

### Lab-Cryptography RSA:

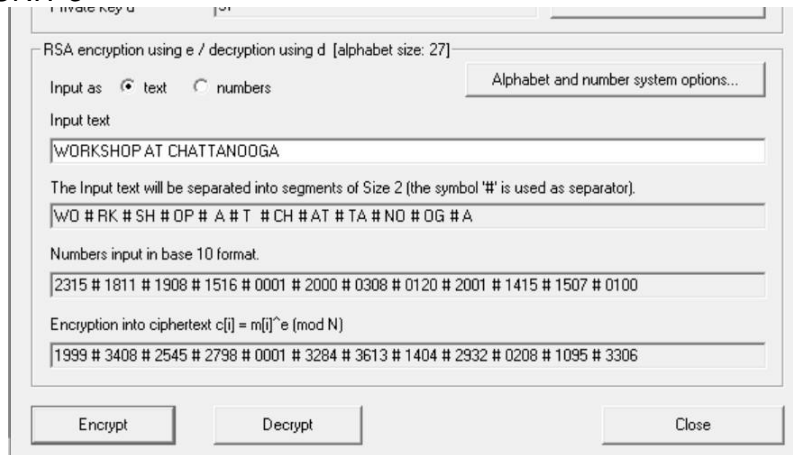
Encryption or decryption of messages using the RSA key pair.

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.

The screenshot shows the 'RSA Demonstration' window. It has a title bar with a close button. The window is divided into several sections:

- Top Section:** A radio button group for 'RSA using the private and public key -- or using only the public key'. The first option, 'Choose two prime numbers p and q...', is selected. It includes a descriptive text about the RSA process.
- Prime number entry:** Two input fields for 'Prime number p' (containing 47) and 'Prime number q' (containing 79). A 'Generate prime numbers...' button is to the right.
- RSA parameters:** Four input fields: 'RSA modulus N' (3713, labeled 'public'), ' $\phi(N) = (p-1)(q-1)$ ' (3588, labeled 'secret'), 'Public key e' (37), and 'Private key d' (97). An 'Update parameters' button is to the right.
- Bottom Section:** A radio button group for 'RSA encryption using e / decryption using d' with 'text' selected. A button 'Alphabet and number system options...' is next to it. Below is a text area with the input 'WORKSHOP AT CHATTANOOGA' and three empty lines for output. At the bottom are three buttons: 'Encrypt', 'Decrypt', and 'Close'.

Farzad Kheirabadi  
CYB 555  
UNIT 3



RSA encryption using e / decryption using d [alphabet size: 27]

Input as ☒ text ☐ numbers Alphabet and number system options...

Input text

WORKSHOP AT CHATTANOOGA

The Input text will be separated into segments of Size 2 (the symbol '#' is used as separator).

WO # RK # SH # OP # A # T # CH # AT # TA # NO # OG # A

Numbers input in base 10 format.

