

OpenSSL

Create Example Reference File, let us create a 1GB large text file using the fallocate command:

```
fallocate -l 1024M test.txt  
echo "LinuxShellTips tutorial on encrypting a large file with OpenSSL in Linux" >> test.txt  
cat test.txt
```

Encrypt File with Password (?????)

```
openssl enc -aes-256-cbc -pbkdf2 -p -in test.txt -out test.txt.enc
```

- enc executes the symmetric key encryption process.
- -aes-256-cbc specifies the use of 256 bits cryptographic key.
- -pbkdf2 is the default algorithm being used.
- -p prints used salt, key, and IV.
- -in points to the input file.
- -out points to the output file.

To decrypt the file, run:

```
openssl aes-256-cbc -d -pbkdf2 -in test.txt.enc -out sample_decrypted.txt
```

“ You will be required to enter the encryption password you generated earlier.

Encrypt File with Key (?????)

```
# generate a key file  
openssl rand 256 > symmetric_keyfile.key  
# use the keyfile to encrypt our file  
openssl enc -in test.txt -out test.txt.enc -e -aes-256-cbc -pbkdf2 -k symmetric_keyfile.key
```

To decrypt the file, run:

```
openssl enc -in test.txt.enc -out draft_decrypted.txt -d -aes-256-cbc -pbkdf2 -k symmetric_keyfile.key
```

?????? (Asymmetric Encryption)

?????????????????????????????: data too large for key size.

```
dnyce@LinuxShellTips:~/LinuxShellTips_Files$ openssl rsautl -encrypt -inkey my_public_key.pem -pubin -in symmetric_keyfile.key -out symmetric_keyfile.key.enc
RSA operation error
140330343245120:error:0406D06E:rsa routines:RSA_padding_add_PKCS1_type_2:data too large for key size:../crypto/rsa/rsa_pk1.c:124:
dnyce@LinuxShellTips:~/LinuxShellTips_Files$ ls -l symmetric_keyfile.key
-rw-rw-r-- 1 dnyce dnyce 256 Cam  5 14:18 symmetric_keyfile.key
dnyce@LinuxShellTips:~/LinuxShellTips_Files$ openssl rsautl -encrypt -inkey my_public_key.pem -pubin -in test.txt -out test.txt.enc
RSA operation error
140589405889856:error:0406D06E:rsa routines:RSA_padding_add_PKCS1_type_2:data too large for key size:../crypto/rsa/rsa_pk1.c:124:
dnyce@LinuxShellTips:~/LinuxShellTips_Files$
```

“ TIP:
??
???

Hashing

????

```
# For file
openssl dgst -sha256 my.file

# For string
echo -n "HelloWorld" | openssl dgst -sha256
```

????

- [OpenSSL ??????????????????????](#)