Prof. Dr. Rudolf Mathar, Jose Calvo, Markus Rothe

Tutorial 5
- Proposed Solution -

Friday, November 27, 2015

Solution of Problem 1

a) With a block cipher $E_K(x)$ with block length k, the message is split into blocks m_i of length k each, $m = (m_0, \dots, m_{n-1})$. Take $m = (m_0)$ and $\hat{m} = (m_0, m_1, m_1)$ with m_0, m_1 arbitrary. Then,

$$h(\hat{m}) = E_{m_0}(m_0) \oplus \underbrace{E_{m_0}(m_1) \oplus E_{m_0}(m_1)}_{=\mathbf{0}} = E_{m_0}(m_0) = h(m)\,.$$

Thus, h is neither second preimage resistant nor collision free.

Given $y \in \mathcal{Y}$, choose m_0. Then calculate

$$c = E_{m_0}(m_0)\,,$$
$$m_1 = D_{m_0}(c \oplus y)\,.$$

It follows that

$$h(m_0, m_1) = E_{m_0}(m_0) \oplus E_{m_0}(D_{m_0}(c \oplus y)) = c \oplus c \oplus y = y\,.$$

Hence, h is *not* preimage resistant, either.

b) $\hat{h}$ replaces XOR ($\oplus$) by AND ($\odot$) and remains the same as h otherwise. Take $m = (m_1, m_1)$, with m_1 chosen arbitraryly. Then,

$$\hat{h} = E_{m_1}(m_1) \odot E_{m_1}(m_1) = E_{m_1}(m_1) = \hat{h}((m_1))\,.$$

$\hat{h}$ is neither second preimage resistant nor collision free.

Solution of Problem 2

Recall Example 10.2: Select q prime, such that $p = 2q + 1$ is also prime (Sophie-Germain-primes). Chose a, b as primitive elements modulo p. A message $m = x_0 + x_1 \cdot q$, with $0 \leq x_0, x_1 \leq q - 1$ is then hashed as

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

This function is slow but collision free.

Claim. If $m \neq m'$ and $h(m) = h'(m)$, then $k = log_a(b) \mod p$ can be determined.

In other words, we show that if $m \neq m'$ with $h(m) = h'(m)$ are known, the discrete logarithm $k = log_a(b) \mod p$ can be determined, which is known to be computationally infeasable. I.e., it is infeasable to find $m \neq m'$ with $h(m) = h'(m)$.

Proof. (proof by contradiction) Let $m = x_0 + x_1 \cdot q$, $m' = x_0' + x_1' \cdot q$.

$$\begin{aligned} & & h(m) &= h'(m) \\ &\Leftrightarrow & a^{x_0} b^{x_1} &\equiv a^{x_0'} b^{x_1'} \mod p \\ &\Leftrightarrow & a^{x_0} a^{kx_1} &\equiv a^{x_0'} a^{kx_1'} \mod p \\ &\Leftrightarrow & a^{k(x_1 - x_1') - (x_0' - x_0)} &\equiv 1 \mod p \end{aligned}$$

Since a is a primitive element modulo p,

$$\begin{aligned} & & k(x_1 - x_1') - (x_0' - x_0) &\equiv 0 \mod (p-1) \\ &\Leftrightarrow & k(x_1 - x_1') &\equiv x_0' - x_0 \mod (p-1)\,. \end{aligned} \tag{$\star$}$$

As $m \neq m'$, it holds that $x_1 - x_1' \not\equiv 0 \mod (p-1)$. Show that $k = \log_a(b) \mod p$ can be efficiently computed. Assume $1 \leq k, k' \leq p - 1$ fulfill ($\star$). Then,

$$\begin{aligned} k(x_1 - x_1') \equiv x_0' - x_0 \mod (p-1) \ \wedge \ k'(x_1 - x_1') \equiv x_0' - x_0 \mod (p-1) \\ \Rightarrow (k - k')(x_1 - x_1') \equiv 0 \mod (p-1)\,. \end{aligned}$$

It holds $-(p-2) \leq k - k' \leq p - 2$ and $x_1 \neq x_1'$ and $-(q-1) \leq x_1 - x_1' \leq q - 1$. Let $d = \gcd(x_1 - x_1', p - 1)$, then, with ($\star$), $d \mid x_0' - x_0$.

(i) $d = 1$: $k - k' \equiv 0 \mod (p-1) \Leftrightarrow k = k' \mod (p-1)$ has one solution for $1 \leq k, k' \leq p - 1$.

(ii) $d > 1$: With ($\star$)

$$k\left(\frac{x_1 - x_1'}{d}\right) \equiv \frac{x_0' - x_0}{d} \mod \left(\frac{p-1}{d}\right) \tag{$\star\star$}$$

It holds $\gcd\left(\frac{x_1 - x_1'}{d}, \frac{p-1}{d}\right) = 1$. With (i), it follows that ($\star\star$) has exactly one solution k_0, which can be determined by using the Extended Euclidean algorithm as in (i).

$$\begin{aligned} & r\left(\frac{x_1 - x_1'}{d}\right) + s\left(\frac{p-1}{d}\right) = 1 \\ \Rightarrow\ & \underbrace{r}_{k_0}\left(\frac{x_1 - x_1'}{d}\right) \equiv \frac{x_0' - x_0}{d} \mod \frac{p-1}{d} \end{aligned}$$

Recall $p-1=2q \Rightarrow d \in \{1,2,q,2q\} \Rightarrow d \in 1,2$ as $(x_1-x_1') \leq q-1$. Check, if $a^{k_0}\underbrace{\left[\text{or } a^{k_0+\frac{p-1}{2}}\right]}_{d=2 \text{ analogously}} \equiv b \mod p$.

□

Solution of Problem 3

a) Having the following expression:

$$h: \{0,1\}^* \to \{0,1\}^*,\ k \mapsto \left(\left\lfloor 10000\left((k)_{10}(1+\sqrt{5})/2 - \left\lfloor (k)_{10}(1+\sqrt{5})/2 \right\rfloor\right)\right\rfloor\right)_2.$$

We want to obtain the upper bound in terms of bit length. Therefore, we will analyze the expression:

$$\alpha = \left((k)_{10}(1+\sqrt{5})/2 - \left\lfloor (k)_{10}(1+\sqrt{5})/2 \right\rfloor\right) < 1$$

but it can be arbitrary close to 1

Hence now the expression is simpler and we can obtain the upper bound:

$$10000\ (\alpha) < 10000 \leq 9999$$

Now applying the logarithm, we obtain the bit length:

$$log_2(9999) \approx 13.288 \leq 14$$

b) We search for a collision:

$$k = 1 \longrightarrow (1+\sqrt{5})/2 = 1.6180$$
$$\longrightarrow (k)_{10}(1+\sqrt{5})/2 - \left\lfloor (k)_{10}(1+\sqrt{5})/2 \right\rfloor = 0.6180$$

Therefore, we need to search for a value x, s.t:

$$x(1+\sqrt{5})/2 = a + 0.6180 + b$$

with a$\in \mathbb{Z}$, b < 0.0001

We create a while loop to obtain the value for the collision:

$x = 2$

while $(0.618 > x((1+\sqrt{5})/2) - \left\lfloor x(1+\sqrt{5})/2 \right\rfloor > 0.618 + 0.0001)$ **do**

$x = x + 1$

end while

Obtaining a value of $k = 10947$, where

$$(h(1))_{10} = 6180$$
$$(h(10947))_{10} = 6180$$

since the values are equal, we obtain a collision.