Quiz 1

- Honor Code: You must work completely independently on this assignment. Do not discuss the questions or answers with each other before the assignment is due. Any breach of the honor code will be handled per the University's policy on academic honesty.
- Follow the instructions very careful. Answers that do not conform to the instructions will not be given credit.
- Submit your answers through Blackboard as a PDF file
- You may use your BCT textbook only. Do not use any other resources.

1. Which of the following is true of SHA-256? There may be zero, one, or more than one true statements.
   a. It has been proven not to have a collision
   b. We hope that there are no collisions
   c. No collision has ever been publicly found
   d. It has been proven that there is no fast way to find collisions

2. How can the hash function "H(x) = x mod 64" be reliably used to determine whether two, highly-sensitive legal documents are identical? Describe the steps in detail.

3. Why does a cryptographic commitment need to use a nonce? Are there any restrictions on what value can be chosen as a nonce? If so, give those restrictions.

4. Suppose you are given the following two puzzles. Which puzzle will take longer to solve? Explain why.
   a. $H(x \circ id_1) \in Y_1$, where id_1 is a specific 100-bit value and Y_1 is the set of 1000-bit values.
   b. $H(x \circ id_2) \in Y_2$, where id_2 is a specific 1000-bit value and Y_2 is the set of 100-bit values.

   Assume H is a puzzle-friendly, cryptographic hash function.