# Assignment 1

2020161 Yashika Singh
2020088 Naman Kaushik

# CA.py

This file is responsible for providing the keys to different clients

It accept keys from clients when they send them encrypted with its own private key

It also send keys by encrypting with its own private keys

# Clients

We have provided three clients can:

-Send their keys to PKDA

- Request for public keys of other clients

- Send messages to other clients

# Hashing

Hashing of the message is done and sent along the encrypted message to ensure that the message does not get tampered with during the transmission.

The received decrypts the message and hashes it to compare with the hash received to ensure integrity.

# Time

A UNIX time stamp is added to the message which enable the receiver to know the time that the request was made at

The time is compared with the current time to get the difference and a time out limit etc. can be set