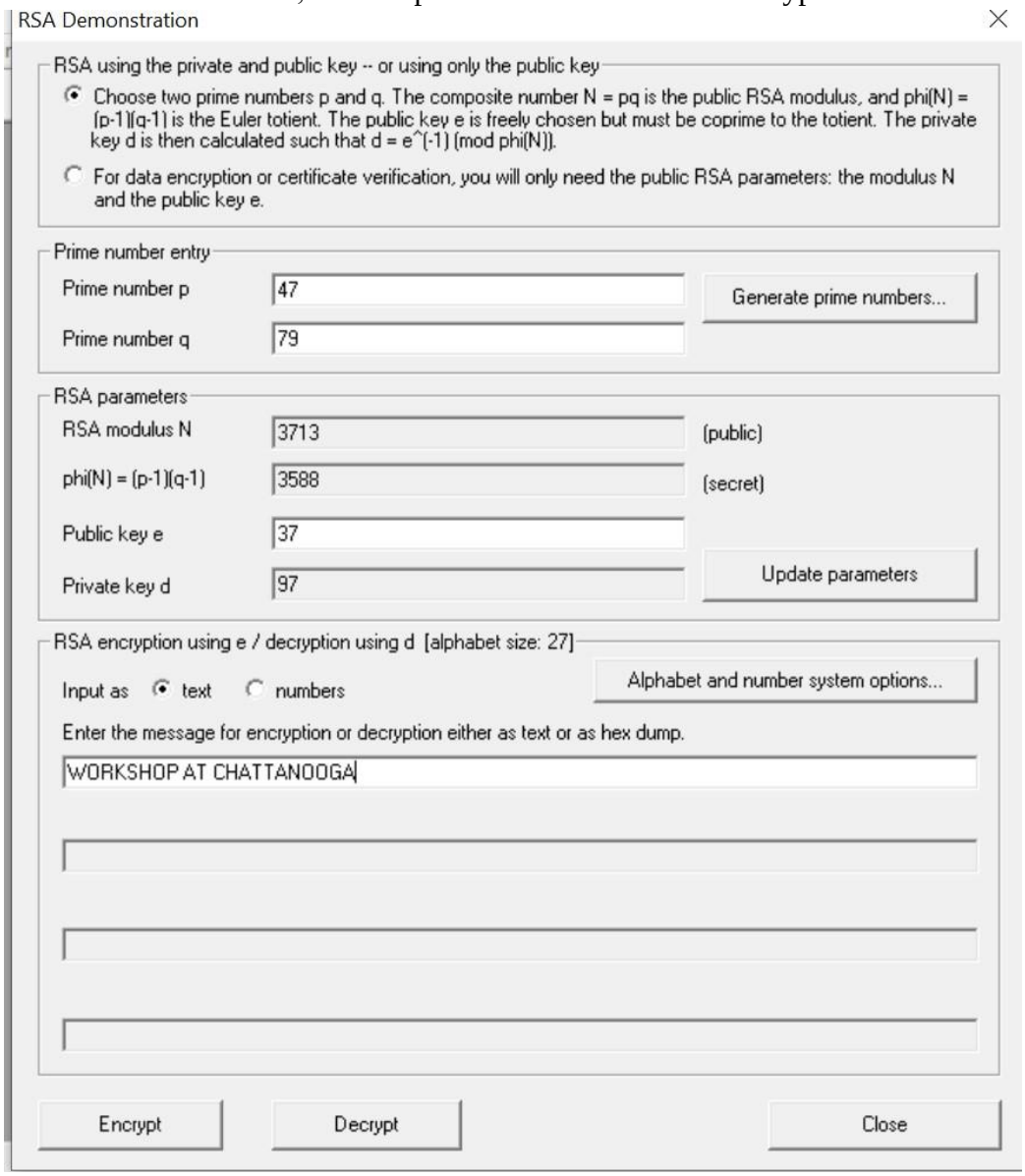
Farzad Kheirabadi
CYB 555
UNIT 3

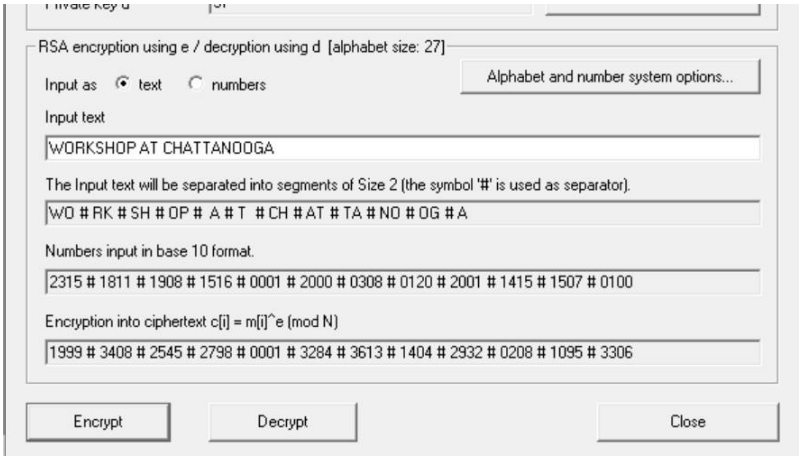
Lab-Cryptography RSA:

Encryption or decryption of messages using the RSA key pair.

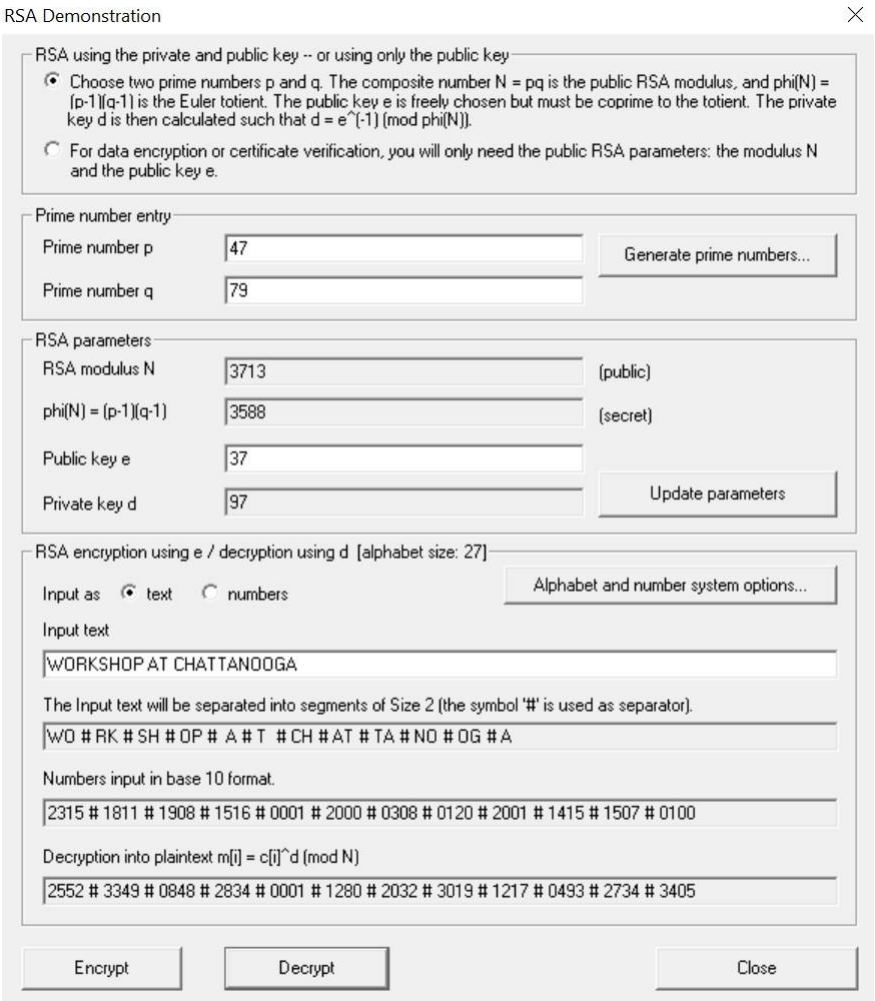
1. Select Individual Procedures/RSA Cryptosystem/RSA Demonstration
2. Enter the RSA key p=47, q=79, e=37. The parameters N = p*q=3713 and phi(N)=3588 and d=97 are calculated.
3. Click “Alphabet and number system” options
4. Choose specify alphabet under Alphabet Options and number system under Method for coding of text into number. Enter 2 in Block length in characters.
5. To confirm your entries, click on OK. You can now enter the input text, “WORKSHOP ATCHATTANOOGA”, in the input line and click on the Encrypt button.



