

Fuat Yiğit Koçyiğit – 16429085948

CMPE325 Section 1

15.05.2022



TED UNIVERSITY

Assignment 4 Report

How to Run the Code

Welcome Screen



Welcome Screen

Firstly, when the code executed, a welcome screen is appearing. The welcome screen has 2 buttons which are "Encrypt" and "Decrypt". When you pressed a button, it opens the required page. When you clicked, the welcome screen still stays visible for letting you open both "Encrypt" and "Decrypt" pages in one time.

Encryption Screen

If you press the "Encrypt" button, it opens the encryption page of my code as it can be seen below.

Encryption Screen

In this page, firstly you need to select the keys for RSA Encryption. There are 4 options. First 3 boxes are randomly generated keys, and the 4th box is for creating your own key.

If you want to use a ready key, select one of the ready key pairs' boxes and **click to it for like 2-3 times**. After you select one of them, the RSA values will be calculated automatically (As it can be seen below).

Selecting a ready key pair

If you want to create your own keys, select the 4th box and write the first values in the P and Q input box. After you entered the key, **you should press the "Enter" key** for confirmation. When you entered all 3 values, the program will calculate the RSA Values automatically (As it can be seen below).

RSA Encryption

Please select the key values to use or select a key pair. (Please select only 1 Check-box)

☐ Key pair 1 => P= 29 , Q= 47, E= 83

☐ Key pair 2 => P= 11 , Q= 29, E= 83

☐ Key pair 3 => P= 19, Q= 47, E= 97

☒ Create new key: P= Q= Enter a prime below 100. Not a divisor of 2

RSA Values

P = 2 Q = 3

Totient = 2

Public Keys: E = 5 N = 6

Private Key: D = 1 N = 6

Please enter the message you want to encrypt here:

Encrypt the Message

Encrypted Message =

You can copy the ciphertext from here or directly decrypt it. **Decrypt Ciphe...** =

Generating a new key

After you selected the values successfully, you should enter the message you wanted to encrypt to the message box. When you finished the message, **you should press the “Enter” key** for confirmation.

When the message confirmation is done too, you can now press the “Encrypt the Message” button. When you pressed it, the ciphertext will be calculated and printed to the red area at right.

RSA Encryption

Please select the key values to use or select a key pair. (Please select only 1 Check-box)

☒ Key pair 1 => P= 29 , Q= 47, E= 83

☐ Key pair 2 => P= 11 , Q= 29, E= 83

☐ Key pair 3 => P= 19, Q= 47, E= 97

☐ Create new key: P= Q= Enter a prime below 100. Not a divisor of 1288

RSA Values

P = 29 Q = 47

Totient = 1288

Public Keys: E = 83 N = 1363

Private Key: D = 419 N = 1363

Please enter the message you want to encrypt here:

Encrypt the Message

Encrypted Message : 4931303127549345112361019

You can copy the ciphertext from here or directly decrypt it. **Decrypt Ciphe...** =

Finished RSA Encryption

After the encryption is finished, you can copy the ciphertext from the text box in right bottom place.

Also, you can directly decrypt the ciphertext from the “Decrypt Ciphertext” button.

RSA Encryption

Please select the key values to use or select a key pair. (Please select only 1 Check-box)

☒ Key pair 1 => P= 29 , Q= 47, E= 83

☐ Key pair 2 => P= 11 , Q= 29, E= 83

☐ Key pair 3 => P= 19, Q= 47, E= 97

☐ Create new key: P= Q= Enter a prime below 100. Not a divisor of 1288

RSA Values

P = 29 Q = 47

Totient = 1288

Public Keys:
E = 83 N = 1363

Private Key:
D = 419 N = 1363

Please enter the message you want to encrypt here:

test123

Encrypt the Message

Encrypted Message : 4931303127549345112361019

You can copy the ciphertext from here or directly decrypt it. 7549345112361019 **Decrypt Ciphe...** = test123

Directly encrypting the message

Encryption Screen

If you press the “Decrypt” button, it opens the decryption page of my code as it can be seen below.

