IV054 Coding, Cryptography and Cryptographic Protocols
2020 - Exercises X.

1. *(4 points)* Consider the following commitment scheme, with the following public information: p a large prime, g a primitive root of $\mathbb{Z}_p^*$. The commitment function is

$$\text{commit}(r, x) = g^r x \mod p,$$

where the committed value x is an element of $\mathbb{Z}_p^*$ and $0 < r < p - 1$ a random integer.

   (a) Define the reveal phase of this protocol.
   (b) Is this protocol hiding?
   (c) Is this protocol binding?

2. *(6 points)* Consider the following modification of ElGamal encryption.
Design elements: A large prime p, q a primitive element of $\mathbb{Z}_p^*$, $y = q^x \mod p$
Public key: p, q, y
Private key: x
Encryption of message M: Choose a random r and compute: $a = q^r \mod p$, $b = y^r q^M$.
Decryption of message (a, b): First calculate $q^M = ba^{-x} \mod p$. Then use Shank's algorithm to obtain M from q^M (this can be done in time $\mathcal{O}(\sqrt{|M|})$, therefore it is efficient for a small message space).

   Show that a trusted tallier can use this cryptosystem to implement an electronic voting system where ℓ voters can cast votes $v_i \in \{0, 1\} \simeq \{\text{no, yes}\}$.

3. *(6 points)* Consider the following coin-tossing protocol using a one-to-one function $f : \{0,1\}^n \to \{0,1\}^{3n}$:

   i. Bob picks a random $r \in \{0,1\}^{3n}$ and sends it to Alice.
   ii. Alice picks a random $x \in \{0,1\}^n$ and computes $f(x)$.
   iii. Alice picks a random $c \in \{0,1\}$. If $c = 0$ she sends $f(x)$ to Bob and $f(x) \oplus r$ otherwise.
   iv. Bob guesses c and tells Alice his guess.
   v. The coin toss is then head if Bob guessed correctly, tail otherwise.

   (a) How does Alice prove to Bob whether his guess was correct or not?
   (b) How can Alice cheat if she is not computationally bounded at all? Show that in such a case her probability of successfully cheating is still only at most 2^{-n}.

4. *(4 points)* Consider the following zero-knowledge protocol where one party P commits to a positive integer value $x \in \{1, \dots, 100\}$ in such a way that she or he can later prove that the committed value is greater than a value y, $y \le x$, chosen by another party V, without revealing the value of x. The protocol goes as follows:

   i. P chooses a secret $s_0 \in \{0,1\}^{2n}$ and computes $H(s_0) = s$ where H is a secure hash function $H : \{0,1\}^* \to \{0,1\}^n$.
   ii. To commit to x, P computes $\mathit{commit}(x) = H^x(s)$ and sends it to V.
   $H^x(s)$ denotes composing H x times: $H(\cdots H(H(s))\cdots)$
   iii. V chooses y, $y \le x$ and queries P to give a proof that the value x he had committed to is greater than y.

   (a) Show how this protocol continues so as P proves to V that $y \le x$ without revealing x.
   (b) Suppose that the goal is to prove that $x \le q$. Propose a modification of the protocol that achieves this goal.

More on next page >>>

5. *(5 points)* Consider the following version of the zero-knowledge proof for graph 3-coloring problem.

   Peggy claims that she can color the graph $G = (V, E)$ with colors (red, blue, green). Let $v_1, \ldots, v_n$ be its vertices. Peggy performs with Vic the following interactions $t \gg |E|$ times.
   Peggy: Selects a random permutation π of colors.
   Peggy: For each vertex create two commitments of the permuted colors $c_i = \mathit{commit}(v_i, \pi(\text{color of } v_i))$ and $c'_i = \mathit{commit}'(v_i, \pi(\text{color of } v_i))$ and sends them to Vic.
   Vic: Chooses uniformly at random two edges $e = (v_j, v_k)$ and $e' = (v_l, v_m)$ and asks Peggy to open commitments c_j, c_k of the vertices v_j, v_k forming the first edge and c'_l, c'_m of the second edge.
   Peggy: Opens the commitments c_j, c_k and c'_l, c'_m.
   Vic: Checks that the committed colors of the vertices forming the edge e are different otherwise rejects. He does the same for the edge e'.

   Decide whether the protocol fulfills the following properties. Prove your answer.

   (a) completeness (show that if Peggy knows 3-coloring of the graph G, she can answer all Vic's challenges);
   (b) soundness (calculate the probability of Vic rejecting after t rounds in case Peggy does not know 3-coloring of the graph G);
   (c) zero-knowledge.

6. *(Xmas bonus, 3 points)* You have received the following picture of Nativity scene from personal collection of Professor Gruska:

(image file attached in PDF or you can find it in study materials).