Prof. Dr. Rudolf Mathar, Jose Calvo, Markus Rothe

Tutorial 2

Friday, November 6, 2015

Problem 1. *(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 2. *(modified Rabin cryptosystem)* Consider the modification of the Rabin Cryptosystem in which $e_K(m) = c = m \cdot (m + B) \mod n$, where $B \in \mathbb{Z}_n$ is part of the public key. Supposing that $p = 199$, $q = 211$, $n = pq$, and $B = 1357$, perform the following computations.

a) Compute the encryption $y = e_K(32767)$.

b) Determine the four possible decryptions of this given ciphertext y.

Problem 3. *(Rabin cryptosystem)* Alice and Bob are using the Rabin Cryptosystem. Bob uses the public key $n = 4757 = 67 \cdot 71$. All integers in the set $\{1, \ldots, n-1\}$ are represented as a bit sequence of 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.