Question 1 ***Block ciphers*** ()

Consider the Cipher feedback (CFB) mode, whose encryption is given as follows:

$$C_i = \begin{cases} \text{IV}, i = 0 \\ E_K(C_{i-1}) \oplus P_i, \text{otherwise} \end{cases}$$

Q1.1 Draw the encryption diagram for CFB mode.

Q1.2 What is the decryption formula for CFB mode?

Q1.3 Select the true statements about CFB mode:

- ☐ Encryption can be paralellized
- ☐ The scheme is IND-CPA secure
- ☐ Decryption can be paralellized

Q1.4 What happens if two messages are encrypted with the same key and nonce? What can the attacker learn about the two messages just by looking at their ciphertexts?

Q1.5 If an attacker recovers the IV used for a given encryption, but not the key, will they be able to decrypt a ciphertext encrypted with the recovered IV and a secret key?

Question 2 ***Crytographic Hashes*** ()

For each of the given functions H below, determine if it is one-way or not, and if it is collision-resistant or not.

Q2.1 $\mathsf{H}(x) = x^2$

- ◯ (A) One way
- ◯ (B) Collision resistant
- ◯ (C) Both
- ◯ (D) Neither

Q2.2 For this part you have access to a SHA-256 hash function. The notation $[x : y]$ refers to a slice of bytes x to $y - 1$.

$\mathsf{H}(x) = \text{SHA-256}(x[0 : \mathsf{len}(x) - 1])$

- ◯ (G) One way
- ◯ (H) Collision resistant
- ◯ (I) Both
- ◯ (J) Neither

Q2.3 $\mathsf{H}(x) = x^3$

- ◯ (A) One way
- ◯ (B) Collision resistant
- ◯ (C) Both
- ◯ (D) Neither

Question 3 ***Confidentiality and integrity*** ()

Alice and Bob want to communicate with confidentiality and integrity. They have:

- Symmetric encryption.
  - Encryption: $\mathsf{Enc}(\mathsf{K}, \mathsf{m})$.
  - Decryption: $\mathsf{Dec}(\mathsf{K}, \mathsf{c})$.
- Cryptographic hash function: $\mathsf{Hash}(\mathsf{m})$.
- MAC: $\mathsf{MAC}(\mathsf{K}, \mathsf{m})$.

They share a symmetric key K and know each other's public key.

We assume these cryptographic tools do not interfere with each other when used in combination; *i.e.*, we can safely use the same key for encryption and MAC.

Alice sends to Bob
1. $\mathsf{c} = \mathsf{Hash}(\mathsf{Enc}(\mathsf{K}, \mathsf{m}))$
2. $\mathsf{c} = \mathsf{c}_1, \mathsf{c}_2$: where $\mathsf{c}_1 = \mathsf{Enc}(\mathsf{K}, \mathsf{m})$ and $\mathsf{c}_2 = \mathsf{Hash}(\mathsf{Enc}(\mathsf{K}, \mathsf{m}))$
3. $\mathsf{c} = \mathsf{c}_1, \mathsf{c}_2$: where $\mathsf{c}_1 = \mathsf{Enc}(\mathsf{K}, \mathsf{m})$ and $\mathsf{c}_2 = \mathsf{MAC}(\mathsf{K}, \mathsf{m})$
4. $\mathsf{c} = \mathsf{c}_1, \mathsf{c}_2$: where $\mathsf{c}_1 = \mathsf{Enc}(\mathsf{K}, \mathsf{m})$ and $\mathsf{c}_2 = \mathsf{MAC}(\mathsf{K}, \mathsf{Enc}(\mathsf{K}, \mathsf{m}))$

Q3.1 Which ones of them can Bob decrypt?

☐ 1 ☐ 2 ☐ 3 ☐ 4

Q3.2 Consider an eavesdropper Eve, who can see the communication between Alice and Bob.

Which schemes, of those decryptable in (a), also provide *confidentiality* against Eve?

☐ 1 ☐ 2 ☐ 3 ☐ 4

Q3.3 Consider a man-in-the-middle Mallory, who can eavesdrop and modify the communication between Alice and Bob.

Which schemes, of those decryptable in (a), provide *integrity* against Mallory?
i.e., Bob can detect any tampering with the message?

☐ 1 ☐ 2 ☐ 3 ☐ 4

Q3.4 Many of the schemes above are insecure against a *replay attack*.

If Alice and Bob use these schemes to send many messages, and Mallory remembers an encrypted message that Alice sent to Bob, some time later, Mallory can send the exact same encrypted message to Bob, and Bob will believe that Alice sent the message *again*.

How to modify those schemes with confidentiality & integrity to prevent replay attack?

◇ The scheme providing confidentiality & integrity is Scheme ☐.

The modification is: