Lehrstuhl für
Theoretische Informationstechnik

RHEINISCH-
WESTFÄLISCHE
TECHNISCHE
HOCHSCHULE
AACHEN

Homework 2 in Cryptography II

Prof. Dr. Rudolf Mathar, Wolfgang Meyer zu Bergsten

08.05.2008

Excercise 4. 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 $a \equiv b \mod p$.

Excercise 5. Show that Algorithm 6 from the lecture notes calculates the Jacobi symbol.

Excercise 6. Bob gets the message

$$(10101011100001101000101110010111110011011100 0, 1306)$$

from Alice. This message was encrypted with the Blum-Goldwasser Cryptosystem with the public key $n = 1333$. The number 1306 represents x_{10}. Decrypt this message.

Note: The security requirement to only use a maximum of $\log_2(\log_2(n))$ bits of the BBS generator is violated in this example. Instead, 5 bits of output are used.

Note: The letters of the alphabet $A, \ldots, Z$ are represented in the following way by 5 bits: $A = 00000,\ B = 00001, \ldots,\ Z = 11001$.