AHSANULLAH UNIVERSITY OF SCIENCE AND TECHNOLOGY

Department of Computer Science and Engineering

Program: Bachelor of Science in Computer Science and Engineering

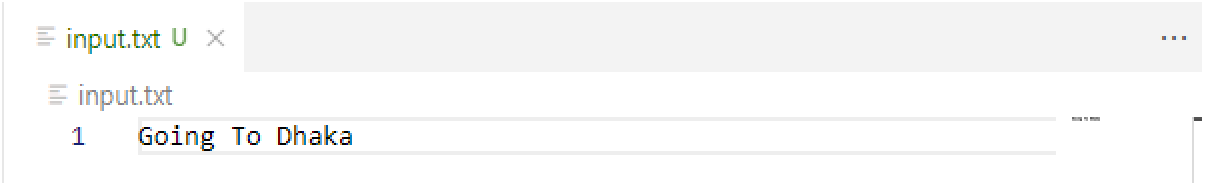
Course Code: CSE 4174
Course Title: Cyber Security Lab
Academic Semester: Spring 2023

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

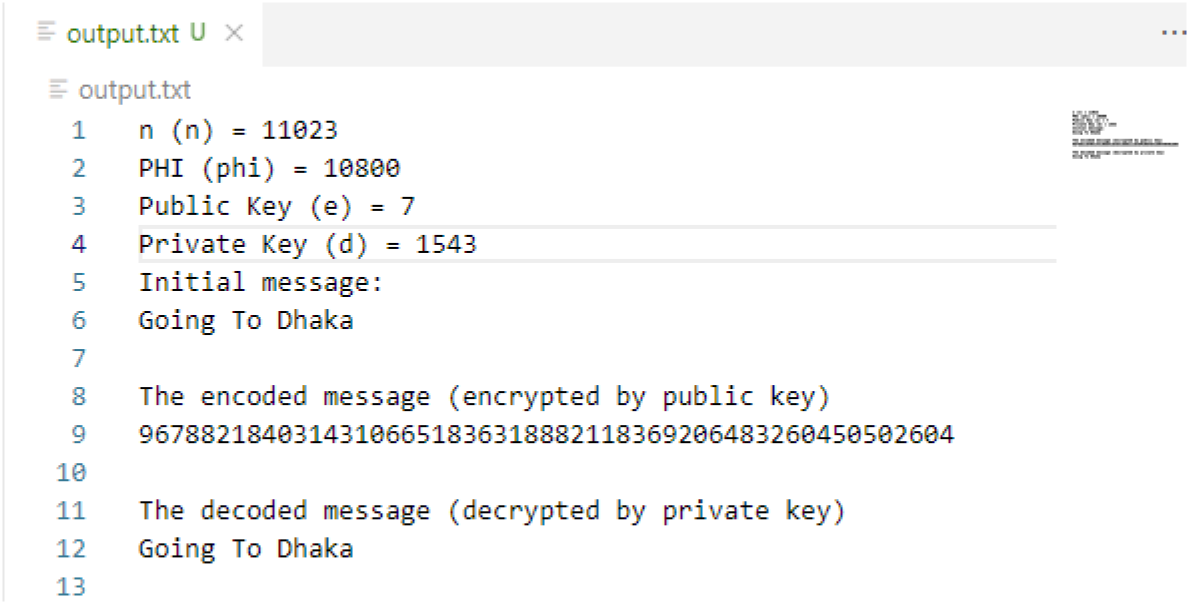
Submitted on: 27/11/23

Submitted by
Name: Abdullah Yusha
Student ID: 20200104113
Lab Section: C1

Console I/O:



```
Going To Dhaka
```



```
n (n) = 11023
PHI (phi) = 10800
Public Key (e) = 7
Private Key (d) = 1543
Initial message:
Going To Dhaka

The encoded message (encrypted by public key)
96788218403143106651836318882118369206483260450502604

The decoded message (decrypted by private key)
Going To Dhaka

```

Code :

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

    cout << "n (n) = " << n << "\n";
    cout << "PHI (phi) = " << PHI << "\n";
    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() {

       // For getting input from input.txt file
   freopen("F:\\GIT\\input.txt", "r", stdin);

    // Printing the Output to output.txt file
   freopen("F:\\GIT\\output.txt", "w", stdout);
   initialize_keys();
    string message ;
    getline(cin,message);
    vector<int> coded = encode_message(message);
    cout << "Initial message:\n"
         << message;
    cout << "\n\nThe encoded message (encrypted by public key)\n";
    for (auto &p : coded)
        cout << p;
    cout << "\n\nThe decoded message (decrypted by private key)\n";
    cout << decode_message(coded) << endl;
    return 0;
}
```