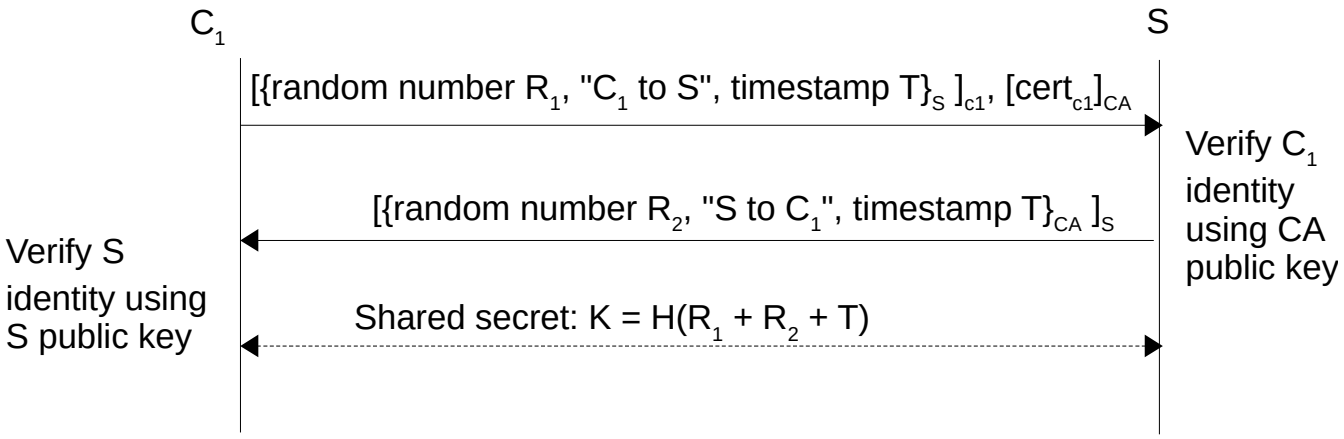
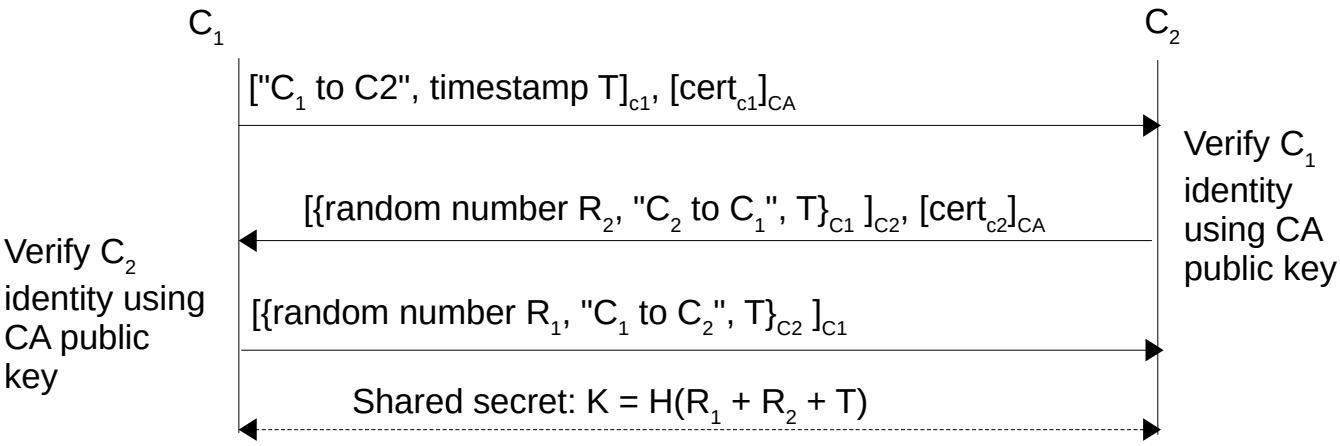
- System Description:
  The system consists of three main entities: chat server, S, chat clients, C_i's, and the certificate authority, CA. The chat clients connect to the chat server to get a directory of other online clients and their IP and port address information. After getting this information about another client, the client connect to the other client and communicate with them directly without the meditation of the chat server.
- Initialization:
  At the start, each of the parties will have the following information stored locally on their keystores. This information should be available to the parties before the start of the system:
  - C_i:
    - $[cert_{Ci}]_{CA}$
    - C_i's private key
    - C_i's public key
    - S's public key
    - CA's public key
  - S:
    - S's private key
    - S's public key
    - CA's public key
- Securely obtaining a symmetric key between a client, C_1, and the server, S:



- Securely obtaining a symmetric key between a client, C_1, and another client, C_2:



- Communication:
  After two parties obtain their shared key, K, for the current session they are engaging in, all their communication from that point onward will be encrypted using symmetric key encryption and MAC'ed using the same key.