16-124-836
Marcel Matti ZAUDER

2.5 Question 5

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

No, it is not because the result of the previous block is always carried over in otder to encrypt/decrypt the next block.

2.5.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?

The error will obvious affect the decryption of the ciphertext block. Furthermore, this error block will stay in the initialization vector for another $64/8 = 8$ blocks, hence, affecting in total 9 blocks.

2.5.C CBC mode

C_1 corrupts P_1 and P_2. Are any blocks beyond P_2 affected?

No, because the blocks beyond do not rely on the information of C_1.

Given a bit error in the source version of P_1. Through how many ciphertext blocks is the error propagated?

This error will affect every ciphertext block that will be encrypted because the previous generated ciphertext is used to encrypt the next block and therefore the error is always propagated.

What is the effect at the receiver?

Because the error was always propagated, the following blocks will be decrypted to the original blocks because the falsely encrypted blocks are then decrypted in a false way as the error propagated through all blocks and therefore the correct blocks are deciphered.