# Homework 8 in Advanced Methods of Cryptography

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

07.12.2010

**Exercise 27.** In the verification step of the ElGamal-Signature one first checks, whether $1 \leq r < p$. Show that an attacker can generate a signature for an arbitrary message $m'$ by intercepting one valid signature $(r, s)$ for a message $m$ if this step is omitted.

Hint: Assume that $h(m)$ is invertible modulo $p - 1$.

**Exercise 28.** Let $p$ prime, $p \equiv 3 \pmod 4$, and $a$ a primitive root modulo $p$. Furthermore, let $y \equiv a^x \pmod p$ a public ElGamal key and let $a \mid p - 1$.

Assume that it is possible to find $z \in \mathbb{Z}$ such that $a^{rz} \equiv y^r \pmod p$.

Show that $(r, s)$ with

$$s = \frac{p-3}{2}(h(m) - rz)$$

is a valid ElGamal signature for a chosen message $m$.

**Exercise 29.** We consider the parameter generation algorithm of DSA.

Given $2^{159} < q < 2^{160}$ and $0 \leq t \leq 8$ such that $2^{511+64t} < p < 2^{512+64t}$ and $q|p - 1$.

Given the following algorithm:

1) Select $g \in \mathbb{Z}_p^*$.
2) Compute $a = g^{\frac{p-1}{q}}$.
3) If $a = 1$ go to 1).
4) Else return $a$.

Prove that $a$ is a generator of the cyclic subgroup of order $q$ in $\mathbb{Z}_p^*$.