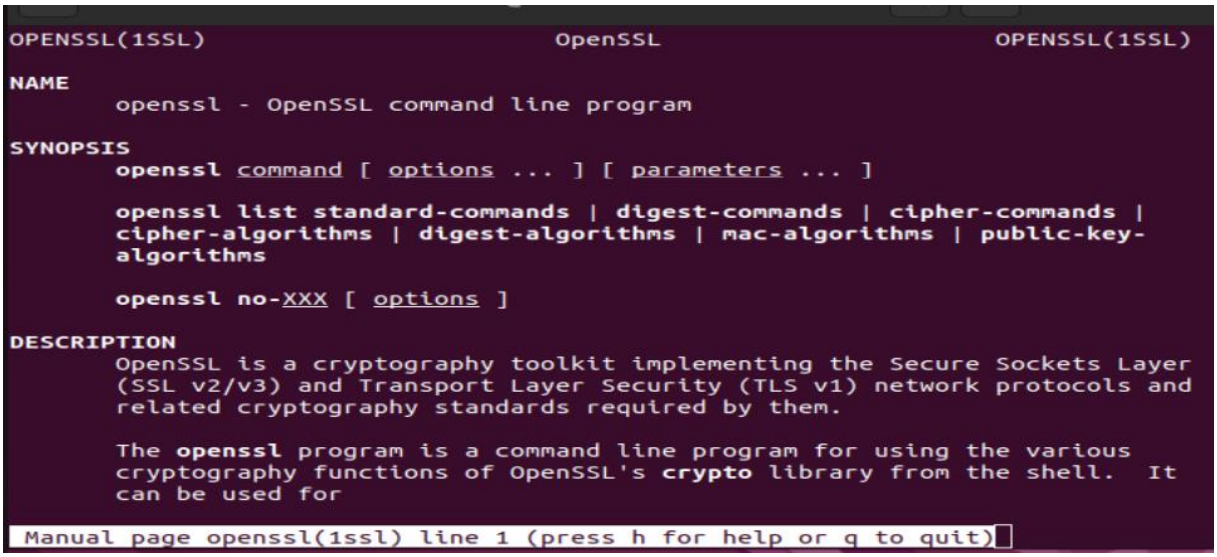
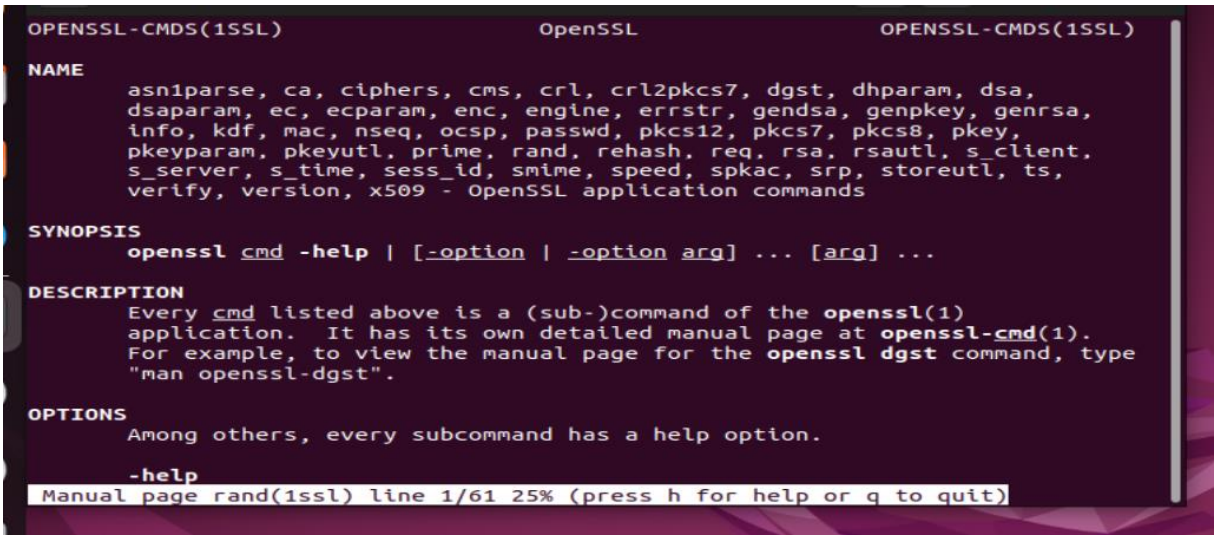
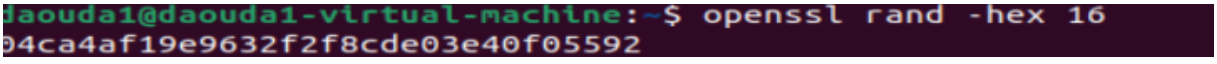
Rapport de TP openssl

Presentation generale :





Générateur pseudo aléatoire :



