Homework 2 in Cryptography II

Prof. Dr. Rudolf Mathar, Peter Schwabe

26.04.2007

Exercise 4.
Prove Euler's criterion: Let $p > 2$ be prime, then

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

Exercise 5.
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 first 2 bits and the last 2 bits being equal. Alice sends the cryptogram $c = 1935$. Decipher this cryptogram.

Exercise 6.
An element $a \in \mathbb{Z}_n^*$ is called an *m-th power residue modulo n* if and only if there exists $x \in Z_n^*$ with $x^m \equiv a \pmod{n}$.

Prove the following statement:
Suppose $\mathbb{Z}_n^*$ is cyclic and $a \in \mathbb{Z}_n^*$. Then a is an m-th power residue modulo n, if and only if $a^{\varphi(n)/d} \equiv 1 \pmod{n}$, where $d = \gcd(m, \varphi(n))$.