Visvesvaraya Technological University

Belagavi, Karnataka – 590018

Report on

Assignment 2

Submitted in partial fulfillment of the requirements for the course

CRYPTOGRAPHY (18CS744)

Submitted by

Prithviraj Patil **1JS19CS125**

Under the guidance of

Mrs. Naidila Sadashiv B. E, M. Tech, Ph.D

Associate professor, Dept. of CSE,

JSS Academy of Technical Education, Bengaluru

JSS Academy of Technical Education, Bengaluru – 560060,

Department of Computer Science and Engineering

2022-2023

```
double q = 7;
double n = p * q;
double e = 2;
double phi = (p - 1) * (q - 1);
while (e < phi) {
    if (gcd(e, phi) == 1)
        break;
    else
        e++;
}
double d = (1 + (k * phi)) / e;
double msg = 12;
printf("Message data = %lf", msg);
double c = pow(msg, e);
c = fmod(c, n);
printf("\nEncrypted data = %lf", c);
double m = pow(c, d);
m = fmod(m, n);
printf("\nOriginal Message Sent = %lf", m);
return 0; }
```

Output :

```
"C:\Users\prith\OneDrive\Documents\c program 2\rsa\bin\Debug\rsa.exe"
Message data = 12.000000
Encrypted data = 3.000000
Original Message Sent = 12.000000
Process returned 0 (0x0)   execution time : 0.097 s
Press any key to continue.
```

```
    // Alice will choose the private key a
    a = 4; // a is the chosen private key
    cout << "The private key a for Alice : " << a << endl;

    x = power(G, a, P); // gets the generated key

    // Bob will choose the private key b
    b = 3; // b is the chosen private key
    cout << "The private key b for Bob : " << b << endl;

    y = power(G, b, P); // gets the generated key

    // Generating the secret key after the exchange
    // of keys
    ka = power(y, a, P); // Secret key for Alice
    kb = power(x, b, P); // Secret key for Bob
    cout << "Secret key for the Alice is : " << ka << endl;

    cout << "Secret key for the Alice is : " << kb << endl;

    return 0;
}
```

Output :

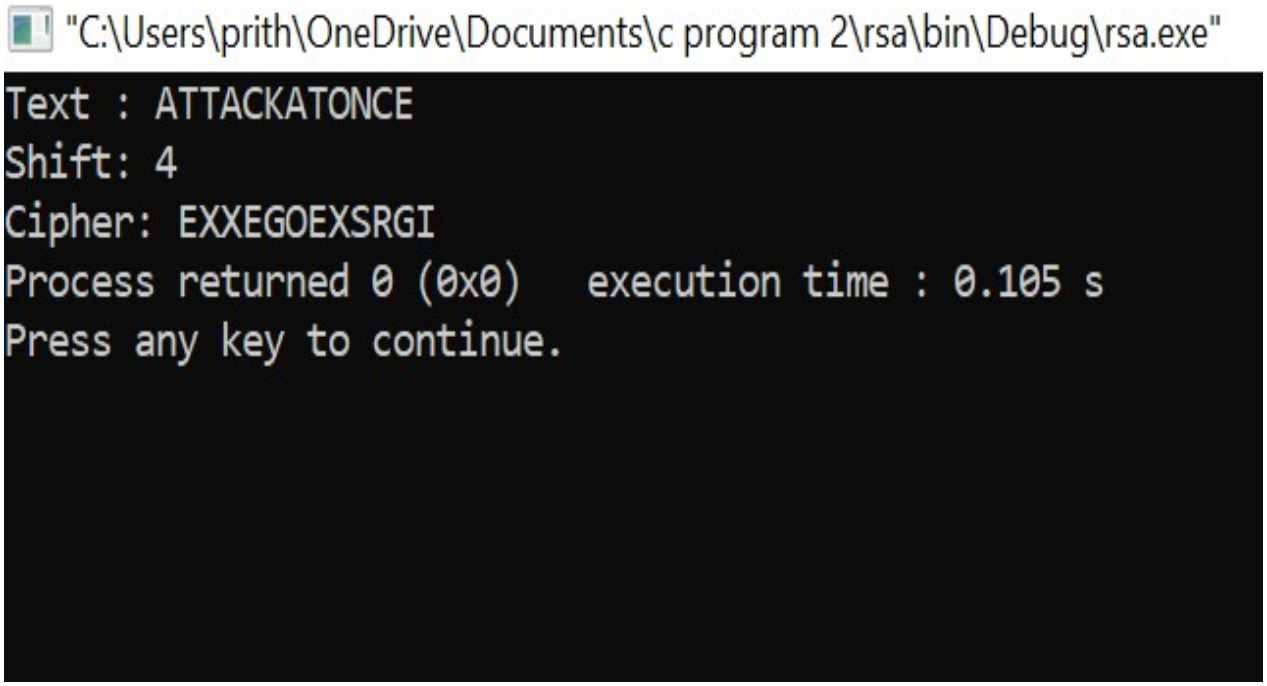
"C:\Users\prith\OneDrive\Documents\c program 2\rsa\bin\Debug\rsa.exe"

```
The value of P : 23
The value of G : 9
The private key a for Alice : 4
The private key b for Bob : 3
Secret key for the Alice is : 9
Secret key for the Alice is : 9

Process returned 0 (0x0)   execution time : 0.123 s
Press any key to continue.
```

```
    // Return the resulting string
    return result;
}
// Driver program to test the above function
int main()
{
    string text = "ATTACKATONCE";
    int s = 4;
    cout << "Text : " << text;
    cout << "\nShift: " << s;
    cout << "\nCipher: " << encrypt(text, s);
    return 0;
}
```

