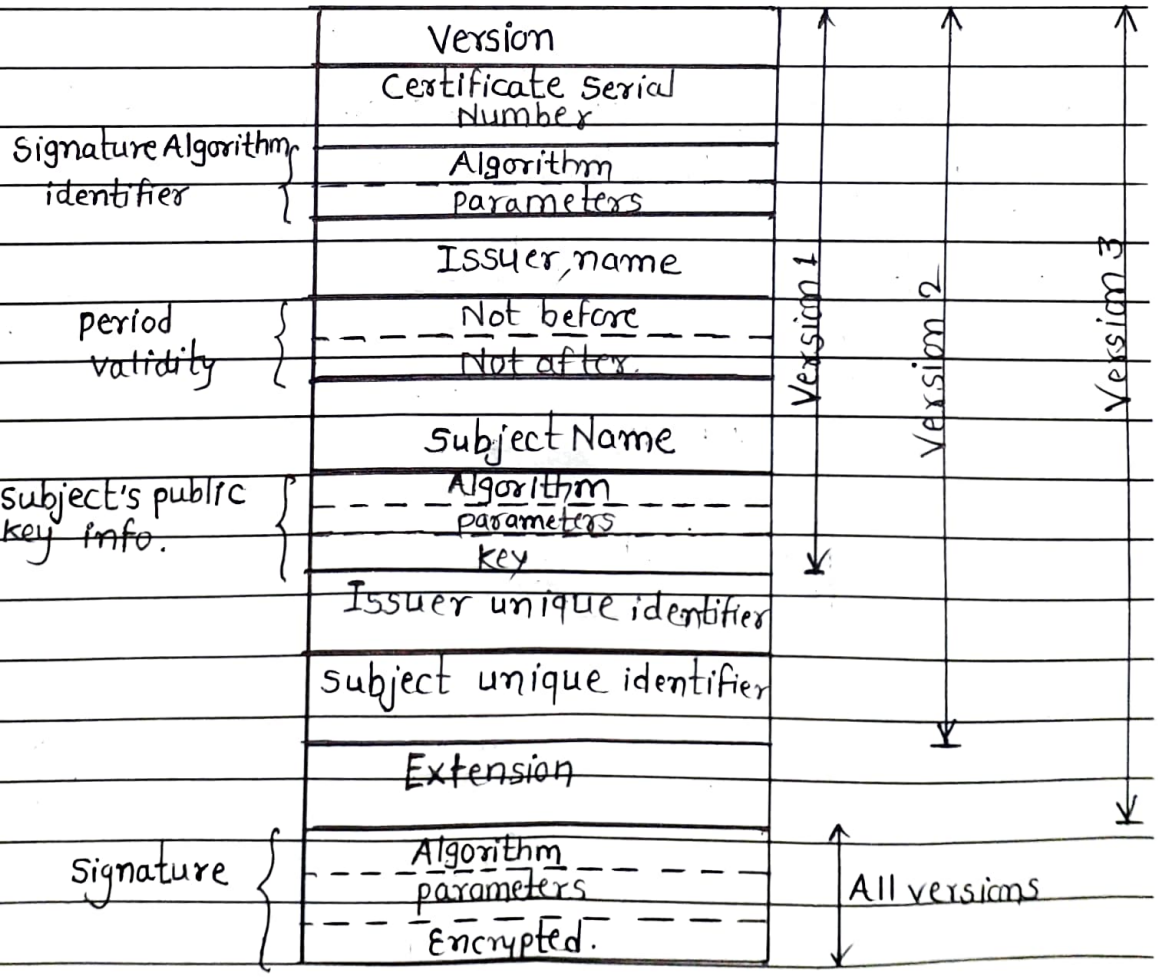
# Assignment No. 2

**Q.1** What is X.509 Directory Authentication service? Give the format of X.509 digital certificate & explain the use of digital signature in it?

