TMA4155 — Exercise 9

Kristian Gjøsteen

2006-11-27

NB! This exercise will be in the auditorium F2.

Task 1 — Hash function analysis

a. Let $h : \{0,1\}^* \to \{0,1\}^n$ be a hash function that is second-preimage and collision resistant. Let $h' : \{0,1\}^* \to \{0,1\}^{n+1}$ be the hash function given by the rule

$$h'(x) = \begin{cases} 0||x & x \in \{0,1\}^n, \\ 1||h(x) & \text{otherwise.} \end{cases}$$

Prove that h' is not preimage resistant, but still second-preimage and collision resistant.

b. *[Variant of Task 2a on the Autumn 2003 exam.]* A common paradigm for constructing a hash function $h : \{0,1\}^* \to \{0,1\}^n$ is to iterate a *compression* function $f : \{0,1\}^l \to \{0,1\}^n$, where $l > n$. The idea is to split the message m into blocks $m_1, m_2, \ldots, m_k$ of length $l - n$ (the hash function's *block length*), then use the rule $y_0 = iv$ for some fixed $iv \in \{0,1\}^n$, and

$$y_i = f(y_{i-1}||m_i)$$

to compute y_k, and set $h(m) = y_k$. To get the length of m divisible by $l - n$, we use any standard padding scheme.

Let $(f', g') : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ be a block cipher with key length n and block length n (the key is the first parameter, the block the second). We can make a compression function $f : \{0,1\}^{2n} \to \{0,1\}^n$ from the block cipher with the rule

$$f(y||m) = f'(y,m).$$

Show how one can find a collision in h.

Task 2 — Advanced hash function analysis

Suppose you have two hash functions $h_0, h_1 : \{0,1\}^* \to \{0,1\}^n$, both of them based on iterating compression functions as described in Task 1b. Let $h : \{0,1\}^* \to \{0,1\}^{2n}$ be the hash function

$$h(x) = h_0(x)||h_1(x).$$

NOTE: We shall ignore padding in this task, and only consider messages built up of complete blocks.

a. Show that you can find a collision in h_0 by trying on average approximately $2^{n/2}$ messages.

b. Let $x_{0,1}$ and $x_{1,1}$ be two bit strings such that $h_0(x_{0,1}) = h_0(x_{1,1})$. Show that you can find strings $x_{0,2}$ and $x_{1,2}$ such that $h_0(x_{0,1}||x_{0,2}) = h_0(x_{0,1}||x_{0,2})$ by trying on average approximately $2^{n/2}$ such strings.

c. Since the length of every $x_{i,j}$ is divisible by the block length for the compression function, show that

$$h_0(x_{0,1}||x_{0,2}) = h_0(x_{0,1}||x_{1,2}) = h_0(x_{1,1}||x_{0,2}) = h_0(x_{1,1}||x_{1,2}).$$

How many collisions for h_0 do you have now? How much work has been expended so far?

d. Repeat this process approximately $n/2$ times, each time finding a new pair $(x_{0,i}, x_{1,i})$. How many collisions for h_0 do you have now? How much work has been expended so far?

e. Among all of the constructed collisions for h_0, is it likely that you will find a collision for h_1? Show that such a collision will lead to a collision for h. How much work was expended in total to find this collision? Compare this with the amount you get from the birthday paradox attack on a hash function with output length $2n$.