COSC 3364 – Principles of Cybersecurity
Lab 02

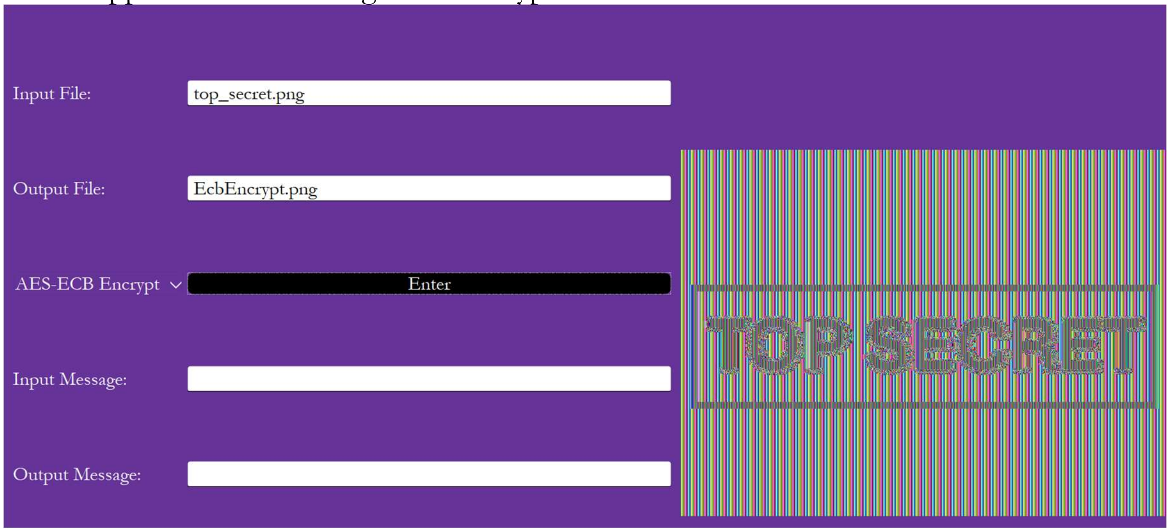
Ethan Conner

09/04/2024

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?



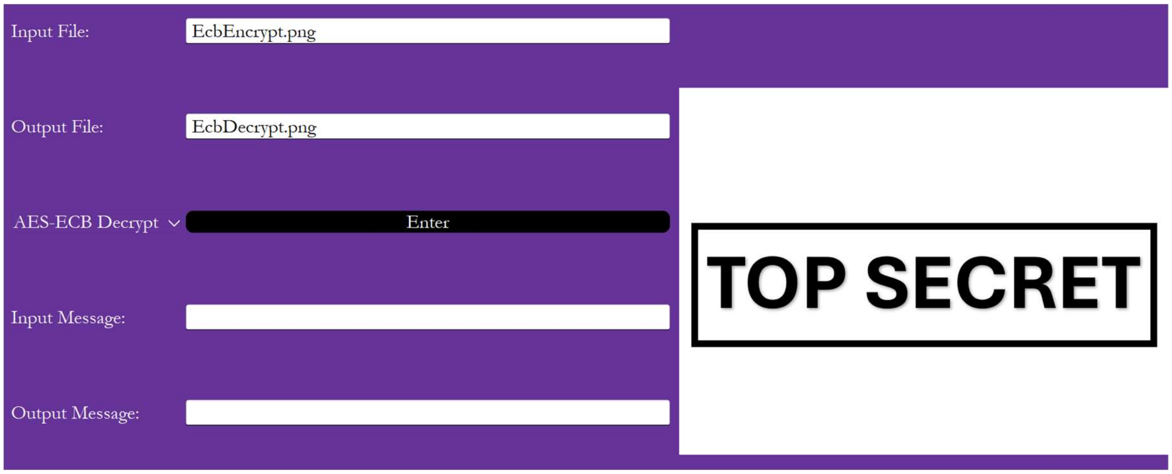
Input File: top_secret.png

Output File: EcbEncrypt.png

AES-ECB Encrypt

Input Message:

Output Message:



Input File: EcbEncrypt.png

Output File: EcbDecrypt.png

AES-ECB Decrypt

Input Message:

