RWTH AACHEN UNIVERSITY Lehrstuhl für Theoretische Informationstechnik

Homework 4 in Cryptography II

Prof. Dr. Rudolf Mathar, Wolfgang Meyer zu Bergsten, Michael Reyer

14.05.2009

Exercise 11. Alice and Bob are using the Rabin cryptosystem. Bob's public key is $n = 4757$. All integers in the set $\{1, \dots, n-1\}$ 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.

Exercise 12. 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.

Exercise 13. Let $p > 2$ be prime. Let $\left(\frac{a}{p}\right)$ be the Legendre symbol. Prove the following calculation rules.

(a) $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$

(b) $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$

(c) $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$, if $a \equiv b \mod p$