KEY EXCHANGE PROTOCOL DESIGN

TRANSPORT LAYER:

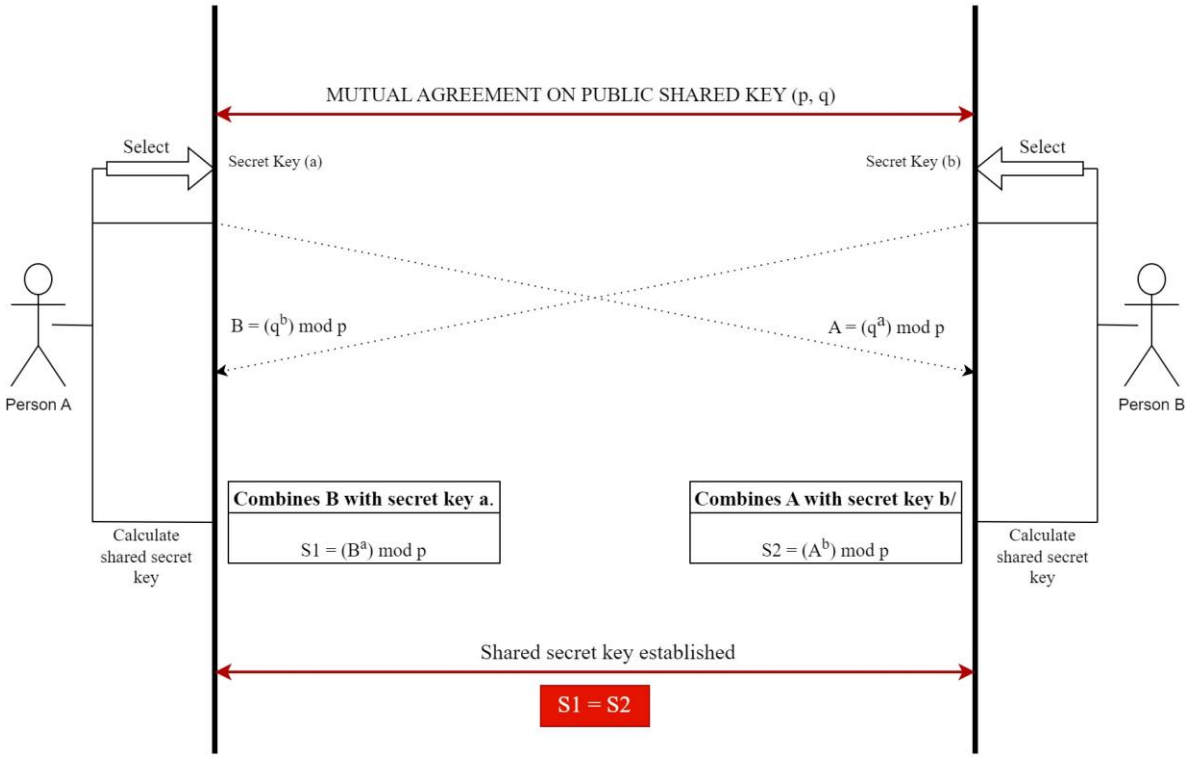
Utilize TCP. It is mandatory as the two-party key exchange requires that the information is received by both sides.

STRUCTURE:

Two-party exchange. Loosely based on client server model. Party can either accept a connection or connect to another. Hence, two options are provided: Accept (accept a connection from the other party) or Connect (to connect with the other party).

KEY-EXCHANGE:

The simple Diffie-Hellman key exchange takes place as illustrated in the diagram below:



ASSUMPTIONS:

We assume that both parties have already agreed on a shared public key (p, q). Hence, p and q values are hardcoded, where p is prime and q is primitive modulo root of p.

RULES:

The user/party must select a secret key (private key). This is provided as input. Private key is between (1, p -1) and must be an integer.

ERROR HANDLING: Ensure proper secret key is selected with respect to value and type (integer).