Reg.No: 210701092

Experiment no: 2a Date: 20/2/24	RSA Algorithm

AIM:
To write the C program to perform RSA Algorithm for Both Encryption And Decryption

ALGORITHM:

Step 1: START
Step 2: Choose two Large prime Number p and q
Step 3: Calculate $n = p*q$ and $z = (1-p)(1-q)$
Step 4: Choose the Number e where $1<e<z$
Step 5: Calculate $d = e^{-1} \bmod (p-1)(q-1)$
Step 6: Bundle the private key as (n,d) And public key as (n,e)
Step 7: Encrypt Using public key And Decrypt Using private key
Step 8: STOP

Exp 2a : RSA Algorithm

Code:

```
//RSA Algorithm
#include <stdio.h>
#include <math.h>

int gcd(int a, int h) {
int temp;
    while (1) {
        temp = a % h;
if (temp == 0)
return h;         a =
h;
        h = temp;
    }
}

int main() {
int p = 3;
int q = 7;

    printf("\nValue of p = %d",p);
printf("\nValue  of  q  =  %d",q);
int n = p * q;
    printf("\nValue of n = %d",n);

    int e = 2;
    int phi = (p - 1) * (q - 1);
while (e < phi) {

        if (gcd(e, phi) == 1)
break;
        else
            e++;
    }


    int k = 2;
    double d = (1 + (k * phi)) / (double)e;

    int msg = 9;

    printf("\n\nMessage data = %d", msg);

    double c = pow(msg, e);
    c = fmod(c, n);
    printf("\nEncrypted data = %.0lf", c);
    double m = pow(c, d);
    m = fmod(m, n);
    printf("\nOriginal Message Sent = %.0lf", m);
```

```
    return 0;
}
```

Output:

```
Value of p = 3
Value of q = 7
Value of n = 21

Message data = 9
Encrypted data = 18
Original Message Sent = 9
```