Assignment # 2
(Last date to submit: 16th October 2021 midnight)

A public key infrastructure (PKI) is an arrangement that binds public keys with respective identities of entities (like people and organizations). The binding is established through a process of registration and issuance of certificates at and by a certificate authority (CA). The primary role of the CA is to digitally sign and publish the public key bound to a given user. This is done using the CA's own private key, so that trust in the user key relies on one's trust in the validity of the CA's key.

Consider a mixed encryption scheme, which combines asymmetric key scheme with symmetric key scheme. We can define a mixed encryption scheme for transmitting a message m by user a A to a user B, as follows:

Let m : message, k : key of a symmetric key scheme, c_s : cipher text obtained after applying key k over m i.e. $E(m, k) = c_s$. sk_A and pk_A be the secret and public keys respectively of public key scheme for user A.

Encryption by user A, works as:

$c_s \leftarrow E(m, k)$, $(c, k') \leftarrow E(D(c_s, k, sk_A), pk_B)$

Decryption by user B, works as:

$(c_s, k) \leftarrow E(D(c, k', sk_B), pk_A)$, if $D(c_s, k) = m$ then output (m), otherwise reject

Implement the following modules (independent), using RSA public-key cryptosystem as asymmetric key scheme and Vigenere as symmetric key scheme:

1. Generation of keys: generation of keys by CA for the users, using only safe primes and publish the public key, digitally signed by CA, in a directory. Private Key will be handed over to the individual user only.
2. Encryption by the sender.
3. Decryption by recipient.

You can use download The GNU Multiple Precision Arithmetic Library and include in your program to handle large integers.