Lehrstuhl für
Theoretische Informationstechnik

RHEINISCH-
WESTFÄLISCHE
TECHNISCHE
HOCHSCHULE
AACHEN

Homework 1 in Cryptography II

Prof. Dr. Rudolf Mathar, Wolfgang Meyer zu Bergsten
24.04.2008

Exercise 1. Prove the Euler criterion:
Let $p > 2$ be prime. $c \in \mathbb{Z}_p^*$ is a quadratic residue modulo p iff $c^{\frac{p-1}{2}} \equiv 1 \bmod p$.

Excercise 2. 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 as bit sequences with 13 bits. In order to be able to identify the correct message, Alice and Bob agreed to only send messages with the first 2 bits and the last 2 bits being equal. Alice sends the cryptogram $c = 1935$. Decipher this cryptogram.

Excercise 3. Create a signature scheme based on the Rabin cryptosystem. With this signature scheme, generate the signature for the message $m = 12211$ and the public key $n = 30353$ (without a hash or redundancy function).
Hint: There is a signature scheme based on RSA.