Page:
Date: / /

ASSIGNMENT B4

Title: Implementation of RSA

Problem Statement: Implementation of RSA

Objective:
1. To understand how RSA works
2. Implementation of RSA

Outcome: Successfully understood and implemented RSA

Requirements: python3, jupyter, 64-bit Linux OS, text editor

Concept related theory:

RSA algorithm involves three steps:

1. Key Generation

The key generation algorithm works as follows:

(i) Generate two large random primes, p and q, of approximately equal size, such that their product $n = pq$ is of the required bit length, eg., 1024 bits

(ii) Compute $n = pq$ and $\phi = (p-1)(q-1)$

(iii) Choose an integer e, $1 < e < \phi$, such that $\gcd(e, \phi) = 1$

(iv) Compute the secret exponent d, $1 < d < \phi$, such that $d = e^{-1} \bmod \phi$ or $ed = 1 \bmod \phi$

(v) The public key is (n, e) and the private key (n, d). Keep all the values d, p, q and ϕ secret.

2. Encryption

Sender A does the following:

(i) Obtains the recipient B's public key (n, e)

(ii) Represents the plaintext message as a positive integer M, such that $1 < M < n$

(iii) Computes the ciphertext $C = M^e \bmod n$

(iv) Sends the ciphertext to B

3. Decryption

Recipient B does the following

(i) Uses his private key (n, d) to compute $m = C^d \bmod n$

(ii) Extracts the plaintext from the message representative m

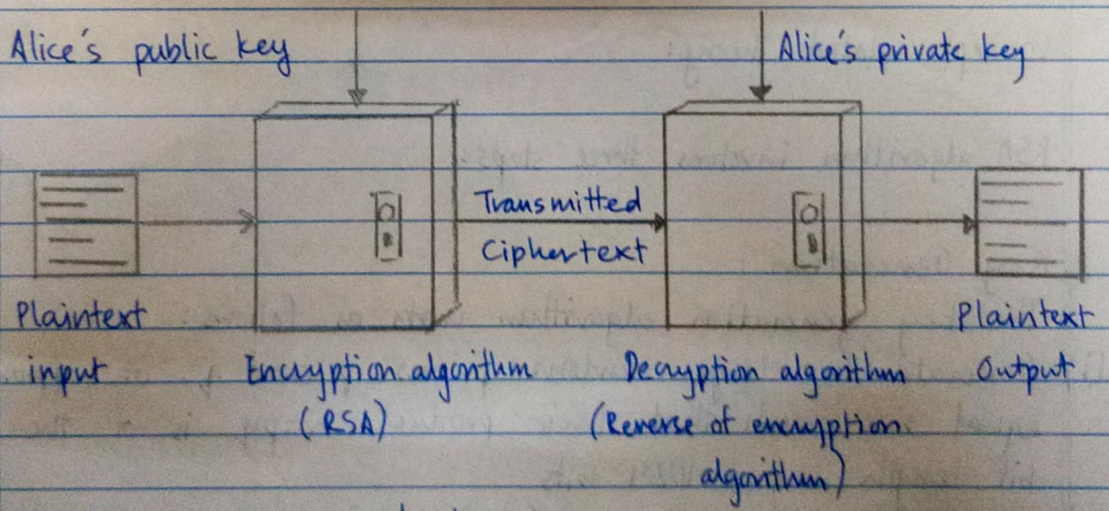

Fig. RSA encryption and decryption

Test Cases

Test Case	Expected Output	Actual Output
P : 3	Public key : 21, 5	Public key : 21, 5
Q : 7	Private key : 5 Cipher : 3	Private key : 5 Cipher : 3
Data: 12	Decrypted data : 120	Decrypted data : 12.0

Conclusion: Successfully implemented RSA