Cryptography Lecture 7 - Detailed MCQs

- 1. In the EAV-security experiment, the attacker's goal is to:
 - a) Guess the encryption key
 - b) Determine which of two chosen messages was encrypted
 - c) Recover both plaintexts
 - d) Detect if two ciphertexts are equal

Answer: b

- 2. A scheme is EAV-secure if:
 - a) No attacker can guess b better than random guessing
 - b) No attacker can guess the key with probability 1
 - c) It uses randomized encryption only
 - d) It hides the length of the message

Answer: a

- 3. In multiple-message indistinguishability, all messages:
 - a) Must be different
 - b) Must have the same length in each pair m0,i, m1,i
 - c) Must be encrypted with different keys
 - d) Must be random strings

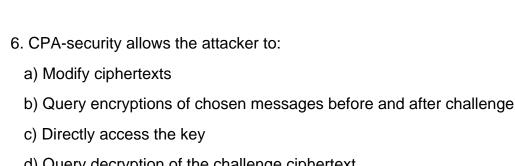
Answer: b

- 4. No deterministic encryption scheme can be multiple-message secure because:
 - a) Deterministic schemes are slow
 - b) Repeated encryptions of the same message produce the same ciphertext
 - c) Keys are too short
 - d) They cannot expand plaintext

Answer: b

- 5. Randomized encryption helps multiple-message security by:
 - a) Making encryption slower
 - b) Producing different ciphertexts for the same message
 - c) Removing the need for keys
 - d) Increasing message length

Answer: b



d) Query decryption of the challenge ciphertext

Answer: b

- 7. If a scheme is CPA-secure, it is also:
 - a) Perfectly secure
 - b) Multiple-message secure
 - c) Deterministic
 - d) Stateless

Answer: b

- 8. No deterministic encryption scheme can be CPA-secure because:
 - a) It requires randomized keys
 - b) The attacker can repeat encryptions and detect patterns
 - c) It leaks key length
 - d) It is not polynomial-time

Answer: b

- 9. The number of functions mapping {0,1}^n to {0,1}^n is:
 - a) 2ⁿ
 - b) 2^{n * 2^n}
 - c) 2^{2n}
 - d) 2^{n^2}

Answer: b

- 10. A pseudorandom function is:
 - a) A function that outputs random numbers
 - b) A keyed function that is indistinguishable from a truly random function
 - c) Any deterministic function
 - d) A function with maximum possible output length

Answer: b

- 11. Which is an insecure PRF example?
 - a) $F(k, x) = AES_k(x)$

- b) F(k, x) = 0^n
 c) F(k, x) = HMAC(k, x)
 d) F(k, x) built from a secure block cipher
 Answer: b
 12. In the PRF definition, F_k is:
 a) The key
 - b) The fixed function obtained when key k is chosen
 - c) The set of all possible keys
 - d) The encryption algorithm

Answer: b

- 13. Which security model is the strongest among those discussed?
 - a) EAV-security
 - b) Multiple-message indistinguishability
 - c) CPA-security
 - d) Perfect secrecy

Answer: c

- 14. In the "Midway" example, the main point was:
 - a) Keys should be reused
 - b) Knowing repeated messages is a security risk
 - c) CPA-security is unrealistic
 - d) Deterministic encryption is fast

Answer: b

- 15. If P is CPA-secure, what is true?
 - a) It must be randomized
 - b) It is necessarily slower than EAV-secure schemes
 - c) It can be broken by multiple-message attacks
 - d) It is only secure for short messages

Answer: a

- 16. In EAV security, the adversary sees:
 - a) The encryption key
 - b) Only the ciphertext of one of two chosen messages
 - c) The decryption oracle output

- d) The random seed Answer: b
- 17. Multiple-message security fails if:
 - a) The scheme is randomized
 - b) The scheme is deterministic
 - c) Keys are refreshed every time
 - d) The scheme hides ciphertext patterns

Answer: b

- 18. CPA-security is considered minimal for modern encryption because:
 - a) It allows key reuse without risk
 - b) It covers chosen-plaintext scenarios common in real systems
 - c) It's easier to implement than EAV
 - d) It is unbreakable even with infinite computation

Answer: b

- 19. The set Func_n contains:
 - a) All possible deterministic encryption keys
 - b) All possible functions mapping n-bit inputs to n-bit outputs
 - c) All possible PRGs
 - d) All possible PRFs

Answer: b

- 20. A PRF family {F_k} is:
 - a) Equal to Func_n
 - b) A tiny subset of Func_n
 - c) Larger than Func_n
 - d) Completely random functions

Answer: b