1.Which classical cryptographic technique involves replacing each plaintext character with another character?
a) Substitution
b) Transposition
c) Symmetric key cryptography
d) Asymmetric key cryptography

View answer
Answer: a) Substitution
Explanation: Substitution involves replacing each plaintext character with another character according to a predetermined key or rule.

2.What is the primary goal of transposition in classical cryptography?
a) Replacing characters with others
b) Rearranging the order of characters
c) Encrypting data with multiple keys
d) Increasing the key size

View answer
Answer: b) Rearranging the order of characters
Explanation: Transposition involves rearranging the order of characters in the plaintext to create the ciphertext.

3.Which classical cryptographic attack involves analyzing the frequency of characters to decrypt a message?
a) Linear cryptanalysis
b) Differential cryptanalysis

c) Frequency analysis
d) Brute force attack

View answer
Answer: c) Frequency analysis
Explanation: Frequency analysis is a classical cryptanalysis technique where the frequency of characters in the ciphertext is analyzed to identify patterns and decrypt the message.

4.Which symmetric key encryption algorithm was widely used in the past but is now considered insecure due to its short key length?
a) DES
b) AES
c) 3DES
d) RSA

View answer
Answer: a) DES
Explanation: DES (Data Encryption Standard) was widely used in the past but is now considered insecure due to its short key length.

5.Which of the following is NOT a mode of operation in symmetric key cryptography?
a) ECB
b) CBC
c) RSA
d) CTR

View answer

Answer: c) RSA
Explanation: RSA is an asymmetric key algorithm, not a mode of operation in symmetric key cryptography.

6.In which mode of operation does each block of plaintext get XORed with the previous block of ciphertext before encryption?
a) ECB
b) CBC
c) CTR
d) OFB

View answer
Answer: b) CBC
Explanation: In CBC (Cipher Block Chaining) mode, each block of plaintext is XORed with the previous block of ciphertext before encryption.

7.Which cryptanalysis technique relies on analyzing the correlation between the bits of plaintext, ciphertext, and the encryption key?
a) Linear cryptanalysis
b) Differential cryptanalysis
c) Frequency analysis
d) Brute force attack

View answer
Answer: b) Differential cryptanalysis
Explanation: Differential cryptanalysis relies on analyzing the correlation between the bits of plaintext, ciphertext, and the encryption key to break the cipher.

8.Which symmetric key encryption algorithm uses a Feistel network structure?
a) AES
b) DES
c) 3DES
d) Blowfish

View answer
Answer: c) 3DES
Explanation: 3DES (Triple Data Encryption Standard) uses a Feistel network structure to encrypt data.

9.Which mode of operation is vulnerable to a padding oracle attack?
a) ECB
b) CBC
c) CTR
d) OFB

View answer
Answer: b) CBC
Explanation: CBC (Cipher Block Chaining) mode is vulnerable to a padding oracle attack.

10.Which symmetric key encryption algorithm is known for its flexibility in supporting key sizes and block sizes?
a) AES
b) DES
c) 3DES
d) Blowfish

View answer
Answer: d) Blowfish
Explanation: Blowfish is known for its flexibility in supporting key sizes and block sizes.

11.What is the primary disadvantage of using the ECB mode of operation?
a) It requires a large initialization vector (IV).
b) It does not provide confidentiality for identical plaintext blocks.
c) It is vulnerable to padding oracle attacks.
d) It is slower compared to other modes.

View answer
Answer: b) It does not provide confidentiality for identical plaintext blocks.
Explanation: ECB (Electronic Codebook) mode does not provide confidentiality for identical plaintext blocks as identical blocks of plaintext are encrypted into identical blocks of ciphertext.

12.Which cryptanalysis technique focuses on exploiting the linearity of a cipher?
a) Linear cryptanalysis
b) Differential cryptanalysis
c) Frequency analysis
d) Brute force attack

View answer
Answer: a) Linear cryptanalysis
Explanation: Linear cryptanalysis focuses on exploiting the linearity of a cipher to break it.

13.In which mode of operation does each plaintext block get encrypted separately and

independently?
a) ECB
b) CBC
c) CTR
d) OFB

View answer
Answer: a) ECB
Explanation: ECB (Electronic Codebook) mode encrypts each plaintext block separately and independently.

14.Which symmetric key encryption algorithm is commonly used for securing electronic communication over the Internet?
a) AES
b) DES
c) 3DES
d) Blowfish

View answer
Answer: a) AES
Explanation: AES (Advanced Encryption Standard) is commonly used for securing electronic communication over the Internet.

15.Which mode of operation is primarily used for full disk encryption and random access data?
a) ECB
b) CBC

c) CTR
d) OFB

View answer
Answer: c) CTR
Explanation: CTR (Counter) mode is primarily used for full disk encryption and random access data.

16.Which cryptanalysis technique involves observing the changes in the ciphertext when the plaintext is slightly altered?
a) Linear cryptanalysis
b) Differential cryptanalysis
c) Frequency analysis
d) Brute force attack

View answer
Answer: b) Differential cryptanalysis
Explanation: Differential cryptanalysis involves observing the changes in the ciphertext when the plaintext is slightly altered to break the cipher.

17.Which symmetric key encryption algorithm is also known as Rijndael?
a) DES
b) AES
c) 3DES
d) Blowfish

View answer

Answer: b) AES
Explanation: AES (Advanced Encryption Standard) is also known as Rijndael.

18.Which mode of operation XORs the plaintext with a random value generated for each block before encryption?
a) ECB
b) CBC
c) CTR
d) OFB

View answer
Answer: d) OFB
Explanation: OFB (Output Feedback) mode XORs the plaintext with a random value generated for each block before encryption.

19.Which symmetric key encryption algorithm is a variant of DES that uses three rounds of encryption for increased security?
a) DES
b) AES
c) 3DES
d) Blowfish

View answer
Answer: c) 3DES
Explanation: 3DES (Triple Data Encryption Standard) is a variant of DES that uses three rounds of encryption for increased security.

20.Which mode of operation is recommended for its parallelizability and resistance to timing attacks?
a) ECB
b) CBC
c) CTR
d) OFB

View answer
Answer: c) CTR
Explanation: CTR (Counter) mode is recommended for its parallelizability and resistance to timing attacks.

Related posts:

1. Introduction to Information Security
2. Introduction to Information Security MCQ
3. Introduction to Information Security MCQ
4. Asymmetric Key Cryptography MCQ
5. Authentication & Integrity MCQ
6. E-mail, IP and Web Security MCQ