Workshop 4 – Public-Key Cryptography and RSA Encryption

Task 1: Review Important Concepts

1. What are the principal elements of a public-key encryption system?

   Answer:
   Public-key systems, do not have a key distribution problem, as is the case with symmetric encryption ciphers, this is because they use asymmetric encryption which does not have a shared symmetric key that is used for both encryption and decryption. Instead every recipient has a public key (e.g. for Alice and Bob, PU_{Alice} ,PU_{Bob}), as well as a private key (e.g. PR_{Alice}, PR_{Bob}). This implementation eliminates the need for a trusted third party to distribute keys to both parties, the reason for this is public keys can be shared, private keys are meant to be kept private. Encryption is carried out with the public keys and decryption is done with the corresponding private key.

   Users who want to have secure encrypted communication can exchange their public keys with others whom they wish to have a secure communication with.

   The second aspect of public key encryption systems is that the sender can sign a message using their private key to secure non-repudiation.

2. What are the roles of the public and private key in a public-key encryption system?

   Answer:
   The sender uses the public key of the receiver, so if Bob is sensing an encrypted message to Alice, he will encrypt using Alice's public key, PU_{Alice} . and the encrypted message can only be decrypted using Alice's private key, PR_{Alice}.

3. What are three broad categories of applications of public-key cryptosystems?

   Answer:
   The three broad categories are
   - Encryption/decryption
   - Digital signatures, and
   - Key exchange

   However, because public key cryptography is usually much slower, the best alternative to get the best of both secure encryption and speed is to use symmetric cryptography while using asymmetric cryptography to encrypt symmetric keys.

4. Why in public-key encryption systems, it should be infeasible to obtain private keys from the public keys.

   Answer:
   The strength and advantage of Public-key encryption techniques is the privacy of the private keys and the assurance that deriving the private key from the public key is computationally infeasible. This is what makes asymmetric key cryptography techniques powerful, it is because of the fact that the other party can hand their public keys to whomever that wants to establish secure and private communication with the other party without the concern for a third party to hand out secure keys to both participants.

   Private and public keys should be mathematically related but also be computationally infeasible to obtain one from, using the other key. For example in the RSA encryption scheme, two prime numbers are used to create the public and private key, the two keys *e* and *d* are related through the expression:

   $$ed \equiv 1 \left(mod\, \phi(n) \right)$$

   The two prime numbers used to produce the encryption and decryption keys are disposed after creating the encryption ($C = E(PU,M) = M^e \bmod n$) and decryption algorithm ($D(PR,C) = C^d \bmod n$). For this reason in the case of the RSA encryption scheme a private key cannot be obtained from a public key. As long as the attacker cannot find $\phi(n)$, the private key is kept hidden, for this it is advised to keep the prime numbers that determine $\phi(n)$ to have bit lengths of 1024.

5. Explain the encryption process and the decryption process of hybrid encryption?

   Answer:
   Hybrid encryption is when the sender (say Alice) uses the receiver's public key to encrypt a shared key for a symmetric cipher.

   Rather than sending the cipher text of the message, Alice encrypts the message using a symmetric key, and sends the ciphertext of the symmetric key using public key encryption.Alice sends and encrypted message using a symmetric cipher, the key for the symmetric cipher is encrypted using a public key and both are sent to the receiver (say Bob)

   Bob will decrypt the symmetric key using his private key. Using the shared symmetric key Bob can then decrypt the message ciphertext that was encrypted using symmetric cryptography.

   Hybrid encryption is where public key encryption is used to deliver a symmetric key to the destination using Public-Key cryptography. This is ideal because public-key encryption of large files is much slower than using symmetric key cryptography.

Task 2: Use an C Implementation of RSA Encryption

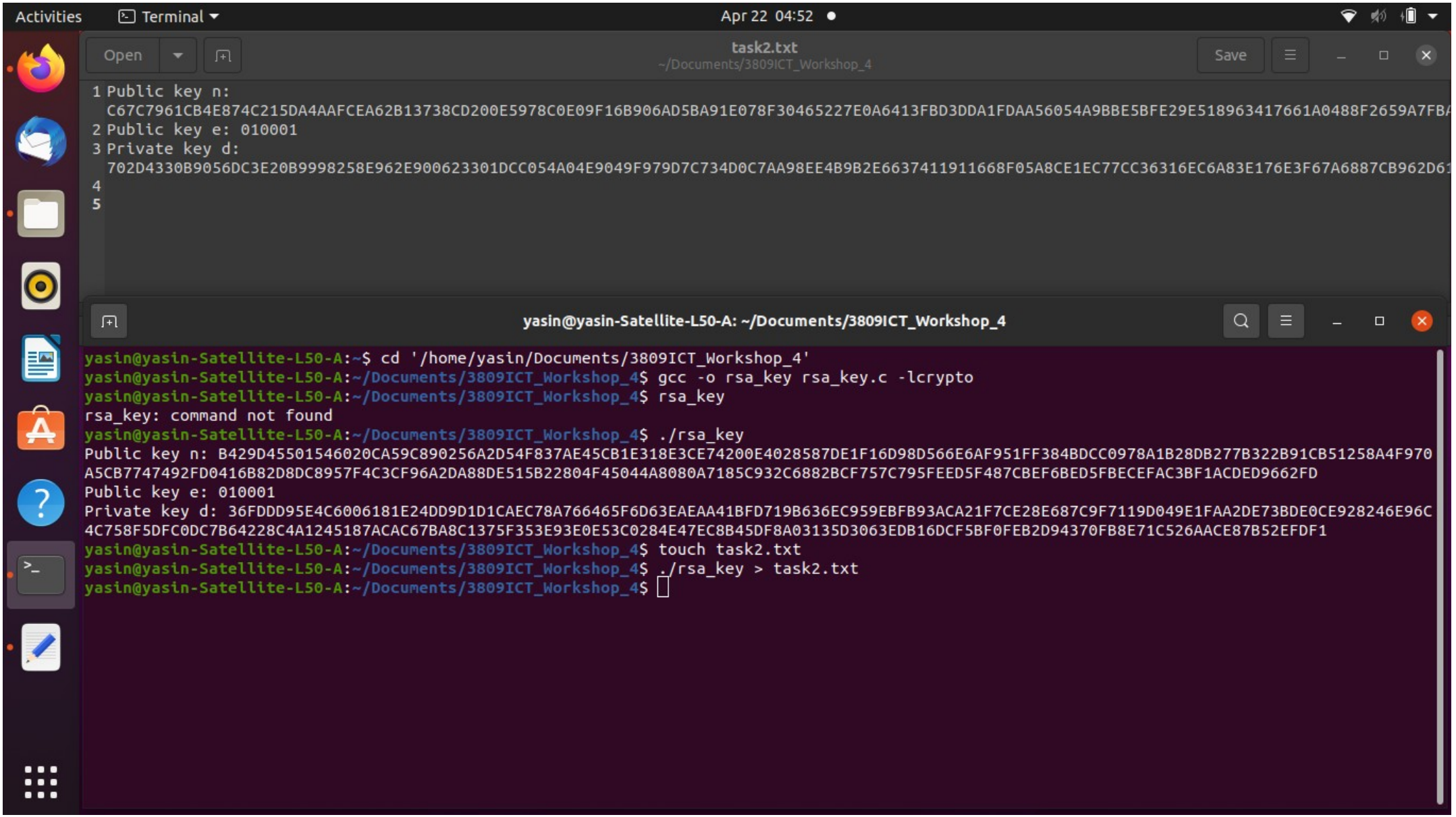
1. Please download the files rsa_key.c, rsa_enc.c and rsa_dec.c from the Week 5 folder on http://networksecurity.griffith.internal.

   We first compile the file rsa_key.c to get an executable rsa_key.

   ```
   $ gcc -o rsa_key rsa_key.c -lcrypto
   ```

   Running rsa_key, we get the public key (*e*, *n*) and private key *d*. Please take a screenshot showing the keys

   Answer:


Activities
Terminal
Apr 22 04:52
Open
task2.txt
~/Documents/3809ICT_Workshop_4
Save
1 Public key n:
C67C7961CB4E874C215DA4AAFCEA62B13738CD200E5978C0E09F16B906AD5BA91E078F30465227E0A6413FBD3DDA1FDAA56054A9BBE5BFE29E518963417661A0488F2659A7FBA
2 Public key e: 010001
3 Private key d:
702D4330B9056DC3E20B9998258E962E900623301DCC054A04E9049F979D7C734D0C7AA98EE4B9B2E6637411911668F05A8CE1EC77CC36316EC6A83E176E3F67A6887CB962D61
4
5
yasin@yasin-Satellite-L50-A: ~/Documents/3809ICT_Workshop_4
yasin@yasin-Satellite-L50-A:~$ cd '/home/yasin/Documents/3809ICT_Workshop_4'
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_4$ gcc -o rsa_key rsa_key.c -lcrypto
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_4$ rsa_key
rsa_key: command not found
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_4$ ./rsa_key
Public key n: B429D45501546020CA59C890256A2D54F837AE45CB1E318E3CE74200E4028587DE1F16D98D566E6AF951FF384BDCC0978A1B28DB277B322B91CB51258A4F970
A5CB7747492FD0416B82D8DC8957F4C3CF96A2DA88DE515B22804F45044A8080A7185C932C6882BCF757C795FEED5F487CBEF6BED5FBECEFAC3BF1ACDED9662FD
Public key e: 010001
Private key d: 36FDDD95E4C6006181E24DD9D1D1CAEC78A766465F6D63EAEAA41BFD719B636EC959EBFB93ACA21F7CE28E687C9F7119D049E1FAA2DE73BDE0CE928246E96C
4C758F5DFC0DC7B64228C4A1245187ACAC67BA8C1375F353E93E0E53C0284E47EC8B45DF8A03135D3063EDB16DCF5BF0FEB2D94370FB8E71C526AACE87B52EFDF1
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_4$ touch task2.txt
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_4$ ./rsa_key > task2.txt
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_4$

2. Let's encrypt your name using rsa_enc.c. First, we need to encode your message into an integer represented in the hexadecimal form. To do so, run

```
$ echo -n "XXXX" | xxd -ps
```

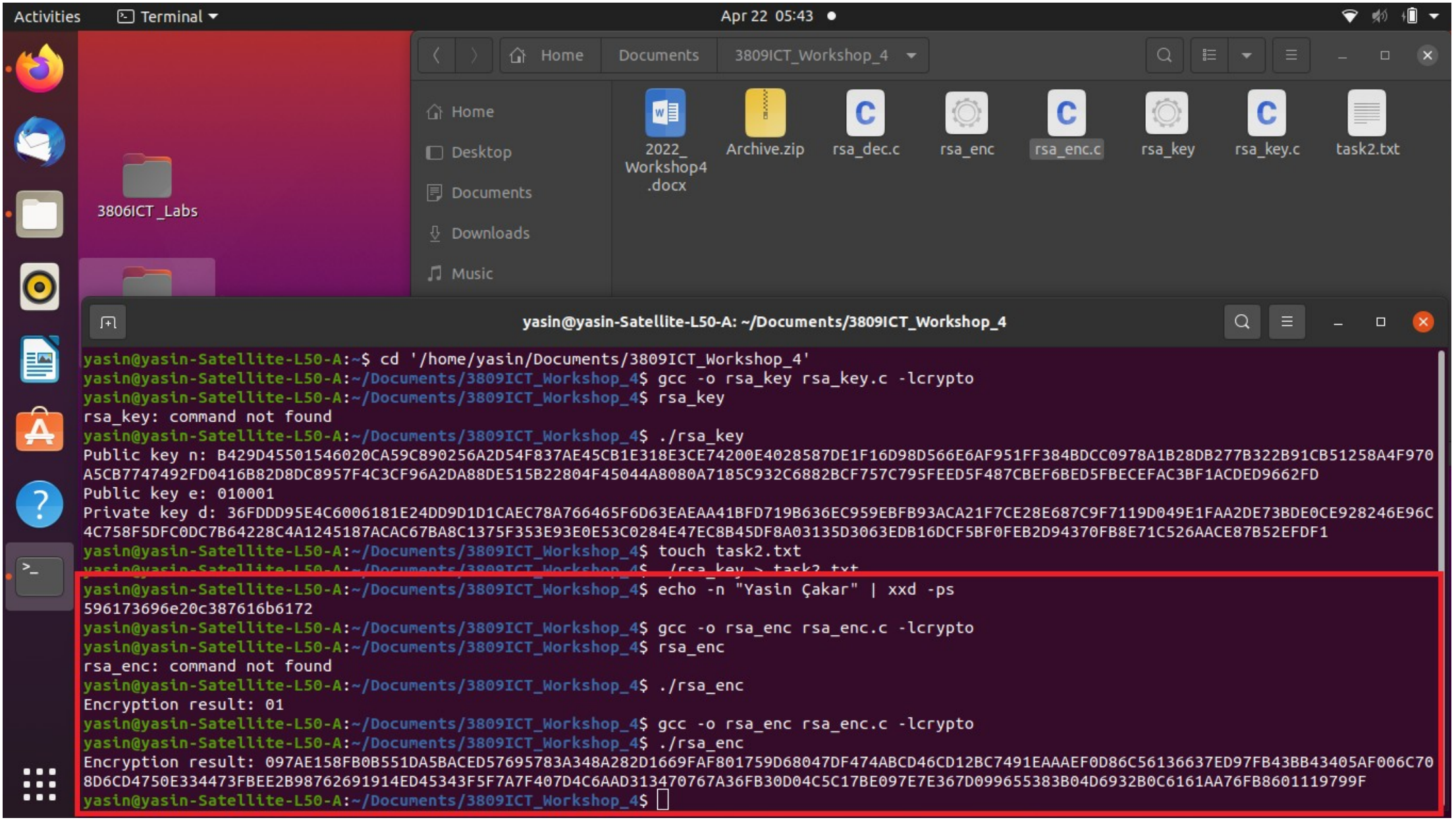
where "XXXX" is your name. The output is set as the plaintext *M*.

Edit the file rsa_enc.c by setting the values for parameters "*n*", "*e*", "*M*" we obtained. Then, compile the file to get an executable and run it:

```
$ gcc -o rsa_enc rsa_enc.c -lcrypto
$ rsa_enc
```

The ciphertext is displayed. Please take a screenshot of the ciphertext.

Answer:


Activities
Terminal
Apr 22 05:43
Home
Documents
3809ICT_Workshop_4
Home
Desktop
Documents
Downloads
Music
2022_ Workshop4 .docx
Archive.zip
rsa_dec.c
rsa_enc
rsa_enc.c
rsa_key
rsa_key.c
task2.txt
3806ICT_Labs
yasin@yasin-Satellite-L50-A: ~/Documents/3809ICT_Workshop_4
yasin@yasin-Satellite-L50-A:~$ cd '/home/yasin/Documents/3809ICT_Workshop_4'
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_4$ gcc -o rsa_key rsa_key.c -lcrypto
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_4$ rsa_key
rsa_key: command not found
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_4$ ./rsa_key
Public key n: B429D45501546020CA59C890256A2D54F837AE45CB1E318E3CE74200E4028587DE1F16D98D566E6AF951FF384BDCC0978A1B28DB277B322B91CB51258A4F970
A5CB7747492FD0416B82D8DC8957F4C3CF96A2DA88DE515B22804F45044A8080A7185C932C6882BCF757C795FEED5F487CBEF6BED5FBECEFAC3BF1ACDED9662FD
Public key e: 010001
Private key d: 36FDDD95E4C6006181E24DD9D1D1CAEC78A766465F6D63EAEAA41BFD719B636EC959EBFB93ACA21F7CE28E687C9F7119D049E1FAA2DE73BDE0CE928246E96C
4C758F5DFC0DC7B64228C4A1245187ACAC67BA8C1375F353E93E0E53C0284E47EC8B45DF8A03135D3063EDB16DCF5BF0FEB2D94370FB8E71C526AACE87B52EFDF1
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_4$ touch task2.txt
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_4$ echo -n "Yasin Çakar" | xxd -ps
596173696e20c387616b6172
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_4$ gcc -o rsa_enc rsa_enc.c -lcrypto
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_4$ rsa_enc
rsa_enc: command not found
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_4$ ./rsa_enc
Encryption result: 01
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_4$ gcc -o rsa_enc rsa_enc.c -lcrypto
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_4$ ./rsa_enc
Encryption result: 097AE158FB0B551DA5BACED57695783A348A282D1669FAF801759D68047DF474ABCD46CD12BC7491EAAAEF0D86C56136637ED97FB43BB43405AF006C70
8D6CD4750E334473FBEE2B98762691914ED45343F5F7A7F407D4C6AAD313470767A36FB30D04C5C17BE097E7E367D099655383B04D6932B0C6161AA76FB8601119799F
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_4$

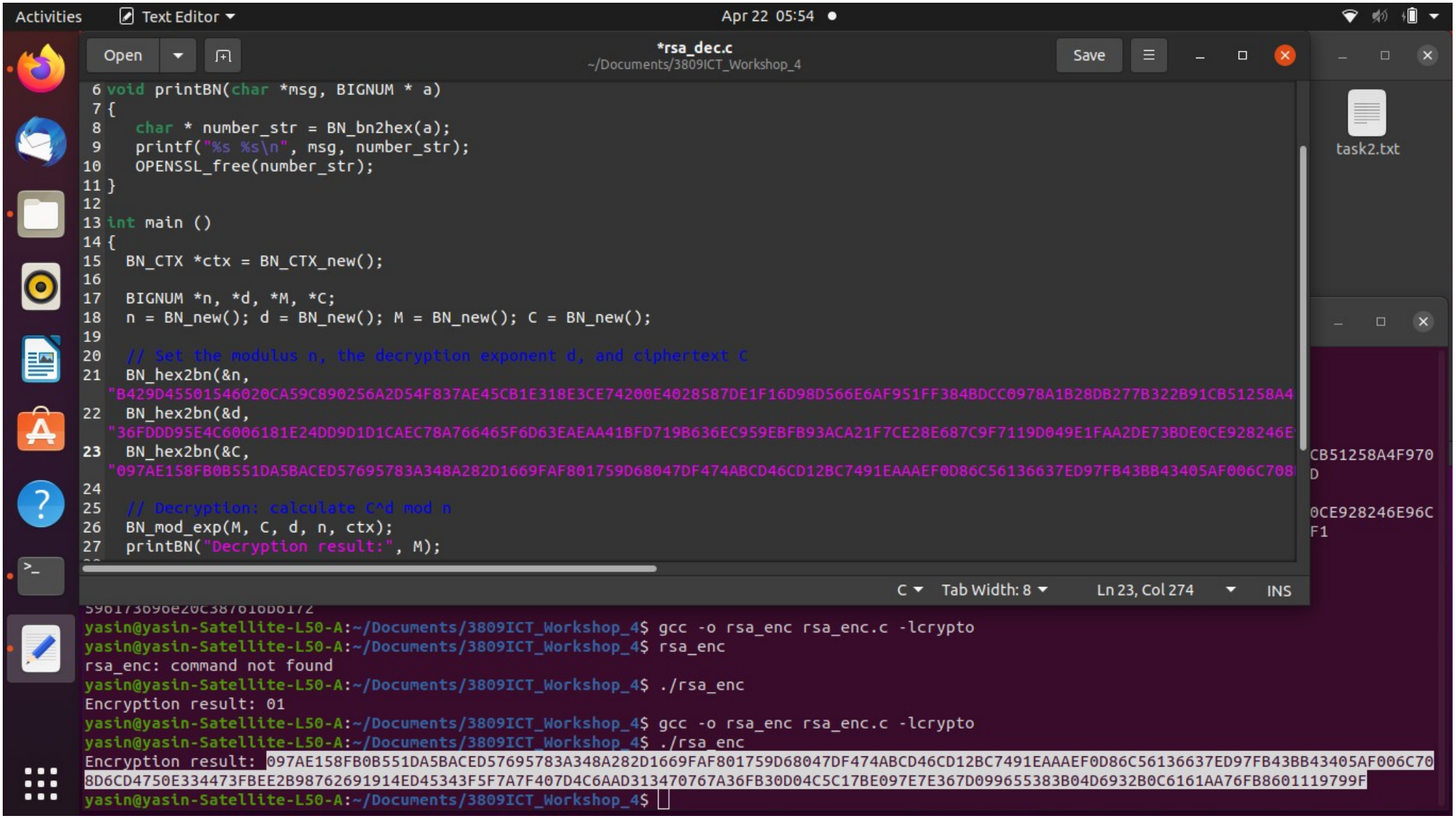
3. Denote the ciphertext by *C*. Edit the file rsa_dec.c by setting the values for parameters "*n*", "*d*", "*C*". Compile the edited rsa_dec.c and run the executable to get recover the hexadecimal encoding of the plaintext.

