*IV054 Coding, Cryptography and Cryptographic Protocols*
**2013 - Exercises VI.**

1. Let $p = 31$ and $q = 7$ be the private keys of the Rabin cryptosystem.
   (a) Encrypt message $m = 53$ to obtain cryptotext $c$.
   (b) Decrypt cryptotext $c$. During the computation you will have to use the Chinese Remainder Theorem four times. Show all computation steps for at least one instance.
2. Use the Shanks algorithm to compute $\log_5 67 \pmod{173}$. Show computation in detail.
3. Consider a variant of Rabin cryptosystem which uses a public key $n = pqr$, where $p$, $q$, $r$ are prime numbers.
   (a) How many possible plaintexts do we obtain after decryption?
   (b) Find a decryption of cryptotext $c = 191$ using private keys $p = 5$, $q = 7$ and $r = 11$.
4. Let $g$ be a generator of the group $(\mathbb{Z}_p^*, \cdot)$. Show that there is a $k \in \mathbb{N}$ such that $g^{k+1} \equiv g^k + 1 \pmod{p}$.
5. Notice that decryption in the Rabin cryptosystem is non-deterministic. Show that we can make decryption deterministic by adding some redundancy in plaintext.
6. Consider the subset of all negligible functions defined as follows:

$$G = \{\rho \,|\, \rho \text{ is a negligible function with } \mathrm{Im}(\rho) \subseteq \mathbb{N}\}.$$

   Which of the following is $(G, \circ)$, if any:
   - semigroup;
   - monoid;
   - group;
   - Abelian group.

   How would the previous answer change if we modify the previous definition of $G$ as follows. Could $G$ be described more accurately in these cases?
   (a) $G = \{\rho \,|\, \rho \text{ is a negligible function with } \mathrm{Im}(\rho) \subseteq \mathbb{N}, \rho \text{ is a strictly increasing function}\}$;
   (b) $G = \{\rho \,|\, \rho \text{ is a negligible function with } \mathrm{Im}(\rho) \subseteq \mathbb{N}, \rho \text{ is a strictly decreasing function}\}$.
7. Let $p$ be a prime. Answer the following questions including proofs of your claims.
   (a) Discuss the number of solutions of the following equation for different values of $a$ and $p$:

$$x^2 \equiv a \pmod{p}.$$

   (b) What is the relationship between the set of primitive elements of the group $(\mathbb{Z}_p^*, \cdot)$ and:
   – the set of quadratic residues modulo $p$
   – the set of quadratic non-residues modulo $p$

   Consider the following cases:
   - $p$ is even;
   - $p$ is odd:
     - $p \equiv 1 \pmod{4}$;
     - $p \equiv 3 \pmod{4}$.

   (Choose from the following relations: trivial subset/superset, nontrivial subset/superset, disjoint sets or neither of these).

More on next page >>>

(c) Determine a necessary and sufficient condition (based on $a, b, d, p$) such that the equation

$$ax^2 + bx \equiv d \pmod{p}$$

has a solution in $\mathbb{Z}_p$ ($a$, $b$, $d \in \mathbb{Z}$). Discuss the number of solutions.

(d) Determine for which primes $p$ the following equation has solution in $\mathbb{Z}_p$:

$$6x^2 + 7x + 2 \equiv 0 \pmod{p}.$$

Discuss the number of solutions. Express the solutions as a linear combination of elements from $(\mathbb{Z}_p, +, \cdot)$.