Date : 3-11-22

Experiment No. 3

3) Suppose Alice wants her friends to encrypt email messages before sending them to her. Write a program to help her friends to encrypt and decrypt the data (RSA algorithm)

```
#include <stdio.h>
#include <stdlib.h>
#include <math.h>
#include <string.h>

long int gcd(long int a, long int b)
{
  if(a==0)
    return b;
  if(b==0)
    return a;
  return gcd(b, a%b);
}
long int isprime(long int a)
{
  int i;
  for(i=2; i<a; i++)
  {
    if((a%i)==0)
      return 0;
  }
  return 1;
}
long int encrypt(char ch, long int n, long int e)
{
  int i;
  long int temp = ch;
```

Date : 3-11-22

Experiment No. 3

```
    for (i=1; i<e; i++)
        temp = (temp * ch) % n;
    return temp;
}
char decrypt (long int ch, long int n, long int d)
{
    int i;
    long int temp = ch;
    for (i=1; i<d; i++)
        ch = (ch * temp) % n;
    return ch;
}
int main()
{
    long int i, len;
    long int p, q, n, phi, e, d, cipher[50];
    char text[50];
    printf("Enter text to be encrypted: ");
    fgets(text, 50, stdin);
    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
    {
```

Date : 3-11-22

Experiment No. 3

```
    e = rand() % phi;
} while (gcd(phi, e) != 1);
do
{
    d = rand() % phi;
} while (((d * e) % phi) != 1);
do
{
    d = rand() % phi;
} while (((d*e) % phi) != 1);

printf("Two prime numbers (p and q)
        are: %ld and %ld \n", p, q);
printf("n = (p*q) = %ld * %ld = %ld \n", p, q, p*q
        );
printf("(p-1) * (q-1) = %ld \n", phi);
printf("private key (n,e) (%ld, %ld) \n", n, e);
printf("Public key (n, d) (%ld, %ld) \n", n, d);
for (i=0; i<len; i++)
    cipher[i] = encrypt(text[i], n, e);
printf("Encrypted message: \n");
for (i=0; i<len; i++)
    printf("%ld", cipher[i]);
for (i=0; i<len; i++)
    text[i] = decrypt(cipher[i], n, d);
printf("\n Decrypted message: ");
for (i=0; i<len; i++)
    printf("%c", text[i]);
printf("\n");
return 0;
}
```

10/11/22

OUTPUT:-

```
./a.out
Enter text to be encrypted : Punya
Two prime numbers (p and q) are : 13 and 23
n = (p * q) = 13 * 23 = 299
(p-1) * (q-1) = 264
Private key (n,e) (299, 103)
Public key (n,d) (299, 223)
Encrypted message : 98225111118413268248116131166
Decrypted message : Punya.
```