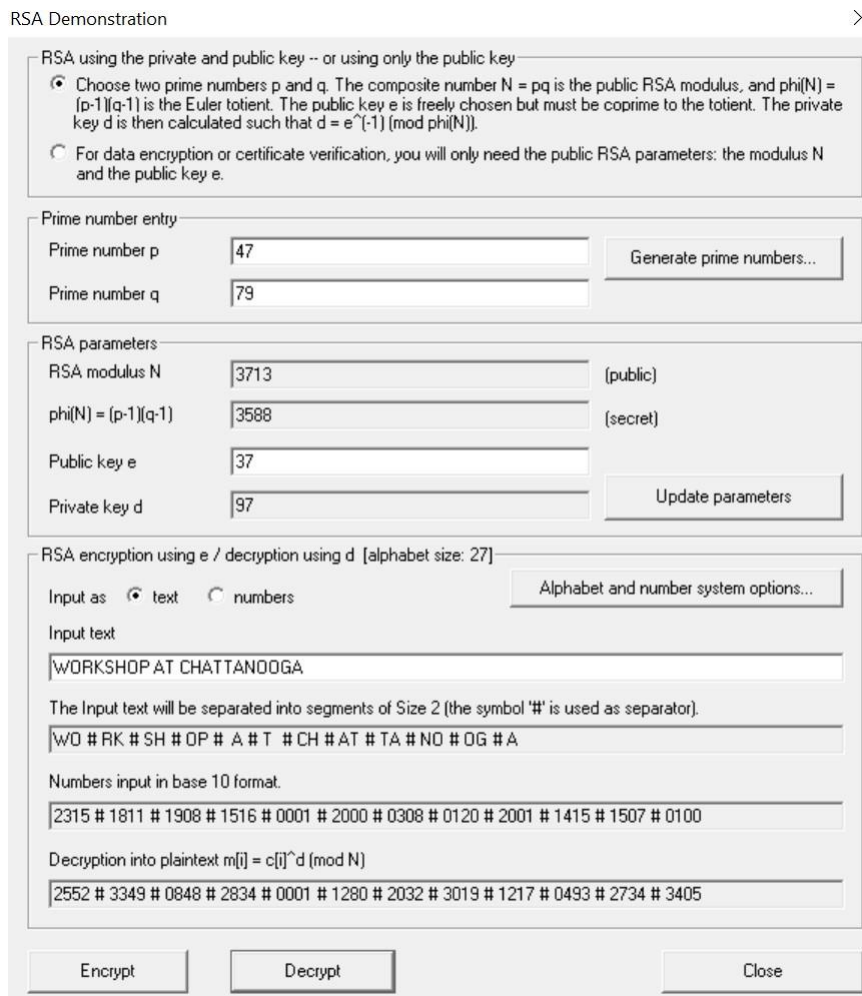
2315 # 1811 # 1908 # 1516 # 0001 # 2000 # 0308 # 0120 # 2001 # 1415 # 1507 # 0100

Encryption into ciphertext  $c[i] = m[i]^e \pmod{N}$

1999 # 3408 # 2545 # 2798 # 0001 # 3284 # 3613 # 1404 # 2932 # 0208 # 1095 # 3306

Encrypt Decrypt Close

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.



RSA Demonstration

RSA using the private and public key -- or using only the public key

- ☒ Choose two prime numbers p and q. The composite number  $N = pq$  is the public RSA modulus, and  $\phi(N) = (p-1)(q-1)$  is the Euler totient. The public key e is freely chosen but must be coprime to the totient. The private key d is then calculated such that  $d = e^{-1} \pmod{\phi(N)}$ .
- ☐ For data encryption or certificate verification, you will only need the public RSA parameters: the modulus N and the public key e.

Prime number entry

Prime number p 47 Generate prime numbers...

Prime number q 79

RSA parameters

RSA modulus N 3713 (public)

$\phi(N) = (p-1)(q-1)$  3588 (secret)

Public key e 37

Private key d 97 Update parameters

RSA encryption using e / decryption using d [alphabet size: 27]

Input as ☒ text ☐ numbers Alphabet and number system options...

Input text

WORKSHOP AT CHATTANOOGA

The Input text will be separated into segments of Size 2 (the symbol '#' is used as separator).

WO # RK # SH # OP # A # T # CH # AT # TA # NO # OG # A

Numbers input in base 10 format.

2315 # 1811 # 1908 # 1516 # 0001 # 2000 # 0308 # 0120 # 2001 # 1415 # 1507 # 0100

Decryption into plaintext  $m[i] = c[i]^d \pmod{N}$

2552 # 3349 # 0848 # 2834 # 0001 # 1280 # 2032 # 3019 # 1217 # 0493 # 2734 # 3405

Encrypt Decrypt Close

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 in Block 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 #

RSA Demonstration ✕

RSA using the private and public key -- or using only the public key

☒ Choose two prime numbers  $p$  and  $q$ . The composite number  $N = pq$  is the public RSA modulus, and  $\phi(N) = (p-1)(q-1)$  is the Euler totient. The public key  $e$  is freely chosen but must be coprime to the totient. The private key  $d$  is then calculated such that  $d = e^{-1} \pmod{\phi(N)}$ .

