**Network Security**

Assignment 3: Project **0**

**Herschelle Gupta 2019045 | Ritik Vatsal 2019321**

**Input/ Output**

All scripts - **Alice**, **Bob**, and **Certifying\_Authority** should be started and running together. For the sake of this assignment, we *assume the role of Alice*, and all inputs are given in **Alice’s** terminal. We have automated Bob’s side, However, both Alice and Bob are functionally similar internally.

Assumptions-

* Everyone knows their own Private & Public Key
* The clients - Alice and Bob, know the Public Key of the Certificate Authority
* The CA has Public Keys of all clients
* Message sizes limited to character 7 characters
* Alice is implemented as a client program, Bob and CA are implemented as servers.
* Decryption is done automatically at the servers but on client side (Alice), it has to be done with the help of given functions.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Alice Knows -

Her Private & Public Key

CA’s Public Key

Alice can -

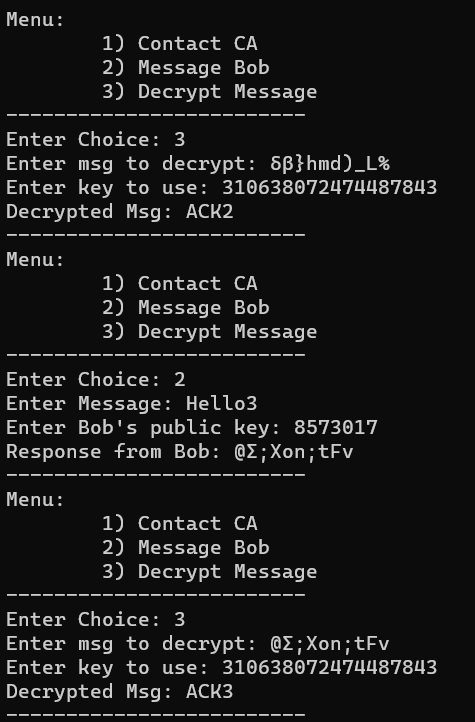
Request Bob’s Public key from the CA

Send a message to Bob

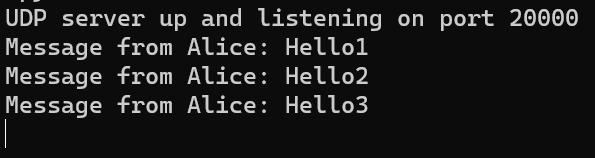
Decrypt Messages using the appropriate key

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

We can see the test case outputs from both Bob and Alice.

Alice -   


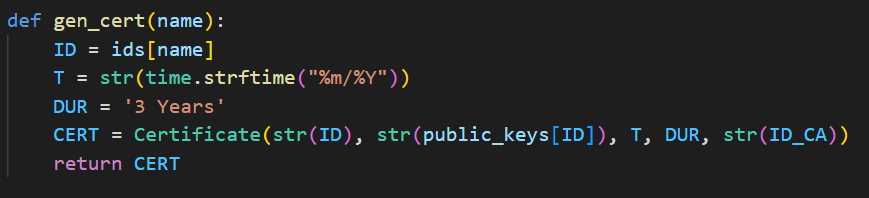
Bob -



\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Working -**

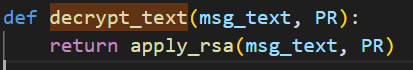
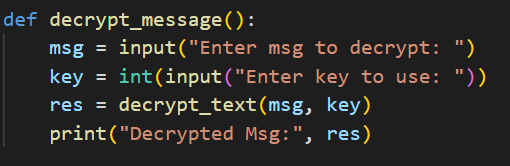
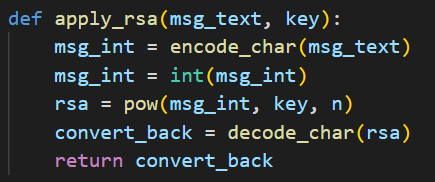
Certificate Generation with Time stamp and Validity -



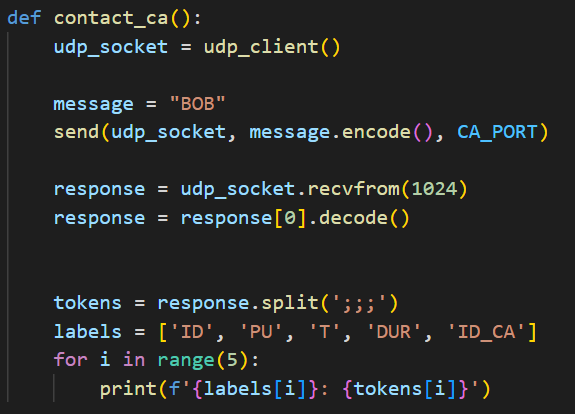
UDP Server -



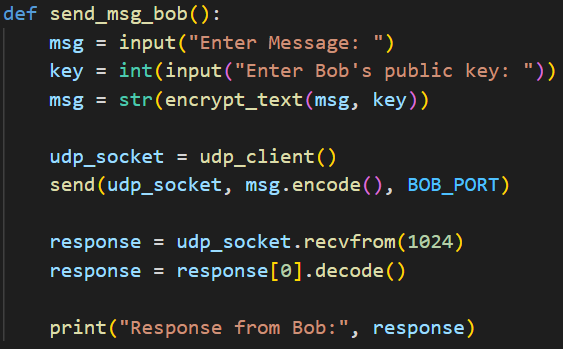
Message Decryption and RSA Implementation -



Contacting CA -



Messaging Bob -



\*\*\*