Symmetric Encryption

OpenSSL has libcrypto library that contains functions for encryption and decryption. This program explores the evp.h library. The basis of the code is this wiki: https://wiki.openssl.org/index.php/EVP_Symmetric_Encryption_and_Decryption.

Source Code

The program is composed of four functions including the main(). The handleError() function is from the wiki entry and catches the possible errors when invoking the EVP methods. encrypt() does the main encryption. It gets the source file from the main() and read the whole file to prepare the encryption. There are 3 important functions for the encryption - EVP_EncryptInit(), which takes in the mode of encryption, the key, and the initialization vector; EVP_EncryptUpdate(); for updating the size of the ciphertext; and EVP_EncryptFinal() for finalizing the result. At this point, the code will have written the encrypted cipher to cbc_ciphertext.txt.

Subsequently, decryption of the ciphertext will be done. In this function, EVP_DecryptInit(), EVP_DecryptUpdate(), and EVP_DecryptFinal() are the main proponents.

Result

After running the program, there should be two files created - cbc_ciphertext.txt and cbc_decrypted.tiff

ECB Mode

The two codes are almost identical except for the fact ECB mode doesn't need an initialization vector.