Question 5:

A) Is it possible to perform encryption and decryption operations in parallel on multiple blocks of plain text in CBC mode? Justify your answer.

B) If a bit error occurs in the transmission of a cipher text character in 8-bit CFB mode, how far does the error propagate?

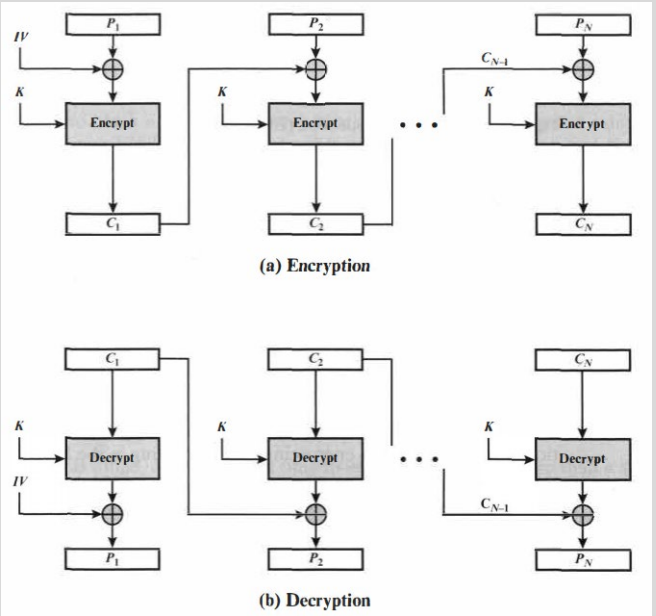
Question 5:

C) With the ECB mode, if there is an error in a block of the transmitted ciphertext, only the corresponding block is affected. However, in the CBC mode, this error propagates. For instance, in the right Figure an error in the transmitted C_1 corrupts P_1 and P_2.

- Are any blocks beyond P_2 affected?

Given a bit error in the source version of P_1…

- Through how many ciphertext blocks is the error propagated?
- What is the effect at the receiver?



CBC Mode