Ro Sham Bo
HW5 - CNS Sapienza

Lombardo Andrea 1893440

5/12/2019

1 Introduction

The main goal of this abstract is to design a protocol which will allow two authenticated players to play Ro Sham Bo games, more commonly known as Rock paper scissors.

Therefore we should speak a little to the Asian origin game, according to which two players compete in real-time challenge, this factor let to avoid the cheating because the two launches should start at the same time. A complete match in this game between two players is composed by a sequence of N=2p+1 ro sham bo games and the match is won with at least p + 1 games. A session game consists to the choice made by the two player without knowing the other player's pick, and the result for identifying who is the winner. Now we analyzed the rules of the game:

- Each player could choice one pick between P,R,S so we identify the pick as a char:
  - Rock ⇒identified by a closed fist
  - Paper ⇒ identified by a flat hand
  - Scissors ⇒ identified by a fist with the index finger and middle finger extended, forming a V
- The rules for proving who is the winner are the following:
  - Rock beats scissors;
  - Scissors beats paper;
  - Paper beats rock;
  - If the two player use the same type of pick there's a a draw;

2 Design

The protocol must guarantee data integrity, avoiding that one player can get an advance from pre-computation or cheating and also the fact that could exist more sessions at the same time. The protocol consists of a sequence of messages exchanged via smartphone between the two players without third party or a person who guarantee rules and the valid player' steps. Every new game started at the same time to the two players and nobody could enter to a started game, the game will end when both players agree on the end. Each player must to send his choice through a message to the adversary and

viceversa. Obviously both the players must choice without knowing what the opponent's pick .

If we identify the two players as Alice and Bob. I design my protocol based on different sections:

- 1)Exchange messages which prove that is starting a new session between Alice and Bob and no third part could interact with the session and this factor is verified by timestamp which is a part of the message and the rest of the message contain the choice made by Alice and the reply of the message contain Bob's choice. The message delivered is composed by two parts: first the encrypted message of the timestamp and Alice's choice converted in ciphertext through the following algorithms AES and the second part of the delivered message message is the output of the SHA-256 algorithm of the ciphertext which helps me to say that the message could be modified. The key is chosen by Alice and it's changed in each new game .When Bob receive the message sent by Alice:
  - 1.1)Build a new message with timestamp of the game and his choice made between P, R,S
  - 1.2)Sent the message as ciphertext with the same pattern, used by Alice's encryption, to Alice
- 2)Exchange messages contain the key which let to discover what's the opponent's choice and verify the timestamp so according to the rule define above each player could himself determine who is the winner.
  - 2.1) Alice encapsulate in the new message the key used to let to Bob to estabilish who won the game.
  - 2.1)Thus Bob checks the timestamp that is the prove of a new game if the check return with a wrong value means that there is no game has not yet finished so the protocol is interrupted
  - 2.2)Bob after received the message makes the same job done by Alice in 2.1 and so also she checks if the timestamp is correct
- 3)Exchange messages which contains who is the winner and the update of the result.

  In detail they send each other a new message with the new points of the match which should assign to the winner player. This help us in order to make them agree on the score. The last message is composed by two parts, a part composed by points and the timestamp of the match, and the other part we have a digital signature of the first part, which is based on DSA, using public key cryptography.

Then players verify the validity of the game and then check the result updating with the result of this last game. The game is stopped when players don't agree on the result or when one arrive to p+1 win matches.

3 Security of the protocol

We need to make sure that the protocol we have devised is resilient to different attacks for example **Replay attacks** which is not possible because timestamp and the symmetric keys are different for each session. The timestamp guarantee also we couldn't have multiple sessions in fact if the check of the timestamp was going bad the players restart game. Repudiating a message cases the session invalidation which doesn't give useful information to the attacker, since we use a DSA signature, based on public key cryptography, if the message is modified the hash does not correspond and the players restart the game. The cheating is also no possible for the fact that nobody neither Alice neither Bob know previous than other the choice made by the other. We have devised a secure protocol which allows two authenticated players to play a Ro Sham Bo game over a channel without intruders
.

References

[1] https://en.wikipedia.org/wiki/Rock-paper-scissors