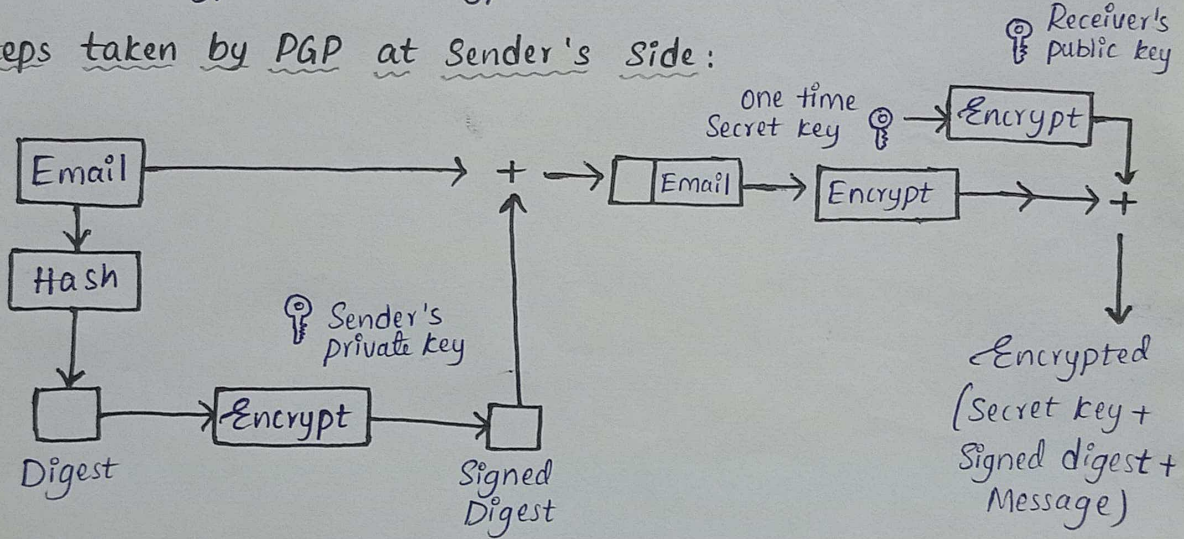
PGP:

- Pretty Good Privacy
- It was invented by phil Zimmerman in 1991
- It was designed to provide all four aspects of Security i.e., privacy, integrity, authentication and non-repudiation.
- PGP uses diffie Hellman digital Signature.
- PGP is an open source and freely available Software package for email security. But, it is not used widely because it requires time and effort to fully encrypt data files.
- PGP uses existing algorithms such as RSA, IDEA, MD5 etc., rather than inventing the new ones.
- The benifit of PGP lies in its unbreakable algorithm. Even government, nation states and hackers can't access the files that are encrypted with PGP.
- PGP is a data encryption and decryption program used for email and file encryption and decryption

Steps taken by PGP at Sender's Side:



