Here are **20 multiple-choice questions based on Chapter 1: Overview** PowerPoint:

Cryptographic Algorithms & Security Concepts

1. Which of the following is NOT a main category of cryptographic algorithms?
   a) Symmetric encryption
   b) Asymmetric encryption
   c) Hash functions
   d) Compression algorithms
2. What is the primary goal of cryptographic hash functions?
   a) Encrypt messages for secure transmission
   b) Ensure data confidentiality
   c) Create a fixed-size representation of data for integrity verification
   d) Generate encryption keys
3. Which concept is NOT part of the CIA triad?
   a) Confidentiality
   b) Integrity
   c) Availability
   d) Authentication
4. What is the purpose of a message authentication code (MAC)?
   a) Encrypt messages using public key cryptography
   b) Authenticate the sender and verify message integrity
   c) Generate digital signatures
   d) Ensure high availability of a system

Network & Computer Security

5. Computer security primarily aims to protect against:
   a) Network congestion
   b) Malicious software and unauthorized access
   c) Hardware failures
   d) Power outages
6. What is a characteristic of network security?
   a) It focuses solely on preventing unauthorized access to a system
   b) It involves protecting data in transit over a network
   c) It only applies to local area networks (LANs)
   d) It is only necessary for large enterprises
7. Which standardization organization is responsible for developing Internet security standards?
   a) NIST
   b) ISO
   c) ITU-T
   d) ISOC
8. The role of NIST in cybersecurity includes:
   a) Defining security regulations for military use only
   b) Developing cryptographic standards and best practices

c) Enforcing security laws worldwide
d) Managing network infrastructure

Security Attacks & Threats

9. Which of the following is a passive attack?
a) Masquerading
b) Denial of service (DoS)
c) Eavesdropping
d) Message modification
10. A replay attack involves:
a) Capturing and resending valid messages to deceive a recipient
b) Intercepting and modifying data before delivery
c) Encrypting messages using outdated algorithms
d) Deleting important log files
11. What is an example of an active attack?
a) Traffic analysis
b) Eavesdropping
c) Modification of messages
d) Release of message contents
12. Which security mechanism focuses on detecting and recovering from attacks?
a) Passive attack prevention
b) Active attack prevention
c) Active attack detection and recovery
d) Cryptographic hashing

Security Mechanisms & Models

13. Which security service ensures that actions taken by an entity can be traced back to them?
a) Confidentiality
b) Integrity
c) Availability
d) Accountability
14. The OSI Security Architecture (X.800) includes which three main security aspects?
a) Security attack, security mechanism, security service
b) Security framework, security policy, security infrastructure
c) Threat modeling, risk assessment, mitigation strategies
d) Data confidentiality, data integrity, data availability
15. Which security mechanism is used to prevent unauthorized use of a resource?
a) Authentication
b) Access control
c) Digital signatures
d) Traffic analysis
16. What is the primary function of a digital signature?
a) Encrypt a message for confidentiality

b) Provide authenticity and integrity for digital messages
c) Generate encryption keys for secure communication
d) Prevent denial-of-service attacks

Levels of Security Impact & Protection

17. A loss of integrity in a hospital's patient database could result in:
    a) Unauthorized access to patient records
    b) Incorrect medical information leading to serious harm
    c) Slower network performance
    d) Difficulty in patient scheduling
18. According to FIPS PUB 199, a **high impact** security breach could:
    a) Cause minor financial loss
    b) Result in major damage and life-threatening injuries
    c) Lead to a temporary degradation of service
    d) Have no noticeable effect on system operations
19. Which level of impact describes a breach that has a **limited adverse effect** on an organization?
    a) Low
    b) Moderate
    c) High
    d) Severe
20. What is the best way to mitigate passive attacks?
    a) Implement real-time monitoring systems
    b) Focus on prevention methods such as strong encryption
    c) Use intrusion detection systems
    d) Deploy firewall solutions

Answers:

Cryptographic Algorithms & Security Concepts

1. **(d)** Compression algorithms
2. **(c)** Create a fixed-size representation of data for integrity verification
3. **(d)** Authentication
4. **(b)** Authenticate the sender and verify message integrity

Network & Computer Security

5. **(b)** Malicious software and unauthorized access
6. **(b)** It involves protecting data in transit over a network
7. **(d)** ISOC
8. **(b)** Developing cryptographic standards and best practices

Security Attacks & Threats

9. **(c)** Eavesdropping
10. **(a)** Capturing and resending valid messages to deceive a recipient
11. **(c)** Modification of messages
12. **(c)** Active attack detection and recovery

Security Mechanisms & Models

13. **(d)** Accountability
14. **(a)** Security attack, security mechanism, security service
15. **(b)** Access control
16. **(b)** Provide authenticity and integrity for digital messages

Levels of Security Impact & Protection

17. **(b)** Incorrect medical information leading to serious harm
18. **(b)** Result in major damage and life-threatening injuries
19. **(a)** Low
20. **(b)** Focus on prevention methods such as strong encryption

---

Here are **20 multiple-choice questions (MCQs)** based on **Chapter 2: Classical Encryption Techniques** PowerPoint.

