Security exercise 02

Introduction

Alice and Bob want to play a game. The game they decide on is a simple game of dice, whoever rolls the higher number on a regular six sided dice wins. Because of the pandemic they can't meet in person and therefore decide to play it online. There is only one problem, they both have major trust issues hence they don't believe their opponent will be truthful about their roll. How can we create a protocol that will still allow them to play dice?

Protocol

The first thing Alice and Bob need to establish is a secure connection. They both have each other's public key through a PKI, therefore Alice can create a session key encrypt with asymmetric encryption using Bob's public key and send this message to Bob. All subsequent requests exchanged between Alice and Bob will be encrypted with this session key using symmetric encryption. Furthermore all requests will have a corresponding signature that will verify if the message was sent from the expected party and that the message has not been interfered with. Now Alice and Bob will both create a commitment. These commitments consist of bytes that have been encrypted with a key that so far only the creator of the commitment knows. With this commit they also send a hash of the key that will eventually open the commit showing the value hidden inside. This is done in order to prevent a player from later finding another key that will lead to a more desirable result. Once both Alice and Bob have each other's commitment they will send the key that will open their commitment. Once their opponent's commit key is received they will hash it and compare it to the hashed key they received earlier, if they are not the same the game cannot continue since one of the players tried to cheat. If however the key is valid they can use it to open the commit and extract the bytes hidden inside. Now Alice and Bob both have two sequences of bytes: one they created themself and one

received from their opponent. They now perform an xor operation on these two byte sequences, convert it to an integer and perform modulus six and add one. This will lead to a value between one and six. By performing these steps they have now created a single dice roll that neither of the players have had the opportunity to cheat unnoticed. Now they simply repeat these steps to calculate another value, whereas the first value is Alice’s dice and the latter is Bob’s.

Now Alice and Bob can play a game of online dice without having to worry about their opponent cheating.