UNIT-II Symmetric Key Ciphers

1. Block cipher principles are based on the design concepts of:
a) Confusion and diffusion
b) Compression and expansion
c) Hashing and salting
d) Padding and truncation
Answer: a

2. In block cipher design, "diffusion" refers to:
a) Hiding the relationship between key and cipher text
b) Spreading the influence of a single plain text bit over many cipher text bits
c) Reducing the key size
d) Increasing block size only
Answer: b

3. In block cipher design, "confusion" refers to:
a) Making the relationship between key and cipher text as complex as possible
b) Spreading plain text influence across the cipher text
c) Reducing the number of rounds
d) Increasing the block size
Answer: a

4. A Feistel cipher structure divides the input block into:
a) Four equal parts
b) Two equal halves
c) Eight blocks
d) A single block
Answer: b

5. DES (Data Encryption Standard) operates on a block size of:
a) 32 bits
b) 56 bits
c) 64 bits
d) 128 bits
Answer: c

6. The actual key length used by DES for encryption (excluding parity bits) is:
a) 56 bits b) 64 bits
c) 48 bits d) 128 bits
Answer: a

7. The DES algorithm performs how many rounds of encryption?

a) 8

b) 10

c) 16

d) 32

Answer: c

8. DES is structured as a:

a) Substitution-only cipher

b) Feistel cipher

c) Stream cipher

d) Public key cipher

Answer: b

9. Triple DES (3DES) was introduced mainly to overcome:

a) The small block size of DES

b) The vulnerability of DES's 56-bit key to brute-force attacks

c) The slow speed of AES

d) The need for asymmetric keys

Answer: b

10. AES (Advanced Encryption Standard) operates on a fixed block size of:

a) 64 bits

b) 128 bits

c) 192 bits

d) 256 bits

Answer: b

11. AES supports key sizes of:

a) 56, 64, and 128 bits

b) 128, 192, and 256 bits

c) 64, 128, and 192 bits

d) 32, 64, and 128 bits

Answer: b

12. AES is based on which structure, unlike DES?

a) Feistel structure

b) Substitution-Permutation Network (SPN)

c) Stream cipher structure

d) Public key structure

Answer: b

13. The number of rounds in AES depends on the:
a) Block size only
b) Key size (10, 12, or 14 rounds for 128, 192, 256-bit keys)
c) Plain text length
d) Mode of operation
Answer: b
14. Which step in AES involves a non-linear byte substitution using a lookup table (S-box)?
a) ShiftRows
b) SubBytes
c) MixColumns
d) AddRoundKey
Answer: b
15. The Blowfish algorithm was designed by:
a) Ron Rivest
b) Bruce Schneier
c) Whitfield Diffie
d) Rivest, Shamir, Adleman
Answer: b
16. Blowfish operates on a block size of:
a) 32 bits
b) 64 bits
c) 128 bits
d) 256 bits
Answer: b
17. Blowfish supports a variable key length ranging from:
a) 8 to 56 bytes (32 to 448 bits)
b) 16 to 32 bits
c) 56 bits fixed
d) 128 bits fixed
Answer: a
18. RC5 is a block cipher characterized mainly by its:
a) Fixed block size and fixed number of rounds only
b) Variable block size, variable key size, and variable number of rounds
c) Use of asymmetric keys

d) Use only in stream mode

Answer: b

19. RC5 was designed by:

a) Bruce Schneier

b) Ron Rivest

c) Whitfield Diffie

d) Martin Hellman

Answer: b

20. IDEA (International Data Encryption Algorithm) operates on a block size of:

a) 64 bits

b) 128 bits

c) 32 bits

d) 256 bits

Answer: a

21. IDEA uses a key size of:

a) 56 bits

b) 64 bits

c) 128 bits

d) 256 bits

Answer: c

22. IDEA performs encryption in how many rounds?

a) 8

b) 16

c) 10

d) 12

Answer: a

23. Which block cipher mode of operation encrypts each block independently of others? a) Cipher Block Chaining (CBC)

b) Electronic Code Book (ECB)

c) Cipher Feedback (CFB)

d) Output Feedback (OFB)

Answer: b

24. A major weakness of the ECB mode is that:

a) It is too slow

b) Identical plain text blocks produce identical cipher text blocks

c) It cannot encrypt large files

d) It requires asymmetric keys

Answer: b

25. In Cipher Block Chaining (CBC) mode, each plain text block is XORed with:

a) The key only

b) The previous cipher text block before encryption

c) A random number

d) The next plain text block

Answer: b

26. Which mode of operation converts a block cipher into a stream cipher by using feedback of successive cipher text segments?