Farzad Kheirabadi
CYB 555
UNIT 3



6. To decrypt, copy text in Encryption into ciphertext 1999 # 3408 # 2545 # 2798 # 0001 # 3284 # 3613 # 1404 # 2932 # 0208 # 1095 # 3306 to input text area. And click the Decrypt button.



Farzad Kheirabadi
CYB 555
UNIT 3

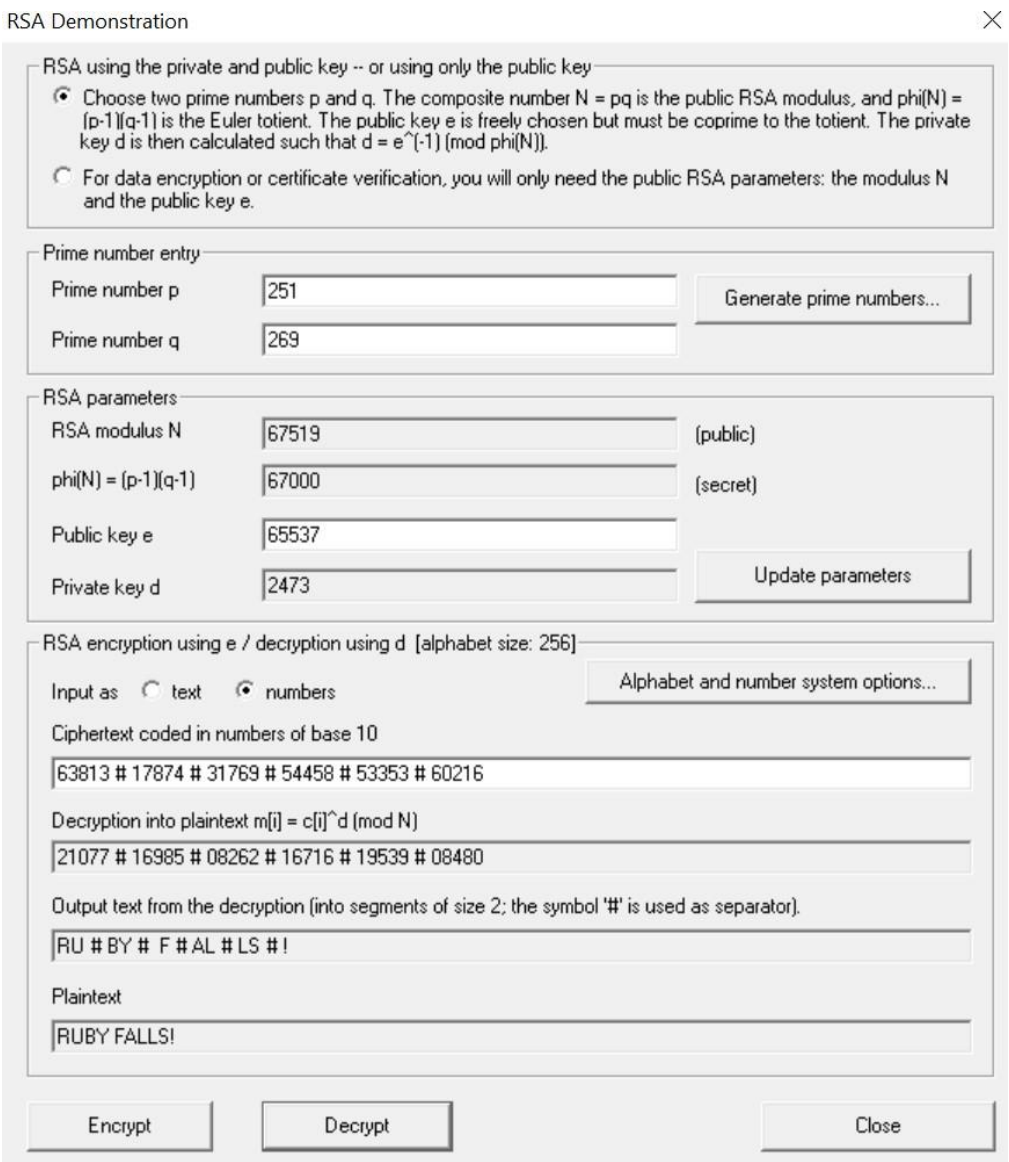
Encryption of the message with block length 1 v.s. encryption of the message with block length 2.

