Q1  

Block Ciphers

Consider the following block cipher mode of operation.

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

\[ M_i \] is the \( i \)th plaintext block. \( C_i \) is the \( i \)th ciphertext block. \( E_K \) is AES encryption with key \( K \).

Q1.1 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
Q1.2 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) —

Q1.3 True or False: If the IV is randomly generated for every encryption, this scheme is IND-CPA secure. Briefly justify your answer.

☐ (A) True  ☐ (B) False  ☐ (C) —  ☐ (D) —  ☐ (E) —  ☐ (F) —
Q2  

IV-e got a question for ya  

Determine whether each of the following schemes is IND-CPA secure. This question has 6 subparts.

Q2.1 AES-CBC where the IV for message $M$ is chosen as HMAC-SHA256($k_2, M$) truncated to the first 128 bits. The MAC key $k_2$ is distinct from the encryption key $k_1$.

Provide a short justification for your answer on your answer sheet.

☐ (A) Insecure  ☐ (C)  ☐ (E)  

☐ (B) Secure  ☐ (D)  ☐ (F)  

Q2.2 AES-CTR where the IV for message $M$ is chosen as HMAC-SHA256($k_2, M$) truncated to the first 128 bits. The MAC key $k_2$ is distinct from the encryption key $k_1$.

Provide a short justification for your answer on your answer sheet.

*Clarification made during the exam:* You can assume that IV refers to the nonce for CTR mode.

☐ (G) Insecure  ☐ (I)  ☐ (K)  

☐ (H) Secure  ☐ (J)  ☐ (L)  

Q2.3 AES-CBC where the IV for message $M$ is chosen as SHA-256($x$) truncated to the first 128 bits. $x$ is a predictable counter starting at 0 and incremented per message.

☐ (A) Insecure  ☐ (C)  ☐ (E)  

☐ (B) Secure  ☐ (D)  ☐ (F)  

Q2.4 AES-CTR where the IV for message $M$ is chosen as SHA-256($x$) truncated to the first 128 bits. $x$ is a predictable counter starting at 0 and incremented per message.

*Clarification made during the exam:* You can assume that IV refers to the nonce for CTR mode.

☐ (G) Insecure  ☐ (I)  ☐ (K)  

☐ (H) Secure  ☐ (J)  ☐ (L)
Q2.5 AES-CBC where the IV for message $M$ is chosen as HMAC-SHA256($k_2 + x, M$) truncated to the first 128 bits. The MAC key $k_2$ is distinct from the encryption key $k_1$ and $x$ is a predictable counter starting at 0 and incremented per message.

○ (A) Insecure ○ (C) — ○ (E) —
○ (B) Secure ○ (D) — ○ (F) —

Q2.6 AES-CTR where the IV for message $M$ is chosen as HMAC-SHA256($k_2 + x, M$) truncated to the first 128 bits. The MAC key $k_2$ is distinct from the encryption key $k_1$ and $x$ is a predictable counter starting at 0 and incremented per message.

*Clarification made during the exam:* You can assume that IV refers to the nonce for CTR mode.

○ (G) Insecure ○ (I) — ○ (K) —
○ (H) Secure ○ (J) — ○ (L) —
Alice wants to send messages to Bob, but Mallory (a man-in-the-middle attacker) will read and tamper with data sent over the insecure channel.

- Alice and Bob share two secret keys $K_1$ and $K_2$
- $K_1$ and $K_2$ have not been leaked (Alice and Bob are the only people who know the keys)
- Enc is an IND-CPA secure encryption scheme
- MAC is a secure (unforgeable) MAC scheme

For each cryptographic scheme, select all true statements.

Clarification during exam: For the answer choice “Bob can always recover the message $M$,” assume that Mallory has not tampered with the message.

Clarification during exam: The answer choice “Bob can guarantee that $M$ has not been changed by Mallory,” this should say "Bob can guarantee that $M$ has not been changed by Mallory without detection."

Q3.1 $\text{Enc}(K_1, M), \text{MAC}(K_2, M)$

- (A) Bob can guarantee $M$ is from Alice
- (B) Bob can guarantee that $M$ has not been changed by Mallory
- (C) Mallory cannot read $M$
- (D) Bob can always recover the message $M$
- (E) None of the above
- (F) ——

Q3.2 $\text{Enc}(K_1, M), \text{MAC}(K_2, \text{Enc}(K_1, M))$

- (G) Bob can guarantee $M$ is from Alice
- (H) Bob can guarantee that $M$ has not been changed by Mallory
- (I) Mallory cannot read $M$
- (J) Bob can always recover the message $M$
- (K) None of the above
- (L) ——
Q3.3 Hash(M), MAC(K₁, M)

- (A) Bob can guarantee M is from Alice
- (B) Bob can guarantee that M has not been changed by Mallory
- (C) Mallory cannot read M
- (D) Bob can always recover the message M
- (E) None of the above

(F) ——

Q3.4 To simplify their schemes, Alice and Bob decide to set K₁ = K₂. (In other words, K₁ and K₂ are the same key.) Does this affect the security of their cryptographic schemes?

- (G) Yes, because they should always use a different key for every algorithm
- (H) Yes, because they should always use a different key for every message
- (I) No, because the encryption and MAC schemes are secure.
- (J) No, because the keys cannot be brute-forced.

(K) ——

(L) ——