RWTH AACHEN UNIVERSITY

Lehrstuhl für Theoretische Informationstechnik

Exercise 6 in Advanced Methods of Cryptography

Prof. Dr. Rudolf Mathar, Henning Maier, Markus Rothe

2014-11-28

Problem 17. *(basic requirements for cryptographic hash functions)* 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 each.
$c \leftarrow E_{m_0}(m_0)$
for $i$ in $1..(n-1)$ do
    $d \leftarrow E_{m_0}(m_i)$
    $c \leftarrow c \oplus d$
end for
$h(m) \leftarrow c$
```

a) Does this function fulfill the basic requirements for a cryptographic hash function?

b) Can these requirements be fulfilled by replacing the operation XOR ($\oplus$) by AND ($\odot$)?

Problem 18. *(codomain of a hash function)* Consider the following hash-function:

$$h: \ \mathbb{N} \to \mathbb{N}_0, \ k \mapsto \lfloor 10000(k(1+\sqrt{5})/2 - \lfloor k(1+\sqrt{5})/2) \rfloor) \rfloor .$$

a) Determine the upper and lower bounds of the codomain of h.

b) Find a collision for h.

Problem 19. *(CBC and CFB for MAC generation)* Both, the CBC mode and the CFB mode, can be used for the generation of a MAC as follows.

- A plaintext is divided into n equally-sized blocks $M_1, ..., M_n$.
- For the CFB-MAC, the ciphertexts are $C_i = M_{i+1} \oplus E_K(C_{i-1})$ for $i = 1, \dots, n-1$ and $\mathrm{MAC}_K^{(n)} = E_K(C_{n-1})$ with initial value $C_0 = M_1$.
- For the CBC-MAC, the ciphertexts are $\hat{C}_i = E_K(\hat{C}_{i-1} \oplus M_i)$ for $i = 1, \dots, n-1$ and $\widehat{\mathrm{MAC}}_K^{(n)} = E_K(\hat{C}_{n-1} \oplus M_n)$ with initial value $\hat{C}_0 = 0$.

Show that the equivalency $\mathrm{MAC}_K^{(n)} = \widehat{\mathrm{MAC}}_K^{(n)}$ holds.

Problem 20. *(derive a message validation protocol)* Suppose Alice transmits the following cryptogram to Bob:

$$c = e(m \parallel h(k_2 \parallel m), k_1).$$

Assume that the message m, the shared keys k_1, k_2, the hash values $h(x)$ and the output of the encryption function have fixed lengths known to Alice and Bob.

a) Derive a protocol for decryption and message validation used by Bob?

b) Modify the given scheme to construct a similar protocol for a public-key cryptosystem. You may use two private-/public key-pairs (K_1, L_1) and (K_2, L_2) and a session key s used in the hash, which is securely transmitted to Bob within the cryptogram c.

c) How can an intruder Eve impersonate Alice to Bob in the system of (b)? How could the attack be prevented?