INFORMATION SECURITY & CRYPTOGRAPHY
ASSIGNMENT- 5

U20C005
BANSI MARAKANA

Using RSA, construct a program to encrypt and decrypt plaintext messages strings.

```
#include <bits/stdc++.h>
#include <iostream>
using namespace std;
bool isprime(int num)
{
    if (num > 2)
    {
        for (int i = 2; i <= (num + 2) / 2; i++)
            if (num % i == 0)
            {
                cout << "\t" << num << " is not a prime number\n\tEnter
another number: ";
                return false;
            }
            else
                return true;
    }
    else if (num == 2)
        return true;
    else
    {
        cout << "\tEnter valid input!!\n";
        return false;
    }
    return false;
}

int takeprime()
{
    int prime;
    cin >> prime;
    if (isprime(prime))
        return prime;
    else
```

```
        takeprime();
    return 0;
}

long long int encrypt_decrypt(int message, int key, int n)
{
    long long int text = 1;
    while (key--)
        text = ((text % n) * (message % n)) % n;
    return text;
}

vector<int> encode_decode(vector<int> input_text, int key, int n)
{
    vector<int> output_text;
    for (auto &value : input_text)
        output_text.push_back(encrypt_decrypt(value, key, n));
    return output_text;
}

int main()
{
    string message;
    int prime1, prime2;
    cout << "Enter 1st prime number: ";
    prime1 = takeprime();
    cout << "\nEnter 2nd prime number: ";
    prime2 = takeprime();
    int e, d, n = prime1 * prime2, fi = (prime1 - 1) * (prime2 - 1);
    cout << "\nEnter value of e: ";
    cin >> e;
    while (1)
    {
        if (__gcd(e, fi) == 1)
            break;
        else
        {
            cout << "\tEnter value of e again: ";
            cin >> e;
        }
```

```
    }
    cout << "\nEnter value of d: ";
    cin >> d;
    while (1)
    {
        if ((d * e) % fi == 1)
            break;
        else
        {
            cout << "\tEnter value of d again: ";
            cin >> d;
        }
    }
    cout << "\nEnter a string(Enter $ to stop): ";
    getline(cin,message,'$');
    int public_key = e, private_key = d;
    vector<int> msg;
    for (auto &value : message)
        msg.push_back((int)value);
    vector<int> coded = encode_decode(msg, e, n);
    cout << "\nEncrypted message is: \n\t";
    string encrypt;
    for (auto &p : coded)
    {
        cout << p;
        encrypt += (char)p;
    }
    cout << "\n\nEncrypted message in ascii format is: \n\t" << encrypt;
    cout << "\n\nDecrypted message: \n\t";
    vector<int> decoded = encode_decode(coded, d, n);
    string decrypt;
    for (auto &p : decoded)
    {
        cout << p;
        decrypt += p;
    }
    cout << "\n\nDecrypted message in ascii format is: " << decrypt;
    return 0;
}
```

```
Enter 1st prime number: 17

Enter 2nd prime number: 11

Enter value of e: 7

Enter value of d: 23

Enter a string(Enter $ to stop): Hello World!!
I am learning Cryptography.$

Encrypted message is:
        175308448481557643155126481443333175617692131764884921266696661377667126777374155137126927317977 7

Encrypted message in ascii format is:
        »▲T00¢L+¢~0É!!»=L\âL0T\~B`BëLC~MIJ¢ë~\I|M

Decrypted message:
        10721011081081113287111114108100333310733297109321081019711411010511010332671141211121161111031149711210412146

Decrypted message in ascii format is:
Hello World!!
I am learning Cryptography.
```