**8.** a) **Write a program to encrypt and decrypt the data using RSA and**

**b) Write a program to exchange the key securely using Diffie-Hellman Key exchange protocol.**

RSA Algorithm

Generating Public Key

1. Select two prime numbers p and q.
2. Compute n=p\*q.
3. Choose e, such that it is an integer and not the factor of n.
4. Public key –(n,e)

Generating Private Key

1. Compute z=(p-1)\*(q-1)
2. Determine the private key d= (k\*z+1)/e, for some integer k.
3. Private key is d.

Diffie Hallman algorithm

1. Consider two prime numbers g and p.
2. Pick a secret number (a) and compute A= ga mod p.
3. Pick a secret number b and compute B= gb mod p
4. Encrypt message with Ba modpand send
5. Decrypt the received message with  Ab mod p.

**a) PROGRAM**

#include <iostream>

#include <stdlib.h>

#include <math.h>

#include <string.h>

using namespace std;

longintgcd(long int a, long int b)

{

if(a == 0)

return b;

if(b == 0)

return a;

returngcd(b, a%b);

}

longintisprime(long int a)

{

inti;

for(i = 2; i< a; i++){

if((a % i) == 0)

return 0;

}

return 1;

}

longint encrypt(char ch, long int n, long int e)

{

inti;

longint temp = ch;

for(i = 1; i< e; i++)

temp = (temp \* ch) % n;

return temp;

}

char decrypt(long intch, long int n, long int d)

{

inti;

longint temp = ch;

for(i = 1; i< d; i++)

ch =(temp \* ch) % n;

returnch;

}

int main()

{

longinti, len;

longint p, q, n, phi, e, d, cipher[50];

char text[50];

cout<< "Enter the text to be encrypted: ";

cin.getline(text, sizeof(text));

len = strlen(text);

do {

p = rand() % 30;

} while (!isprime(p));

do {

q = rand() % 30;

} while (!isprime(q));

n = p \* q;

phi = (p - 1) \* (q - 1);

do {

e = rand() % phi;

} while (gcd(phi, e) != 1);

do {

d = rand() % phi;

} while (((d \* e) % phi) != 1);

cout<< "Two prime numbers (p and q) are: " << p << " and " << q <<endl;

cout<< "n(p \* q) = " << p << " \* " << q << " = " << p\*q <<endl;

cout<< "(p - 1) \* (q - 1) = "<< phi <<endl;

cout<< "Public key (n, e): (" << n << ", " << e << ")\n";

cout<< "Private key (n, d): (" << n << ", " << d << ")\n";

for (i = 0; i<len; i++)

cipher[i] = encrypt(text[i], n, e);

cout<< "Encrypted message: ";

for (i = 0; i<len; i++)

cout<< cipher[i];

for (i = 0; i<len; i++)

text[i] = decrypt(cipher[i], n, d);

cout<<endl;

cout<< "Decrypted message: ";

for (i = 0; i<len; i++)

cout<< text[i];

cout<<endl;

return 0;

}

**OUTPUT**

exam@dell:~$ g++ rsa.cpp

exam@dell:~$ ./a.out

Enter the text to be encrypted: rvcecse

Two prime numbers (p and q) are: 13 and 23

n(p \* q) = 13 \* 23 = 299

(p - 1) \* (q - 1) = 264

Public key (n, e): (299, 103)

Private key (n, d): (299, 223)

Encrypted message: 11419683758318475

Decrypted message: rvcecse

**b) PROGRAM**

#include <stdio.h>

// Function to compute a^m mod n

int compute(int a, int m, int n)

{

int r;

int y = 1;

while (m > 0)

{

r = m % 2;

// fast exponention

if (r == 1)

y = (y\*a) % n;

a = a\*a % n;

m = m / 2;

}

return y;

}

// C program to demonstrate Diffie-Hellman algorithm

int main()

{

int p = 23; // modulus

int g = 5; // base

int a, b; // a - Alice's Secret Key, b - Bob's Secret Key.

int A, B; // A - Alice's Public Key, B - Bob's Public Key

// choose secret integer for Alice's Pivate Key (only known to Alice) srand(time(0)) ;

a = rand(); // or use rand()

// Calculate Alice's Public Key (Alice will send A to Bob)

A = compute(g, a, p);

// choose secret integer for Bob's Pivate Key (only known to Bob)

srand(time(0)) ;

b = rand(); // or use rand()

// Calculate Bob's Public Key (Bob will send B to Alice)

B = compute(g, b, p);

// Alice and Bob Exchanges their Public Key A & B with each other

// Find Secret key

Int keyA = compute(B, a, p);

Int keyB = compute(A, b, p);

printf("\nAlice's Secret Key is %d\nBob's Secret Key is %d\n\n", keyA, keyB);

return 0;

}

**OUTPUT**

RUN-1

exam@dell:~$ ./a.out

Alice's Secret Key is 4

Bob's Secret Key is 4

RUN-2

exam@dell:~$ ./a.out

Alice's Secret Key is 11

Bob's Secret Key is 11

RUN-3

exam@dell:~$ ./a.out

Alice's Secret Key is 10

Bob's Secret Key is 10