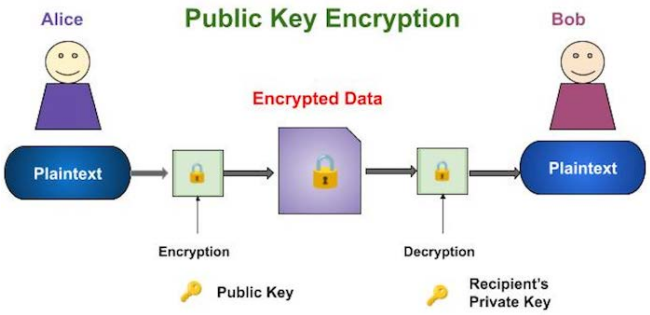
Bharatiya Vidya Bhavan's
SARDAR PATEL INSTITUTE OF TECHNOLOGY
(Autonomous Institute Affiliated to University of Mumbai)
Munshi Nagar, Andheri (W), Mumbai – 400 058.

Experiment No. 3

Aim –Implement RSA algorithm.

Problem Definition– The experiment uses asymmetric and symmetric cryptosystem to provide two security services. First, this experiment covers key distribution problem using asymmetric cryptosystem. The asymmetric cryptosystems allows sharing secret key between sender and receiver through a third party entity. Second, symmetric cryptosystem covers sending large message from the sender to the receiver using the secret key shared in the first step.

Theory –Public-key cryptography, or asymmetric cryptosystem, is the field of cryptographic systems that use pairs of related keys. Each key pair consists of a public key and a corresponding private key. Key pairs are generated with cryptographic algorithms based on mathematical problems termed one-way functions. Security of public-key cryptography depends on keeping the private key secret; the public key can be openly distributed without compromising security.



The useful Links–

1. Asymmetric cryptosystem and RSA Algorithm
   https://www.youtube.com/watch?v=vf1z7GlG6Qo

Details of Experimentation – You need to implement three network services using socket programming namely i) Third Party entity, ii) Sender Entity and iii) Receiver Entity. One of the group member implements the third party entity service. While second group member implements both the sender and receiver services. All three services may run on different port numbers e.g. Third party on 4444, Receiver service on port no 3333.

Third Party entity provides network services which allow registration of public key along with identity (assume some names e.g. name like alice, bob etc) and providing public key of registered identity on a request. The second part consists of menu socket programming sender and receiver programs.

The sender socket program should provide three options namely i) Registration request of sender's identity to the third party for the public key, ii) Send a message to the receiver through two stages: First, share a secret key for encryption of the message to the receiver using asymmetric cryptosystem. Second, send the message using symmetric cryptosystem. iii) The third menu driven option is exiting from the sender program/service.

The receiver socket program should provide three options namely i) Registration request of receiver's identity to the third party for the public key, ii) the receiver should continuously waiting for any message received from the sender and then print it. The receiving of message is performed through symmetric cryptosystem while key is shared using asymmetric cryptosystem. iii) The third menu driven option is exiting from the sender program/service.

Input – The input for this experiment is i) Sufficiently large symmetric key, ii) small asymmetric key and iii) Large input message of more than 1000 letters. Note you need to use some mapping to convert letter to number and vice versa. Further, you may assume any other data required for this experimentation.

Output and Submission –

1) Source code of all three entities. All these files should be in one folder named "source-codes-<your UID>"
2) All the communication input, output, keys etc in a TEXT file [NO word file] named "input-output-<your UID>"
3) Upload Part-1 and Part-2 as zipped file named "Exp3-<your UID>"