1. Create the RSA key p=251, q=269, e=65537. The value of N is 67519 the value of phi(N) is 67000, the value of private key d is 2473

2. Click Alphabet and number system options Choose All 256 ASCII characters under Alphabet options, b-adic under Method for coding and a block into numbers and 1 inBlock length in characters.

3. To confirm your entries, click on OK. You can now enter the input text, "RUBYFALLS!", in the input line and click on the Encrypt button.

The encrypted version of this is the number sequence is 63813 # 17874 # 31769 #



54458 # 53353 # 60216. If you insert these numbers into the input line and then choose Decrypt, the original plaintext will be restored.

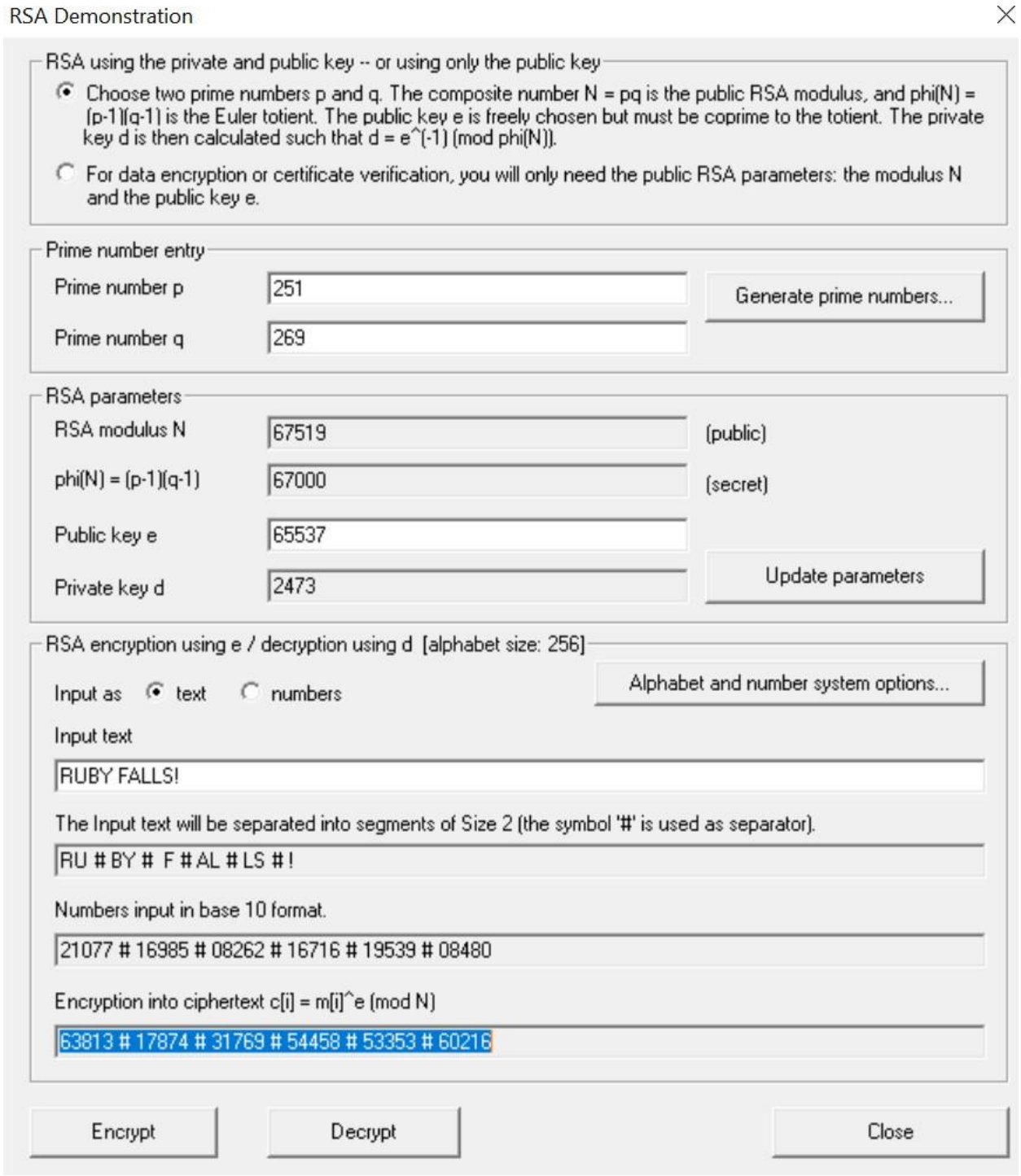
Farzad Kheirabadi
CYB 555
UNIT 3

4. Click “Alphabet and number system” options

Choose All 256 ASCII characters under Alphabet options, b-adic under Method for coding and a block into numbers and 2 in Block length in characters.

5. To confirm your entries, click on OK.

6. You will receive a cipher text that is only half as long: 63813 # 17874 # 31769 # 54458 # 53353 # 60216.



Farzad Kheirabadi
CYB 555
UNIT 3

Attack on RSA encryption with short RSA modulus

