TRƯỜNG ĐẠI HỌC BÁCH KHOA TP.HỒ CHÍ MINH
KHOA KHOA HỌC VÀ KỸ THUẬT MÁY TÍNH

LAB 2

MÔN: *MẬT MÃ VÀ AN NINH MẠNG*

RSA

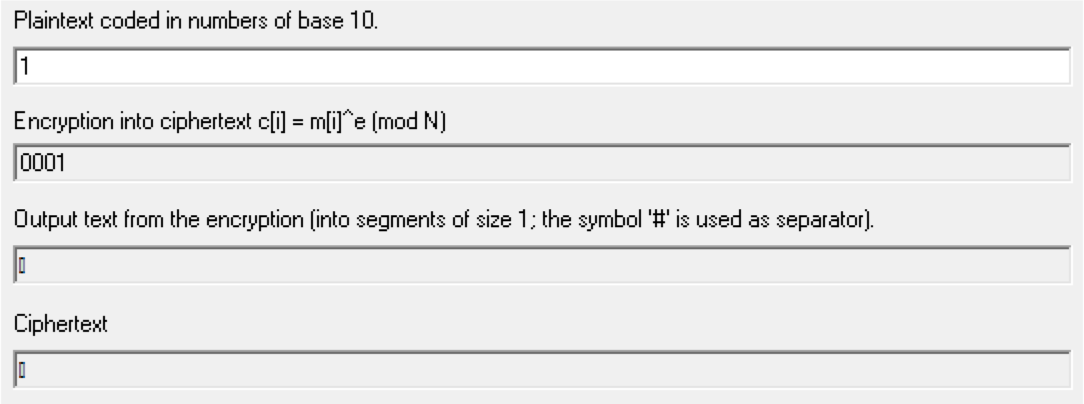
Sinh Viên Thực Hiện :	**TRẦN VĂN LẮM**
MSSV:	**51201830**
Nhóm:	**A03-**
Giáo Viên Hướng Dẫn:	**NGUYỄN NHẬT NAM**

TP.HỒ CHÍ MINH, tháng 9 năm 2015

Part 1. **RSA DEMONSTRATION**

16bits

Plaintext: 1



Plaintext coded in numbers of base 10.

1

Encryption into ciphertext c[i] = m[i]^e (mod N)

0001

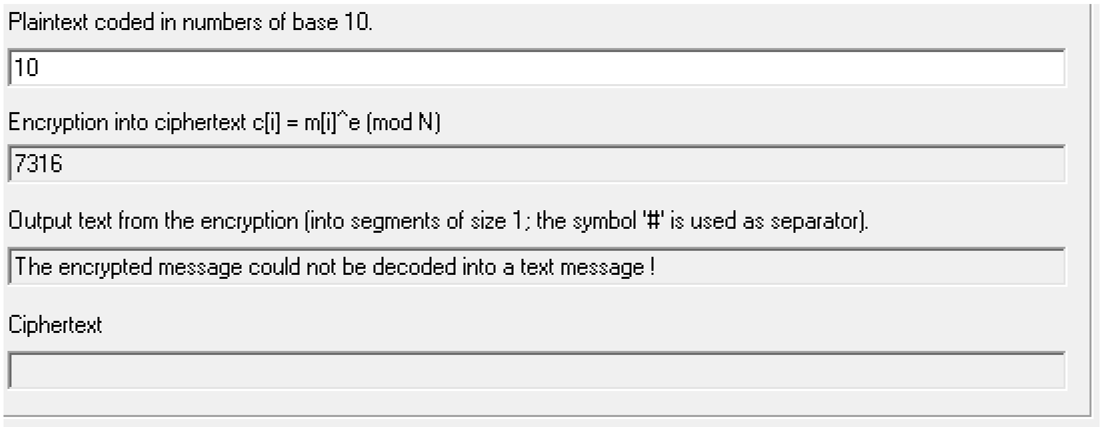
Output text from the encryption (into segments of size 1; the symbol '#' is used as separator).

▯

Ciphertext

▯

Plaintext: 10



Plaintext coded in numbers of base 10.

