Q1  **AES-GROOT**  
Tony Stark develops a new block cipher mode of operation as follows:

\[
\begin{align*}
C_0 &= IV \\
C_1 &= E_K(K) \oplus C_0 \oplus M_1 \\
C_i &= E_K(C_{i-1}) \oplus M_i \\
C &= C_0 \parallel C_1 \parallel \cdots \parallel C_n
\end{align*}
\]

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

Q1.1 (3 points) Write the decryption formula for \( M_i \) using AES-GROOT. You don’t need to write the formula for \( M_1 \).

Q1.2 (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.

Q1.3 (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. \( C_0, M_2, C_0' \)).

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 $M_4$.

Q1.4 (5 points) First, the adversary sends a value $M''$ to the challenger. Express your answer in terms of $C_i, M'_i, C'_i$ (for any $i$).

Q1.5 (5 points) The challenger sends back the encryption of $M''$ as $C''$. Write an expression for $M_4$ in terms of $C_i, M'_i, C'_i, M''_i, C''_i$ (for any $i$).

Q1.6 (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

Q1.7 (2 points) Let $C$ be the encryption of some plaintext $M$. If Mallory flips the last bit of $C_3$, which of the following blocks of plaintext no longer decrypt to its original value? Select all that apply.

- $M_1$
- $M_3$
- None of the above
- $M_2$
- $M_4$
Q1.8 (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