COMP435 In-Class Practice 9/22/25 Name: _____

Question 1: RSA Practice Answer the following questions related to RSA encryption and decryption.

1. Choose primes $p = 3$ and $q = 5$.
   (a) Compute N and $\varphi(N)$.
   (b) Let $e = 3$. Verify that $\gcd(e, \varphi(N)) = 1$.
   (c) Find the private exponent d such that $ed \equiv 1 \pmod{\varphi(N)}$.
2. Alice wants to send the message $m = 2$.
   (a) Compute the ciphertext $c = m^e \bmod N$.
   (b) Bob decrypts by computing $m' = c^d \bmod N$. Show the arithmetic and confirm that $m' = m$.

Question 2: 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?