10

Encryption into ciphertext c[i] = m[i]^e (mod N)

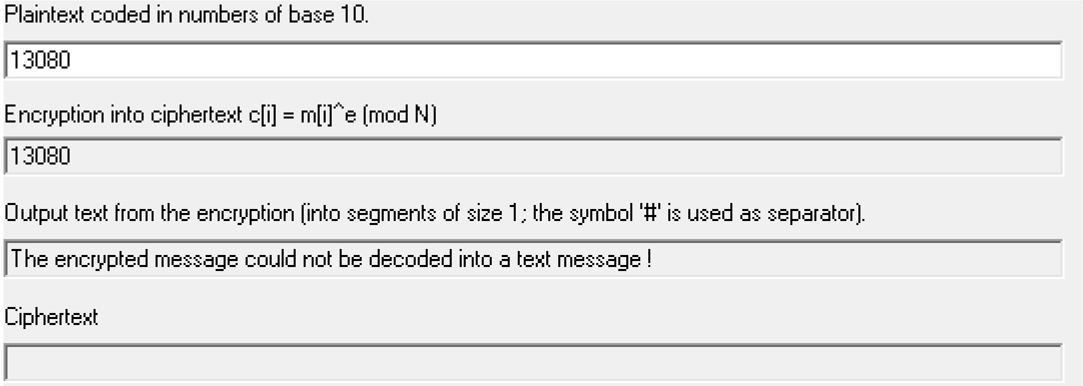
7316

Output text from the encryption (into segments of size 1; the symbol '#' is used as separator).

The encrypted message could not be decoded into a text message !

Ciphertext

Plaintext: N-1



Plaintext coded in numbers of base 10.

13080

Encryption into ciphertext c[i] = m[i]^e (mod N)

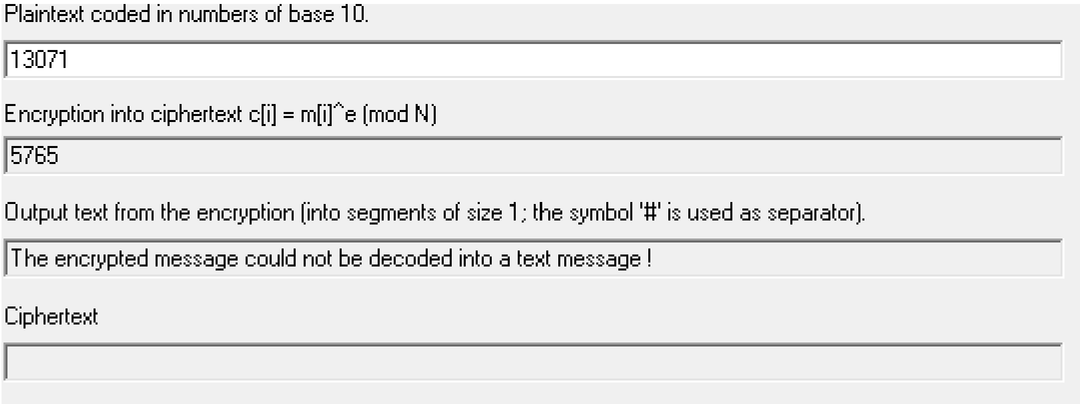
13080

Output text from the encryption (into segments of size 1; the symbol '#' is used as separator).

The encrypted message could not be decoded into a text message !

Ciphertext

Plaintext N-10:



Plaintext coded in numbers of base 10.

13071

Encryption into ciphertext c[i] = m[i]^e (mod N)

5765

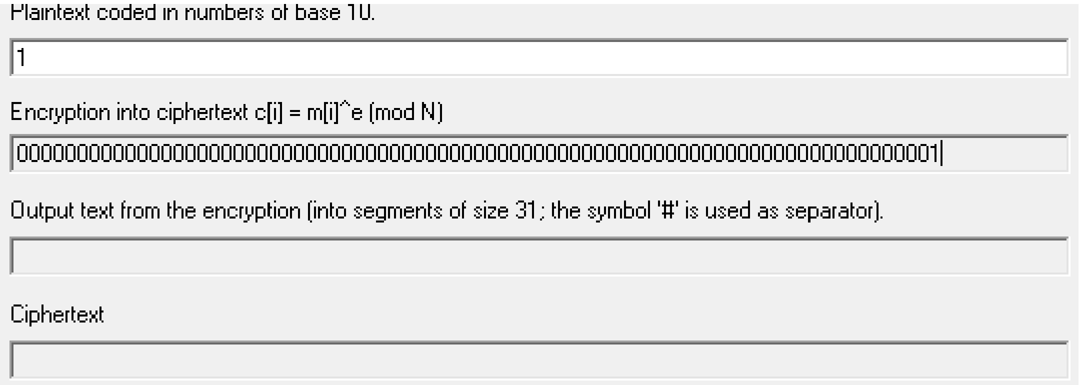
Output text from the encryption (into segments of size 1; the symbol '#' is used as separator).