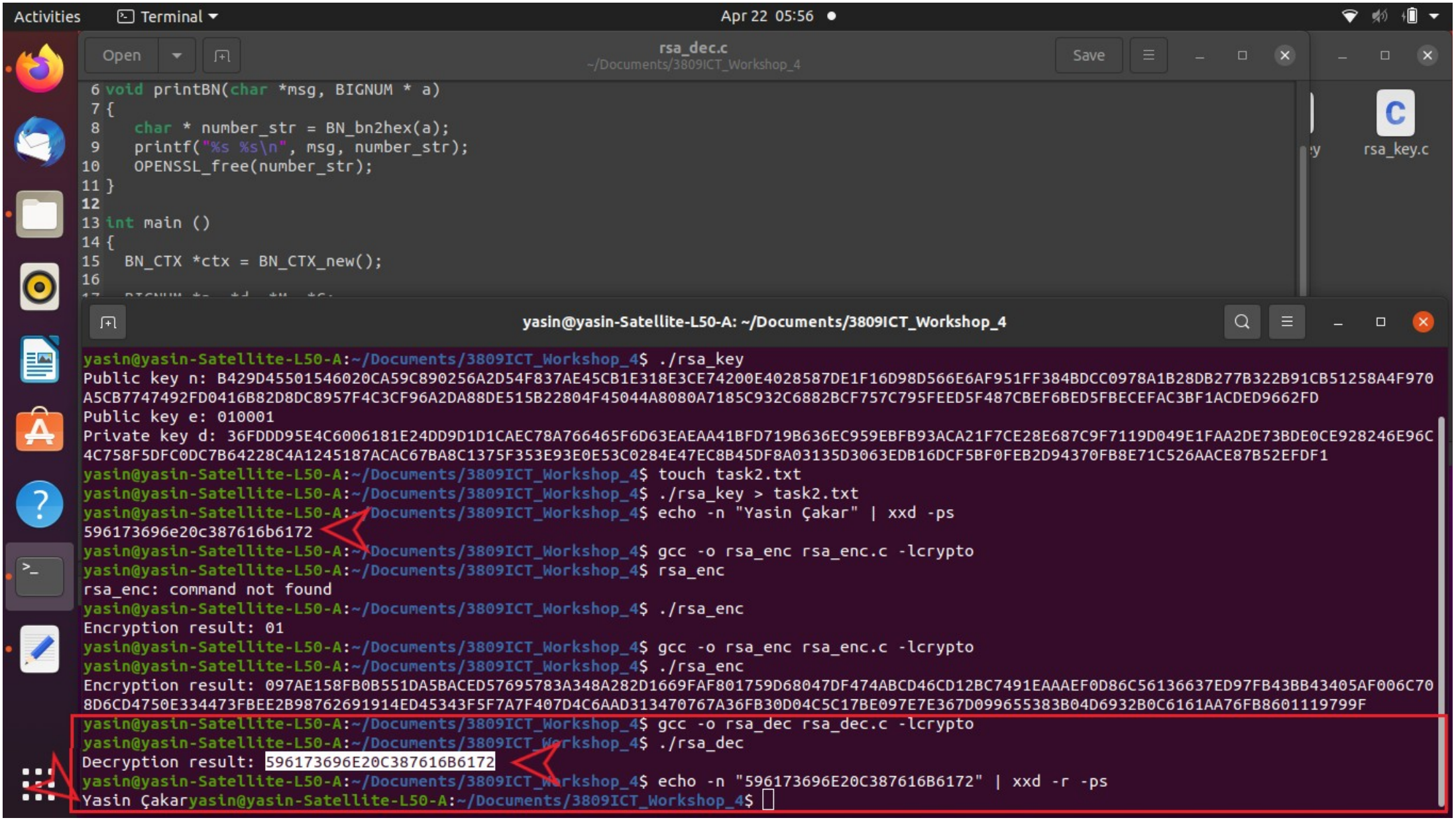
```
$ gcc -o rsa_dec rsa_dec.c -lcrypto
$ rsa_dec
```

Decode it and compare with your name (YYYY is the hexadecimal encoding).

```
$ echo -n YYYY | xxd -r -ps
```

Answer:


Activities
Text Editor
Apr 22 05:54
Open
*rsa_dec.c
~/Documents/3809ICT_Workshop_4
Save
task2.txt
void printBN(char *msg, BIGNUM * a)
{
char * number_str = BN_bn2hex(a);
printf("%s %s\n", msg, number_str);
OPENSSL_free(number_str);
}
int main ()
{
BN_CTX *ctx = BN_CTX_new();
BIGNUM *n, *d, *M, *C;
n = BN_new(); d = BN_new(); M = BN_new(); C = BN_new();
// Set the modulus n, the decryption exponent d, and ciphertext C
BN_hex2bn(&n,
"B429D45501546020CA59C890256A2D54F837AE45CB1E318E3CE74200E4028587DE1F16D98D566E6AF951FF384BDCC0978A1B28DB277B322B91CB51258A4
BN_hex2bn(&d,
"36FDDD95E4C6006181E24DD9D1D1CAEC78A766465F6D63EAEAA41BFD719B636EC959EBFB93ACA21F7CE28E687C9F7119D049E1FAA2DE73BDE0CE928246E
BN_hex2bn(&C,
"097AE158FB0B551DA5BACED57695783A348A282D1669FAF801759D68047DF474ABCD46CD12BC7491EAAAEF0D86C56136637ED97FB43BB43405AF006C708
// Decryption: calculate C^d mod n
BN_mod_exp(M, C, d, n, ctx);
printBN("Decryption result:", M);
C
Tab Width: 8
Ln 23, Col 274
INS
CB51258A4F970
D
0CE928246E96C
F1
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_4$ gcc -o rsa_enc rsa_enc.c -lcrypto
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_4$ rsa_enc
rsa_enc: command not found
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_4$ ./rsa_enc
Encryption result: 01
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_4$ gcc -o rsa_enc rsa_enc.c -lcrypto
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_4$ ./rsa_enc
Encryption result: 097AE158FB0B551DA5BACED57695783A348A282D1669FAF801759D68047DF474ABCD46CD12BC7491EAAAEF0D86C56136637ED97FB43BB43405AF006C70
8D6CD4750E334473FBEE2B98762691914ED45343F5F7A7F407D4C6AAD313470767A36FB30D04C5C17BE097E7E367D099655383B04D6932B0C6161AA76FB8601119799F
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_4$


Activities
Terminal
Apr 22 05:56
Open
rsa_dec.c
~/Documents/3809ICT_Workshop_4
Save
rsa_key.c
yasin@yasin-Satellite-L50-A: ~/Documents/3809ICT_Workshop_4
6 void printBN(char *msg, BIGNUM * a)
7 {
8 char * number_str = BN_bn2hex(a);
9 printf("%s %s\n", msg, number_str);
10 OPENSSL_free(number_str);
11 }
12
13 int main ()
14 {
15 BN_CTX *ctx = BN_CTX_new();
16
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_4$ ./rsa_key
Public key n: B429D45501546020CA59C890256A2D54F837AE45CB1E318E3CE74200E4028587DE1F16D98D566E6AF951FF384BDCC0978A1B28DB277B322B91CB51258A4F970
A5CB7747492FD0416B82D8DC8957F4C3CF96A2DA88DE515B22804F45044A8080A7185C932C6882BCF757C795FEED5F487CBEF6BED5FBECEFAC3BF1ACDED9662FD
Public key e: 010001
Private key d: 36FDDD95E4C6006181E24DD9D1D1CAEC78A766465F6D63EAEAA41BFD719B636EC959EBFB93ACA21F7CE28E687C9F7119D049E1FAA2DE73BDE0CE928246E96C
4C758F5DFC0DC7B64228C4A1245187ACAC67BA8C1375F353E93E0E53C0284E47EC8B45DF8A03135D3063EDB16DCF5BF0FEB2D94370FB8E71C526AACE87B52EFDF1
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_4$ touch task2.txt
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_4$ ./rsa_key > task2.txt
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_4$ echo -n "Yasin Çakar" | xxd -ps
596173696e20c387616b6172
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_4$ gcc -o rsa_enc rsa_enc.c -lcrypto
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_4$ rsa_enc
rsa_enc: command not found
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_4$ ./rsa_enc
Encryption result: 01
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_4$ gcc -o rsa_enc rsa_enc.c -lcrypto
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_4$ ./rsa_enc
Encryption result: 097AE158FB0B551DA5BACED57695783A348A282D1669FAF801759D68047DF474ABCD46CD12BC7491EAAAEF0D86C56136637ED97FB43BB43405AF006C70
8D6CD4750E334473FBEE2B98762691914ED45343F5F7A7F407D4C6AAD313470767A36FB30D04C5C17BE097E7E367D099655383B04D6932B0C6161AA76FB8601119799F
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_4$ gcc -o rsa_dec rsa_dec.c -lcrypto
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_4$ ./rsa_dec
Decryption result: 596173696E20C387616B6172
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_4$ echo -n "596173696E20C387616B6172" | xxd -r -ps
Yasin Çakaryasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_4$

Task 3: Use RSA Tools from OpenSSL

In this task, we perform RSA operations using OpenSSL.

1. We first generate an RSA public/private key pair. We specify the modulo number n to be 2048 bits, which is recommended for Internet security communication. Below the option aes128 means we will use AES with 128-bit keys to encrypt the public/private key pair, so they can be securely store locally. If you do not specify this option, the public/private key file is not encrypted.

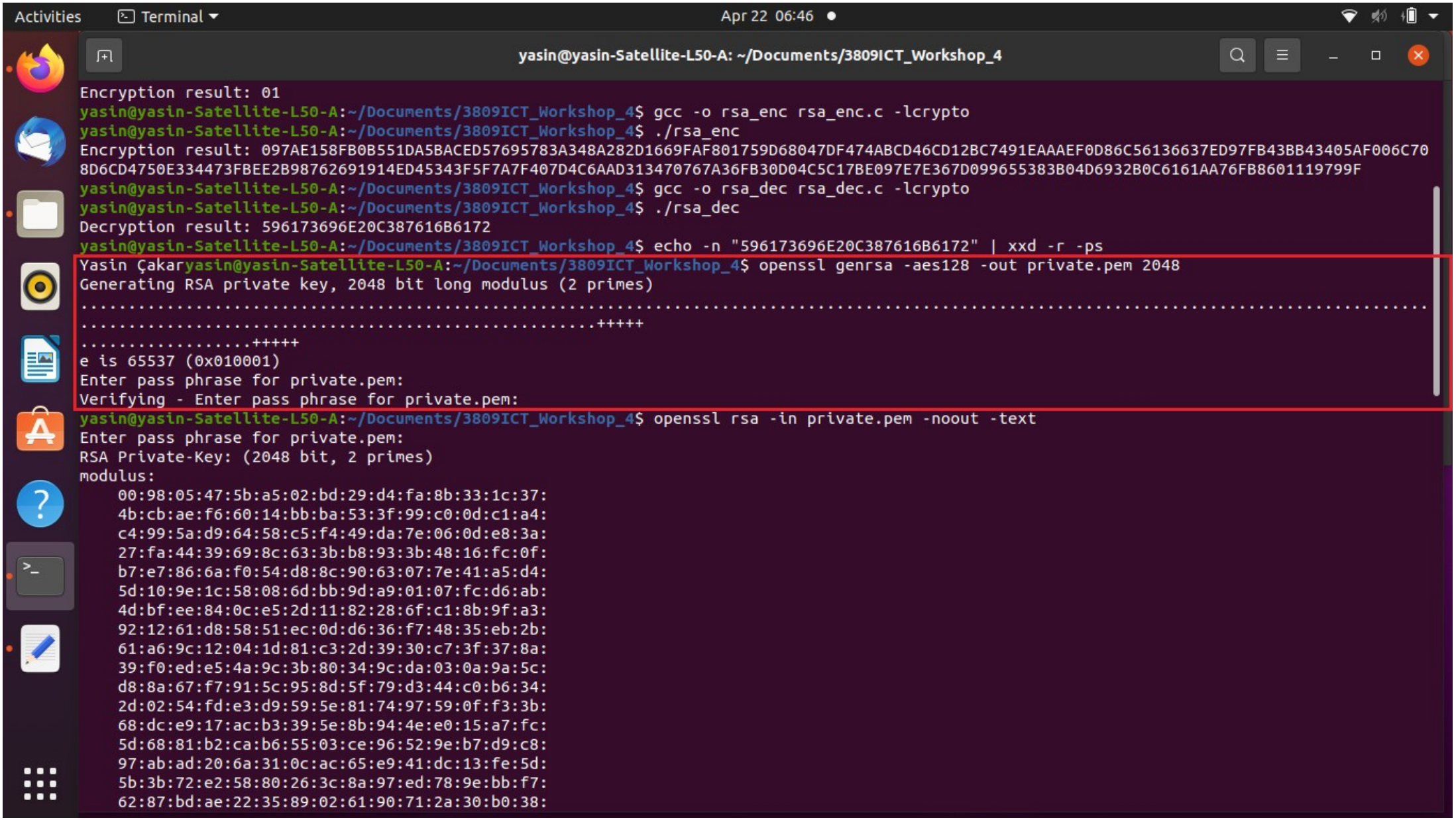
   ```
   $ openssl genrsa -aes128 -out private.pem 2048
   ```

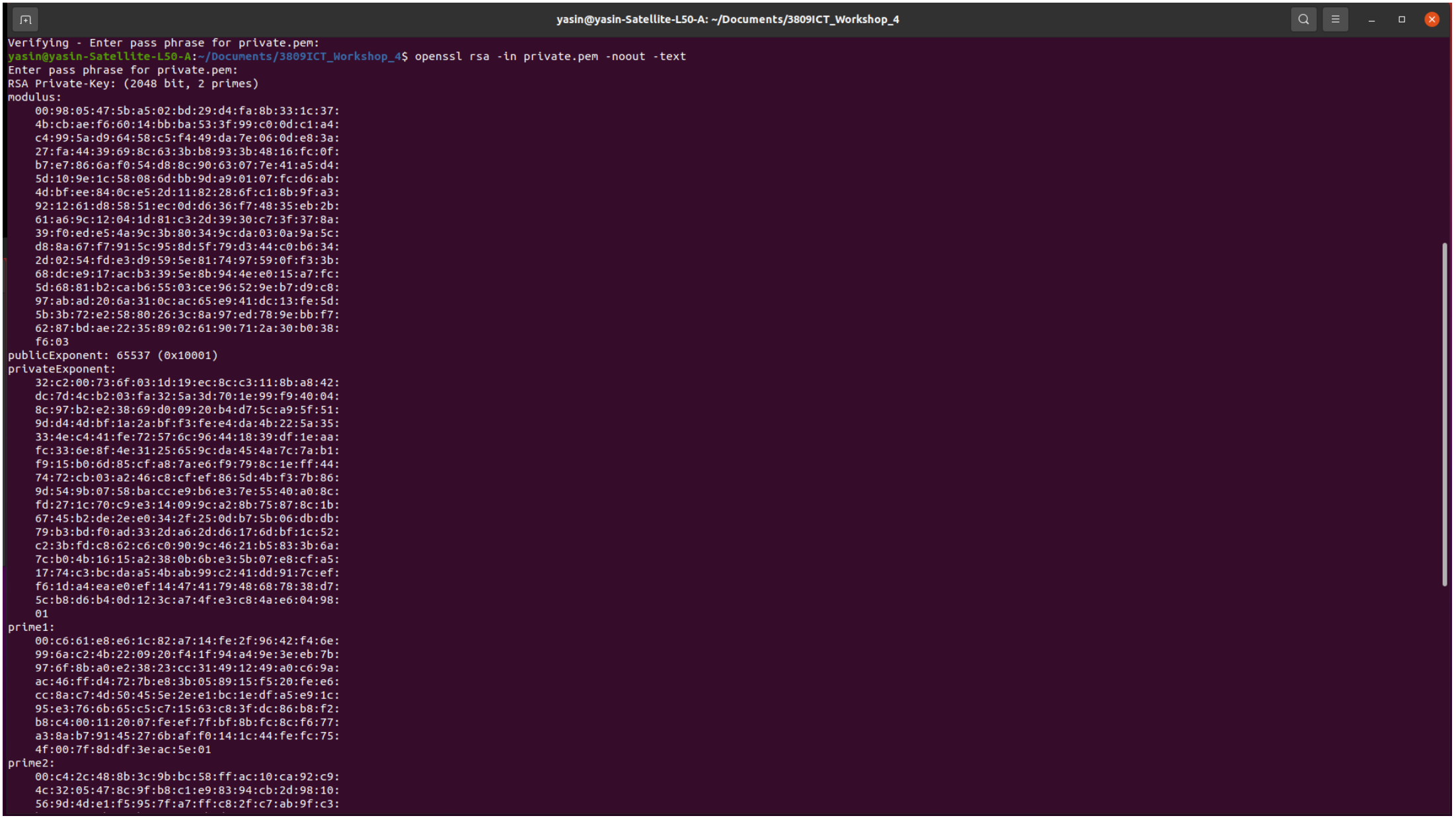
   You will be asked to entre a passphrase (password). The passphrase is used to generate an AES key, which will then be used to encryption the public/private key file private.pem. As discussed in Task 4 of Workshop 3. This passphrase needs to be strong enough. Part of the file private.pem is encoded by Distiguished Encoding Rules (DER). We can view the public/private key file.

