Cryptography

JOACHIM VON ZUR GATHEN, JÉRÉMIE DETREY

6. Tutorial: Cryptographic hash functions

Exercise 6.1 (Derivated hash functions).

Let $h_0 \colon \{0,1\}^{2m} \to \{0,1\}^m$ be a collision-resistant hash function with $m \in \mathbb{N}_{>0}$.

Note: in the following, "|" denotes the concatenation of bit strings.

(i) We construct a hash function $h_1 \colon \{0,1\}^{4m} \to \{0,1\}^m$ as follows: Interpret the bit string $x \in \{0,1\}^{4m}$ as $x = (x_1|x_2)$, where both $x_1, x_2 \in \{0,1\}^{2m}$ are words with $2m$ bits. Then compute the hash value $h_1(x)$ as

$$h_1(x) = h_0(h_0(x_1)|h_0(x_2)).$$

Show that h_1 is collision-resistant.

Solution. Assume we find have a collision of h_1: $x = (x_1|x_2)$ and $y = (y_1|y_2)$ in $\{0,1\}^{4m}$ such that

$$h_1(x) = h_0(h_0(x_1)|h_0(x_2)) = h_0(h_0(y_1)|h_0(y_2)) = h_1(y).$$

In the case that $(h_0(x_1)|h_0(x_2)) \neq (h_0(y_1)|h_0(y_2))$, we then have a collision of h_0. And if $(h_0(x_1)|h_0(x_2)) = (h_0(y_1)|h_0(y_2))$, we then have at least one collision of h_0. ◯

(ii) Let $i \in \mathbb{N}$, $i \geq 1$. We define a hash function $h_i \colon \{0,1\}^{2^{i+1}m} \to \{0,1\}^m$ recursively using h_{i-1} in the following way: Interpret the bit string $x \in \{0,1\}^{2^{i+1}m}$ as $x = (x_1|x_2)$, where both $x_1, x_2 \in \{0,1\}^{2^i m}$ are words with $2^i m$ bits. Then the hash value $h_i(x)$ is defined as

$$h_i(x) = h_0(h_{i-1}(x_1)|h_{i-1}(x_2)).$$

Show that h_i is collision-resistant.

Solution. Proof by induction on i. ◯

Exercise 6.2 (DLP and hash functions).

The numbers $q = 7541$ and $p = 15083 = 2q + 1$ are prime. We choose the group $G = \{z \mid \text{ord } z | q\} < \mathbb{Z}_p^\times$. Let $\alpha = 604$ and $\beta = 3791$ be elements of G.

(i) Show that both elements α and β have order q in $\mathbb{Z}_p^\times$ and (thus) generate the same subgroup.

Solution. Since q is prime and $\alpha^q = 1$ and $\beta^q = 1$, we have that ord $\alpha =$ ord $\beta = q$. And since $\#\mathbb{Z}_p^\times = p - 1 = 2q$, $\langle\alpha\rangle = \langle\beta\rangle = G$. ◯

(ii) Consider the hash function

$$\begin{array}{rccc} h: & \mathbb{Z}_q \times \mathbb{Z}_q & \longrightarrow & G \\ & (x_1, x_2) & \longmapsto & \alpha^{x_1}\beta^{x_2}. \end{array}$$

Compute $h(7431, 5564)$ and $h(1459, 954)$.

Solution. $h(7431, 5564) = \alpha^{7431}\beta^{5564} = 14461$ and $h(1459, 954) = \alpha^{1459}\beta^{954} = 14461$. ◯

(iii) Find $\log_\alpha \beta$.

Solution. Since $\alpha^{7431}\beta^{5564} = \alpha^{1459}\beta^{954}$, we have

$$\alpha^{7431-1459} = \alpha^{5972} = \beta^{2931} = \beta^{954-5564}.$$

As $2931^{-1} = 4680$ in $\mathbb{Z}_q$, $\beta = \alpha^{5972 \cdot 4680} = \alpha^{2014}$. We obtain $\log_\alpha \beta = 2014$. ◯

(iv) Prove that for any p, q (both prime with q dividing $p - 1$) finding a collision of h solves a discrete logarithm in the order q subgroup of $\mathbb{Z}_p^\times$ (which is thought to be difficult...).

Solution. A collision of h is x_1, x_2, y_1 and y_2 in $\mathbb{Z}_q$ such that $\alpha^{x_1}\beta^{x_2} = \alpha^{y_1}\beta^{y_2}$ in G, with $x_1 \neq y_1$ or $x_2 \neq y_2$.

We can prove that we cannot have either $x_1 = y_1$ or $x_2 = y_2$ unless we have both, which contradicts the collision hypothesis.

Then, we have $\alpha^{x_1 - y_1} = \beta^{y_2 - x_2}$, and since q is prime, we can invert $y_2 - x_2$ in $\mathbb{Z}_q$ to obtain

$$\log_\alpha \beta = \frac{x_1 - y_1}{y_2 - x_2}.$$

◯

Exercise 6.3 (Hash functions for long messages).

We want to use the previous discrete-logarithm-based hash function to build a hash function for messages of arbitrary length, as seen in the lecture.

First of all, we need to tweak our original hash function so that it complies with a few requirements: since we are now working at the bit level, we need a hash function $\tilde{h}$ from $\mathbb{Z}_2^m$ to $\mathbb{Z}_2^t$.

(i) What are the conditions on m and t so that $\tilde{h}$ remains collision-resistant?

Solution. We need the largest m and the smallest t such that the two functions $\mathbb{Z}_2^m \longrightarrow \mathbb{Z}_q \times \mathbb{Z}_q$ and $\mathbb{Z}_p^\times \longrightarrow \mathbb{Z}_2^t$ are both injective. ◯

(ii) Compute m and t.

Solution. $m = 2\lfloor \log_2(q-1) \rfloor = 24$ and $t = \lfloor \log_2(p-1) \rfloor + 1 = 14$. ◯

(iii) Recall the method for hashing long messages. Give the corresponding pseudo-code.

Solution. See the lecture notes. ◯

(iv) Hash the two bit strings 100 and 110001101001001110.

Solution.

$$\begin{aligned} H(100) &= \tilde{h}(\tilde{h}(000000000\ 0\ 100000000)\ 1\ 011000000) \\ &= \tilde{h}(11001001000000\ 1\ 011000000) \\ &= 01011100111000, \text{ and} \end{aligned}$$

$$\begin{aligned} &H(110001101001001110) \\ &= \tilde{h}(\tilde{h}(\tilde{h}(000000000\ 0\ 110001101)\ 1\ 001001110)\ 1\ 000000000) \\ &= \tilde{h}(\tilde{h}(00110011011101\ 1\ 001001110)\ 1\ 000000000) \\ &= \tilde{h}(101110001000011\ 1\ 000000000) \\ &= 01011100111000. \end{aligned}$$

◯

(v) Find a collision of $\tilde{h}$ and of h.

Solution. We find that $h(147, 52) = h(285, 7)$. ◯

(vi) Conclude on the discrete logarithm of β in base α.

Solution. We verify that $\log_\alpha \beta = \frac{147-285}{7-52} = 2014$ in $\mathbb{Z}_q$. ◯