Lab: Asymmetric Encryption Using RSA

Overview:

In this lab, you will learn how to encrypt and decrypt files using RSA encryption with OpenSSL. This will involve generating RSA keys, encrypting a file using the public key, and decrypting it using the private key.

Learning Objectives:
After completing this lab, you will be able to:

- Create RSA key pairs for encryption
- Encrypt and decrypt files using RSA

Step 1: Generate RSA Private Key

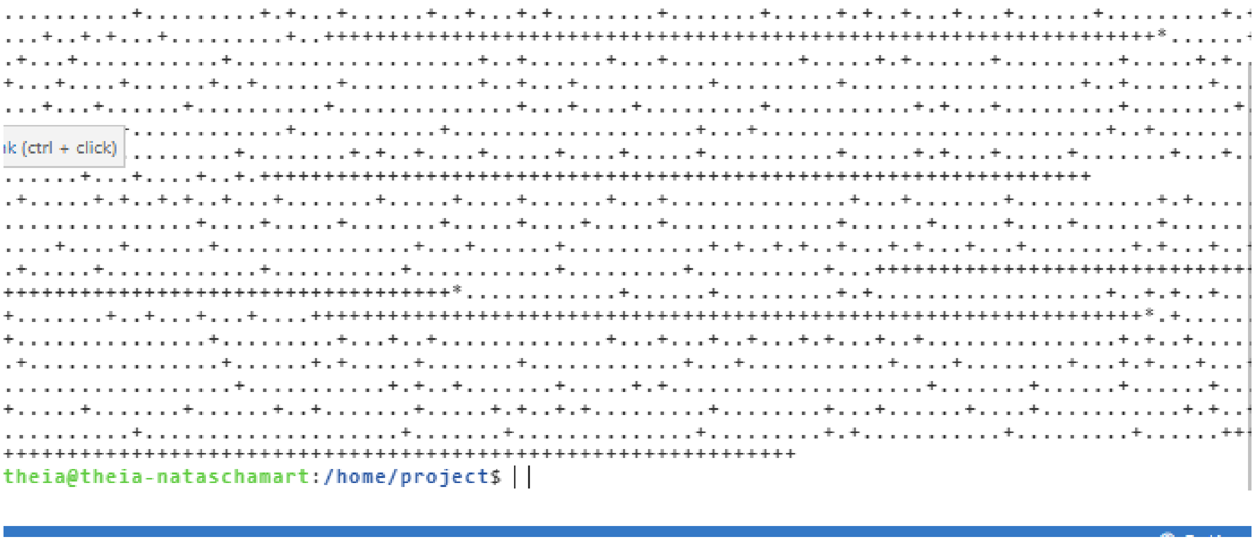
1. 1

```
openssl genpkey -algorithm RSA -out private_key.pem -pkeyopt rsa_keygen_bits:2048
```

Copied!Wrap Toggled!Executed!

Command Description

Command/Option	Description
openssl genpkey	Generates a private key.
-algorithm RSA	Specifies the RSA algorithm for key generation.
-out private_key.pem	Output file where the private key will be stored.
-pkeyopt rsa_keygen_bits:2048	Option to specify the key size, here 2048 bits for RSA key generation.



```
..........+.........+.+...+......+..+...+.+........+.......+.....+.+..+...+...+......+.........+.
...+..+.+...+.........+..+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++*......
.+...+...........+...................+..+......+...+..........+.....+.+......+.........+.....+.+.
+...+....+......+..+......+..........+..+...+..........+.........+..................+..+......+..
...+...+......+..........+..............+...+....+.........+...........+.+...+.........+........+
         +............+...........+...................+...+...........................+..+.......
ik (ctrl + click)........+........+.+..+....+.....+....+.....+..........+.....+.+...+.....+.......+...+.
......+...+....+..+.+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
.+.....+.+..+.+..+...+.......+.....+....+......+...+..............+...+.......+...........+.+....
...............+....+.....+.......+.....+....+.....+.............+......+.....+....+......+......
....+....+......+...............+...+......+...........+.+..+.+..+...+.+...+...+........+.+...+..
.+.....+............+..........+...........+.........+..........+...+++++++++++++++++++++++++++++
+++++++++++++++++++++++++++++++++++*............+......+.........+.+..................+..+.+..+..
+.......+..+...+...+....+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++*.+.....
+...............+.........+...+..+.............+...+...+..+...+.+...+..+...............+.+..+....
.+...............+......+.+.....+.......+............+...+...........+....+........+...+.+...+...
..................+...........+.+..+.......+.....+.+....................+.......+......+......+..
+.....+.......+......+..+.......+.....+.+..+.+.........+........+...+......+....+...........+.+..
..........+....................+.......+..............+.........+.+...........+.........+......++
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
theia@theia-nataschamart:/home/project$
```

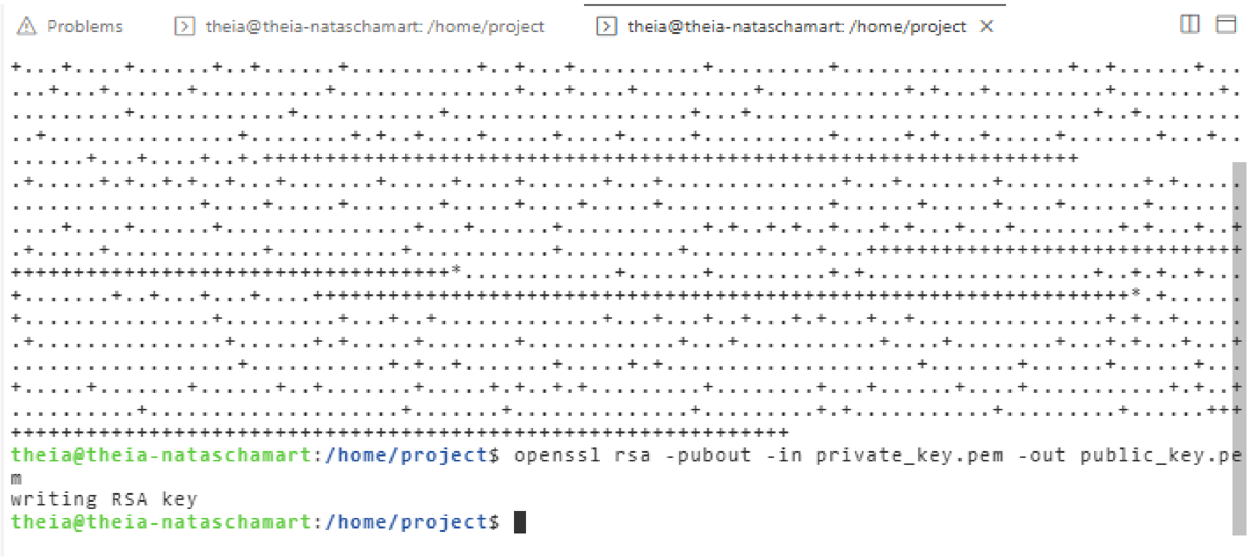
Step 2: Extract Public Key from Private Key

```
openssl rsa -pubout -in private_key.pem -out public_key.pem
```

Copied!Wrap Toggled!Executed!

Command Description

Command/Option	Description
openssl rsa	RSA-specific utility in OpenSSL, used for key management.
-pubout	Tells OpenSSL to extract the public key from the private key.
-in private_key.pem	Input file, in this case, the private key.
-out public_key.pem	Output file where the public key will be saved.