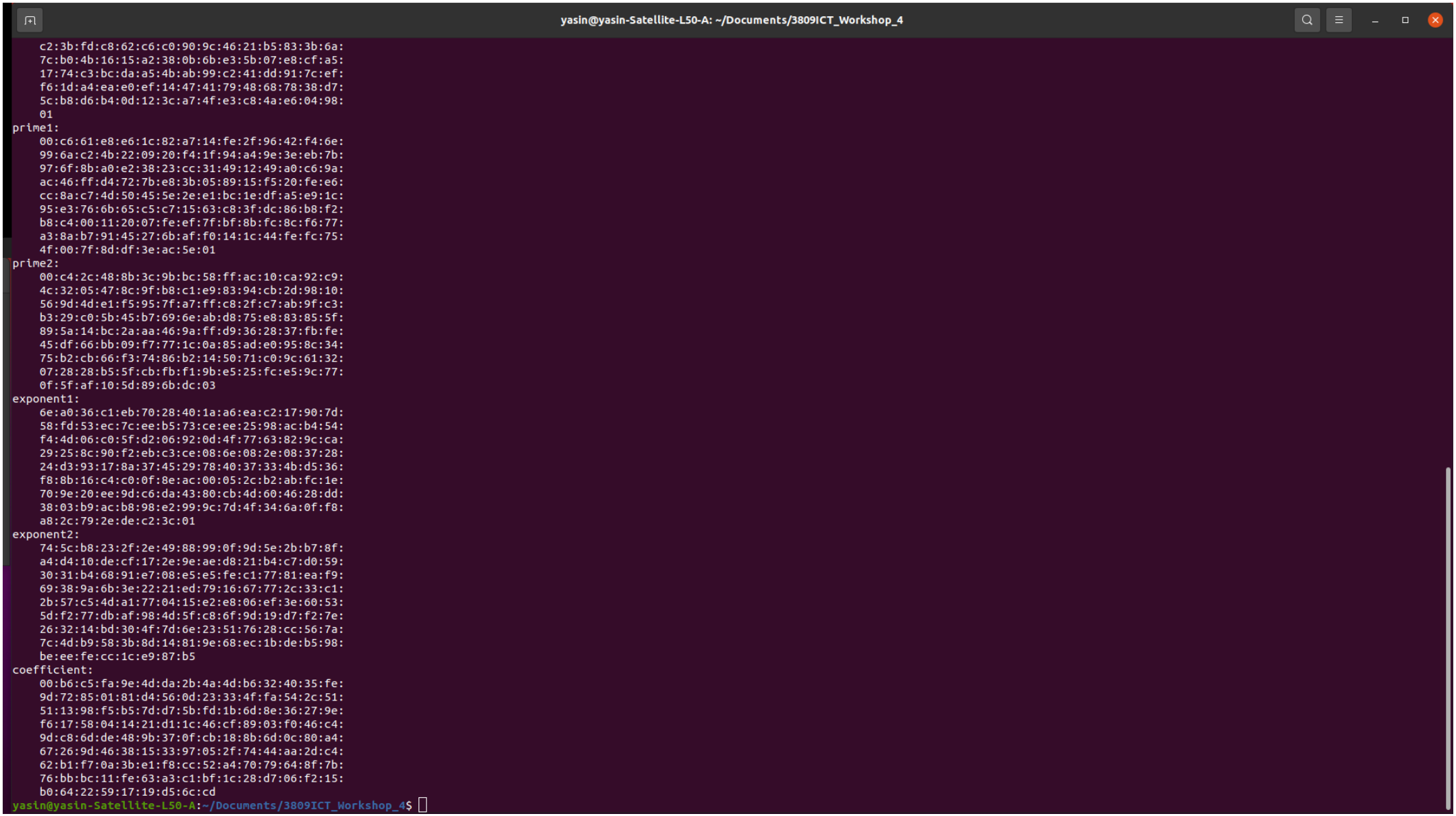
   ```
   $ openssl rsa -in private.pem -noout -text
   ```

   Q: What are the values of the private key (d, n) and public key (e, n)?

   Answer:


Activities
Terminal
Apr 22 06:46
yasin@yasin-Satellite-L50-A: ~/Documents/3809ICT_Workshop_4
Encryption result: 01
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_4$ gcc -o rsa_enc rsa_enc.c -lcrypto
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_4$ ./rsa_enc
Encryption result: 097AE158FB0B551DA5BACED57695783A348A282D1669FAF801759D68047DF474ABCD46CD12BC7491EAAAEF0D86C56136637ED97FB43BB43405AF006C70
8D6CD4750E334473FBEE2B98762691914ED45343F5F7A7F407D4C6AAD313470767A36FB30D04C5C17BE097E7E367D099655383B04D6932B0C6161AA76FB8601119799F
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_4$ gcc -o rsa_dec rsa_dec.c -lcrypto
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_4$ ./rsa_dec
Decryption result: 596173696E20C387616B6172
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_4$ echo -n "596173696E20C387616B6172" | xxd -r -ps
Yasin Çakaryasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_4$ openssl genrsa -aes128 -out private.pem 2048
Generating RSA private key, 2048 bit long modulus (2 primes)
.....
.....+++++
.....+++++
e is 65537 (0x010001)
Enter pass phrase for private.pem:
Verifying - Enter pass phrase for private.pem:
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_4$ openssl rsa -in private.pem -noout -text
Enter pass phrase for private.pem:
RSA Private-Key: (2048 bit, 2 primes)
modulus:
00:98:05:47:5b:a5:02:bd:29:d4:fa:8b:33:1c:37:
4b:cb:ae:f6:60:14:bb:ba:53:3f:99:c0:0d:c1:a4:
c4:99:5a:d9:64:58:c5:f4:49:da:7e:06:0d:e8:3a:
27:fa:44:39:69:8c:63:3b:b8:93:3b:48:16:fc:0f:
b7:e7:86:6a:f0:54:d8:8c:90:63:07:7e:41:a5:d4:
5d:10:9e:1c:58:08:6d:bb:9d:a9:01:07:fc:d6:ab:
4d:bf:ee:84:0c:e5:2d:11:82:28:6f:c1:8b:9f:a3:
92:12:61:d8:58:51:ec:0d:d6:36:f7:48:35:eb:2b:
61:a6:9c:12:04:1d:81:c3:2d:39:30:c7:3f:37:8a:
39:f0:ed:e5:4a:9c:3b:80:34:9c:da:03:0a:9a:5c:
d8:8a:67:f7:91:5c:95:8d:5f:79:d3:44:c0:b6:34:
2d:02:54:fd:e3:d9:59:5e:81:74:97:59:0f:f3:3b:
68:dc:e9:17:ac:b3:39:5e:8b:94:4e:e0:15:a7:fc:
5d:68:81:b2:ca:b6:55:03:ce:96:52:9e:b7:d9:c8:
97:ab:ad:20:6a:31:0c:ac:65:e9:41:dc:13:fe:5d:
5b:3b:72:e2:58:80:26:3c:8a:97:ed:78:9e:bb:f7:
62:87:bd:ae:22:35:89:02:61:90:71:2a:30:b0:38:


yasin@yasin-Satellite-L50-A: ~/Documents/3809ICT_Workshop_4
Verifying - Enter pass phrase for private.pem:
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_4$ openssl rsa -in private.pem -noout -text
Enter pass phrase for private.pem:
RSA Private-Key: (2048 bit, 2 primes)
modulus:
00:98:05:47:5b:a5:02:bd:29:d4:fa:8b:33:1c:37:
4b:cb:ae:f6:60:14:bb:ba:53:3f:99:c0:0d:c1:a4:
c4:99:5a:d9:64:58:c5:f4:49:da:7e:06:0d:e8:3a:
27:fa:44:39:69:8c:63:3b:b8:93:3b:48:16:fc:0f:
b7:e7:86:6a:f0:54:d8:8c:90:63:07:7e:41:a5:d4:
5d:10:9e:1c:58:08:6d:bb:9d:a9:01:07:fc:d6:ab:
4d:bf:ee:84:0c:e5:2d:11:82:28:6f:c1:8b:9f:a3:
92:12:61:d8:58:51:ec:0d:d6:36:f7:48:35:eb:2b:
61:a6:9c:12:04:1d:81:c3:2d:39:30:c7:3f:37:8a:
39:f0:ed:e5:4a:9c:3b:80:34:9c:da:03:0a:9a:5c:
d8:8a:67:f7:91:5c:95:8d:5f:79:d3:44:c0:b6:34:
2d:02:54:fd:e3:d9:59:5e:81:74:97:59:0f:f3:3b:
68:dc:e9:17:ac:b3:39:5e:8b:94:4e:e0:15:a7:fc:
5d:68:81:b2:ca:b6:55:03:ce:96:52:9e:b7:d9:c8:
97:ab:ad:20:6a:31:0c:ac:65:e9:41:dc:13:fe:5d:
5b:3b:72:e2:58:80:26:3c:8a:97:ed:78:9e:bb:f7:
62:87:bd:ae:22:35:89:02:61:90:71:2a:30:b0:38:
f6:03
publicExponent: 65537 (0x10001)
privateExponent:
32:c2:00:73:6f:03:1d:19:ec:8c:c3:11:8b:a8:42:
dc:7d:4c:b2:03:fa:32:5a:3d:70:1e:99:f9:40:04:
8c:97:b2:e2:38:69:d0:09:20:b4:d7:5c:a9:5f:51:
9d:d4:4d:bf:1a:2a:bf:f3:fe:e4:da:4b:22:5a:35:
33:4e:c4:41:fe:72:57:6c:96:44:18:39:df:1e:aa:
fc:33:6e:8f:4e:31:25:65:9c:da:45:4a:7c:7a:b1:
f9:15:b0:6d:85:cf:a8:7a:e6:f9:79:8c:1e:ff:44:
74:72:cb:03:a2:46:c8:cf:ef:86:5d:4b:f3:7b:86:
9d:54:9b:07:58:ba:cc:e9:b6:e3:7e:55:40:a0:8c:
fd:27:1c:70:c9:e3:14:09:9c:a2:8b:75:87:8c:1b:
67:45:b2:de:2e:e0:34:2f:25:0d:b7:5b:06:db:db:
79:b3:bd:f0:ad:33:2d:a6:2d:d6:17:6d:bf:1c:52:
c2:3b:fd:c8:62:c6:c0:90:9c:46:21:b5:83:3b:6a:
7c:b0:4b:16:15:a2:38:0b:6b:e3:5b:07:e8:cf:a5:
17:74:c3:bc:da:a5:4b:ab:99:c2:41:dd:91:7c:ef:
f6:1d:a4:ea:e0:ef:14:47:41:79:48:68:78:38:d7:
5c:b8:d6:b4:0d:12:3c:a7:4f:e3:c8:4a:e6:04:98:
01
prime1:
00:c6:61:e8:e6:1c:82:a7:14:fe:2f:96:42:f4:6e:
99:6a:c2:4b:22:09:20:f4:1f:94:a4:9e:3e:eb:7b:
97:6f:8b:a0:e2:38:23:cc:31:49:12:49:a0:c6:9a:
ac:46:ff:d4:72:7b:e8:3b:05:89:15:f5:20:fe:e6:
cc:8a:c7:4d:50:45:5e:2e:e1:bc:1e:df:a5:e9:1c:
95:e3:76:6b:65:c5:c7:15:63:c8:3f:dc:86:b8:f2:
b8:c4:00:11:20:07:fe:ef:7f:bf:8b:fc:8c:f6:77:
a3:8a:b7:91:45:27:6b:af:f0:14:1c:44:fe:fc:75:
4f:00:7f:8d:df:3e:ac:5e:01
prime2:
00:c4:2c:48:8b:3c:9b:bc:58:ff:ac:10:ca:92:c9:
4c:32:05:47:8c:9f:b8:c1:e9:83:94:cb:2d:98:10:
56:9d:4d:e1:f5:95:7f:a7:ff:c8:2f:c7:ab:9f:c3:


yasin@yasin-Satellite-L50-A: ~/Documents/3809ICT_Workshop_4
c2:3b:fd:c8:62:c6:c0:90:9c:46:21:b5:83:3b:6a:
7c:b0:4b:16:15:a2:38:0b:6b:e3:5b:07:e8:cf:a5:
17:74:c3:bc:da:a5:4b:ab:99:c2:41:dd:91:7c:ef:
f6:1d:a4:ea:e0:ef:14:47:41:79:48:68:78:38:d7:
5c:b8:d6:b4:0d:12:3c:a7:4f:e3:c8:4a:e6:04:98:
01
prime1:
00:c6:61:e8:e6:1c:82:a7:14:fe:2f:96:42:f4:6e:
99:6a:c2:4b:22:09:20:f4:1f:94:a4:9e:3e:eb:7b:
97:6f:8b:a0:e2:38:23:cc:31:49:12:49:a0:c6:9a:
ac:46:ff:d4:72:7b:e8:3b:05:89:15:f5:20:fe:e6:
cc:8a:c7:4d:50:45:5e:2e:e1:bc:1e:df:a5:e9:1c:
95:e3:76:6b:65:c5:c7:15:63:c8:3f:dc:86:b8:f2:
b8:c4:00:11:20:07:fe:ef:7f:bf:8b:fc:8c:f6:77:
a3:8a:b7:91:45:27:6b:af:f0:14:1c:44:fe:fc:75:
4f:00:7f:8d:df:3e:ac:5e:01
prime2:
00:c4:2c:48:8b:3c:9b:bc:58:ff:ac:10:ca:92:c9:
4c:32:05:47:8c:9f:b8:c1:e9:83:94:cb:2d:98:10:
56:9d:4d:e1:f5:95:7f:a7:ff:c8:2f:c7:ab:9f:c3:
b3:29:c0:5b:45:b7:69:6e:ab:d8:75:e8:83:85:5f:
89:5a:14:bc:2a:aa:46:9a:ff:d9:36:28:37:fb:fe:
45:df:66:bb:09:f7:77:1c:0a:85:ad:e0:95:8c:34:
75:b2:cb:66:f3:74:86:b2:14:50:71:c0:9c:61:32:
07:28:28:b5:5f:cb:fb:f1:9b:e5:25:fc:e5:9c:77:
0f:5f:af:10:5d:89:6b:dc:03
exponent1:
6e:a0:36:c1:eb:70:28:40:1a:a6:ea:c2:17:90:7d:
58:fd:53:ec:7c:ee:b5:73:ce:ee:25:98:ac:b4:54:
f4:4d:06:c0:5f:d2:06:92:0d:4f:77:63:82:9c:ca:
29:25:8c:90:f2:eb:c3:ce:08:6e:08:2e:08:37:28:
24:d3:93:17:8a:37:45:29:78:40:37:33:4b:d5:36:
f8:8b:16:c4:c0:0f:8e:ac:00:05:2c:b2:ab:fc:1e:
70:9e:20:ee:9d:c6:da:43:80:cb:4d:60:46:28:dd:
38:03:b9:ac:b8:98:e2:99:9c:7d:4f:34:6a:0f:f8:
a8:2c:79:2e:de:c2:3c:01
exponent2:
74:5c:b8:23:2f:2e:49:88:99:0f:9d:5e:2b:b7:8f:
a4:d4:10:de:cf:17:2e:9e:ae:d8:21:b4:c7:d0:59:
30:31:b4:68:91:e7:08:e5:e5:fe:c1:77:81:ea:f9:
69:38:9a:6b:3e:22:21:ed:79:16:67:77:2c:33:c1:
2b:57:c5:4d:a1:77:04:15:e2:e8:06:ef:3e:60:53:
5d:f2:77:db:af:98:4d:5f:c8:6f:9d:19:d7:f2:7e:
26:32:14:bd:30:4f:7d:6e:23:51:76:28:cc:56:7a:
7c:4d:b9:58:3b:8d:14:81:9e:68:ec:1b:de:b5:98:
be:ee:fe:cc:1c:e9:87:b5
coefficient:
00:b6:c5:fa:9e:4d:da:2b:4a:4d:b6:32:40:35:fe:
9d:72:85:01:81:d4:56:0d:23:33:4f:fa:54:2c:51:
51:13:98:f5:b5:7d:d7:5b:fd:1b:6d:8e:36:27:9e:
f6:17:58:04:14:21:d1:1c:46:cf:89:03:f0:46:c4:
9d:c8:6d:de:48:9b:37:0f:cb:18:8b:6d:0c:80:a4:
67:26:9d:46:38:15:33:97:05:2f:74:44:aa:2d:c4:
62:b1:f7:0a:3b:e1:f8:cc:52:a4:70:79:64:8f:7b:
76:bb:bc:11:fe:63:a3:c1:bf:1c:28:d7:06:f2:15:
b0:64:22:59:17:19:d5:6c:cd
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_4$

private key (*d*, *n*)

d =

privateExponent:
32:c2:00:73:6f:03:1d:19:ec:8c:c3:11:8b:a8:42:
dc:7d:4c:b2:03:fa:32:5a:3d:70:1e:99:f9:40:04:
8c:97:b2:e2:38:69:d0:09:20:b4:d7:5c:a9:5f:51:
9d:d4:4d:bf:1a:2a:bf:f3:fe:e4:da:4b:22:5a:35:
33:4e:c4:41:fe:72:57:6c:96:44:18:39:df:1e:aa:
fc:33:6e:8f:4e:31:25:65:9c:da:45:4a:7c:7a:b1:
f9:15:b0:6d:85:cf:a8:7a:e6:f9:79:8c:1e:ff:44:
74:72:cb:03:a2:46:c8:cf:ef:86:5d:4b:f3:7b:86:
9d:54:9b:07:58:ba:cc:e9:b6:e3:7e:55:40:a0:8c:
fd:27:1c:70:c9:e3:14:09:9c:a2:8b:75:87:8c:1b:
67:45:b2:de:2e:e0:34:2f:25:0d:b7:5b:06:db:db:
79:b3:bd:f0:ad:33:2d:a6:2d:d6:17:6d:bf:1c:52:
c2:3b:fd:c8:62:c6:c0:90:9c:46:21:b5:83:3b:6a:
7c:b0:4b:16:15:a2:38:0b:6b:e3:5b:07:e8:cf:a5:
17:74:c3:bc:da:a5:4b:ab:99:c2:41:dd:91:7c:ef:
f6:1d:a4:ea:e0:ef:14:47:41:79:48:68:78:38:d7:
5c:b8:d6:b4:0d:12:3c:a7:4f:e3:c8:4a:e6:04:98:
01

public key (*e*, *n*)

e=

publicExponent: 65537 (0x10001)

n=

modulus:
00:98:05:47:5b:a5:02:bd:29:d4:fa:8b:33:1c:37:
4b:cb:ae:f6:60:14:bb:ba:53:3f:99:c0:0d:c1:a4:
c4:99:5a:d9:64:58:c5:f4:49:da:7e:06:0d:e8:3a:
27:fa:44:39:69:8c:63:3b:b8:93:3b:48:16:fc:0f:
b7:e7:86:6a:f0:54:d8:8c:90:63:07:7e:41:a5:d4:
5d:10:9e:1c:58:08:6d:bb:9d:a9:01:07:fc:d6:ab:
4d:bf:ee:84:0c:e5:2d:11:82:28:6f:c1:8b:9f:a3:
92:12:61:d8:58:51:ec:0d:d6:36:f7:48:35:eb:2b:
61:a6:9c:12:04:1d:81:c3:2d:39:30:c7:3f:37:8a:
39:f0:ed:e5:4a:9c:3b:80:34:9c:da:03:0a:9a:5c:
d8:8a:67:f7:91:5c:95:8d:5f:79:d3:44:c0:b6:34:
2d:02:54:fd:e3:d9:59:5e:81:74:97:59:0f:f3:3b:
68:dc:e9:17:ac:b3:39:5e:8b:94:4e:e0:15:a7:fc:
5d:68:81:b2:ca:b6:55:03:ce:96:52:9e:b7:d9:c8:
97:ab:ad:20:6a:31:0c:ac:65:e9:41:dc:13:fe:5d:
5b:3b:72:e2:58:80:26:3c:8a:97:ed:78:9e:bb:f7:
62:87:bd:ae:22:35:89:02:61:90:71:2a:30:b0:38:
f6:03