Output:



```
    // Following function generates
    // the encrypted vector
    encrypt(cipherMatrix, keyMatrix, messageVector);
    string CipherText;
    // Generate the encrypted text from
    // the encrypted vector
    for (int i = 0; i < 3; i++)
        CipherText += cipherMatrix[i][0] + 65;
    // Finally print the ciphertext
    cout << " Ciphertext:" << CipherText;
}
// Driver function for above code
int main()
{
    // Get the message to be encrypted
    string message = "ACT";
    // Get the key
    string key = "GYBNQKURP";
    HillCipher(message, key);
    return 0;
}
```

Output:

```
"C:\Users\prith\OneDrive\Documents\c program 2\rsa\bin\Debug\rsa.exe"
 Ciphertext:POH
Process returned 0 (0x0)   execution time : 0.105 s
Press any key to continue.
```

Output:

"C:\Users\prith\OneDrive\Documents\c program 2\rsa\bin\Debug\rsa.exe"

```
Encryption:

After initial permutation: 14A7D67818CA18AD
After splitting: L0=14A7D678 R0=18CA18AD

Round 1 18CA18AD 5A78E394 194CD072DE8C
Round 2 5A78E394 4A1210F6 4568581ABCCE
Round 3 4A1210F6 B8089591 06EDA4ACF5B5
Round 4 B8089591 236779C2 DA2D032B6EE3
Round 5 236779C2 A15A4B87 69A629FEC913
Round 6 A15A4B87 2E8F9C65 C1948E87475E
Round 7 2E8F9C65 A9FC20A3 708AD2DDB3C0
Round 8 A9FC20A3 308BEE97 34F822F0C66D
Round 9 308BEE97 10AF9D37 84BB4473DCCC
Round 10 10AF9D37 6CA6CB20 02765708B5BF
Round 11 6CA6CB20 FF3C485F 6D5560AF7CA5
Round 12 FF3C485F 22A5963B C2C1E96A4BF3
Round 13 22A5963B 387CCDAA 99C31397C91F
Round 14 387CCDAA BD2DD2AB 251B8BC717D0
Round 15 BD2DD2AB CF26B472 3330C5D9A36D
Round 16 19BA9212 CF26B472 181C5D75C66D

Cipher Text: C0B7A8D05F3A829C
```

```
Decryption

After initial permutation: 19BA9212CF26B472
After splitting: L0=19BA9212 R0=CF26B472

Round 1 CF26B472 BD2DD2AB 181C5D75C66D
Round 2 BD2DD2AB 387CCDAA 3330C5D9A36D
Round 3 387CCDAA 22A5963B 251B8BC717D0
Round 4 22A5963B FF3C485F 99C31397C91F
Round 5 FF3C485F 6CA6CB20 C2C1E96A4BF3
Round 6 6CA6CB20 10AF9D37 6D5560AF7CA5
Round 7 10AF9D37 308BEE97 02765708B5BF
Round 8 308BEE97 A9FC20A3 84BB4473DCCC
Round 9 A9FC20A3 2E8F9C65 34F822F0C66D
Round 10 2E8F9C65 A15A4B87 708AD2DDB3C0
Round 11 A15A4B87 236779C2 C1948E87475E
Round 12 236779C2 B8089591 69A629FEC913
Round 13 B8089591 4A1210F6 DA2D032B6EE3
Round 14 4A1210F6 5A78E394 06EDA4ACF5B5
Round 15 5A78E394 18CA18AD 4568581ABCCE
Round 16 14A7D678 18CA18AD 194CD072DE8C

Plain Text: 123456ABCD132536
```