Assignment 2, part 3 by Staffan Lundstrom, roll no 03005201

1. C1 goes in to the first block and corrupts the output P1. It also corrupts P2 since the output from the second block is XORed with C1. The rest is not affected by this error on C1.

2. The whole cipher text becomes corrupted due to an error in P1. This is because C1 is corrupted by P1. C1 is used for encrypting C2 and therefore C2 is also corrupted and so on. So the error is rippled through all blocks.

3. If a bit error occurs in the P*i*:th transmitted byte during the encryption process in CFB mode, then C*i* is affected. The error is propagated to the shift register and stored in the last byte. There will be a delay of 64/8 = 8 turns before the corrupted byte is used again. Hence, this error will repeat every 8^{th} byte. For the decryption process the error is analog.