→ The email message is hashed by using a hashing function to create a digest

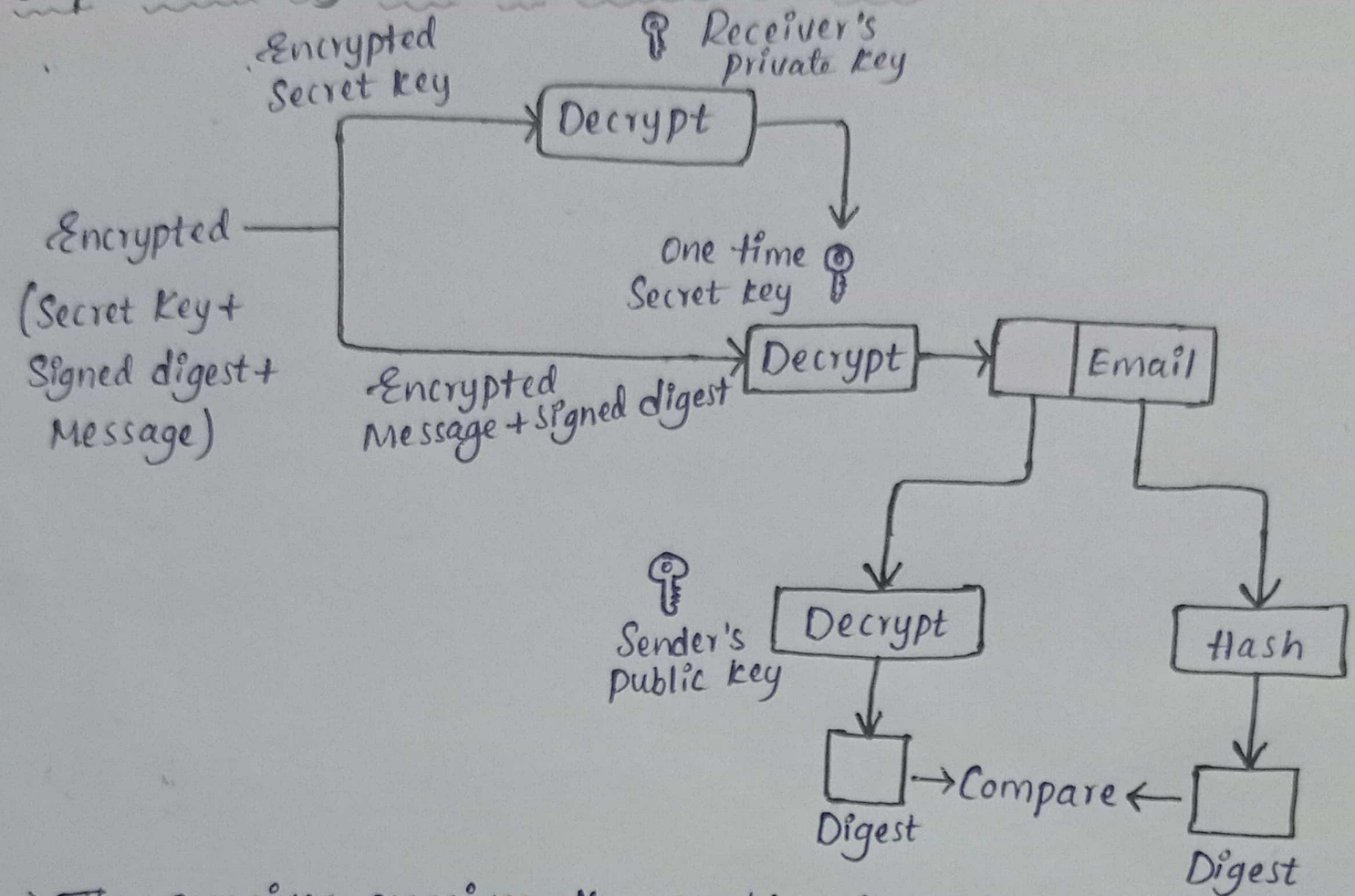
→ The digest is then encrypted to form a Signed digest by using the Sender's private key, and then Signed digest is added to the original email message.

→ The original message and Signed digest are encrypted by using a one-time Secret key created by the Sender

→ The Secret key is encrypted by using a receiver's public key

→ Both the encrypted secret key and the encrypted combination of message and Signed digest are sent together.

Steps taken by PGP at receiver's Side:



→ The receiver receives the combination of encrypted secret key, ~~and~~ message and signed digest

→ The encrypted secret key is decrypted by using the receiver's private key to get the one-time secret key.

→ The secret key is then used to decrypt the combination of message and digest

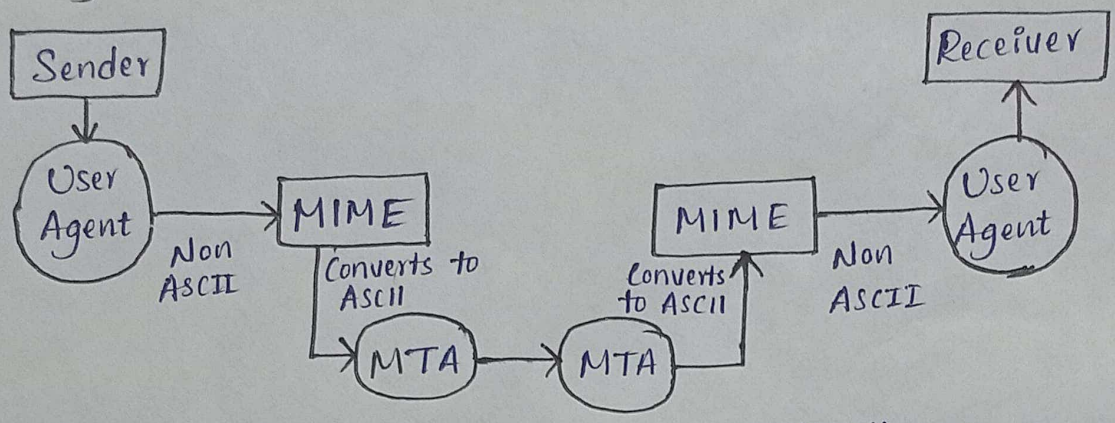
→ The digest is decrypted by using the sender's public key, and the original message is hashed by using a hash function to create a digest

→ Both the digests are compared, if both of them are equal that means all the aspects of security are preserved.