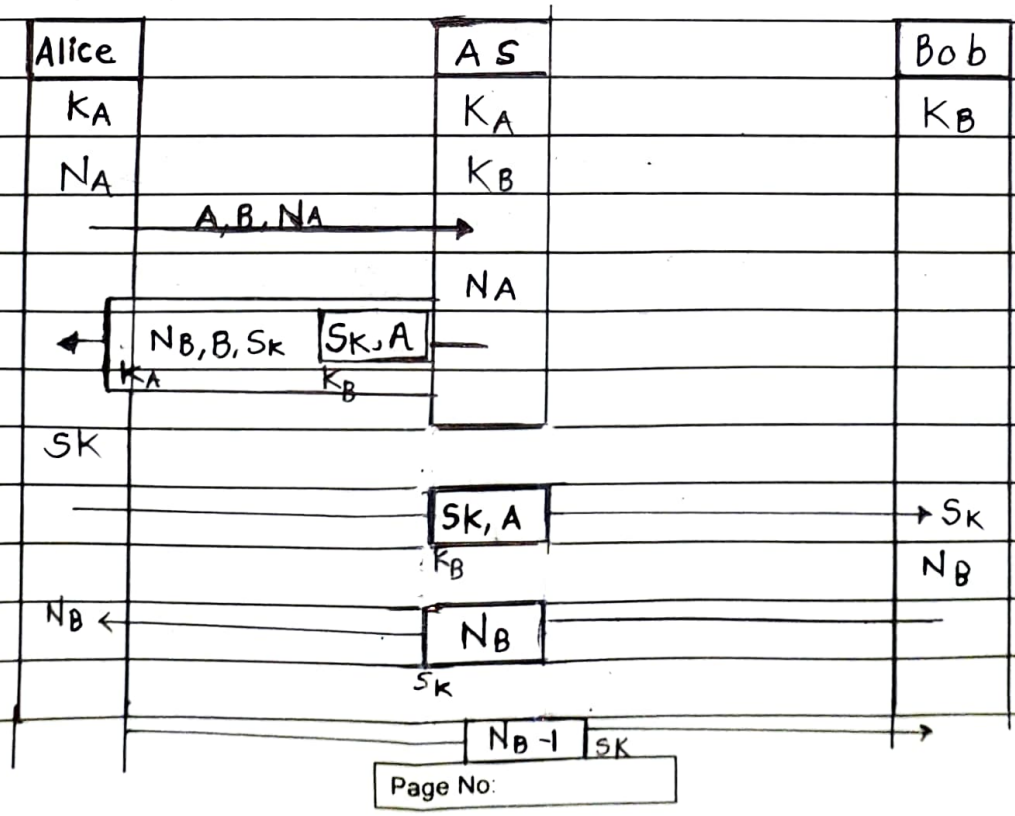
→ X.509 is a standard format for public key certificates digital documents to verify that a public key belongs to the user, computer or service identity contained within the certificate, X.509 has been adapted for internet use by the IETF's Public-key Infrastructure (X.509) (PKIX) working group.



- A public key certificate is digitally signed document that is commonly used for authentication & secure exchange of information on open networks.
- A certificate securely binds a public key to the entity that holds the corresponding private key.
- Certificates are digitally signed by the issuing certification authority (CA). They create a trust relationship between two unknown entities.
- The purpose of digital signature is to verify the "issuer of the certificate" i.e. the a third-party will be using the subject's public-key provided the digital certificate is issued & signed by a Trusted authority.

Q.2 Explain Symmetric key Management authentication protocols - Needham Shroedar Protocols ?

→



The Needham-Schroeder public-key protocol is based on public-key cryptography. This protocol is intended to provide mutual authentication between two parties.

