Homework 4 in Cryptography II

Prof. Dr. Rudolf Mathar, Wolfgang Meyer zu Bergsten

05.06.2008

Exercise 10. 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:

1. With the birthday paradox, determine the number of messages that have to be created to find a collision with a probability larger than 0.86.

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

Excercise 11. With a block cipher $E_K(x)$ with the 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 $1..(n-1)$:
    $d \leftarrow E_{m_0}(m_i)$
    $c \leftarrow c \oplus d$
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?