

Kolej Tunku Abdul Rahman

School of Arts and Science



AAMS 5144 Cryptography Practical 2

Course: ACN2

Tutorial Group: M1

Group Member:

Name	ID Number	Contribution
Lai Choon Siang*	06WAB11778	30%
Foo Hwui Ling	06WAB11777	30%
Lim Lee Get	06WAB13458	20%
Wong Sin Yee	06WAB13363	20%

Table of Contents

1.Generate keys using RSA.....	1
2.Encrypt message of 3 characters.....	6
3.Decrypt ciphertext of 15 bits.....	10
4.Cryptanalysis.....	14

1. Generate keys using RSA

1.1. Generate random numbers of 7 bits

The algorithm used in this part is Blum-Blum-Shub random number generator. BBS Generator generates a seed, s_0 which is any element of quadratic residues modulo n ($QR(n)$) where $n = p \times q$, and p, q is two prime numbers such that $p \equiv q \equiv 3 \pmod{4}$.

Then compute the sequence s_1, s_2, \dots, s_i by successive squaring modulo n , and then reduce each s_i modulo 2 to obtain z_i which is a series of bits.

$$s_{i+1} = s_i^2 \pmod{n}$$

$$z_i = s_i \pmod{2}$$

1.2. Test for primality

To test for primality, we used Miller Rabin test but not too successful. Then we complement the test with an effort trying to factorize the number. If a factor is returned then the number is not a prime. The factoring algorithm picked is the $p-1$ method however if the exact algorithm as introduced in the notes is used, then there will be composite number not being able to be factorized. Therefore an improved algorithm is used based on the PMinusOne method. Instead of fixing $a = 2$, another loop is used to loop the initial value of a from 2 to 99. Then more of the composite numbers will have a factor.

1.3. Obtain 2 prime numbers. (p and q)

After obtaining 2 random numbers from BBS Generator and tested for primality, let the 2 numbers be p and q .

1.4. Compute n (public key) and $\Phi(n)$

n is the public key for RSA where as $\Phi(n)$ is to be kept secret to generate the secret key, a .

$$n = p \times q$$

$$\Phi(n) = (p-1)(q-1)$$

1.5. Generate a random number, b (public key), such that $\text{gcd}(b, \Phi(n)) = 1$

Generate a random number, b , using BBS Generator and check the Greatest Common Divisor of b and $\Phi(n)$. b is the public key for RSA.

1.6. Find the secret key, a

Then, compute a , which is the secret key.

$$a = b^{-1} \text{ mod } \Phi(n)$$

1.7. Screenshots of the Program

```
C:\Program Files\Microsoft Visual Studio\MyProjects\Cryptography\Debug\Cr...
"C:\Program Files\Microsoft Visual Studio\MyProjects\Cryptography\Debug\Cryptography.exe"

=====
AAMS 5144 - Cryptography Practical 2
Main Menu (Enter the Corresponding Module Number)
=====

1. Publish Public Key
2. Encrypt a String
3. Decrypt a String
4. Encrypt a Binary Number
5. Decrypt a Binary Number
6. Breaking a RSA Cryptosystem
7. RSA Cryptosystem Testing
0. Exit the System

Group Members :
a. Foo Hwui Ling
b. Lai Choon Siang
c. Lim Lee Get
d. Wong Sin Yee

Course / Tutorial Group : ACN 2 / M1
Lecturer / Tutor : Mr. Teo Kok Chau

=====

Enter the destination module (0 or other numbers exits the system)
> 1
```

Figure 1.1 Displaying the Main Menu

```
C:\Program Files\Microsoft Visual Studio\MyProjects\Cryptography\Debug\Cr...

=====
Publish Public Key
=====

Status: Generating p to calculate n. (Please wait)

Blum-Blum-Shub Generator: Generating p.
Blum-Blum-Shub Generator: Generating q. (trial count: 3)
Blum-Blum-Shub Generator: p = 11, q = 79
Blum-Blum-Shub Generator: Returns Random Number = 94 (trial count: 1)

System: p = 94 is not prime, regenerating p.

Blum-Blum-Shub Generator: Generating p.
Blum-Blum-Shub Generator: Generating q.
```

Figure 1.2 Generating P to Calculate Public Key n

```
"C:\Program Files\Microsoft Visual Studio\MyProjects\Cryptography\Debug\Cr... - [ ] X
=====
Publish Public Key
=====

Status: Generating q to calculate n. (Please wait)

Blum-Blum-Shub Generator: Generating p.
Blum-Blum-Shub Generator: Generating q. (trial count: 2)
Blum-Blum-Shub Generator: p = 103, q = 79
Blum-Blum-Shub Generator: Returns Random Number = 10 (trial count: 1)

System: q = 10 is not prime, regenerating q.

Blum-Blum-Shub Generator: Generating p.
Blum-Blum-Shub Generator: Generating q.
```