Clés secrètes

```
daouda1@daouda1-virtual-machine:~$ touch test
daouda1@daouda1-virtual-machine:~$ openssl enc -bf-cbc -in test -out test.chiffre
enter BF-CBC encryption password:
Verifying - enter BF-CBC encryption password:
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
Error setting cipher BF-CBC
40D733A6A67F0000:error:0308010C:digital envelope routines:inner_evp_generic_fetch:uns
upported:../crypto/evp/evp_fetch.c:349:Global default library context, Algorithm (BF-
CBC : 11), Properties ()
daouda1@daouda1-virtual-machine:~$
```

```
daouda1@daouda1-virtual-machine:~$ openssl enc -bf-cbc-d -in test.chiffre -out test.d
echiffre
enc: Unknown cipher: bf-cbc-d
enc: Use -help for summary.
40F7FAC3377F0000:error:0308010C:digital envelope routines:inner_evp_generic_fetch:uns
upported:../crypto/evp/evp_fetch.c:349:Global default library context, Algorithm (bf-
cbc-d : 0), Properties (<null>)
```


b6edd10559b20cb0a3ddaeb15e5267cc

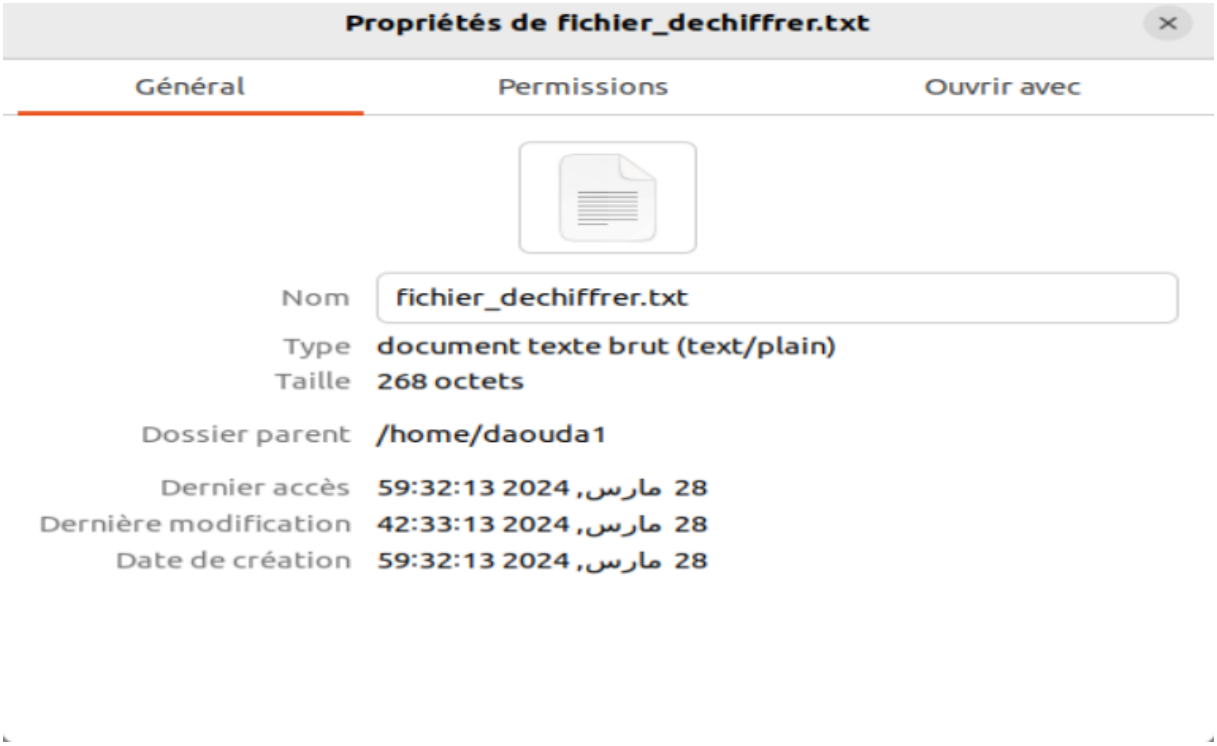
b6edd10559b20cb0a3ddaeb15e5267cc : motdepasse

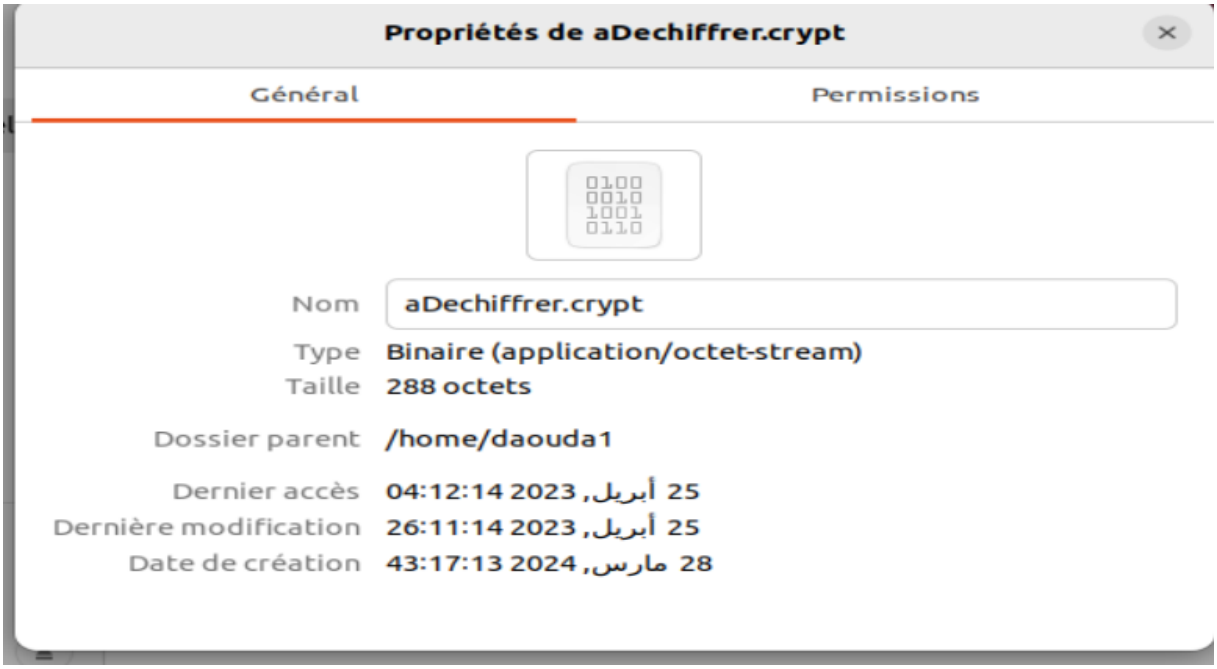
42b4d74317a4a6a995b1324b2ab7a75a

Un ou plusieurs hashs ne semblent pas valides.

