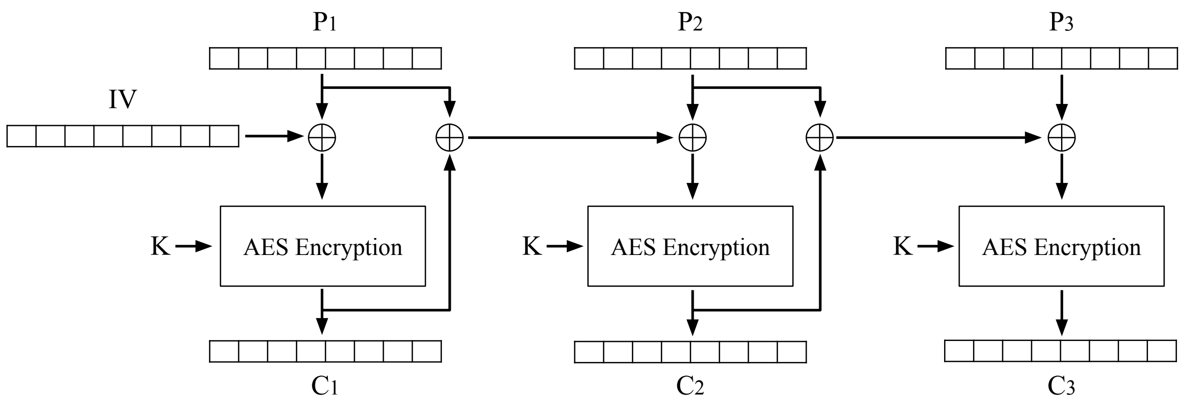
Q1 *EvanBlock Cipher* **(24 points)**

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 ***AES-GROOT*** **(30 points)**

Tony Stark develops a new block cipher mode of operation as follows:

$$
\begin{aligned}
C_0 &= IV \\
C_1 &= E_K(K) \oplus C_0 \oplus M_1 \\
C_i &= E_K(C_{i-1}) \oplus M_i \\
C &= C_0 \| C_1 \| \cdots \| C_n
\end{aligned}
$$

For all parts, assume that IV is randomly generated per encryption unless otherwise stated.

Q2.1 (3 points) Write the decryption formula for M_i using AES-GROOT.

Q2.2 (3 points) AES-GROOT is not IND-CPA secure. Which of the following most accurately describes a way to break IND-CPA for this scheme?

- ◯ It is possible to compute a deterministic value from each ciphertext that is the same if the first blocks of the corresponding plaintexts are the same.
- ◯ C_1 is deterministic. Two ciphertexts will have the same C_1 if the first blocks of the corresponding plaintexts are the same.
- ◯ It is possible to learn the value of K, which can be used to decrypt the ciphertext.
- ◯ It is possible to tamper with the value of IV such that the decrypted plaintext block M_1 is mutated in a predictable manner.

Q2.3 (5 points) AES-GROOT is vulnerable to plaintext recovery of the first block of plaintext. Given a ciphertext C of an unknown plaintext M and different plaintext-ciphertext pair (M', C'), provide a formula to recover M_1 in terms of C_i, M'_i, and C'_i (for any i, e.g. C_0, M'_2, C'_6).

Recall that the IV for some ciphertext C can be referred to as C_0.

If AES-GROOT is implemented with a fixed $IV = 0^b$ (a fixed block of b 0's), the scheme is vulnerable to full plaintext recovery under the chosen-plaintext attack (CPA) model. Given a ciphertext C of an unknown plaintext and different plaintext-ciphertext pair (M', C'), describe a method to recover plaintext block M_4.

Q2.4 (5 points) First, the adversary sends a value M'' to the challenger. Express your answer in terms of in terms of C_i, M'_i, and C'_i (for any i).

Q2.5 (5 points) The challenger sends back the encryption of M'' as C''. Write an expression for M_4 in terms of C_i, M'_i, C'_i, M''_i, and C''_i (for any i).

Q2.6 (4 points) Which of the following methods of choosing IV allows an adversary under CPA to fully recover an arbitrary plaintext (not necessarily using your attack from above)? Select all that apply.

- ☐ IV is randomly generated per encryption
- ☐ $IV = 1^b$ (the bit 1 repeated b times)
- ☐ IV is a counter starting at 0 and incremented per encryption
- ☐ IV is a counter starting at a randomly value chosen once during key generation and incremented per encryption
- ☐ None of the above

Q2.7 (2 points) Let C be the encryption of some plaintext M. If Mallory flips with the last bit of C_3, which of the following blocks of plaintext no longer decrypt to its original value? Select all that apply.

- ☐ M_1
- ☐ M_2
- ☐ M_3
- ☐ M_4
- ☐ None of the above

Q2.8 (3 points) Which of the following statements are true for AES-GROOT? Select all that apply.

- ☐ Encryption can be parallelized
- ☐ Decryption can be parallelized
- ☐ AES-GROOT requires padding
- ☐ None of the above