COMP 4541 – Homework 1

A. K. Goharshady

Release Date: March 5, 2024
Deadline: March 19, 2024 (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. Your solutions must be 100% your own work. 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 3% of your total grade.

Alice, Bob and Carol are playing a game in which one of them is selected as a loser and has to pay some money to the others. The game is quite simple. They each choose either 0 or 1. The player whose choice is in the minority loses, i.e. one loses if they choose 0 and both other players choose 1 or vice versa. It is possible that there is no loser, e.g. if all players choose 1. In that case, the game will be restarted and played for another round.

Unfortunately, Alice, Bob and Carol are in different countries and they have to play the game 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, Bob or Carol or otherwise tamper with the result of the game. These malicious actors can read the messages and also change them, but they cannot stop the messages. Moreover, they are discreet and will not change a message if this can be detected in your protocol. Also, none of the players (Alice, Bob or Carol) are trustworthy and they might want to cheat in order to win the game or at least decrease their chance of losing.

1. Design a secure protocol to play this game over the internet. 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, Carol or any third party on the network. In your proof, mention explicitly which properties of each cryptographic primitive are being used in each part of the argument.

Exercise 2

This exercise accounts for 4% of your total grade.

Alice wants to auction her highly-prized copy of the lecture notes of COMP 4541 on the internet. As you can imagine, there are many buyers who would like to bid in this auction. Alice announces her email address and RSA public key pk_A on her website. Anyone can now send Alice encrypted emails. Alice knows that her lecture notes can sell for a high price, but she is worried that the auction bidders might try to underbid strategically. For example, maybe Bob is willing to pay 5000 dollars, but he thinks that others will not bid so high, so he instead bids only 1000 dollars. To avoid this problem, Alice decides to employ a so-called Vickrey auction. See https://en.wikipedia.org/wiki/Vickrey_auction. In this kind of auction, no bidder should know other participants' bids when placing their own bid. Then, the highest bidder is chosen as the winner but they only have to pay as much as the second-highest bid. Assume that the list of bidders is known in advance and each bidder i has also provided their public key pk_i which is known to everyone. Moreover, assume that no two people bid the same amount.

1. Design a secure protocol to perform the Vickrey auction on the internet, assuming the same threats and risks as in the previous exercise. Argue why your protocol is safe, no one can tamper with the results, and no one can cheat.

2. Design an extension of the protocol in the previous part which also provides privacy for all bidders, except the winner and the second-highest bidder. We say that bidder i has privacy if no one other Alice and bidder i herself can know her bid.

3. Design a variant which provides privacy for all bidders except the winner. This variant must provide privacy even to the second-highest bidder.

Note that in all three protocols above, every participant should be convinced that there was no cheating in the auction. Moreover, every participant should find out who the winner was, how much they bid, and how much they have to pay.

Exercise 3

This exercise accounts for 3% of your total grade.

Consider the Central Bank Digital Currency (CBDC) discussed in Lecture 10, in which a central bank keeps track of the ledger but anyone can create accounts and transact. Can the central bank perform the following actions? If yes, explain how. If no, explain why.

1. Freeze a specific coin (output) so that it cannot be spent.
2. Confiscate or change the ownership of a coin (output).
3. Reverse a transaction that was already on the chain.
4. Spend a coin that does not belong to the central bank.
5. Blacklist a certain individual and disallow their transactions.
6. Whitelist certain individuals and only allow transactions from them.
7. Identify every transaction's payer and payee (in the sense of obtaining their real-world identity).
8. Allow transactions only if both the payer and the payee are fully identified in the real world.
9. Create two different valid chains of bank-certified transactions.