Encrypt Decrypt

```
daouda1@daouda1-virtual-machine:~$ openssl enc -des-ede-cbc -d -in aDechiffrer.crypt -out fichier_dechiffrer.txt -pass pass:printemp
s
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
daouda1@daouda1-virtual-machine:~$ cat fichier_dechiffrer.txt
April 25th, 2023;

We are in ENSA of Khouribga, Moulau Sultan Sulimane University of Beni Mellal;


Hello IRIC Students

If you come to read this message, this means you have successfully decrypted the targeted file.

Congratulations !!!


See you in next labs
```


Propriétés de fichier_dechiffrer.txt
Général
Permissions
Ouvrir avec
Nom
fichier_dechiffrer.txt
Type
document texte brut (text/plain)
Taille
268 octets
Dossier parent
/home/daouda1
Dernier accès
59:32:13 2024 ,مارس 28
Dernière modification
42:33:13 2024 ,مارس 28
Date de création
59:32:13 2024 ,مارس 28


Propriétés de aDechiffrer.crypt
Général
Permissions
Nom
aDechiffrer.crypt
Type
Binaire (application/octet-stream)
Taille
288 octets
Dossier parent
/home/daouda1
Dernier accès
04:12:14 2023 ,أبريل 25
Dernière modification
26:11:14 2023 ,أبريل 25
Date de création
43:17:13 2024 ,مارس 28

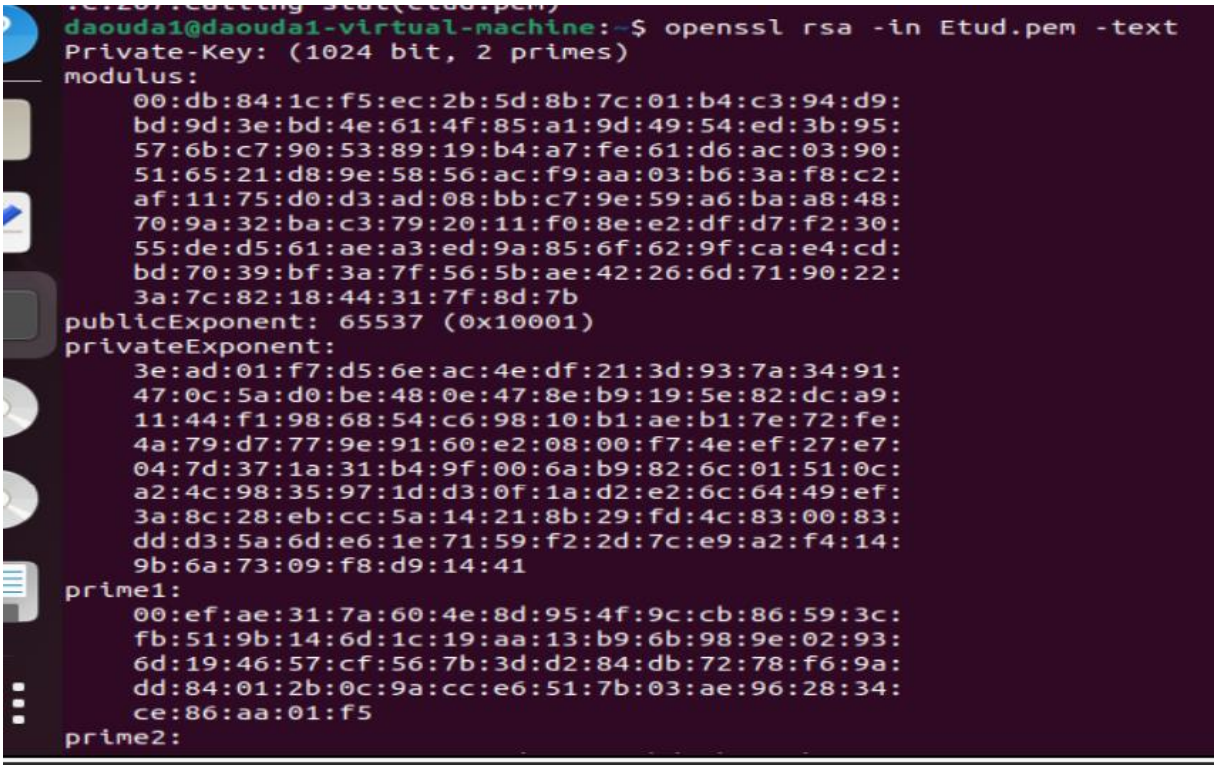

Propriétés de aDechiffrer.crypt
Général
Permissions
Nom
aDechiffrer.crypt
Type
Binaire (application/octet-stream)
Taille
288 octets
Dossier parent
/home/daouda1
Dernier accès
04:12:14 2023 ,أبريل 25
Dernière modification
26:11:14 2023 ,أبريل 25
Date de création
43:17:13 2024 ,مارس 28

