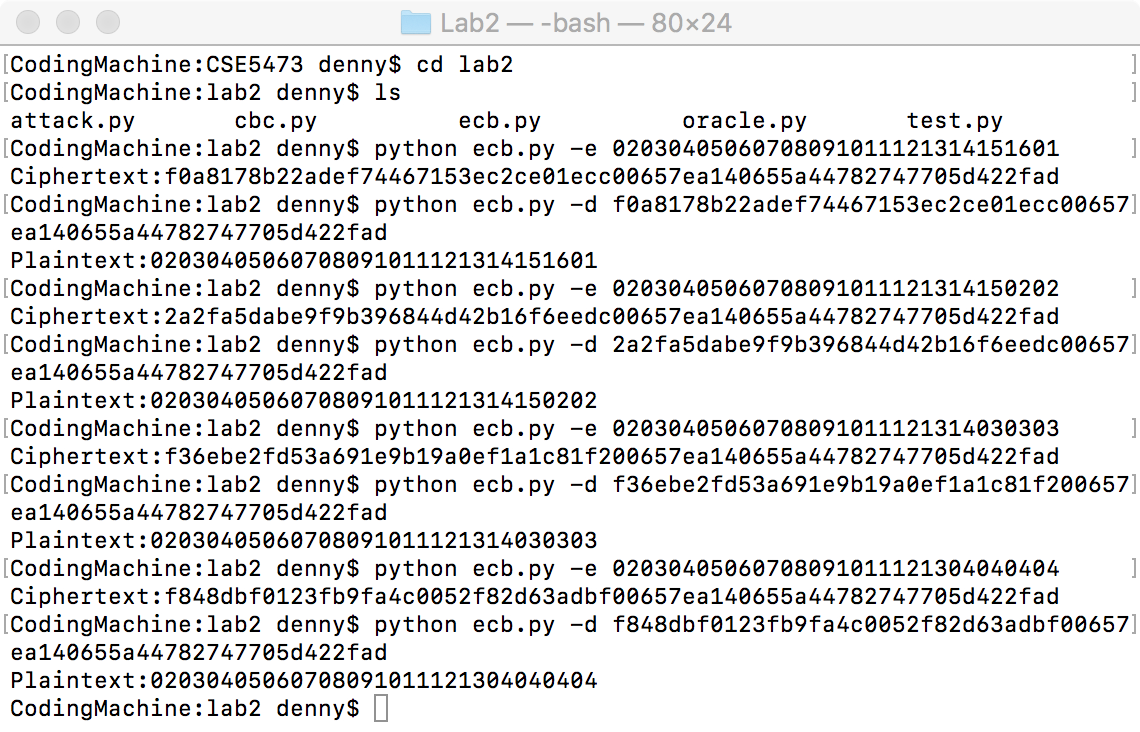
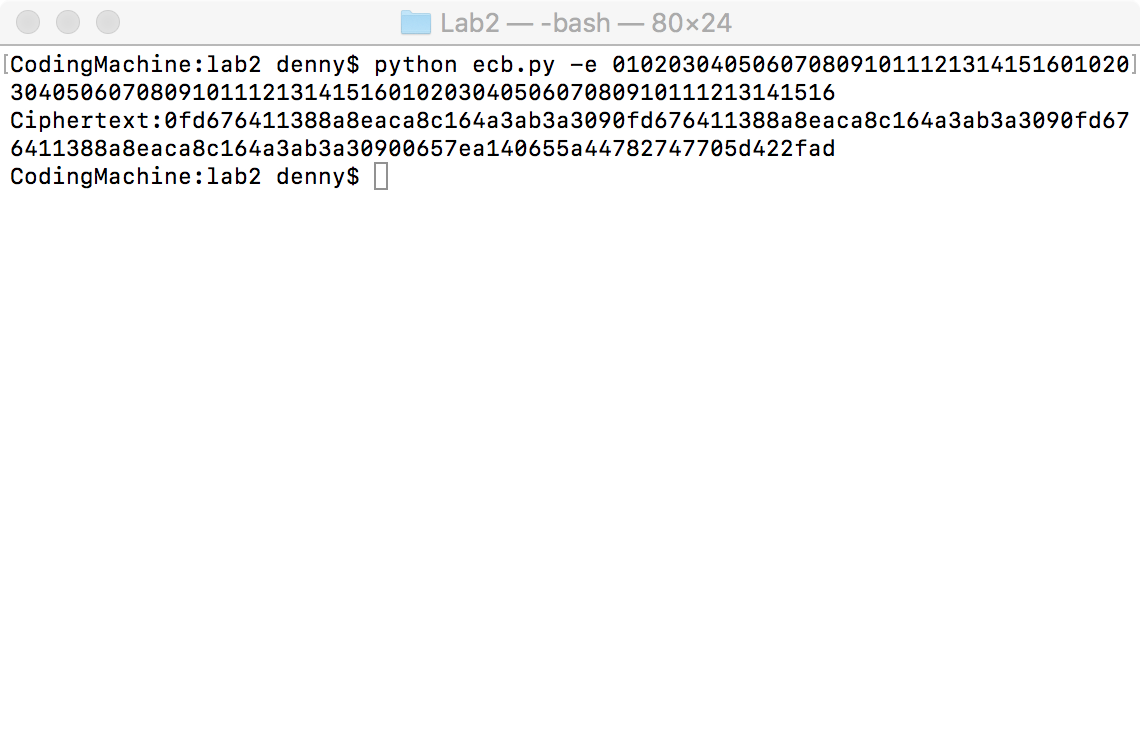
CSE5473\_Lab2