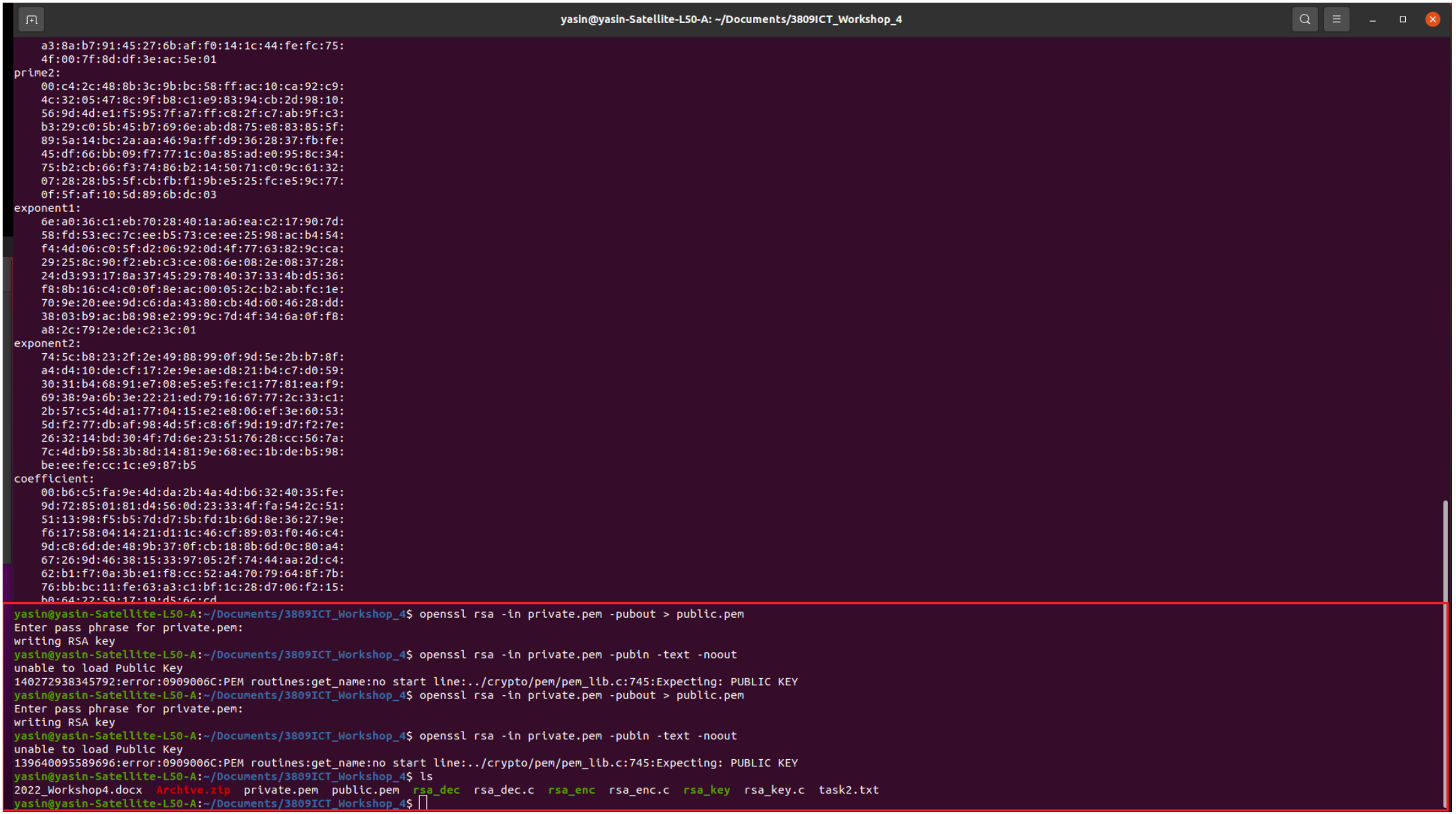
2. We extract the public key from key file private.pem to perform encryption.

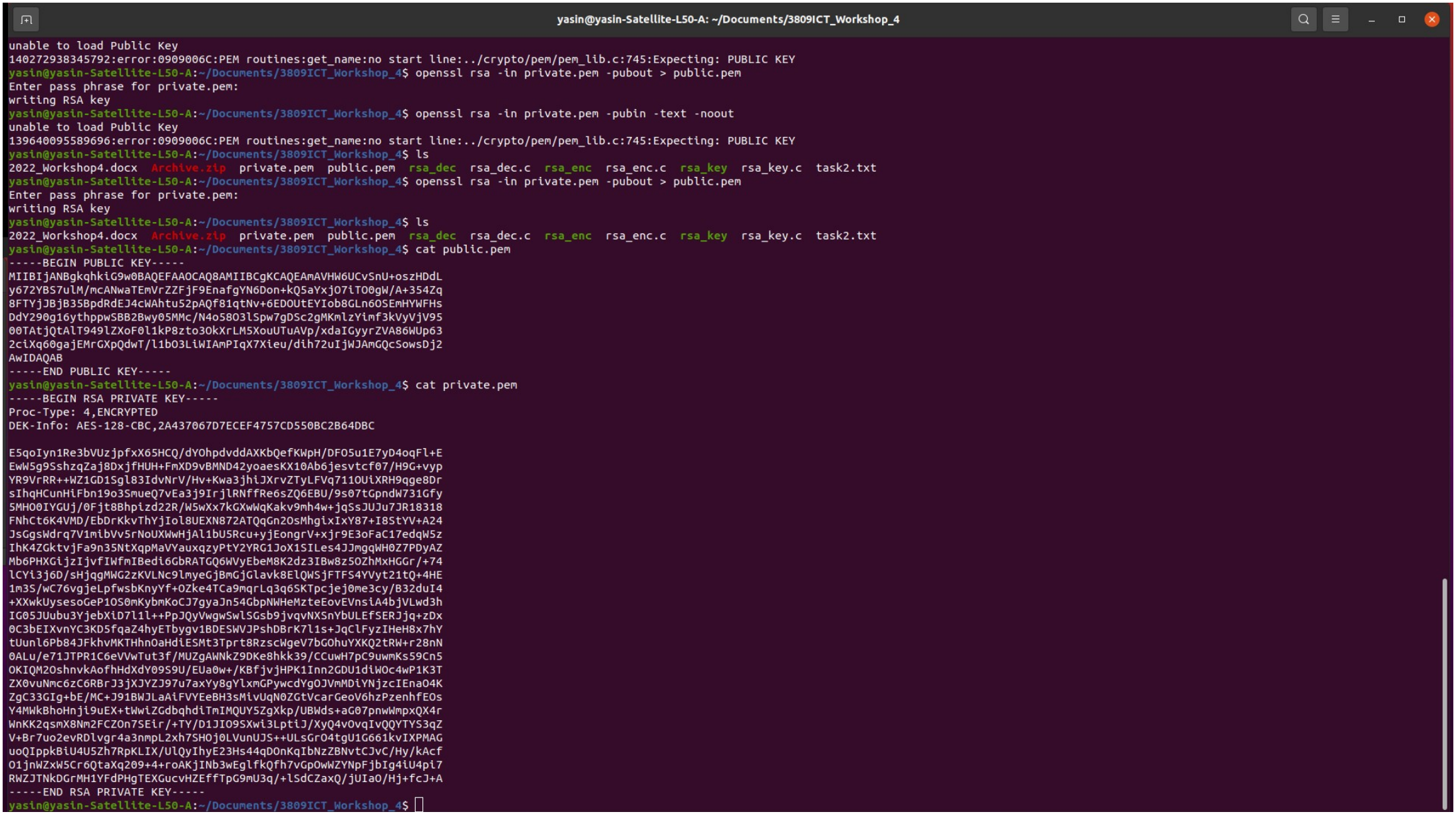
```
$ openssl rsa -in private.pem -pubout > public.pem
```

We can then view the public key values. The option -inpub is included to indicate that the input file is a public-key file.

```
$ openssl rsa -in public.pem -pubin -text -noout
```

Answer:


yasin@yasin-Satellite-L50-A: ~/Documents/3809ICT_Workshop_4
a3:8a:b7:91:45:27:6b:af:f0:14:1c:44:fe:fc:75:
4f:00:7f:8d:df:3e:ac:5e:01
prime2:
00:c4:2c:48:8b:3c:9b:bc:58:ff:ac:10:ca:92:c9:
4c:32:05:47:8c:9f:b8:c1:e9:83:94:cb:2d:98:10:
56:9d:4d:e1:f5:95:7f:a7:ff:c8:2f:c7:ab:9f:c3:
b3:29:c0:5b:45:b7:69:6e:ab:d8:75:e8:83:85:5f:
89:5a:14:bc:2a:aa:46:9a:ff:d9:36:28:37:fb:fe:
45:df:66:bb:09:f7:77:1c:0a:85:ad:e0:95:8c:34:
75:b2:cb:66:f3:74:86:b2:14:50:71:c0:9c:61:32:
07:28:28:b5:5f:cb:fb:f1:9b:e5:25:fc:e5:9c:77:
0f:5f:af:10:5d:89:6b:dc:03
exponent1:
6e:a0:36:c1:eb:70:28:40:1a:a6:ea:c2:17:90:7d:
58:fd:53:ec:7c:ee:b5:73:ce:ee:25:98:ac:b4:54:
f4:4d:06:c0:5f:d2:06:92:0d:4f:77:63:82:9c:ca:
29:25:8c:90:f2:eb:c3:ce:08:6e:08:2e:08:37:28:
24:d3:93:17:8a:37:45:29:78:40:37:33:4b:d5:36:
f8:8b:16:c4:c0:0f:8e:ac:00:05:2c:b2:ab:fc:1e:
70:9e:20:ee:9d:c6:da:43:80:cb:4d:60:46:28:dd:
38:03:b9:ac:b8:98:e2:99:9c:7d:4f:34:6a:0f:f8:
a8:2c:79:2e:de:c2:3c:01
exponent2:
74:5c:b8:23:2f:2e:49:88:99:0f:9d:5e:2b:b7:8f:
a4:d4:10:de:cf:17:2e:9e:ae:d8:21:b4:c7:d0:59:
30:31:b4:68:91:e7:08:e5:e5:fe:c1:77:81:ea:f9:
69:38:9a:6b:3e:22:21:ed:79:16:67:77:2c:33:c1:
2b:57:c5:4d:a1:77:04:15:e2:e8:06:ef:3e:60:53:
5d:f2:77:db:af:98:4d:5f:c8:6f:9d:19:d7:f2:7e:
26:32:14:bd:30:4f:7d:6e:23:51:76:28:cc:56:7a:
7c:4d:b9:58:3b:8d:14:81:9e:68:ec:1b:de:b5:98:
be:ee:fe:cc:1c:e9:87:b5
coefficient:
00:b6:c5:fa:9e:4d:da:2b:4a:4d:b6:32:40:35:fe:
9d:72:85:01:81:d4:56:0d:23:33:4f:fa:54:2c:51:
51:13:98:f5:b5:7d:d7:5b:fd:1b:6d:8e:36:27:9e:
f6:17:58:04:14:21:d1:1c:46:cf:89:03:f0:46:c4:
9d:c8:6d:de:48:9b:37:0f:cb:18:8b:6d:0c:80:a4:
67:26:9d:46:38:15:33:97:05:2f:74:44:aa:2d:c4:
62:b1:f7:0a:3b:e1:f8:cc:52:a4:70:79:64:8f:7b:
76:bb:bc:11:fe:63:a3:c1:bf:1c:28:d7:06:f2:15:
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_4$ openssl rsa -in private.pem -pubout > public.pem
Enter pass phrase for private.pem:
writing RSA key
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_4$ openssl rsa -in private.pem -pubin -text -noout
unable to load Public Key
140272938345792:error:0909006C:PEM routines:get_name:no start line:../crypto/pem/pem_lib.c:745:Expecting: PUBLIC KEY
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_4$ openssl rsa -in private.pem -pubout > public.pem
Enter pass phrase for private.pem:
writing RSA key
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_4$ openssl rsa -in private.pem -pubin -text -noout
unable to load Public Key
139640095589696:error:0909006C:PEM routines:get_name:no start line:../crypto/pem/pem_lib.c:745:Expecting: PUBLIC KEY
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_4$ ls
2022_Workshop4.docx Archive.zip private.pem public.pem rsa_dec rsa_dec.c rsa_enc rsa_enc.c rsa_key rsa_key.c task2.txt
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_4$


yasin@yasin-Satellite-L50-A: ~/Documents/3809ICT_Workshop_4
unable to load Public Key
140272938345792:error:0909006C:PEM routines:get_name:no start line:../crypto/pem/pem_lib.c:745:Expecting: PUBLIC KEY
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_4$ openssl rsa -in private.pem -pubout > public.pem
Enter pass phrase for private.pem:
writing RSA key
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_4$ openssl rsa -in private.pem -pubin -text -noout
unable to load Public Key
139640095589696:error:0909006C:PEM routines:get_name:no start line:../crypto/pem/pem_lib.c:745:Expecting: PUBLIC KEY
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_4$ ls
2022_Workshop4.docx Archive.zip private.pem public.pem rsa_dec rsa_dec.c rsa_enc rsa_enc.c rsa_key rsa_key.c task2.txt
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_4$ openssl rsa -in private.pem -pubout > public.pem
Enter pass phrase for private.pem:
writing RSA key
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_4$ ls
2022_Workshop4.docx Archive.zip private.pem public.pem rsa_dec rsa_dec.c rsa_enc rsa_enc.c rsa_key rsa_key.c task2.txt
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_4$ cat public.pem
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAmAVHW6UCvSnU+oszHDdL
y672YBS7ulM/mcANwaTEmVrZZFjF9EnafgYN6Don+kQ5aYxjO7iTO0gW/A+354Zq
8FTYjJBjB35BpdRdEJ4cWAhtu52pAQf81qtNv+6EDOUtEYIob8GLn6OSEmHYWFHs
DdY290g16ythppwSBB2Bwy05MMc/N4o58O3lSpw7gDSc2gMKmlzYimf3kVyVjV95
00TAtjQtAlT949lZXoF0l1kP8zto3OkXrLM5XouUTuAVp/xdaIGyyrZVA86WUp63
2ciXq60gajEMrGXpQdwT/l1bO3LiWIAmPIqX7Xieu/dih72uIjWJAmGQcSowsDj2
AwIDAQAB
-----END PUBLIC KEY-----
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_4$ cat private.pem
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,2A437067D7ECEF4757CD550BC2B64DBC

E5qoIyn1Re3bVUzjpfxX65HCQ/dYOhpdvddAXKbQefKWpH/DFO5u1E7yD4oqFl+E
EwW5g9SshzqZaj8DxjfHUH+FmXD9vBMND42yoaesKX10Ab6jesvtcf07/H9G+vyp
YR9VrRR++WZ1GD1Sgl83IdvNrV/Hv+Kwa3jhiJXrvZTyLFVq711OUiXRH9qge8Dr
sIhqHCunHiFbn19o3SmueQ7vEa3j9IrjlRNffRe6sZQ6EBU/9s07tGpndW731Gfy
5MHO0IYGUj/0Fjt8Bhpizd22R/W5wXx7kGXwWqKakv9mh4w+jqSsJUJu7JR18318
FNhCt6K4VMD/EbDrKkvThYjIol8UEXN872ATQqGn2OsMhgixIxY87+I8StYV+A24
JsGgsWdrq7V1mibVv5rNoUXWwHjAl1bU5Rcu+yjEongrV+xjr9E3oFaC17edqW5z
IhK4ZGktvjFa9n35NtXqpMaVYauxqzyPtY2YRG1JoX1SILes4JJmgqWH0Z7PDyAZ
Mb6PHXGijzIjvfIWfmIBedi6GbRATGQ6WVyEbeM8K2dz3IBw8z5OZhMxHGGr/+74
lCYi3j6D/sHjqgMWG2zKVLNc9lmyeGjBmGjGlavk8ElQWSjFTFS4YVyt21tQ+4HE
1m3S/wC76vgjeLpfwsbKnyYf+OZke4TCa9mqrLq3q6SKTpcjej0me3cy/B32duI4
+XXwkUysesoGeP1OS0mKybmKoCJ7gyaJn54GbpNWHeMzteEovEVnsiA4bjVLwd3h
IG05JUubu3YjebXiD7l1l++PpJQyVwgwSwlSGsb9jvqvNXSnYbULEfSERJjq+zDx
0C3bEIXvnYC3KD5fqaZ4hyETbygv1BDESWVJPshDBrK7l1s+JqClFyzIHeH8x7hY
tUunl6Pb84JFkhvMKTHhnOaHdiESMt3Tprt8RzscWgeV7bGOhuYXKQ2tRW+r28nN
0ALu/e71JTPR1C6eVVwTut3f/MUZgAWNkZ9DKe8hkk39/CCuwH7pC9uwmKs59Cn5
OKIQM2OshnvkAofhHdXdY09S9U/EUa0w+/KBfjvjHPK1Inn2GDU1diWOc4wP1K3T
ZX0vuNmc6zC6RBrJ3jXJYZJ97u7axYy8gYlxmGPywcdYgOJVmMDiYNjzcIEnaO4K
ZgC33GIg+bE/MC+J91BWJLaAiFVYEeBH3sMivUqN0ZGtVcarGeoV6hzPzenhfEOs
Y4MWkBhoHnji9uEX+tWwiZGdbqhdiTmIMQUY5ZgXkp/UBWds+aG07pnwWmpxQX4r
WnKK2qsmX8Nm2FCZOn7SEir/+TY/D1JIO9SXwi3LptiJ/XyQ4vOvqIvQQYTYS3qZ
V+Br7uo2evRDlvgr4a3nmpL2xh7SHOj0LVunUJS++ULsGrO4tgU1G661kvIXPMAG
uoQIppkBiU4U5Zh7RpKLIX/UlQyIhyE23Hs44qDOnKqIbNzZBNvtCJvC/Hy/kAcf
O1jnWZxW5Cr6QtaXq209+4+roAKjINb3wEglfkQfh7vGpOwWZYNpFjbIg4iU4pi7
RWZJTNkDGrMH1YFdPHgTEXGucvHZEffTpG9mU3q/+lSdCZaxQ/jUIaO/Hj+fcJ+A
-----END RSA PRIVATE KEY-----
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_4$

