Homework 12 in Advanced Methods of Cryptography - Proposal for Solution -

Prof. Dr. Rudolf Mathar, Michael Reyer, Henning Maier
15.01.2013

Solution to Exercise 37.

(a) $\gcd(a, p-1) \in \{1, 2, q, 2q\}$ for all $a \in \mathbb{N}$ since the factorization is $p - 1 = 1 \cdot 2 \cdot q$.

(b) p, q are prime with $p = 2q + 1$ ($\Rightarrow$ Sophie-Germain primes), a, b are primitive elements, and $0 \le m \le q^2 - 1$. The hash function is defined by:

$$h(m) = a^{x_0} b^{x_1} \mod p$$

with $0 \le x_0, x_1 \le q - 1 \wedge m = x_0 + x_1 q$. The given function is slow but collision-free.

Proof: Assume there is a collision, i.e., at least one pair of messages satisfies:

$$m \neq m' \wedge h(m) = h(m').$$

It is to show that the discrete logarithm $k = \log_a(b) \mod p$ can be determined if a collision is known. The two different messages are as in Ex. 10.2:

$$\begin{aligned} m &= x_0 + x_1 q, \\ m' &= x_0' + x_1' q, \end{aligned}$$

and the common hash-value is:

$$\begin{aligned} h(m) &= h(m'), \\ \overset{Ex.10.2}{\Leftrightarrow} k(x_1 - x_1') &\equiv x_0' - x_0 \pmod{p-1}. \end{aligned} \tag{1}$$

Furthermore, $x_1 - x_1' \not\equiv 0 \pmod{p-1}$, otherwise it would follow that $m = m'$.

To determine k, assume both $0 \le k, k' < p - 1$ fulfil (1). Then

$$\begin{aligned} k(x_1 - x_1') &\equiv x_0' - x_0 \pmod{p-1} \wedge \\ k'(x_1 - x_1') &\equiv x_0' - x_0 \pmod{p-1} \\ \Rightarrow (k - k')(x_1 - x_1') &\equiv 0 \pmod{p-1}. \end{aligned} \tag{2}$$

It holds:

$$\begin{aligned} -(p-1) < k - k' < p - 1 \wedge \\ x_1 \neq x_1' \wedge \\ -(q-1) \le x_1 - x_1' \le q - 1. \end{aligned}$$

Let $d = \gcd(x_1 - x_1', p - 1)$, then it follows from (1) that $d \mid (x_0' - x_0)$:

1) $d = 1 \Rightarrow k - k' \equiv 0 \pmod{p-1} \Rightarrow k \equiv k' \pmod{p-1}$, i.e., there is the solution:

$$k = (x_1 - x_1')^{-1}(x_0' - x_0) \mod (p-1).$$

2) $d > 1$:

$$\overset{(1)}{\Rightarrow} k\left(\frac{x_1 - x_1'}{d}\right) \equiv \left(\frac{x_0' - x_0}{d}\right)\left(\mathrm{mod}\,\frac{p-1}{d}\right). \tag{3}$$

It holds $\gcd\left(\frac{x_1-x_1'}{d}, \frac{p-1}{d}\right) = 1 \overset{1)}{\Rightarrow}$ (3) has exactly one solution $k_0 < \frac{p-1}{d}$:

$$k_0 = \left(\frac{x_1 - x_1'}{d}\right)^{-1}\left(\frac{x_0' - x_0}{d}\right)\left(\mathrm{mod}\,\frac{p-1}{d}\right). \tag{4}$$

For the solution of (1), this yields multiple candidates: $k_l = k_0 + \left(\frac{p-1}{d}\right) \cdot l$, with $l = 0, \ldots, d-1$.

Recall from (a) that $p - 1 = 2q \Rightarrow d \in \{1, 2, q, 2q\} \Rightarrow d \in \{1, 2\}$ as $(x_1 - x_1') \leq q - 1 \Rightarrow d = 2$ as $d > 1$.

Check all candidates k_0, k_1, i.e., check if $a^{k_0} \equiv b \pmod{p}$ or if $a^{k_0 + \frac{p-1}{2}} \equiv b \pmod{p}$ holds.

The candidate fulfilling the concruence is $\log_a(b)$.

Altogether, finding collisions is hard because the determination of a discrete logarithm is computationally extensive.