Problems
theia@theia-nataschamart: /home/project
theia@theia-nataschamart: /home/project

```
+...+....+......+..+......+..........+..+...+..........+.........+..................+..+......+...
...+...+......+..........+..............+...+....+.........+...........+.+...+.........+........+.
.........+............+...........+...................+...+...........................+..+........
..+...............+........+.+..+....+.....+....+.....+..........+.....+.+...+.....+.......+...+..
......+...+....+..+.+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
.+.....+.+..+.+..+...+.......+.....+....+......+...+..............+...+.......+...........+.+.....
...............+....+.....+.......+.....+....+.....+.............+......+.....+....+......+.......
....+....+......+...............+...+......+...........+.+..+.+..+...+.+...+...+........+.+...+..+
.+.....+............+..........+...........+.........+..........+...++++++++++++++++++++++++++++++
+++++++++++++++++++++++++++++++++++*............+......+.........+.+..................+..+.+..+...
+.......+..+...+...+....+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++*.+......
+...............+.........+...+..+.............+...+...+..+...+.+...+..+...............+.+..+.....
.+...............+......+.+.....+.......+............+...+...........+....+........+...+.+...+...+
..................+...........+.+..+.......+.....+.+....................+.......+......+......+...
+.....+.......+......+..+.......+.....+.+..+.+.........+........+...+......+....+...........+.+..+
..........+....................+.......+..............+.........+.+...........+.........+......+++
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
theia@theia-nataschamart:/home/project$ openssl rsa -pubout -in private_key.pem -out public_key.pe
m
writing RSA key
theia@theia-nataschamart:/home/project$ 
```

Step 3: Create a Test File

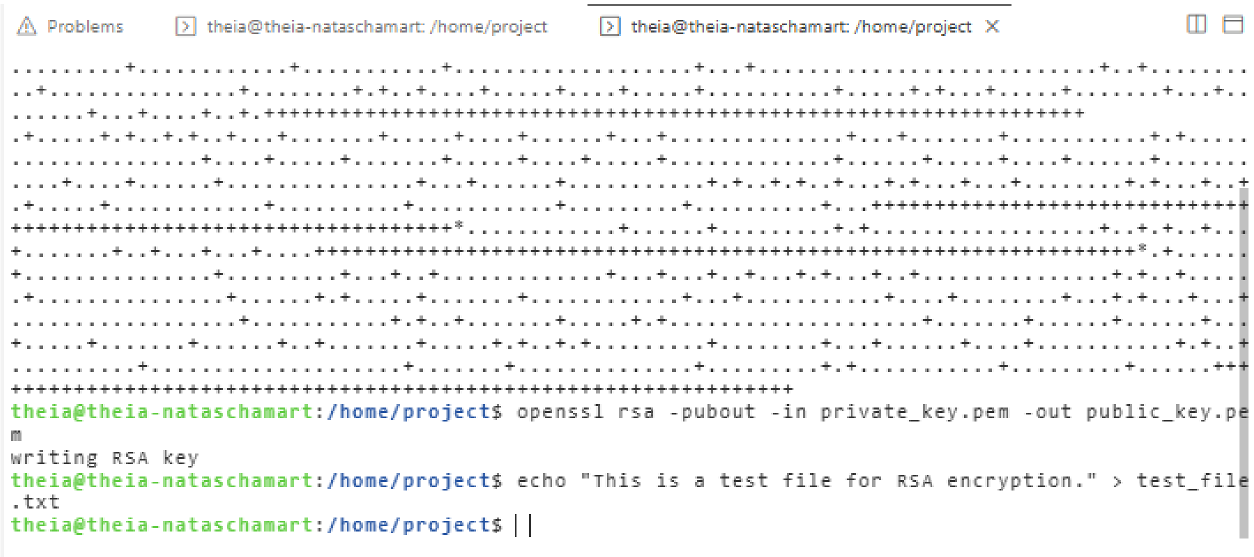
1. 1

```
echo "This is a test file for RSA encryption." > test_file.txt
```

Copied!Wrap Toggled!Executed!

Command Description

Command/Option	Description
echo	Command to output the specified string to a file or terminal.
“This is a test file…”	The actual text content that will be written to the file.
> test_file.txt	Redirects the output of echo to a file named test_file.txt.


Problems
theia@theia-nataschamart: /home/project
theia@theia-nataschamart: /home/project

```
.........+............+...........+..................+...+...........................+..+........
..+...............+.........+.+..+....+.....+....+......+...........+......+.+...+......+.......+...+..
......+...+....+..+.+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
.+.....+.+..+.+..+...+.........+......+.....+.......+...+..............+...+........+...........+.+.....
...............+....+.....+.......+......+....+.....+..............+.......+.....+....+......+.......
....+....+......+...............+...+......+...........+.+..+.+..+...+.+...+...+.........+.+...+..+
.+.....+..........+..........+...........+.........+..........+...++++++++++++++++++++++++++++++
++++++++++++++++++++++++++++++++++++*...........+......+.........+.+...................+..+.+..+..
+.......+..+...+...+....+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++*.+......
+...............+.........+...+..+..............+...+..+...+..+...+..+..................+.+..+.....
.+...............+........+.+.....+........+..............+...+...........+....+...........+...+.+...+...+
..................+...........+.+..+........+.....+.+......................+.......+.......+.......+...
+.....+.......+......+..+.......+.....+.+..+.+.........+.......+...+......+....+...........+.+..+
..........+...................+.......+..............+.........+.+...........+.........+......+++
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
theia@theia-nataschamart:/home/project$ openssl rsa -pubout -in private_key.pem -out public_key.pe
m
writing RSA key
theia@theia-nataschamart:/home/project$ echo "This is a test file for RSA encryption." > test_file
.txt
theia@theia-nataschamart:/home/project$ ||
```

Step 4: Encrypt the Test File using RSA public key

Step A: Encrypt the File

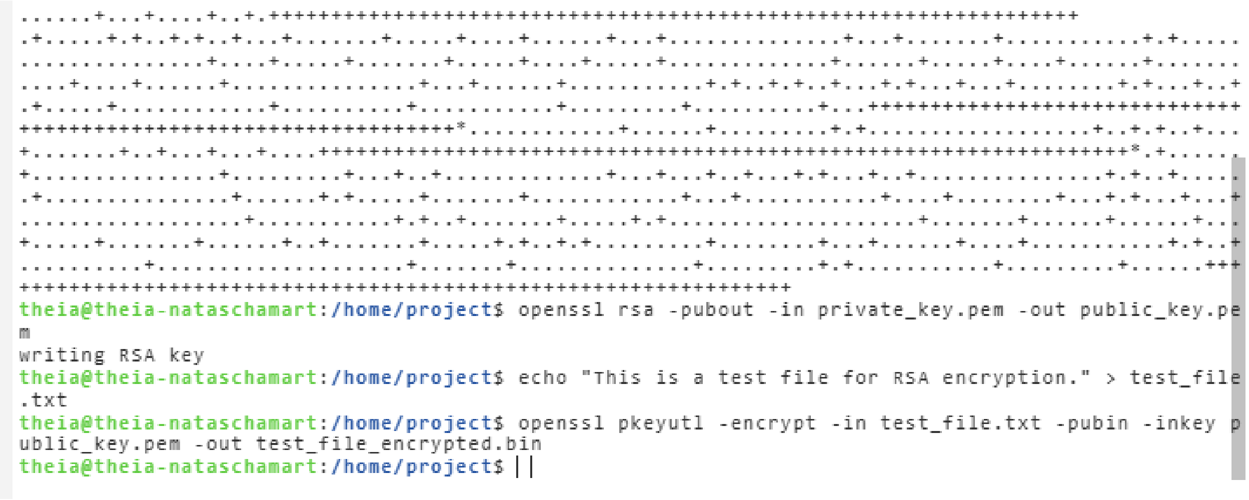
1. 1

```
openssl pkeyutl -encrypt -in test_file.txt -pubin -inkey public_key.pem -out 

test_file_encrypted.bin
```

Copied!Wrap Toggled!Executed!

