(D) Neither

## CS 161 Computer Security

Discussion 5

### Cryptographic Hashes and MACs

# Question 1 Crytographic Hashes For each of the given functions H below, determine if it is one-way or not, and if it is collisionresistant or not. Q1.1 $H(x) = x^2$ (A) One way (B) Collision resistant $\bigcirc$ (C) Both oAssignment Project Exam Help Q1.2 For this part you have access to a SHA-256 hash function. The notation [x:y] refers to a slice of bytes x to y-1. //powcoder.com H(x) = SHA-256(2[0:len(x)-1]) $\bigcap$ (G) One way dd WeChat powcoder (I) Both (J) Neither Q1.3 $H(x) = x^3$ (A) One way (B) Collision resistant $\bigcirc$ (C) Both

#### Question 2 MAC Madness

(18 min)

Evan wants to store a list of every CS161 student's firstname and lastname, but he is afraid Mallory will tamper with his list.

Evan is considering adding a cryptographic value to each record to ensure its integrity. For each scheme, determine what Mallory can do without being detected.

Assume MAC is a secure MAC, H is a cryptographic hash, and Mallory does not know Evan's secret key k. Assume that firstname and lastname are all lowercase and alphabetic (no numbers or special characters) and that usernames must be unique.

| Q2.1 | (3 points) H(firstname  lastname)   |
|------|---|
|      | (A) Mallory can modify a record to be a value of her choosing   |
|      | $\bigcirc$ (B) Mallory can modify a record to be a specific value (not necessarily of her choosing)   |
|      | (C) Mallory cannot modify a record without being detected   |
|      | Assignment Project Exam Help  |
| Q2.2 | O (F) — https://powcoder.com (3 points) MAC(k, firstname   flastname)   |
|      | Hint: Can you think of two different records that would have the same MAC?  O (G) Mallory can modify a record to be a visue of her choosing |
|      | (H) Mallory can modify a record to be a specific value (not necessarily of her choosing)  |
|      | (I) Mallory cannot modify a record without being detected   |
|      | $\bigcirc$ (J) —  |
|      | $\bigcirc$ (K) —  |
|      | $\bigcirc$ (L) —  |
| Q2.3 | (3 points) $MAC(k, firstname)$ "-"  lastname), where "-" is a hyphen character.   |
|      | (A) Mallory can modify a record to be a value of her choosing   |
|      | $\bigcirc$ (B) Mallory can modify a record to be a specific value (not necessarily of her choosing)   |
|      | (C) Mallory cannot modify a record without being detected   |
|      | $\bigcirc$ (D) —  |

|      | (E) —  |  |
|------|--|--|
|      | (F) —  |  |
| Q2.4 | (3 points) $MAC(k, H(firstname)    H(lastname)    $   | e))  |
|      | (G) Mallory can modify a record to be a v  | value of her choosing                          |
|      | (H) Mallory can modify a record to be a sp   | ecific value (not necessarily of her choosing) |
|      | (I) Mallory cannot modify a record without   | out being detected                             |
|      | (J) —  |  |
|      | ○ (K) ——   |  |
|      | (L) —  |  |
| Q2.5 | (3 points) $MAC(k, firstname) \parallel MAC(k, lastname) \parallel$ |  |
|      | (B) Mallory can modify a record to be a sp   |  |
|      | O(C) Mallory campismodif Paccycl Can   | Cterng GOM                                     |
|      | O(D) — A 1 1 XX 7 C1 4   | 1  |
|      | Add WeChat   | powcoder                                       |
|      | (F) —  |  |
| Q2.6 | (3 points) Which of Evan's schemes guarant   | ee confidentiality on his records?             |
|      | O(G) All 5 schemes   | (J) None of the schemes                        |
|      | (H) Only the schemes with a MAC  | (K) —  |
|      | (I) Only the schemes with a hash   | (L) —  |

# Question 3 Confidentiality and integrity Alice and Bob want to communicate with confidentiality and integrity. They have: Symmetric encryption. Encryption: Enc(K, m).

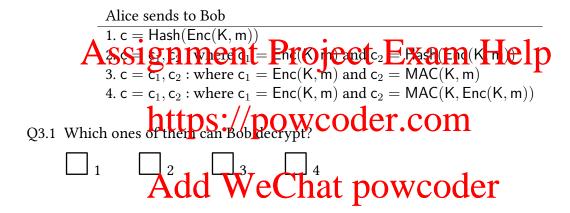
- Decryption: Dec(K, c).

- Cryptographic hash function: Hash(m).
- MAC: MAC(K, m).

They share a symmetric key K and know each other's public key.

We assume these cryptographic tools do not interfere with each other when used in combination; *i.e.*, we can safely use the same key for encryption and MAC.

()



| Q3.2 | onsider an eavesdropper Eve, who can see the communication between Alice and Bob             |
|------|--|
|      | which schemes, of those decryptable in (a), also provide <i>confidentiality</i> against Eve? |
|      | $\square_1$ $\square_2$ $\square_3$ $\square_4$  |

| Q3.3 | Consider a man-in-the-middle Mallory, who can eavesdrop and modify the communication between Alice and Bob.  |
|------|--|
|      | Which schemes, of those decryptable in (a), provide <i>integrity</i> against Mallory? <i>i.e.</i> , Bob can detect any tampering with the message? |
|      | $\square_1$ $\square_2$ $\square_3$ $\square_4$  |
|      |  |
|      |  |
|      |  |
|      |  |
| Q3.4 | Many of the schemes above are insecure against a replay attack.  |
|      | If Alice and 150 use these schemes to send many messages, and Malory remembers an  |
|      | encrypted message that Alice sent to Bob, some time later, Mallory can send the exact  |
|      | same encrypted message to Bob, and Bob will believe that Alice sent the message again  |
|      | How to modify those schemes with confidentiality & integrity to prevent replay attack?   |
|      | ♦ The scheme providing confidentiality & integrity is Scheme   |
|      | The modification is: We Chat powcoder  |
|      |  |