Quiz 1
Ranran He

1. BCD

2. Step 1: We can first generate a random value nonce, then put the first document and nonce into the hash function to get the result1.
   Step 2: use the nonce in step 1 to do hash function again with the second document and get the result2.
   Step 3: Compare the two results – result1 and result2. If they are the same, then we can tell these two documents are the same, otherwise, they are not.

3. A nonce will make the inputs spread out to get larger set of outputs, which will give the hash function the property of hiding.
   The nonce is a random secret value. It should be chosen from a probability distribution which has high min-entropy and should be changed every time when we do a commitment.

4. A
   A puzzle will be harder to solve when it goes from a smaller set to a larger set. For option A, id1, as input, is a 100-bit value which is a smaller set than the 1000-bit outputs set, however, B gives id2 as a 1000-bit value as input which is a larger set than its output Y which is 100-bit. Thus, A is harder to solve.