Command Description

Command/Option	Description
openssl pkeyutl	Utility for performing public key cryptographic operations (encryption, decryption, and so on).
-encrypt	Specifies that the operation is encryption.
-in test_file.txt	Input file, in this case, the Test File to encrypt.
-pubin	Indicates that the provided key is a public key.
-inkey public_key.pem	Specifies the public key file to use for encryption.
-out test_file_encrypted.bin	Output file where the encrypted file will be stored.



```
......+...+....+..+.+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
.+.....+.+..+.+..+...+.......+.....+....+......+...+...............+...+.......+..........+..+....
...............+....+.....+.......+.....+....+.....+.............+......+.....+....+......+.......
....+....+......+...............+...+......+...........+.+..+.+..+...+.+...+...+........+.+...+..+
.+.....+............+..........+...........+.........+..........+...++++++++++++++++++++++++++++++
+++++++++++++++++++++++++++++++++++*.............+.....+.........+.+..................+..+.+..+...
+.......+..+...+...+....+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++*.+......
+...............+.........+...+..+.............+...+...+..+...+.+...+..+...............+.+..+.....
.+...............+......+.+.....+.......+............+...+...........+....+........+...+.+...+...+
..................+...........+.+..+.......+.....+.+....................+.......+......+......+...
+.....+.......+......+..+.......+.....+.+..+.+.........+........+...+......+....+...........+.+..+
..........+....................+.......+..............+.........+.+...........+.........+......+++
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
theia@theia-nataschamart:/home/project$ openssl rsa -pubout -in private_key.pem -out public_key.pe
m
writing RSA key
theia@theia-nataschamart:/home/project$ echo "This is a test file for RSA encryption." > test_file
.txt
theia@theia-nataschamart:/home/project$ openssl pkeyutl -encrypt -in test_file.txt -pubin -inkey p
ublic_key.pem -out test_file_encrypted.bin
theia@theia-nataschamart:/home/project$ ||
```

Step B: Open and Verify that File is Encrypted

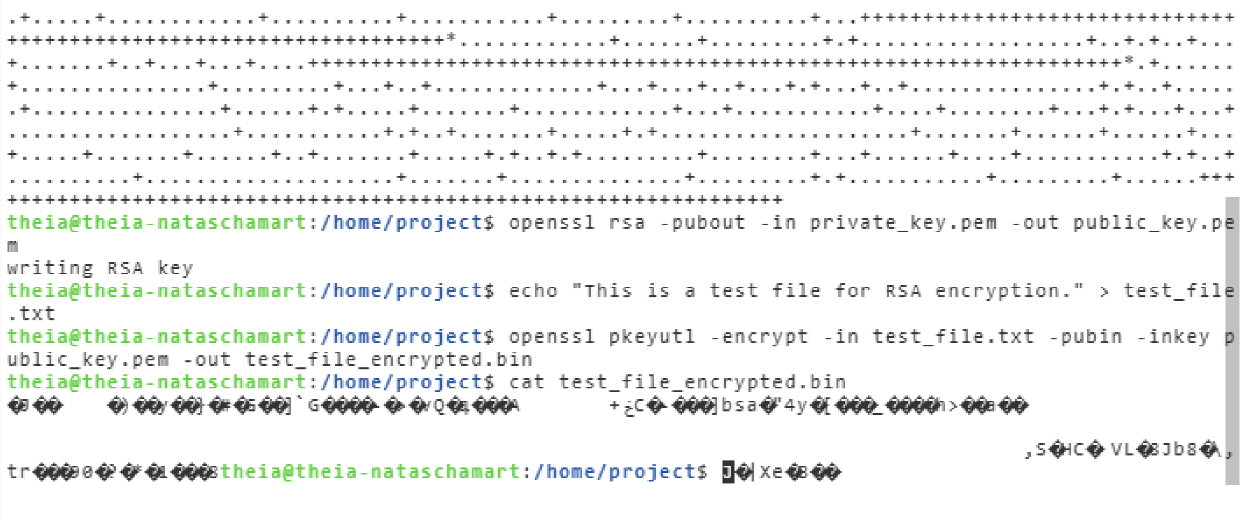
1. 1

```
cat test_file_encrypted.bin
```

Copied!Wrap Toggled!Executed!

Command/Option	Description
cat	Displays the contents of a file.
test_file_encrypted.bin	The file with the encrypted binary data.

You should see unreadable binary data, confirming that the file has been encrypted



```
.+.....+............+..........+...........+.........+..........+...++++++++++++++++++++++++++++++
+++++++++++++++++++++++++++++++++++*.............+.....+.........+.+..................+..+.+..+...
+.......+..+...+...+....+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++*.+......
+...............+.........+...+..+.............+...+...+..+...+.+...+..+...............+.+..+.....
.+...............+......+.+.....+.......+............+...+...........+....+........+...+.+...+...+
..................+...........+.+..+.......+.....+.+....................+.......+......+......+...
+.....+.......+......+..+.......+.....+.+..+.+.........+........+...+......+....+...........+.+..+
..........+....................+.......+..............+.........+.+...........+.........+......+++
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
theia@theia-nataschamart:/home/project$ openssl rsa -pubout -in private_key.pem -out public_key.pe
m
writing RSA key
theia@theia-nataschamart:/home/project$ echo "This is a test file for RSA encryption." > test_file
.txt
theia@theia-nataschamart:/home/project$ openssl pkeyutl -encrypt -in test_file.txt -pubin -inkey p
ublic_key.pem -out test_file_encrypted.bin
theia@theia-nataschamart:/home/project$ cat test_file_encrypted.bin
�B��    �)��y��}�#�G��]`G���� � �vQ�d���A       +¿C� ���]bsa�'4y�[���_����h>��a��

                                                                                  ,S�HC� VL�8Jb8�A,
tr���0�?�'�1���8theia@theia-nataschamart:/home/project$ J�|Xe�B��
```

