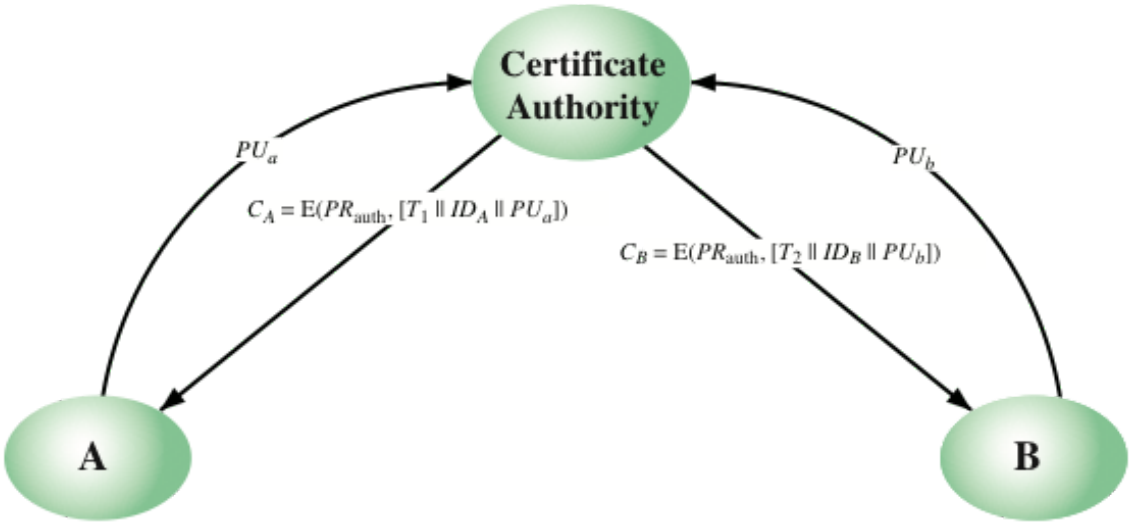
By-Varun Singhal(MT20099)
Sachin Kotiyal(MT20093)

CSE 540 Network Security
Assignment 3
Project 0(Public Key certification Authority)

Certification Authority: A certificate authority (CA), also sometimes referred to as a certification authority, is a company or organization that acts to validate the identities of entities (such as websites, email addresses, companies, or individual persons) and bind them to cryptographic keys through the issuance of electronic documents known as digital certificates.



(a) Obtaining certificates from CA

- Assume A and B are under the same CA.
- A request CA for public key of B and B request CA for public key of A.
- So CA sends to client correspondence their requested public key.
- A digital certificate provides:
  - Authentication, by serving as a credential to validate the identity of the entity that it is issued to.
  - Encryption, for secure communication over insecure networks such as the Internet.
  - Integrity of documents signed with the certificate so that they cannot be altered by a third party in transit.

Program Architecture: Program has been divided into 3 parts : One server (CA) and two clients.

- **Server (CA) :**There are 2 main components of certification authority.
  - Receive Request : It is used to receive requests or verify requests from clients(client i.e.A is requesting the public key of B.
  - Return Certificate : It is used to return certificates for whom clients want to communicate.
- **Client:**There are 3 main functions in the client.
  - Get_PUA : Used to get public key of client1 i.e. B
  - Get_PRA : Used to get the private key of client1.
  - Send message : Main driver function of the client used to send messages to other clients.

Model Working: Suppose client A wants to send a message to client B so he needs to get a verified public key of client B.

- And we all know the verified public key of every client is stored at CA(certificate authority), which acts as the center of trust.
- CA provides the public key of client B.
- Now client A encrypts the message using that public key and sends it to client B.
- Client B receives and decrypts the message with its private key.
- Client B sends the Acknowledgement to Client A.

Conclusion: We have developed a minimal working model of CA.

- The real architecture of CA and the process of verification of domains is so robust that it's very hard to break.
- In real life, a client doesn’t request a CA every time it tries to connect a new domain, instead that verified certificates of CA are already placed inside the browser.