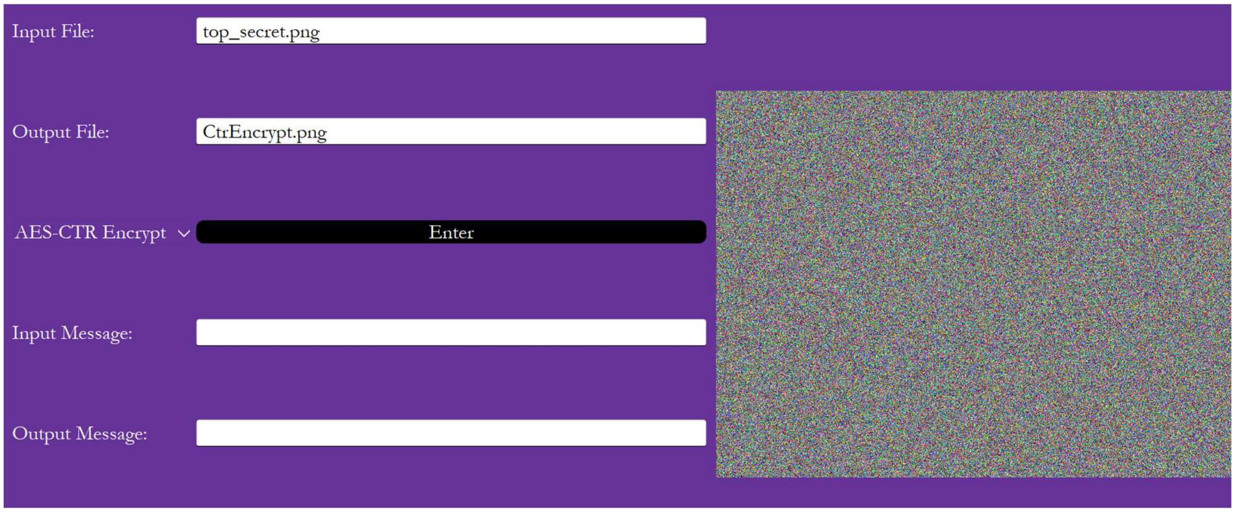
Output Message:

The image turned slightly harder to read, but was still recognizable.

   b. Why did this occur?

AES is a block encryption so when you use ECB mode the regularities of data can be seen by doing block encryption. Similar colors (black letters on white background) can be seen.

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**).



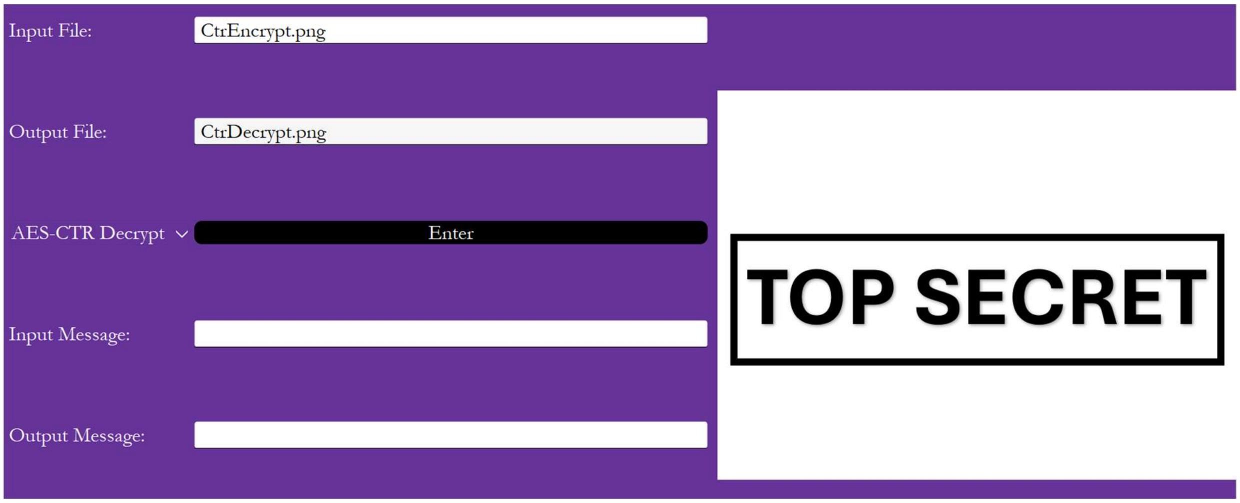
Input File: top_secret.png

Output File: CtrEncrypt.png

AES-CTR Encrypt

Input Message:

Output Message:



Input File: CtrEncrypt.png

Output File: CtrDecrypt.png

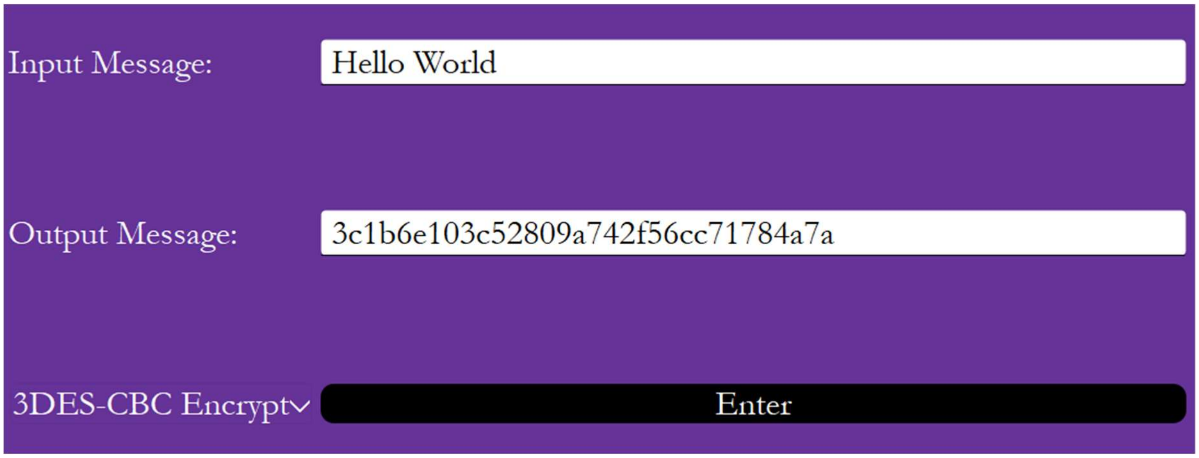
AES-CTR Decrypt

Input Message:

Output Message:

Triple Data Encryption Standard

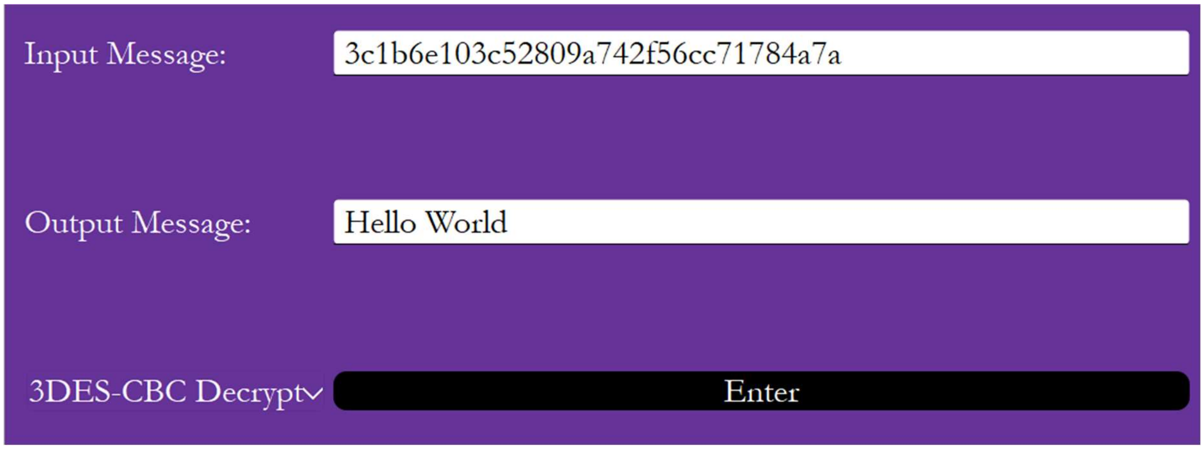
1. Develop a function named **des3_cbc_encrypt_msg()** & **des3_cbc_decrypt_msg()** that accepts and returns plaintext/ciphertext respectively to perform 3DES encryption using block cipher mode: Cipher Block Chaining. Take a screenshot of the application with the encrypted and then decrypted top-secret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



Input Message: Hello World

Output Message: 3c1b6e103c52809a742f56cc71784a7a

3DES-CBC Encrypt



Input Message: 3c1b6e103c52809a742f56cc71784a7a

Output Message: Hello World

3DES-CBC Decrypt

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