Step 5: Decrypt the Test File using RSA private key

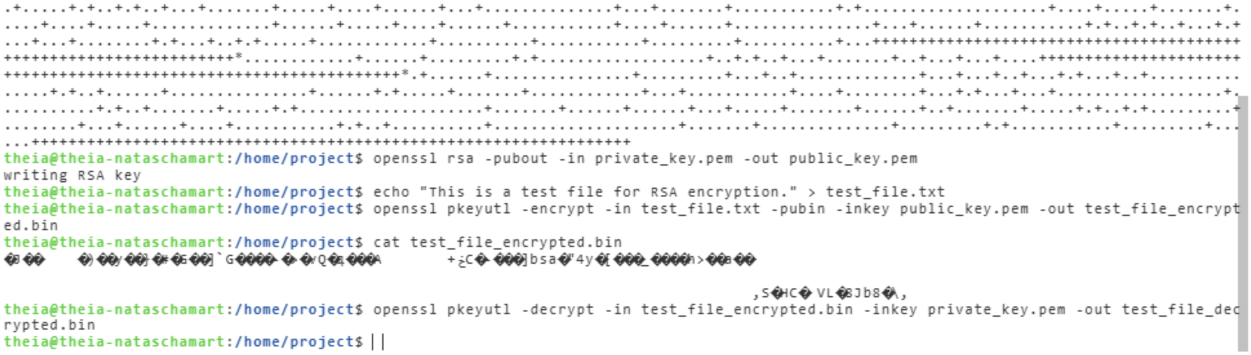
Step A: Decrypt the File

```
1. 1
openssl pkeyutl -decrypt -in test_file_encrypted.bin -inkey private_key.pem -
out test_file_decrypted.bin
```

Copied!Wrap Toggled!Executed!

Command Description

Command/Option	Description
openssl pkeyutl	Utility for performing public key cryptographic operations.
-decrypt	Specifies that the operation is decryption.
-in test_file_encrypted.bin	Input file, in this case, the encrypted test file.
-inkey private_key.pem	Specifies the RSA private key to use for decryption.
-out test_file_decrypted.bin	Output file where the decrypted file will be saved.



```
.+.....+.+..+.+..+...+.......+.....+....+......+...+..............+...+.......+...........+.+...................+....+.....+.......+.
....+....+.....+.............+......+.....+....+......+...........+....+......+...............+...+......+...........+.+..+.+..+...+.+
...+...+........+.+...+..+.+.....+.............+..........+..........+...........+..........+...+++++++++++++++++++++++++++++++++++++++
+++++++++++++++++++++++++*............+......+.........+.+..................+..+.+..+...+.......+..+...+...+....+++++++++++++++++++++++
++++++++++++++++++++++++++++++++++++++++++*.+......+...............+.........+...+..+..............+...+...+..+...+.+...+..+..........
.....+.+..+......+...............+......+.+.....+.......+.........+...+............+...+.....+.......+...+.+...+...+..................+.
..........+.+..+.......+.....+.+.....................+.......+.......+.......+...+.....+.......+......+..+.........+.....+.+..+.+.........+
........+...+......+....+...........+.+..+..........+..................+.......+...............+.........+.+...........+.........+...
...++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
theia@theia-nataschamart:/home/project$ openssl rsa -pubout -in private_key.pem -out public_key.pem
writing RSA key
theia@theia-nataschamart:/home/project$ echo "This is a test file for RSA encryption." > test_file.txt
theia@theia-nataschamart:/home/project$ openssl pkeyutl -encrypt -in test_file.txt -pubin -inkey public_key.pem -out test_file_encrypt
ed.bin
theia@theia-nataschamart:/home/project$ cat test_file_encrypted.bin
�B��    �)��y��}�#�G��]`G���� � �wQ�ą���A        +¿C� ���]bsa�"4y�[���_����h>��a��

                                                                          ,S�HC� VL�8Jb8�A,
theia@theia-nataschamart:/home/project$ openssl pkeyutl -decrypt -in test_file_encrypted.bin -inkey private_key.pem -out test_file_dec
rypted.bin
theia@theia-nataschamart:/home/project$ ||
```

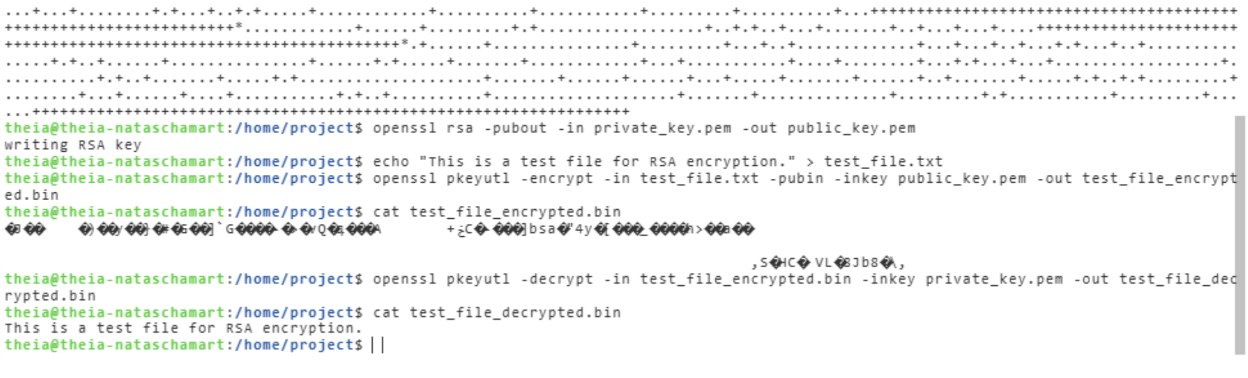
Step B: Open and Verify that File is Decrypted

```
1. 1
cat test_file_decrypted.bin
```

Copied!Wrap Toggled!Executed!

Command/Option	Description
cat	Displays the contents of a file.
test_file_decrypted.bin	The file with the decrypted data.

You should see the original text: **This is a test file for RSA encryption.**

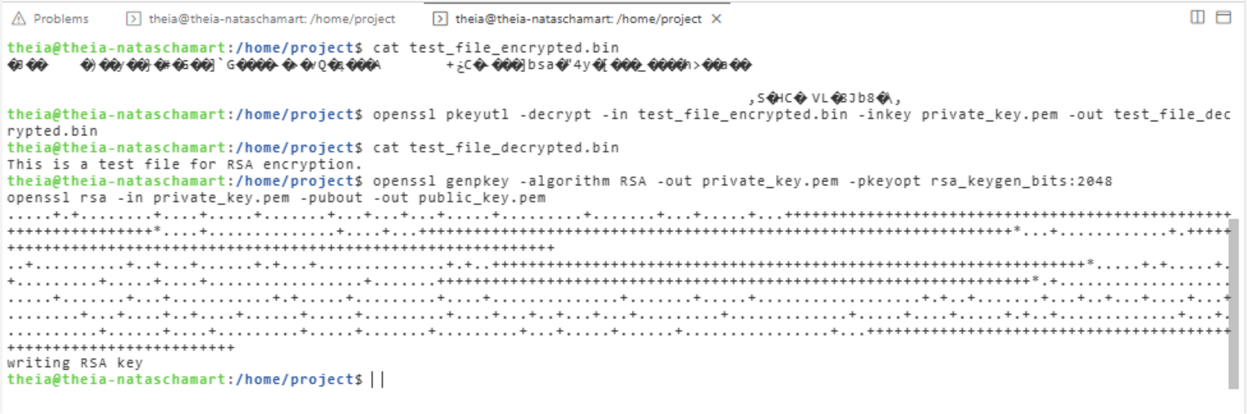


```
...+...+........+.+...+..+.+.....+............+..........+...........+.........+..........+...+++++++++++++++++++++++++++++++++++++++++
+++++++++++++++++++++++++*............+......+.........+.+..................+..+.+..+...+.......+..+...+...+...+++++++++++++++++++++
+++++++++++++++++++++++++++++++++++++++++++*.+......+...............+.........+...+..+.............+...+...+..+...+.+...+..+..........
.....+.+..+......+..............+......+.+.....+.......+...........+...+...........+....+........+...+.+...+...+.................+.
..........+.+..+.......+.....+.+.....................+.......+.......+.....+...+.....+.......+.......+..+........+.....+.+..+.+........+
........+...+......+....+..........+.+..+.........+.....................+.......+..............+.........+.+...........+.........+...
...+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
theia@theia-nataschamart:/home/project$ openssl rsa -pubout -in private_key.pem -out public_key.pem
writing RSA key
theia@theia-nataschamart:/home/project$ echo "This is a test file for RSA encryption." > test_file.txt
theia@theia-nataschamart:/home/project$ openssl pkeyutl -encrypt -in test_file.txt -pubin -inkey public_key.pem -out test_file_encrypt
ed.bin
theia@theia-nataschamart:/home/project$ cat test_file_encrypted.bin
�B��     �)��y��}�#�G��]`G����-�-�vQ�q���A       +¿C�-���]bsa�"4y�[���_����h>��a��

                                                                                    ,S�HC� VL�BJb8�A,
theia@theia-nataschamart:/home/project$ openssl pkeyutl -decrypt -in test_file_encrypted.bin -inkey private_key.pem -out test_file_dec
rypted.bin
theia@theia-nataschamart:/home/project$ cat test_file_decrypted.bin
This is a test file for RSA encryption.
theia@theia-nataschamart:/home/project$ ||
```

