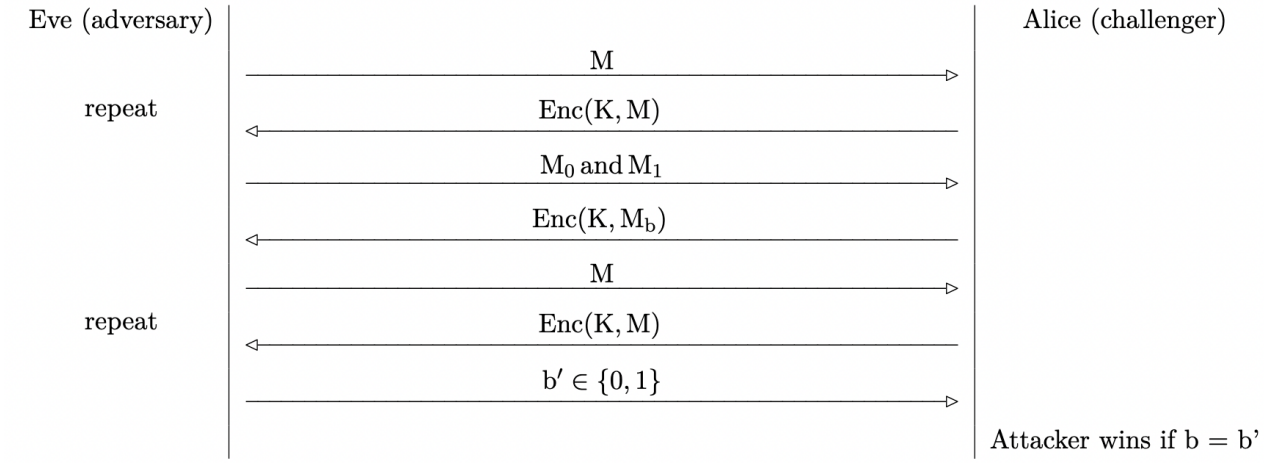
# CS 161 Summer 2024 — Introduction to Computer Security — Discussion 4

**Question 1** ***IND-CPA***

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 With what messages $M_0$ and $M_1$ should the adversary provide the challenger?

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

Q1.3 The challenger will now flip a random bit $b \in \{0, 1\}$, encrypt $M_b$, and send back $C = \mathsf{Enc}(k, M_b) = M_b \oplus k$ to the adversary. How does the adversary determine $b$ with probability $> \frac{1}{2}$?

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

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

**Question 2** ***Block Ciphers I***

Consider the Cipher feedback (CFB) mode, whose encryption is given as follows:

$$C_i = \begin{cases} \text{IV}, i = 0 \\ E_K(C_{i-1}) \oplus P_i, \text{otherwise} \end{cases}$$

Q2.1 Draw the encryption diagram for CFB mode.

Q2.2 What is the decryption formula for CFB mode?

Q2.3 Select the true statements about CFB mode:

- ☐ Encryption can be paralellized
- ☐ The scheme is IND-CPA secure
- ☐ Decryption can be paralellized

Q2.4 What happens if two messages are encrypted with the same key and IV? What can the attacker learn about the two messages just by looking at their ciphertexts?

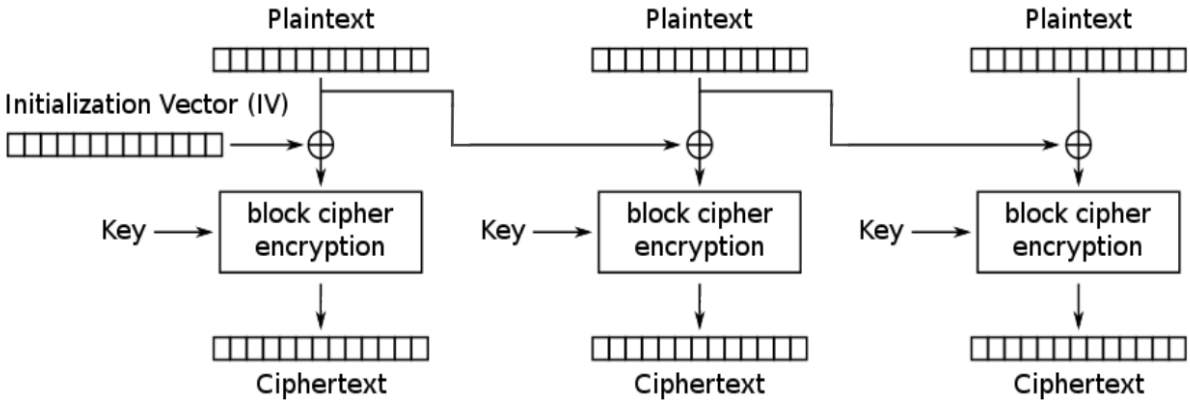
Q2.5 If an attacker recovers the IV used for a given encryption, but not the key, will they be able to decrypt a ciphertext encrypted with the recovered IV and a secret key?

**Question 3** ***Block Ciphers II***

Consider the following block cipher mode of operation.

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

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




Q3.1 Which of the following is true about this scheme? Select all that apply.

☐ (A) The encryption algorithm is parallelizable

☐ (B) 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

☐ (C) 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

☐ (D) If two plaintext blocks are identical, then the corresponding ciphertext blocks are also identical

☐ (E) The encryption algorithm requires padding the plaintext

☐ (F) None of the above

Q3.2 TRUE or FALSE: If the $IV$ is always a block of all 0s for every encryption, this scheme is IND-CPA secure. Briefly justify your answer.

◯ (G) True ◯ (H) False ◯ (I) —— ◯ (J) —— ◯ (K) —— ◯ (L) ——

Q3.3 TRUE or FALSE: If the $IV$ is randomly generated for every encryption, this scheme is IND-CPA secure. Justify your answer.

◯ (A) True ◯ (B) False ◯ (C) —— ◯ (D) —— ◯ (E) —— ◯ (F) ——