1. **Define CIA triad. Explain network security model**

The CIA triad is a fundamental concept in information security that represents three core principles: Confidentiality, Integrity, and Availability. These principles form the foundation for designing and implementing security measures to protect information assets and ensure the secure operation of systems and networks.

Confidentiality:

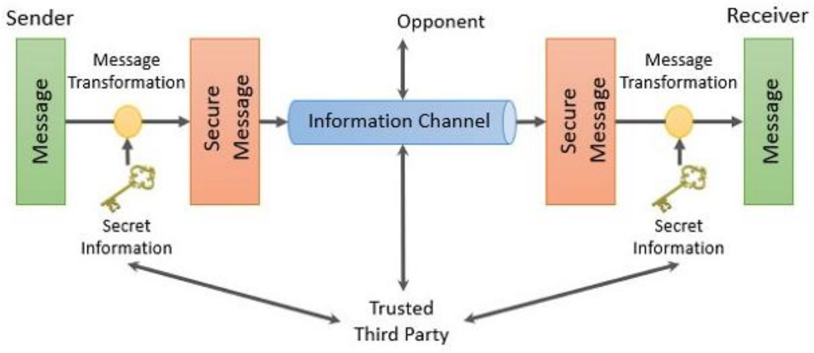
Confidentiality refers to the assurance that information is only accessible to authorized individuals, entities, or systems. It ensures that sensitive data remains private and protected from unauthorized access, disclosure, or exposure. Measures to achieve confidentiality include encryption, access controls, authentication mechanisms, data classification, and security policies that restrict access based on the principle of least privilege.

Integrity:

Integrity ensures that information remains accurate, complete, and unaltered during storage, transmission, and processing. It guards against unauthorized modification, tampering, or corruption of data. Integrity mechanisms include data validation, checksums, digital signatures, hash functions, and access controls that prevent unauthorized users from modifying or manipulating information.

Availability:

Availability ensures that information and resources are accessible and usable when needed by authorized users. It safeguards against disruptions, downtime, or denial of service (DoS) attacks that could impair or interrupt access to critical systems or data. Availability measures include redundancy, fault tolerance, disaster recovery planning, system monitoring, and network resilience to mitigate the impact of outages or attacks and ensure continuous operation.



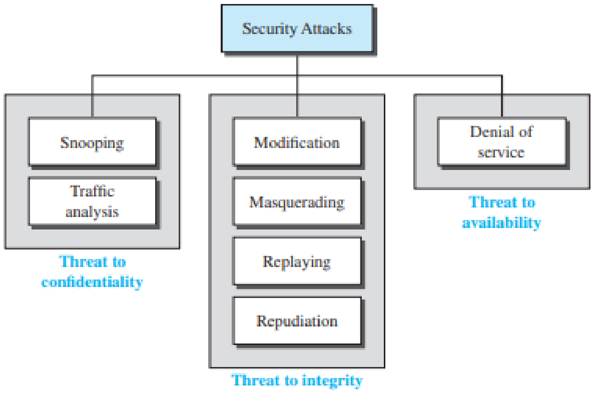
Network Security Model

1. An encryption algorithm encodes plaintext into ciphertext and decodes cypher text back into plain text. The strength of the algorithm relies on its ability to withstand cracking attempts by adversaries.
2. Secure generation, distribution and usage of a secret key exclusively shared between the communicating parties over the computer network. A trusted third party facilitates the secret key exchange in the network security model in CNS.
3. Communication protocols enable the application of the chosen encryption powered by the secretly shared key to deliver security services like confidentiality, integrity and authentication of the sender.

2. **Define network security attacks. Explain types of attacks.**

Network security attacks refer to deliberate, malicious activities aimed at compromising the confidentiality, integrity, or availability of computer networks, systems, or data. These attacks are perpetrated by individuals, groups, or automated tools with the intention of gaining unauthorized access, stealing sensitive information, disrupting services, or causing damage to network infrastructure. Network security attacks can take various forms and exploit vulnerabilities in network protocols, software applications, hardware devices, or human behavior.

Types of attacks:



Snooping: Snooping refers to unauthorized access to or interception of data. For example, a file transferred through the Internet may contain confidential information. An unauthorized entity may intercept the transmission and use the contents for her own benefit. To prevent snooping, the data can be made nonintelligible to the intercepter by using encipherment techniques, discussed later.

Traffic Analysis: Although encipherment of data may make it nonintelligible for the intercepter, they can obtain some other types of information by monitoring online traffic. For example, they can find the electronic address (such as the e-mail address) of the sender or the receiver. They can collect pairs of requests and responses to help them guess the nature of the transaction.

Modification After intercepting or accessing information, the attacker modifies the information to make it beneficial to herself. For example, a customer sends a message to a bank to initiate some transaction. The attacker intercepts the message and changes the type of transaction to benefit herself. Note that sometimes the attacker simply deletes or delays the message to harm the system or to benefit from it.

