Week 8: Cryptography: Hash Functions, MACs and Authentication

Confidentiality and Integrity

Question 1: Alice and Bob want to communicate with confidentiality and integrity. They share a symmetric key K and have the following:

- Symmetric encryption:
  - Encryption using key k and message m as Enc(K, m) = c
  - Decryption using key k and ciphertext c as Dec(K, c) = m
- Cryptographic hash function: Hash(m).
- MAC: MAC(K, m).

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 = Hash(Enc(K, m))
2. c = c1, c2: where c1 = Enc(K, m) and c2 = Hash(Enc(K, m))
3. c = c1, c2: where c1 = Enc(K, m) and c2 = MAC(K, m)
4. c = c1, c2: where c1 = Enc(K, m) and c2 = MAC(K, Enc(K, m))

Q1.1 Which of the above four can Bob decrypt?

Q1.2 Consider an eavesdropper Eve, who can see the communication between Alice and Bob. Which schemes, of those decryptable in (2.1), also provide confidentiality against Eve?

Q1.3 Consider a meddler-in-the-middle Mallory, who can eavesdrop and modify the communication between Alice and Bob. Which schemes, of those decryptable in (1.1), provide integrity against Mallory? I.e., Bob can detect any tampering with the message?

Q1.4 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. How can we modify these schemes with ***confidentiality & integrit****y* to prevent replay attack?

The scheme providing confidentiality & integrity is Scheme _______

The modification is:

Question 2: MACs

Evan wants to store a list of every CS88 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 the following:

- 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,
- The usernames must be unique.

Q2.1 H (firstname || 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

Q2.2 MAC(k, firstname || lastname) Hint: Can you think of two different records that would have the same MAC?

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

Q2.3 MAC(k, firstname || "-" || 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

Q2.4 MAC(k, H(firstname)|| H(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

Q2.5 MAC(k, firstname) // MAC(k, lastnam

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

Q2.6 Which of Evan's schemes guarantee confidentiality on his records?

A. All 5 schemes
B. Only the schemes with a MAC
C. Only the schemes with a hash
D. None of these schemes