Homework 6 in Advanced Methods of Cryptography

Prof. Dr. Rudolf Mathar, Henning Maier, Georg Bocherer

23.11.2010

Exercise 20. Consider the following function:

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

Here, $\lfloor x \rfloor$ is the floor function of x (round down to the next integer smaller than x). For computing $h(k)$, the bitstring k is identified with the positive integer it represents. The result is then converted to binary representation.
(example: $k = 10011$, $(k)_{10} = 19$, $h(k) = (7426)_2 = 1110100000010$)

a) Determine the maximal length of the output of h.

b) Give a collision for h.

Exercise 21. Consider the following functions. Check if they fulfil the necessary properties of hash functions.

(a) Let p a 1024 bit prime, a a primitive root modulo p. Define $h: \mathbb{Z} \to \mathbb{Z}_p^*, \ x \mapsto a^x \bmod p$.

(b) Let $g: \{0,1\}^* \to \{0,1\}^n$ a cryptographic hash function, $n \in \mathbb{N}$. Define $h: \{0,1\}^* \to \{0,1\}^{n+1}$ as follows: If $x \in \{0,1\}^n$, then $h(x) = (1, x)$. In other cases, $h(x) = (0, g(x))$.

Exercise 22. Consider two hash functions, one with an output length of 64 bits and another one with an output length of 128 bits.

For each of these functions, do the following:

- Determine the number of messages that have to be created to find a collision with a probability larger than 0.86 by means of the birthday paradox.

Exercise 23. Let $p > 2$ be prime, $a, b \in \mathbb{Z}_p^*$. Show that if a, b are both not quadratic residues, then ab is a quadratic residue. Do not use Euler's criterion, its corollary or the Legendre symbol in your proof.
Hint: Use a primitve element to generate $\mathbb{Z}_p^*$.