Weaver
Spring 2022

CS 161
Computer Security

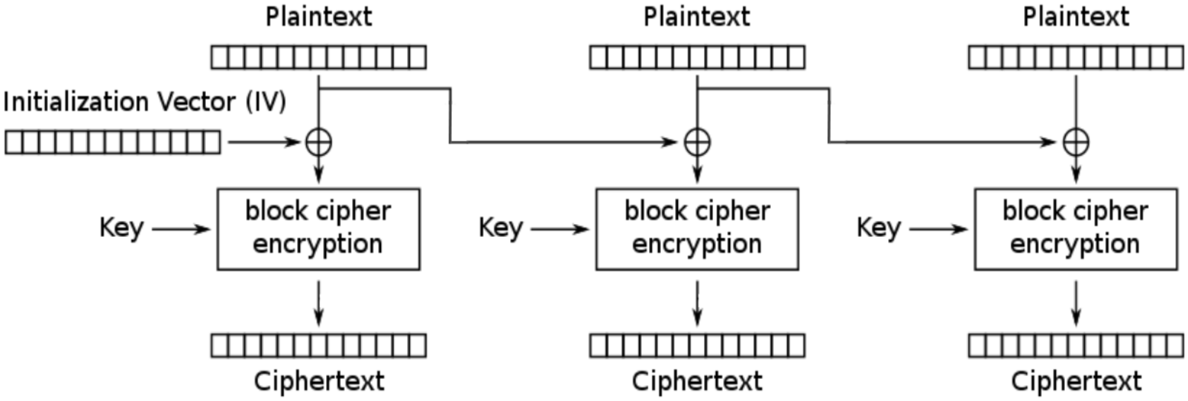
Exam Prep 4

Q1 *Block Ciphers* (0 points)

Consider the following block cipher mode of operation.

M_i is the ith plaintext block. C_i is the ith ciphertext block. E_K is AES encryption with key K.

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



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

Solution:

(A) True. By looking at the equation or the diagram, we can see that ciphertext block C_i does not depend on any previous ciphertext block (it only depends on plaintext blocks M_{i-1} and M_i).

(B) False. Since the plaintext block is passed through a block cipher, changing one byte of block cipher input will cause the block cipher output to be completely different.

(C) False. Changing one byte of M_i will change one byte of $M_i \oplus M_{i+1}$, the input to the block cipher. Again, changing one byte of block cipher input will cause the block cipher output to be completely different.

(D) False. Since the plaintext block is XOR'd with the previous block of plaintext before being passed into a block cipher, the corresponding ciphertext blocks are not necessarily identical.

(E) True. The plaintext is passed as an input to the block cipher, so it must be padded to a multiple of the block size.

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) ——

Solution: False. There is no randomness, so the scheme must be deterministic, and deterministic schemes cannot be IND-CPA secure.

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) ——

Solution: False. Intuitively, note that the randomness in the IV is not passed to subsequent blocks. The second block uses the second plaintext block M_2 and the previous plaintext block M_1 as block cipher input, but never uses the IV. This is the case for all subsequent blocks as well.

As a result, this scheme still leaks the existence of identical blocks. Formally, here are some ways Eve could win the IND-CPA game:

- Sending $M_0 = X\|X\|X$ and $M_1 = X\|Y\|Z$ results in the last two blocks of C_0 being identical
- Sending $M_0 = 0\|X$ and $M_1 = Y\|X$ results in distinguishable ciphertexts
- Sending the same message twice results in everything but the first block of the ciphertext being identical

Q2 *IV-e got a question for ya* **(0 points)**

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) ——

Solution: For any given message, the IV will be the same each time it's encrypted $\Longrightarrow$ deterministic scheme.

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) ——

Solution: For any given message, the IV will be the same each time it's encrypted $\Longrightarrow$ deterministic scheme.

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) ——

Solution: CBC mode requires its IVs to be random and thus unpredictable. To break IND-CPA, the adversary could send its first challenge as $M =$ SHA-256(0), which would result in $C =$ AES-CBC$_k$(SHA-256$(0) \oplus$ SHA-256$(0)) =$ AES-CBC$_k(0)$. Next, the adversary would send the challenge $M_0 =$ SHA-256(1), $M_1 \neq M_0$, and the adversary knows that the challenger encrypted M_0 if $C_b = C$ and M_1 otherwise.

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) ——

Solution: CTR mode is secure even with predictable nonces, so long as you never reuse a counter in any block. Note that if x were used directly as the nonce, this would be insecure. Consider two 2-block messages M_0 and M_1. The first message would be encrypted with $x = 0$, so the two blocks encrypt the counter 0 and 1. THe second message would be encrypted with $x = 1$, so the two blocks encrypt the counter 1 and 2, breaking security.

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) ——

Solution: The IV is unpredictable to the attacker, even though the adversary can view previous IVs due to the properties of the HMAC.

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) ——

Solution: The IV is unpredictable to the attacker, even though the adversary can view previous IVs due to the properties of the HMAC.

Q3 *Encryption and Authentication* (0 points)

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 $\mathsf{Enc}(K_1, M), \mathsf{MAC}(K_2, M)$

■ (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) ——

Solution: Bob can guarantee the message is from Alice and has not been tampered with because MACs provide authenticity and integrity.

However, MACs do not provide confidentiality, so Bob cannot guarantee that Mallory cannot read the message.

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

■ (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) ——

Solution: This is the encrypt-then-MAC approach from lecture, which guarantees confidentiality, integrity, and authenticity. This means Bob can guarantee M is from Alice, that M has not been tampered with, and that Mallory cannot read M.

Q3.3 $\mathsf{Hash}(M), \mathsf{MAC}(K_1, M)$

□ (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) ——

Solution: Bob cannot guarantee M is from Alice because he does not have the original message M to verify the MAC. Similarly, without M, Bob cannot guarantee that the message has not been tampered with. Since MACs do not provide confidentiality, Bob cannot guarantee that Mallory cannot read the message. Since the message is not encrypted, and hashes and MACs are not designed to be reversed, Bob cannot recover the message.

Q3.4 To simplify their schemes, Alice and Bob decide to set $K_1 = K_2$. (In other words, K_1 and K_2 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) ——

Solution: As described in lecture, key reuse (reusing the same key for different algorithms) can affect the security of cryptographic schemes, because the algorithms may interfere with each other.