The encrypted message could not be decoded into a text message !

Ciphertext

256bits

Plaintext : 1



Plaintext coded in numbers of base 10.

1

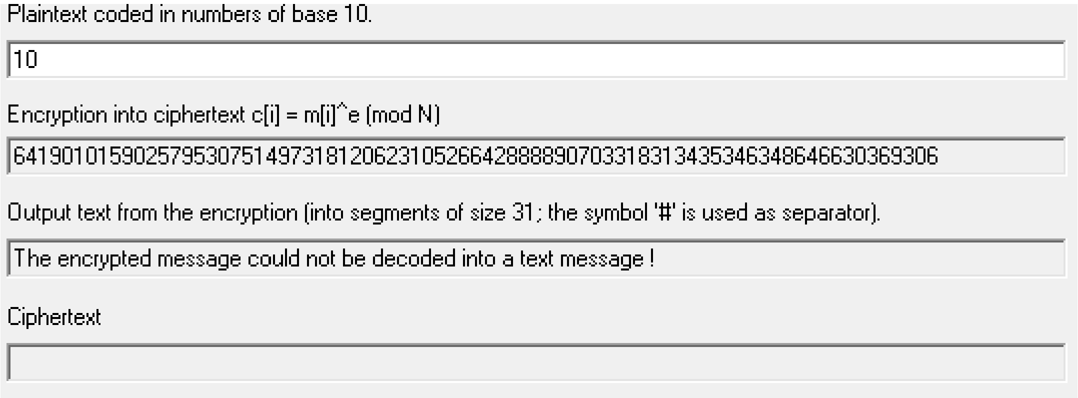
Encryption into ciphertext c[i] = m[i]^e (mod N)

00000000000000000000000000000000000000000000000000000000000000000000000000001

Output text from the encryption (into segments of size 31; the symbol '#' is used as separator).

Ciphertext

Plaintext : 10



Plaintext coded in numbers of base 10.

10

Encryption into ciphertext c[i] = m[i]^e (mod N)

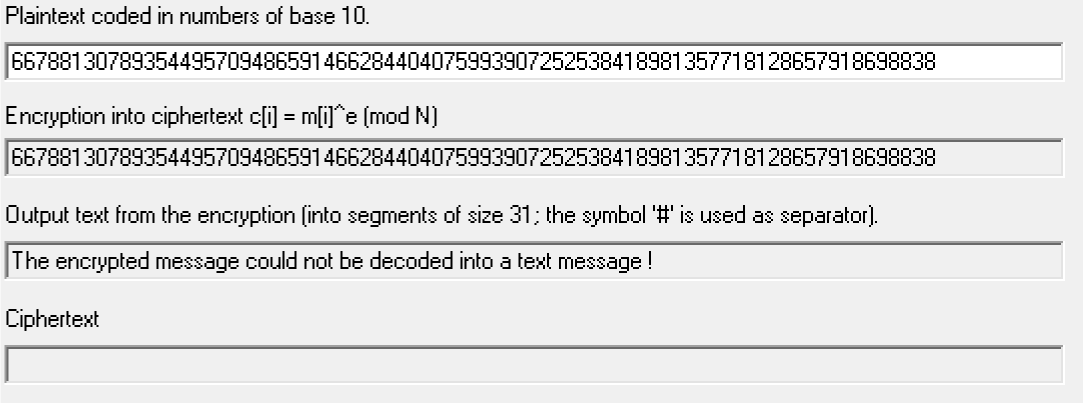
64190101590257953075149731812062310526642888890703318313435346348646630369306

Output text from the encryption (into segments of size 31; the symbol '#' is used as separator).

The encrypted message could not be decoded into a text message !

