OPENSSL Tutorial

Install OpenSSL from https://www.openssl.org

Download and install OpenSSL from https://www.openssl.org/source/ Use openSSL version 3.0
Installation instructions are https://github.com/openssl/openssl/blob/master/INSTALL.md

After you install try out small examples.
Demo folder contains small examples. Try out examples.
Create Folder Examples. Download a file, say unsw-logo.jpeg.
Practice exercises on symmetric ciphers.
Try out simple examples using your command prompt.

1. **AES:** Check the list of available ciphers with openssl list-cipher-commands.
2. **AES Encryption:** openssl enc -aes-128-cbc -pass pass:comp6453 -p -in unsw-logo.jpeg -out unsw.enc
3. This creates a new file unsw.enc. Open it and see what it reads like.
4. **AES Decryption:** openssl enc -aes-128-cbc -pass pass: comp6453 -p -d -in unsw.enc -out new.jpeg
5. **This creates another new file new.**jpeg. Check if it matches the original file.

Understanding AES.
Encryption

1. -aes-128-cbc — the cipher name(symmetric cipher : AES-128 in CBC mode)
2. -pass pass:<password> — to specify the password (here password is comp6453)
3. -P — Print out the salt, key and IV used.
4. -in file— input file /input file absolute path (here unsw-logo.jpeg)
5. -out file— output file /output file absolute path(here unsw.enc)

Decryption

6. -d: Decryption
7. -in file— input file /input file absolute path (here the encrypted file unsw.enc)
8. -out file— output file /output file absolute path(here new.jpeg)

Note: Salt is used for password-based key, so that the same password does not yielf the same key. In the case of openSSL, it chooses a IV. If you are using AES in a c code with openssl library you can input the IV.

Play with other ciphers and the configurations like AES-256 in different modes, RC4 etc.

Practice exercises on Hash Functions.

1. openssl dgst -sha256 unsw-logo.jpeg
2. Verify with your default sha function provided by your OS. For example in MACOS, shasum -a 256 unsw-logo.jpeg yields the same value.
3. Play with other parameters and other hash functions like MD5, SHA3 etc.

Check how Crypto algorithms are implemented. The c sources are available in the crypto folder in your openssl/demos folder.