# Ro-Sham-Bo

HW5-CNS Sapienza

Hassaan Ahmed Qureshi - 1906852

December 5,2019

## Contents

# 1 Introduction

In this report I will design a protocol which will allow two players to play Ro-Sham-Bo game. This game is more commonly known as Rock-Paper-Scissors in which two or three players randomly choose a move i.e. Rock, Paper or Scissors which beat each other in priority such that Rock beats Scissors, Scissors beats Paper and Paper beats Rock. The protocol is designed keepiing in mind that the two players do not know or trust each other. The protocol is based on a sequence of N = 2p+1. In this protocol Hashing function SHA256 is used along with nonse to make sure both players don't involve in foul play.

Since the game is online and live and not played on any third-party trusted server, therefore there is no chance for any bruteforce attack.

# 2 Game Protocol

- Alice sends a simple String message to check if Bob is available to play the game, to which Bob replies.

- Alice chooses her move generates a simple nonce and encrypts both using SHA256 (nonce, MA) Bob does the same by sending his move SHA256 (nonce, MB).

- Alice and Bob sends nonce to each other.

- Alice computes hash and checks whether the move Bob send is the same, otherwise stop the game. Similarly Bob does the same. They are able to compute MA and MB.

- Alice and Bob both computes each others moves and the score is updated on the scoreboard.

# 3 Conclusion

The nonce here allows the game to prevent any game dictionary attack or replay attacks. If any one of the player tries to cheat, the other player will know in such a way that the player would not be able to compute other's message. Thus changing the result is useless as it is previously sent to the other player and record cannot be changed. To improve data ingrity, we can use cyclic reducdant check on every message the player sends to the other player. Since the game score is updated locally and therefore both know the score of the other player