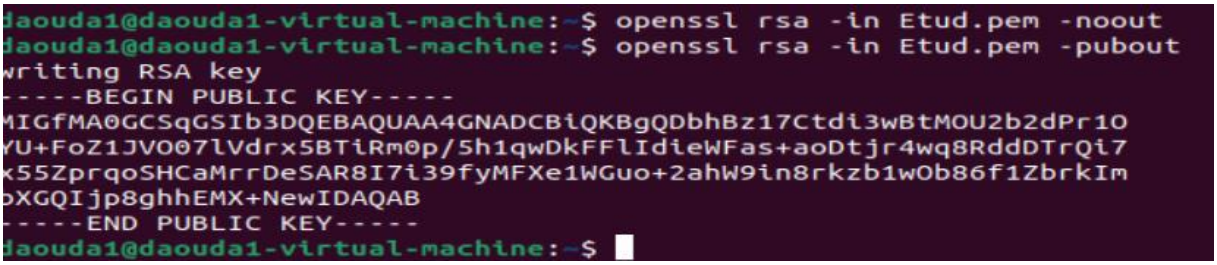
Clés publiques :

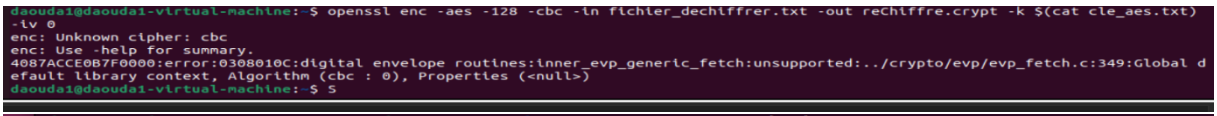
```
daouda1@daouda1-virtual-machine:~$ openssl genrsa -out courte.pem 512
daouda1@daouda1-virtual-machine:~$ openssl genrsa -out Etud.pem 1024
daouda1@daouda1-virtual-machine:~$ ls
aDechiffrer.crypt  clair.txt   Etud.pem               Images    Public           test
aDechiffrer.zip    courte.pem  fichier_dechiffrer     Modèles   snap             test.chiffre
Bureau             Documents   fichier_dechiffrer.txt Musique  Téléchargements  Vidéos
daouda1@daouda1-virtual-machine:~$
```

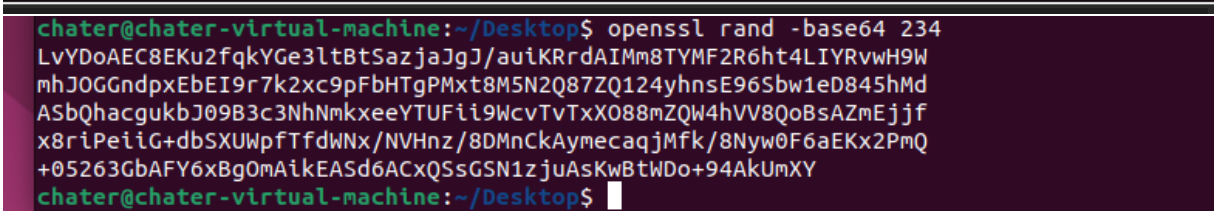

```
daouda1@daouda1-virtual-machine:~$ openssl genrsa -out courte.pem 512
daouda1@daouda1-virtual-machine:~$ openssl genrsa -out Etud.pem 1024
daouda1@daouda1-virtual-machine:~$ ls
aDechiffrer.crypt  clair.txt   Etud.pem               Images    Public           test
aDechiffrer.zip    courte.pem  fichier_dechiffrer     Modèles   snap             test.chiffre
Bureau             Documents   fichier_dechiffrer.txt Musique  Téléchargements  Vidéos
daouda1@daouda1-virtual-machine:~$
```


```
daouda1@daouda1-virtual-machine:~$ openssl rsa -in courte.pem -text
Private-Key: (512 bit, 2 primes)
modulus:
    00:c1:d8:2c:ea:1a:87:a2:46:31:32:a1:77:ee:21:
    f5:f8:47:36:f6:8a:8a:01:32:96:5f:97:f1:7a:a4:
    ac:52:b1:e1:f4:3c:50:d1:8c:a3:40:c7:20:08:86:
    93:e2:d2:30:e8:34:00:66:34:22:f9:3e:29:4f:f3:
    f9:73:b2:fe:d3
publicExponent: 65537 (0x10001)
privateExponent:
    0a:48:00:f9:d9:b6:5f:f1:01:23:02:55:6e:17:f7:
    07:d8:1f:1e:2c:72:ed:65:55:7c:74:7e:a6:56:9d:
    9d:35:22:40:b9:78:66:e9:58:da:3e:b1:96:3d:4c:
    52:4e:af:5f:ee:3f:28:d5:8e:5f:f5:4c:70:85:25:
    70:70:98:61
prime1:
    00:ff:6d:c4:cd:ef:05:1e:30:96:41:76:f3:ea:19:
    d2:01:bc:70:09:a9:2f:85:d4:fe:26:14:f6:58:e2:
    3f:8a:a7
prime2:
    00:c2:47:26:6a:67:d9:ba:6a:13:20:c8:72:f4:0d:
    1f:e0:52:88:3a:8f:e4:8f:c6:01:3c:3f:4a:f5:e2:
    04:eb:f5
exponent1:
    22:68:2a:e6:82:97:f1:e5:21:98:57:e9:ab:53:27:
    12:cc:cb:5a:c1:cb:80:ff:9b:ec:8d:4e:51:d2:c8:
    34:69
exponent2:
    0c:96:3b:80:ed:55:87:e4:53:74:ee:47:b4:54:1d:
    5a:95:3e:4a:3d:04:5b:e4:42:34:3b:0d:8a:3c:a8:
    80:f9
coefficient:
    00:ec:88:10:25:4b:81:7c:ec:c6:50:a7:df:af:98:
    40:d0:e7:a6:5b:48:24:3c:01:85:e5:da:43:db:c1:
```