3. Now, we perform encryption. We first create the plaintext XXXX (you should replace XXXX by your names; spaces between names are allowed). We use the following command:

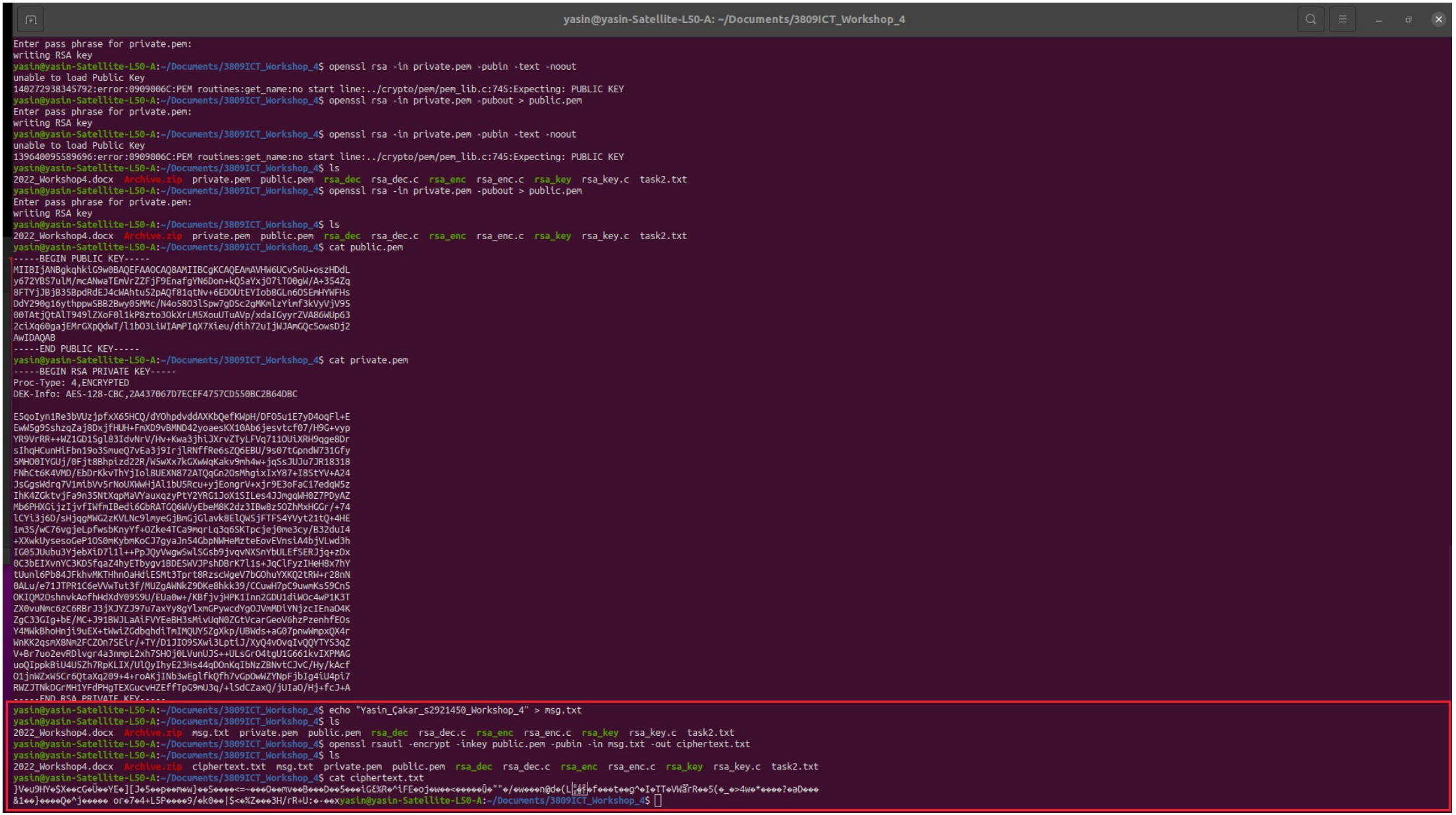
```
$ echo "XXXX" > msg.txt
$ openssl rsautl -encrypt -inkey public.pem -pubin -in msg.txt
-out ciphertext.txt
```

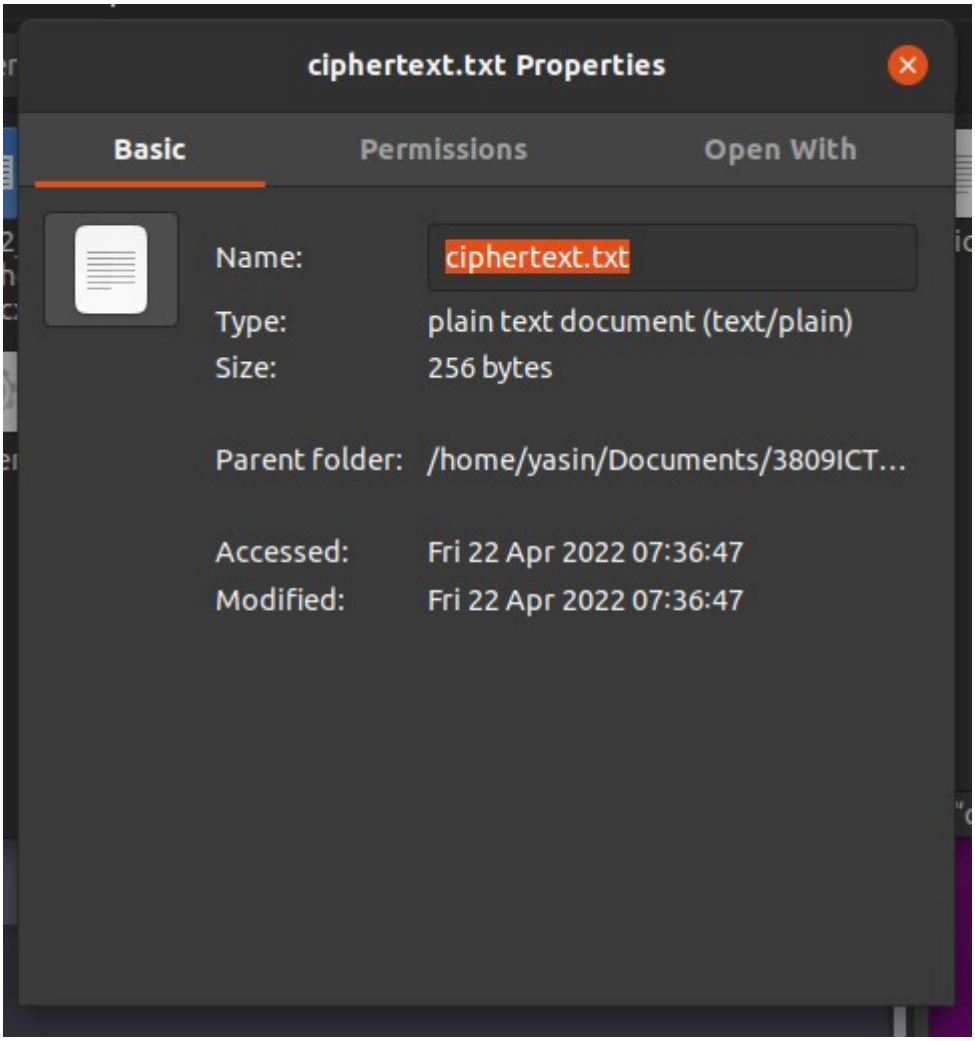
You can view the ciphertext and should notice that it is not readable.

Q: Check the size of the file ciphertext.txt. What is the size? Why is it of that size?
Q: You name is likely to have a hexadecimal (ASCII) encoding shorter than the public modulo number *n* (in hexadecimal). What happen if you encrypt a plaintext longer than *n*? Create a plaintext that is larger than *n*. Then, try to encrypt it in the above way and tell what happened.

(Please save this file as hybrid_plain.txt for Task 4)

Answer:


yasin@yasin-Satellite-L50-A: ~/Documents/3809ICT_Workshop_4
Enter pass phrase for private.pem:
writing RSA key
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_4$ openssl rsa -in private.pem -pubin -text -noout
unable to load Public Key
140272938345792:error:0909006C:PEM routines:get_name:no start line:../crypto/pem/pem_lib.c:745:Expecting: PUBLIC KEY
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_4$ openssl rsa -in private.pem -pubout > public.pem
Enter pass phrase for private.pem:
writing RSA key
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_4$ openssl rsa -in private.pem -pubin -text -noout
unable to load Public Key
139640095589696:error:0909006C:PEM routines:get_name:no start line:../crypto/pem/pem_lib.c:745:Expecting: PUBLIC KEY
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_4$ ls
2022_Workshop4.docx Archive.zip private.pem public.pem rsa_dec rsa_dec.c rsa_enc rsa_enc.c rsa_key rsa_key.c task2.txt
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_4$ openssl rsa -in private.pem -pubout > public.pem
Enter pass phrase for private.pem:
writing RSA key
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_4$ ls
2022_Workshop4.docx Archive.zip private.pem public.pem rsa_dec rsa_dec.c rsa_enc rsa_enc.c rsa_key rsa_key.c task2.txt
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_4$ cat public.pem
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAmAVHW6UCvSnU+oszHDdL
y672YBS7ulM/mcANwaTEmVrZZFjF9EnafgYN6Don+kQ5aYxjO7iTO0gW/A+354Zq
8FTYjJBjB35BpdRdEJ4cWAhtu52pAQf81qtNv+6EDOUtEYIob8GLn6OSEmHYWFHs
DdY290g16ythppwSBB2Bwy05MMc/N4o58O3lSpw7gDSc2gMKmlzYimf3kVyVjV95
00TAtjQtAlT949lZXoF0l1kP8zto3OkXrLM5XouUTuAVp/xdaIGyyrZVA86WUp63
2ciXq60gajEMrGXpQdwT/l1bO3LiWIAmPIqX7Xieu/dih72uIjWJAmGQcSowsDj2
AwIDAQAB
-----END PUBLIC KEY-----
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_4$ cat private.pem
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,2A437067D7ECEF4757CD550BC2B64DBC
E5qoIyn1Re3bVUzjpfxX65HCQ/dYOhpdvddAXKbQefKWpH/DFO5u1E7yD4oqFl+E
EwW5g9SshzqZaj8DxjfHUH+FmXD9vBMND42yoaesKX10Ab6jesvtcf07/H9G+vyp
YR9VrRR++WZ1GD1Sgl83IdvNrV/Hv+Kwa3jhiJXrvZTyLFVq711OUiXRH9qge8Dr
sIhqHCunHiFbn19o3SmueQ7vEa3j9IrjlRNffRe6sZQ6EBU/9s07tGpndW731Gfy
5MHO0IYGUj/0Fjt8Bhpizd22R/W5wXx7kGXwWqKakv9mh4w+jqSsJUJu7JR18318
FNhCt6K4VMD/EbDrKkvThYjIol8UEXN872ATQqGn2OsMhgixIxY87+I8StYV+A24
JsGgsWdrq7V1mibVv5rNoUXWwHjAl1bU5Rcu+yjEongrV+xjr9E3oFaC17edqW5z
IhK4ZGktvjFa9n35NtXqpMaVYauxqzyPtY2YRG1JoX1SILes4JJmgqWH0Z7PDyAZ
Mb6PHXGijzIjvfIWfmIBedi6GbRATGQ6WVyEbeM8K2dz3IBw8z5OZhMxHGGr/+74
lCYi3j6D/sHjqgMWG2zKVLNc9lmyeGjBmGjGlavk8ElQWSjFTFS4YVyt21tQ+4HE
1m3S/wC76vgjeLpfwsbKnyYf+OZke4TCa9mqrLq3q6SKTpcjej0me3cy/B32duI4
+XXwkUysesoGeP1OS0mKybmKoCJ7gyaJn54GbpNWHeMzteEovEVnsiA4bjVLwd3h
IG05JUubu3YjebXiD7l1l++PpJQyVwgwSwlSGsb9jvqvNXSnYbULEfSERJjq+zDx
0C3bEIXvnYC3KD5fqaZ4hyETbygv1BDESWVJPshDBrK7l1s+JqClFyzIHeH8x7hY
tUunl6Pb84JFkhvMKTHhnOaHdiESMt3Tprt8RzscWgeV7bGOhuYXKQ2tRW+r28nN
0ALu/e71JTPR1C6eVVwTut3f/MUZgAWNkZ9DKe8hkk39/CCuwH7pC9uwmKs59Cn5
OKIQM2OshnvkAofhHdXdY09S9U/EUa0w+/KBfjvjHPK1Inn2GDU1diWOc4wP1K3T
ZX0vuNmc6zC6RBrJ3jXJYZJ97u7axYy8gYlxmGPywcdYgOJVmMDiYNjzcIEnaO4K
ZgC33GIg+bE/MC+J91BWJLaAiFVYEeBH3sMivUqN0ZGtVcarGeoV6hzPzenhfEOs
Y4MWkBhoHnji9uEX+tWwiZGdbqhdiTmIMQUYSZgXkp/UBWds+aG07pnwWmpxQX4r
WnKK2qsmX8Nm2FCZOn7SEir/+TY/D1JIO9SXwi3LptiJ/XyQ4vOvqIvQQYTYS3qZ
V+Br7uo2evRDlvgr4a3nmpL2xh7SHOj0LVunUJS++ULsGrO4tgU1G661kvIXPMAG
uoQIppkBiU4U5Zh7RpKLIX/UlQyIhyE23Hs44qDOnKqIbNzZBNvtCJvC/Hy/kAcf
O1jnWZxW5Cr6QtaXq209+4+roAKjINb3wEglfkQfh7vGpOwWZYNpFjbIg4iU4pi7
RWZJTNkDGrMH1YFdPHgTEXGucvHZEffTpG9mU3q/+lSdCZaxQ/jUIaO/Hj+fcJ+A
-----END RSA PRIVATE KEY-----
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_4$ echo "Yasin_Çakar_s2921450_Workshop_4" > msg.txt
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_4$ ls
2022_Workshop4.docx Archive.zip msg.txt private.pem public.pem rsa_dec rsa_dec.c rsa_enc rsa_enc.c rsa_key rsa_key.c task2.txt
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_4$ openssl rsautl -encrypt -inkey public.pem -pubin -in msg.txt -out ciphertext.txt
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_4$ ls
2022_Workshop4.docx Archive.zip ciphertext.txt msg.txt private.pem public.pem rsa_dec rsa_dec.c rsa_enc rsa_enc.c rsa_key rsa_key.c task2.txt
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_4$ cat ciphertext.txt
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_4$



The size of the ciphertext file was 250 bytes, it is necessary the file size to be in the range of zero to 2048 bits to use this particular RSA public-key encryption method.

This is similar to how the Caeser and Vigenère cipher needing to have a modulus range of 25 or 26 (if a character is used to represent space).

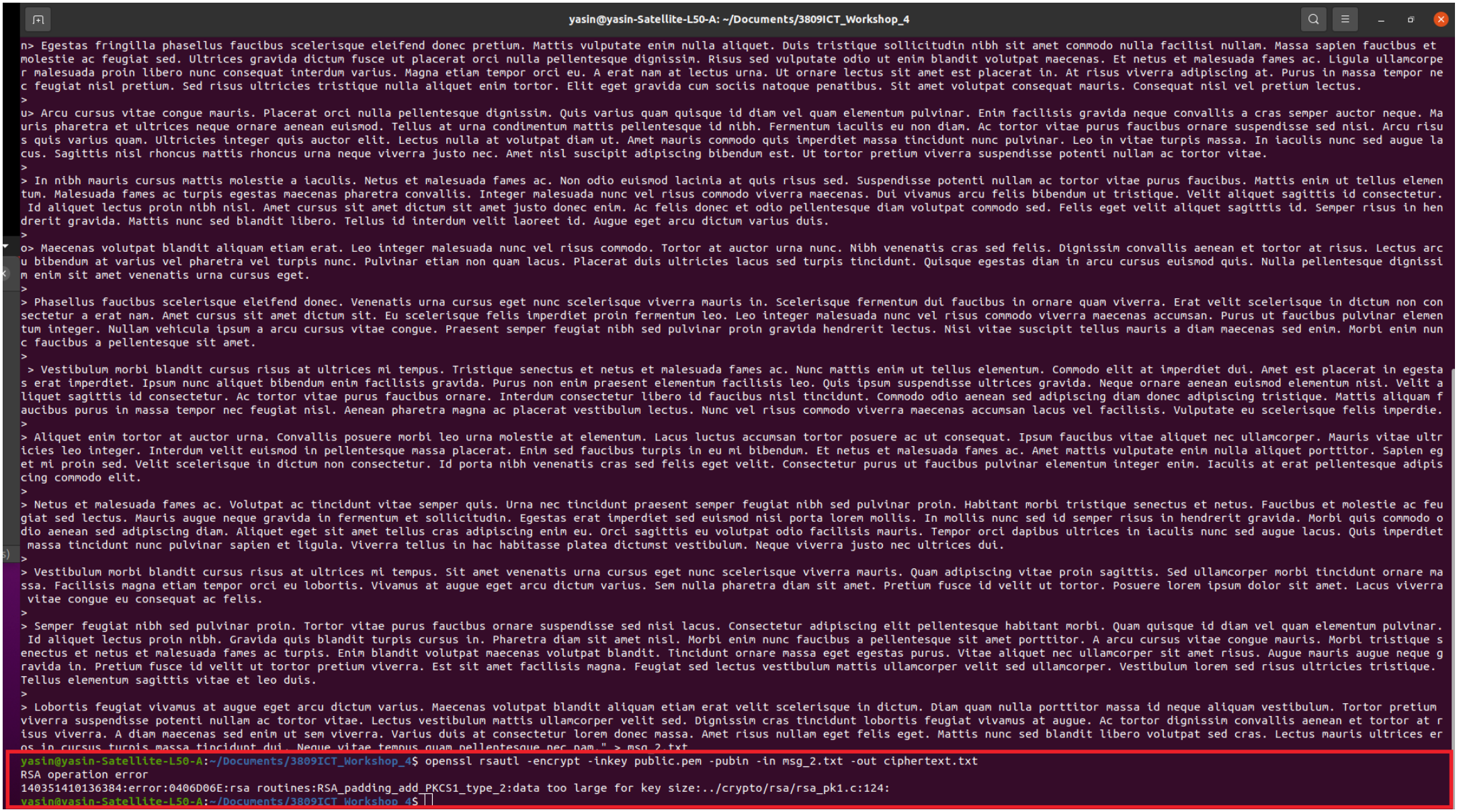
The length of the file has to be in the range of the key length unless the cipher can partition the data into block of smaller bit sizes chunks for encryption like the CBC mode ciphers.

