Chair for Theoretical Information Technology | RWTH AACHEN UNIVERSITY

Prof. Dr. Rudolf Mathar, Dr. Arash Behboodi, Markus Rothe

Exercise 12

Friday, July 13, 2018

Problem 1. *(exponential congruences)* Let $x, y \in \mathbb{Z}, a \in \mathbb{Z}_n^\star \setminus \{1\}$, and $\mathrm{ord}_n(a) = \min\{k \in \{1, \dots, \varphi(n)\} \mid a^k \equiv 1 \mod n\}$. Show that

$$a^x \equiv a^y \mod n \iff x \equiv y \mod \mathrm{ord}_n(a)\,.$$

Problem 2. (*How not to use the ElGamal cryptoystem*) Alice and Bob are using the ElGamal cryptosystem. The public key of Alice is $(p, a, y) = (3571, 2, 2905)$. Bob encrypts the messages m_1 and m_2 as

$$\mathbf{C}_1 = (1537, 2192) \text{ and } \mathbf{C}_2 = (1537, 1393).$$

a) Show that the public key is valid.

b) What did Bob do wrong?

c) The first message is given as $m_1 = 567$. Determine the message m_2.

Problem 3. *(properties of quadratic residues)* 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 $a \equiv g^i \mod p$.

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 $a \cdot b$ is a quadratic residue modulo p if and only if a and b are both either quadratic residues or quadratic non-residues modulo p.

Problem 4. *(Euler's criterion)* Prove Euler's criterion (Proposition 9.2): Let $p > 2$ be prime, then

$$c \in \mathbb{Z}_p^* \text{ is a quadratic residue modulo } p \Leftrightarrow c^{\frac{p-1}{2}} \equiv 1 \mod p\,.$$