The analysis is performed in two stages: first of all the prime factorization of the RSA modulus is calculated using factorization, and then in the second stage the secret key for encryption of the message is determined. After this, the cipher text can be decrypted with the cracked secret key.

We will figure out plaintext given
RSA modulus n = 639784868795271438588314150 41
Public exponent e = 17579
Cipher text = 45411667895024938209259253423,
165970916214320200763115522 01,
46468979279750354732637631044, 32870167545903741339819671379

1. Factorization of the RSA modulus with the aid of prime factorization.
To break down the natural number, select menu sequence Indiv. Procedure/RSACryptosystem / Factorization of a Number.

2. The two components of the public key is
RSA modulus n = 639784868795271438588314150 41
Public exponent e = 17579
Enter n=639784868795271438588314150 41 as input and click Continue.

It is interesting to see which procedure broke down the RSA modulus the fastest.

Calculate the secret key d from the prime factorization of n and the public key e:
With the knowledge of the
prime factors p = 145295143558111 and q =
440334654777631and the
public key e = 17579, we are in a position to decrypt the ciphertext.

3. Open the next dialog box via menu selection Indiv. Procedure/RSA Cryptosystem/RSADemonstration:
4. Enter p = 145295143558111 and q = 440334654777631 and the public key e = 17579.

