fr

Exercice 1. [Paradoxe des anniversaires]
On considère la fonction de hachage $H : \{0,1\}^t \longrightarrow \{0,1\}^m$ avec $t > m$ et on pose $n = 2^m = |\{0,1\}^m|$. On dispose de k messages $\{x_i\}_{1 \leq i \leq k}$ aléatoires ($k << n$). On supposera les hachages $z_i = H(x_i)$ comme aléatoires.
On souhaite déterminer la probabilité pour obtenir au moins une collisions à partir des messages x_i.

1. On note p_k la probabilité que les $\{z_i\}_{1 \leq i \leq k}$ soient tous différents. Montrer que :
$$p_k = \prod_{i=1}^{k-1} \left(1 - \frac{i}{n}\right)$$
2. Montrer que $\forall x \in \mathbb{R}, e^{-x} \geq 1 - x$
3. La probabilité d'obtenir au moins une collision est $1 - p_k$. Soit $0 < \alpha < 1$. Montrer que :
$$1 - p_k > \alpha \Longrightarrow k > \sqrt{2n \ln\left(\frac{1}{1-\alpha}\right)} = \mathcal{O}(\sqrt{n})$$
4. Application numérique : On considère une assemblée de k personnes. Quelle est la probabilité qu'au moins d'entre d'entre-elles aient leur anniversaire le même jour (en ne tenant pas compte de l'année) ? Pour quelle valeur minimale de k cette prabability est elle supérieure à $\frac{1}{2}$? à 99% ?

Exercice 2. [Construction d'une fonction de compression] On se propose de construire une fonctions de compression
$$h : \{0,1\}^{2m-2} \longrightarrow \{0,1\}^m$$
résistante aux collisions. On utilise pour cela une fonction à sens unique (ici, le logarithme discret pour $m = 1024$ bits $= 64$ octets typiquement. On considère en effet qu'on ne sait pas calculer le logarithme discret pour de tels nombres entiers). Une construction de type Merkle-Damgård fournira alors une fonction de hachage résistante aux collisions. On rappelle qu'une fonction de hachage est dite **résistante aux collisions** s'il est difficile (i.e extrêmement coûteux) de trouver (x, y) avec $x \neq y$ tels que $H(x) = H(y)$.
On procède comme suit :
– On choisit p et q deux nombres premiers tels que $q = \frac{p-1}{2}$. Autrement dit, $p = 2q+1$. On suppose que p comporte m bits (ainsi q en comportera $m-1$).
– On considère alors les groupes multiplicatifs $\mathbb{Z}_p^\times$ (resp. $\mathbb{Z}_q^\times$).
On a donc $\mathbb{Z}_p^\times = \{1, 2, \ldots, p-1\}$ (resp. $\mathbb{Z}_q^\times = \{1, 2, \ldots, q-1\}$).

– Soient α et β deux générateurs de $\mathbb{Z}_p^\times$ ($\alpha \neq \beta$). Autrement dit :

$$\mathbb{Z}_p^\times = \{\alpha^0, \alpha^1, \alpha^2, \ldots, \alpha^{p-2}\} = \{\beta^0, \beta^1, \beta^2, \ldots, \beta^{p-2}\}$$

On pose $\lambda = \log_\alpha(\beta) : \alpha^\lambda = \beta \mod p$. On suppose que λ n'est pas connu et extrêmement coûteux à calculer

– On suppose α, β et p connus publiquement et on définit :

$$\begin{array}{rccl} h: & \mathbb{Z}_q \times \mathbb{Z}_q & \longrightarrow & \mathbb{Z}_p \\ & (x_1, x_2) & \longrightarrow & \alpha^{x_1}\beta^{x_2} \mod p \end{array}$$

1. Application numérique : pour $p = 83$, $q = 41$, $\alpha = 15$ et $\beta = 22$, calculer le résumé de $(12, 34)$. Sur quelle calcul repose la résistance aux collisions de la fonction h ?

   Pour montrer que h est résistante aux collisions, on raisonne par l'absurde :
   - On suppose disposer d'une collision. Autrement dit, on suppose disposer de $x = (x_1, x_2) \in \mathbb{Z}_q^2$ et $y = (y_1, y_2) \in \mathbb{Z}_q^2$ avec $x \neq y$ tel que $h(x) = h(y)$
   - On montre qu'on peut alors facilement calculer λ.

   Dans toute la suite, on pose $d = pgcd(y_2 - x_2, p - 1)$
2. Quels sont les diviseurs de $p - 1$? En déduire que $d \in \{1, 2, q, p - 1\}$.
3. Montrer que $-q < y_2 - y_1 < q$ et en déduire que $d \neq q$.
4. Montrer que $\alpha^{x_1 - y_1} \equiv \beta^{y_2 - x_2} \mod p$
5. On suppose que $d = p - 1$. Montrer que $x = y$. En déduire que $d \neq p - 1$.
6. On suppose que $d = 1$. Montrer que $\lambda = (x_1 - y_1)(y_2 - x_2)^{-1} \mod p - 1$.
7. On suppose que $d = 2 = pgcd(y_2 - x_2, 2q)$. On en déduit donc $pgcd(y_2 - x_2, q) = 1$ et on pose $u = (y_2 - x_2)^{-1} \mod q$
   (a) Montrer que $\beta^q \equiv -1 \mod p$. En déduire : $\beta^{u(y_2 - x_2)} \equiv \pm\beta \mod p$.
   (b) Montrer que soit $\lambda = u(x_1 - y_1) \mod p - 1$ soit $\lambda = u(x_1 - y_1) + q \mod p - 1$
8. Conclure en donnant un algorithme qui prend en entrée une collision $x = (x_1, x_2) \in \mathbb{Z}_q^2$ et $y = (y_1, y_2) \in \mathbb{Z}_q^2$ et renvoit λ. Majorer le coût de cet algorithme et en déduire que h est résistante aux collisions.