**COMP435 9/17/25 Practice** Name: _____

**Question 1: RSA** Professor Reckless decides to develop their own scheme for distributing exam grades while maintaining confidentiality. First, Prof. Reckless asks each student to generate an RSA public-private key pair and post the public key $(e, N)$ to the class forum. Prof. Reckless then meets with each student individually to make sure they have the correct public key associated with each student. When it is time to distribute grades, Prof. Reckless encrypts each student's grade, $g$, using the student's public key (computing $c \equiv g^e \pmod{N}$) and posts the encrypted grade ($c$), along with the student's name, to the class forum. Because only the intended student has the right private key, only they will be able to decrypt the posted grade to learn what their grade is. What is wrong with this scheme?

**Question 2: Collision Resistant Hash Functions** We are going to define the semantics of a collision resistant hash function. We can describe a collision resistant hash function as a function where it is hard to find m, m' such that....