Blockchain Quiz

Name: Roll number:

Instructions: Choose all the correct options. If all the options are correct and "All of the above" is in the options, choose all the options.

1. Which of the following statement(s) about the birthday paradox in hash functions are true?
    a. It refers to the likelihood of two people sharing the same birthday
    b. It illustrates the probability of hash collisions as more data is hashed
    c. It is a term used in cryptographic attacks
    d. It only applies to hash functions with small input sizes

Ans: a,b,c.

2. In the Merkle-Damgard Construction
    a. The number of instances or rounds of hash functions are fixed
    b. Has been introduced to process arbitrary lengths of data
    c. The final depends only on the last round of the hashing instance
    d. The initialization vector depends on the message to be hashed

Ans: b. The number of rounds of hash function in Merkle-Damgard constructions is $|M|/n_2$. Intialization vector is constant. The final output depends on all the inputs.

3. The hash and sign paradigm
    a. Helps to prevent forgery attacks
    b. Improves the efficiency
    c. Reduces the signature length
    d. Increases the malleability of the signature

Ans: a, b, c. All the 3 points discussed in class. If a signature is malleable it is the flaw of the signature scheme. Not due to the addition of hash functions.

4. Let $H_1:\{0,1\}^n \rightarrow \{0,1\}^m$ and $H_2:\{0,1\}^n \rightarrow \{0,1\}^m$ be two hash functions. Define a hash function $H:\{0,1\}^n \rightarrow \{0,1\}^{2m}$ by $H(x) = H_1(x) \,||\, H_2(x)$, where "||" denotes the concatenation of two strings. Given that the hash function H_1 is collision resistant. Which of the following option(s) are true?
    a. Both hash functions H and H_2 must be collision resistant
    b. H_2 is collision resistant but H may not be collision resistant
    c. H is collision resistant but H_2 may not be collision resistant
    d. Both H and H_2 are not collision resistant

Ans: c. H must be collision-resistant but we can't say about anything on H_2. It maybe collision resistant or maybe collision non-resistant.

5. Which of the following is true about hash pointers in blockchain technology?
    a. They store the hash of previous block's transactions
    b. They store the entire previous block's data
    c. They help create a secure and tamper-resistant chain of blocks
    d. They make block validation faster and more efficient

Ans: c.

6. What is the purpose of a hash pointer in data structures?

a. To store the data itself
b. To uniquely identify data or nodes
c. To provide a link to the next node in a linked list
d. To ensure data integrity

Ans: b,d. Each block has unique hash. So Hash pointers can uniquely identify a block as well as guarantees its integrity.

7. Which of the following are advantages of digital signatures over traditional handwritten signatures?

a. Ease of verification
b. Non-repudiation
c. Inability to forge
d. Ability to sign physical documents

Ans: a, b, c. We just need the private key of any entity in the world to verify its signature. Non-repudiation or Inability to forge means breaking the underlying hard mathematical problem which is considered impossible.

8. Which of the following statement(s) are true about ECDSA?

a. ECDSA is a symmetric encryption algorithm.
b. ECDSA will be secure even if a quantum computer (powerful enough) is built
c. ECDSA relies on the mathematics of elliptic curves
d. ECDSA requires a public key and a private key

Ans:c,d. ECDSA is a public-key cryptographic scheme. ECDSA is based on discrete logs hence not quantum secure.

9. Which step(s) are involved in the ECDSA signature generation process?

a. Hashing the message
b. Generating a random number
c. Computing a random point on the curve
d. Sharing the private key

Ans: a, b, c. It is a hash-and-sign paradigm. We have to choose a random number and the random number multiplied with the generator gives a random point.

10. In the hash and sign paradigm, if the hash used is not collision resistant then which of the following(s) are true?

a. An adversary can forge the digital signature
b. Non-Repudiation is still valid
c. The integrity of the digital signature scheme is violated
d. All of the above

Ans: a,c. An adversary can find x' such tha H(x)=H(x'). A signer can use the same logic to deny the signature.