RSA Decryption

Please enter the message you want to decrypt here:

Please enter the keys here:

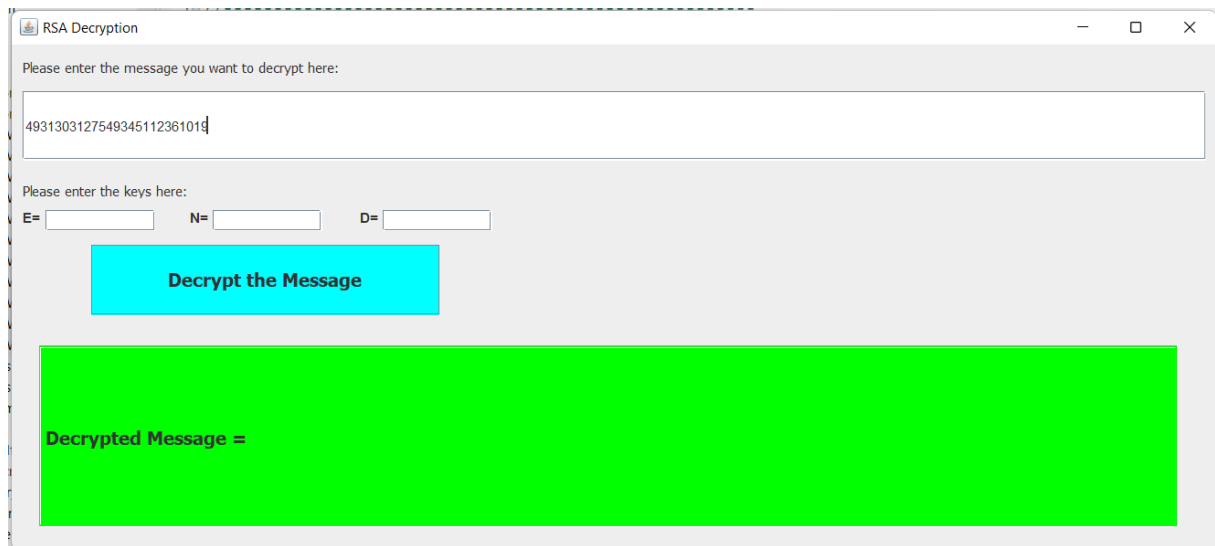
E= N= D=

Decrypt the Message

Decrypted Message =

Decryption Screen

In this page, you firstly need to enter the ciphertext you wanted to decrypt. When you entered the ciphertext, **you should press the “Enter” key** to confirm it.



The screenshot shows a window titled "RSA Decryption". It has a text input field with the value "4931303127549345112361019". Below this, there are three input fields for keys: "E=", "N=", and "D=", all of which are currently empty. A blue button labeled "Decrypt the Message" is positioned below the key inputs. At the bottom, there is a large green rectangular area with the text "Decrypted Message =" inside it.

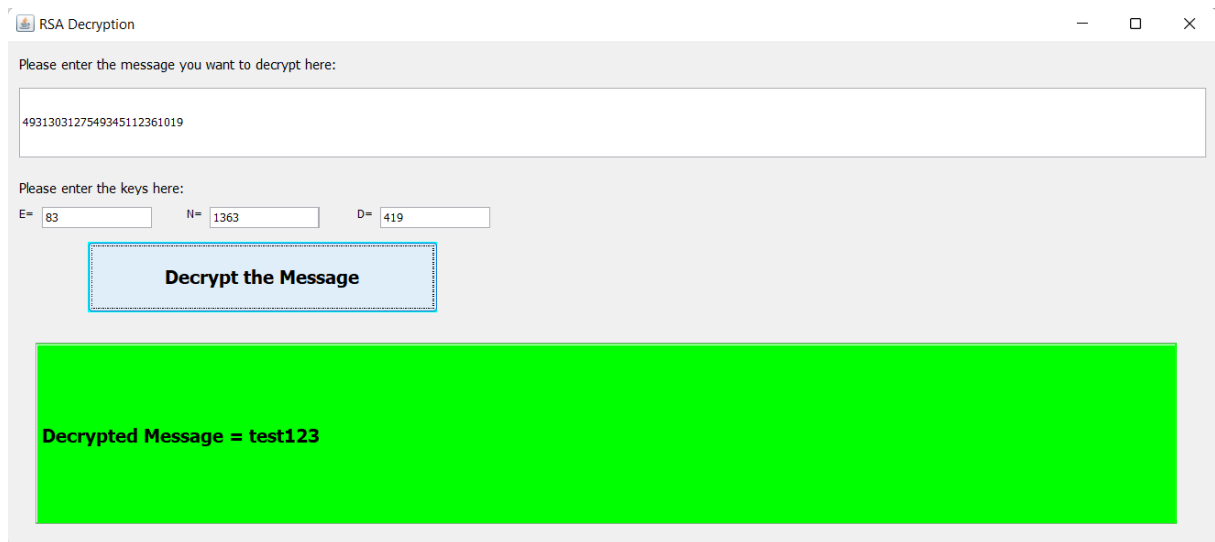
Entering the Ciphertext

After you confirmed the ciphertext, you should enter the E, N and D values for decryption. When you entered every value, **you should press the “Enter” key every time to confirm it.**



