Task 2

The image named original.bmp is encrypted using both ECB and CBC modes.

aes-256-ecb

Key generation: openssl rand -hex 32

Encryption: openssl enc -aes-256-ecb -e -in original.bmp -out aes-256-ecb_encrypted_image.bmp -K 49eb92082f8aa10901a012fb6c6099d72762a4916a41e07d9b667ff4da3bc9c3

aes-256-cbc

Key generation: openssl rand -hex 32

Iv generation: openssl rand -hex 16

Encryption: openssl enc -aes-256-cbc -e -in original.bmp -out aes-256-cbc_encrypted_image -K 4527a64b77cd37c8008b5b6ec10c8a81ff22dada3e551bb7cf01a4d52fa60e0b -iv aa094344c6fa88ee76ad64562875305b

The following commands were used to open the encrypted images:

ghex aes-256-ecb_encrypted_image.bmp &

ghex aes-256-cbc_encrypted_image.bmp &

The following command was used to open the original image:

ghex original.bmp &

Then, the first 54 bytes of the encrypted images were replaced by those of the original image.

Observation:

The original image contains a flower. The image encrypted in ecb mode looks slightly similar to the original image, but no flower like pattern was recognization. But this lacks diffusion. On the other hand, the image encrypted in cbc mode is completely different from the original image and unrecognizable. It has more diffusion than ecb mode.