Cryptography Notes

Example: decrypt using openssl in linux when the key and initialization vector is known -

openssl enc -pbkdf2 -nosalt -aes-256-cbc -d -in cipher.txt.enc -base64 -K 5284A3B154D99487D9D8D8508461A478C7BEB67081A64AD9A15147906E8E8564 -iv 1907C5E255F7FC9A6B47B0E789847AED

Example: create a new key and IV (run the following) -  
openssl enc -pbkdf2 -nosalt -aes-256-cbc -k [password here] -P > key\_and\_IV

Example: view the new key\_and\_IV file -

key=E11244295150E6713CD76E9A5112347093BDB6ACBF0C8021ABAE29881130B210

iv =6B7F0C406297F0D90E3BD65AD1FB94BA

Example: encrypt a message with a newly created Key and IV -

openssl enc -pbkdf2 -nosalt -aes-256-cbc -in meetingplace\_update.txt -out meetingplace\_update.txt.enc -base64 -K E11244295150E6713CD76E9A5112347093BDB6ACBF0C8021ABAE29881130B210 -iv 6B7F0C406297F0D90E3BD65AD1FB94BA