Ciphertext

Plaintext: N-1



Plaintext coded in numbers of base 10.

```
66788130789354495709486591466284404075993907252538418981357718128657918698838
```

Encryption into ciphertext c[i] = m[i]^e (mod N)

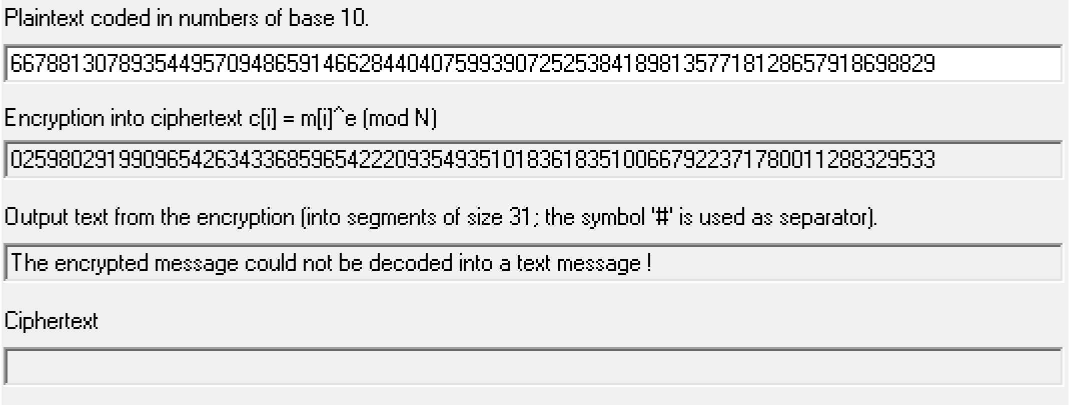
```
66788130789354495709486591466284404075993907252538418981357718128657918698838
```

Output text from the encryption (into segments of size 31; the symbol '#' is used as separator).

```
The encrypted message could not be decoded into a text message !
```

Ciphertext

Plaintext: N-10



Plaintext coded in numbers of base 10.

```
66788130789354495709486591466284404075993907252538418981357718128657918698829
```

Encryption into ciphertext c[i] = m[i]^e (mod N)

```
02598029199096542634336859654222093549351018361835100667922371780011288329533
```

Output text from the encryption (into segments of size 31; the symbol '#' is used as separator).

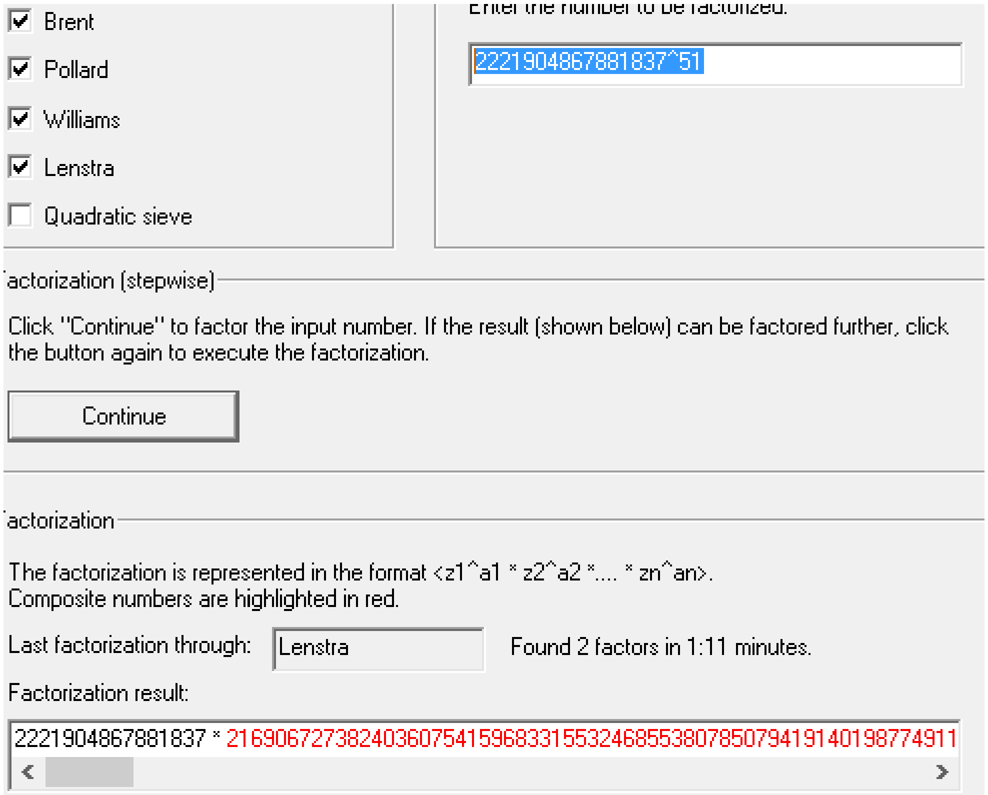
```
The encrypted message could not be decoded into a text message !
```