Figure 1.3 Generating Q to Calculate Public Key n

```
"C:\Program Files\Microsoft Visual Studio\MyProjects\Cryptography\Debug\Cr... - [ ] X
=====
Publish Public Key
=====

Status: Generating B. (Please wait)

Blum-Blum-Shub Generator: Generating p.
Blum-Blum-Shub Generator: Generating q. (trial count: 2)
Blum-Blum-Shub Generator: p = 3, q = 83
Blum-Blum-Shub Generator: Returns Random Number = 22 (trial count: 1)

Error: b = 22 returned is not valid, regenerating.

Blum-Blum-Shub Generator: Generating p.
Blum-Blum-Shub Generator: Generating q.
```

Figure 1.4 Generating Public Key B

```
=====  
Publish Public Key  
=====  
Status: Publishing Public Keys.  
The RSA public key n is 7171  
The RSA public key b is 101  
=====  
Press any key to continue . . .
```

Figure 1.5 Displaying Public Keys

```
=====  
Publish Public & Private Keys  
=====  
Status: Publishing Public and Private Keys.  
The RSA public key n is 7171  
The RSA public key b is 101  
The RSA public key n = 7171 is a product of p = 71 and q = 101  
Therefore the Phi-N is calculated to be 7000  
The RSA private key a is therefore 901  
=====  
Press any key to continue . . .
```

Figure 1.6 Displaying Private Keys

2. Encrypt message of 3 characters.

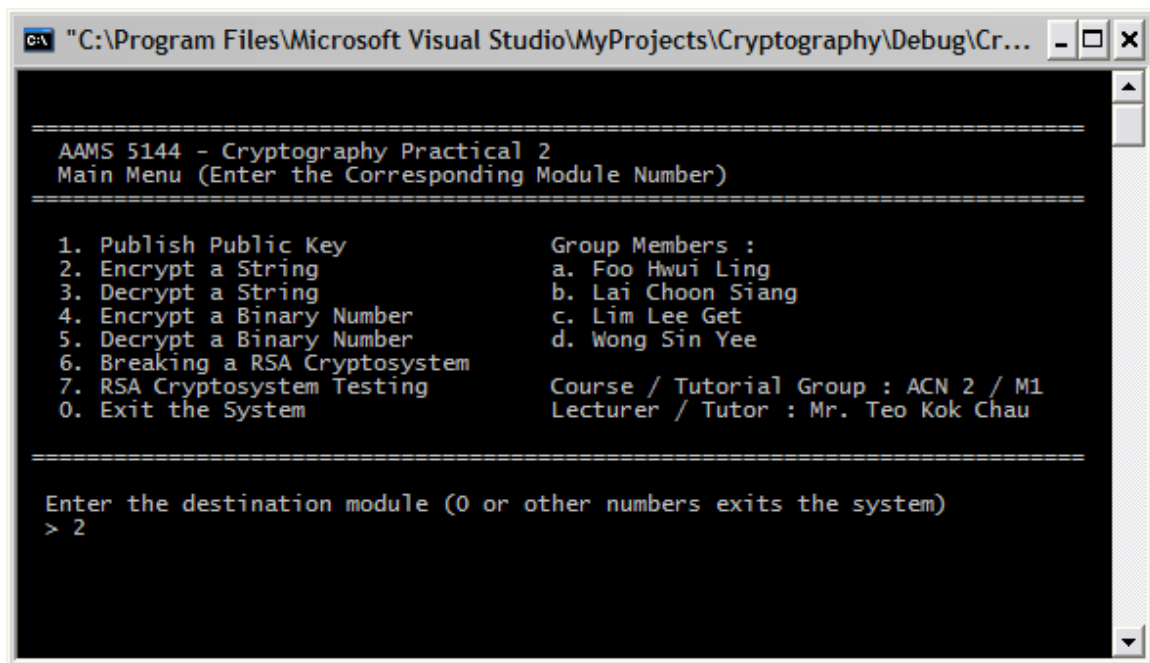
To encrypt a message of 3 characters, conversion from characters to numbers is needed. The decoding of the number is based on the encoding algorithm as below (Computer Science at University of Rhode Island, n.d.):

$$X = (x_1 * 26^0) + (x_2 * 26^1) + (x_3 * 26^2) \dots + (x_n * 26^{n-1})$$

To encrypt a message:

