* Labortory Practice II (Information Security) - Experiment Number - 5.

Name :- Kaustubh Shrikant Kabra.
Class :- Third Year Engineering.
Div :- A
ERP Number :- 38
Deptarment :- Computer Department
College :- AISSMS's IOIT.

Title :-

RSA Algorithm

Aim :-

Write a Java/C/C++/Python program to implement RSA algorithm.

Objective :-

1. To understand and learn RSA algorithm.
2. Use RSA algorithm to implement a program.

Theory :-

RSA Algorithm is an asymmetric cryptography algorithm; this means that it uses a public key and a private key two different, mathematically linked keys. As their names suggest a public key is secret and must not be shared with anyone.

The following describes how asymmetric cryptography works:-

Sender $\xrightarrow{\text{Data}}$ Encryption ⟶ lipher text → Decryption
(sender encrypts data with receiver's public key) ↓ Data
Receiver

An example of asymmetric crypotography:

1. A client (for example browser) sends its public key to the server and requests for some data.

2. The server encrypts the data using clients public key and sends the encrypted data.

3. Client receives this data and decrypts it.

RSA Algorithm Mechanism -

- Select two prime's no's. Suppose $P = 53$ and $Q = 59$,
  Now first part of the public key:
  $n = P * Q = 3127.$

- We also need a small exponent say e:
  But e must be-
  i) An integer
  ii) Not be a factor of n.
  iii) $1 < e < \phi(n)$
  Let us now consider it to be equal to 3.

- Our Public Key is made of n and e.

→ Generating Private Key :-

- We need to calculate $\phi(n)$
  such that $\phi(n) = (P-1)(Q-1)$
  So, $\phi(n) = 3016$.

- Now calculate Private Key d:
  $d = (K * \phi(n) + 1) / e$ for some integer K
  for $K=2$, value of d is 2011.

- Now we are ready with our - Public Key ($n=3127$ and $e=3$) and Private Key ($d=2011$).
  Now we encrypt "Hi".

- Convert letters to numbers : $H = 8$ and $I = 9$.

- Thus Encrypted Data $c = 89^e \bmod n$. Thus our Encrypted data comes out to be 1394.

- Now we will decrypt 1394 :
  Decrypted data $= c^d \bmod n$.

- Thus our Encrypted Data comes out to be 89.
  $8=H$ and $I=9$ i.e. "HI".

Conclusion :-

Thus we encrypted and decrypted string data using RSA algorithm technique.