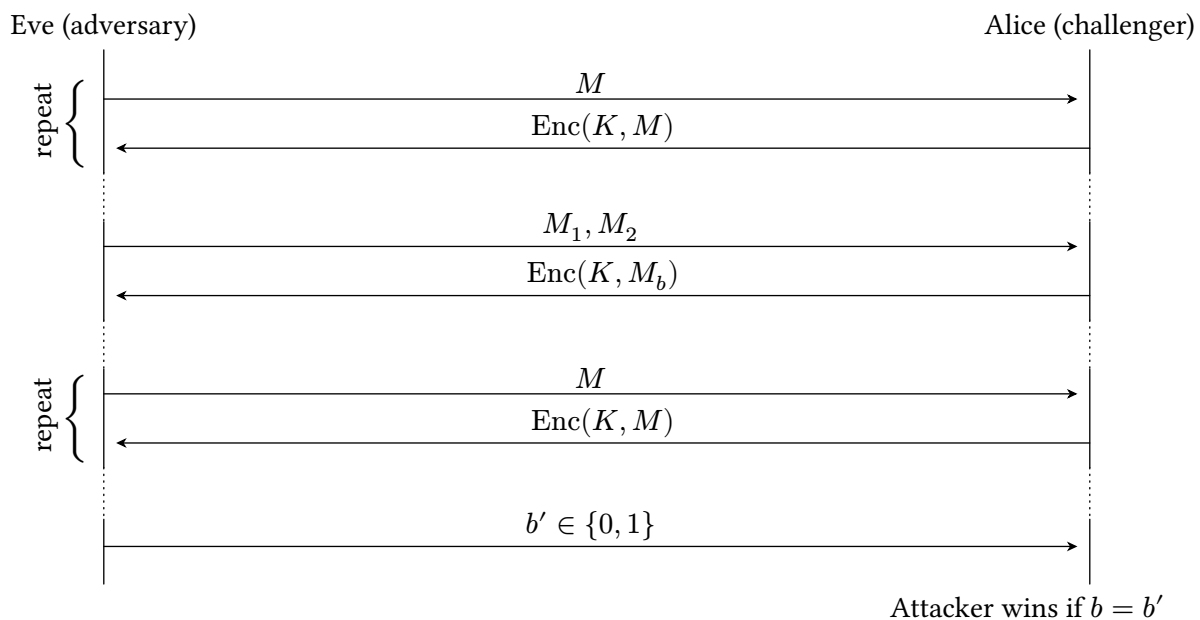


**Q1 IND-CPA**

**(5 points)**

When formalizing the notion of confidentiality, as provided by a proposed encryption scheme, we introduce the concept of indistinguishability under a chosen plaintext attack, or IND-CPA security. A scheme is considered *IND-CPA secure* if an attacker cannot gain any information about a message given its ciphertext. This definition can be defined as an experiment between a challenger and adversary, detailed in the diagram below:



Consider the one-time pad encryption scheme discussed in class. For parts (a) – (c), we will prove why one-time pad is not IND-CPA secure and, thus, why a key should not be reused for one-time pad encryption.

Q1.1 (1 point) What messages ( $M_0$  and  $M_1$ ) should the adversary provide the challenger?

Q1.2 (1 point) Now, for which message(s) should the adversary request an encryption from the challenger during the query phase?



(Question 1 continued...)

Q1.3 (1 point) The challenger now randomly selects  $b \in \{0, 1\}$ , encrypts  $M_b$ , and sends back  $C = \text{Enc}(k, M_b) = M_b \oplus K$  to the adversary. How can the adversary find  $b$  with probability  $> \frac{1}{2}$ ?

Q1.4 (1 point) Putting it all together, explain how an adversary can always win the IND-CPA game with a probability 1 against a deterministic encryption algorithm. *Note: Given an identical plaintext, a deterministic encryption algorithm will produce identical ciphertext.*

Q1.5 (1 point) Assume that an adversary chooses an algorithm and runs the IND-CPA game a large number of times, winning with a probability of 0.6. Is the encryption scheme IND-CPA secure? Why or why not?