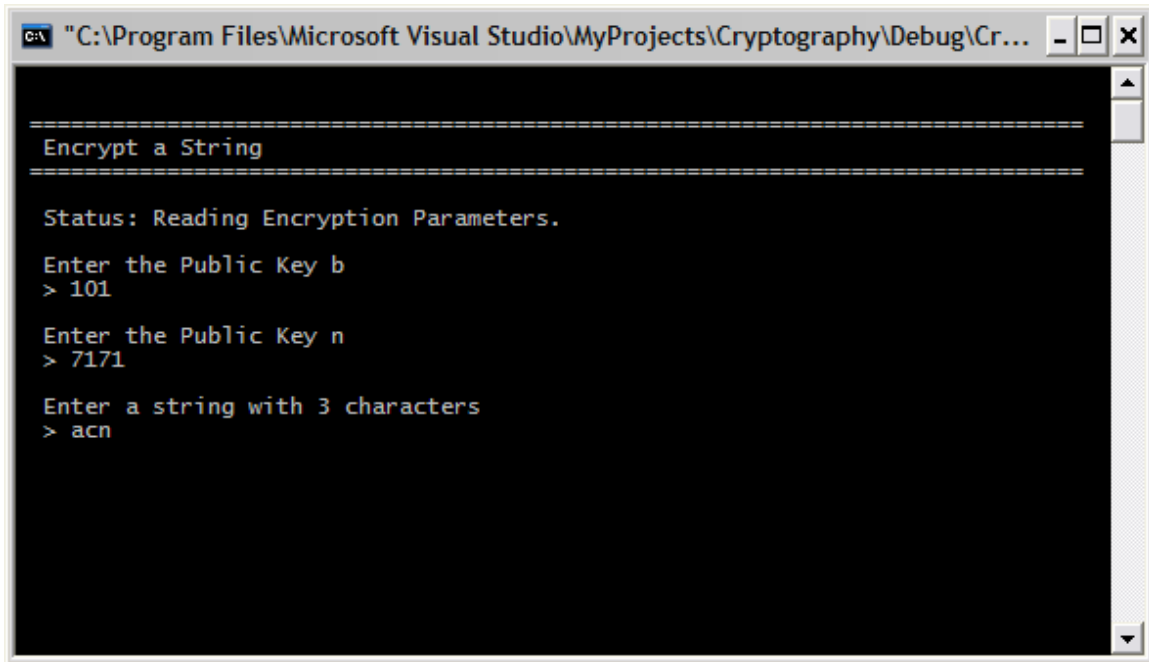
$$e_k(x) = x^b \text{ mod } n$$

where b and n are the public keys.



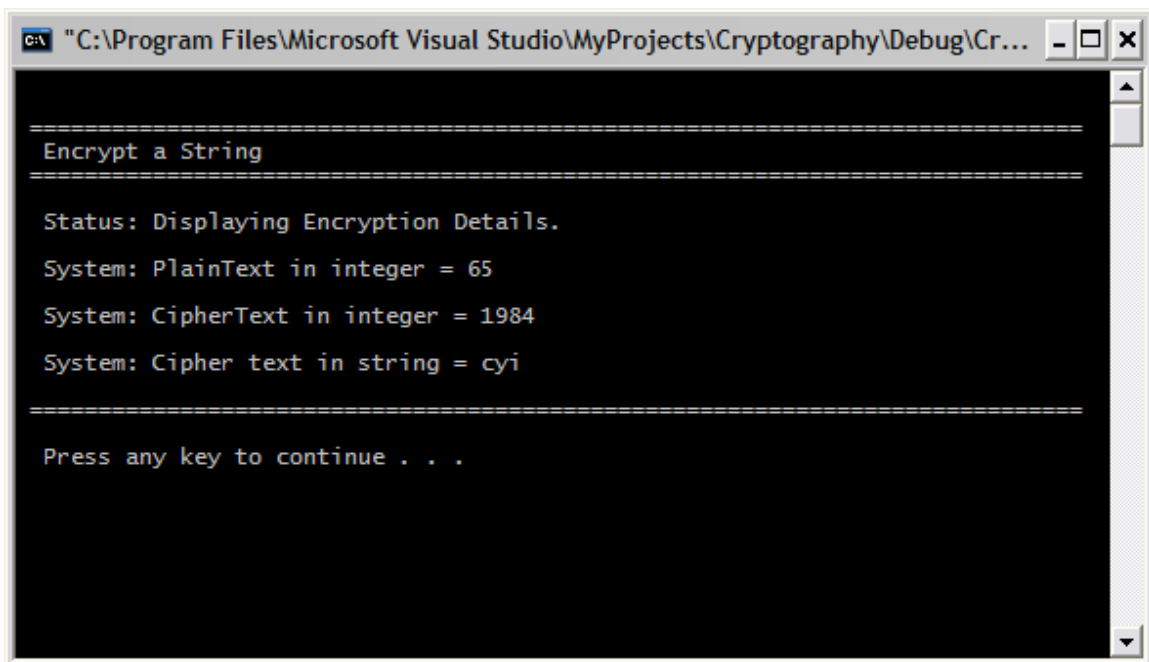
```
"C:\Program Files\Microsoft Visual Studio\MyProjects\Cryptography\Debug\Cr... - □ ×
=====
AAMS 5144 - Cryptography Practical 2
Main Menu (Enter the Corresponding Module Number)
=====
1. Publish Public Key                Group Members :
2. Encrypt a String                  a. Foo Hwui Ling
3. Decrypt a String                  b. Lai Choon Siang
4. Encrypt a Binary Number           c. Lim Lee Get
5. Decrypt a Binary Number           d. Wong Sin Yee
6. Breaking a RSA Cryptosystem
7. RSA Cryptosystem Testing          Course / Tutorial Group : ACN 2 / M1
0. Exit the System                  Lecturer / Tutor : Mr. Teo Kok Chau
=====
Enter the destination module (0 or other numbers exits the system)
> 2
```

