Question 1 ***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.

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

◯ (A) Mallory can modify a record to be a value of her choosing

◯ (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

◯ (D) —

◯ (E) —

◯ (F) —

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

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

◯ (G) Mallory can modify a record to be a value 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

◯ (J) —

◯ (K) —

◯ (L) —

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

- ◯ (A) Mallory can modify a record to be a value of her choosing
- ◯ (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
- ◯ (D) ——
- ◯ (E) ——
- ◯ (F) ——

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

- ◯ (G) Mallory can modify a record to be a value 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
- ◯ (J) ——
- ◯ (K) ——
- ◯ (L) ——

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

- ◯ (A) Mallory can modify a record to be a value of her choosing
- ◯ (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
- ◯ (D) ——
- ◯ (E) ——
- ◯ (F) ——

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

- ◯ (G) All 5 schemes
- ◯ (H) Only the schemes with a MAC
- ◯ (I) Only the schemes with a hash
- ◯ (J) None of the schemes
- ◯ (K) ——
- ◯ (L) ——

Question 2 ***Key Exchange Protocols*** **()**

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 $g^b \bmod p$.

Q2.1 Which of these values (a, b, g, and p) are publicly known and which must be kept private?

Q2.2 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 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.

Now consider the following key exchange protocols which can be used by Alice (A) and Bob (B) to agree upon a shared key, K.

ElGamal-Based Key Exchange

Message 1	$A \rightarrow B$:	$\{K\}_{PK_B}$
	Key exchanged	
Message 2	$A \leftarrow B$:	$\{secret1\}_K$
Message 3	$A \rightarrow B$:	$\{secret2\}_K$

Diffie-Hellman Key Exchange

Message 1	$A \rightarrow B$:	$g^a \mod p$
Message 2	$A \leftarrow B$:	$g^b \mod p$
	Key exchanged	
	$K = g^{ab} \mod p$	
Message 3	$A \leftarrow B$:	$\{secret1\}_K$
Message 4	$A \rightarrow B$:	$\{secret2\}_K$

Some additional details:

- PK_B is Bob's long-lived public key.
- 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.

Q2.1 Is the confidentiality of Alice and Bob's prior ElGamal-based communication in jeopardy?

Q2.2 What about Alice and Bob's Diffie-Hellman-based communication?

Question 3 ***Public Key Encryption*** ()

The El Gamal encryption scheme is reproduced below:

- **Key Generation**: public key $= (g, h, p)$, where $h = g^k \pmod{p}$, private key $= k$
- **Encryption**: $c = (c_1, c_2) = (g^r \bmod p, m \times h^r \bmod p)$, where r is randomly sampled from $\{1, \ldots, p-1\}$.
- **Decryption**: $m = c_1^{-k} \times c_2 \pmod{p}$

Look at each scenario below and select the appropriate options.

Q3.1 With El Gamal, it is not a problem if the adversary can learn the value of g somehow.

◯ (A) True

◯ (B) False

◯ (C) ——

◯ (D) ——

◯ (E) ——

◯ (F) ——

Q3.2 With El Gamal, it is not a problem if the value r used during encryption is accidentally revealed after the encryption is complete.

◯ (G) True

◯ (H) False

◯ (I) ——

◯ (J) ——

◯ (K) ——

◯ (L) ——

Now imagine that Alice (A) and Bob (B) want to communicate over an insecure network and they know each other's public key. Consider the following message exchange:

A: Hey Bob, it's Alice. How many dollars do I owe you?
B: 10000

The message is encrypted with Alice's public key using ElGamal encryption.
Alice decrypted this successfully, but suddenly remembered that she only owed Bob $100.

Q3.1 Assume Bob would not lie. How did an attacker tamper with the message?

Q3.2 What could Bob have additionally sent that would've stopped this attack?