IV054 Coding, Cryptography and Cryptographic Protocols
2012 - Exercises X.

1. Consider the coin-flipping by telephone protocol (Protocol 2 from the lecture). Let $p = 19$, $q = 23$ and $y = 192$. Show computation steps in detail.

2. The following thread appeared in the discussion group of IV054 after the notebook score statistics in Information System had broken:

   "Colleagues, I would like to know what is the average of points we have received for our assignments."

   How would you solve this problem if students do not want to individually reveal the number of points they have received?

3. Let $n = pq$ where p, q are primes. Propose an interactive proof system which allows Peggy to prove to Victor that $a \in \mathbb{Z}_n^*$ is not a quadratic residue mod n. For both honest and dishonest Victor, decide whether your protocol has the zero-knowledge property. Explain your reasoning.

4. Despite being very far from each other, Alice and Bob have decided to play poker. They have invented the following protocol to deal cards:

   (a) Let $p = 2q + 1$ where p, q are primes and let g be a generator of a subgroup of order q in $\mathbb{Z}_p^*$.

   (b) Alice has a public key $y_A = g^{x_A} \pmod p$ and Bob has a public key $y_B = g^{x_B} \pmod p$ where $x_A, x_B \in \mathbb{Z}_q$.

   (c) The cards are represented by a set $\{y_1, \dots, y_{52}\}$ of mutually different quadratic residues mod p known to both Alice and Bob.

   (d) Alice for each $i \in \{1, \dots, 52\}$ independently and randomly chooses r_i from $\mathbb{Z}_q$ and computes a pair $C_i = (g^{r_i} \pmod p,\ y_A^{r_i} y_i \pmod p)$. Then she randomly permutes these pairs and sends them to Bob.

   (e) Bob randomly chooses five pairs from the received pairs (let us denote them $C_1^*, \dots, C_5^*$) and sends them to Alice. These pairs represent Alice's cards.

   (f) Bob randomly chooses five pairs from the remaining pairs (let us denote them $C_1' = (z_{1,1},\ z_{1,2}), \dots, C_5' = (z_{5,1}, z_{5,2})$). For each $i \in \{1, \dots, 5\}$ Bob independently and randomly chooses r_i', s_i from $\mathbb{Z}_q$, computes a triplet

   $$C_i'' = (g^{r_i'} \pmod p,\ z_{i,1} g^{s_i} \pmod p,\ z_{i,2} y_B^{r_i'} y_A^{s_i} \pmod p)$$

   and sends these triplets to Alice.

   (g) For each received triplet $C_i'' = (w_{i,1},\ w_{i,2},\ w_{i,3})$, where $i \in \{1, \dots, 5\}$, Alice computes a pair $C_i^R = (w_{i,1},\ \frac{w_{i,3}}{w_{i,2}^{x_A}} \pmod p)$ and sends these pairs to Bob. These pairs represent Bob's cards.

   Prove that both Alice and Bob can compute which cards they have.

5. Does the 3-SAT problem have a zero-knowledge proof? Discuss.

6. Show how to construct a bit–commitment scheme from a cryptographically secure pseudo–random generator G. Discuss the binding and hiding properties of your protocol.

7. Let $m = pq$ be a modulus and let y be a quadratic non-residue modulo m. Consider the following bit commitment scheme:

   $$commit(r, b) = y^b r^2 \pmod m$$

   where $r \in \mathbb{Z}_m^*$ and $b \in \{0, 1\}$. Is the proposed scheme

   (a) binding (computationally or perfectly)?

   (b) hiding (computationally or perfectly)?