Exercises

Exercise 1: Encrypt and Decrypt a Small Message Using RSA

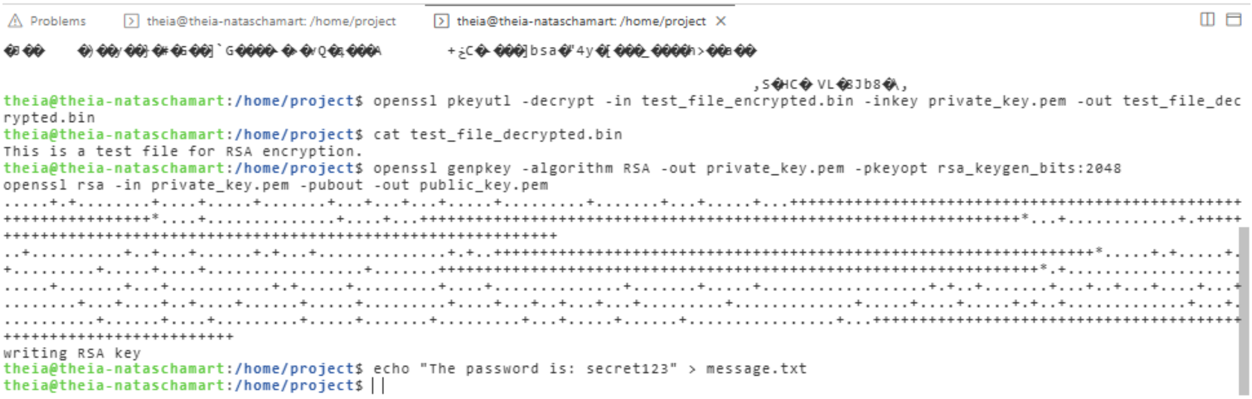
Objective: Learn to encrypt and decrypt a short message using RSA.
Task Details:
Step 1: Generate RSA Key Pair:



Problems
theia@theia-nataschamart: /home/project
theia@theia-nataschamart: /home/project

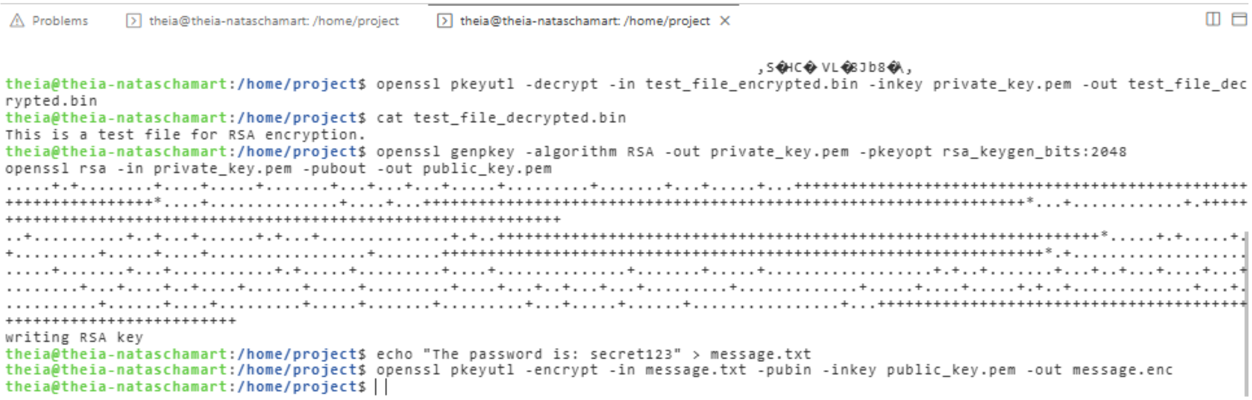
```
theia@theia-nataschamart:/home/project$ cat test_file_encrypted.bin
�B��     �)��y��}�#�G��]`G����-�-�vQ�q���A       +¿C�-���]bsa�"4y�[���_����h>��a��

                                                                                    ,S�HC� VL�BJb8�A,
theia@theia-nataschamart:/home/project$ openssl pkeyutl -decrypt -in test_file_encrypted.bin -inkey private_key.pem -out test_file_dec
rypted.bin
theia@theia-nataschamart:/home/project$ cat test_file_decrypted.bin
This is a test file for RSA encryption.
theia@theia-nataschamart:/home/project$ openssl genpkey -algorithm RSA -out private_key.pem -pkeyopt rsa_keygen_bits:2048
openssl rsa -in private_key.pem -pubout -out public_key.pem
.....+.+........+....+.....+.......+...+...+...+.....+.........+.......+...+.....+...++++++++++++++++++++++++++++++++++++++++++++++++++
++++++++++++++++*....+.............+....+...+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++*...+............+.+++++
+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
..+..........+..+...+......+.+...+.............+.+..++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++*.....+.+.....+.
+.........+.....+....+.................+.......++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++*.+.................
.....+.......+...+............+.+.....+.........+....+..............+.......+.....+..................+.+..+.......+...+..+...+....+...+
........+...+....+..+....+......+.....+.........+....+...+..+...+...+.........+...........+.....+....+.....+.+..+.............+...+.
..........+......+....+.........+.....+.......+.........+...+.....+......+...............+...+++++++++++++++++++++++++++++++++++++++++
+++++++++++++++++++++++++
writing RSA key
theia@theia-nataschamart:/home/project$ ||
```

Step 2: Create a Short Message


Problems
theia@theia-nataschamart: /home/project
theia@theia-nataschamart: /home/project

