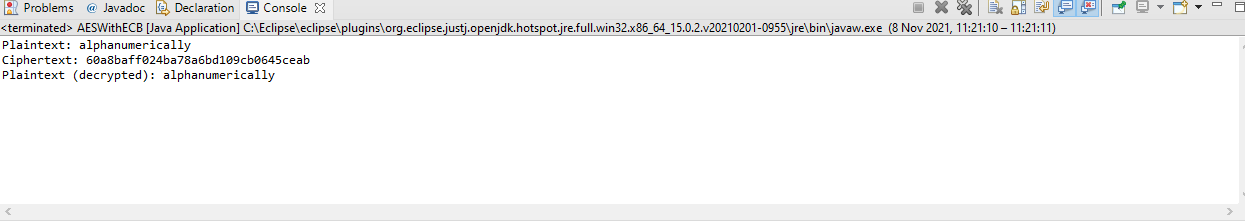
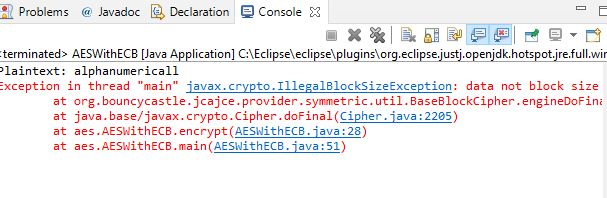
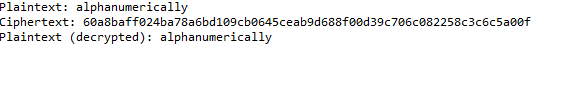
# Cryptography Lab 4

## ECB Mode

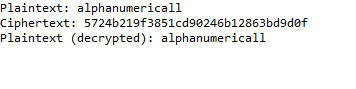


When plaintext is not a multiple

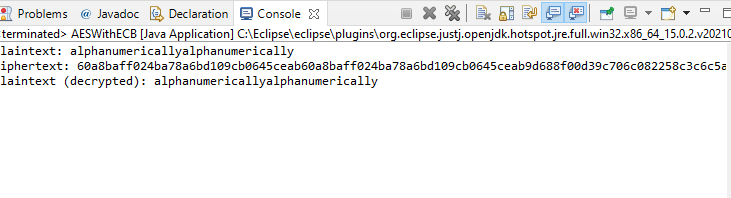
PKCS#7 padding



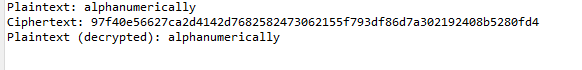
No longer must be multiple



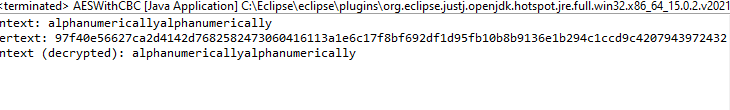
Repeats of strings have the same ciphertext



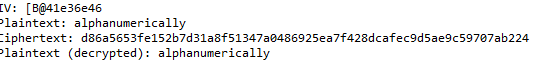
## CBC Mode



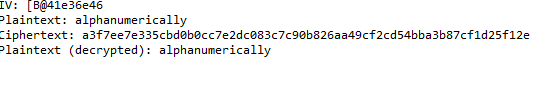
No longer repeats

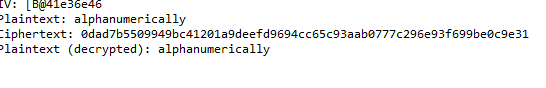


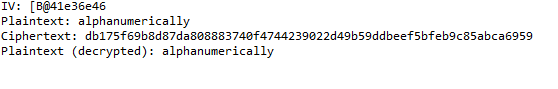
System.out.println(“IV: “ + iv);



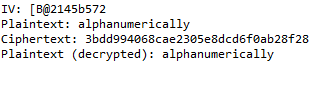
The Ciphertext changes each time



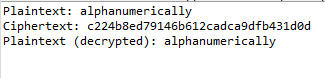




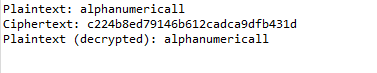
Ciphertext Stealing (Makes it much shorter)



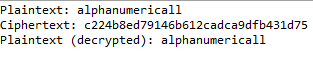
## CTR Mode



Removing a letter from the ciphertext (lost 2 letters from the ciphertext when lose 1 letter from the plaintext)



Added pkcs7padding, unnecessary though as it works without



Ciphertext doesn’t repeat when Plaintext Repeats

