Problem 5 ***Alternate Feedback*** **(24 points)**

The following is a diagram of the FFM (F*ed Feedback Mode) block cipher mode of encryption. We assume that the block cipher is a secure block cipher with a 128b block size and key size. Yes, indeed, the initial block encrypts the key with itself...

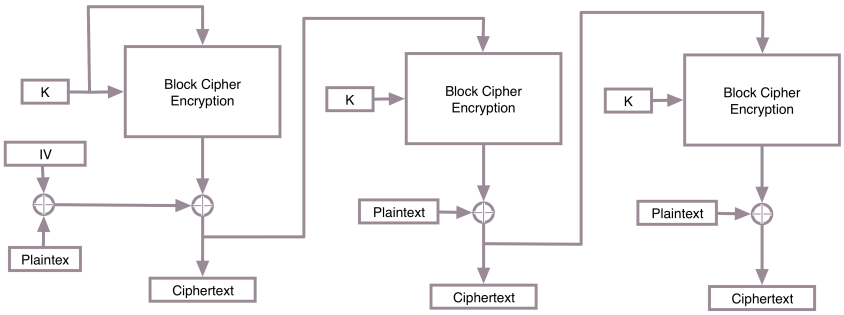
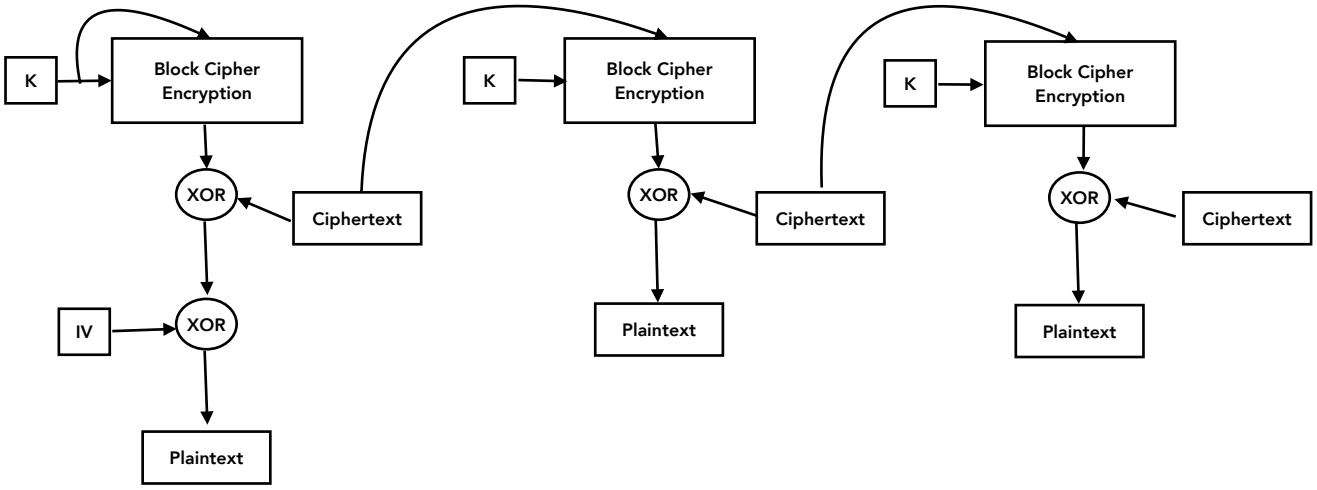


Figure 1: FFM Encryption Mode

(a) (4 points) Draw what the decryption mode will have to look like



(b) (4 points) If you reuse the IV for two secret messages, M and M', both using the same key, producing two ciphertexts C and C' seen by the eavesdropper, what can the eavesdroper learn? Assume that the first bit of M and M' are different but the rest of the bits may or may not be the same.

All the indices of matching bits in the first blocks of M and M'. The encryption of K, xor'd with the same IV will not change. If you xor the first blocks of both ciphertexts, the result will be 0 wherever the bits match. This is not true for other blocks, since the first block of ciphertext is fed into AES-encryption to get the next ciphertext block, which will be different for the two cases.

(c) (4 points) If the first bit of the ciphertext is corrupted in transmission after the encryption is complete and then decrypted, which bits of the decrypted plaintext will be corrupted? (Hint: which decrypted blocks are affected by the first block of ciphertext)

First bit of decrypted block 1 and all of decrypted block 2.

(d) (4 points) Can this encryption algorithm be parallelized?

○ Yes ● No

(e) (4 points) Can the decryption be parallelized?

● Yes ○ No

(f) (4 points) Is this IND-CPA? Why or why not? (Hint: For IND-CPA, the game can progress multiple times with the same key but a different IV each time and the adversary should still not be able to distinguish which of the two messages is encrypted.)

No. Suppose you encrypt M twice with the same key but different IV. The first blocks of the the ciphertexts will be:
E(K, K) xor IV xor P1
E(K, K) xor IV2 xor P1

An eavesdropper can xor these together and get IV xor IV2. Since both IV and IV2 are public, this would indicate that the first blocks of plaintext in both messages are the same.