Tianyuan Li

2.

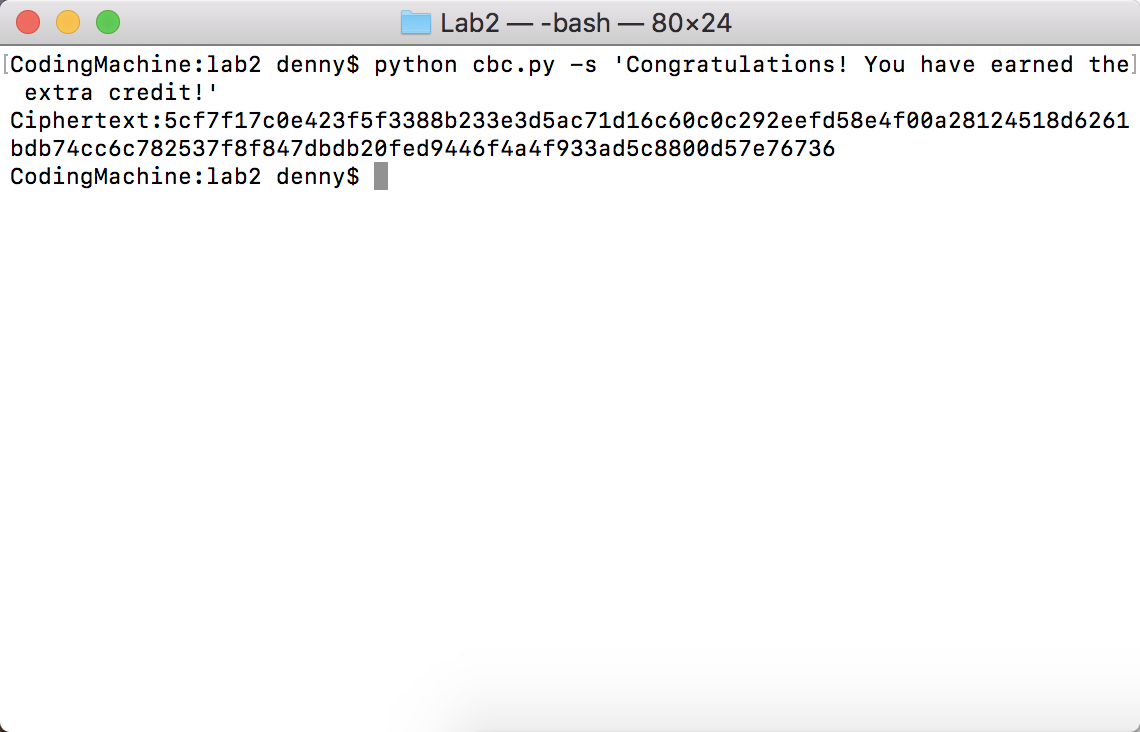


As shown in the figure above. After encrypting and then decrypting the hexadecimal strings with paddings, we get the original plaintext.