Figure 2.7 Displaying the Main Menu



```
c:\ "C:\Program Files\Microsoft Visual Studio\MyProjects\Cryptography\Debug\Cr... - □ X  
=====  
Encrypt a String  
=====  
Status: Reading Encryption Parameters.  
Enter the Public Key b  
> 101  
Enter the Public Key n  
> 7171  
Enter a string with 3 characters  
> acn
```

Figure 2.8 Entering Encryption Parameters



```
c:\ "C:\Program Files\Microsoft Visual Studio\MyProjects\Cryptography\Debug\Cr... - □ X  
=====  
Encrypt a String  
=====  
Status: Displaying Encryption Details.  
System: PlainText in integer = 65  
System: CipherText in integer = 1984  
System: Cipher text in string = cyi  
=====  
Press any key to continue . . .
```

Figure 2.9 Displaying Encryption Result

```
C:\ "C:\Program Files\Microsoft Visual Studio\MyProjects\Cryptography\Debug\Cr... - [ ] X
=====
AAMS 5144 - Cryptography Practical 2
Main Menu (Enter the Corresponding Module Number)
=====

1. Publish Public Key          Group Members :
2. Encrypt a String           a. Foo Hwui Ling
3. Decrypt a String            b. Lai Choon Siang
4. Encrypt a Binary Number     c. Lim Lee Get
5. Decrypt a Binary Number     d. Wong Sin Yee
6. Breaking a RSA Cryptosystem
7. RSA Cryptosystem Testing    Course / Tutorial Group : ACN 2 / M1
0. Exit the System             Lecturer / Tutor : Mr. Teo Kok Chau
=====

Enter the destination module (0 or other numbers exits the system)
> 3
```

Figure 2.10 System Displaying the Main Menu

```
C:\ "C:\Program Files\Microsoft Visual Studio\MyProjects\Cryptography\Debug\Cr... - [ ] X
=====
Decrypt a String
=====

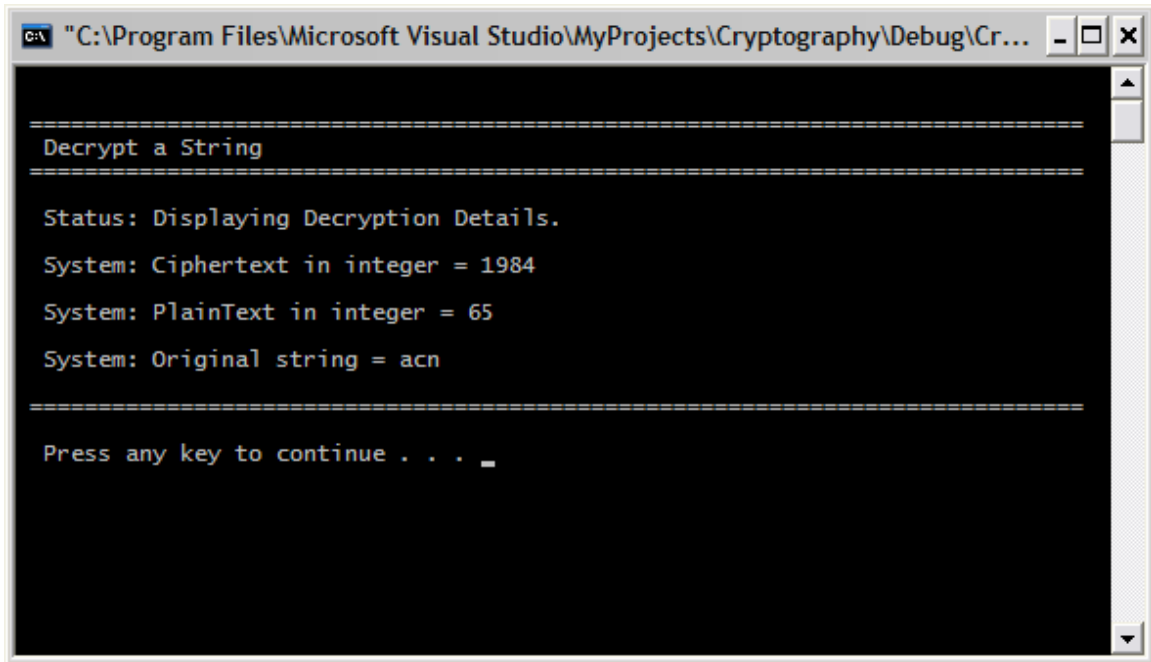
Status: Reading Decryption Parameters.

Enter the Private Key a
> 901

Enter the Public Key n
> 7171

Enter a string with 3 characters
> cyi
```

