IV054 Coding, Cryptography and Cryptographic Protocols

2009 – Exercises VI.

1. Let $p = 541$, $q = 2$ and $x = 101$. Decrypt the following ElGamal ciphers $c_1 = (54, 300)$ and $c_2 = (54, 301)$.

2. Consider the Generalized Rabin cryptosystem with $p = 31$, $q = 59$ and $B = 15$. Suppose we want to transmit the message $m = 20$. Show in detail encryption and decryption steps.

3. Let p, q be distinct primes such that $p \equiv q \equiv 3 \pmod 4$. Consider the following encryption scheme for encryption of 1-bit messages.
   Public key is a number $n = pq$ and private key is a pair (p, q). Message m is encrypted by computing $c = (-1)^m r^2 \pmod n$ where $r \in \{1, \ldots, n-1\}$ is randomly chosen and $gcd(r, n) = 1$. After receiving the cryptotext the receiver determines whether it is a quadratic residue or not and decrypts.

   a) Show correctness of this encryption scheme.

   b) Show that given a public key n and cryptotexts c_1, c_2 that were computed using n and encrypt messages m_1, m_2 it is possible to efficiently compute a cryptotext c' that encrypts a message $m' = m_1 \oplus m_2$ without knowing neither m_1 nor m_2.

   c) Show that given a public key n and a cryptotext c that encrypts a message m it is possible to efficiently generate a random cryptotext c^* which encrypts m too (again, without knowing m).

4. a) Find all solutions of the congruence $x^2 \equiv 2 \pmod{1081}$. Use the Chinese Remainder Theorem.

   b) Find all solutions of the congruence $x^{10} \equiv 1 \pmod{101}$. Use the fact that 2 is a generator of the group $(\mathbb{Z}_{101}^*, \cdot)$.

5. $r \in Z_n^*$ is called a quadratic residue modulo n if there is $s \in Z_n^*$ such that $s^2 \equiv r \pmod n$. Show that the set Q of all quadratic residues modulo n is a subgroup of the group $(\mathbb{Z}_n^*, \cdot)$.

6. Consider the uniform distribution of birthdays in a 365-day year and a group of 50 people. What is the probability that two people in the group have a birthday on the same day?
   From the original group 23 people have been chosen. What is the probability of two of them having a birthday on the same day?