daouda1@daouda1-virtual-machine:~$ openssl rsa -in Etud.pem -text
Private-Key: (1024 bit, 2 primes)
modulus:
00:db:84:1c:f5:ec:2b:5d:8b:7c:01:b4:c3:94:d9:
bd:9d:3e:bd:4e:61:4f:85:a1:9d:49:54:ed:3b:95:
57:6b:c7:90:53:89:19:b4:a7:fe:61:d6:ac:03:90:
51:65:21:d8:9e:58:56:ac:f9:aa:03:b6:3a:f8:c2:
af:11:75:d0:d3:ad:08:bb:c7:9e:59:a6:ba:a8:48:
70:9a:32:ba:c3:79:20:11:f0:8e:e2:df:d7:f2:30:
55:de:d5:61:ae:a3:ed:9a:85:6f:62:9f:ca:e4:cd:
bd:70:39:bf:3a:7f:56:5b:ae:42:26:6d:71:90:22:
3a:7c:82:18:44:31:7f:8d:7b
publicExponent: 65537 (0x10001)
privateExponent:
3e:ad:01:f7:d5:6e:ac:4e:df:21:3d:93:7a:34:91:
47:0c:5a:d0:be:48:0e:47:8e:b9:19:5e:82:dc:a9:
11:44:f1:98:68:54:c6:98:10:b1:ae:b1:7e:72:fe:
4a:79:d7:77:9e:91:60:e2:08:00:f7:4e:ef:27:e7:
04:7d:37:1a:31:b4:9f:00:6a:b9:82:6c:01:51:0c:
a2:4c:98:35:97:1d:d3:0f:1a:d2:e2:6c:64:49:ef:
3a:8c:28:eb:cc:5a:14:21:8b:29:fd:4c:83:00:83:
dd:d3:5a:6d:e6:1e:71:59:f2:2d:7c:e9:a2:f4:14:
9b:6a:73:09:f8:d9:14:41
prime1:
00:ef:ae:31:7a:60:4e:8d:95:4f:9c:cb:86:59:3c:
fb:51:9b:14:6d:1c:19:aa:13:b9:6b:98:9e:02:93:
6d:19:46:57:cf:56:7b:3d:d2:84:db:72:78:f6:9a:
dd:84:01:2b:0c:9a:cc:e6:51:7b:03:ae:96:28:34:
ce:86:aa:01:f5
prime2:


daouda1@daouda1-virtual-machine:~$ openssl rsa -in Etud.pem -noout
daouda1@daouda1-virtual-machine:~$ openssl rsa -in Etud.pem -pubout
writing RSA key
-----BEGIN PUBLIC KEY-----
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDbhBz17Ctdi3wBtMOU2b2dPr1O
YU+FoZ1JVO07lVdrx5BTiRm0p/5h1qwDkFFlIdieWFas+aoDtjr4wq8RddDTrQi7
x55ZprqoSHCaMrrDeSAR8I7i39fyMFXe1WGuo+2ahW9in8rkzb1wOb86f1ZbrkIm
bXGQIjp8ghhEMX+NewIDAQAB
-----END PUBLIC KEY-----
daouda1@daouda1-virtual-machine:~$


daouda1@daouda1-virtual-machine:~$ openssl enc -aes -128 -cbc -in fichier_dechiffrer.txt -out rechiffre.crypt -k $(cat cle_aes.txt)
-iv 0
enc: Unknown cipher: cbc
enc: Use -help for summary.
4087ACCE0B7F0000:error:0308010C:digital envelope routines:inner_evp_generic_fetch:unsupported:../crypto/evp/evp_fetch.c:349:Global d
efault library context, Algorithm (cbc : 0), Properties (<null>)
daouda1@daouda1-virtual-machine:~$ S

