SSH Protocol Specification

Chirag Satish

1. Client sends a message to the server indicating that it wants to initiate the file transfer protocol.

   C→S: (CLIENT_INIT_EXCHANGE)

2. Server responds to the client's initiate request by sending its public key, with message header as SERVER_INIT_RESPONSE.

   S→C: (SERVER_INIT_RESPONSE, K_S^+)

3. The client now generates a 256-bit pseudo random number, which serves as the session key, and encrypts it with the server's public key.

   C→S: E(K_S^+, SK)

4. The server decrypts the session key with its private key and sends a message to the client indicating that it is ready for file transfer.

   S→C: (SERVER_INIT_ACK)

5. The client now reads the file, encrypts it block-wise with the session key and sends the blocks to the server.

   C→S: E(SK, FILE-BLOCK)

6. The server decrypts the blocks using the session key and writes them to the file "./shared/<file-name>".

Notations used:

C – Client

S – Server

SK – Session Key

E(K, Data) – Encrypted Message of data with key K