Homework 7 in Advanced Methods of Cryptography

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

30.11.2010

Exercise 24. 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?

Exercise 25. Besides the CBC mode, the CFB mode can be used for the generation of a MAC. The plaintext consists of the blocks $M_1, ..., M_n$, and we set the initialization vector $C_0 := M_1$. Now, we encrypt $M_2, ..., M_n$ in CFB mode with key K, which results in the ciphertexts $C_1, ..., C_{n-1}$. 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 $C_0 := 0$.

Exercise 26. Assume the following one-way hash function for messages m of length l. n denotes the product of two primes.

i) The initial value is $h_0 = 0$.

ii) Calculate $h_i \equiv 2^{(h_{i-1}+m_i)} \pmod n$ for $i \in 1, ..., l$.

(a) Calculate the hash value $h(m) = h_l$ for the message $m = (3, 33, 13, 25)$ with the given function using $n = 221$.

(b) Sign the hash of the message given above with the ElGamal signature scheme. Use the parameters $p := 4793, x_A := 9177, a := 4792$ and the session key $k = 2811$. Before signing, check if these parameters fulfill the requirements of the signature scheme. If necessary, a parameter can be substituted by the corresponding $p := 8501, x_A := 257$ or $a := 1400$.