MIME :

- Multipurpose Internet Mail Extension
- It is the foundation for S/MIME
- MIME was proposed by Bell Communication in 1991
- It is used to extend the capabilities of Internet e-mail protocols such as SMTP.
- The MIME protocol allows the users to exchange various types of Non-ASCII data such as pictures, audio, video and various types of documents and files in the email.

Working of MIME :



Suppose a user want to send an email through a user Agent and it is in a Non-ASCII format so there is a MIME protocol that converts it into 7-bit NVT ASCII format. The message is transferred through the e-mail System to the other side in the 7-bit format now MIME protocol again converts it back into Non-ASCII code and now the user agent finally passes the email to the receive

MIME Header:

MIME header is added to the original email header, which contains five additional fields

(i) MIME Version : It defines the version of the MIME protocol

(ii) Content type : Type of data used in the body of the message. They are of different types like text data, audio, images or video.

(iii) Content-Type Encoding: Defines the method used for encoding the message. Like 7-bit encoding, 8-bit encoding etc.,

(iv) Content Id : It is used for uniquely identifying the message

(v) Content Description: It defines whether the body is actually an image, video or audio

S/MIME :

- Secure/Multipurpose Internet Mail Extension
- It is based on the MIME standard
- It provides security services for electronic mail.
- It is designed to provide all four aspects of security
  - → privacy
  - → Integrity
  - → Authentication
  - → Non-repudiation
- It offers two crucial functionalities :

(i) Encryption: S/MIME encrypts email content using public key cryptography. only the recipient/receiver with the corresponding private key can decrypt and access the message.

(ii) Digital Signature: S/MIME allows users to digitally sign emails. This verifies the sender's identity and ensures the message hasn't been altered during transmission.

Web security:- Web security means providing security for the data which is transmitted through the network.

Ex: client & server client sends request to the server and the server will provide service to the client. for this purpose we will use a protocol called SSL protocol.

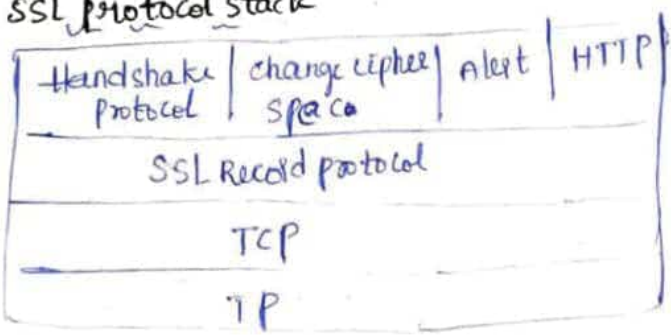
SSL (Secure socket layer)

* By this layer we will provide a security to a data which is sent over the n/w. it will provide a security for the data which is transferred b/w web browser and the server.
* SSL uses different protocols
  1) SSL Record protocol 2) Handshake protocol 3) change cipher spec protocol 4) Alert protocol

All these protocols are included in the secure socket layer. These protocols are also known as SSL protocol stack.

* Connection :- Establish a connection b/w client & server for data transfer
  Session : Association b/w client & server (time period)
  Sessions have multiple connections. All these sessions are created by Handshake protocol.
* SSL is developed by netscape communication
* SSL is a protocol for establishing secure links b/w N/w & computers
* The main purpose of SSL is to provide confidentiality, authentication and data integrity.

SSL protocol stack



* SSL mainly used for web security
* SSL mainly consists of 4 protocols.
* these protocols are stacked using SSL protocol stack.
* SSL record protocol lies above TCP & below HTTP.

