Prof. Dr. Rudolf Mathar, Dr. Michael Reyer, Jose Leon, Qinwei He

Exercise 5

Friday, November 24, 2017

Problem 1. *(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 2. *(forging an ElGamal signature with hash function)* An attacker has intercepted one valid signature (r, s) of the ElGamal signature scheme and a hashed message $h(m)$ which is invertible modulo $p - 1$.

Show that the attacker can generate a signature (r', s') for any hashed message $h(m')$, if $1 \leq r < p$ is not verified.

Problem 3. *(forging an ElGamal signature without hash function)* Let p be prime with $p \equiv 3 \mod 4$, and let a be a primitive element modulo p. Furthermore, let $y \equiv a^x \mod p$ be a public ElGamal key and let $a \mid p-1$. Here, no hash function is used for the ElGamal signature. Assume that it is possible to find $z \in \mathbb{Z}$ such that $a^{rz} \equiv y^r \mod p$.

Show that (r, s) with $s = (p-3)2^{-1}(m - rz)$ yields a valid ElGamal signature for a chosen message m.