- Suppose Alice (A) initiates the communication to Bob (B). S is a server (KDC) trusted by both parties in the communication.
- $K_{AS}$ is a symmetric key known to only A & S
- $K_{BS}$ is a symmetric key known only to B & S.
- $N_A$ & $N_B$ are nonces generated by A & B resp.
- $K_{AB}$ is a symmetric, generated key, which will be the session key of the session between A & B.
- The protocol can be specified as follows in security protocol notation :-

i) $A \rightarrow S : A, B, N_A$

Alice sends a message to the server identifying herself & Bob, telling the server that she wants to communicate with Bob.

ii) $S \rightarrow A \{ N_A, K_{AB}, B \{ K_{AB}, A \} K_{BS} \} K_{AS}$

The server generates the session key, $K_{AB}$ & sends back to Alice a copy encrypted under $K_{BS}$ for Alice to forward to Bob & also a copy for Alice.

iii) $A \longrightarrow B \{K_{AB}, A\} K_{BS}$

Alice forwards the key to Bob who can decrypt it with the key he shares with the server, thus authenticating the data.

iv) $B \longrightarrow A \{N_B\} K_{AB}$

Bob sends Alice a nonce encrypted under $K_{AB}$ to show that he has the key.

v) $A \longrightarrow B : \{N_B - 1\} K_{AB}$

Alice performs a simple operation on the nonce re-encrypt it & send it back verifying that she is still alive & that she holds the key.

Q.3 Explain PKI.

→ Public Key Infrastructure (PKI) is the framework of encryption & cyber security that protects communication between the server & the client.

**PKI Architecture :-**

The PKI Architecture components are grouped into the following broad functional catagories.

Experiment No. Date :

<table>
<tr><td colspan="3">[Applications]</td></tr>
<tr><td rowspan="4">System security Enabling Services.</td><td>Secure Protocols</td><td>Security Policy Services</td></tr>
<tr><td>Protocol security services</td><td></td></tr>
<tr><td>Long-Term Key Services</td><td>Supporting services.</td></tr>
<tr><td>Cryptographic Services</td><td></td></tr>
<tr><td></td><td>Cryptographic Primitives</td><td></td></tr>
</table>

- **System-security Enabling Services :-**
  Allows a user's or other principal's identity to be established & associated with their actions in the system.

- **Cryptographic primitives :-**
  Provide a cryptographic functions on which public-key security is based.

- **Long-term key services :-**
  To manage their own long-term keys & certificates & to receive & check the validity of other principal's certificates.

- **Protocol security services :-**
  Provide security functionality suitable for use by implementation of security-aware

applications, such as secure protocols.

- **Secure Protocols :-**

These provide secure interapplication communication for security-unaware & "mildly" secure-aware applications.

- **Security Policy services :-**

Provide the policy-related information which must be carried in secure protocols to enable access control.

- **Supporting services :**

Provide functionality in which is required for secure operation, but not directly involved in security policy enforcement.

Q.4 Explain Kerberos.

→ Kerberos is a computer network security protocol that authenticates the services requests between two or more trusted users across the internet.

It uses secret-key-cryptography and a trusted third party (KDC) for authenticating client server applications & verifying user's identities.

The main components of Kerberos are :-

- **Authentication server (AS) :-**

The AS performs the initial authentication & ticket for Ticket Granting service.

- **TGS (Ticket Granting Server) :-**

The TGS is an application server that issues the ticket for the server.

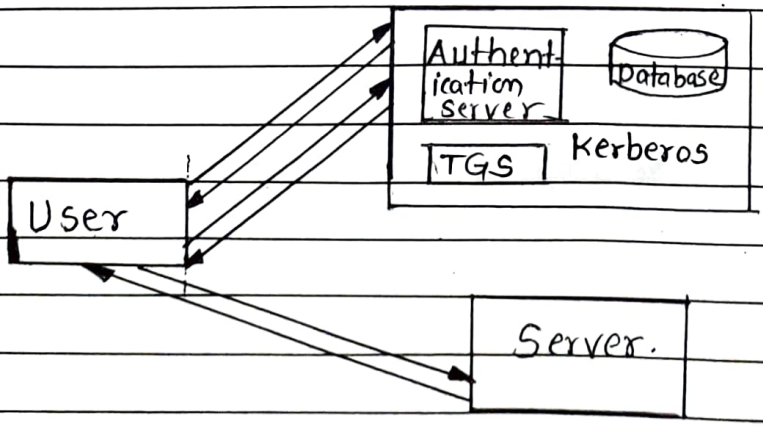
- **Client :-**

The client initiates the communication for a service request.