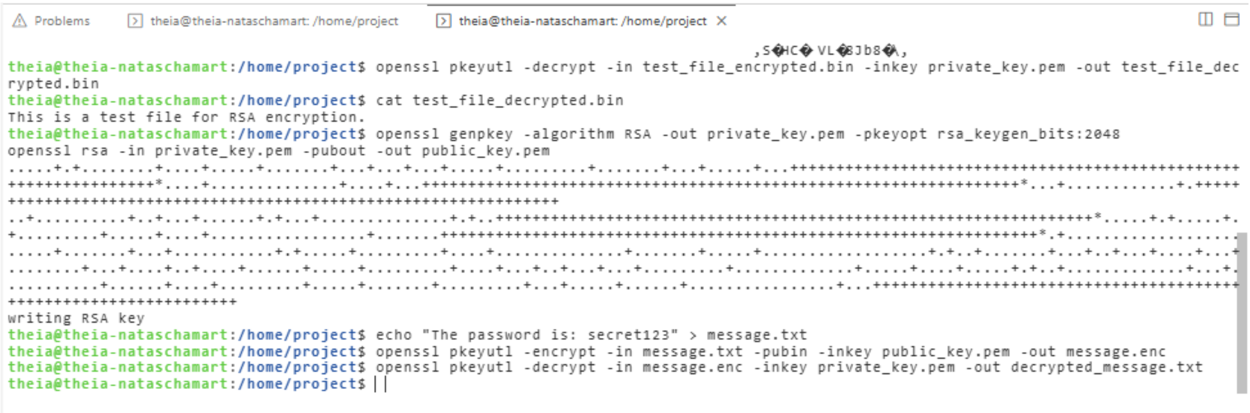
```
�B ��      �) ��y ��} �# �G ��] `G���� � �vQ�& ���A        +¿C� ���]bsa�"4y�[ ���_����n>��a��

                                                                                        ,S�HC� VL�BJb8�A,
theia@theia-nataschamart:/home/project$ openssl pkeyutl -decrypt -in test_file_encrypted.bin -inkey private_key.pem -out test_file_dec
rypted.bin
theia@theia-nataschamart:/home/project$ cat test_file_decrypted.bin
This is a test file for RSA encryption.
theia@theia-nataschamart:/home/project$ openssl genpkey -algorithm RSA -out private_key.pem -pkeyopt rsa_keygen_bits:2048
openssl rsa -in private_key.pem -pubout -out public_key.pem
.....+.+........+....+.....+.......+...+...+...+.....+.........+.......+...+.....+...+++++++++++++++++++++++++++++++++++++++++++++++++
++++++++++++++++*....+..............+....+...+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++*...+...........+.+++++
+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
..+..........+..+...+......+.+...+.............+.+..+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++*.....+.+.....+.
+.........+.....+....+.................+.......++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++*.+.................
.....+.......+...+...........+.+.....+.........+....+...............+.......+.....+..................+.+..+.......+...+..+...+.....+...+
........+...+....+..+....+......+.....+.........+....+...+..+...+...+.........+.............+.....+....+.....+.+..+.............+...+.
..........+......+....+.........+.....+.......+.........+...+.....+......+................+...++++++++++++++++++++++++++++++++++++++++
+++++++++++++++++++++++++
writing RSA key
theia@theia-nataschamart:/home/project$ echo "The password is: secret123" > message.txt
theia@theia-nataschamart:/home/project$ ||
```

Step 3: Encrypt the Message


Problems
theia@theia-nataschamart: /home/project
theia@theia-nataschamart: /home/project

```
                                                                                        ,S�HC� VL�BJb8�A,
theia@theia-nataschamart:/home/project$ openssl pkeyutl -decrypt -in test_file_encrypted.bin -inkey private_key.pem -out test_file_dec
rypted.bin
theia@theia-nataschamart:/home/project$ cat test_file_decrypted.bin
This is a test file for RSA encryption.
theia@theia-nataschamart:/home/project$ openssl genpkey -algorithm RSA -out private_key.pem -pkeyopt rsa_keygen_bits:2048
openssl rsa -in private_key.pem -pubout -out public_key.pem
.....+.+........+....+.....+.......+...+...+...+.....+.........+.......+...+.....+...+++++++++++++++++++++++++++++++++++++++++++++++++
++++++++++++++++*....+..............+....+...+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++*...+...........+.+++++
+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
..+..........+..+...+......+.+...+.............+.+..+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++*.....+.+.....+.
+.........+.....+....+.................+.......++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++*.+.................
.....+.......+...+...........+.+.....+.........+....+...............+.......+.....+..................+.+..+.......+...+..+...+.....+...+
........+...+....+..+....+......+.....+.........+....+...+..+...+...+.........+.............+.....+....+.....+.+..+.............+...+.
..........+......+....+.........+.....+.......+.........+...+.....+......+................+...++++++++++++++++++++++++++++++++++++++++
+++++++++++++++++++++++++
writing RSA key
theia@theia-nataschamart:/home/project$ echo "The password is: secret123" > message.txt
theia@theia-nataschamart:/home/project$ openssl pkeyutl -encrypt -in message.txt -pubin -inkey public_key.pem -out message.enc
theia@theia-nataschamart:/home/project$ ||
```

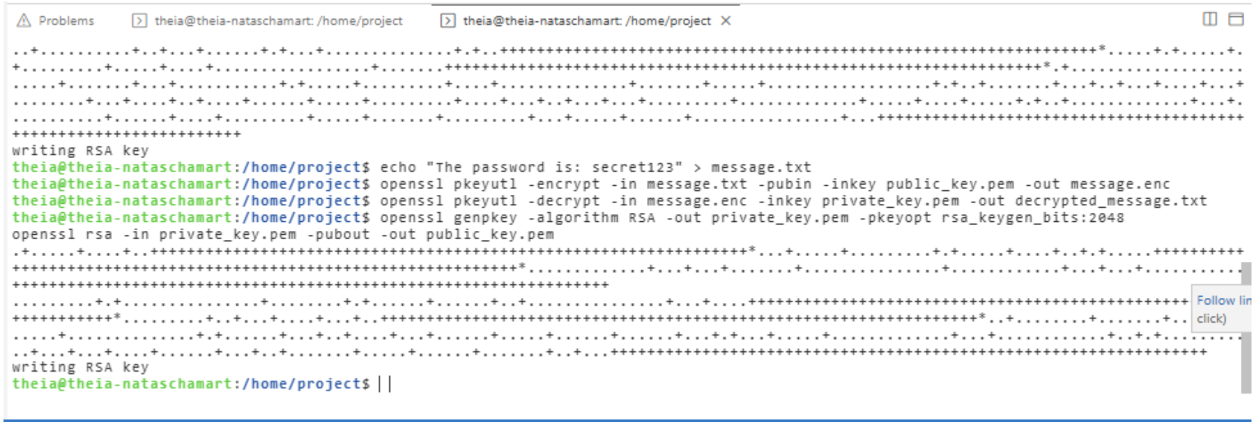
Step 4: Decrypt the Encrypted Message:


Problems
theia@theia-nataschamart: /home/project
theia@theia-nataschamart: /home/project

```
                                                                                        ,S�HC� VL�BJb8�A,
theia@theia-nataschamart:/home/project$ openssl pkeyutl -decrypt -in test_file_encrypted.bin -inkey private_key.pem -out test_file_dec
rypted.bin
theia@theia-nataschamart:/home/project$ cat test_file_decrypted.bin
This is a test file for RSA encryption.
theia@theia-nataschamart:/home/project$ openssl genpkey -algorithm RSA -out private_key.pem -pkeyopt rsa_keygen_bits:2048
openssl rsa -in private_key.pem -pubout -out public_key.pem
.....+.+........+....+.....+.......+...+...+...+.....+.........+.......+...+.....+...+++++++++++++++++++++++++++++++++++++++++++++++++
++++++++++++++++*....+..............+....+...+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++*...+...........+.+++++
+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
..+..........+..+...+......+.+...+.............+.+..+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++*.....+.+.....+.
+.........+.....+....+.................+.......++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++*.+.................
.....+.......+...+...........+.+.....+.........+....+...............+.......+.....+..................+.+..+.......+...+..+...+.....+...+
........+...+....+..+....+......+.....+.........+....+...+..+...+...+.........+.............+.....+....+.....+.+..+.............+...+.
..........+......+....+.........+.....+.......+.........+...+.....+......+................+...++++++++++++++++++++++++++++++++++++++++
+++++++++++++++++++++++++
writing RSA key
theia@theia-nataschamart:/home/project$ echo "The password is: secret123" > message.txt
theia@theia-nataschamart:/home/project$ openssl pkeyutl -encrypt -in message.txt -pubin -inkey public_key.pem -out message.enc
theia@theia-nataschamart:/home/project$ openssl pkeyutl -decrypt -in message.enc -inkey private_key.pem -out decrypted_message.txt
theia@theia-nataschamart:/home/project$ ||
```

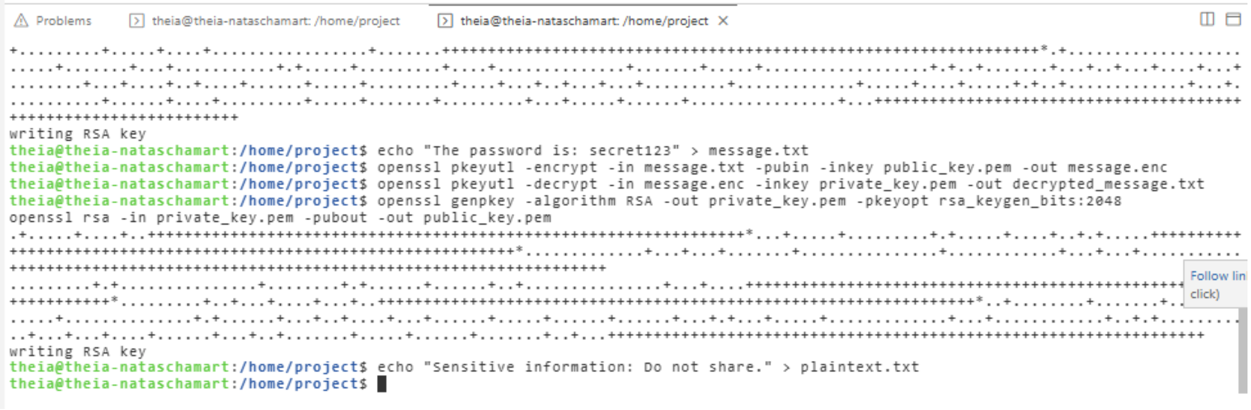
Exercise 2: RSA Key Pair Generation and File Encryption

Objective: Generate an RSA key pair and use it to encrypt and decrypt a file.
Task Details:
Step 1: Generate RSA Key Pair:


Problems
theia@theia-nataschamart: /home/project
theia@theia-nataschamart: /home/project
Follow lin
click)

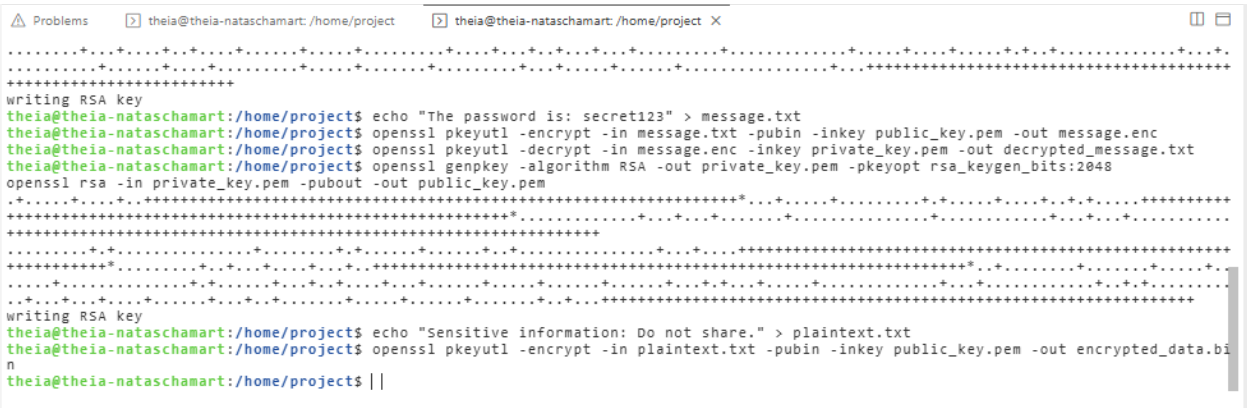
```
..+..........+..+...+......+.+...+.............+.+..+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++*.....+.+.....+.
+.........+.....+....+................+.......++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++*.+..................
.....+.......+...+...........+.+.....+.........+....+..............+.......+.....+.................+.+..+.......+...+..+...+....+...+
........+...+....+..+....+......+.....+.........+....+...+..+...+...+.........+.............+.....+....+.....+.+..+.............+...+.
..........+......+....+.........+.....+.......+.........+...+.....+......+...............+...++++++++++++++++++++++++++++++++++++++++
+++++++++++++++++++++++++
writing RSA key
theia@theia-nataschamart:/home/project$ echo "The password is: secret123" > message.txt
theia@theia-nataschamart:/home/project$ openssl pkeyutl -encrypt -in message.txt -pubin -inkey public_key.pem -out message.enc
theia@theia-nataschamart:/home/project$ openssl pkeyutl -decrypt -in message.enc -inkey private_key.pem -out decrypted_message.txt
theia@theia-nataschamart:/home/project$ openssl genpkey -algorithm RSA -out private_key.pem -pkeyopt rsa_keygen_bits:2048
openssl rsa -in private_key.pem -pubout -out public_key.pem
.+.....+....+..++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++*...+.....+.........+.+.....+....+..+.+.....++++++++++
+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++*.............+...+...+.......+...............+............+...+...+..........
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
.........+.+...............+........+.+......+......+..+..............+...+....++++++++++++++++++++++++++++++++++++++++++++++++++++
+++++++++++*.........+..+...+....+...+..++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++*..+........+.......+..
.....+..............+.+......+...+..+....+...+......+.....+......+......+...+.+...+.....+............+...+............+..+.+........
..+...+...+....+......+...+..+.......+.....+......+.......+..+...++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
writing RSA key
theia@theia-nataschamart:/home/project$ ||
```

Step 2: Create a New File


Problems
theia@theia-nataschamart: /home/project
theia@theia-nataschamart: /home/project
Follow lin
click)