☐ For data encryption or certificate verification, you will only need the public RSA parameters: the modulus  $N$  and the public key  $e$ .

Prime number entry

Prime number  $p$

Prime number  $q$

RSA parameters

RSA modulus  $N$   (public)

$\phi(N) = (p-1)(q-1)$   (secret)

Public key  $e$

Private key  $d$

RSA encryption using  $e$  / decryption using  $d$  [alphabet size: 256]

Input as ☐ text ☒ numbers 

Ciphertext coded in numbers of base 10

Decryption into plaintext  $m[i] = c[i]^d \pmod{N}$

Output text from the decryption (into segments of size 2; the symbol '#' is used as separator).

Plaintext

Farzad Kheirabadi

CYB 555

UNIT 3

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

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.

RSA Demonstration ×

☒ RSA using the private and public key -- or using only the public key

☒ Choose two prime numbers  $p$  and  $q$ . The composite number  $N = pq$  is the public RSA modulus, and  $\phi(N) = (p-1)(q-1)$  is the Euler totient. The public key  $e$  is freely chosen but must be coprime to the totient. The private key  $d$  is then calculated such that  $d = e^{-1} \pmod{\phi(N)}$ .

☐ For data encryption or certificate verification, you will only need the public RSA parameters: the modulus  $N$  and the public key  $e$ .

Prime number entry

Prime number  $p$

Prime number  $q$

RSA parameters

RSA modulus  $N$   (public)

$\phi(N) = (p-1)(q-1)$   (secret)

Public key  $e$

Private key  $d$

RSA encryption using  $e$  / decryption using  $d$  [alphabet size: 256]

Input as ☒ text ☐ numbers 

Input text

The Input text will be separated into segments of Size 2 (the symbol '#' is used as separator).

Numbers input in base 10 format.

Encryption into ciphertext  $c[i] = m[i]^e \pmod{N}$

### 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  $n = 63978486879527143858831415041$

Public exponent  $e = 17579$

Cipher text = 45411667895024938209259253423,

16597091621432020076311552201,

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/RSA Cryptosystem / Factorization of a Number.

2. The two components of the public key is

RSA modulus  $n = 63978486879527143858831415041$

Public exponent  $e = 17579$

Enter  $n=63978486879527143858831415041$  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  $q =$

$440334654777631$  and 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

Farzad Kheirabadi

CYB 555

UNIT 3

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

RSA using the private and public key -- or using only the public key

☒ Choose two prime numbers  $p$  and  $q$ . The composite number  $N = pq$  is the public RSA modulus, and  $\phi(N) = (p-1)(q-1)$  is the Euler totient. The public key  $e$  is freely chosen but must be coprime to the totient. The private key  $d$  is then calculated such that  $d = e^{-1} \pmod{\phi(N)}$ .

☐ For data encryption or certificate verification, you will only need the public RSA parameters: the modulus  $N$  and the public key  $e$ .

Prime number entry

Prime number  $p$

Prime number  $q$

RSA parameters

RSA modulus  $N$   (public)

$\phi(N) = (p-1)(q-1)$   (secret)

Public key  $e$

Private key  $d$

RSA encryption using  $e$  / decryption using  $d$  [alphabet size: 27]

Input as ☐ text ☒ numbers 

Ciphertext coded in numbers of base 10

Decryption into plaintext  $m[i] = c[i]^d \pmod{N}$

Output text from the decryption (into segments of size 14; the symbol '#' is used as separator).

