Symmetric Key Encryption and Decryption using OpenSSL and AES Symmetric Key Algorithm

# OpenSSL Installation

## Windows

**Link to Video:**

<https://youtu.be/Ts-gBfAW28c>

If you are using Microsoft Windows operating system, then download and install OpenSSl from the following link:

<http://downloads.sourceforge.net/gnuwin32/openssl-0.9.8h-1-bin.zip>

Unzip the file.

Locate the openssl.exe file in the **bin** folder.

Double click the openssl.exe file, you will see a window opens with the following promp:

OpenSSL> ***[type your commands here]***

You are ready to run OpenSSL command.

## MacOS

OpenSSL is already installed on your Mac computer.

In your Mac, run the Terminal application.

In the Terminal window, type openssl and press Enter.

See next page for more instructions…

# **Encrypting a text file using the AES Symmetric Key Algorithm**

Assume that you have a plain-text file, called **textFile.txt**, with your name and student ID in that file. The may look like the followings:

**textFile.txt**

|  |
| --- |
| *Student ID: S1234567*  *Name: ABCDEF* |

**Link to Video:** <https://drive.google.com/file/d/1eT8Vf8kpun7qVBCaz-wArvSsYFaJ4hph/view?usp=sharing>

Encrypt the text file generates a binary ciphertext file called **secret.txt** using the following command:

**aes-256-ecb -in textFile.txt -out secret.txt**

Now a password will be asked. Enter 1234 as password.

**Decrypting a ciphertext file using the AES Symmetric Key Algorithm**

Decrypt the **secret.txt** file using the following command to obtain the plaintext file:

**aes-256-ecb -d -in secret.txt -out decrypt.txt**

Enter 1234 as password.

Check the file **decrypt.txt** where you should find the same content as in **textFile.txt**.