Network Security

Exercises 2
Question 5

Tobias Famos
16-933-764

March 13, 2022

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, as the next block encryption or decryption is dependent on the previous one.

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?

All the way to the end.

Are there any blocks beyond P2 affected?

Yes all the following Blocks are affected as the next block is always dependent on the previous one. Thus P3 is affected because P2 is Affected and P4 is affected because P3 is affected and so on.

How many cipher blocks are affected?

All of the blocks are affected in the error propagation.

What is the effect at the receiver?

The decrypted message is not readable.