IV054 Coding, Cryptography and Cryptographic Protocols
2018 - Exercises X.

1. Consider the Protocol 2 for coin-flipping by phone from the lecture with the following parameters: $p = 31$, $q = 43$ and $x = 354$. Describe the steps in details.

2. Suppose that for the last homework assignment score statistics from teacher's notebook was not published in the information system and you want to compute with your colleagues the average score of points. How would you solve this problem if your colleagues do not want to individually reveal the number of received points?

3. Consider the following commitment scheme, with public information as follows: p a large prime, q a large prime dividing $(p-1)$, $g \in \mathbb{Z}_p^*$ of order q, and $h = g^k \mod p$, with $0 < k < q$ a random integer not known to any party. The commitment function is

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

   where x is the committed bit and $0 < r < q$ is a random integer.

   (a) Define the reveal phase of this protocol.

   (b) Discuss the binding and hiding properties of this protocol. Are they computationally/information theoretically secure?

   (c) What happens if Bob (the receiver) knows $\log_g h$?

   (d) What happens if Alice (the sender) knows $\log_g h$?

4. Consider the following coin flip protocol. Let $n = pq$, where p and q are large primes.

   i. Alice generates a random integer $0 \leq a < n - 1$ and sends $c = a^2 \mod n$ as her commitment to Bob.

   ii. Bob guesses the parity of a and tells his guess to Alice.

   iii. Alice reveals a to Bob and Bob checks that $c = a^2 \mod n$.

   iv. If Bob guessed correctly, he wins the coin flip.

   Is the proposed protocol fair?

5. Assuming the infeasibility of computing discrete logarithms, show that the commitment scheme based on discrete logarithm from the lecture is computationally binding.

6. Alice and Bob used the Diffie-Hellman key exchange protocol to agree on a shared symmetric cipher key. Peggy and Victor intercepted their communication and Peggy somehow found out the key. She wants to sell the key to Victor. Peggy will not reveal the key until Victor pays her, but Victor first wants to be sure Peggy actually knows the key.
   How can Peggy convince Victor that she knows the key without revealing any information about the key, such that Victor is at least 99% sure that Peggy is not lying?

7. Consider the commitment scheme based on discrete logarithm from the lecture with commitment phase simplified to be $c = g^r m \mod p$ to commit an $m \in \mathbb{Z}_p$. Discuss the binding and hiding properties of this scheme.