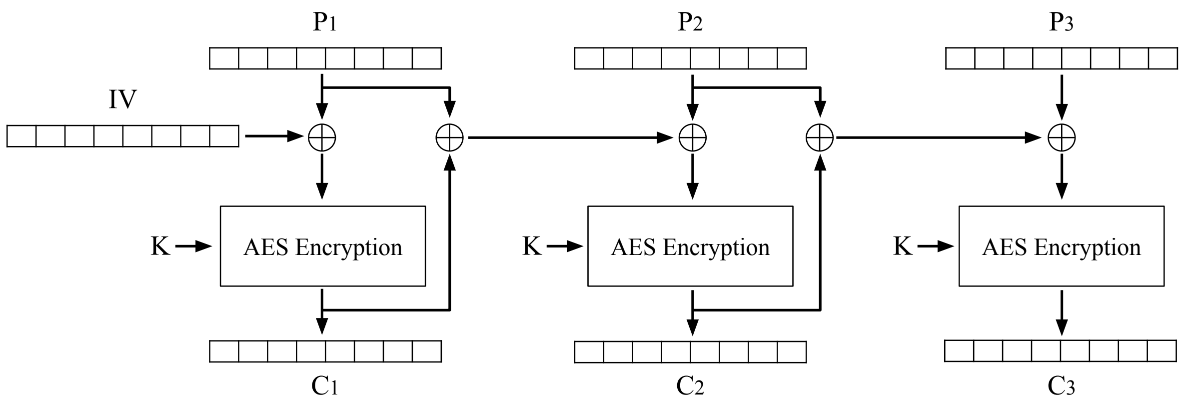
Q1 *EvanBlock Cipher* (24 points)

EvanBot invents a new block cipher chaining mode called the EBC (EvanBlock Cipher). The encryption diagram is shown below:



Q1.1 (2 points) Write the encryption formula for C_i, where $i > 1$. You can use E_K and D_K to denote AES encryption and decryption respectively.

Q1.2 (2 points) Write the decryption formula for P_i, where $i > 1$. You can use E_K and D_K to denote AES encryption and decryption respectively.

Q1.3 (4 points) Select all true statements about this scheme.

☐ It is IND-CPA secure if we use a random IV for every encryption.

☐ It is IND-CPA secure if we use a hard-coded, constant IV for every encryption.

☐ Encryption can be parallelized.

☐ Decryption can be parallelized.

☐ None of the above

Q1.4 (4 points) Alice has a 4-block message (P_1, P_2, P_3, P_4). She encrypts this message with the scheme and obtains the ciphertext $C = (IV, C_1, C_2, C_3, C_4)$.

Mallory tampers with this ciphertext by changing the IV to 0. Bob receives the modified ciphertext $C' = (0, C_1, C_2, C_3, C_4)$.

What message will Bob compute when he decrypts the modified ciphertext C'?

X represents some unpredictable "garbage" output of the AES block cipher.

- ○ (P_1, P_2, P_3, P_4)
- ○ (X, X, P_3, P_4)
- ○ (X, X, X, X)
- ○ (X, P_2, X, P_4)
- ○ (X, P_2, P_3, P_4)
- ○ None of the above

Alice has a 3-block message (P_1, P_2, P_3). She encrypts this message with the scheme and obtains the ciphertext $C = (IV, C_1, C_2, C_3)$.

Mallory tampers with this ciphertext by swapping two blocks of ciphertext. Bob receives the modified ciphertext $C' = (IV, C_2, C_1, C_3)$.

When Bob decrypts the modified ciphertext C', he obtains some modified plaintext $P' = (P'_1, P'_2, P'_3)$. In the next three subparts, write expressions for P'_1, P'_2, and P'_3.

Q1.5 (4 points) P'_1 is equal to these values, XORed together. Select as many options as you need.

For example, if you think $P'_1 = P_1 \oplus C_2$, then bubble in P_1 and C_2.

☐ P_1 ☐ P_2 ☐ P_3 ☐ IV ☐ C_1 ☐ C_2 ☐ C_3

Q1.6 (4 points) P'_2 is equal to these values, XORed together. Select as many options as you need.

☐ P_1 ☐ P_2 ☐ P_3 ☐ IV ☐ C_1 ☐ C_2 ☐ C_3

Q1.7 (4 points) P'_3 is equal to these values, XORed together. Select as many options as you need.

☐ P_1 ☐ P_2 ☐ P_3 ☐ IV ☐ C_1 ☐ C_2 ☐ C_3

Q2 *Cryptography: All or Nothing Security* (20 points)

EvanBot decides to modify AES-CTR in order to provide **all-or-nothing security**. All-or-nothing security means that modifying *any* part of the ciphertext will make the *entire* plaintext decrypt to some sort of "garbage" output.

EvanBot designs the following scheme to encrypt $M = (M_1, M_2, \ldots, M_n)$:

1. EvanBot generates a new random key K_2 on top of the original key K_1. Note that K_2 is **not** known to the decryptor, even though K_1 is.
2. EvanBot transforms M into a "pseudomessage" M' by setting $M'_i = M_i \oplus E_{K_2}(i)$.
3. EvanBot adds the block $M'_{n+1} = H(M'_1 \oplus 1) \oplus H(M'_2 \oplus 2) \oplus \ldots \oplus H(M'_n \oplus n) \oplus K_2$.
4. EvanBot derives the ciphertext $C = \mathsf{Enc}(K_1, M')$ using AES-CTR with key K_1 and IV IV.

First, we will walk through the decryption process for this all-or-nothing scheme. Fill in the blanks for the following by answering the multiple-choice subparts below:

1. CodaBot receives C.
2. CodaBot decrypts C with key K_1 to recover ________________.
3. CodaBot sets K_2 = $M'_{n+1} \oplus$ ________________.
4. CodaBot finds i-th original message block as $M_i =$ ________________.

Q2.1 (2 points) Select the correct option for the blank on Step 2:

- ○ K_2
- ○ $M'_i \oplus E_{K_2}(i)$
- ○ $H(M'_1 \oplus 1) \oplus \ldots \oplus H(M'_n \oplus n)$
- ○ M'

Q2.2 (2 points) Select the correct option for the blank on Step 3:

- ○ K_2
- ○ $M'_i \oplus E_{K_2}(i)$
- ○ $H(M'_1 \oplus 1) \oplus \ldots \oplus H(M'_n \oplus n)$
- ○ M'

Q2.3 (2 points) Select the correct option for the blank on Step 4:

- ○ K_2
- ○ $M'_i \oplus E_{K_2}(i)$
- ○ $H(M'_1 \oplus 1) \oplus \ldots \oplus H(M'_n \oplus n)$
- ○ M'

Q2.4 (5 points) Explain how modifying an arbitrary ciphertext block prevents recovery of ***any block*** of the original message.

HINT: Show that we cannot recover K_2 if any ciphertext block is modified.

Q2.5 (5 points) EvanBot wonders if it's really necessary to have the hash function used in Step 3, and decides to replace Step 3 with this new step:

3. EvanBot adds the block $(M_1' \oplus 1) \oplus (M_2' \oplus 2) \oplus \ldots \oplus (M_n' \oplus n) \oplus K_2$ to the end of M'.

Show that it is possible to tamper with the order of the message blocks, i.e. by swapping two blocks. Note that "tamper" means the message will be decrypted to something different, but not all blocks will turn to garbage (i.e. not "all or nothing").

Q2.6 (4 points) Does the original all-or-nothing scheme (from the beginning of the question) provide integrity?

○ Yes ○ No

Explain why or why not.