Replaying In replaying, the attacker obtains a copy of a message sent by a user and later tries to replay it. For example, a person sends a request to her bank to ask for payment to the attacker, who has done a job for her. The attacker intercepts the message and sends it again to receive another payment from the bank.

Denial of Service Denial of service (DoS) is a very common attack. It may slow down or totally interrupt the service of a system. The attacker can use several strategies to achieve this. She might send so many bogus requests to a server that the server crashes because of the heavy load. The attacker might intercept and delete a server’s response to a client, making the client believe that the server is not responding. The attacker may also intercept requests from the clients, causing the clients to send requests many times and overload the system.

3. **Define cryptography. Differentiate between symmetric and asymmetric cryptography.**

Cryptography is the science and practice of securing communication and data by converting it into a form that is unintelligible to anyone except those authorized to access it. It involves techniques for encrypting and decrypting information to protect its confidentiality, integrity, and authenticity.

Symmetric Key Encryption	**Asymmetric Key Encryption**
It only requires a single key for both encryption and decryption.	It requires two keys, a public key and a private key, one to encrypt and the other one to decrypt.
The size of cipher text is the same or smaller than the original plain text.	The size of cipher text is the same or larger than the original plain text.
The encryption process is very fast.	The encryption process is slow.
It is used when a large amount of data is required to transfer.	It is used to transfer small amounts of data.
It only provides confidentiality.	It provides confidentiality, authenticity, and non-repudiation.
The length of key used is 128 or 256 bits	The length of key used is 2048 or higher
In symmetric key encryption, resource utilization is low as compared to asymmetric key encryption.	In asymmetric key encryption, resource utilization is high.
It is efficient as it is used for handling large amount of data.	It is comparatively less efficient as it can handle a small amount of data.
Security is less as only one key is used for both encryption and decryption purpose.	It is more secure as two keys are used here- one for encryption and the other for decryption.
The Mathematical Representation is as follows- $P = D (K, E(K, P))$ where K= encryption and decryption key P= plain text D =Decryption E(K, P) =Encryption of plain text using K	The Mathematical Representation is as follows- $P = D(Kd, E (Ke,P))$ where Ke = encryption key Kd =decryption key D= Decryption E(Ke, P)= Encryption of plain text using encryption key Ke. P =plain text
Examples: 3DES, AES, DES and RC4	Examples: Diffie-Hellman, ECC, El Gamal, DSA and RSA

4. **Explain public and private key.**

Public key cryptography is a method of encrypting or signing data with two different keys and making one of the keys, the public key, available for anyone to use. The other key is known as the private key. Data encrypted with the public key can only be decrypted with the private key. Because of this use of two keys instead of one, public key cryptography is also known as asymmetric cryptography. It is widely used, especially for TLS/SSL, which makes HTTPS possible.

The private key is used in both **encryption** as well as decryption. This key is shared between the sender and receiver of the encrypted sensitive information. The private key is also called "symmetric" because it is shared by both parties. Private key cryptography is faster than public-key cryptography mechanism. A private key is generally a lengthy, non-guessable sequence of bits created randomly or pseudo-randomly. The complexity and length of a private key define how easy it is for an attacker to carry out a bruteforce attack, in which they test out several keys until they find the appropriate one.

5. **Explain working procedure of RSA algorithm for encryption and decryption.**

   The RSA algorithm is a widely used asymmetric encryption algorithm named after its inventors, Ron Rivest, Adi Shamir, and Leonard Adleman. It is based on the mathematical properties of prime numbers and modular arithmetic and is commonly used for secure communication, digital signatures, and key exchange.

   Working Procedure of RSA Algorithm for Encryption:

   1. Key Generation:
      - Choose two distinct prime numbers, p and q.
      - Compute their product, $n = p * q$, which is used as the modulus for both the public and private keys.
      - Compute Euler's totient function, $\varphi(n) = (p - 1) * (q - 1)$, which is used to generate the public and private exponents.
      - Choose a public exponent, e, that is relatively prime to $\varphi(n)$ and less than $\varphi(n)$.
      - The public key is represented by the pair (e, n), where e is the public exponent and n is the modulus.

2. Encryption:

- To encrypt a message M, which is represented as an integer between 0 and n - 1, the sender uses the recipient's public key (e, n).
- Compute the ciphertext C as C ≡ M^e (mod n), where "^" denotes exponentiation and "mod" denotes the modulus operation.
- The ciphertext C is the encrypted message that can be sent securely to the recipient.

Working Procedure of RSA Algorithm for Decryption:

1. Key Generation (continued):

- Compute the modular multiplicative inverse of the public exponent e modulo φ(n), denoted as d.
- The private key is represented by the pair (d, n), where d is the private exponent and n is the modulus.

2. Decryption:

- To decrypt the ciphertext C received from the sender, the recipient uses their private key (d, n).
- Compute the plaintext message M as M ≡ C^d (mod n), where "^" denotes exponentiation and "mod" denotes the modulus operation.
- The plaintext message M is the decrypted message that was originally sent by the sender.