Task 1: Image Encryption with ECB and CBC

1. Image Encryption with Electronic Code Book(ECB)

When ECB is used, our encrypted image is similar to original image. There are more than one reason for it. Firstly, ECB encryption mode does not use initial vector because this encryption mode encrypt image block by block. Secondly, ECB is basic version of blockcipher encryption. In ECB, ciphertext related to plaintext, so encrypted image wich ECB used for it can be decrypted successfully.

This command can be used to encrypt an original image:

-$ openssl enc -aes-128-ecb -in original.bmp -out ecb.bmp -K
-$ 00112233445566778889aabbccddeeff

2. Image Encryption with Cipher Block Chain(CBC)

When CBC is used, our encrypted image is not similar to original image. There are more than one reason for it. Firstly, CBC encryption mode uses initial vector. In this mode, encrypted blocks are used from next block as a input. Therefore, first block of text need initial vector. Secondly, CBC is improved mode of encryption modes. CBC encryption mode have some advantages. It provide secure encryption to us because it use xor operation in encryption. Xor operation is used for all blocks with previous block. Therefore, encrypted image does not similar to original image.

This command can be used to encrypt an original image:

-$ openssl enc -aes-128-cbc -in original.bmp -out cbc.bmp -K
-$ 00112233445566778889aabbccddeeff -iv 0102030405060708