COMP 4901W – Homework 1

A. K. Goharshady

Release Date: February 21, 2022
Deadline: March 8th, 2022 (23:59 HKT)

This homework accounts for 10% of your total grade. You should submit your solutions on Canvas as a single pdf file. Handwritten and scanned solutions will not be accepted since the TAs might be unable to read your handwriting. However, you can draw your figures, if any, by hand. You are also allowed to discuss the problems with your classmates but you have to write your solution on your own. All submissions will go through a plagiarism check. The deadline is firm and no extensions will be granted. You will receive feedback on your submission and normally be allowed to resubmit once. We reserve the right to disallow resubmissions if your original submission is of a very low quality or shows a lack of effort.

Exercise 1

This exercise accounts for 5% of your total grade.

Alice and Bob want to play rock-paper-scissors over the internet. Assume that any message sent over the internet will be delivered in at most 1 minute. However, there might be malicious actors on the network who try to impersonate Alice or Bob or otherwise tamper with the result of the game. Also, both Alice and Bob might want to cheat in order to win the game or at least increase their chance of winning.

1. Design a secure protocol for playing rock-paper-scissors. Formally specify the steps, the time between the steps and the cryptographic primitives used in the protocol.
2. Can either party cheat in this protocol? If so, can the cheating be provably detected? If it cannot be provably detected, go back to Step 1 and design a better protocol.
3. Prove that your protocol is immune to tampering by Alice, Bob or any third party on the network. In your proof, mention explicitly which properties of each primitive are being used in each part of the argument.

Exercise 2

This exercise accounts for 5% of your total grade.

Alice and Bob want to communicate over an unsecured network, e.g. the internet. Each message m in their communications is simply a word out of a predefined English dictionary. They know of symmetric cryptography and decide to use a variant of one-time pad. Their variant uses prime numbers instead of xor. They first choose a large prime number p and announce it on the network. They also use a shared secret key $k \in \{0, 1, \ldots, p-1\}$ that is known only to Alice and Bob. They denote the m-th word in the dictionary (in alphabetical order) by the number m. Assume that p is so large that every word can be represented in this manner. Whenever one of them wants to send a message m, they first compute $e = Enc_k(m) := (m + k) \mod p$ and send e over the network. The other side then computes $d = Dec_k(e) := (e - k) \mod p$.

1. Is this a valid symmetric encryption scheme?
2. Is this scheme secure for a one-time communication? If not, how can we make it secure? Prove that the original method or your variant discloses no information about the message to an eavesdropper Eve.
3. Is it secure for multiple rounds of communication? If not, how can we make it secure? Prove that the original method or your variant discloses no information about the message to an eavesdropper Eve.

Exercise 3

This is an extra-credit exercise. You are not required to submit a solution. However, any points you achieve here can be used to compensate potential lost points in other exercises or future homeworks. This exercise can compensate for up to 5% of your total grade.

Recall that computing discrete logarithms is assumed to be a hard problem. Let p be a large prime number and g a primitive root modulo p, i.e. $\{g^1, g^2, \dots, g^{p-1}\} \equiv_p \{1, 2, \dots, p-1\}$.

Both Alice and Bob know the integer values p, g, and m. Alice claims that she also knows an integer value k, such that $g^k \equiv_p m$. Bob does not believe her. Alice wants to convince Bob that she knows such a k. Of course, she can just disclose k and then Bob can check whether g^k is really equivalent to m modulo p. However, Alice wants to keep k a secret. More formally, she does not want Bob to be able to compute k based on the information given to him by Alice. Yet she also wants to convince Bob with high probability that she actually knows k.

1. For any probability bound $pr \in [0, 1)$, design a protocol that convinces Bob with probability at least pr that Alice knows such a value k.
2. Is it possible for Bob to obtain k based on the information disclosed to him in your protocol? If not, formally prove this. If yes, go back to Step 1.

Tip: Think of how RSA signatures work.