5. Click on Alphabet and number system options and make the following settings:Alphabet options: Specify alphabet

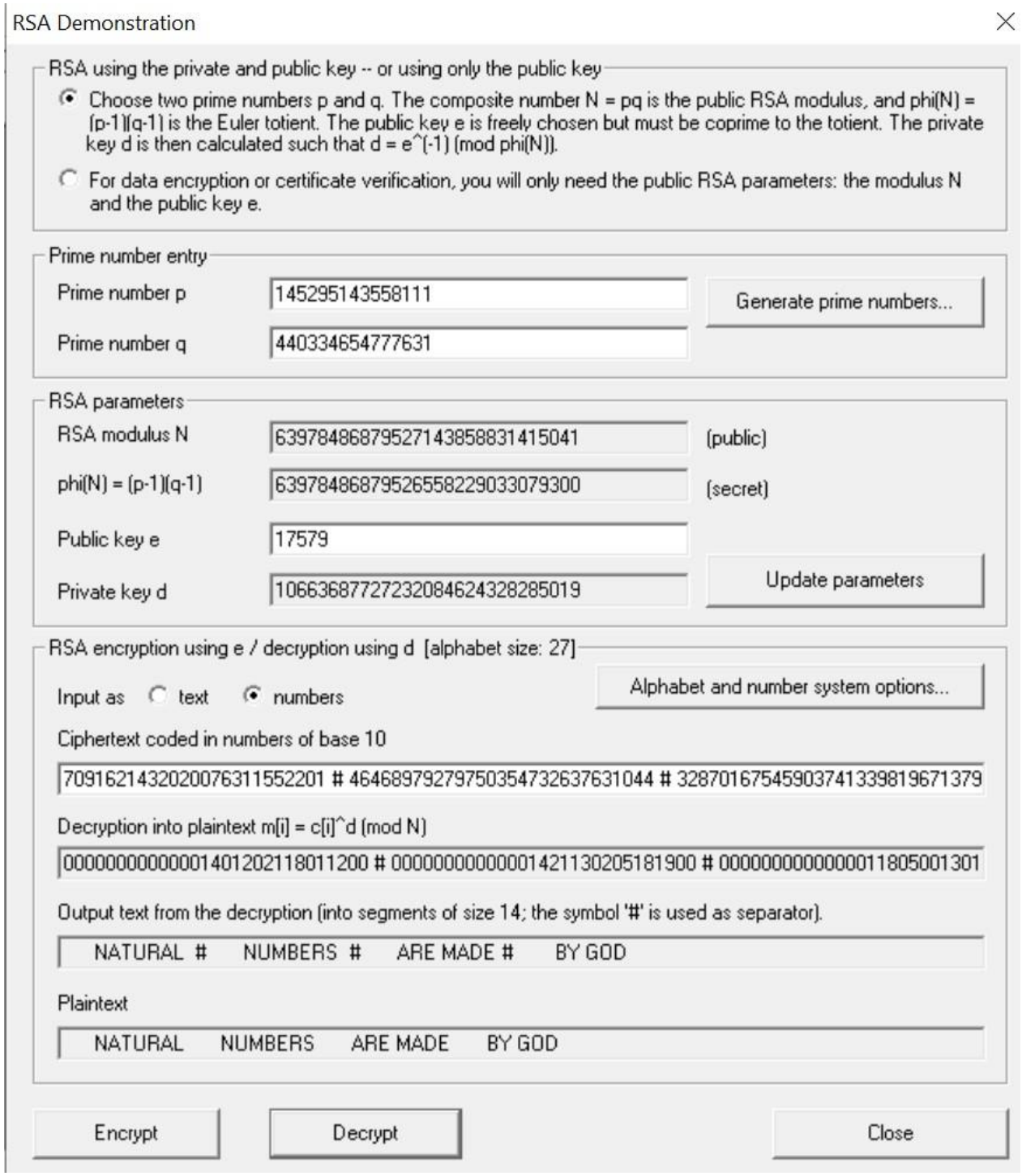
RSA variant: Normal

Method for coding a block into number: Number systemBlock length: 14

Number system: Decimal

6. Enter the following cipher text in the input text field. And click the Decrypt button.45411667895024938209259253423,
16597091621432020076311552201,
46468979279750354732637631044,
32870167545903741339819671379

