Lecture 15 – Network Security & Cryptography Quiz

1. Which component of the CIA triad is violated when an attacker successfully performs a denial-of-service (DoS) attack on a web server?
A. Confidentiality
B. Integrity
C. Availability
D. Authenticity

ANS:

2. In practical secure communication protocols, what is the main role of public-key cryptography?
A. Encrypt all bulk data because it is faster than symmetric ciphers
B. Generate message authentication codes for each packet
C. Establish a shared symmetric session key, then use symmetric encryption for data
D. Compress data before transmission

ANS:

3. Which of the following is a passive attack on a communication channel?
A. Replay of captured messages
B. Denial-of-service
C. Traffic analysis
D. Modification of messages

ANS:

4. In an active attack, where an attacker captures a valid message and later retransmits it to produce an unauthorized effect, the attack is called:
A. Masquerade
B. Replay
C. Eavesdropping
D. Traffic analysis

ANS:

5. Which term best describes the set of reachable and exploitable vulnerabilities in a system, including network, software, and human factors?
A. Attack tree
B. Risk surface
C. Attack surface
D. Threat model

ANS:

6. Which of the following is a countermeasure objective described in the lecture?
A. Obfuscate, Encrypt, Encode
B. Prevent, Detect, Recover
C. Block, Filter, Route
D. Hash, Sign, Compress

ANS:

7. In symmetric (secret-key) encryption, which of the following must be true for secure communication?
A. Sender and receiver share the same secret key
B. Sender and receiver use different public keys
C. Only the sender knows the key
D. Only the receiver knows the key

ANS:

8. A monoalphabetic substitution cipher that maps each letter of the alphabet to another letter is an example of:
- A. Stream cipher
- B. Block cipher
- C. Simple substitution cipher
- D. One-time pad

ANS:

9. In Cipher Block Chaining (CBC) mode, the input to the encryption algorithm for a block P_i is:
- A. current plaintext block P_i only
- B. current plaintext block P_i XOR previous ciphertext block C_{i-1}
- C. C_{i-1} only
- D. P_i XOR the secret key

ANS:

10. Which statement about the Data Encryption Standard (DES) is correct according to the lecture?
A. DES uses a 128-bit key and is still considered secure today
B. DES uses a 64-bit key but only 56 bits are effective for security
C. DES is a stream cipher designed for software only
D. DES was designed specifically for elliptic curve cryptography

ANS:

11. Triple DES (3DES) improves upon DES primarily by:
A. Reducing the key size to speed up brute-force search

B. Repeating DES three times with multiple keys to increase effective key length
C. Switching from a block cipher to a stream cipher
D. Using elliptic curves instead of modular arithmetic

ANS:

12. In public-key cryptography, which property must hold for the key pair (public key, private key)?
A. It must be easy to compute the private key from the public key
B. Both keys must remain secret from all outsiders
C. It must be computationally infeasible to derive the private key from the public key
D. The public and private keys are identical

ANS:

13. Which protocol is specifically used for establishing a shared secret key over an insecure channel, rather than directly encrypting data?
A. RSA
B. Diffie–Hellman key exchange
C. AES
D. DES

ANS:

14. In the Diffie–Hellman key exchange, a large prime p and a generator g are chosen such that:
A. p is any integer and g is any real number
B. p is a sufficiently large prime and g is a generator less than p
C. Both p and g must be private random numbers
D. p is the shared secret and g is the session key

ANS:

15. Which of the following best describes a key requirement for random numbers used in cryptographic applications?
A. They must be easy to predict based on previous values
B. They must follow a simple repeating pattern
C. They should be uniformly distributed and unpredictable
D. They should be generated using the system clock only

ANS:

16. When a sender encrypts data (or a hash of the data) with their private key and the receiver verifies it using the sender's public key, which property is primarily achieved?
A. Confidentiality of the message contents
B. Integrity and non-repudiation
C. Key exchange without prior agreement

D. Reduction of the attack surface

ANS: