Prof. Dr. Rudolf Mathar, Jose Calvo, Markus Rothe

Tutorial 3

Friday, November 13, 2015

Problem 1. *(coin flipping)* Consider the coin flipping protocol. Let $p > 2$ be prime.

a) Show that if $x \equiv -x \mod p$, then $x \equiv 0 \mod p$.

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

c) Alice chooses $n = p^2$ as the secret key, but Bob suspects that Alice has cheated. Can Bob discover her attempt to cheat? Can Bob use Alice' cheating as an advantage for himself?

Problem 2. *(Legendre symbol)* Let $\left(\frac{a}{p}\right)$ be the Legendre symbol, with $p > 2$ prime. 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 $a \equiv b \mod p$

Problem 3. *(Jacobi symbol)* Show that Algorithm 6 from the lecture notes computes the Jacobi symbol.

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

$$\left(\frac{m}{n}\right) = (-1)^{\frac{m-1}{2}\frac{n-1}{2}} \cdot \left(\frac{n}{m}\right) \qquad \text{law of quadratic reciprocity}$$

$$\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$$