- **server :-**

The server host the service which the user wants to access.

Overview of kerberos :-



• Step 1 :-

User login & request services on the host. Thus user requests for ticket-granting service.

• Step 2 :-

AS verifies user's access right using database & then gives ticket-granting-ticket & session key.

• Step 3 :-

The decryption of the message is done using the password then & send the ticket to the TGS.

• Step 4 :

The TGS decrypts the ticket sent by User & authenticator verifies the request then creates the ticket for requesting services from the server.

• Step 5 :-

The User sends the Ticket & Authenticator to the server.

• Step 6 :- The server verifies the ticket & ~~Ti~~ authenticators then generate access to the service.

Q.5 Explain Cryptographic Hash Functions ? Applications of

→ There are many applications of hashing, including modern day cryptography hash functions some of these applications are listed below.

• Message digest :-

Cryptographic hash functions are the functions which produce an output from which reaching the input is close to impossible.

• Password Verification :-

Cryptographic hash functions are very commonly used in password verification. for eg. You enter your email & password to authenticate that the account you are trying to use belongs to you.

• Digital Signature :-

Another important application which is similar to the message authentication application is the digital signature.
The operation of the digital signature is similar to MAC.

• Other Applications :-

- Hash functions are commonly used to create a one-way password file.
- Hash functions can be used for intrusion detection & virus detection.
- A cryptographic hash function can be used to construct

a pseudorandom function (PRF) or a PRNG.

6. Explain SHA-512 with neat schematic diagrams?

→ It takes an input message of a minimum length less than $2^{64}$ bits & produced an output of 160 bit message digest.

- The processing of SHA is much similar to MD5.

1> Append Padding bits :-

- Padding means addition of bits to the original message
- To make length of original message to a value 64 bits less than multiple of 512.
- The message is padded to make the length of message 448 mod 512.
- The padding message consists of a single 1-bit, followed by many 0 bits as required.
- The length of padding bits is between 1 to 512.

2> Append length :-

- A block of 64 bits is appended to a message. 64 bits of original message is appended to the result of above step 1. (original message + padding)

3) Initialize MD buffer :-

- A 160-bit buffer is used to store the intermediate as well as the final result.
- The buffer is represented as five 32-bit registers as P, Q, R, S, T as

P = 67452301
Q = FFCDAB89
R = 98BADCEF
S = 10325476
T = C3D2E1E0.

- It uses a big endian method, first four registers are same as MD5. These five registers P, Q, R, S, T are requested as

P = 67 45 32 01
Q = EF CD AB 89
R = 98 BA DC FE
S = 10 23 54 96
T = C3 D2 F1 F0.