In the next pages is a demonstration of too large file stored as msg_2.txt, before attempting to encrypt to ciphertext.


Activities
Firefox Web Browser
Apr 22 07:46
Lecture 4 – 3809ICT/7809
Send Anywhere - File tran
Achieve more with Send
c cedilla - Google Search
Lorem Ipsum – Generato
https://loremipsum.io
LOREM IPSUM GENERATOR
Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.
20
PARAGRAPHS
GENERATE!
COPY
DISCOVER MORE!
Take a deep dive and try our list of over 40 unique generators, find placeholder images for your next design, or add a lorem ipsum plugin to the CMS or text editor of your choice.
shopify
No coding or design experience required
Start Free Trial
https://loremipsum.io/#


yasin@yasin-Satellite-L50-A: ~/Documents/3809ICT_Workshop_4
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_4$ echo "Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Malesuada nunc vel risus commodo viverra maecenas accumsan. Hendrerit gravida rutrum quisque non tellus orci ac. Purus semper eget duis at tellus at urna condimentum. Duis ultricies lacus sed turpis tincidunt id. Tellus elementum sagittis vitae et leo duis ut diam quam. Eget felis eget nunc lobortis mattis aliquam faucibus purus. Et malesuada fames ac turpis. Vel turpis nunc eget lorem dolor sed viverra ipsum. Vulputate dignissim suspendisse in est ante in nibh mauris cursus. Eros in cursus turpis massa tincidunt dui. Mattis ullamcorper velit sed ullamcorper morbi.
>
e> Nibh cras pulvinar mattis nunc sed blandit libero volutpat sed. Aliquet nibh praesent tristique magna sit amet. Nisi vitae suscipit tellus mauris a diam maecenas sed enim. Elementum eu facilisis sed odio morbi quis commodo odio. Arcu felis bibendum ut tristique. Fames ac turpis egestas sed tempus urna. Dui sapien eget mi proin sed libero. Lobortis mattis aliquam faucibus purus in massa. Nunc consequat interdum varius sit amet mattis vulputate enim. Purus gravida quis blandit turpis cursus in hac. Risus feugiat in ante metus dictum at tempor. Habitant morbi tristique senectus et netus. Massa massa ultricies mi quis. Tortor id aliquet lectus proin nibh nisl condimentum id.
>
> Tellus orci ac auctor augue mauris augue. Sem nulla pharetra diam sit. Augue ut lectus arcu bibendum at varius vel pharetra vel. Velit scelerisque in dictum non consectetur a. Quis risus sed vulputate odio. Aliquam ultrices sagittis orci a scelerisque. Ac turpis egestas integer eget aliquet. Praesent elementum facilisis leo vel fringilla est ullamcorper eget. Fringilla est ullamcorper eget nulla facilisi etiam dignissim diam. Sed faucibus turpis in eu.
>
> Malesuada fames ac turpis egestas maecenas pharetra. Sit amet mauris commodo quis imperdiet massa tincidunt nunc pulvinar. Nunc vel risus commodo viverra. Diam quis enim lobortis scelerisque fermentum dui faucibus in. Tincidunt lobortis feugiat vivamus at augue. Quisque sagittis purus sit amet. Mi eget mauris pharetra et ultrices. Aliquam ultrices sagittis orci a scelerisque purus semper eget. Enim diam vulputate ut pharetra. Est sit amet facilisis magna etiam. Pellentesque habitant morbi tristique senectus et netus et malesuada.
>
> Urna nunc id cursus metus aliquam eleifend mi. Fermentum dui faucibus in ornare. Massa vitae tortor condimentum lacinia quis vel. Nec tincidunt praesent semper feugiat. Consectetur purus ut faucibus pulvinar. Ullamcorper morbi tincidunt ornare massa eget. Purus ut faucibus pulvinar elementum integer enim neque volutpat ac. Quis imperdiet massa tincidunt nunc pulvinar sapien et. Eget nunc scelerisque viverra mauris in aliquam sem fringilla. Suspendisse sed nisi lacus sed viverra tellus.
>
> Magna fringilla urna porttitor rhoncus dolor purus. Massa ultricies mi quis hendrerit dolor magna eget est lorem. Non enim praesent elementum facilisis leo. Commodo odio aenean sed adipiscing. Eget egestas purus viverra accumsan. Eleifend quam adipiscing vitae proin sagittis nisl rhoncus mattis. Ut sem nulla pharetra diam sit amet. Mauris in aliquam sem fringilla ut morbi tincidunt augue. Erat nam at lectus urna duis convallis. Id aliquet lectus proin nibh nisl condimentum id. Sed vulputate odio ut enim blandit volutpat maecenas volutpat.
>
> Euismod lacinia at quis risus sed vulputate odio. Volutpat odio facilisis mauris sit amet. Nunc sed velit dignissim sodales ut. Leo a diam sollicitudin tempor. Egestas purus viverra accumsan in nisl nisi. Vitae congue eu consequat ac felis donec et odio pellentesque. Suscipit adipiscing bibendum est ultricies integer quis auctor elit. Elementum eu facilisis sed odio morbi. Aenean vel elit scelerisque mauris pellentesque pulvinar pellentesque habitant. Id diam maecenas ultricies mi eget mauris pharetra. Sed id semper risus in. Et odio pellentesque diam volutpat commodo. Mi bibendum neque egestas congue quisque. Dui sapien eget mi proin sed libero enim sed faucibus. Nibh tellus molestie nunc non blandit massa enim. A cras semper auctor neque vitae tempus quam. Sed felis eget velit aliquet sagittis id consectetur purus.
>
> Metus dictum at tempor commodo. Blandit turpis cursus in hac habitasse. Magna ac placerat vestibulum lectus. Semper feugiat nibh sed pulvinar proin gravida hendrerit lectus a. Mauris sit amet massa vitae tortor. Vitae congue eu consequat ac. Nibh cras pulvinar mattis nunc sed blandit libero. Tellus elementum sagittis vitae et leo duis ut diam. Morbi quis commodo odio aenean sed adipiscing diam. Lorem mollis aliquam ut porttitor leo a. Vestibulum lectus mauris ultrices eros. Amet commodo nulla facilisi nullam vehicula ipsum. Venenatis cras sed felis eget velit aliquet sagittis. Tempor orci eu lobortis elementum nibh tellus. Auctor augue mauris augue neque gravida. Mauris vitae ultricies leo integer. Laoreet non curabitur gravida arcu ac tortor dignissim.
>
c> Scelerisque eleifend donec pretium vulputate sapien nec sagittis. Semper eget duis at tellus at urna condimentum mattis. Eu volutpat odio facilisis mauris sit amet. Tortor id aliquet lectus proin nibh. Non tellus orci ac auctor augue mauris. Morbi leo urna molestie at. Aliquam ultrices sagittis orci a scelerisque purus semper. At tellus at urna condimentum. Metus dictum at tempor commodo ullamcorper. Ultrices sagittis orci a scelerisque purus semper eget duis. Habitasse platea dictumst vestibulum rhoncus est pellentesque elit ullamcorper dignissim. Urna neque viverra justo nec ultrices. Ut faucibus pulvinar elementum integer enim neque. Hendrerit gravida rutrum quisque non. Elementum integer enim neque volutpat. Pharetra sit amet aliquam id diam maecenas ultricies. Enim tortor at auctor urna nunc id. Tincidunt augue interdum velit euismod in pellentesque massa placerat duis.
>
n> Egestas fringilla phasellus faucibus scelerisque eleifend donec pretium. Mattis vulputate enim nulla aliquet. Duis tristique sollicitudin nibh sit amet commodo nulla facilisi nullam. Massa sapien faucibus et molestie ac feugiat sed. Ultrices gravida dictum fusce ut placerat orci nulla pellentesque dignissim. Risus sed vulputate odio ut enim blandit volutpat maecenas. Et netus et malesuada fames ac. Ligula ullamcorper malesuada proin libero nunc consequat interdum varius. Magna etiam tempor orci eu. A erat nam at lectus urna. Ut ornare lectus sit amet est placerat in. At risus viverra adipiscing at. Purus in massa tempor nec feugiat nisl pretium. Sed risus ultricies tristique nulla aliquet enim tortor. Elit eget gravida cum sociis natoque penatibus. Sit amet volutpat consequat mauris. Consequat nisl vel pretium lectus.
>
u> Arcu cursus vitae congue mauris. Placerat orci nulla pellentesque dignissim. Quis varius quam quisque id diam vel quam elementum pulvinar. Enim facilisis gravida neque convallis a cras semper auctor neque. Mauris pharetra et ultrices neque ornare aenean euismod. Tellus at urna condimentum mattis pellentesque id nibh. Fermentum iaculis eu non diam. Ac tortor vitae purus faucibus ornare suspendisse sed nisi. Arcu risus quis varius quam. Ultricies integer quis auctor elit. Lectus nulla at volutpat diam ut. Amet mauris commodo quis imperdiet massa tincidunt nunc pulvinar. Leo in vitae turpis massa. In iaculis nunc sed augue lacus. Sagittis nisl rhoncus mattis rhoncus urna neque viverra justo nec. Amet nisl suscipit adipiscing bibendum est. Ut tortor pretium viverra suspendisse potenti nullam ac tortor vitae.
>
> In nibh mauris cursus mattis molestie a iaculis. Netus et malesuada fames ac. Non odio euismod lacinia at quis risus sed. Suspendisse potenti nullam ac tortor vitae purus faucibus. Mattis enim ut tellus elementum. Malesuada fames ac turpis egestas maecenas pharetra convallis. Integer malesuada nunc vel risus commodo viverra maecenas. Dui vivamus arcu felis bibendum ut tristique. Velit aliquet sagittis id consectetur. Id aliquet lectus proin nibh nisl. Amet cursus sit amet dictum sit amet justo donec enim. Ac felis donec et odio pellentesque diam volutpat commodo sed. Felis eget velit aliquet sagittis id. Semper risus in hendrerit gravida. Mattis nunc sed blandit libero. Tellus id interdum velit laoreet id. Augue eget arcu dictum varius duis.
>

is orci a scelerisque purus semper eget duis. Habitasse platea dictumst vestibulum rhoncus est pellentesque elit ullamcorper dignissim. Urna neque viverra justo nec ultrices. Ut faucibus pulvinar elementum integer enim neque. Hendrerit gravida rutrum quisque non. Elementum integer enim neque volutpat. Pharetra sit amet aliquam id diam maecenas ultricies. Enim tortor at auctor urna nunc id. Tincidunt augue interdum velit euismod in pellentesque massa placerat duis.
>
n> Egestas fringilla phasellus faucibus scelerisque eleifend donec pretium. Mattis vulputate enim nulla aliquet. Duis tristique sollicitudin nibh sit amet commodo nulla facilisi nullam. Massa sapien faucibus et molestie ac feugiat sed. Ultrices gravida dictum fusce ut placerat orci nulla pellentesque dignissim. Risus sed vulputate odio ut enim blandit volutpat maecenas. Et netus et malesuada fames ac. Ligula ullamcorper malesuada proin libero nunc consequat interdum varius. Magna etiam tempor orci eu. A erat nam at lectus urna. Ut ornare lectus sit amet est placerat in. At risus viverra adipiscing at. Purus in massa tempor nec feugiat nisl pretium. Sed risus ultricies tristique nulla aliquet enim tortor. Elit eget gravida cum sociis natoque penatibus. Sit amet volutpat consequat mauris. Consequat nisl vel pretium lectus.
>
u> Arcu cursus vitae congue mauris. Placerat orci nulla pellentesque dignissim. Quis varius quam quisque id diam vel quam elementum pulvinar. Enim facilisis gravida neque convallis a cras semper auctor neque. Mauris pharetra et ultrices neque ornare aenean euismod. Tellus at urna condimentum mattis pellentesque id nibh. Fermentum iaculis eu non diam. Ac tortor vitae purus faucibus ornare suspendisse sed nisi. Arcu risus quis varius quam. Ultricies integer quis auctor elit. Lectus nulla at volutpat diam ut. Amet mauris commodo quis imperdiet massa tincidunt nunc pulvinar. Leo in vitae turpis massa. In iaculis nunc sed augue lacus. Sagittis nisl rhoncus mattis rhoncus urna neque viverra justo nec. Amet nisl suscipit adipiscing bibendum est. Ut tortor pretium viverra suspendisse potenti nullam ac tortor vitae.
>
> In nibh mauris cursus mattis molestie a iaculis. Netus et malesuada fames ac. Non odio euismod lacinia at quis risus sed. Suspendisse potenti nullam ac tortor vitae purus faucibus. Mattis enim ut tellus elementum. Malesuada fames ac turpis egestas maecenas pharetra convallis. Integer malesuada nunc vel risus commodo viverra maecenas. Dui vivamus arcu felis bibendum ut tristique. Velit aliquet sagittis id consectetur. Id aliquet lectus proin nibh nisl. Amet cursus sit amet dictum sit amet justo donec enim. Ac felis donec et odio pellentesque diam volutpat commodo sed. Felis eget velit aliquet sagittis id. Semper risus in hendrerit gravida. Mattis nunc sed blandit libero. Tellus id interdum velit laoreet id. Augue eget arcu dictum varius duis.
>
o> Maecenas volutpat blandit aliquam etiam erat. Leo integer malesuada nunc vel risus commodo. Tortor at auctor urna nunc. Nibh venenatis cras sed felis. Dignissim convallis aenean et tortor at risus. Lectus arcu bibendum at varius vel pharetra vel turpis nunc. Pulvinar etiam non quam lacus. Placerat duis ultricies lacus sed turpis tincidunt. Quisque egestas diam in arcu cursus euismod quis. Nulla pellentesque dignissim enim sit amet venenatis urna cursus eget.
>
> Phasellus faucibus scelerisque eleifend donec. Venenatis urna cursus eget nunc scelerisque viverra mauris in. Scelerisque fermentum dui faucibus in ornare quam viverra. Erat velit scelerisque in dictum non consectetur a erat nam. Amet cursus sit amet dictum sit. Eu scelerisque felis imperdiet proin fermentum leo. Leo integer malesuada nunc vel risus commodo viverra maecenas accumsan. Purus ut faucibus pulvinar elementum integer. Nullam vehicula ipsum a arcu cursus vitae congue. Praesent semper feugiat nibh sed pulvinar proin gravida hendrerit lectus. Nisi vitae suscipit tellus mauris a diam maecenas sed enim. Morbi enim nunc faucibus a pellentesque sit amet.
>
 > Vestibulum morbi blandit cursus risus at ultrices mi tempus. Tristique senectus et netus et malesuada fames ac. Nunc mattis enim ut tellus elementum. Commodo elit at imperdiet dui. Amet est placerat in egestas erat imperdiet. Ipsum nunc aliquet bibendum enim facilisis gravida. Purus non enim praesent elementum facilisis leo. Quis ipsum suspendisse ultrices gravida. Neque ornare aenean euismod elementum nisi. Velit aliquet sagittis id consectetur. Ac tortor vitae purus faucibus ornare. Interdum consectetur libero id faucibus nisl tincidunt. Commodo odio aenean sed adipiscing diam donec adipiscing tristique. Mattis aliquam faucibus purus in massa tempor nec feugiat nisl. Aenean pharetra magna ac placerat vestibulum lectus. Nunc vel risus commodo viverra maecenas accumsan lacus vel facilisis. Vulputate eu scelerisque felis imperdie.
>
> Aliquet enim tortor at auctor urna. Convallis posuere morbi leo urna molestie at elementum. Lacus luctus accumsan tortor posuere ac ut consequat. Ipsum faucibus vitae aliquet nec ullamcorper. Mauris vitae ultricies leo integer. Interdum velit euismod in pellentesque massa placerat. Enim sed faucibus turpis in eu mi bibendum. Et netus et malesuada fames ac. Amet mattis vulputate enim nulla aliquet porttitor. Sapien eget mi proin sed. Velit scelerisque in dictum non consectetur. Id porta nibh venenatis cras sed felis eget velit. Consectetur purus ut faucibus pulvinar elementum integer enim. Iaculis at erat pellentesque adipiscing commodo elit.
>
> Netus et malesuada fames ac. Volutpat ac tincidunt vitae semper quis. Urna nec tincidunt praesent semper feugiat nibh sed pulvinar proin. Habitant morbi tristique senectus et netus. Faucibus et molestie ac feugiat sed lectus. Mauris augue neque gravida in fermentum et sollicitudin. Egestas erat imperdiet sed euismod nisi porta lorem mollis. In mollis nunc sed id semper risus in hendrerit gravida. Morbi quis commodo odio aenean sed adipiscing diam. Aliquet eget sit amet tellus cras adipiscing enim eu. Orci sagittis eu volutpat odio facilisis mauris. Tempor orci dapibus ultrices in iaculis nunc sed augue lacus. Quis imperdiet massa tincidunt nunc pulvinar sapien et ligula. Viverra tellus in hac habitasse platea dictumst vestibulum. Neque viverra justo nec ultrices dui.
>
> Vestibulum morbi blandit cursus risus at ultrices mi tempus. Sit amet venenatis urna cursus eget nunc scelerisque viverra mauris. Quam adipiscing vitae proin sagittis. Sed ullamcorper morbi tincidunt ornare massa. Facilisis magna etiam tempor orci eu lobortis. Vivamus at augue eget arcu dictum varius. Sem nulla pharetra diam sit amet. Pretium fusce id velit ut tortor. Posuere lorem ipsum dolor sit amet. Lacus viverra vitae congue eu consequat ac felis.
>
> Semper feugiat nibh sed pulvinar proin. Tortor vitae purus faucibus ornare suspendisse sed nisi lacus. Consectetur adipiscing elit pellentesque habitant morbi. Quam quisque id diam vel quam elementum pulvinar. Id aliquet lectus proin nibh. Gravida quis blandit turpis cursus in. Pharetra diam sit amet nisl. Morbi enim nunc faucibus a pellentesque sit amet porttitor. A arcu cursus vitae congue mauris. Morbi tristique senectus et netus et malesuada fames ac turpis. Enim blandit volutpat maecenas volutpat blandit. Tincidunt ornare massa eget egestas purus. Vitae aliquet nec ullamcorper sit amet risus. Augue mauris augue neque gravida in. Pretium fusce id velit ut tortor pretium viverra. Est sit amet facilisis magna. Feugiat sed lectus vestibulum mattis ullamcorper velit sed ullamcorper. Vestibulum lorem sed risus ultricies tristique. Tellus elementum sagittis vitae et leo duis.
>
> Lobortis feugiat vivamus at augue eget arcu dictum varius. Maecenas volutpat blandit aliquam etiam erat velit scelerisque in dictum. Diam quam nulla porttitor massa id neque aliquam vestibulum. Tortor pretium viverra suspendisse potenti nullam ac tortor vitae. Lectus vestibulum mattis ullamcorper velit sed. Dignissim cras tincidunt lobortis feugiat vivamus at augue. Ac tortor dignissim convallis aenean et tortor at risus viverra. A diam maecenas sed enim ut sem viverra. Varius duis at consectetur lorem donec massa. Amet risus nullam eget felis eget. Mattis nunc sed blandit libero volutpat sed cras. Lectus mauris ultrices eros in cursus turpis massa tincidunt dui. Neque vitae tempus quam pellentesque nec nam." > msg_2.txt