Figure 2.11 Entering the Data for Verification



The image shows a Windows command prompt window with a title bar that reads "C:\Program Files\Microsoft Visual Studio\MyProjects\Cryptography\Debug\Cr...". The window contains the following text:

```
=====  
Decrypt a String  
=====  
Status: Displaying Decryption Details.  
System: Ciphertext in integer = 1984  
System: PlainText in integer = 65  
System: Original string = acn  
=====  
Press any key to continue . . . _
```

Figure 2.12 System Showing the Decryption Result

3. Decrypt ciphertext of 15 bits.

To decrypt a ciphertext:

$$d_k(y) = y^a \text{ mod } n$$

where n is the public key and a is the secret key.

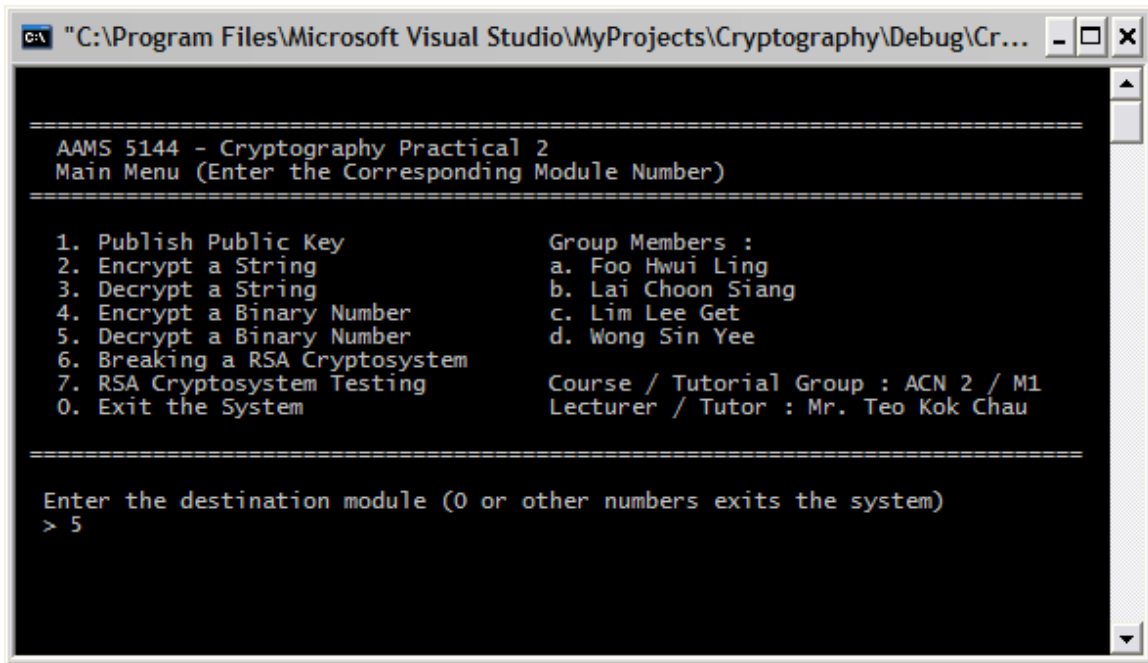


Figure 3.13 System Displaying Menu

```
C:\Program Files\Microsoft Visual Studio\MyProjects\Cryptography\Debug\Cr...  
=====  
Decrypting a Binary Number  
=====  
Status: Reading Decryption Parameters  
Enter a binary number of 15 bits long  
> 000011110101001  
Please input the private key A  
> 901  
Please input the public key N  
> 7171
```