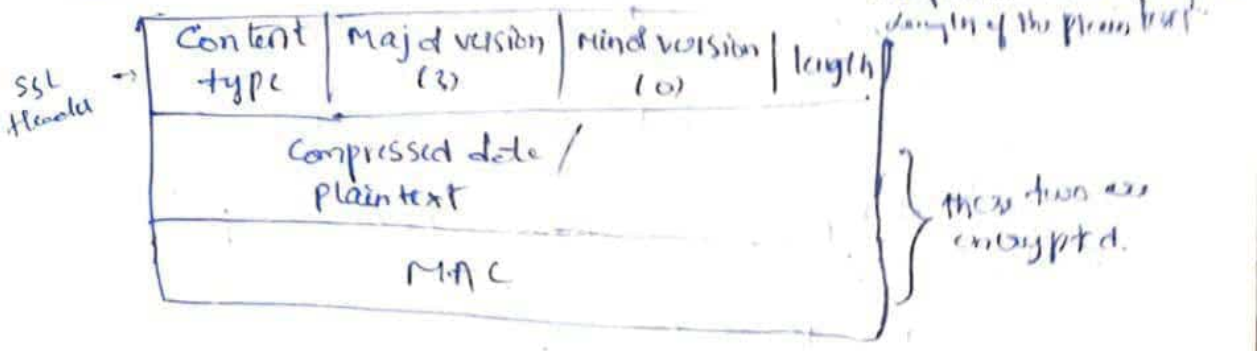
SSL Record protocol:

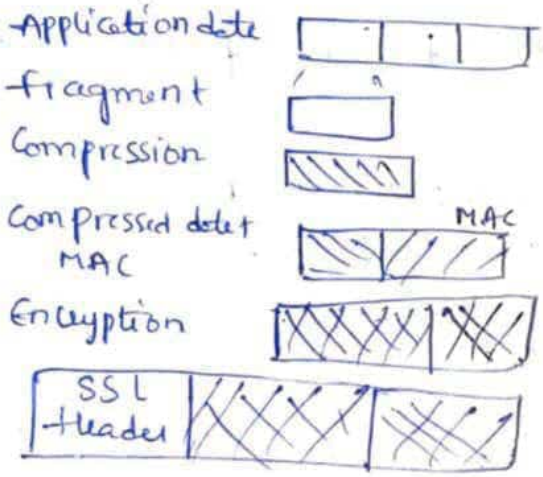
1. Application data given, divided into blocks of fragments
   Compression is optional. Apply any secure Hash Alg SHA alg or MD5 alg on this compressed frag and generate MAC. And this MAC is Appended to compressed fragment. Apply encryption technique to provide confidentiality. we have to send data from one layer to another layer (source & dest) we have to include headers.

it is known as SSL Header. SSL Header consists of 4 bytes

1. Content type 2. Major version (3) 3. Minor version (0) 4. length (if compression is performed length of the compressed data) if compression is not performed length of the plain text

↓
the higher layer which process the data.





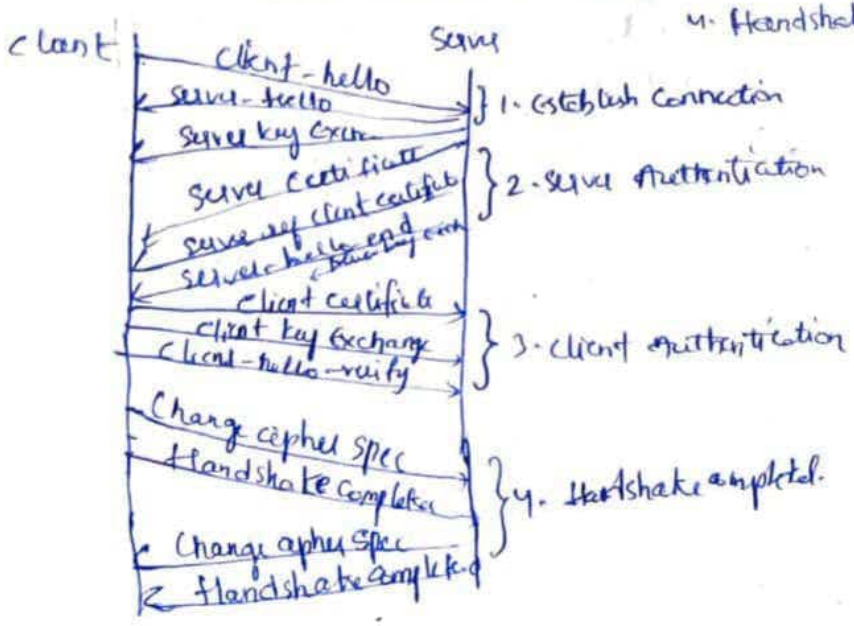
→ SSL Record protocol generates o/p the o/p is in pending state

Handshake protocol.

→ used to establish a session b/w client & server.

→ It consists of 4 phases.

