Q1. What type of cipher is AES?
Stream cipher
Block cipher
Substitution cipher
Transposition cipher
Answer: Block cipher
Explanation: AES is a block cipher that encrypts data in fixed-size blocks.

Q2. What is the block size of AES?
128 bits
192 bits
256 bits
64 bits
Answer: 128 bits
Explanation: AES operates on 128-bit blocks regardless of key size.

Q3. Which key sizes does AES support?
128, 192, and 256 bits
56, 112, and 168 bits
64, 128, and 256 bits
32, 64, and 128 bits
Answer: 128, 192, and 256 bits
Explanation: AES supports three key sizes: 128, 192, and 256 bits.

Q4. How many rounds does AES-128 use?
10
12
14
16
Answer: 10
Explanation: AES-128 uses 10 rounds of processing.

Q5. How many rounds does AES-256 use?
10
12

14
16
Answer: 14
Explanation: AES-256 uses 14 rounds of processing.

Q6. AES is based on which mathematical structure?
Substitution-permutation network
Feistel network
Hill cipher
One-time pad
Answer: Substitution-permutation network
Explanation: AES uses a substitution-permutation network for encryption.

Q7. What is the size of the AES state?
4x4 bytes
8x8 bytes
2x2 bytes
16x16 bytes
Answer: 4x4 bytes
Explanation: AES state is a 4x4 matrix of bytes (128 bits).

Q8. Which step in AES provides diffusion?
ShiftRows
SubBytes
AddRoundKey
KeyExpansion
Answer: ShiftRows
Explanation: ShiftRows shifts bytes in rows to spread the data (diffusion).

Q9. Which AES step provides non-linearity?
SubBytes
MixColumns
AddRoundKey
ShiftRows

Answer: SubBytes
Explanation: SubBytes uses S-box substitutions introducing non-linearity.

Q10. What does the MixColumns step do?
Performs matrix multiplication to mix bytes within a column
Shifts the bytes in each row
Adds the round key
Expands the key
Answer: Performs matrix multiplication to mix bytes within a column
Explanation: MixColumns mixes the data within each column to enhance diffusion.

Q11. What is the AddRoundKey step in AES?
XORing the state with the round key
Substituting bytes with S-box
Shifting rows
Mixing columns
Answer: XORing the state with the round key
Explanation: AddRoundKey mixes the current round key by XOR operation.

Q12. How is the AES key schedule generated?
Using the Rijndael key schedule algorithm
Using a Feistel network
Randomly for each round
Using DES key schedule
Answer: Using the Rijndael key schedule algorithm
Explanation: AES uses Rijndael key schedule to derive round keys.

Q13. Which AES mode provides confidentiality without integrity?
ECB
GCM
CCM
Authenticated Encryption
Answer: ECB
Explanation: ECB mode encrypts blocks independently and is vulnerable to pattern leaks.

Q14. Which mode of AES combines encryption and authentication?
GCM (Galois/Counter Mode)
CBC
CFB
ECB
Answer: GCM (Galois/Counter Mode)
Explanation: GCM mode provides both confidentiality and data authenticity.

Q15. Why is ECB mode generally discouraged?
Because it leaks data patterns
Because it is slow
Because it requires a large key
Because it is only for streaming
Answer: Because it leaks data patterns
Explanation: ECB encrypts identical plaintext blocks to identical ciphertext blocks.

Q16. AES was selected as the standard by which organization?
NIST
NSA
FBI
IBM
Answer: NIST
Explanation: NIST selected AES as the encryption standard in 2001.

Q17. Which algorithm was AES designed to replace?
DES
Blowfish
RC4
Twofish
Answer: DES
Explanation: AES replaced DES due to DES's shorter key size and vulnerabilities.

Q18. How does AES resist differential and linear cryptanalysis?
Through multiple rounds of substitution and permutation
By using very large keys

By hashing the plaintext
By compressing data
Answer: Through multiple rounds of substitution and permutation
Explanation: The design of AES provides strong resistance to such attacks.

Q19. What is the minimum recommended key size for AES to be secure today?
128 bits
56 bits
64 bits
256 bits
Answer: 128 bits
Explanation: AES-128 is currently considered secure, though 256-bit is preferred for extra security.

Q20. In AES, which operation is applied last in each round except the final?
MixColumns
AddRoundKey
SubBytes
ShiftRows
Answer: AddRoundKey
Explanation: AddRoundKey is the last step in each round to combine data with the round key.