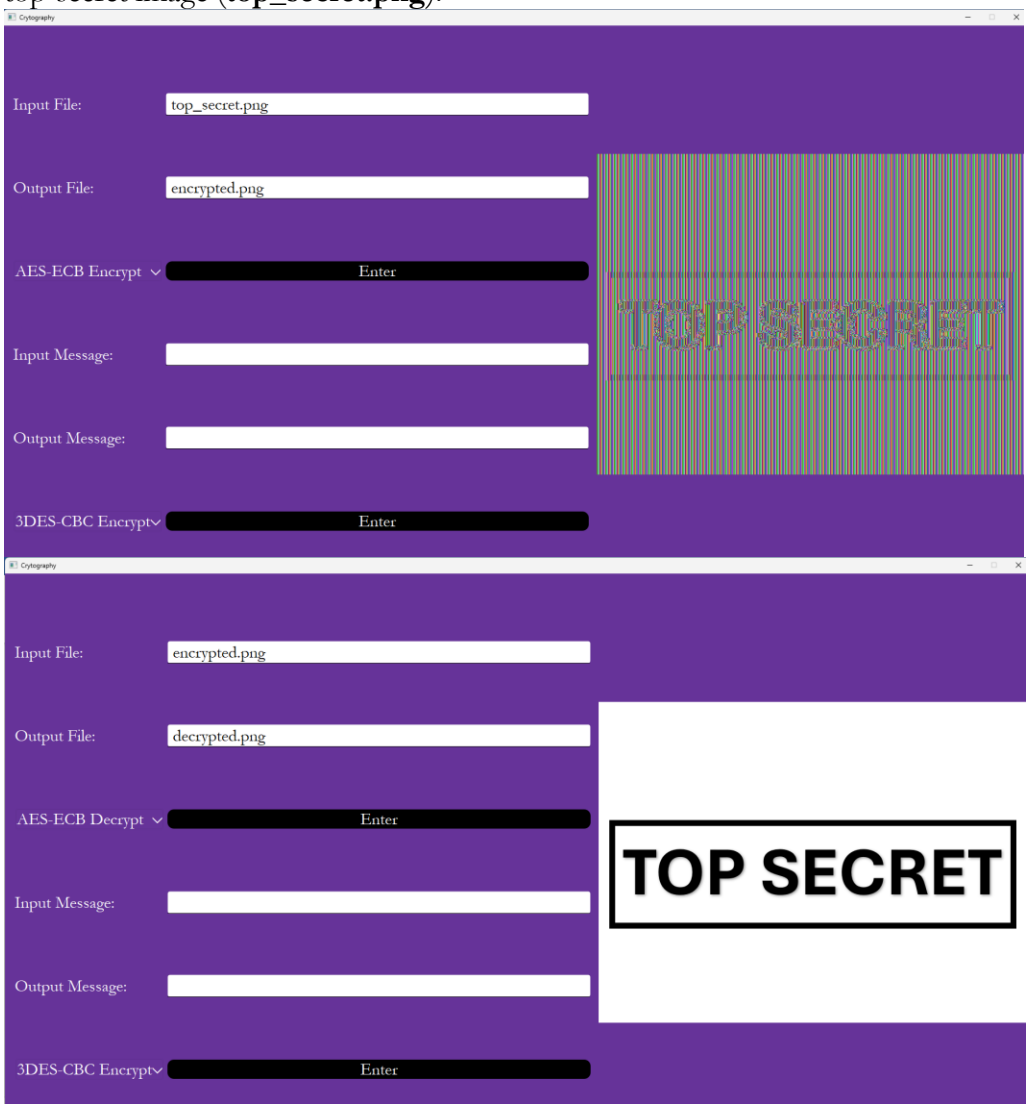
COSC 3364 – Principles of Cybersecurity
Lab 02
Advanced Encryption Standard

