**PRACTICAL-5**

**AIM:** **Bob is going to send his encrypted file using public key shared by Alice using Publickey infrastructure. Alice will decrypt the file by using her private key and ensure the**

**confidentiality. Implement the following scenario using RSA algorithm. After applying RSA,**

**analyse the processing power of computer and speed with respective to time. Try using 1024**

**bit of key. Discuss what are the issues with this scenario**

****

**Software Requirements:** c compiler

**Theory/Logic**:

RSA algorithm is asymmetric cryptography algorithm. Asymmetric actually means that it works on two different keys i.e. Public Key and Private Key. As the name describes that the Public Key is given to everyone and Private key is kept private

**Algorithm**:Begin

1. Choose two prime numbers p and q.

2. Compute n = p\*q.

3. Calculate phi = (p-1) \* (q-1).

4. Choose an integer e such that 1 < e < phi(n) and gcd(e, phi(n)) = 1; i.e., e and phi(n) are

coprime.

5. Calculate d as d ≡ e−1 (mod phi(n)); here, d is the modular multiplicative inverse of e

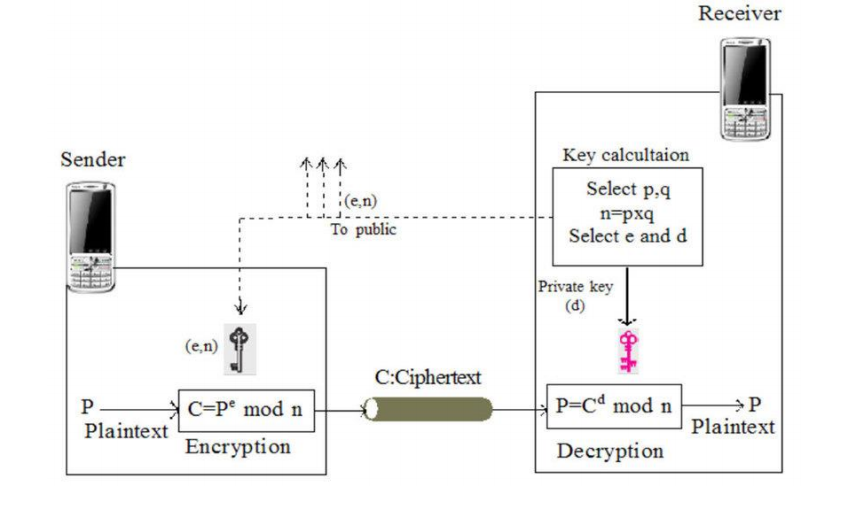
modulo phi(n).

6. For encryption, c = me mod n, where m = original message.

7. For decryption, m = c d mod n.

End

**Logical Diagram:**

****

**Code:**

#include<iostream>

#include<math.h>

using namespace std;

// Calculate gcd

int gcd(int a, int b) {

int t;

while(1) {

t= a%b;

if(t==0)

return b;

a = b;

b= t;

}

}

int main() {

//Two random prime numbers

double p = 13;

double q = 11;

double n=p\*q;//calculate n

double track;

double phi= (p-1)\*(q-1);//calculate phi

//public key

//e stands for encrypt

double e=7;

//for checking that 1 < e < phi(n) and gcd(e, phi(n)) = 1; i.e., e and phi(n) are coprime.

while(e<phi) {

track = gcd(e,phi);

if(track==1)

break;

else

e++;

}

//private key

//d stands for decrypt

//choosing d such that it satisfies d\*e = 1 mod phi

double d1=1/e;

double d=fmod(d1,phi);

double message = 9;

double c = pow(message,e); //encrypt the message

double m = pow(c,d);

c=fmod(c,n);

m=fmod(m,n);

cout<<"Plain Text Data = "<<message;

cout<<"\n"<<"p = "<<p;

cout<<"\n"<<"q = "<<q;

cout<<"\n"<<"n = pq = "<<n;

cout<<"\n"<<"phi = "<<phi;

cout<<"\n"<<"e = "<<e;

cout<<"\n"<<"d = "<<d;

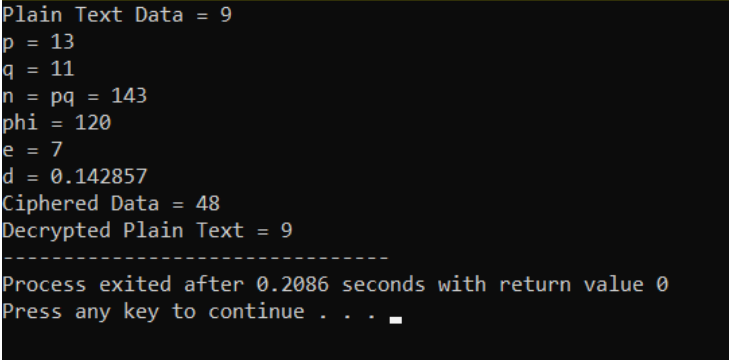
cout<<"\n"<<"Ciphered Data = "<<c;

cout<<"\n"<<"Decrypted Plain Text = "<<m;

return 0;

}

**Output:**

****

**Conclusion:** Hence we have studied what is Asymmetric Cryptography and learn

about RSA algorithm, also implemented it (both Encryption and

Decryption) for integer type message