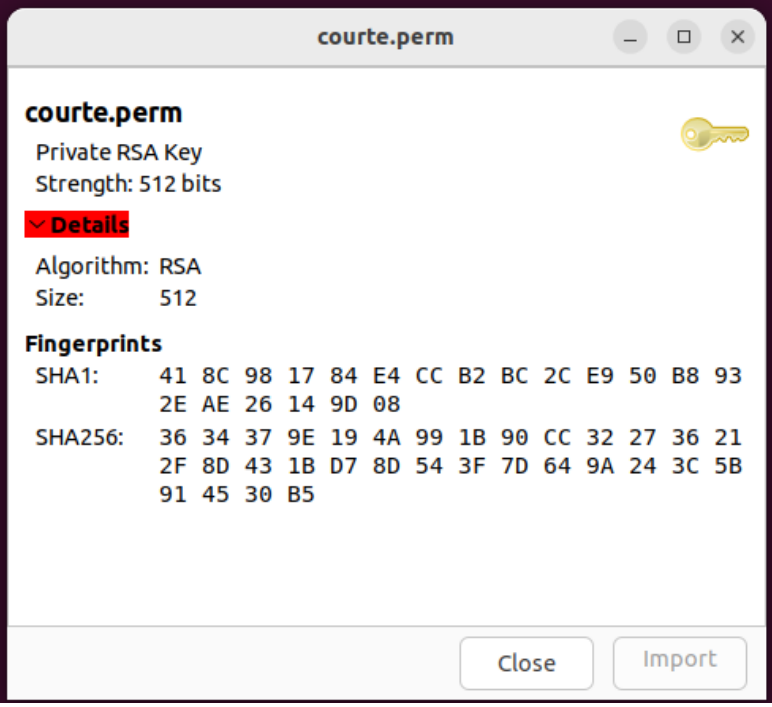

chater@chater-virtual-machine:~/Desktop$ openssl rand -base64 234
LvYDoAEC8EKu2fqkYGe3ltBtSazjaJgJ/auiKRrdAIMm8TYMF2R6ht4LIYRvwH9W
mhJOGGndpxEbEI9r7k2xc9pFbHTgPMxt8M5N2Q87ZQ124yhnsE96Sbw1eD845hMd
ASbQhacgukbJ09B3c3NhNmkxeeYTUFii9WcvTvTxXO88mZQW4hVV8QoBsAZmEjjf
x8riPeiiG+dbSXUWpfTfdWNx/NVHnz/8DMnCkAymecaqjMfk/8Nyw0F6aEKx2PmQ
+05263GbAFY6xBgOmAikEASd6ACxQSsGSN1zjuAsKwBtWDo+94AkUmXY
chater@chater-virtual-machine:~/Desktop$

```
chater@chater-virtual-machine:~$ openssl help
help:

Standard commands
asn1parse         ca                ciphers           cmp
cms               crl               crl2pkcs7         dgst
dhparam           dsa               dsaparam          ec
ecparam           enc               engine            errstr
fipsinstall       gendsa            genpkey           genrsa
help              info              kdf               list
mac               nseq              ocsp              passwd
pkcs12            pkcs7             pkcs8             pkey
pkeyparam         pkeyutl           prime             rand
rehash            req               rsa               rsautl
s_client          s_server          s_time            sess_id
smime             speed             spkac             srp
storeutl          ts                verify            version
x509

Message Digest commands (see the `dgst' command for more details)
blake2b512        blake2s256        md4               md5
rmd160            sha1              sha224            sha256
sha3-224          sha3-256          sha3-384          sha3-512
sha384            sha512            sha512-224        sha512-256
```

