Cryptography I, winter 2005/06

JOACHIM VON ZUR GATHEN, MICHAEL NÜSKEN

9. Exercise sheet
Hand in before Monday, 2006/01/23, 14^{00} in b-it 1.22.

Exercise 9.1 (DLP and hash functions). (8 points)

The numbers $q = 7541$ and $p = 15083 = 2q + 1$ are prime. We choose the group $G = \{z \mid \operatorname{ord} z | q\} < \mathbb{Z}_p^\times$. 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. $\boxed{2}$

(ii) Consider the hash function $\boxed{2}$

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

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

(iii) Find $\log_\alpha \beta$. $\boxed{2}$

(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...). $\boxed{2}$

Exercise 9.2 (Hash functions for long messages). (5 points)

The MUPAD notebook `long-hash` contains the definition of the hash function h^* for long messages that was presented in class. The function h from Exercise 9.1 is used for our hash function $h_0 : \mathbb{Z}_2^m \to \mathbb{Z}_2^t$. Furthermore, some messages are defined.

(i) The notebook does not work yet. Spot and correct the error. $\boxed{1}$

(ii) Compute the hash values of all messages. $\boxed{1}$

(iii) Are there collisions? For each collision of h^* compute a collision of h. $\boxed{2}$

(iv) Compute $\log_\alpha \beta$ from one of these collisions. $\boxed{1}$

Note: As usual, you can find the file `long-hash` on our web page.

Exercise 9.3 (Derivated hash functions). (6 points)

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

(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 3

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

Show: h_1 ist collision-resistant.

1 (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: h_i is collision-resistant.

2 (iii) The number $p = 2027$ is prime. Now define $h_0 : \{0,1\}^{22} \to \{0,1\}^{11}$ as follows: Let $x = (b_{21}, \ldots, b_0)$ be the binary representation of x. Then $x_1 = \sum_{0 \leq i \leq 10} b_{11+i} 2^i \bmod p$ and $x_2 = \sum_{0 \leq i \leq 10} b_i 2^i \bmod p$. Show that the numbers 5 and 7 have order $p-1$ modulo p. Now compute $y = 5^{x_1} \cdot 7^{x_2} \bmod p$ and let $h(x) = (B_{10}, \ldots, B_0)$ be the binary representation of y, i.e. $y = \sum_{0 \leq i < 11} B_i 2^i$. Compute from h_0 the hash function $h_2 \colon \{0,1\}^{88} \to \{0,1\}^{11}$ analogous to (ii). Use the birthday attack to find a collision of h_0 and h_1. (For this you should of course use a computer algebra system, e.g. MuPAD.)

Note: "|" denotes the concatenation of bit strings, MuPAD a dot **.** is used.