Figure 3.14 Entering Decryption Details

```
C:\Program Files\Microsoft Visual Studio\MyProjects\Cryptography\Debug\Cr...  
=====  
Decrypting a Binary Number  
=====  
Status: Displaying Decryption Details  
System: Cipher text in decimal is 1961  
System: Plaintext in decimal is 42  
=====  
Press any key to continue . . .
```

Figure 3.15 Displaying Decryption Result

```
c:\ "C:\Program Files\Microsoft Visual Studio\MyProjects\Cryptography\Debug\Cr... - [ ] X
=====
AAMS 5144 - Cryptography Practical 2
Main Menu (Enter the Corresponding Module Number)
=====

1. Publish Public Key           Group Members :
2. Encrypt a String             a. Foo Hwui Ling
3. Decrypt a String             b. Lai Choon Siang
4. Encrypt a Binary Number      c. Lim Lee Get
5. Decrypt a Binary Number      d. Wong Sin Yee
6. Breaking a RSA Cryptosystem
7. RSA Cryptosystem Testing
0. Exit the System

Course / Tutorial Group : ACN 2 / M1
Lecturer / Tutor : Mr. Teo Kok Chau

=====

Enter the destination module (0 or other numbers exits the system)
> 4
```

Figure 3.16 System Displaying Menu

```
c:\ "C:\Program Files\Microsoft Visual Studio\MyProjects\Cryptography\Debug\Cr... - [ ] X
=====
Encrypting a Binary Number
=====

Status: Reading Encryption Parameters

Please input the Public Key b
> 101

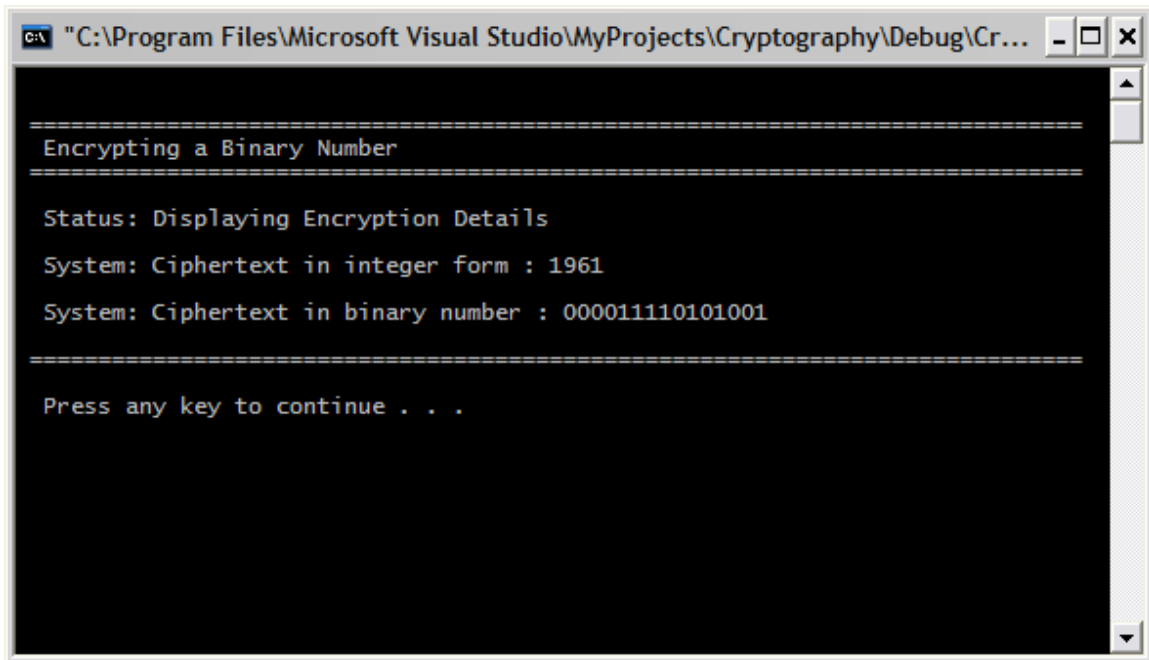
Please input the Public Key n
> 7171

Please input the plain text in number within the range [1, 32767]
> 40004

Error: Please enter a number in range [1, 32767]

Please input the plain text in number within the range [1, 32767]
> 42
```