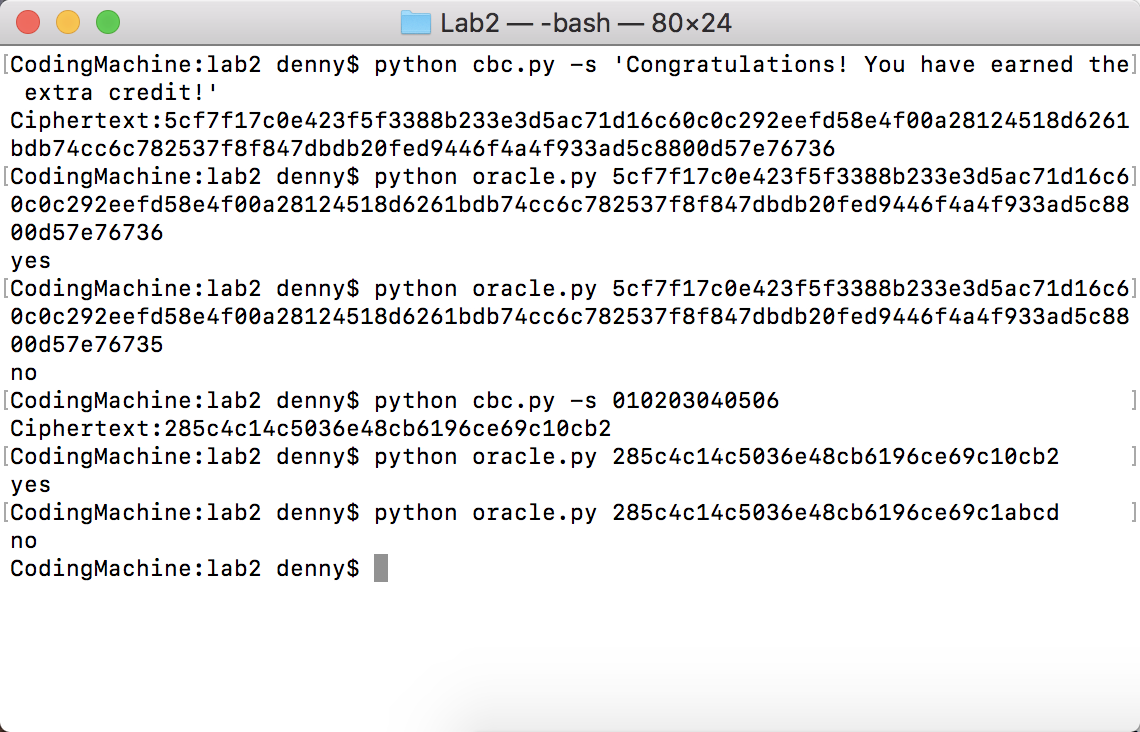


From the figure, we can see the repeated ciphertext blocks after encryption. The padding block after encryption is “00657ea140655a44782747705d422fad”, which should look like “10101010101010101010101010101010” in the plaintext after padding.

3.

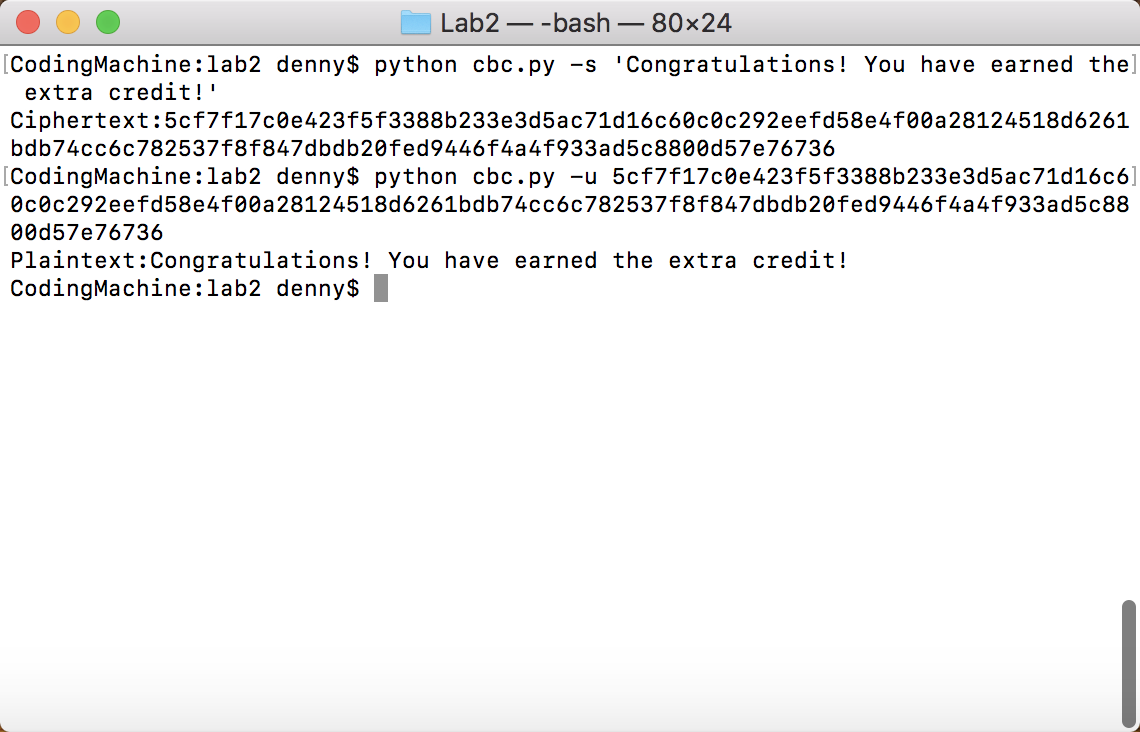


4.



As the figure shown, I tested the program by passing a correct padding ciphertext from encrypting test strings or hexadecimal strings and got “yes”. Then I modified a few bits of the correct padding ciphertext and got “no”.

6.



As shown in the figure, I decrypted the entire cipher text and did not encounter difficulty.