4) Process message in 512 bits (32 bits 16 words) block :-

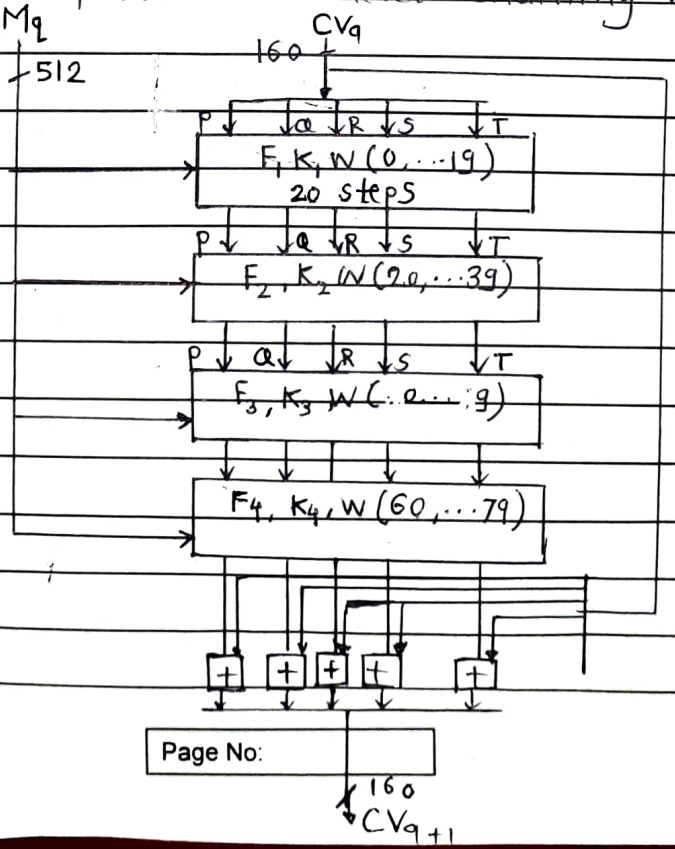
- It consists of four rounds of 20 steps each as shown in fig.
- These rounds referred as F1, F2, F3, F4 have similar structure.

- Each round takes input 512 bit block, processds it & produce 160 bit output.
- The output of the fourth round is added to the first round $CV_q$ to produce $CV_{q+1}$.
- Each round also uses an additive constant K1.

K1 = 5A 82 79 99
K2 = 6E AB 86 93
K3 = A6 32 BC C1
K4 = EF GH AB CD

(5) Output :-

- After process all 512 bit blocks, the 160 bit message digest is produced as an output.
- The SHA compression function uses a feed forward operation where the chaining variable $CV_q$ input of the first round is added to the output obtained after execution of 80 steps to produce the next chaining variable $CV_{q+1}$



