Homework 2 in Cryptography II

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

11.05.2010

Exercise 5.

Prove Euler's criterion: Let $p > 2$ be prime, then

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

Exercise 6. Alice and Bob are using the Rabin cryptosystem. Bob's public key is $n = 4757$. All integers in the set $\{1, \ldots, n-1\}$ are represented as bit sequences with 13 bits. In order to be able to identify the correct message, Alice and Bob agreed to only send messages with the last 2 bits set to 1. Alice sends the cryptogram $c = 1935$. Decipher this cryptogram.

Exercise 7. Alice is using the ElGamal encryption system for encrypting the messages m_1 and m_2. The generated cryptograms are

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

The public key of Alice is $(p, a, y) = (3571, 2, 2905)$.

a) What did Alice do wrong?

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