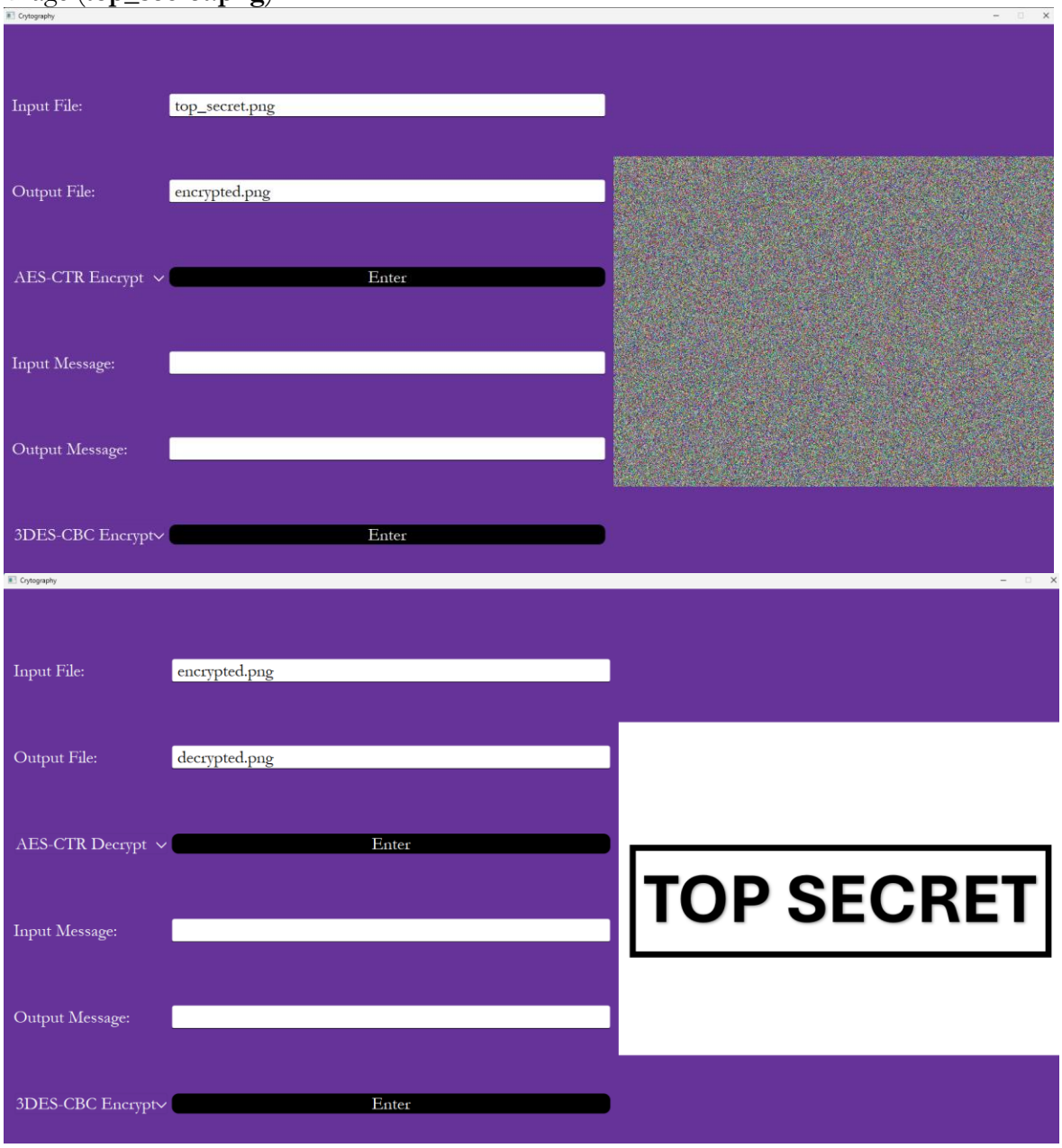
1. Develop functions named **aes_ecb_encrypt_img()** & **aes_ecb_decrypt_img** that accepts an input image filename and output image filename to perform AES encryption using block cipher mode: Electronic Codebook. Take a screenshot of the application with the encrypted and then decrypted top-secret image (**top_secret.png**).



   a. What happened with the image after encryption?
      The image became harder to read. However, the image can still be read even after encryption.

