Name: Aya Ahmed Musad Husein

Section : 1

BN: 15

Code: 9202338

Assignment Report

In this Assignment , we are implementing RSA Algorithm :

Key Generation

1)Select p, q p and q both prime, p != q

2)Calculate n = p * q

3)Calcuate fi(n) = (p - 1)(q - 1)

4)Select integer e gcd (fi(n), e) = 1; 1 < e < f(n)

5)Calculate d d = e^(-1) (mod fi(n))

6)Public key PU = {e, n}

7)Private key PR = {d, n}

Encryption

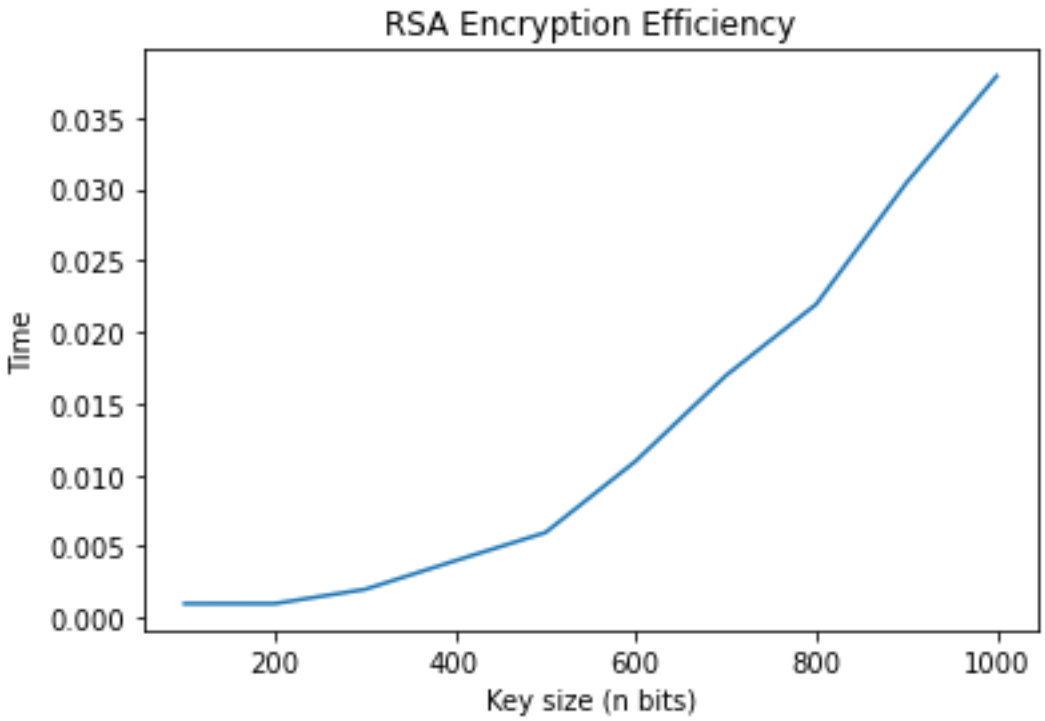
Plaintext: M < n

Ciphertext: C = M^(e) mod n

Decryption

Plaintext: M = C^(d) mod n

Applying the algorithm , we can notice that , increasing key size , makes time taken for encryption grow exponentialy ,



But on the other side , we can see that it also makes time needed for attack grow exponentialy , so it is some how a trade off between security and speed , so we need to choose key size as wise as we can .