Plaintext

Check your results: "NATURAL NUMBERS ARE MADE BY GOD"

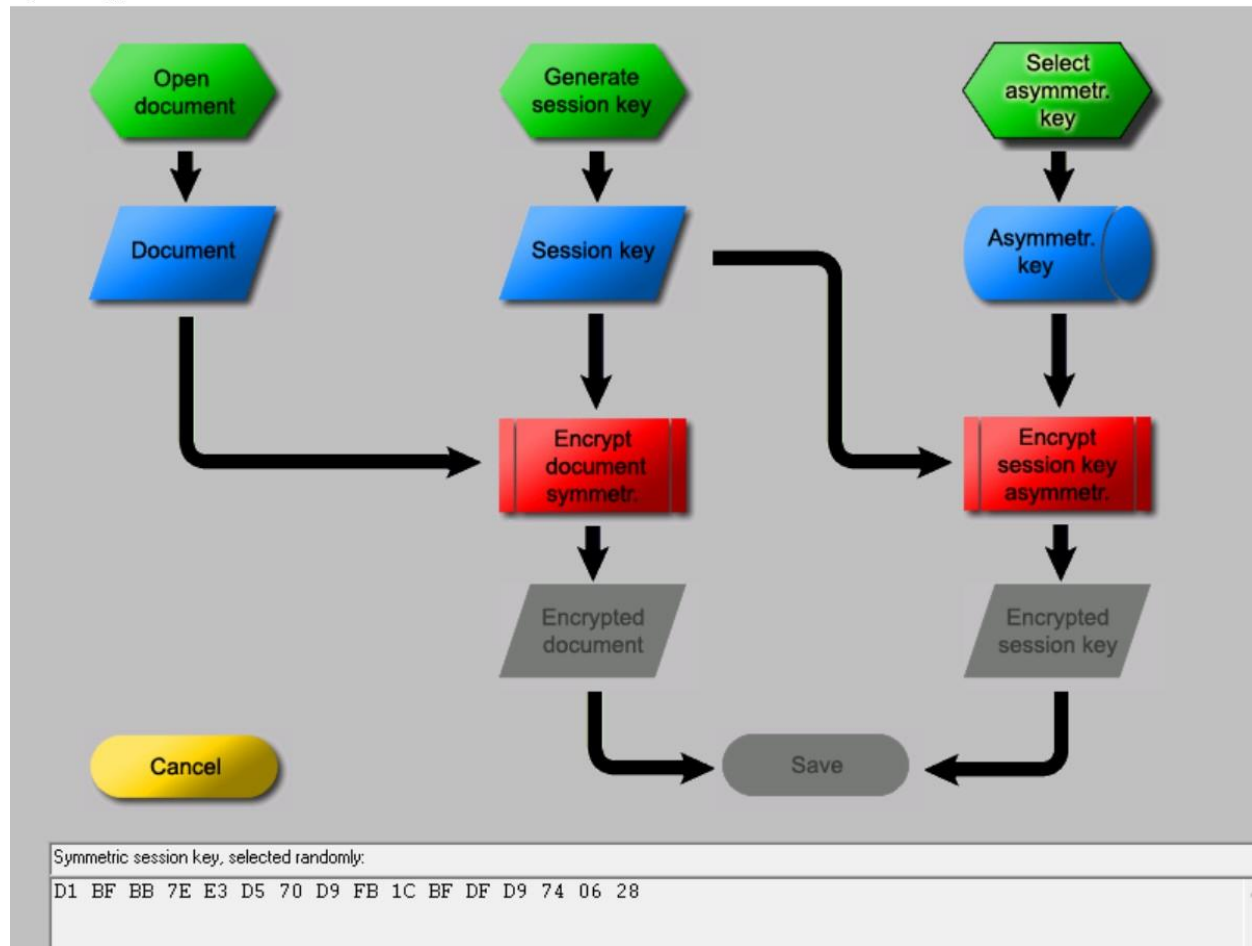
Side Channel Attack to RSA:

1. Select from menu: "Analysis" \ "Asymmetric Encryption" \ "Side-Channel Attack on Textbook 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 ”.

