Encryption Question

A symmetric encryption system consists of three main components: A key generator K, An encryption algorithm E and a decryption algorithm D.
For two users Alice and Bob, the generator K generates a shared secret key K_{ab}. Then one of the two users takes a plaintext message P and with the use of this shared key produces an encrypted ciphertext message $C = E(K_{ab}, P)$. The message can now be sent over an insecure channel. The recipient can retrieve the original message $P = D(K_{ab}, C)$.

What are the three basic requirements to make the system secure?

1- Without knowledge of the key it is computationally infeasible to compute P from C.
2- Even with many ciphertexts exchanged by Alice and Bob it is computationally infeasible to infer the key.
3- Alice and Bob must store the key K_{ab} securely.

Modes of Operation Problem

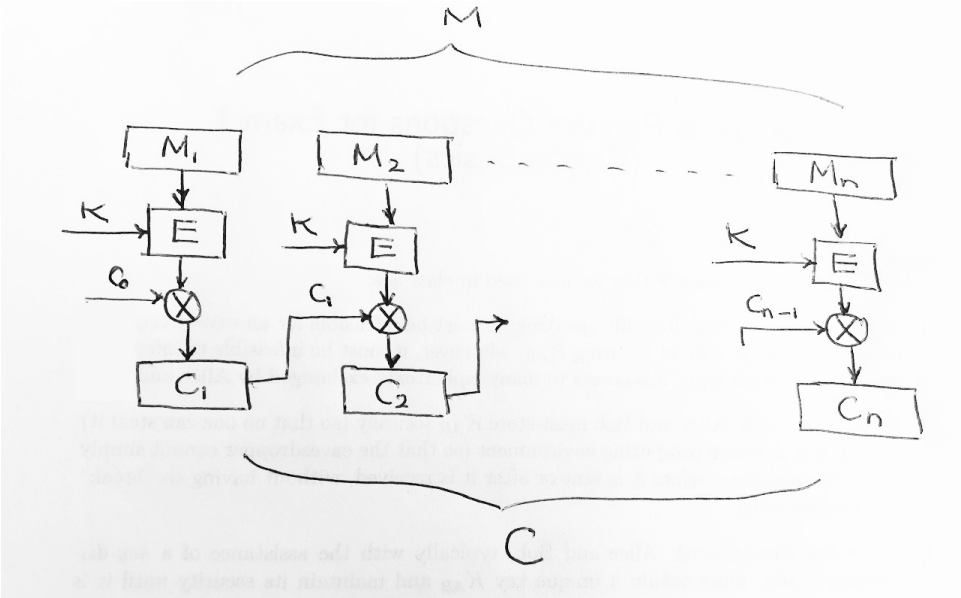
An AES encryption system uses a 128-bit key K to encrypt a message M that consists of n 128-bit blocks (M_1, M_2, …..M_n) and produces n 128-bit blocks of ciphertext (C_1, C_2, …..C_n)

The encryption process is as follows.
The sender first chooses a random 128-bit string to be used as C_0
Then for all i>0, the i^{th} cipher text block is given as

$Ci = C_{i-1}$ EXOR E(K, M_i)

The ciphertext would then be the concatenation of
$C_1 || C_2 || \ldots C_n$

a- Draw a sketch of this mode of operation showing M_1, M_2, …..M_n and their corresponding ciphertext blocks.



b- What is the purpose of using C_0?

C_0 is an *initialization vector* IV and is intended to ensure that identical blocks of M_i do not produce identical block of C_i

c- Is this mode of operation secure? If so why so and if not give a reason.

No, it is not secure. Since the eavesdropper has all C_i then the inverse property of the EXOR enables them to acquire all values of E(K, M_i). This is in essence equivalent to the ECB mode of operation.

d- What change would you make to this scheme to improve security?

Replace the given Ci with Ci = E(K, C_{i-1} EXOR M_i)
Which is in essence CBC.