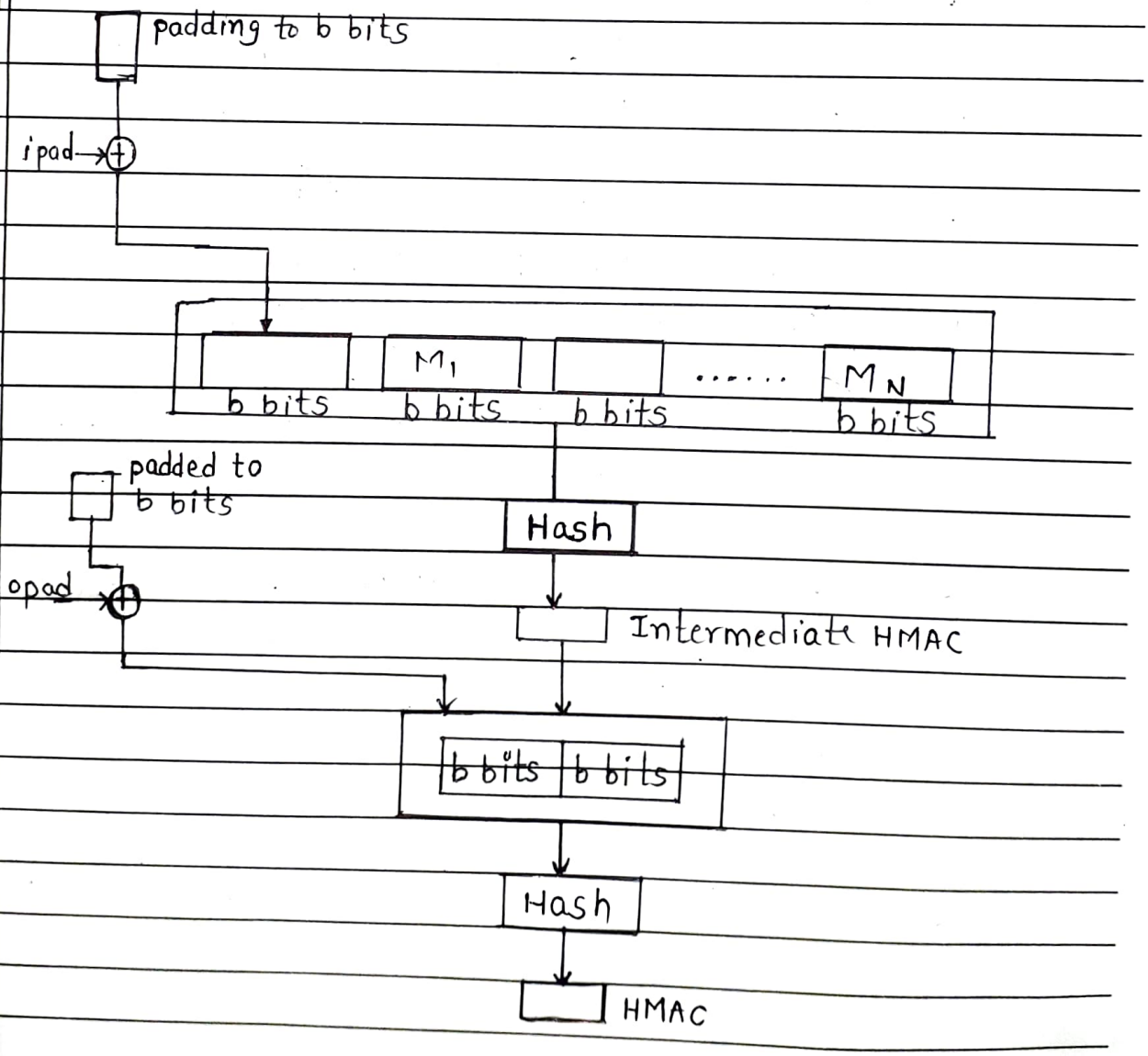

Page No:

Q.7 Explain HMAC.

→ A Hash-based Message Authentication Code (HMAC) is a nested MAC to include cryptographic is a hash function and a secret key in derieving the message authentication code.

- Typically, MD5, SHA-1 or SHA-256 cryptographic hash functions are used to calculate the HMAC value.

Working :-



Step 1:-

The message is divided in N block. Each block is of b bits.

Step 2:

To match the key length with size of every block. the secret-key is left padded with 0's to create b bit key

step 3:-

The result of previous step is X-ORed with input pad (ipad) to create b-bit block.

step 4:-

The resulting block is prepended to the N-block Message. Now, we have N+1 blocks.

step 5:- The result of the previous step is applied to hashing algorithm to create n-bit digest

Step 6: The inter-mediate HMAC is left padded with 0's to create b bit block.

step 7: steps 2 & 3 are now repeated but with new constants, output pad (opad).

step 8:- The resulting block is prepended to the block of step 6.

Step 9 :- The result of step 8 is applied to same hashing algorithm to create final n-bit HMAC.

Q.8 What are requirements of Message Authentication Code (MAC) & functions ?

→ A message authentication code (MAC) is a cryptographic checksum on data that uses a session key to detect both accidental & intentional modifications of the data.

A MAC requires two inputs : a message & a secret key known only to the originator of the message and it intended recipient (s). This allows the recipient of the message to verify the integrity of the message and authenticate that the messages sender has shared secret key. If a sender doesn't know the secret key the hash value would then be different, which would tell the recipient that the message was not from the original sender.

• Functions :-

- It is used to establish the authenticity & hence, the integrity of the message.
- It is used to confirm that the message came from the stated user/sender not from impaster and has not been changed.

Q.9 What is Digital signature ?

→ A digital signature is a mathematical technique used to validate the authenticity & integrity of a message, software or digital document. It allows us to verify the author name, date & time of signature & authenticate the message contents.

∴ Digital signatures are created & verified by using public key / asymmetric key cryptography.

Q.10 Explain various Digital signature schemas ?

→

1) RSA Digital Signature scheme.

The concept of RSA is also used for signing & verifying a message which is called as RSA digital signature scheme.

