Security 1 - Mandatory Hand-in 2

Sam Al-Sapti (sals@itu.dk)

October 25, 2022

Part 1

To solve the problem at hand, the following protocol can be used:

1. Alice and Bob agree on a cyclic group $(\mathbb{Z}_p^*, \cdot)$ with generators g and h.
2. Using Pedersen commitments, Alice samples a random $r \in \mathbb{Z}_p^*$ and a die throw m, and sends commitment $c = C(m, r)$ to Bob.
3. Bob sends a die throw t to Alice.
4. Alice sends (m, r) to Bob, who then verifies that $c = C(m, r)$.
5. Alice and Bob each compute the final value m XOR t.

To ensure confidentiality, integrity and authenticity, a secure channel is established with mutual TLS (mTLS), meaning that both communicating parties authenticate themselves with certificates. For the purposes of this assignment, I will be using self-signed certificates instead of signing them by a certificate authority (CA).

Part 2

TLS is used as a key exchange protocol to obtain a shared symmetric key for encryption. This is to ensure confidentiality. Furthermore, with mTLS, both parties authenticate themselves with their personal certificates. This part ensures authenticity from both sides. Lastly, as part of the TLS protocol, each message is sent along with a message authentication code (MAC). This ensures integrity. It also ensures authenticity, as only the parties participating in the key exchange will be able to create the MACs.

The commitments ensure that no party can cheat with their die throw. Each party can send their die throw without first learning the other party's throw, such that no party has any influence on the final result.