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

1. Let $p$ be a large prime. Let $g < p$ be an integer such that $g$ is a generator of the group $(\mathbb{Z}_p^*, \cdot)$. Discuss security of the following commitment scheme for numbers from $\{0, 1, \ldots, p-1\}$:

   *Commit* To commit to $m$ Alice randomly chooses $r \in \{0, 1, \ldots, p-1\}$ and sends $c = g^r m \pmod p$ to Bob.

   *Open* To open her commitment Alice sends $r$ and $m$ to Bob.

2. Peggy and Vic play the following game. They have very large paper full of small, randomly placed, letters and digits but there is only one digit 7. The goal is to find 7 sooner than the other player. After some time Peggy found 7 but Vic does not believe her. How can Peggy prove to Vic that she knows the position of 7 without revealing it. A non-cryptographic solution is acceptable.

3. Consider the coin flipping by telephone (Protocol 2 from the lecture). Let $p = 227$, $q = 179$ and $x = 13548$. Show computation steps in detail.

4. For given two non-isomorphic graphs $G$ and $H$ of $n$ vertices, Peggy tries to convince Victor that $G \ncong H$. Suppose she has an efficient way of distinguishing non-isomorphic graphs and she does not want to reveal him any information about it. Take a look at the following protocol:

   (a) Victor takes a disjoint graph $\langle G, H\rangle$ and relabels it as $\langle F_1, F_2\rangle$ in a random order. Then he passes the new graph to Peggy, while keeping the relabelling in private.

   (b) Peggy determines which of $F_1$ and $F_2$ is isomorphic to $G$.

   (c) Repeat the steps (a) and (b) until Victor is convinced.

   What is wrong with the proposed proof? Give a way to correct it.

5. Consider edge-matching puzzles. That is, a puzzle (similar to jigsaw puzzles) where:

   - pieces are identically shaped (for simplicity, consider squares and $\sqrt{n} \times \sqrt{n}$ grid);
   - it can be verified in $\Theta(1)$ whether two edges of two pieces match (assume only edges can match or mismatch);
   - there is no global image to guide a puzzle solver;
   - the fact that pieces match locally does not guarantee that the pieces stay together in this position in the overall solution.

   (a) Propose a zero-knowledge proof protocol that convinces Victor that Peggy has the solution (note the problem is NP complete).
   Prove that your solution is a zero-knowledge proof protocol. Show soundness error of your protocol (when performed only once, and when performed $k$ times).

   (b) Is your zero-knowledge proof protocol valid even if one can distinguish whether a piece belongs to the edge of the grid, to a corner, or neither of those? Does this change complexity of the task?

6. Consider `Bit commitment scheme I` presented on slide 13 in the lecture.

   (a) For which $n$ would the scheme be binding if we used $m \in \mathbb{Z}_n^*$ instead of $\mathrm{QNR}(n)$?

   (b) What is the cardinality of $\mathrm{QNR}^*(n)$ for $n = pq$ ($p$ and $q$ primes), where $\mathrm{QNR}^*(n)$ is the set of invertible quadratic non-residues?