Homework 5 in Cryptography II

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

28.05.2009

Exercise 14. Show that Algorithm 6 from the lecture notes calculates the Jacobi symbol.

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

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

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

Exercise 15. Let p be prime, g a primitive element modulo p and $a, b \in \mathbb{Z}_p^*$. Show the following:

(a) a is a quadratic residue modulo p if and only if there exists an even $i \in \mathbb{N}_0$ with $a \equiv g^i \pmod{p}$.

(b) If p is odd, then exactly one half of the elements $x \in \mathbb{Z}_p^*$ are quadratic residues modulo p.

(c) The product ab is a quadratic residue modulo p if and only if a and b are both either quadratic residues or quadratic non-residues modulo p.

Exercise 16. Establish a message decryption with the Goldwasser-Micali cryptosystem. Start by finding the cryptosystem's parameters.

(a) Find a pseudo-square modulo $n = p \cdot q = 31 \cdot 79$ using the algorithm from the lecture notes. Start with $a = 10$ and increase a by 1 until you find a quadratic non-residue modulo p. For b, start with $b = 17$ and proceed analoguously.

(b) Decrypt the ciphertext $c = (1418, 2150, 2153)$.