Assignment B4

Execution Date: 19/05/2021
Submission Date: 21/05/2021

Title: RSA algorithm

Problem Statement:
To implement RSA algorithm

Objectives:
Learn basic concepts of RSA
Implement RSA algorithm

Outcomes:
Students will be able to understand and implement RSA algorithm.

Software Requirements:
- Jupyter Notebook
- Python 3.8.5
- 64 bit operating system

Hardware Requirements:
- Computer with 64 bit processor

Theory:

RSA is one of the first public key crypto system and is widely used for secure data transmission.

It is a public key encryption algorithm. It is a block cipher which converts plain text into cipher text at sender side and vice a versa at receivers side.

A user of RSA creates and publishes a public key based on two large prime numbers. The prime numbers must be kept secret.

RSA is relatively slow algorithm, because of this, it is less commonly used to encrypt user data, More often, RSA posses encrypted shared key for symmetric key cryptography which in turn can perform bulk encryption operations at much higher speed.

Algorithm:

1) Select the two prime numbers where $a \neq b$

2) Compute $n = a * b$

3) Compute $\phi(n) = (a-1) * (b-1)$

4) Select e such that e is a coprime of $\phi(n)$
i.e. $\gcd(e, \phi(n)) = 1$ and $1 < e < \phi(n)$

5) Calculate private key d such that

$$(e * d) \bmod \phi(n) = 1$$

6) public key = { e,n}

private key = { d,n}

7) cipher text = $(data)^e$ mod n

8) plain text = $(cipher\ text)^d$ mod n

Example:

1) Let a=2 , b=7

2) n= 2* 7 = 14

3) ∅(n)= (2-1)* (7-1) = 6

4) Let e=5

∴ gcd (5,6)=1

5) Let d=11

e*d = 5*11 = 55

(e*d) mod ∅(n)= 55 mod 6 = 1

6) public key = (5,14)
private key = (11,14)

7) let $p = 3$

$\therefore c = p^e \bmod n = 3^5 \bmod 14$

$= 243 \bmod 14$

$c = 5$

8) For decryption

$p = c^d \bmod n$

$= 5^{11} \bmod n = 48828125 \bmod 14$

$p = 3$

Test Cases:

Description	Expected O/P	Actual O/P
1) Try with random prime numbers	Get decrypted text which is same as plain text	Successful
2) Try with given example a=2,b=7	Get decrypted text which is same as plain text, e=5 & d=11	Successful

Conclusion:

Therefore, we have successfully completed and implemented RSA algorithm.