Cybersecurity - Homework 7

Vlad Turno (1835365)

December 10, 2025

1) Introduction

In order to securely allow Alice and Bob to play a dice game where each player rolls a number k of six-sided dice and compare the sums of all rolls to determine the winner, we have to design a protocol that ensures fairness, security and integrity to prevent cheating by ensuring that neither player can manipulate their dice rolls or view the other player's rolls before results are revealed.
For transparency, both players should be able to verify the integrity of each round.

2) Design Choices

Here's a general protocol we could use for Alice and Bob to play dice:

2.1) Roll Mechanism

To ensure fairness the dice rolls should be randomized securely and the best approach is to use a secure random number generator PRNG.
This step can be achieved with a trusted cryptographic library.
For each round, each player rolls k six-sided dices, each dice roll is generated randomly using a cryptographic random number generator and once both players have rolled the results are hidden from each other until the game is complete.

2.2) Cheating Prevention

To prevent any form of cheating, players simply should not be able to see their own dice rolls or the opponent's rolls before both sets of dice rolls are revealed at the same time.
This can be achieved by implementing a secure (cryptographic) roll commitment where before rolling the dice both players generate a cryptographic hash commitment of their dice rolls.
This ensures that the player cannot change their rolls after committing, as they have already "sealed" them with the hash mechanism.

2.3) Roll Reveal

After both players have rolled, they reveal their dice rolls along with the commitments.
The commitment should match the actual dice rolls, proving that the player couldn't have altered the results after committing.

3) Multiple Matches

A match consists of multiple independent games and the total number of games in a match should be predefined.
Each round consists of Alice and Bob rolling their k dices and comparing the sums.
After all rounds are completed the player who has won the most rounds is declared the winner.
In case of a tie in rounds, the match can either end as a draw or go to a tiebreaker (additional round).

4) Security Issues

To guarantee randomness, the use of a secure PRNG is crucial: if the PRNG is compromised, it might allow a player to predict or manipulate their dice rolls.
The cryptographic hash commitment prevents a player from changing their dice rolls after committing to them, ensuring that they cannot cheat by rolling a favorable result after seeing the opponent's rolls.
To prevent replay attacks (where a player reuses an old roll), each commitment should include a unique nonce or timestamp.