Homework 3 in Advanced Methods of Cryptography

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

02.11.2010

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 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 last 2 bits set to 1. Alice sends the cryptogram $c = 1935$. Decipher this cryptogram.

Exercise 10.

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 $n = 30353$.
Hint: There is a signature scheme based on RSA.

Exercise 11. 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?