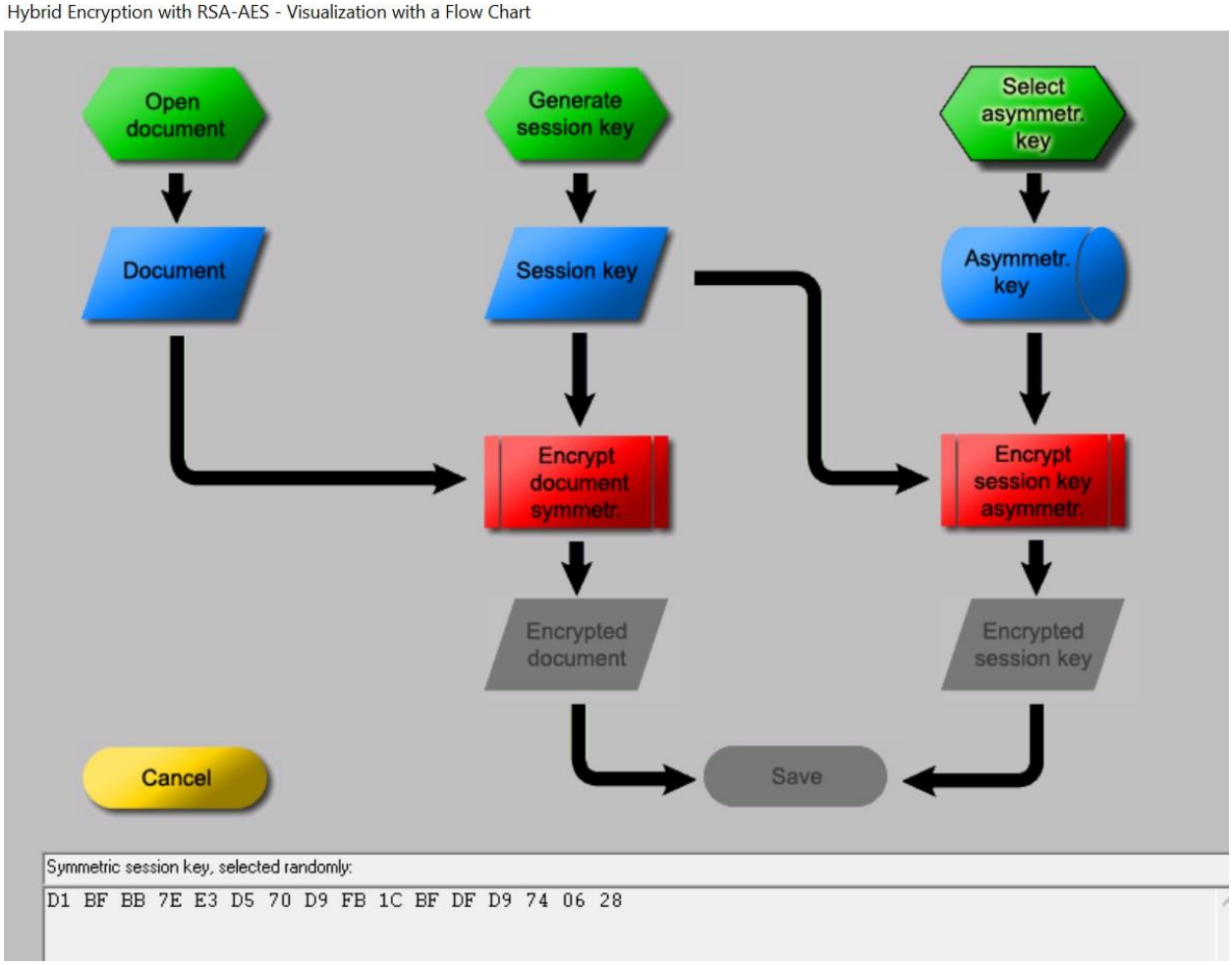
Farzad Kheirabadi
CYB 555
UNIT 3



Check your results: “NATURAL NUMBERS ARE MADE BY GOD”
Side Channel Attack to RSA:

1. Select from menu: “Analysis” \“Asymmetric Encryption” \“Side-Channel Attack onTextbook RSA”

2. Click “Introduction to the scenario”.
3. Click “Perform preparation” and click “OK”
4. Click “OK” again.
5. Click “Generate session key” and “Session Key”. The generated session key is “D1 BF BB 7E E3 D5 70 D9 FB 1C BF DF D9 74 06 28 ”.



