1.
(b)

(c)

(d)

2.
(a) In CFB mode, the decryption process uses the previous ciphertext block to decrypt the current ciphertext block. If there is an error in the transmission of C2, it will affect the decryption of M2 and M3. Here's the impact on each block Mi:

- M1: Correctly decrypted (not dependent on C2)
- M2: Incorrectly decrypted (directly affected by the error in C2)
- M3: Incorrectly decrypted (C2 is used in the decryption of M3)
- M4 - M10: Correctly decrypted (not dependent on C2, as the error in C2 does not propagate further)

(b) In CBC mode, a repeating IV reduces the security of the encryption because it leads to deterministic encryption, making it vulnerable to chosen plaintext attacks (CPA).
To determine the relationship between C and M (and C' and M'), Eve can perform the following CPA attack:

1. Choose a new message M" = M xor M'.
2. Ask Bob to encrypt M" using the same key and the repeating IV.
3. Observe the resulting ciphertext C".

Since the encryption is deterministic and the same IV is used, we have:
C"[1] = E_k(IV xor M"[1]) and C[1] = E_k(IV xor M[1])
Now, Eve can compute C_xor = C"[1] xor C[1]:
C_xor = E_k(IV xor M"[1]) xor E_k(IV xor M[1])
Notice that C_xor = E_k(IV xor (M[1] xor M'[1])).
Now, Eve can compare C_xor with C'[1]:

- If C_xor = C'[1], then C is the encryption of M (and C' is the encryption of M').
- If C_xor ≠ C'[1], then C is the encryption of M' (and C' is the encryption of M).

The encryption scheme using a repeating IV in CBC mode is not CPA-secure, as Eve can perform a chosen plaintext attack to determine which ciphertext corresponds to which plaintext.