☐ Secure      ☐ Insecure

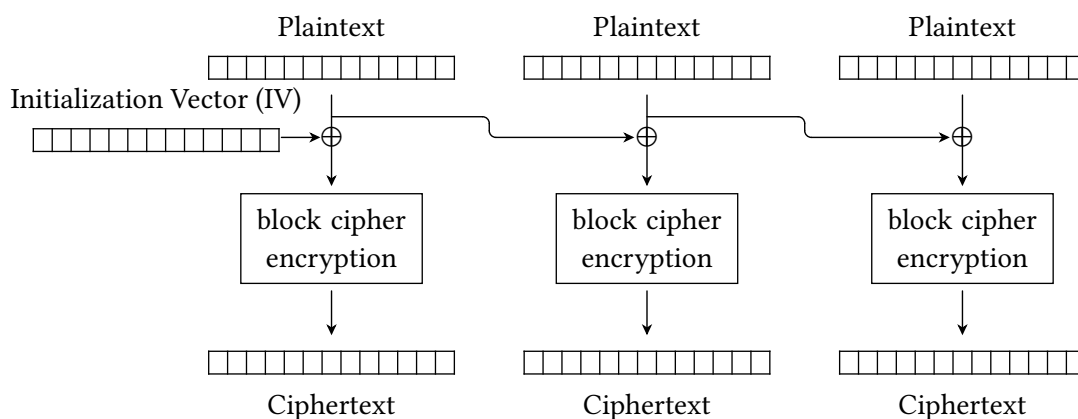
## Q2 Block Ciphers 3

(3 points)

Consider the following block cipher mode of operation.

$M_i$  is the  $i$ -th block of plaintext.  $C_i$  is the  $i$ -th block of ciphertext.  $E_K$  is AES encryption with key  $K$ .

$$C_0 = M_0 = \text{IV} \quad C_i = E_K(M_{i-1} \oplus M_i)$$



Q2.1 (1 point) Which of the following is true about this scheme? Select all that apply.

- ☐ The encryption algorithm is parallelizable
- ☐ If one byte of a plaintext block  $M_i$  is changed, then the corresponding ciphertext block  $C_i$  will be different in exactly one byte.
- ☐ If one byte of a plaintext block  $M_i$  is changed, then the next ciphertext block  $C_{i+1}$  will be different in exactly one byte
- ☐ If two plaintext blocks are identical, then the corresponding ciphertext blocks are also identical
- ☐ The encryption algorithm requires padding the plaintext
- ☐ None of the above

Q2.2 (1 point) TRUE OR FALSE: If the IV is always a block of all 0's for every encryption, this scheme is IND-CPA secure. Briefly justify your answer.

- ☐ TRUE      ☐ FALSE

(Question 2 continued...)

Q2.3 (1 point) TRUE OR FALSE: If the  $IV$  is randomly generated for every encryption, this scheme is IND-CPA secure. Justify your answer.

☐ TRUE      ☐ FALSE

### Q3 *Ra's al Gamal*

(3 points)

Recall the ElGamal scheme from lecture:

- $\text{KeyGen}() = (b, B = g^b \bmod p)$
- $\text{Enc}(B, M) = (C_1 = g^r \bmod p, C_2 = B^r \times M \bmod p)$

Q3.1 (1 point) Is the ciphertext  $(C_1, C_2)$  decryptable by someone who knows the private key  $b$ ? If you answer yes, provide a decryption formula. You may use  $C_1$ ,  $C_2$ ,  $b$ , and any public values.

☐ Yes

☐ No

Q3.2 (1 point) Consider an adversary that can efficiently break the discrete log problem. Can the adversary decrypt the ciphertext  $(C_1, C_2)$  without knowledge of the private key? If you answer yes, briefly state how the adversary can decrypt the ciphertext.

☐ Yes

☐ No

Q3.3 (1 point) Consider an adversary that can efficiently break the Diffie-Hellman problem. Can the adversary decrypt the ciphertext  $(C_1, C_2)$  without knowledge of the private key? If you answer yes, briefly state how the adversary can decrypt the ciphertext.

☐ Yes

☐ No