Q1 *AES-161* **(23 points)**

Alice has created a scheme called AES-161 to send messages to Bob securely in the presence of a man-in-the-middle attacker Mallory. Alice and Bob both share a symmetric key K that is secret from everyone else.

The encryption scheme for AES-161 is as follows:

$$C_1 = E_K(IV_1 \oplus M_1)$$
$$C_2 = E_K(C_1 \oplus IV_2 \oplus M_2)$$
$$C_i = E_K(C_{i-1} \oplus C_{i-2} \oplus M_i)$$

Q1.1 (3 points) Write the decryption formula of AES-161 for M_i, for $i > 2$.

Q1.2 (4 points) Is this scheme IND-CPA secure with randomly generated IVs? If you mark "Yes", provide a brief justification (10 words or fewer; no formal proof necessary). If you mark "No", provide a strategy to win the IND-CPA game with probability greater than $1/2$.

○ Yes ○ No

Consider the following attack, called the FEI attack:

Given a ciphertext C of a known plaintext M, Mallory wishes to provide C' such that some subset of blocks of Mallory's choosing would be decrypted to M'_i, where both i and M'_i are **any values of Mallory's choosing**. For other values of i, the corresponding M'_is **can be anything**.

For example, let's say Mallory wants to provide a C' so that the first and last blocks of an 8-block message are decrypted into values M'_1 and M'_8 of her choosing while blocks 2 through 7 are not necessarily values of her choosing. In other words, when Bob decrypts the ciphertext C', he will get

$$M'_1 \| x_1 \| x_2 \| x_3 \| x_4 \| x_5 \| x_6 \| M'_8$$

where x_i refers to any value.

Q1.3 (6 points) Alice wishes to send a 3-block message M. Mallory wants to perform the FEI attack on the third block.

Provide a formula for all C'_i that differ from their corresponding C_i in terms of M_i, C_i, M'_i, and C'_i for specific values of i. Your formula may also include any public values. You don't need to provide a formula for any $C'_i = C_i$.

Q1.4 (5 points) Assume that Alice is sending a 9-block message. What is the maximum number of blocks that Mallory can perform the FEI attack on?

Q1.5 (5 points) Assume that Alice is sending a 9-block message. Mallory wants to perform the FEI attack on the maximum number of blocks. You can pick which blocks the FEI attack is performed on.

Provide a formula for all C_i' that differ from their corresponding C_i in terms of M_i, C_i, M_i', and C_i' for specific values of i. Your formula may also include any public values. You don't need to provide a formula for any $C_i' = C_i$.

Q2 *AES-GROOT* **(30 points)**

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

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

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. You don't need to write the formula for M_1.

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