Figure 3.17 Entering Encryption Data into the System



The image shows a Windows command prompt window with a title bar that reads "C:\Program Files\Microsoft Visual Studio\MyProjects\Cryptography\Debug\Cr...". The window contains the following text:

```
=====  
Encrypting a Binary Number  
=====  
Status: Displaying Encryption Details  
System: Ciphertext in integer form : 1961  
System: Ciphertext in binary number : 000011110101001  
=====  
Press any key to continue . . .
```

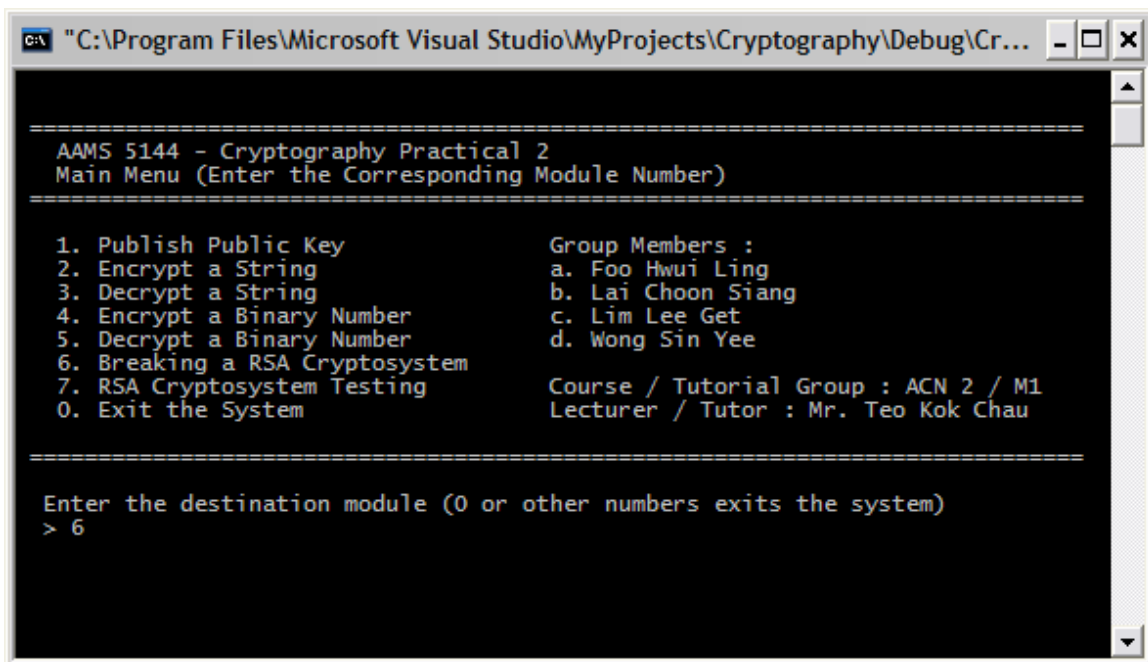
Figure 3.18 Displaying Encryption Result

4. Cryptanalysis.

To find the secret key of a RSA system, the following steps are performed:

1. Obtain n , the public key, then uses $p-1$ factoring algorithm to factorize n to get p and q .
2. Compute $\Phi(n)$.
3. Then compute a by using the formula: $a = b^{-1} \text{ mod } \Phi(n)$, where b is the public key.

The test data used is provided by the group led by Cheah Joo Xiang from ACN2 using key generated by their 7 bit system.



```
C:\Program Files\Microsoft Visual Studio\MyProjects\Cryptography\Debug\Cr... - [ ] X
=====
AAMS 5144 - Cryptography Practical 2
Main Menu (Enter the Corresponding Module Number)
=====

1. Publish Public Key          Group Members :
2. Encrypt a String           a. Foo Hwei Ling
3. Decrypt a String            b. Lai Choon Siang
4. Encrypt a Binary Number     c. Lim Lee Get
5. Decrypt a Binary Number     d. Wong Sin Yee
6. Breaking a RSA Cryptosystem
7. RSA Cryptosystem Testing    Course / Tutorial Group : ACN 2 / M1
0. Exit the System             Lecturer / Tutor : Mr. Teo Kok Chau
=====

Enter the destination module (0 or other numbers exits the system)
> 6
```

Figure 4.19 System Displaying the Main Menu

```
C:\Program Files\Microsoft Visual Studio\MyProjects\Cryptography\Debug\Cr...  
=====   
Breaking Cryptosystem  
=====   
Status: Reading Public Key Details  
Please enter the Public Key n  
> 10541  
Please insert the public key b  
> 125
```

