Q1. What type of cipher is DES?

Stream cipher
Block cipher
Substitution cipher
Transposition cipher
Answer: Block cipher
Explanation: DES is a block cipher encrypting data in 64-bit blocks.

Q2. What is the block size of DES?

56 bits
64 bits
128 bits
32 bits
Answer: 64 bits
Explanation: DES processes data in 64-bit blocks.

Q3. What is the key size of DES?

56 bits
64 bits
128 bits
112 bits
Answer: 56 bits
Explanation: Although key input is 64 bits, only 56 bits are used as key.

Q4. How many rounds of processing does DES use?

8
10
16
32
Answer: 16
Explanation: DES performs 16 rounds of Feistel network processing.

Q5. DES is based on which structure?

Feistel network
Substitution-permutation network

Caesar cipher
Hill cipher
Answer: Feistel network
Explanation: DES uses a Feistel structure for encryption and decryption.

Q6. What is the function of the S-boxes in DES?
Permute the bits
Substitute bits to introduce non-linearity
Generate keys
Expand the block size
Answer: Substitute bits to introduce non-linearity
Explanation: S-boxes perform substitution to enhance security.

Q7. Which of these is NOT part of the DES round function?
Expansion permutation
Key mixing (XOR)
Substitution with S-boxes
Hashing the block
Answer: Hashing the block
Explanation: Hashing is not part of the DES round function.

Q8. What is the role of the initial permutation (IP) in DES?
Encrypt the block
Rearrange input bits for processing
Generate the key
Pad the input data
Answer: Rearrange input bits for processing
Explanation: IP rearranges bits but does not add security itself.

Q9. How is the DES key schedule generated?
By rotating key bits in each round
By hashing the key
By using a random key for each round
By permuting and selecting bits from the key

Answer: By permuting and selecting bits from the key
Explanation: Key schedule uses permutation and rotation to generate round keys.

Q10. What is the length of each subkey used in DES rounds?
48 bits
56 bits
64 bits
32 bits
Answer: 48 bits
Explanation: Each round uses a 48-bit subkey derived from the main key.

Q11. Which mode is commonly used with DES for encrypting multiple blocks?
ECB
CBC
CFB
All of the above
Answer: All of the above
Explanation: DES can be used in multiple modes like ECB, CBC, CFB, etc.

Q12. What is a major weakness of DES today?
Small key size vulnerable to brute force
Too slow for modern use
Cannot encrypt binary data
Not well documented
Answer: Small key size vulnerable to brute force
Explanation: 56-bit key is now too short, vulnerable to brute-force attacks.

Q13. What does the 'E' expansion permutation do in DES?
Expands 32-bit half-block to 48 bits
Compresses 64-bit block to 32 bits
Generates keys
Permutes the ciphertext
Answer: Expands 32-bit half-block to 48 bits
Explanation: The E expansion duplicates bits to match subkey length.

Q14. How does DES achieve diffusion?
Through substitution in S-boxes
Through permutation and Feistel rounds
By XOR with the key
By compressing the data
Answer: Through permutation and Feistel rounds
Explanation: Multiple rounds and permutations spread plaintext bits across ciphertext.

Q15. What is the final permutation (FP) in DES?
It reverses the initial permutation
It generates the key
It pads the input
It adds non-linearity
Answer: It reverses the initial permutation
Explanation: FP undoes the IP to produce final ciphertext.

Q16. In DES, what is the size of the right half-block processed each round?
64 bits
32 bits
16 bits
48 bits
Answer: 32 bits
Explanation: DES splits 64-bit blocks into two 32-bit halves.

Q17. What cryptanalytic method was famously used to break DES?
Differential cryptanalysis
Linear cryptanalysis
Brute force
All of the above
Answer: All of the above
Explanation: Various methods including brute force and differential attacks have been used.

Q18. Triple DES (3DES) increases security by:
Using three different keys to encrypt data

Doubling block size
Using a different algorithm
Compressing the key
Answer: Using three different keys to encrypt data
Explanation: 3DES applies DES encryption three times with different keys.

Q19. Why was DES replaced by AES as a standard?
AES supports larger keys and blocks
DES was too slow
AES is older
DES was too complicated
Answer: AES supports larger keys and blocks
Explanation: AES offers better security with larger key sizes and block sizes.

Q20. Which organization originally developed DES?
NSA
NIST
IBM
FBI
Answer: IBM
Explanation: IBM developed DES, then it was adopted as a standard by NIST.