CS161 Fall 2025 — Introduction to Computer Security — Discussion 5

Q1 *MAC Madness* **(18 points)**

Evan wants to store a list of every CS161 student's `firstname` and `lastname`, but they are afraid that Mallory will tamper with their 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 concatenation does not add any delimiter (e.g. a space or tab), so `nick`$\|$`weaver` $=$ `nickweaver`.

Q1.1 (3 points) $\mathsf{H}(\texttt{firstname}\|\texttt{lastname})$

- ◯ Mallory can modify a record to be a value of her choosing
- ◯ Mallory can modify a record to be a specific value (not necessarily of her choosing)
- ◯ Mallory cannot modify a record without being detected

Q1.2 (3 points) $\mathsf{MAC}(k, \texttt{firstname}\|\texttt{lastname})$

Hint: Can you think of two different records that would have the same MAC?

- ◯ Mallory can modify a record to be a value of her choosing
- ◯ Mallory can modify a record to be a specific value (not necessarily of her choosing)
- ◯ Mallory cannot modify a record without being detected

Q1.3 (3 points) $\mathsf{MAC}(k, \texttt{firstname}\|\texttt{"-"}\|\texttt{lastname})$, where "-" is a hyphen character

- ◯ Mallory can modify a record to be a value of her choosing
- ◯ Mallory can modify a record to be a specific value (not necessarily of her choosing)
- ◯ Mallory cannot modify a record without being detected

Q1.4 (3 points) $\mathsf{MAC}(k, \mathsf{H}(\texttt{firstname})\|\mathsf{H}(\texttt{lastname}))$

- ◯ Mallory can modify a record to be a value of her choosing
- ◯ Mallory can modify a record to be a specific value (not necessarily of her choosing)
- ◯ Mallory cannot modify a record without being detected

(Question 1 continued...)

Q1.5 (3 points) $\mathsf{MAC}(k, \texttt{firstname}) \| \mathsf{MAC}(k, \texttt{lastname})$

- ◯ Mallory can modify a record to be a value of her choosing
- ◯ Mallory can modify a record to be a specific value (not necessarily of her choosing)
- ◯ Mallory cannot modify a record without being detected

Q1.6 (3 points) Which of Evan's schemes guarantee confidentiality on his records?

- ◯ All 5 schemes
- ◯ Only the schemes with a hash
- ◯ Only the schemes with a MAC
- ◯ None of the above

Q2 *Confidentiality and Integrity* **(4 points)**

Alice and Bob want to communicate with confidentiality and integrity. They have:

- Symmetric Encryption:
  - Encryption: $\mathsf{Enc}(K, m)$
  - Decryption: $\mathsf{Dec}(K, m)$
- Cryptographic Hash Function: $\mathsf{Hash}(m)$
- MAC: $\mathsf{MAC}(K, m)$

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.

Alice sends to Bob
1. $c = \mathsf{Hash}(\mathsf{Enc}(K, m))$
2. $c = c_1, c_2$: where $c_1 = \mathsf{Enc}(K, m)$ and $c_2 = \mathsf{Hash}(c_1)$
3. $c = c_1, c_2$: where $c_1 = \mathsf{Enc}(K, m)$ and $c_2 = \mathsf{MAC}(K, m)$
4. $c = c_1, c_2$: where $c_1 = \mathsf{Enc}(K, m)$ and $c_2 = \mathsf{MAC}(K, c_1)$

Q2.1 (1 point) In which schemes can Bob successfully decrypt m given c?

☐ 1 ☐ 2 ☐ 3 ☐ 4

Q2.2 (1 point) Consider an eavesdropper Eve, who can see the communication between Alice and Bob.

Out of all of the schemes decryptable in 2.1, which schemes also provide *confidentiality* against Eve?

☐ 1 ☐ 2 ☐ 3 ☐ 4

Q2.3 (1 point) Consider a man-in-the-middle Mallory, who can eavesdrop and modify the communication between Alice and Bob.

Out of all of the schemes decryptable in 2.1, which schemes also provide *integrity* against Mallory? *i.e.,* Bob can detect any tampering with the message?

☐ 1 ☐ 2 ☐ 3 ☐ 4

Q2.4 (1 point) Many of the schemes above are insecure against a *replay attack*.

If Alice and Bob use these schemes to send many messages, and Mallory 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*.

For each scheme that has **both** confidentiality against Eve (2.2) *and* integrity against Mallory (2.3), how can the scheme be modified to prevent a replay attack?

Q3 *Key Exchange Protocols* **(3 points)**

Recall that in a Diffie-Hellman key exchange, there are values a,b,g, and p. Alice computes $g^a \bmod p$ and Bob computes $g^b \bmod p$.

Q3.1 (1 point) Which of these values (a,b,g, and p) are publicly known and which must be kept private?

a	b	g	p
◯ Public	◯ Public	◯ Public	◯ Public
◯ Private	◯ Private	◯ Private	◯ Private

Q3.2 (1 point) Mallory can eavesdrop, intercept, and modify everything sent between Alice and Bob. Alice and Bob perform Diffie-Hellman to agree on a shared symmetric key K. After the exchange, Bob gets the feeling that something went wrong and calls Alice. He compares his value of K to Alice's and realizes that they are different. Explain what Mallory has done.

Q3.3 (1 point) Assume that K, the Diffie-Hellman exponents a and b, and the messages themselves are destroyed once all messages are sent. That is, these values are not stored on Alice and Bob's devices after they are done communicating.

Eavesdropper Eve records all communications between Alice and Bob, but is unable to decrypt them. At some point in the future, Eve is lucky and manages to compromise Bob's computer.

Is the confidentiality of Alice and Bob's prior **Diffie-Hellman**-based communication in jeopardy? Explain why.

◯ Yes ◯ No