1. Establish connection 2. Server authentication 3. client Authentication 4. Handshake completion.



Change cipher spec:

until the completion of Handshake protocol, the o/p of SSL record protocol is in pending state.

SSL Record → output → Pending state

Handshake completed	current state

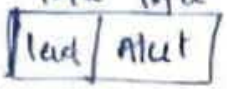
Conversion of pending state to current state is known as change cipher spec.

→ change cipher spec protocol consists of 1 byte msg.

Alert protocol:

→ Convey some msgs b/w client & server.

→ this protocol is divided into 2 fields. Each field contains 1 byte



1st field is represented as level, 2nd field is Represented as Alert

level = 1 means warning, there is no impact on the connection b/w sender & receiver

level = 2 means fatal error. ↓ means break the connection b/w sender & receiver. we cannot resume if we want to have to restart the connection.

warning msg:
1. Bad Certificate
2. No "
3. certificate expired
4. unknown certificate
5. unsupported certificate
6. certificate Revoke
7. Close notify

fatal error:
1. Handshake failure
2. Decompression failure
3. illegal parameter
4. Bad Record MAC
5. unexpected msg

* SSL Certificate is a digital certificate used to verify & secure the website.

Ipsec :-

→ the Ipsec stands for Internet protocol security.
→ It is an internet engineering task force (IETF) standard suite of protocols b/w 2 communication points, across the Ip network that provide authentication, integrity and confidentiality.
→ It can also defines the encrypted, decrypted and authenticated packets.
→ the protocols needed for security key exchange and key management are defined in it.
→ Ipsec provides data security at the Ip packet level.

Components (or) elements of Ipsec :

It has the following components (or) elements:

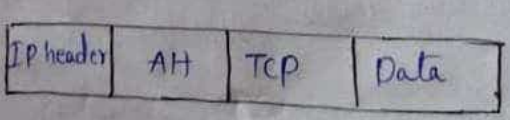
1. ESP → Encapsulating security payload
2. AH → Authentication Header
3. IkE → Internet key exchange

ESP:

It provides data integrity, encryption, authentication and anti-replay.
It can also provides authentication for payload.

AH:

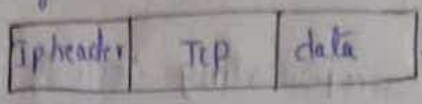
→ It can also provides data integrity, authentication, and anti-replay and it does not provide encryption.
→ It does not protect data confidentiality.

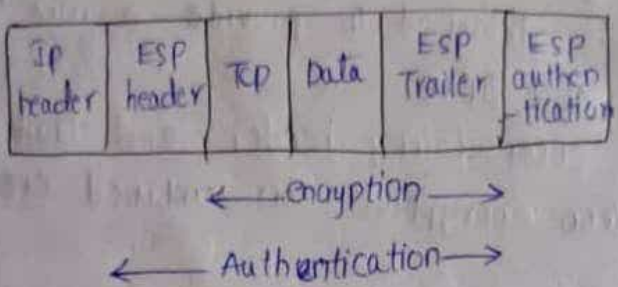


IKE:

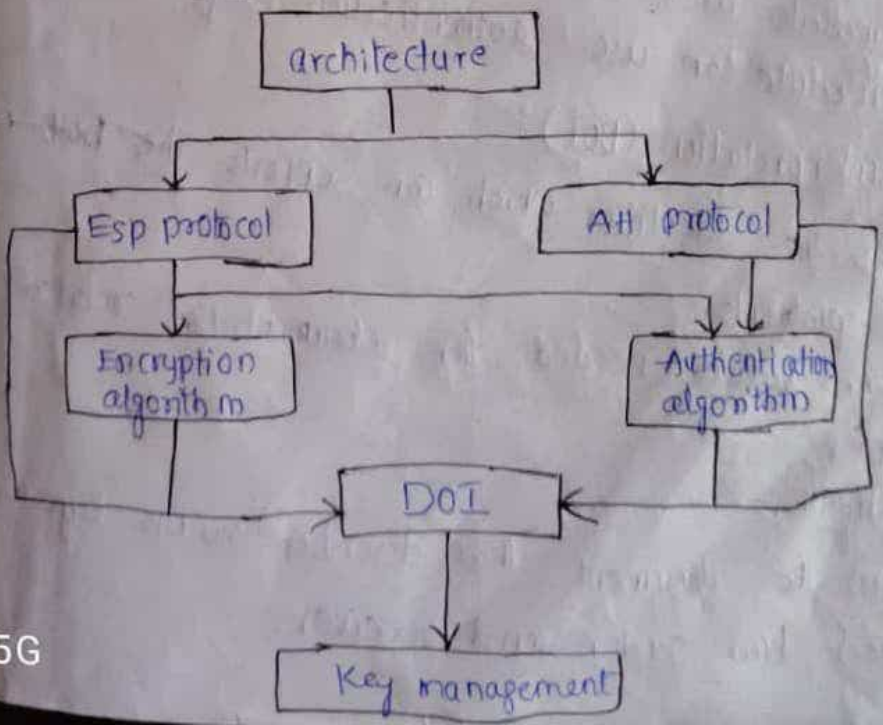
→ It is a network security protocol designed to dynamically exchange encryption keys and find a way over security association b/w 2 devices.
→ IkE provides message content protection and also an open frame for implementing standard algorithms such as

