Musterlösung Cryptography II Übung 6 29.11.11

Exercise 18

Given 2 hash functions with output length 64/128 bits

(a) How many messages have to be created such that the prob. of a collision exceeds 0,86?

Birthday paradox: k objects, n bins

$P_{k,n}$ (prob. of „no collision")

is bounded by: $P_{k,n} \leq e^{-\frac{k(k-1)}{2n}}$

$\Rightarrow 1 - P_{k,n} \geq 1 - e^{-\frac{k(k-1)}{2n}} \geq p$

$\Leftrightarrow e^{-\frac{k(k-1)}{2n}} \leq 1 - p$

$\Leftrightarrow k^2 - k + 2n \ln(1-p) = \left(k - \frac{1}{2} + \frac{1}{2}\sqrt{1 - 8n\ln(1-p)}\right)\left(k - \frac{1}{2} - \frac{1}{2}\sqrt{1 - 8n\ln(1-p)}\right) \geq 0$

With $n = 2^{64}$ and $p = 0{,}86$

$\Rightarrow k_{64} = 8.517 \cdot 10^{9}$

With $n = 2^{128}$ and $p = 0{,}86$

$\Rightarrow k_{128} = 3.658 \cdot 10^{19}$

The number of messages is given by k_{64} and k_{128} respectively

(b)

Hardware Ressources	64 bit	128 bit
hash function executions	k_{64}	k_{128}
memory size	$k_{64} \cdot 64\,bit \,\hat{=}\, 63{,}5\,GB$	$k_{128} \cdot 128\,bit = 545 \cdot 10^{11}\,GB$
comparisons	$0, 1, 2, \ldots, k_{64}-1$ $= \sum_{i=0}^{k_{64}-1} i = \frac{1}{2}(k_{64}-1)k_{64}$ $= 3{,}63 \cdot 10^{19}$	$\frac{1}{2} k_{128}(k_{128}-1)$ $= 6.69 \cdot 10^{38}$

Exercise 19

cryptographic hash function shall fulfill

1. $h(m)$ easy to compute
2. $y \in Y$; infeasible to find $m : h(m) = y$; preimage resistant / one way function
3. $m \in M$; infeasible to find $m' : h(m) = h(m')$; second preimage resistant
4. $m \in M$; infeasible to find $m, m' : h(m) = h(m')$; strongly collision free

Musterlösung <u>Cryptography II Übung 6</u> 29.11.11

a) Given block cipher E_k with block length k:

$m = (m_0, m_1, \dots, m_{n-1})$ and has hash function given as

$C \leftarrow E_{m_0}(m_0)$
for $i = 1 \dots (n-1)$
  $C \leftarrow C \oplus E_{m_0}(m_i)$
end
$h(m) \leftarrow C$

Take $m = (m_0)$ and $\hat{m} = (m_0, m_1, m_1)$ m_0, m_1 are arbitrary

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

h is neither second preimage resistant nor collision free

b) Take $m = (m_1, m_1)$ m_1 arbitrary

$\Rightarrow \hat{h}(m) = E_{m_0}(m_1) \odot E_{m_0}(m_1) = E_{m_0}(m_1) = \hat{h}(m_1)$

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

<u>Exercise 17</u>

Ex. 10.2 : p, q prime, $p = 2q+1$; a, b primitive elements

$0 \le m \le q^2 - 1$

$\Rightarrow h(m) = a^{x_0} \cdot b^{x_1} \bmod p$ with $0 \le x_0, x_1 \le q-1$ $\wedge\ m = x_0 + x_1 q$

slow, but collision free

Proof (indirect): $m \ne m' \wedge h(m) = h(m') \Rightarrow k = \log_a(b) \bmod p$ can be determined

$\Rightarrow h(m) = h(m') \Leftrightarrow k(x_1 - x_1') \equiv x_0' - x_0 \mod p-1$ (*)
$[x_1 - x_1' \not\equiv 0 \mod p-1]$

Determine k: $k(x_1 - x_1') \equiv x_0' - x_0 \ \wedge\ k'(x_1 - x_1') \equiv x_0' - x_0 \mod p-1$
$\Rightarrow (k-k')(x_1 - x_1') \equiv 0 \mod p-1$
It holds that $-(p-2) \le k - k' \le p-2$

Let $d = \gcd(x_1 - x_1', p-1) \overset{(*)}{\Rightarrow} d \mid x_0' - x_0$
(a) $d = 1 \Rightarrow k - k' = 0 \mod p-1 \Rightarrow k = k' \mod p-1$
(b) $d > 1 \overset{(*)}{\Rightarrow} k\left(\frac{x_1 - x_1'}{d}\right) \equiv \left(\frac{x_0' - x_0}{d}\right) \mod \left(\frac{p-1}{d}\right)$ (**)
It holds $\gcd\left(\frac{x_1 - x_1'}{d}, \frac{p-1}{d}\right) = 1 \overset{(a)}{\Rightarrow}$ (**) has exactly 1 solution which can be easily calculated by the Ext. Euclidean Alg.
$\Rightarrow r\left(\frac{x_1 - x_1'}{d}\right) + s\left(\frac{p-1}{d}\right) = 1$
$\Rightarrow r \cdot \frac{x_0' - x_0}{d} \frac{x_1 - x_1'}{d} \equiv \frac{x_0' - x_0}{d} \mod \frac{p-1}{d}$

Recall $p-1 = 2 \cdot q \Rightarrow d \in \{1, 2, q, 2q\} \Rightarrow d \in \{1, 2\}$ as $x_1 - x_1' \le q-1$
check if $a^{k_0} \equiv b \bmod p$ or if $d = 2$ if $a^{k_0 + \frac{p-1}{2}} \equiv b \bmod p$