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

Question 1: Collision Resistant Hash Functions Complete the definition: a hash function h is collision resistant if it is computationally infeasible to find messages m and m' such that...

Question 2: Can Collisions Exist? A hash function accepts messages of any length and produces a 256-bit hash. Which statement is correct? Select one.

- ◯ A collision-resistant hash function has no collisions.
- ◯ Collisions must exist, but finding one should be computationally infeasible.
- ◯ Any two messages of the same length have the same hash.
- ◯ Different messages always have different hashes.

Question 3: Which Hash Property? Match each attack goal to the property it would defeat. Use each letter once.

A. Collision resistance **B.** Second pre-image resistance
C. Pre-image resistance

3.1. Given only a hash value H, find any message whose hash is H. _____

3.2. Given a particular contract, create a different contract with the same hash. _____

3.3. Create any two different documents that have the same hash; neither document is fixed in advance. _____

Question 4: A Toy Hash Suppose $h(m)$ is the sum of the decimal digits of a nonnegative integer m, modulo 10. For example, $h(123) = 6$. Give a different integer with the same hash as 123. Would this function be collision resistant? Briefly explain.