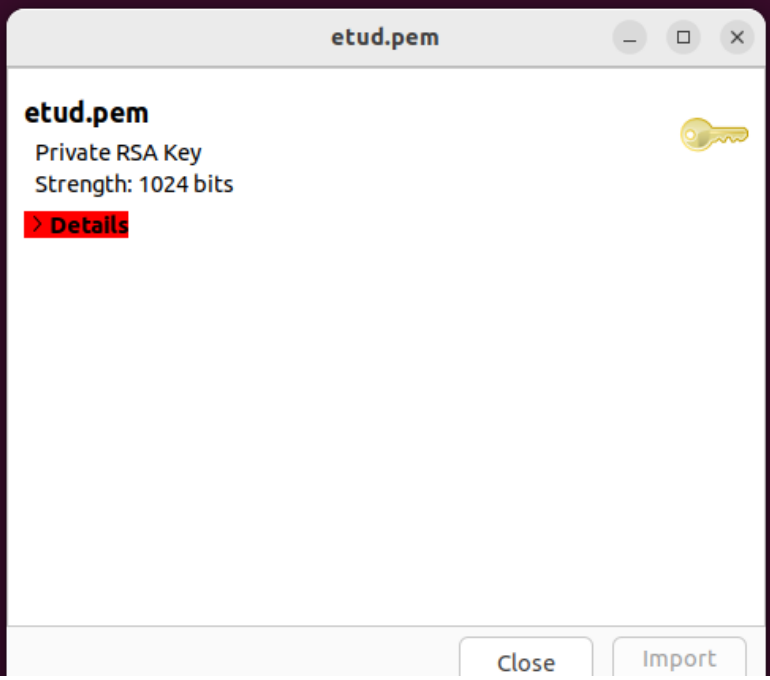
```
OPENSSL-CMDS(1SSL)                OpenSSL               OPENSSL-CMDS(1SSL)

NAME
       asn1parse, ca, ciphers, cms, crl, crl2pkcs7, dgst, dhparam, dsa,
       dsaparam, ec, ecparam, enc, engine, errstr, gendsa, genpkey, genrsa,
       info, kdf, mac, nseq, ocsp, passwd, pkcs12, pkcs7, pkcs8, pkey,
       pkeyparam, pkeyutl, prime, rand, rehash, req, rsa, rsautl, s_client,
       s_server, s_time, sess_id, smime, speed, spkac, srp, storeutl, ts,
       verify, version, x509 - OpenSSL application commands

SYNOPSIS
       openssl cmd -help | [-option | -option arg] ... [arg] ...

DESCRIPTION
       Every cmd listed above is a (sub-)command of the openssl(1)
       application.  It has its own detailed manual page at openssl-cmd(1).
       For example, to view the manual page for the openssl dgst command, type
       "man openssl-dgst".

OPTIONS
       Among others, every subcommand has a help option.

       -help
           Print out a usage message for the subcommand.

SEE ALSO
       openssl(1), openssl-asn1parse(1), openssl-ca(1), openssl-ciphers(1),
       openssl-cms(1), openssl-crl(1), openssl-crl2pkcs7(1), openssl-dgst(1),
       openssl-dhparam(1), openssl-dsa(1), openssl-dsaparam(1), openssl-ec(1),
       openssl-ecparam(1), openssl-enc(1), openssl-engine(1),
       openssl-errstr(1), openssl-gendsa(1), openssl-genpkey(1),
       openssl-genrsa(1), openssl-info(1), openssl-kdf(1), openssl-mac(1),
       openssl-nseq(1), openssl-ocsp(1), openssl-passwd(1), openssl-pkcs12(1),
       openssl-pkcs7(1), openssl-pkcs8(1), openssl-pkey(1),
       openssl-pkeyparam(1), openssl-pkeyutl(1), openssl-prime(1),
       openssl-rand(1), openssl-rehash(1), openssl-req(1), openssl-rsa(1),
       openssl-rsautl(1), openssl-s_client(1), openssl-s_server(1),
       openssl-s_time(1), openssl-sess_id(1), openssl-smime(1),
       openssl-speed(1), openssl-spkac(1), openssl-srp(1),
Manual page rand(1ssl) line 1/61 72% (press h for help or q to quit)
```

```
chater@chater-virtual-machine:~$ cd Desktop/
chater@chater-virtual-machine:~/Desktop$ touch text.txt
chater@chater-virtual-machine:~/Desktop$ openssl enc -bf-cbc -in text -out  text.chiffre^
C
chater@chater-virtual-machine:~/Desktop$ touch text.chiffre
chater@chater-virtual-machine:~/Desktop$ openssl enc -bf-cbc -in text -out  text.chiffre
Can't open "text" for reading, No such file or directory
807BD10707750000:error:80000002:system library:BIO_new_file:No such file or directory:../
crypto/bio/bss_file.c:67:calling fopen(text, rb)
807BD10707750000:error:10000080:BIO routines:BIO_new_file:no such file:../crypto/bio/bss_
file.c:75:
chater@chater-virtual-machine:~/Desktop$ openssl enc -bf-cbc -in text.txt -out  text.chif
fre
enter BF-CBC encryption password:
Verifying - enter BF-CBC encryption password:
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
Error setting cipher BF-CBC
803B5CF4FF720000:error:0308010C:digital envelope routines:inner_evp_generic_fetch:unsuppo
rted:../crypto/evp/evp_fetch.c:349:Global default library context, Algorithm (BF-CBC : 11
), Properties ()
chater@chater-virtual-machine:~/Desktop$
```

```
r@chater-virtual-machine:~/Desktop$ openssl enc -base64 -d -in text.chiffre -out tex
chiffre
r@chater-virtual-machine:~/Desktop$ cat text.dechiffre
r@chater-virtual-machine:~/Desktop$ openssl enc -base64 -d -in text.chiffre -out tex
chiffre
r@chater-virtual-machine:~/Desktop$ cat text.dechiffre
r@chater-virtual-machine:~/Desktop$ openssl rsa -in <fichier> <taille>
 syntax error near unexpected token `<'
r@chater-virtual-machine:~/Desktop$ openssl genrsa -out courte.perm 512
r@chater-virtual-machine:~/Desktop$
```



```
r@chater-virtual-machine:~/Desktop$ openssl enc -base64 -d -in text.chiffre -out tex
chiffre
r@chater-virtual-machine:~/Desktop$ cat text.dechiffre
r@chater-virtual-machine:~/Desktop$ openssl enc -base64 -d -in text.chiffre -out tex
chiffre
r@chater-virtual-machine:~/Desktop$ cat text.dechiffre
r@chater-virtual-machine:~/Desktop$ openssl rsa -in <fichier> <taille>
 syntax error near unexpected token `<'
r@chater-virtual-machine:~/Desktop$ openssl genrsa -out courte.perm 512
r@chater-virtual-machine:~/Desktop$ openssl genrsa -out etud.pem 1024
r@chater-virtual-machine:~/Desktop$
```




```
    44:93:08:a5:40:56:c3:cc:f3:61:59:c6:e0:87:ee:
    dc:17:db:e9:75:ec:b7:0b:f4:7b:d9:ce:de:8f:0b:
    2c:da:0f:00:54:32:47:72:e9:b5:21:15:3b:c8:b1:
    29:cd:51:38:3d
exponent1:
    00:9d:a9:51:7c:95:66:c7:cf:f3:f4:e5:fc:58:4e:
    3f:f1:6a:84:4e:d7:9a:09:9c:0b:1e:f4:8c:20:ef:
    63:71:2d:d2:59:90:14:c9:b1:3d:93:29:7d:95:29:
    82:54:d9:7f:be:a3:8d:fa:1e:92:d6:10:6e:3e:71:
    49:29:e0:20:01
exponent2:
    0f:43:19:2d:e3:56:d5:ad:9d:0c:18:06:d3:d5:cc:
    5e:09:57:2e:5d:83:03:53:84:b3:ab:44:d8:26:67:
    f2:78:cf:5c:99:67:79:35:55:5a:f9:23:c9:26:e6:
    8e:78:25:81:60:bb:27:63:06:2b:61:85:46:a9:b9:
    20:6b:8f:d1
coefficient:
    02:6f:14:6b:50:ea:fb:42:99:b2:bc:25:14:d1:c1:
    3b:a6:ce:45:02:53:ea:22:b4:6a:1a:9e:74:43:a7:
    cc:ba:2d:d6:1a:70:16:70:7d:59:e7:e9:fd:bb:4f:
    e0:89:d2:a9:17:79:c0:a7:43:19:f6:30:fc:30:fc:
    cb:9c:c6:d9
writing RSA key
-----BEGIN PRIVATE KEY-----
MIICdgIBADANBgkqhkiG9w0BAQEFAASCAmAwggJcAgEAAoGBAN5oIB95GHcB17Q/
e6UdIqIL5nKaxRyXlayEKrFkwAe0ZgClnfhniU1C2ucDHKCQG2AlepqrNzqBHMRD
apMqoJoudIZj5wN7KwMMFa/RXSsdwOCeRVFwzehJBDuWVMdPtUe0A1qeyYXtVvlo
WskbCP50cxzv66QGm+D5U3Mhkag9AgMBAAECgYA6rOnco8wKlZfo2964/ujGK7GO
hrp+ApfgPbYtutDWt4c5oHf+swIMOhkaXT3ONnaidQDVkVouuyVluguB6/sWdD0+
d0gYLU1lp+EVbQIsiwhdYqy72xovdqhAYfTxnul7F1gfW0rjJjV8+SsKpgZrpkpy
IwZHxPFXwmQeP2eAAQJBAPTEuNQNEiPFnHP2QY6pPr1X9Jt2//JbEQjjaDsQULtf
GR1g1mWy+nvga+N3xILRors2yfoVpLL9lphPIAbZMAECQQDonLja4Y+ooSUDZdwI
X0STCKVAVsPM82FZxuCH7twX2+l17LcL9HvZzt6PCyzaDwBUMkdy6bUhFTvIsSnN
UTg9AkEAnalRfJVmx8/z9OX8WE4/8WqETteaCZwLHvSMIO9jcS3SWZAUybE9kyl9
lSmCVNl/vqON+h6S1hBuPnFJKeAgAQJAD0MZLeNW1a2dDBgG09XMXglXLl2DA1OE
s6tE2CZn8njPXJlneTVVWvkjySbmjnglgWC7J2MGK2GFRqm5IGuP0QJAAm8Ua1Dq
+0KZsrwlFNHBO6bORQJT6iK0ahqedEOnzLot1hpwFnB9Wefp/btP4InSqRd5wKdD
GfYw/DD8y5zG2Q==
-----END PRIVATE KEY-----
```