Figure 4.20 Entering Cryptosystem Parameters

```
C:\Program Files\Microsoft Visual Studio\MyProjects\Cryptography\Debug\Cr...  
=====   
Breaking Cryptosystem  
=====   
Status: Printing Summary  
System: The Public Key n = 10541 is a product of p = 127 and q = 83  
System: The Phi-n is 10332  
System: The Public Key b is 125  
System: The private key a is 2645  
=====   
Press any key to continue . . . _
```

Figure 4.21 System Displaying Cryptosystem Details

```
C:\ "C:\Program Files\Microsoft Visual Studio\MyProjects\Cryptography\Debug\Cr... - [ ] X
=====
AAMS 5144 - Cryptography Practical 2
Main Menu (Enter the Corresponding Module Number)
=====

1. Publish Public Key          Group Members :
2. Encrypt a String           a. Foo Hwui Ling
3. Decrypt a String           b. Lai Choon Siang
4. Encrypt a Binary Number    c. Lim Lee Get
5. Decrypt a Binary Number    d. Wong Sin Yee
6. Breaking a RSA Cryptosystem
7. RSA Cryptosystem Testing   Course / Tutorial Group : ACN 2 / M1
0. Exit the System           Lecturer / Tutor : Mr. Teo Kok Chau
=====

Enter the destination module (0 or other numbers exits the system)
> 3_
```

Figure 4.22 System Showing Menu

```
C:\ "C:\Program Files\Microsoft Visual Studio\MyProjects\Cryptography\Debug\Cr... - [ ] X
=====
Decrypt a String
=====

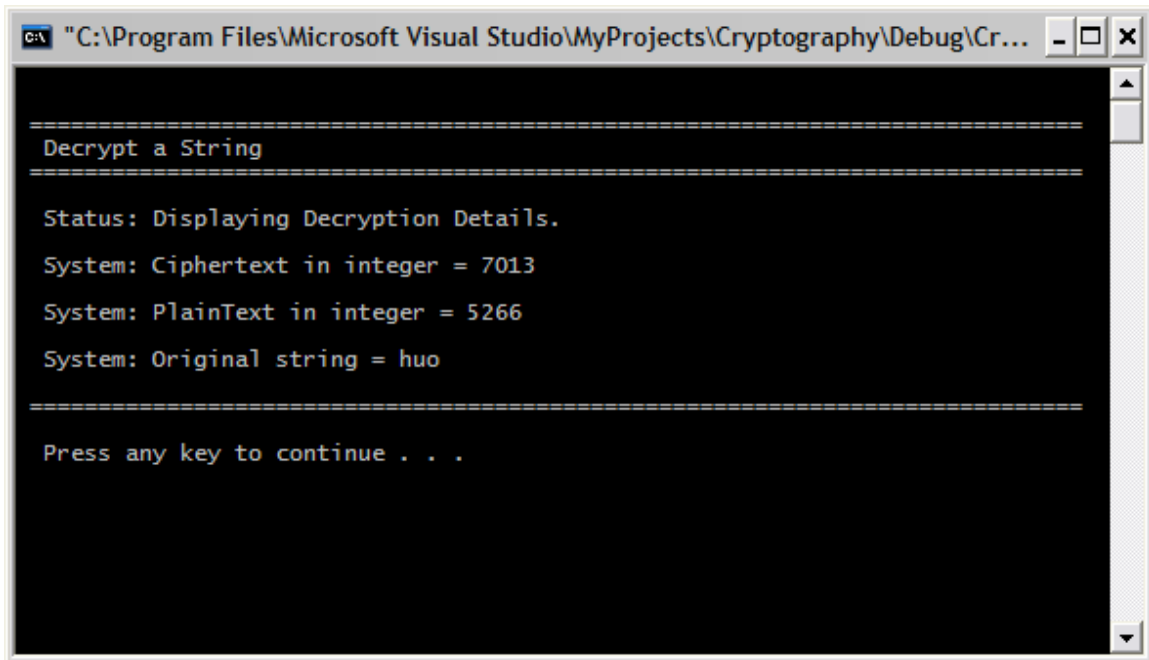
Status: Reading Decryption Parameters.

Enter the Private Key a
> 2645

Enter the Public Key n
> 10541

Enter a string with 3 characters
> kjt
```

Figure 4.23 Entering Decryption Details



The image shows a Windows command prompt window with a title bar that reads "C:\Program Files\Microsoft Visual Studio\MyProjects\Cryptography\Debug\Cr...". The window contains the following text:

```
=====  
Decrypt a String  
=====  
Status: Displaying Decryption Details.  
System: Ciphertext in integer = 7013  
System: PlainText in integer = 5266  
System: Original string = huo  
=====  
Press any key to continue . . .
```

Figure 4.24 System Displaying Decryption Result