REPORT

Dipen Kumar (2018CS50098)
Manoj Kumar (2018CS50411)

We used gmpy2 for large number calculations
We used only two strong prime number for creating secret and public key. We pass two different values for bits for RSA key generations to created two distinct secret and private key for sender and receiver. We did same for CA authority and hence all three have different secret and public key.

CA signs secret and public keys for both and it is check which encrypting and decrypting and if found not correctly signed the sending and receiving is stoped.

Algorithm for vegenere is simply adding key and taking modulo with charset size() decryption is as simple like subtracting key and taking modulo with key.

Algorithm for RSA is as mentioned in lecture slides that is Enciper and decipher of message using public and secret key after the message is broken down in blocks and encoded in number on radix = charset. Block size is appropriately chosen with respecyion to “n” created while RSA key generation. This is the number taken modulo after message encoded in number raised to power “e” and “d” for enchiper and decipher respectively.

Encryption and decryption is done based “e” and “d” in public and secret keys. D is multiplicative modulo inverse of e on n.