# Homework 3 in Advanced Methods of Cryptography

Prof. Dr. Rudolf Mathar, Michael Reyer, Henning Maier

08.11.2011

## Exercise 8.

Prove *Euler's criterion* (cf. *Proposition 9.2* given in the lecture notes):
Let $p > 2$ be prime. $c \in \mathbb{Z}_p^*$ is a quadratic residue mod $p$ if and only if $c^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.

## Exercise 9.

Alice and Bob are using the Rabin cryptosystem. Bob's public key is $n = 4757$. All integers in the set $\{1, \ldots, n-1\}$ are represented by sequences of 13 bits. In order to identify the correct message, Alice and Bob agreed to only send messages with the last 2 bits set to 1. Suppose Alice sends the cryptogram $c = 1935$:

(a) Find the private key by factoring the public key $n = pq$.

(b) Decipher the cryptogram c and identify the correct message $m$.

## Exercise 10.

Consider the coin flipping protocol. Let $p > 2$ be prime.

(a) Show that if $x \equiv -x \pmod{p}$, then $x \equiv 0 \pmod{p}$.

(b) Suppose $x, y \not\equiv 0 \pmod{p}$ and $x^2 \equiv y^2 \pmod{p^2}$. Show that $x \equiv \pm y \pmod{p^2}$.

(c) Suppose Alice cheats when flipping coins over the telephone by choosing $p = q$. Show that Bob always loses if he trusts Alice.

(d) Bob suspects that Alice has cheated. Why is it not wise for Alice to choose $n = p^2$ as secret key, can Bob discover her attempt to cheat? Can Bob use her cheat as an advantage for himself?