Ciphertext

`Tương tự với 2048bits: ta thấy khi encrytion N-1 thì ciphertext giống với plaintext`

`Part 2:` **FACTORING**

One minute : 2221904867881837^51



☑ Brent

☑ Pollard

☑ Williams

☑ Lenstra

□ Quadratic sieve

Enter the number to be factorized:

2221904867881837^51

actorization (stepwise)

Click "Continue" to factor the input number. If the result (shown below) can be factored further, click the button again to execute the factorization.

actorization

The factorization is represented in the format <z1^a1 * z2^a2 *.... * zn^an>.
Composite numbers are highlighted in red.

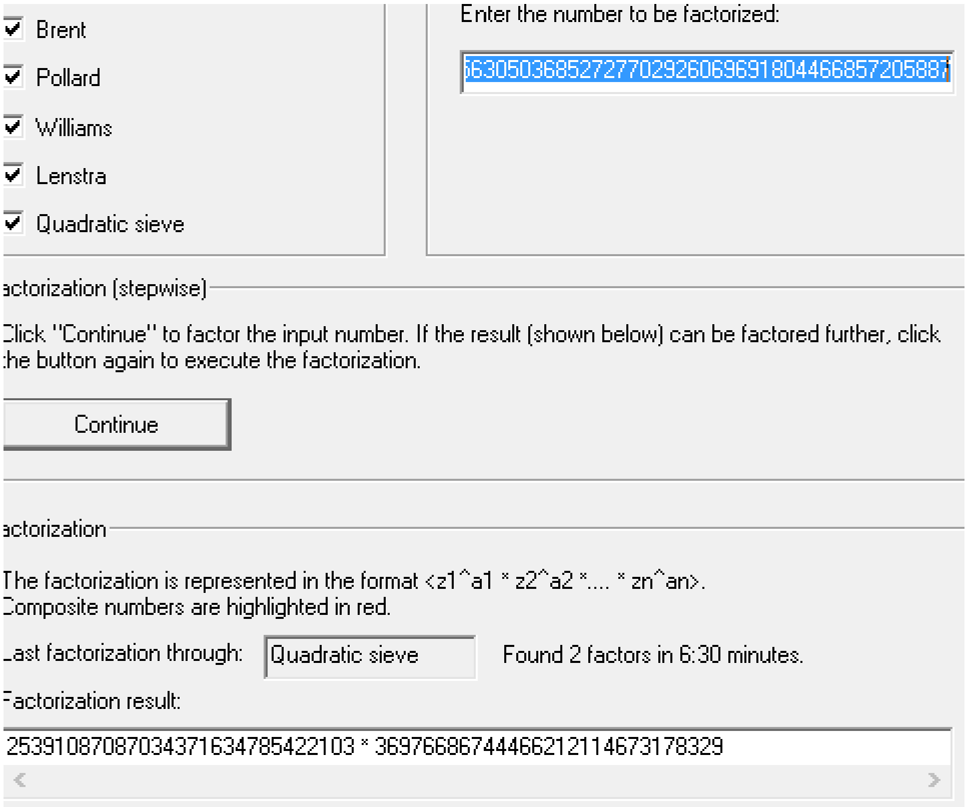
Last factorization through: Lenstra

Found 2 factors in 1:11 minutes.

Factorization result:

2221904867881837 * 21690672738240360754159683315532468553807850794191401987749 11

Five minutes: N: 93887827331873105630503685272770292606969180446685720588 7



☑ Brent

☑ Pollard

☑ Williams

☑ Lenstra

☑ Quadratic sieve

Enter the number to be factorized:

563050368527277029260696918044668572058 87

actorization (stepwise)

Click "Continue" to factor the input number. If the result (shown below) can be factored further, click the button again to execute the factorization.

actorization

The factorization is represented in the format <z1^a1 * z2^a2 *.... * zn^an>.
Composite numbers are highlighted in red.

Last factorization through: Quadratic sieve

Found 2 factors in 6:30 minutes.

Factorization result:

25391087087034371634785422103 * 369766867444662121146731783 29