CH-1

1. **What is security?**
   Security is keeping unauthorized entities from doing things you don't want them to do.
2. **Briefly explain security components.**
   - **Confidentiality**
     The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.
   - **Integrity**
     Data integrity
     The property that data has no been changed, destroyed, or lost in an unauthorized or accidental manner.
     System integrity
     The quality that a system has when it can perform its intended function in a unimpaired manner, free from deliberate or inadvertent unauthorized manipulation.
   - **Availability**
     The property of a system or a system resource being accessible and usable upon demand by an authorized system entity, according to performance specifications for the system.
3. **What is Vulnerability?**
   An error or weakness in the design, implementation, or operation of a system.
4. **What is attack?**
   A means of exploit some vulnerability in a system.
5. **What is Threat?**
   An adversary that is motivated and capable of exploiting a vulnerability.
6. **What is Active attack?**
   An active attack is a network exploit in which a hacker attempts to make changes to data on the target or data enroute to the target
7. **What is Passive attack?**
   The purpose is solely to gain information about the target and no data is changed on the target. Therefor, attempting to break the system solely based upon observed data.
8. **Difference between active and passive attack**

Active attack	Passive Attack
In an active attack, Modification in information takes place.	While in a passive attack, modification in the information does not take place.
Active attack in a danger to integrity as well as availability	Passive attack in a danger to confidentiality
In an active attack, attention in on prevention	While in passive attack attention in on detection
Due to active attack, the execution system is always damaged	While due to passive attack, there is no harm to the system
In an active attack, victim gets informed about the attack	While in a passive attack, victim does not get informed about the attack.
System resources can be changed	System resource are not changing
Can be easily detected	Very difficult to detect
The duration of an active attack is short	The duration of a passive attack is long
Complexity is High	Complexity is low

9. **What is security services?**
   Security service is a service which ensures adequate security of the systems or of data transfers.
10. **Categories of security services**
    - Authentication
    - Access control
    - Data confidentiality
    - Data integrity
    - Non-repudiation
    - Availability service
11. **Nonrepudiation**
    Protection against denial by one of the entities involved in a communication of having participated in the communication.
12. **Security mechanism**
    Feature designed to detect, prevent, or recover from a security attack. Security mechanism are used to implement security services.

CH-2

13. **What is a cryptosystem?**
    A crypto system is pair of algorithms that take a key and convert plaintext to ciphertext and back.
14. **What is the requirement for secure use of conventional encryption?**
    There are two requirements for secure use of conventional encryption.
    - We need a strong encryption algorithm
    - Sender and receiver must have obtained copies of the secret key in a secure fashion and must keep the key secure.
15. **Write the classification of cryptosystem.**
    By type of encryption operations used
    - Substitution
    - Transposition

    By number of keys used

    - Single-key or private
    - Two-key or public

    By the way in which plaintext is processed

    - Block
    - Stream
16. **What is cryptanalysis? write the approaches.**
    The process of attempting to discover plaintext (X) or key (K) or both is known as cryptanalysis.
    Approaches:
    1. Cryptanalytic attack
    2. Brute-force attack
17. **What is substitution technique?**
    A substitution technique is one in which the letters of plaintext are replaced by other letters or by numbers or symbols.

18. **Write some substitution technique**
    - Caesar Cipher
    - Monoalphabetic cipher
    - playfair cipher
    - hill cipher

CH-4

19. **What is transposition cipher?**
    A transposition cipher is a method of encryption where the letters or characters or a message are rearranged according to a specific rule, without altering the actual letters themselves.
    It is a form of symmetric encryption, meaning the same key used to encrypt the message is also used to decrypt it.

20. **Write some transposition cipher.**
    - Rail Fence Cipher
    - Route Cipher
    - Columnar Cipher
21. **Uses of transposition algorithms**
    - Ancient Rome
    - American Civil War
    - WWI
22. **Write the encryption process of rail fence cipher.**
    - Create a table with rows equals to key and columns equal to length of plaintext(avoid spaces)
    - Fill the table in zig-zag form
    - Read row by row
23. **Write the encryption process of rail fence cipher**
    - Create a table with rows equals to key and columns equal to length of plaintext(avoid spaces)
    - Mark the position where texts will be placed.
    - Fill the table in zig-zag form
    - Read row by row
24. **Key Generation block diagram.**