AHSANULLAH UNIVERSITY OF SCIENCE AND TECHNOLOGY

Department of Computer Science and Engineering

Program: Bachelor of Science in Computer Science and Engineering

Course Code: **CSE 4174**
Course Title: **Cyber Security Lab**
Academic Semester: **Spring 2023**

Assignment Topic: **RSA (Rivest-Shamir-Adleman) Algorithm**

Submitted on: **2nd December, 2023**

Submitted by

Name: **Meherin Sultana**
Student ID: **20200104036**
Lab Section: **A2**

Question:

Devise a program using the RSA algorithm demonstrating the key set up and encryption-decryption.

Code (implemented in C++):

```
#include <bits/stdc++.h>
using namespace std;

int public_key;
int private_key;
int n;

void initialize_keys()
{
   int prime1 = 73;
   int prime2 = 151;
   n = prime1 * prime2;
   int PHI = (prime1 - 1) * (prime2 - 1);
   cout << "Value of n: " << n << "\n";
   cout << "PHI (phi): " << PHI << "\n";

   int e=2, d=2;;
   while (1)
   {
      if (__gcd(e, PHI) == 1)
         break;
      e++;
   }
   public_key = e;
```

```
    while (1)
    {
        if ((d * e) % PHI == 1)
            break;
        d++;
    }
    private_key = d;

    cout << "Public Key (e): " << e << "\n";
    cout << "Private Key (d): " << d << "\n";
}

long long int encrypt_message(double message)
{
    int e = public_key;
    long long int encrypted_text = 1;
    while (e--)
    {
        encrypted_text *= message;
        encrypted_text %= n;
    }
    return encrypted_text;
}

long long int decrypt_message(int encrypted_text)
{
    int d = private_key;
    long long int decrypted = 1;
    while (d--)
    {
        decrypted *= encrypted_text;
        decrypted %= n;
```

```
    }
    return decrypted;
}

vector<int> encode_message(string message)
{
    vector<int> form;
    for (auto &letter : message)
        form.push_back(encrypt_message((int)letter));
    return form;
}

string decode_message(vector<int> encoded)
{
    string s;
    for (auto &num : encoded)
        s += decrypt_message(num);
    return s;
}

int main()
{
    initialize_keys();
    string message ;
    cout<<"Enter the text: ";
    getline(cin,message);

    vector<int> coded = encode_message(message);
    cout << "\nInitial message:\n"<< message;
    cout << "\n\nAfter encryption using public key:\n";
    for (auto &p : coded)
        cout << p;
```

```
    cout << "\n\nAfter decryption using private key:\n";
    cout << decode_message(coded) << endl;
    return 0;
}
```

Output: