CSE350: NETWORK SECURITY

PROGRAMMING ASSIGNMENT 3

Ananya Garg (2022068), Ananya Gupta (2021012)

Introduction

Project 0: RSA-based Public-key Certification Authority (CA)

Built a public-key Certification Authority (CA), that responds to requests from clients that seek their own RSA-based public-key certificates OR that of other clients

Built 2 clients, A and B, that:

- send requests to the CA for their own public-key certificates OR that of other clients, and
- exchange text messages with each other in a confidential manner, suitably encrypted with the public key of the receiver, but only after they know the other client's public key in a secure manner.

A sample certificate for A is of the form as given below:

$[(ID_A, PU_A, T_A, DUR_A, INFO_{CA})||ENC_{PR-CA}(ID_A, PU_A, T_A, DUR_A, INFO_{CA})]$

- ID_A is the user ID
- PU_A is the public key of A
- T_A is the time of issuance of the certificate
- DUR_A is the duration for which the certificate is valid
- $INFO_{CA}$ is information about certification authority
- ENC is the encryption algorithm used by CA
- $PR - CA$ is the public key of the certification authority

Assumptions

- Clients already (somehow) know their own [public-key, private-key] but do not have their certificates or that of others.
- The format of the certificate and the hashing function are publicly available.
- Clients know the public key of the CA.

- CA has the public keys of all clients (handled by gRPC)

Encryption and Decryption

RSA is used for encryption and decryption. Large prime numbers p and q are generated to get n=p*q and ϕ=(p-1)*(q-1).
This further allowed to generate numbers d and e. Chose e such that:

$$1 < e < \phi \; and \; gcd(e, \phi) = 1$$

Used keys for encryption and decryption as below:

$$C = M^e (mod\, n)$$

$$M = C^d (mod\, n)$$

where, M is a plaintext such that M<n and C is the ciphertext.

Encryption

- RSA encryption involves generating public and private keys.
- In the code, RequestCertificate method in the CA class signs certificate data using CA's private key.
- This is then appended to the original message and sent to the client.
- Clients use the public key to encrypt data before sending it to the other client.

Decryption

- Decryption in the code involves verifying signatures and decrypting messages on the client side.
- When a certificate is received the client verifies its authenticity using the CA's public key.
- If the signature is valid, decryption is successful, and the client can trust the received certificate for secure communication.
- Clients also send messages to each other while encrypting and decrypting them back and forth.

Constraints

Specially chosen n, and blocks of data of size k bits s.t. $2^k < n \leq 2^{k+1}$
This constraint is inherent in the RSA algorithm. It is satisfied by default in our code.