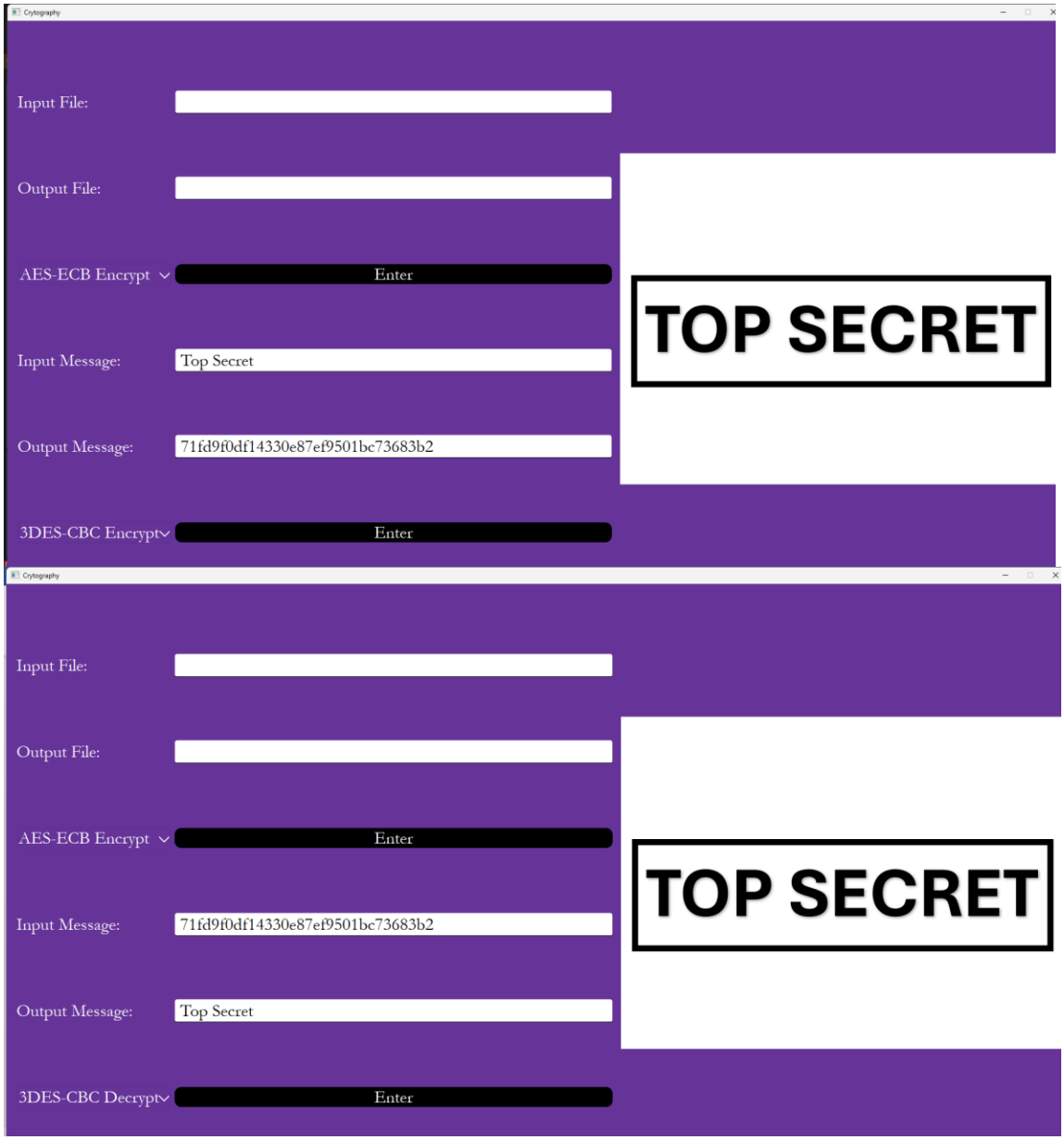
   b. Why did this occur?
      Because AES is a block encryption, when using ECB, the regularities of data can be seen. The simplicity of the image allows for the black pixels to be seen over the white ones.

2. Develop functions named **aes_ctr_encrypt_img()** & **aes_ctr_decrypt_img** that accepts an input image filename and output image filename to perform AES encryption using block cipher mode: Counter. Take a screenshot of the application with the encrypted and then decrypted top-secret image (**top_secret.png**).



Triple Data Encryption Standard

1. Develop a function named **des3_cbc_encrypt_msg()** & **des3_cbc_decrypt_msg()** that accepts and returns plaintext/ciphertext respectively to perform 3DES encryption using block cipher mode: Cipher Block Chaining. Take a screenshot of the application with the encrypted and then decrypted top-secret message ("**Top Secret**").



Helpful Functions

cv2.imread(filename[, flags])->retval

The function imread loads an image from the specified file and returns it.

Parameters:

filename – Name of file to be loaded

flags – Flag that can take values of cv::ImreadModes

cv2.imwrite(filename, img[, params])->retval

The function imwrite saves the image to the specified file.

Parameters:

filename – Name of file to be written

img – Image to be saved

params – Format-specific parameters encoded as pairs, see cv::ImwriteFlags