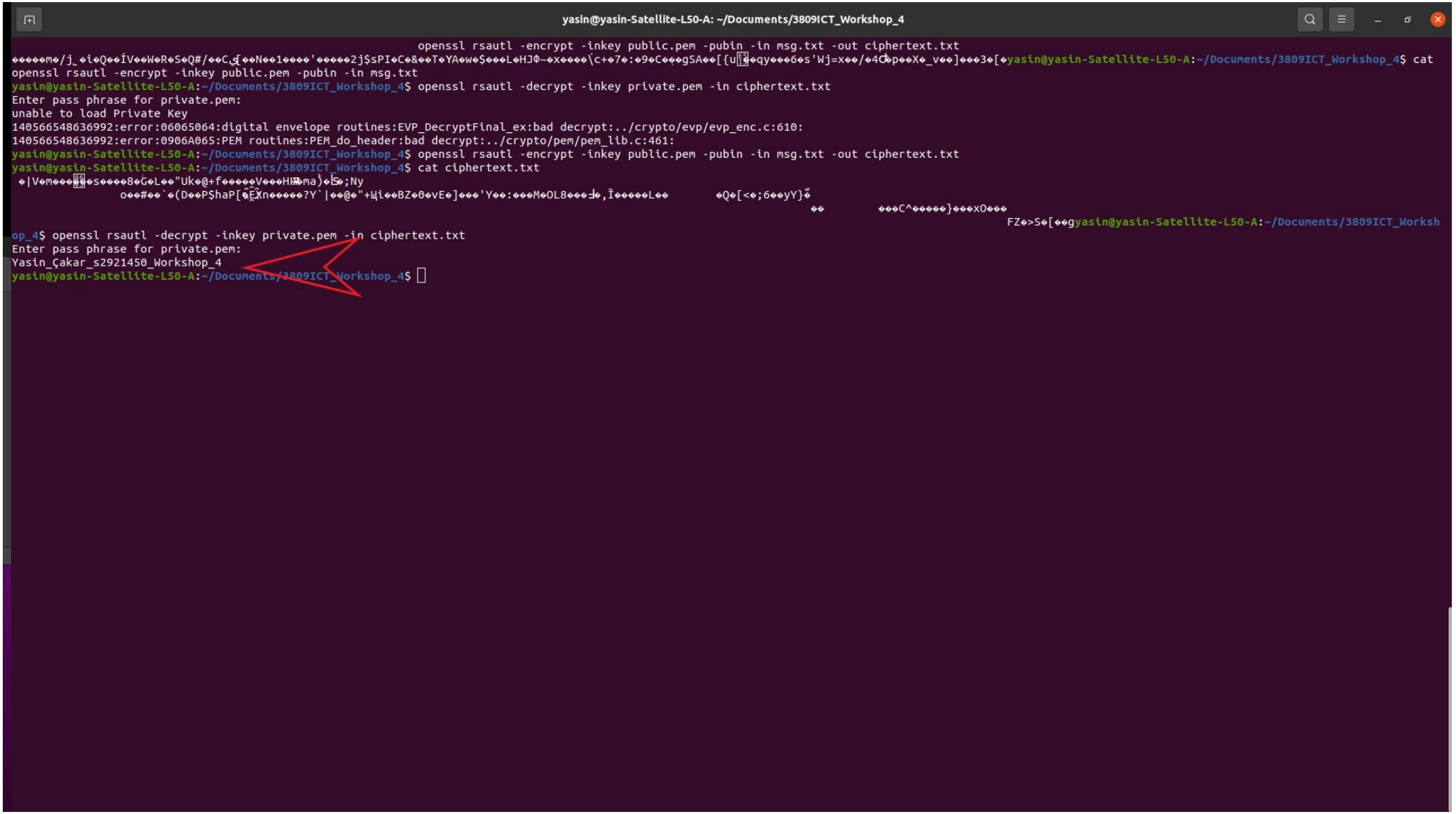

yasin@yasin-Satellite-L50-A: ~/Documents/3809ICT_Workshop_4
n> Egestas fringilla phasellus faucibus scelerisque eleifend donec pretium. Mattis vulputate enim nulla aliquet. Duis tristique sollicitudin nibh sit amet commodo nulla facilisi nullam. Massa sapien faucibus et molestie ac feugiat sed. Ultrices gravida dictum fusce ut placerat orci nulla pellentesque dignissim. Risus sed vulputate odio ut enim blandit volutpat maecenas. Et netus et malesuada fames ac. Ligula ullamcorper malesuada proin libero nunc consequat interdum varius. Magna etiam tempor orci eu. A erat nam at lectus urna. Ut ornare lectus sit amet est placerat in. At risus viverra adipiscing at. Purus in massa tempor nec feugiat nisl pretium. Sed risus ultricies tristique nulla aliquet enim tortor. Elit eget gravida cum sociis natoque penatibus. Sit amet volutpat consequat mauris. Consequat nisl vel pretium lectus.
>
u> Arcu cursus vitae congue mauris. Placerat orci nulla pellentesque dignissim. Quis varius quam quisque id diam vel quam elementum pulvinar. Enim facilisis gravida neque convallis a cras semper auctor neque. Mauris pharetra et ultrices neque ornare aenean euismod. Tellus at urna condimentum mattis pellentesque id nibh. Fermentum iaculis eu non diam. Ac tortor vitae purus faucibus ornare suspendisse sed nisi. Arcu risus quis varius quam. Ultricies integer quis auctor elit. Lectus nulla at volutpat diam ut. Amet mauris commodo quis imperdiet massa tincidunt nunc pulvinar. Leo in vitae turpis massa. In iaculis nunc sed augue lacus. Sagittis nisl rhoncus mattis rhoncus urna neque viverra justo nec. Amet nisl suscipit adipiscing bibendum est. Ut tortor pretium viverra suspendisse potenti nullam ac tortor vitae.
>
> In nibh mauris cursus mattis molestie a iaculis. Netus et malesuada fames ac. Non odio euismod lacinia at quis risus sed. Suspendisse potenti nullam ac tortor vitae purus faucibus. Mattis enim ut tellus elementum. Malesuada fames ac turpis egestas maecenas pharetra convallis. Integer malesuada nunc vel risus commodo viverra maecenas. Dui vivamus arcu felis bibendum ut tristique. Velit aliquet sagittis id consectetur. Id aliquet lectus proin nibh nisl. Amet cursus sit amet dictum sit amet justo donec enim. Ac felis donec et odio pellentesque diam volutpat commodo sed. Felis eget velit aliquet sagittis id. Semper risus in hendrerit gravida. Mattis nunc sed blandit libero. Tellus id interdum velit laoreet id. Augue eget arcu dictum varius duis.
>
o> Maecenas volutpat blandit aliquam etiam erat. Leo integer malesuada nunc vel risus commodo. Tortor at auctor urna nunc. Nibh venenatis cras sed felis. Dignissim convallis aenean et tortor at risus. Lectus arcu bibendum at varius vel pharetra vel turpis nunc. Pulvinar etiam non quam lacus. Placerat duis ultricies lacus sed turpis tincidunt. Quisque egestas diam in arcu cursus euismod quis. Nulla pellentesque dignissim enim sit amet venenatis urna cursus eget.
>
> Phasellus faucibus scelerisque eleifend donec. Venenatis urna cursus eget nunc scelerisque viverra mauris in. Scelerisque fermentum dui faucibus in ornare quam viverra. Erat velit scelerisque in dictum non consectetur a erat nam. Amet cursus sit amet dictum sit. Eu scelerisque felis imperdiet proin fermentum leo. Leo integer malesuada nunc vel risus commodo viverra maecenas accumsan. Purus ut faucibus pulvinar elementum integer. Nullam vehicula ipsum a arcu cursus vitae congue. Praesent semper feugiat nibh sed pulvinar proin gravida hendrerit lectus. Nisi vitae suscipit tellus mauris a diam maecenas sed enim. Morbi enim nunc faucibus a pellentesque sit amet.
>
> Vestibulum morbi blandit cursus risus at ultrices mi tempus. Tristique senectus et netus et malesuada fames ac. Nunc mattis enim ut tellus elementum. Commodo elit at imperdiet dui. Amet est placerat in egestas erat imperdiet. Ipsum nunc aliquet bibendum enim facilisis gravida. Purus non enim praesent elementum facilisis leo. Quis ipsum suspendisse ultrices gravida. Neque ornare aenean euismod elementum nisi. Velit aliquet sagittis id consectetur. Ac tortor vitae purus faucibus ornare. Interdum consectetur libero id faucibus nisl tincidunt. Commodo odio aenean sed adipiscing diam donec adipiscing tristique. Mattis aliquam faucibus purus in massa tempor nec feugiat nisl. Aenean pharetra magna ac placerat vestibulum lectus. Nunc vel risus commodo viverra maecenas accumsan lacus vel facilisis. Vulputate eu scelerisque felis imperdie.
>
> Aliquet enim tortor at auctor urna. Convallis posuere morbi leo urna molestie at elementum. Lacus luctus accumsan tortor posuere ac ut consequat. Ipsum faucibus vitae aliquet nec ullamcorper. Mauris vitae ultricies leo integer. Interdum velit euismod in pellentesque massa placerat. Enim sed faucibus turpis in eu mi bibendum. Et netus et malesuada fames ac. Amet mattis vulputate enim nulla aliquet porttitor. Sapien eget mi proin sed. Velit scelerisque in dictum non consectetur. Id porta nibh venenatis cras sed felis eget velit. Consectetur purus ut faucibus pulvinar elementum integer enim. Iaculis at erat pellentesque adipiscing commodo elit.
>
> Netus et malesuada fames ac. Volutpat ac tincidunt vitae semper quis. Urna nec tincidunt praesent semper feugiat nibh sed pulvinar proin. Habitant morbi tristique senectus et netus. Faucibus et molestie ac feugiat sed lectus. Mauris augue neque gravida in fermentum et sollicitudin. Egestas erat imperdiet sed euismod nisi porta lorem mollis. In mollis nunc sed id semper risus in hendrerit gravida. Morbi quis commodo odio aenean sed adipiscing diam. Aliquet eget sit amet tellus cras adipiscing enim eu. Orci sagittis eu volutpat odio facilisis mauris. Tempor orci dapibus ultrices in iaculis nunc sed augue lacus. Quis imperdiet massa tincidunt nunc pulvinar sapien et ligula. Viverra tellus in hac habitasse platea dictumst vestibulum. Neque viverra justo nec ultrices dui.
>
> Vestibulum morbi blandit cursus risus at ultrices mi tempus. Sit amet venenatis urna cursus eget nunc scelerisque viverra mauris. Quam adipiscing vitae proin sagittis. Sed ullamcorper morbi tincidunt ornare massa. Facilisis magna etiam tempor orci eu lobortis. Vivamus at augue eget arcu dictum varius. Sem nulla pharetra diam sit amet. Pretium fusce id velit ut tortor. Posuere lorem ipsum dolor sit amet. Lacus viverra vitae congue eu consequat ac felis.
>
> Semper feugiat nibh sed pulvinar proin. Tortor vitae purus faucibus ornare suspendisse sed nisi lacus. Consectetur adipiscing elit pellentesque habitant morbi. Quam quisque id diam vel quam elementum pulvinar. Id aliquet lectus proin nibh. Gravida quis blandit turpis cursus in. Pharetra diam sit amet nisl. Morbi enim nunc faucibus a pellentesque sit amet porttitor. A arcu cursus vitae congue mauris. Morbi tristique senectus et netus et malesuada fames ac turpis. Enim blandit volutpat maecenas volutpat blandit. Tincidunt ornare massa eget egestas purus. Vitae aliquet nec ullamcorper sit amet risus. Augue mauris augue neque gravida in. Pretium fusce id velit ut tortor pretium viverra. Est sit amet facilisis magna. Feugiat sed lectus vestibulum mattis ullamcorper velit sed ullamcorper. Vestibulum lorem sed risus ultricies tristique. Tellus elementum sagittis vitae et leo duis.
>
> Lobortis feugiat vivamus at augue eget arcu dictum varius. Maecenas volutpat blandit aliquam etiam erat velit scelerisque in dictum. Diam quam nulla porttitor massa id neque aliquam vestibulum. Tortor pretium viverra suspendisse potenti nullam ac tortor vitae. Lectus vestibulum mattis ullamcorper velit sed. Dignissim cras tincidunt lobortis feugiat vivamus at augue. Ac tortor dignissim convallis aenean et tortor at risus viverra. A diam maecenas sed enim ut sem viverra. Varius duis at consectetur lorem donec massa. Amet risus nullam eget felis eget. Mattis nunc sed blandit libero volutpat sed cras. Lectus mauris ultrices eros in cursus turpis massa tincidunt dui. Neque vitae tempus quam pellentesque nec nam." > msg_2.txt
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_4$ openssl rsautl -encrypt -inkey public.pem -pubin -in msg_2.txt -out ciphertext.txt
RSA operation error
140351410136384:error:0406D06E:rsa routines:RSA_padding_add_PKCS1_type_2:data too large for key size:../crypto/rsa/rsa_pk1.c:124:
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_4$

4. We can decrypt the ciphertext to recover the plaintext by doing the following:

   ```
   $ openssl rsautl -decrypt -inkey private.pem -in ciphertext.txt
   ```

   Answer:

   In the last activity output for msg_2.txt was specified as ciphertext.txt, for this reason encryption for msg.txt was run once more to avoid decrypting an empty file.

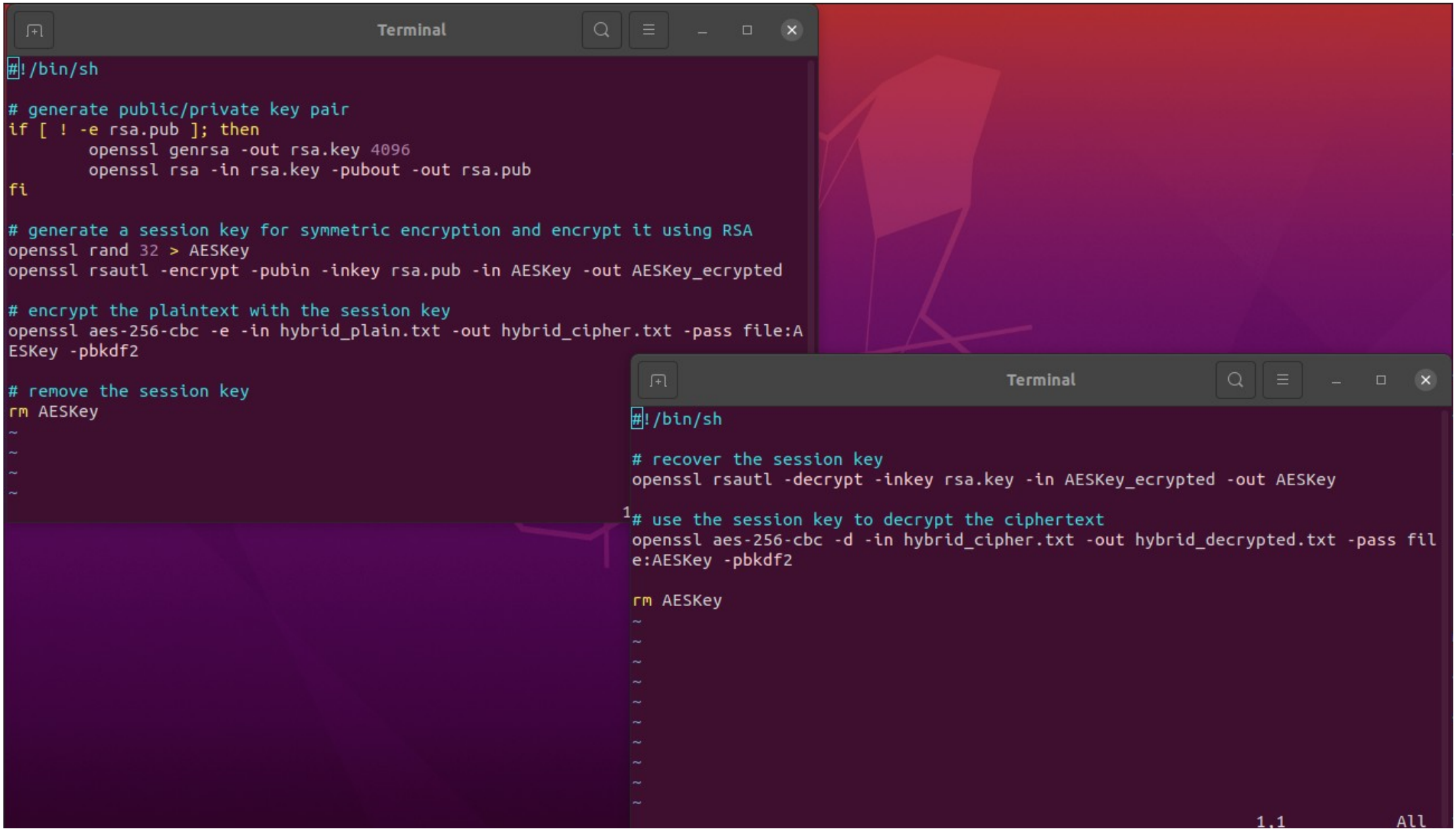

yasin@yasin-Satellite-L50-A: ~/Documents/3809ICT_Workshop_4
openssl rsautl -encrypt -inkey public.pem -pubin -in msg.txt -out ciphertext.txt
openssl rsautl -encrypt -inkey public.pem -pubin -in msg.txt
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_4$ openssl rsautl -decrypt -inkey private.pem -in ciphertext.txt
Enter pass phrase for private.pem:
unable to load Private Key
140566548636992:error:06065064:digital envelope routines:EVP_DecryptFinal_ex:bad decrypt:../crypto/evp/evp_enc.c:610:
140566548636992:error:0906A065:PEM routines:PEM_do_header:bad decrypt:../crypto/pem/pem_lib.c:461:
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_4$ openssl rsautl -encrypt -inkey public.pem -pubin -in msg.txt -out ciphertext.txt
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_4$ cat ciphertext.txt
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_4$ openssl rsautl -decrypt -inkey private.pem -in ciphertext.txt
Enter pass phrase for private.pem:
Yasin_Çakar_s2921450_Workshop_4
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_4$

Task 4: Perform Hybrid Encryption

Assume we have a file named hybrid_plain.txt that has size larger than 5000 bits (e.g., the one you created in Task 3). In this Task, we encrypt it using hybrid encryption using RSA and AES implemented in OpenSSL.

