1. Give formulas for decryption for each of the modes of encryption discussed in class. Recall that they are ECB, CBC, OFB, CTR, CFB. For which modes can the decryption be parallelized? Don’t try to parallelize the steps of one instance of the block cipher. The only useful way to parallelize decryption is to run several independent instances of the block cipher on different cores. Assume you have many cores, perhaps one for each block of ciphertext.

2. Suppose that a plaintext of length 640 bits is enciphered using DES with one of the encryption modes, yielding a ciphertext of length 640 bits. The ciphertext is then sent by radio to a receiver, who will decipher it. Now suppose that during transmission bit 183 is complemented by radio interference. How many bits deciphered MAY be incorrect if the encryption mode is:
   (a) ECB?
   (b) CBC?
   (c) OFB?
   (d) CTR?
   (e) CFB?

Explain how you got each answer.