This screenshot shows the same "RSA Decryption" window, but now the key input fields are populated. The "E=" field contains "83", the "N=" field contains "1363", and the "D=" field contains "419". The "Decrypt the Message" button remains visible. The green area at the bottom still displays "Decrypted Message =".

After you confirmed the key values, you should press the “Decrypt the Message” button for decryption. After you pressed it, it will decrypt the message and print it to the green area below (as it can be seen below).



The screenshot shows a window titled "RSA Decryption". It contains two input sections. The first section, labeled "Please enter the message you want to decrypt here:", has a text box containing the ciphertext "4931303127549345112361019". The second section, labeled "Please enter the keys here:", has three input boxes: "E=" with the value "83", "N=" with the value "1363", and "D=" with the value "419". Below these inputs is a blue button labeled "Decrypt the Message". At the bottom of the window is a large green rectangular area displaying the text "Decrypted Message = test123".

Finished RSA Decryption

Exiting the Program

You can press the "X" button in everywhere for finishing and exiting the program.



Finishing the Program

Error Conditions

1) When you entered a non-prime number to the key value parts, it will not save it as a key value even if you confirm it.

The screenshot shows the 'RSA Encryption' application window. Under 'Please select the key values to use or select a key pair. (Please select only 1 Check-box)', the 'Create new key:' checkbox is checked. The 'P=' field contains '12', 'Q=' contains '90', and 'E=' contains '100'. Below this, the 'RSA Values' section shows 'P = 0', 'Q = 0', and 'Totient = 0'. The 'Public Keys:' section shows 'E = 0' and 'N = 0'. The 'Private Key:' section shows 'D = 0' and 'N = 0'. A text input field for the message is empty. To the right, the 'Encrypted Message =' area is a solid red rectangle. At the bottom, there is a blue 'Encrypt the Message' button and a 'Decrypt Ciphe...' button. A red error message is displayed in the bottom right corner, but its text is not legible.

Error 1

2) When you entered a number that is a divisor of the totient, it will open an error page and request you to enter a different E value.

The screenshot shows the 'RSA Encryption' application window with an error dialog box open. In the 'Create new key:' section, 'P=' is '2', 'Q=' is '3', and 'E=' is '8'. The 'RSA Values' section shows 'P = 2', 'Q = 3', and 'Totient = 2'. The 'Public Keys:' section shows 'E = 0' and 'N = 6'. The 'Private Key:' section shows 'D = 0' and 'N = 6'. A text input field for the message is empty. To the right, the 'Encrypted Message =' area is a solid red rectangle. At the bottom, there is a blue 'Encrypt the Message' button and a 'Decrypt Ciphe...' button. An error dialog box is open in the center, titled 'Error', with the message 'The number was a divisor of 2' and an 'OK' button.

Error 2

Assumptions

1) It is possible to select more than 1 boxes in the selecting key pair part in encryption page.

The program assumes that the last checked box is actual tick and makes its calculations according to that.

The screenshot shows a window titled "RSA Encryption". It contains a section for selecting key values with three checked checkboxes: "Key pair 1 => P= 29 , Q= 47, E= 83", "Key pair 2 => P= 11 , Q= 29, E= 83", and "Key pair 3 => P= 19, Q= 47, E= 97". Below this is a "Create new key:" section with input fields for P, Q, and a note "Enter a prime below 100. Not a divisor of 828". The "RSA Values" section displays P = 19, Q = 47, Totient = 828, Public Key: E = 97, N = 893, and Private Key: D = 153, N = 893. There is a text input field for the message to encrypt, a large red box for the encrypted message, a blue "Encrypt the Message" button, and a section for copying ciphertext or decrypting it.

Selecting more than one boxes (3rd one is calculated in this example)

2) The user should click more than 2 times for a correct calculation of RSA values.