Hybrid Encryption with RSA-AES - Visualization with a Flow Chart



6. Click “Select asymmetr. 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).

Current Status of Trudy



Action log:

- Trudy has intercepted the message Alice sent to Bob
- Trudy has isolated the encrypted session key from the message
- Trudy has created 130 modified session keys up to now
- 66 of 130 modified messages were successfully decrypted by Bob's server

Intercepted, encrypted session key:

6419692924F2B478ED6C885BFA3D0A2C0DE4950EAD26A74537D89A545015EE603200E37BD5B5F4565F2E

Modified and encrypted session keys:

Modified and encrypted session key (hexadecimal):

AEA9D882C7E0A336EBBF9A1F71CBB8347C64836753A86B3059071B0CCDAE92320CD05492A2A01E...  
78015A1A0B43CBC64A90372DA0BD07535FA563C79A64B2D6E369E0B9FA57646D3A852806BB9A760...  
BDF3B4593DE5F5BD82CF2693B58472BFD882B1618EF3260DFFF801E44933DB2DF0C04EA2B5DB39...  
60D0722E2E51C1711A2E78BFCE6EF61CAD59005CFA24BEFE3C91F25F05D6FA9DD80533CF48D72D...  
57BR27F1RRF40F253FA3FFA2A52507FC5B5174721F2FAAF2D3FFFR894510R17FFDF3874FR19F256

Decrypted session key (calculated by Trudy, based on Bob's responses):

D1BFBB7EE3D570D9FB1CBFDFD9740628

Message (calculated by Trudy using the decrypted session key):

Starting example for the CrypTool version family 1.x (CT1)

CrypTool 1 (CT1) is a comprehensive and free educational program  
about cryptography and cryptanalysis  
offering extensive online help and many visualizations.

OK

The session key is D1BFBB7EE3D570D9FB1CBFDFD9740628 which matches the one generated 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.

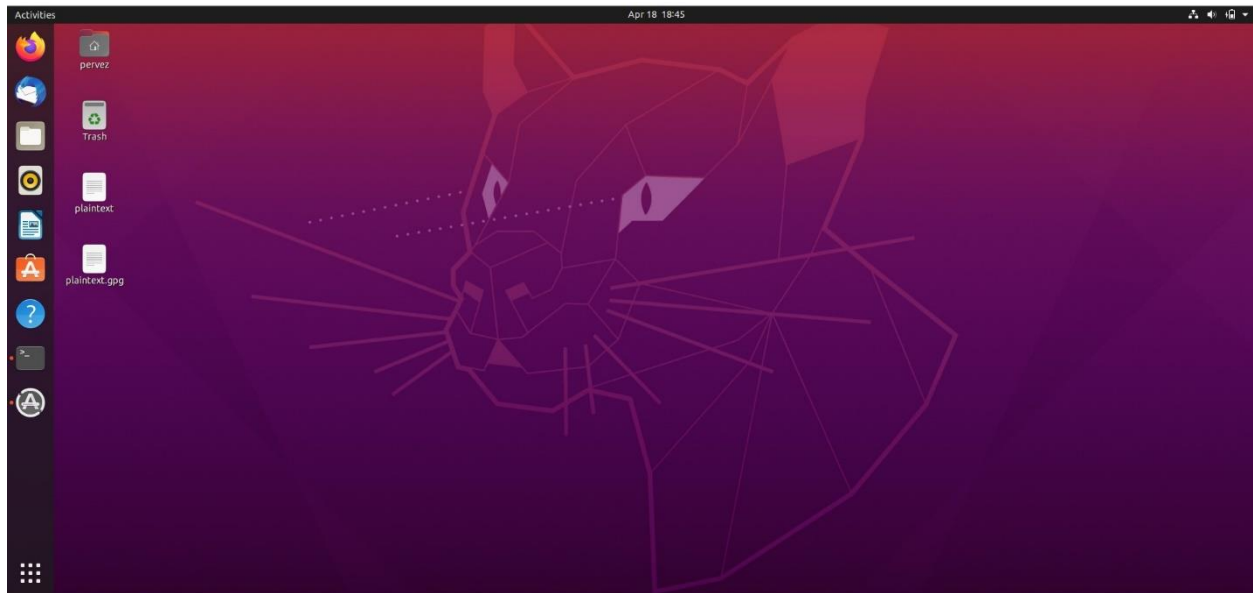
Farzad Kheirabadi

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.