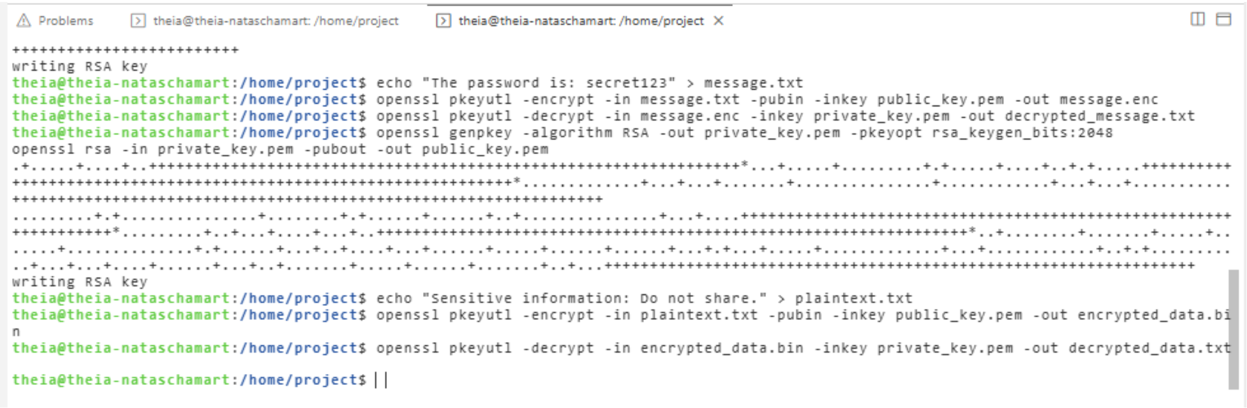
```
+.........+.....+....+................+.......++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++*.+..................
.....+.......+...+...........+.+.....+.........+....+..............+.......+.....+.................+.+..+.......+...+..+...+....+...+
........+...+....+..+....+......+.....+.........+....+...+..+...+...+.........+.............+.....+....+.....+.+..+.............+...+.
..........+......+....+.........+.....+.......+.........+...+.....+......+...............+...++++++++++++++++++++++++++++++++++++++++
+++++++++++++++++++++++++
writing RSA key
theia@theia-nataschamart:/home/project$ echo "The password is: secret123" > message.txt
theia@theia-nataschamart:/home/project$ openssl pkeyutl -encrypt -in message.txt -pubin -inkey public_key.pem -out message.enc
theia@theia-nataschamart:/home/project$ openssl pkeyutl -decrypt -in message.enc -inkey private_key.pem -out decrypted_message.txt
theia@theia-nataschamart:/home/project$ openssl genpkey -algorithm RSA -out private_key.pem -pkeyopt rsa_keygen_bits:2048
openssl rsa -in private_key.pem -pubout -out public_key.pem
.+.....+....+..++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++*...+.....+.........+.+.....+....+..+.+.....++++++++++
+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++*.............+...+...+.......+...............+............+...+...+..........
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
.........+.+...............+........+.+......+......+..+..............+...+....++++++++++++++++++++++++++++++++++++++++++++++++++++
+++++++++++*.........+..+...+....+...+..++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++*..+........+.......+..
.....+..............+.+......+...+..+....+...+......+.....+......+......+...+.+...+.....+............+...+............+..+.+........
..+...+...+....+......+...+..+.......+.....+......+.......+..+...++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
writing RSA key
theia@theia-nataschamart:/home/project$ echo "Sensitive information: Do not share." > plaintext.txt
theia@theia-nataschamart:/home/project$ 
```

Step 3: Encrypt the Message


Problems
theia@theia-nataschamart: /home/project
theia@theia-nataschamart: /home/project

```
........+...+....+..+....+......+.....+.........+....+...+..+...+...+.........+.............+.....+....+.....+.+..+.............+...+.
..........+......+....+.........+.....+.......+.........+...+.....+......+...............+...++++++++++++++++++++++++++++++++++++++++
+++++++++++++++++++++++++
writing RSA key
theia@theia-nataschamart:/home/project$ echo "The password is: secret123" > message.txt
theia@theia-nataschamart:/home/project$ openssl pkeyutl -encrypt -in message.txt -pubin -inkey public_key.pem -out message.enc
theia@theia-nataschamart:/home/project$ openssl pkeyutl -decrypt -in message.enc -inkey private_key.pem -out decrypted_message.txt
theia@theia-nataschamart:/home/project$ openssl genpkey -algorithm RSA -out private_key.pem -pkeyopt rsa_keygen_bits:2048
openssl rsa -in private_key.pem -pubout -out public_key.pem
.+.....+....+..++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++*...+.....+.........+.+.....+....+..+.+.....++++++++++
+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++*.............+...+...+.......+...............+............+...+...+..........
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
.........+.+...............+........+.+......+......+..+..............+...+....++++++++++++++++++++++++++++++++++++++++++++++++++++
+++++++++++*.........+..+...+....+...+..++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++*..+........+.......+......+..
.....+..............+.+......+...+..+....+...+......+.....+......+......+...+.+...+.....+............+...+............+..+.+........
..+...+...+....+......+...+..+.......+.....+......+.......+..+...++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
writing RSA key
theia@theia-nataschamart:/home/project$ echo "Sensitive information: Do not share." > plaintext.txt
theia@theia-nataschamart:/home/project$ openssl pkeyutl -encrypt -in plaintext.txt -pubin -inkey public_key.pem -out encrypted_data.bi
n
theia@theia-nataschamart:/home/project$ ||
```

Step 4: Decrypt the Encrypted Message:


Problems
theia@theia-nataschamart: /home/project
theia@theia-nataschamart: /home/project

```
+++++++++++++++++++++++++
writing RSA key
theia@theia-nataschamart:/home/project$ echo "The password is: secret123" > message.txt
theia@theia-nataschamart:/home/project$ openssl pkeyutl -encrypt -in message.txt -pubin -inkey public_key.pem -out message.enc
theia@theia-nataschamart:/home/project$ openssl pkeyutl -decrypt -in message.enc -inkey private_key.pem -out decrypted_message.txt
theia@theia-nataschamart:/home/project$ openssl genpkey -algorithm RSA -out private_key.pem -pkeyopt rsa_keygen_bits:2048
openssl rsa -in private_key.pem -pubout -out public_key.pem
.+.....+....+..+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++*...+.....+.........+.+.....+....+..+.+.....++++++++++
+++++++++++++++++++++++++++++++++++++++++++++++++++++++*.............+...+...+.......+...............+............+...+...+...........
+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
.........+.+...............+........+.+......+......+..+...............+...+....++++++++++++++++++++++++++++++++++++++++++++++++++++++
+++++++++++*.........+..+...+....+...+..+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++*..+........+.......+.....+..
.....+..............+.+......+...+..+....+...+......+.....+......+......+...+.+...+.....+.............+...+............+..+.+.........
..+...+...+....+......+...+..+.......+.....+......+.......+..+...+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
writing RSA key
theia@theia-nataschamart:/home/project$ echo "Sensitive information: Do not share." > plaintext.txt
theia@theia-nataschamart:/home/project$ openssl pkeyutl -encrypt -in plaintext.txt -pubin -inkey public_key.pem -out encrypted_data.bi
n
theia@theia-nataschamart:/home/project$ openssl pkeyutl -decrypt -in encrypted_data.bin -inkey private_key.pem -out decrypted_data.txt

theia@theia-nataschamart:/home/project$ ||
```