Cybersecurity - Homework 6

Vlad Turno (1835365)

December 1, 2025

1) Introduction

In order to securely allow Alice and Bob to play rock/paper/scissors through a network with protection against cheating, we need to create a protocol that ensures:
- Secrecy: Alice and Bob must each be able to select their moves secretly, such that neither party knows the other's move before the game ends.
- Integrity: The chosen moves must be verifiable so that neither party can change their move after the game starts.
- Fairness: Alice and Bob cannot cheat, even if one of them tries to manipulate the process (for example, by revealing their move beforehand).
To achieve this, we will need to use cryptographic primitives like hash functions and zero-knowledge proofs, as well as secure commitment schemes to make sure that neither player can alter their move once they've committed to it.

2) Protocol

Here's a general protocol we could use for Alice and Bob to play a secure version of rock/paper/scissors. It will cover an initial setup phase, a commitment phase and a reveal phase where the winner will be determined:

2.1) Setup

Both Alice and Bob agree on a public cryptographic hash function like SHA-256 that they will use to hash their moves and commitments.
Alice and Bob each choose a secret random value that will be used as a salt for their respective moves.

2.2) Commitment

Alice chooses her move (rock,paper or scissors) and creates a random salt value. Then she computes the commitment to her move as *CommitA = Hash(MoveA,SaltA)* ad sent her commitment along her salt to Bob, who will do exactly the same with his *CommitB = Hash(MoveB,SaltB)*.

2.3) Reveal

After both Alice and Bob have sent their commitments, they can now reveal their actual moves. Alice reveals her actual move *MoveA* along with her salt *SaltA* she used to compute *CommitA* and so will do Bob.
Both Alice and Bob then independently verify that the revealed moves match the commitment by checking *Hash(MoveA,SaltA) = CommitA* and *Hash(MoveB,SaltB) = CommitB*

2.4) Winning

Once both players have verified their moves, the winner is determined based on the classic rules (rock beats scissors, scissors beats paper, paper beats rock) and the winner is declared based on the comparison of the revealed moves. If Alice and Bob wish to play multiple rounds they can run this protocol independently for each round.

3) Features

The protocol is resistant against cheating since Alice and Bob can't change their moves after the commitment phase because the hash commitment guarantees that the move was fixed at the time the commitment was made. Even if one of them tries to cheat by changing their move after seeing the other player's move, they won't be able to match the original commitment, and the other party can easily verify the discrepancy.

The protocol ensures fairness because both players have equal opportunity to reveal their moves without knowing the other player's move in advance.

The protocol finally ensures secrecy since the moves are hidden from the other player until both parties reveal them, ensuring that neither player has an advantage based on prior knowledge.
Ulterior enhancements for ensuring further security could include a timed-commitment mechanism or a proof mechanism to declare a move to be valid without revealing it, adding another layer of security.