L3 – Computer Systems – Semester 6 (2024/2025)

Computer Security - Interrogation (10 pts) /Correction

Circle the right answers (-0.25 incorrect answer, -0.25 two erasures):

1. In modern cryptography, the role of a key is primarily to:

A) Generate random data streams

B) Compress plaintext into smaller blocks

C) Parameterize the encryption algorithm for specific outputs

D) Hide the algorithm itself

2. The strength of a cryptographic system depends most on:

A) Complexity of the cipher text format

B) Regular encryption changes

C) Usage of different encryption algorithms

D) Length and randomness of the key

3. Key management primarily involves:

A) Updating the cipher system periodically

B) Secure generation, storage, and distribution of keys

C) Encrypting key metadata

D) Ensuring large key sizes only

4. To mitigate interception during key transfer, one effective method is to:

A) Transmit key fragments over independent channels

B) Compress the key before sending

C) Add redundant padding

D) Hide the key in https queries

5. Key longevity principles recommend that keys should:

A) Be stored encrypted and reused indefinitely

B) Have a defined expiration and replacement cycle

C) Be private after days of use

D) Only be changed when detected

6. In ECB mode, identical plaintext blocks result in:

A) Randomized ciphertext

B) Ciphertext of variable lengths

C) Identical ciphertext blocks

D) Different ciphertexts due to key rotation

7. A known flaw of ECB encryption is its inability to:

A) Perform fast encryption

B) Encrypt multiple files simultaneously

C) Accept keys larger than 128 bits

D) Hide structure and patterns in data

8. Initialization vectors (IVs) in CBC are used to:

A) Compress the first block

B) Encrypt messages' headers separately

C) Randomize the first block to prevent pattern leakage

D) Increase encryption speed

9. PCBC mode was notably implemented in:

A) Kerberos v4 authentication protocol

B) Bitcoin Core protocol

C) HTTPS transactions

D) PKI certification

10. In OFB mode, feedback for encryption is based on:

A) Previous ciphertext block

B) Output of the previous encryption function

C) IV XOR plaintext

D) Plaintext bitstream

11. CTR mode replaces the shift register used in CFB with:

A) Initialization vector duplication

B) Nonce concatenation

C) Incremented counters encrypted each cycle

D) Randomized XOR

12. Continuous encryption is preferred when:

A) Low storage is critical

B) Minimizing single-bit error propagation is important

C) Large file size optimization is required

D) Network latency must be minimized

13. Which algorithm is classified as symmetric?

A) Advanced Encryption Standard

B) Diffie-Hellman

C) RSA

D) ElGamal

14. In public-key cryptography, a message encrypted with a public key can be decrypted by:

A) The same public key

B) The matching private key

C) Any private key

D) A derived symmetric key

15. Modular exponentiation in RSA is used to:

A) Generate prime numbers quickly

B) Create key pairs

C) Efficiently compute encryption and decryption

D) Help find inverse modulo

16. Fermat's Little Theorem is useful in cryptography for:

A) Helps find Bézout coefficients

B) Verifying modular relationships

C) Encrypting large files

D) Key compression

17. SHA-1 differs from MD5 primarily by:

A) Faster computation

B) Reduced rounds

C) Simpler collision resistance

D) Longer hash output

18. MD5 is a hashing algorithm that outputs:

A) 64 bits

B) 192 bits

C) 128 bits

D) 256 bits

19. PGP (Pretty Good Privacy) strengthens security by:

A) Using only symmetric encryption

B) Relying solely on one-way hashing

C) Combining symmetric encryption with public-key encryption

D) Chaining multiple RSA encryptions

20. A dictionary attack improves on brute-force attacks by:

A) Testing all binary combinations

B) Testing commonly known words

C) Randomly mutating keyspaces

D) Reverse engineering hash functions

For those who did not pass the interrogation assessment (refer to Exercise 1 of the exam as 'Interrogation mark')