a) ECB

b) CBC

c) Cipher Feedback (CFB)

d) None of the above

Answer: c

27. In Output Feedback (OFB) mode, the feedback is:

a) The cipher text

b) The output of the encryption function (independent of cipher text)

c) The plain text directly

d) The key only

Answer: b

28. Counter (CTR) mode operates by:

a) Chaining cipher text blocks together

b) Encrypting successive values of a counter and XORing with plain text

c) Using only substitution

d) Requiring a different key for each block

Answer: b

29. A stream cipher encrypts data:

a) One block of fixed size at a time

b) One bit or byte at a time

c) Only using public keys

d) Only in offline mode

Answer: b

30. Compared to block ciphers, stream ciphers are generally:

a) Slower and more complex

b) Faster and simpler in hardware

c) Used only for asymmetric encryption

d) Not used in real-time applications

Answer: b

31. RC4 is an example of a:

a) Block cipher

b) Stream cipher

c) Hash function

d) Asymmetric cipher

Answer: b

32. RC4 was designed by:

a) Bruce Schneier

b) Ron Rivest

c) Whitfield Diffie

d) Martin Hellman

Answer: b

33. RC4 generates a pseudo-random keystream that is combined with plain text using: a) AND operation

b) XOR operation

c) Multiplication

d) Modulo division only

Answer: b

34. RC4 was widely used in which of the following protocols (now considered insecure)? a) AES-GCM

b) WEP and early SSL

c) RSA-OAEP

d) Diffie-Hellman

Answer: b

Asymmetric Key Ciphers

35. Public key cryptosystems are based on the use of:

a) A single shared secret key

b) Two mathematically related keys — one public, one private

c) No keys at all

d) Three keys used together

Answer: b

36. The concept of public key cryptography was first introduced by:

a) Rivest, Shamir, and Adleman

b) Diffie and Hellman

c) Bruce Schneier

d) Claude Shannon

Answer: b

37. In a public key cryptosystem, if a message is encrypted with the receiver's public key, it can only be decrypted with the:

a) Sender's public key

b) Receiver's private key

c) Sender's private key

d) Any public key

Answer: b

38. For authentication/digital signatures, a sender encrypts with their:

a) Public key

b) Private key

c) Receiver's public key

d) Receiver's private key

Answer: b

39. The security of the RSA algorithm relies on the difficulty of:

a) Factoring large prime numbers (factoring the product of two large primes)

b) Solving linear equations

c) Reversing hash functions

d) Performing XOR operations

Answer: a

40. In RSA, the public key consists of:

a) {n, d}

b) {n, e}

c) {p, q}

d) {e, d}

Answer: b

41. In RSA, n is computed as:

a) n = p + q

b) n = p × q, where p and q are large primes

c) n = p / q

d) n = p mod q

Answer: b

42. In RSA, the private key exponent d is chosen such that:

a) $d \times e \equiv 1 \mod \varphi(n)$

b) $d = e$

c) $d \times e = n$

d) $d = n \mod e$

Answer: a

43. The encryption operation in RSA is given by:

a) $C = M \times e \mod n$

b) C = M^e mod n

c) C = M + e mod n

d) C = e^M mod n

Answer: b

44. The decryption operation in RSA is given by:

a) M = C^d mod n

b) $M = C \times d \mod n$

c) M = C + d mod n

d) M = d^C mod n

Answer: a

45. The ElGamal cryptosystem's security is based on the difficulty of solving the:

a) Integer factorization problem

b) Discrete logarithm problem

c) Knapsack problem

d) Traveling salesman problem

Answer: b

46. ElGamal encryption produces a cipher text that consists of:

a) A single value

b) A pair of values

c) Three separate keys

d) A hash digest only

Answer: b

47. Diffie-Hellman key exchange allows two parties to:

a) Encrypt messages directly

b) Establish a shared secret key over an insecure channel without prior shared secrets

c) Generate digital signatures

d) Compress data

Answer: b

48. The security of the Diffie-Hellman algorithm is based on the difficulty of computing: a) Discrete logarithms

b) Prime factors

c) Matrix inverses

d) Hash collisions

Answer: a

49. A major vulnerability of the basic Diffie-Hellman key exchange (without authentication) is its susceptibility to:

a) Brute-force attack only

b) Man-in-the-middle attack

c) Birthday attack

d) Replay attack only

Answer: b

50. The Knapsack algorithm in cryptography is based on the:

a) Discrete logarithm problem

b) Subset sum (knapsack) problem, which is NP-complete

c) Prime factorization problem

d) Graph coloring problem

Answer: b