6. Click “Select assymmetr. key".
7. Select Bob’s key and click “OK”.
8. Click “Encrypt document symmetry.”, “Encrypt session key asymmetry.” and “Save”.
9. Click “Transmit message” and “Decrypt message”.
10. Enter 1234 and click “OK”.
11. Click “Intercept message” and “Start attack cycle”.
12. Click the “All steps at once” button.
13. Click “OK” and icon of Trudy (Attacker).

Farzad Kheirabadi
CYB 555
UNIT 3

The session key is D1BFBB7EE3D570D9FB1CBFDFD9740628 which matches the onegenerated in Step 5.

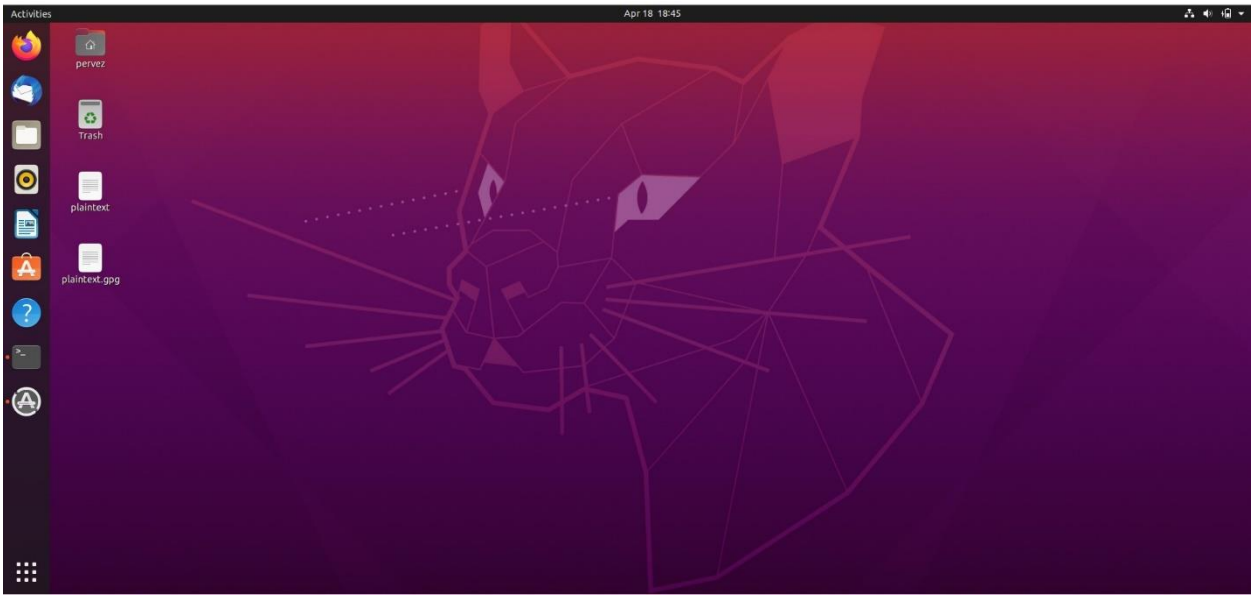
LAB-CRYPTOGRAPHY GPG:

Encrypt a text string and decrypt using symmetric encryption and gpg. You will need to install a linux VM. Submit screenshots.

Farzad Kheirabadi
CYB 555
UNIT 3

1. Create a .txt file(plaintext.txt) with string in it.
2. Now open terminal and enter the this command gpg -h
3. Now encrypt the .txt file using the following command. gpg -c (symmetric encryption command)

A new file will be created with the .gpg extension.



4. The text file(plaintext.txt) is encrypted.

Farzad Kheirabadi
CYB 555
UNIT 3