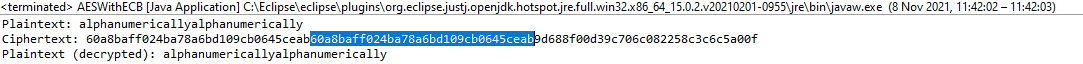
# Lab 4 08/11/2021

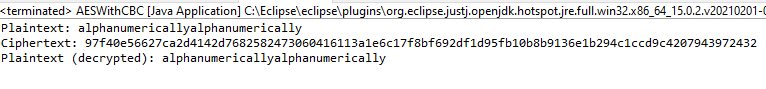
1.Can you demonstrate the weakness of ECB when encrypting the following plaintext:



If you see the first part of the ciphertext and then see highlighted part, they are the same, and the end is all padding.

2.Can you demonstrate that the weakness of ECB is not present in CBC when encrypting the

following plaintext:



There is no repeat of any cipher text in the ciphertext.

3.Can you modify the above code to use Ciphertext Stealing instead of padding? Hint: The

required `transformation' string is "AES/CBC/CS3Padding". What is the impact on the length

of the ciphertext?

## 1st Run



## 2nd Run with CS3



May be hard to distinguish between both diagrams, however the cipher text in the second run with CS3 padding is significantly shorter.

4. How is a random IV shared between the person encrypting the plaintext and the person decrypting the corresponding ciphertext? What happens if you run the program multiple times? Do you always get the same ciphertext? Note that we are using the Java class java.util.SecureRandom rather than java.util.Random.

What is the significance of this?

## 1st Run:



## 2nd Run:



See that both times the code is executed that the ciphertext is completely different. Using secure random keeps the IV random each time it is ran.

4.What happens if your plaintext is not a multiple of the block size? What happens if you add padding? Is it necessary?

Doesn’t need padding as it will encrypt the plaintext that are smaller than the key.

## 1st Run



## 2nd Run



Both executions have different ciphertext results.