1. What is the main weakness of the Caesar Cipher?

A) It uses multiple keys
B) It shifts letters by a fixed number, making it predictable
C) It is too complex to break
D) It requires a one-time pad

2. Which cipher replaces each letter with another letter based on a fixed shift?

A) Vigenère Cipher
B) Monoalphabetic Cipher
C) Caesar Cipher
D) Rail Fence Cipher

3. What is the key space size for a standard Caesar Cipher?

A) 10
B) 25
C) 50
D) 100

4. Which cipher uses a single alphabetic substitution but with a complex key mapping?

A) Playfair Cipher
B) Monoalphabetic Cipher
C) Columnar Transposition
D) Polyalphabetic Cipher

5. Which of these is NOT a classical encryption technique?

A) Transposition Cipher
B) Substitution Cipher
C) RSA Cipher
D) Caesar Cipher

6. What is the main difference between transposition and substitution ciphers?

A) Transposition changes letter order, substitution changes letters themselves
B) Transposition is unbreakable, substitution is not
C) Substitution is used in modern cryptography
D) They are the same thing

7. Which cipher arranges text in a zigzag pattern?

A) Columnar Transposition
B) Rail Fence Cipher
C) Caesar Cipher
D) Playfair Cipher

8. In a Rail Fence Cipher with 3 rails, how is "HELLO WORLD" written?

A) HOL ELWR OD
B) HLOOL ELWRD
C) HELLO WORLD
D) None of the above

9. The Playfair Cipher encrypts text using which technique?

A) A single shift pattern
B) A 5x5 matrix of letters
C) A set of prime numbers
D) A binary system

10. What is the key requirement for using the Playfair Cipher?

A) A numeric key
B) A keyword with no repeating letters
C) A public-private key pair
D) A shift value

11. In a Columnar Transposition Cipher, how is text arranged?

A) In a grid based on a keyword
B) In a 5x5 square
C) Using frequency analysis
D) By shifting letters

12. What happens if the message length does not fit the column size in a Columnar Transposition Cipher?

A) The message is shortened
B) Extra letters (padding) are added
C) The message is ignored
D) Encryption fails

13. What is a major weakness of Monoalphabetic Ciphers?

A) Easily broken with frequency analysis
B) Requires a computer to decrypt
C) Uses an unpredictable key
D) Takes too long to encrypt

14. How does a Polyalphabetic Cipher improve security?

A) Uses multiple substitution alphabets
B) Changes the order of letters
C) Requires multiple keys
D) Uses binary numbers

15. The Vigenère Cipher is an example of which type of encryption?

A) Transposition
B) Polyalphabetic Substitution
C) Monoalphabetic Substitution
D) Symmetric Key Encryption

16. What is the primary defense of the Vigenère Cipher against frequency analysis?

A) Each letter is encrypted differently based on its position
B) It uses a single shift value
C) It requires advanced mathematics
D) It has an unbreakable key

17. Which technique was historically used in WWII encryption machines like the Enigma?

A) Monoalphabetic Cipher
B) Playfair Cipher
C) Polyalphabetic Cipher
D) Transposition Cipher

18. How do you decrypt a Columnar Transposition Cipher?

A) Reverse the order of letters
B) Rearrange letters back into their original columns
C) Shift letters backward
D) Use frequency analysis

19. What makes Playfair Cipher more secure than a simple substitution cipher?

A) It encrypts digraphs (letter pairs) instead of single letters
B) It uses a numeric key
C) It mixes substitution and transposition
D) It requires a large computer

20. Which classical encryption technique is the foundation for modern cryptography?

A) Rail Fence Cipher
B) Vigenère Cipher
C) Caesar Cipher
D) RSA Algorithm

Answers:

1. B) It shifts letters by a fixed number, making it predictable

2. C) Caesar Cipher

3. B) 25

4. B) Monoalphabetic Cipher

5. C) RSA Cipher

6. A) Transposition changes letter order, substitution changes letters themselves

7. B) Rail Fence Cipher

8. B) HLOOL ELWRD

9. B) A 5x5 matrix of letters

10. B) A keyword with no repeating letters

11. A) In a grid based on a keyword

12. B) Extra letters (padding) are added

13. A) Easily broken with frequency analysis

14. A) Uses multiple substitution alphabets

15. B) Polyalphabetic Substitution

16. A) Each letter is encrypted differently based on its position

17. C) Polyalphabetic Cipher

18. B) Rearrange letters back into their original columns

19. A) It encrypts digraphs (letter pairs) instead of single letters

20. B) Vigenère Cipher