COMP435 In-Class Practice 10/28/26 Name: _____

Question 1: Security of MACs Alice sends Bob a message over a network where an active attacker can read and modify anything in transit. The two scenarios are depicted on slide 50 in lecture 9.

1. Alice sends the pair (msg, H) with $H = h(msg)$.
2. Alice and Bob share a secret key k. Alice sends (msg, tag) with $tag = MAC_k(msg)$.

For each protocol, what security properties does Bob get—if any—when he receives the pair and the check passes?

Question 2: RSA Digital Signatures In this toy RSA example, Alice's private signing exponent is $s = 3$, her public verification exponent is $v = 7$, and $N = 33$. Use the simplified formulas from the slides (without hashing or padding). Alice sends the message $m = 2$ along with her signature.

2.1. Compute her signature: $sig = m^s \bmod N$.

2.2. Bob checks whether $sig^{\,v} \bmod N = m$. Verify the signature. *Hint: compute* 8^2 *and* 8^4 *modulo 33, then use* $8^7 = 8^4 \cdot 8^2 \cdot 8$.

2.3. Does sending (m, sig) keep the message confidential? Why?

Question 3: Encrypt, Then Sign Alice wants to send Bob a confidential message that he can verify came from her. Each has a public/private key pair, and both know the correct public key for the other person. Assume secure encryption and signature schemes.

3.1. Fill in each blank with whose key is used and whether it is public or private.

Step	Key used
Alice encrypts the message to get c.	
Alice signs c to get tag.	
Bob verifies the signature on c.	
Bob decrypts c.	

3.2. Alice sends (c, tag). Mallory replaces c with a different ciphertext but keeps Alice's original tag. Should Bob's signature check pass? Briefly explain.