Quiz 2

- 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 types of modifications of a block chain data structure can be detected by someone who holds a hash pointer to the latest block? Select all that apply.
    a. Insertion of a block
    b. Deletion of a block
    c. Tampering of data in a block
    d. Re-ordering of blocks

2. Which of these keys are required for verifying a signature? Select all that apply.
    a. The secret key
    b. The public key
    c. Both the secret and the public key
    d. None. Keys are required only for signing; anyone can verify the signature without a key

3. If you generate numerous identities (public keys) for yourself and interact online using those different identities. Select all that apply.
    a. It is essential to have a good source of randomness. Otherwise adversaries might be able to deduce your secret key and take control of your identities.
    b. Adversaries may be able to link your identities because public keys generated on the same computer tend to look similar
    c. Adversaries may be able to de-anonymize you by analyzing your activity patterns

4. Alice and Bob use ScroogeCoin. Alice owns ten coins, each under a different address (public key) and each of value 3.0. She would like to transfer coins of value 5.0 to Bob. Recall that the PayCoins transaction consumes (and destroys) some coins, and creates new coins of the same total value. Alice's transfer will require, at a minimum:
    a. One PayCoins transaction, one new coin created, and one signature
    b. One PayCoins transaction, two new coins created, and two signatures
    c. Two PayCoins transactions, two new coins created, and four signatures
    d. Two PayCoins transactions, one new coin created, and two signatures