Homework 3 in Cryptography II

Prof. Dr. Rudolf Mathar, Wolfgang Meyer zu Bergsten, Steven Corroy

18.05.2010

Exercise 8.

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 9.

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 $a \equiv b \mod p$

Exercise 10.

Show that Algorithm 6 from the lecture notes calculates the Jacobi symbol.

Hint: Use the following equations for any odd integers $n, m > 2$.

$$\begin{aligned} \left(\frac{m}{n}\right) &= (-1)^{\frac{m-1}{2}\frac{n-1}{2}} \cdot \left(\frac{n}{m}\right) \quad \text{law of quadratic reciprocity} \\ \left(\frac{2}{n}\right) &= (-1)^{\frac{n^2-1}{8}} \end{aligned}$$