Certificat :

```
chater@chater-virtual-machine:~/Desktop$ openssl req -new -key etud.pem -out marequete.pem
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:maroc
String too long, must be at most 2 bytes long
Country Name (2 letter code) [AU]:ma
State or Province Name (full name) [Some-State]:oued zem
Locality Name (eg, city) []:oued zem
Organization Name (eg, company) [Internet Widgits Pty Ltd]:ensa
Organizational Unit Name (eg, section) []:ensa
Common Name (e.g. server FQDN or YOUR name) []:chater
Email Address []:chater@gmail.iric

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:chater
An optional company name []:ensa
chater@chater-virtual-machine:~/Desktop$
```

```
chater@chater-virtual-machine:~/Desktop$ openssl req -in marequete.pem -text -noout
Certificate Request:
    Data:
        Version: 1 (0x0)
        Subject: C = ma, ST = oued zem, L = oued zem, O = ensa, OU = ensa, CN = chater, ema
ilAddress = chater@gmail.iric
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (1024 bit)
                Modulus:
                    00:de:68:20:1f:79:18:77:01:d7:b4:3f:7b:a5:1d:
                    22:a2:0b:e6:72:9a:c5:1c:97:95:ac:84:2a:b1:64:
                    c0:07:b4:66:00:a5:9d:f8:67:89:4d:42:da:e7:03:
                    1c:a0:90:1b:60:25:7a:9a:ab:37:3a:81:1c:c4:43:
                    6a:93:2a:a0:9a:2e:74:86:63:e7:03:7b:2b:03:0c:
                    15:af:d1:5d:2b:1d:c0:e0:9e:45:51:70:cd:e8:49:
                    04:3b:96:54:c7:4f:b5:47:b4:03:5a:9e:c9:85:ed:
                    56:f9:68:5a:c9:1b:08:fe:74:73:1c:ef:eb:a4:06:
                    9b:e0:f9:53:73:21:91:a8:3d
                Exponent: 65537 (0x10001)
        Attributes:
            unstructuredName         :ensa
            challengePassword        :chater
            Requested Extensions:
    Signature Algorithm: sha256WithRSAEncryption
    Signature Value:
        a3:08:4e:9d:25:cb:a6:fc:2a:8c:3b:c1:07:00:a3:39:6e:a8:
        80:78:8a:21:86:b8:dd:d5:e4:50:f1:31:fc:b6:9b:1b:3b:c2:
        d6:5c:be:00:c5:01:00:6b:ea:f9:b3:2d:07:7a:7a:2a:d4:92:
        0a:6d:4a:11:1f:af:0e:8f:5a:a1:b0:00:e4:cd:07:95:5c:cc:
        d4:bf:db:9b:ff:10:9d:14:c3:00:f4:25:44:bb:88:23:30:0b:
        22:be:9c:64:19:fe:64:9e:e1:f3:5a:0e:de:1e:d0:e1:27:87:
        de:28:18:e7:69:b5:eb:bf:ca:9d:9b:cd:8c:2d:03:90:b5:81:
        fb:1b
chater@chater-virtual-machine:~/Desktop$
```


PAR :

Chater Ahmed

Coulibaly Daouda David