SHA and MD5.
→ It establish shared symmetric key
→ It provides key management and security association management.





Ipsec Architecture:-
→ The Ipsec architecture uses 2 protocols to secure the traffic (or) data flow.
→ these protocols are ESP (Encapsulating security payload) and AH (Authentication header).
→ The Ipsec architecture includes protocols, algorithms, DOI, and key management.
→ All these components are very important in order to provide the 3 main services.
They are: 1. Confidentiality
2. Authenticity
3. Integrity



Working :-

Esp :-

→ the Esp stands for encapsulating security payload.
→ the Esp header is designed to provide a mix of security services in IPv4 and IPV6.
→ It consists of an encapsulating header and trailer used to provide encapsulation encryption (or combined encryption/ authentication.
→ the current specification is RFC 4303.

AH :-

It stands for authentication header.
→ An extension header is to provide message authentication.
→ current specification is RFC 4302.

Encryption algorithm:

→ the Encryption algorithms encrypt data with key.
→ the Esp module in Ipsec uses encryption algorithms.

Authentication algorithms:

→ Authentication algorithms produce an integrity checksum value (or digest that is based on the data and a key.
→ the AH module uses authentication algorithms.
→ the Esp module can use authentication algorithms as well

Domain of Interpretation (DOI) :-

→ the DOI is the identifier which can supports the both AH and Esp protocols.
→ It contains values needed for documentation related to each other.

Key management :-

It contains the document that describes how the keys are exchanged b/w sender and receiver.

Applications of Ipsec :-

→ used to secure branch office connectivity over the internet.
→ Secure remote access over the internet.
→ protects a secure host on an internal n/w from unwanted n/w traffic.
→ To provide security for routers sending routing data across the public internet.
→ Provides authentication to the data users.

Advantages :-

1. It can provides strong cryptographic security services that helps to protect sensitive data and ensures n/w security privacy.
2. Flexibility :- provides security for a wide range of network topologies, including point-to-point, End-to-End, Site-to-site and remote access connections.
3. Scalability : Ipsec can be used to secure large-scale networks
4. Improved n/w performance:
It can helps improve n/w performance by reducing n/w congestion and improving n/w efficiency.

Disadvantages :-

1. Limited protection:
Ipsec only provides protection for ip traffic, and other protocols.
2. Compatability Issues:
Ipsec can have compatability issues with some n/w devices and applications.

System security:

→ The security of a computer system is a crucial task.
→ It is a process of ensuring the confidentiality and Integrity of the OS.
→ The security of a system can be threatened via 2 violations:

1. Threat
2. Attack.

1. Threat: A program that has the potential to cause serious damage to the system.

2. Attack: An attempt to break security and make unauthorized use of an asset.

→ security can be compromised via any of the following branches mentioned:

1. Breach of confidentiality → involves unauthorized reading of data
2. Breach of Integrity → involves unauthorized modification of data
3. Breach of availability → involves unauthorized destruction of data
4. Theft of service → involves unauthorized use of resources.
5. Deniel of service → involves preventing legitimate use of the system.

Security System Goal:-

Based on the above breaches, the following security goals are aimed:

1. Integrity
2. Secrecy
3. Availability

Types of threats:- divided into 2 types:

1. program threats
2. System threats

1. program threats:

1. virus
2. Trojan horse
3. logic Bomb
4. Trap door
5. Worm.

2. System threats:

1. Worm
2. port scanning
3. Denial of service.

→ The security measures can be Taken as;

1. physical
2. Human
3. operating system
4. Networking system.