Eighth Homework Cybersecurity

Andrea Morelli 1845525

1 First Ideas and assumptions

So the first idea that came into my mind was to use some sort of cryptographic protocol to allow the two players to communicate and play together without worrying about the adversary cheating.
The idea of the protocol is to firstly exchange hashes of their choices and then verify that the other player choice will produce the hashes previously sent.This has to be done in a good way otherwise collisions could occur and one player could cheat.
The first thing that i supposed was that both the players would not try to violate the protocol but just exploit it to win.
The second was that they have a channel to communicate and that the messages are not altered by a man in the middle or lost.
The third is that they wait their turn and don't send a message if the other player has not responded yet.

2 The Protocol

That is the protocol i devised where we have two player A and B that play in a round R:
$A \to B : T_A$
$B \to A : T_B$
$A \to B :$ HMAC$(K_A, C_A \,\|T_B\|\, R)$,
$B \to A :$ HMAC$(K_B, C_B \,\|T_A\|\, R)$
$A \to B : C_A$
$B \to A : C_B$
$A \to B : K_A$
$B \to A : K_B$
$R = R + 1$
In this protocol in every round R both A and B exchange two random salts T_A and T_B.
Then they calculate the hmac with for example the digest sha512 algorithm (not broken) with a random key (K_A or K_B) that is generated in every round,with data that is the concatenation of their choice (C_A or C_B) , the previously received salt and the round.
Then to verify that the other player was not cheating, they exchange firstly their choice for the round and then their key and both verify that the hmac of salts,choice and round with the key received is equal to the one previously received.Finally they both increase the round value.

If the round is equal to the decided number of games to play than they stop and show who won the most games otherwise they continue to play this time with an increased round.

3 Considerations

Both the two players when they first start communicating will set the round value to 0 and will gradually increase it everytime a game is played.The hmac will use a criptographic hash function that is not broken and that will have a big dimension for example sha512 or sha256 where the birthday bound is big. The key generated from the players to the hmac has to be random and big for example 256 or 512 bits .
The same thing should be applied to salts generated(have to be big and random) but the salt can be a big string of like 200 characters.
The hmac will produce a digest with an hash algorithm using also a key.

Hmac is used to reduce the risks of having collisions since there is also the need of the key and the salt is used to increase the dimension of the data since there could be collisions if only the choice is used because one could find a collision with a key.
Having a salt and a key hashed function instead is a good security measure and will guarantee that the players could not cheat.

4 Progression Of The Games

Both the players would keep the amount of games they played R and won and once N games are played (that is previously agreed on)they will stop and know who won.
The choices are rock paper or scissor that could be encoded in 0 1 or 2 and considering the rules of the game rock will beat scissor, paper will beat rock and scissor will beat paper, they can decide who won the game.
Every round they will generate new salts , new keys, their choice for the round and the number of the round.