Anthony Constantino
HW 3

Suppose two plaintext samples P and Q are encrypted using a block cipher with the same secret key K and the same initialization vector IV (or nonce) for those modes that require it. Suppose each plaintext sample is divided into 100 blocks (including padding). If all the plaintext blocks of P and Q are the same, except for block 10, in which they differ by 1 bit, compare the corresponding ciphertext for each block cipher mode

ECB – everything is the same except for block 10 because it doesn't use the IV
CBC – blocks 1-9 will be the same everything after that will differ
CTR – everything will be the same except block 10 because each of them is done individually
CFB – blocks 1-9 will be the same everything after that will differ
OFB – blocks 1-9 will be the same everything after that will differ

Same as #1, except assume P and Q are encrypted with a different IV (nonce) as recommended by cryptographers.

ECB – everything is the same except for block 10 because it doesn't use the IV
CBC – everything is different because the IV is different and all upcoming blocks are dependent on previous blocks
CTR – everything is different because there is a new/different IV for each block
CFB – everything is different because the IV is different and all upcoming blocks are dependent on previous blocks
OFB – everything is different because the IV is different and all upcoming blocks are dependent on previous blocks

Suppose two ciphertext samples P and Q are decrypted using key K and the same IV (or nonce) when required. Suppose each ciphertext sample of 100 blocks differs by 1 bit in block 25 only. Compare the corresponding plaintext blocks following decryption of P and Q for each block cipher mode.

ECB – only block 25 differs
CBC – blocks 25 and onward will differ
CTR – only block 25 differs
CFB – blocks 25 and onward will differ
OFB – only block 25 differs

Assume each ciphertext block is stored on a separate disk block that can be accessed independently. Suppose only block 50 of an encrypted file of 100 blocks needs to be accessed. Which specific blocks of ciphertext must be accessed to obtain the plaintext for block 50 for the following modes?

ECB – only block 50
CBC – block 49 and 50
CTR – only block 50

CFB – block 49 and 50
OFB – only block 50

Which modes permit parallel encryption?
ECB, CTR

Which modes permit parallel decryption?
ECB, CBC, CTR, CFB

Which modes permit pre-computation of the key stream?
CTR, OFB