Prof. Dr. Rudolf Mathar, Jose Calvo, Markus Rothe

Tutorial 7

Friday, December 18, 2015

Problem 1. *(verifying an ElGamal signature)* The hashed message $h(m) = 65$ was signed using the ElGamal signature scheme with public parameters $y = 399$, $p = 859$, and $a = 206$.

Verify the signature $(r, s) = (373, 15)$.

Problem 2. *(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.

Problem 3. *(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 4. *(variations of the ElGamal signature scheme)* The ElGamal signature scheme computes the signature as $s = k^{-1}(h(m) - xr) \mod (p-1)$. Consider the following variations of the ElGamal signature scheme.

a) Consider the signing equation $s = x^{-1}(h(m) - kr) \mod (p-1)$.
Show that $a^{h(m)} \equiv y^s r^r \mod p$ is a valid verification procedure.

b) Consider the signing equation $s = xh(m) + kr \mod (p-1)$.
Propose a valid verification procedure.

c) Consider the signing equation $s = xr + kh(m) \mod (p-1)$.
Propose a valid verification procedure.