1. Download the two bash scripts, hybrid_enc.sh and hybrid_dec.sh, from the Week 5 folder on http://networksecurity.griffith.internal.

   Answer:


Terminal
#!/bin/sh
# generate public/private key pair
if [! -e rsa.pub]; then
openssl genrsa -out rsa.key 4096
openssl rsa -in rsa.key -pubout -out rsa.pub
fi
generate a session key for symmetric encryption and encrypt it using RSA
openssl rand 32 > AESKey
openssl rsautl -encrypt -pubin -inkey rsa.pub -in AESKey -out AESKey_ecrypted
encrypt the plaintext with the session key
openssl aes-256-cbc -e -in hybrid_plain.txt -out hybrid_cipher.txt -pass file:A
ESKey -pbkdf2
remove the session key
rm AESKey
Terminal
#!/bin/sh
recover the session key
openssl rsautl -decrypt -inkey rsa.key -in AESKey_ecrypted -out AESKey
use the session key to decrypt the ciphertext
openssl aes-256-cbc -d -in hybrid_cipher.txt -out hybrid_decrypted.txt -pass fil
e:AESKey -pbkdf2
rm AESKey
1,1
All

2. Read the scripts and try to understand how they work.

   Answer:

   In the hybrid_enc.sh file, initially a private key is created, from this private key a public key is generated next.

   In the next two lines an AES key is generated and encrypted.

   Next the AES key is used to encrypt the file names “hybrid_plain.txt”, after which the AES key is deleted from the directory.

   In the decryption shell file operations occur in the reverse order. The AES key is decrypted to get the key in usable format, this key is then used to decrypt the ciphertext produced in the step explained above.

3. Run hybrid_enc.sh to encrypt the file hybrid_plain.txt.

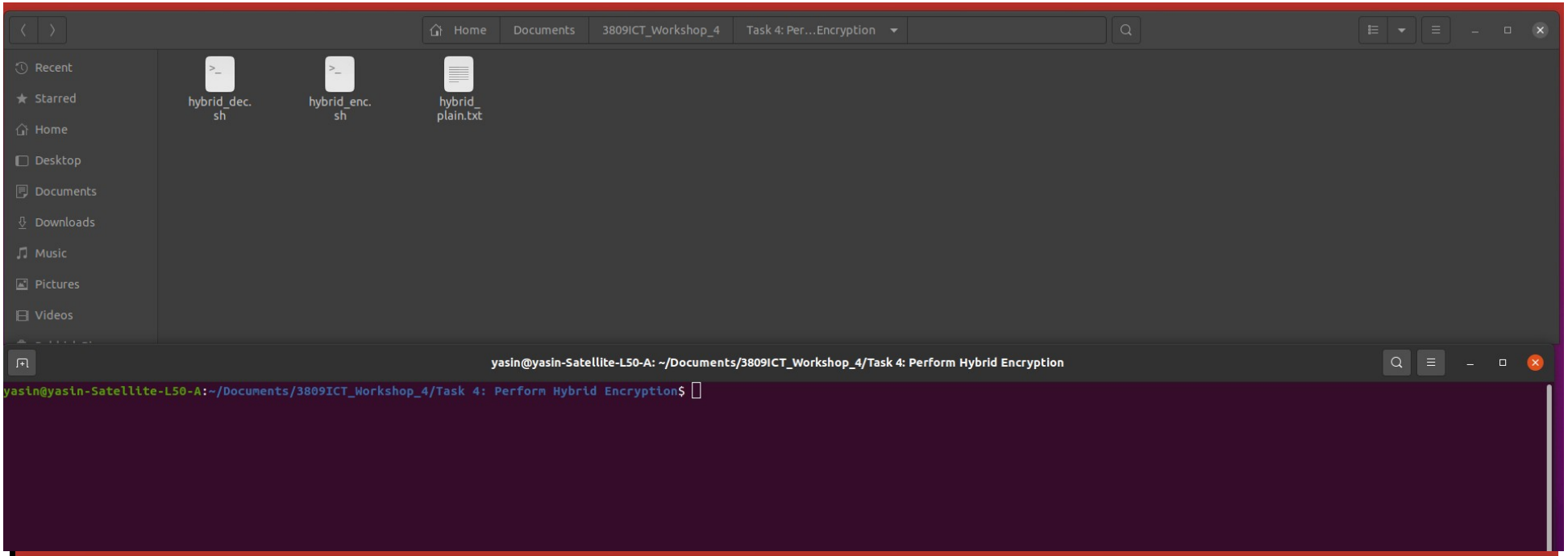
   ```
   $ sh hybrid_enc.sh
   ```

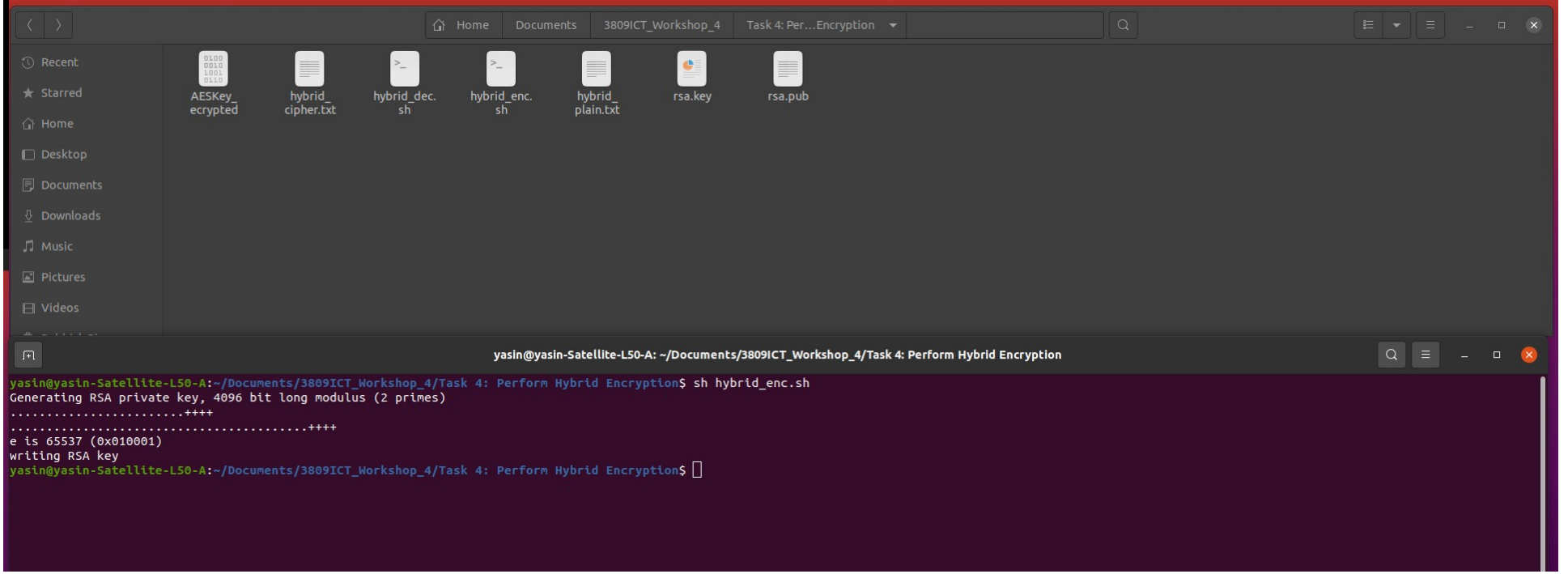
   Check the new files created after running the scripts.

   Q: Which files constitute the ciphertext of the hybrid encryption?

   Answer:

   The ciphertext file is the “hybrid_cipher.txt” file. After the execution of this shell command the original session key is deleted. All other files are the public keys used to encrypt the AES key, and the instructions to encrypt the plaintext file.

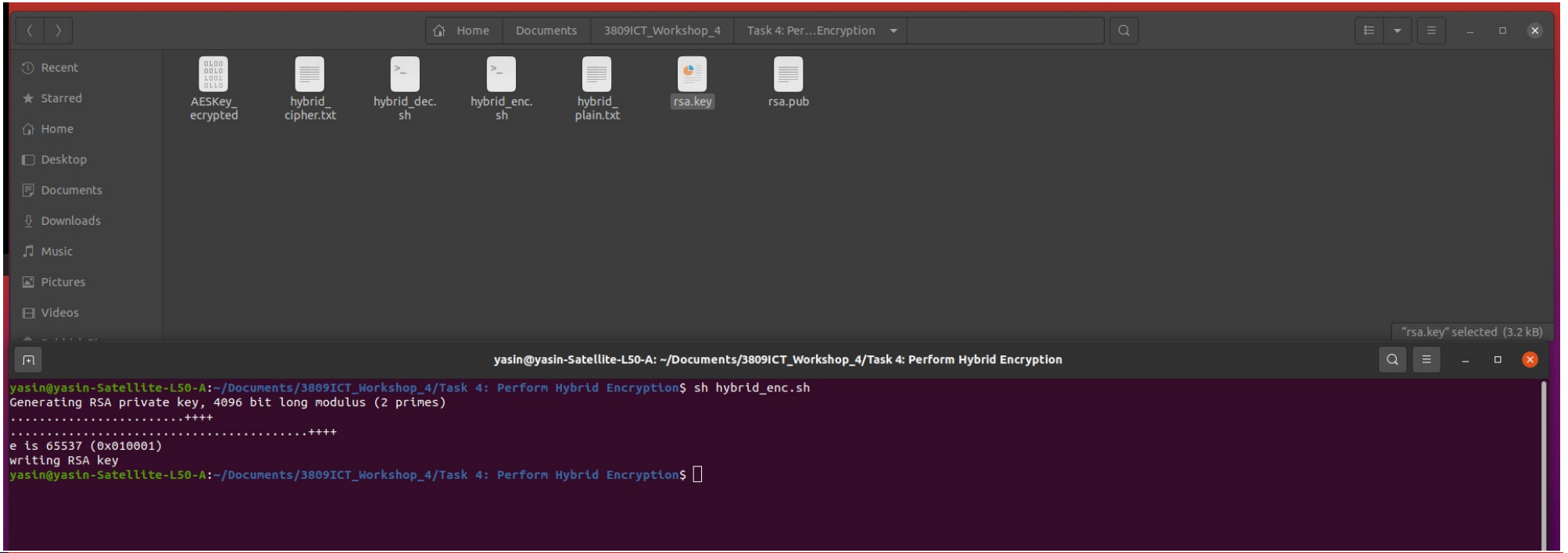

Home
Documents
3809ICT_Workshop_4
Task 4: Per…Encryption
Recent
Starred
Home
Desktop
Documents
Downloads
Music
Pictures
Videos
hybrid_dec.sh
hybrid_enc.sh
hybrid_plain.txt
yasin@yasin-Satellite-L50-A: ~/Documents/3809ICT_Workshop_4/Task 4: Perform Hybrid Encryption
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_4/Task 4: Perform Hybrid Encryption$

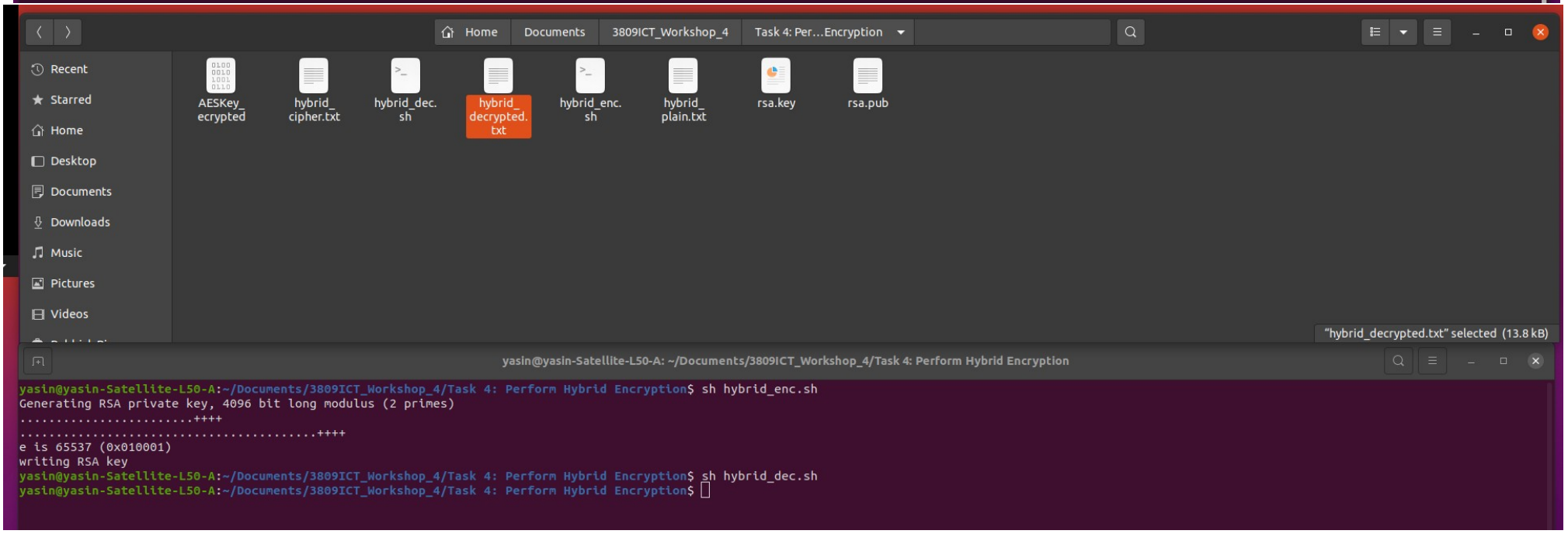

Home
Documents
3809ICT_Workshop_4
Task 4: Per…Encryption
Recent
Starred
Home
Desktop
Documents
Downloads
Music
Pictures
Videos
AESKey_ecrypted
hybrid_cipher.txt
hybrid_dec.sh
hybrid_enc.sh
hybrid_plain.txt
rsa.key
rsa.pub
yasin@yasin-Satellite-L50-A: ~/Documents/3809ICT_Workshop_4/Task 4: Perform Hybrid Encryption
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_4/Task 4: Perform Hybrid Encryption$ sh hybrid_enc.sh
Generating RSA private key, 4096 bit long modulus (2 primes)
.....++++
.....++++
e is 65537 (0x010001)
writing RSA key
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_4/Task 4: Perform Hybrid Encryption$

4. Run hybrid_dec.sh to decrypt the ciphertext. Check if the decryption worked.

   ```
   $ sh hybrid_dec.sh
   ```

   Answer:


Home
Documents
3809ICT_Workshop_4
Task 4: Per...Encryption
Recent
Starred
Home
Desktop
Documents
Downloads
Music
Pictures
Videos
AESKey_ecrypted
hybrid_cipher.txt
hybrid_dec.sh
hybrid_enc.sh
hybrid_plain.txt
rsa.key
rsa.pub
"rsa.key" selected (3.2 kB)
yasin@yasin-Satellite-L50-A: ~/Documents/3809ICT_Workshop_4/Task 4: Perform Hybrid Encryption
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_4/Task 4: Perform Hybrid Encryption$ sh hybrid_enc.sh
Generating RSA private key, 4096 bit long modulus (2 primes)
.....++++
.....++++
e is 65537 (0x010001)
writing RSA key
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_4/Task 4: Perform Hybrid Encryption$


Home
Documents
3809ICT_Workshop_4
Task 4: Per...Encryption
Recent
Starred
Home
Desktop
Documents
Downloads
Music
Pictures
Videos
AESKey_ecrypted
hybrid_cipher.txt
hybrid_dec.sh
hybrid_decrypted.txt
hybrid_enc.sh
hybrid_plain.txt
rsa.key
rsa.pub
"hybrid_decrypted.txt" selected (13.8 kB)
yasin@yasin-Satellite-L50-A: ~/Documents/3809ICT_Workshop_4/Task 4: Perform Hybrid Encryption
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_4/Task 4: Perform Hybrid Encryption$ sh hybrid_enc.sh
Generating RSA private key, 4096 bit long modulus (2 primes)
.....++++
.....++++
e is 65537 (0x010001)
writing RSA key
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_4/Task 4: Perform Hybrid Encryption$ sh hybrid_dec.sh
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_4/Task 4: Perform Hybrid Encryption$

Task 5: Calculate RSA Encryption/Decryption by Hand

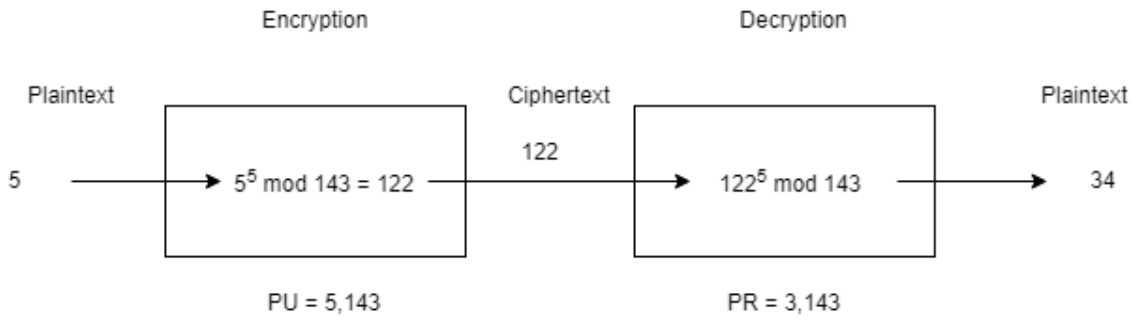
Bob somehow generates his RSA public key as (e = 5, n = 143) and private decryption key (d = 3, n=143).

1. What is the ciphertext of plaintext M = 5? Following the encryption process of RSA encryption algorithms, do the calculation and show the result.
   Answer:

$$M=5, C=E(PU, M)=M^e \bmod n¿ 5^5 \bmod 143¿ 122$$

2. Decrypt the ciphertext you obtained from step 1. Check whether the plaintext is recovered and give the reason.
   Answer:

$$D=E(PR, C)=C^d \bmod n¿ 122^3 \bmod 143¿ 34$$



What can be seen here is that the encryption and decryption keys are not mathematically related, so Bob has made a mistake in either choosing two prime values to produce ϕ(n) or has made an error in executing the two prime numbers in the formula to produce a public key and a private key where both are mathematically related through the mathematical expression ed = 1 • (mod ϕ(n)).

Acknowledgement: This lab instruction is partially based on the SEED labs from the SEED project led by Professor Wenliang Du, Syracuse University.