# Homework 7 in Cryptography II

Prof. Dr. Rudolf Mathar, Wolfgang Meyer zu Bergsten, Michael Reyer
25.06.2009

**Exercise 20.** 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:

a) 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.

b) Determine the hardware resources required for this attack in terms of memory size, number of comparisons and number of hash function executions.

**Exercise 21.** Using a block cipher $E_K(x)$ with block length $k$ and key $K$ a hash function $h(m)$ is provided in the following way:

Append $m$ with zero bits until it is a multiple of $k$, divide $m$ into $n$ blocks of $k$ bits.
$c \leftarrow E_{m_0}(m_0)$
**for** $i$ **in** $1 \ldots (n-1)$
  $d \leftarrow E_{m_0}(m_i)$
  $c \leftarrow c \oplus d$
**end for**
$h(m) \leftarrow c$

Does this function fulfill the basic requirements for a cryptographic hash function? Can these requirements be fulfilled by replacing the XOR-operation by a logical AND?

**Exercise 22.** Besides the CBC mode, the CFB mode can be used for the generation of a MAC. The plaintext consists of the blocks $M_1, \ldots, M_n$, and we set the initialization vector $C_0 := M_1$. Now, we encrypt $M_2, \ldots, M_n$ in CFB mode with key $K$, which results in the ciphertexts $C_1, \ldots, C_{n-1}$. For the MAC, we use $MAC_K := E_K(C_{n-1})$.

Show that this scheme results in the same MAC as the algorithm in example 10.5 from the lecture notes with the initial value set to $C_0 := \mathbf{0}$.