Key generation :-

Key generation in RSA digital signature scheme is exactly same as key generation in RSA cryptosystem.

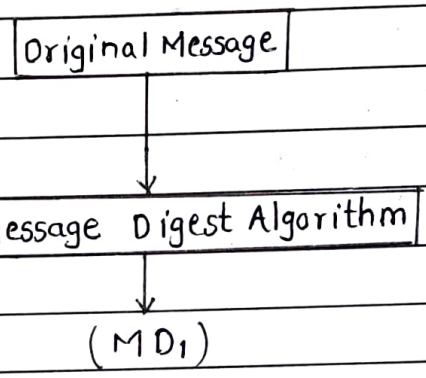
$$n = p * q$$

$$\phi(n) = (p-1)(q-1)$$

The sender calculate totient function $\phi(n)$. He then selects an encryption key e, publicly announces (n, e) & calculates the decryption key d such that $d = e^{-1} \bmod (\phi(n))$

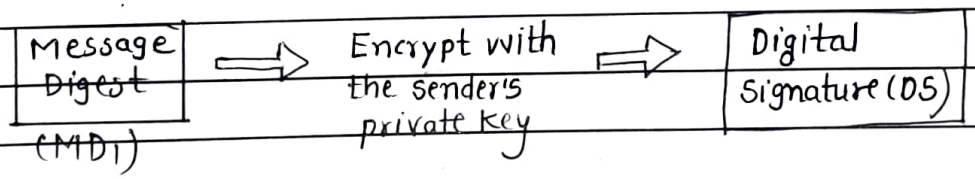
Working :-

▶ Step 1 :-




The sender uses the message digest algorithm to calculate the message digest (MD1) over the original message.

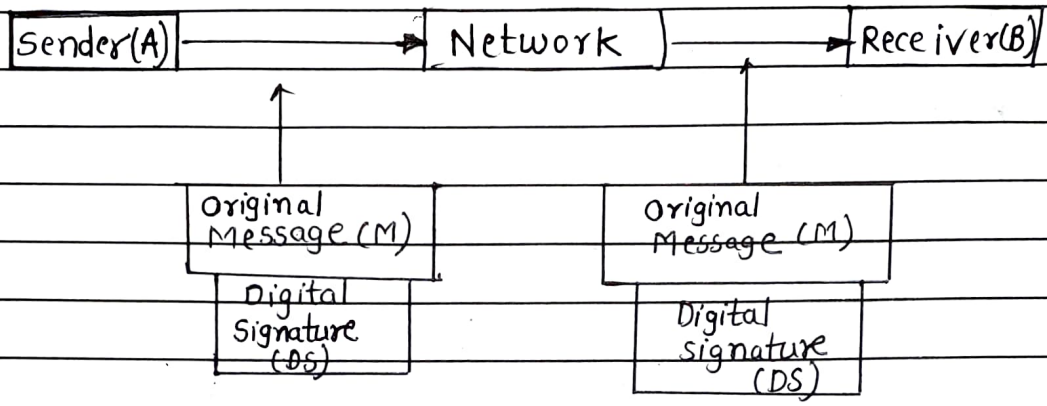
▶ step 2 :-




The sender now encrypts the message digest with his private key. The private key would be, $M^d \bmod n$.

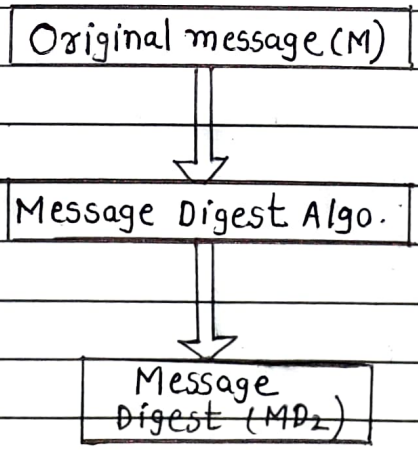
▶ step 3 :-

Now the sender sends the original message along with digital signature to the receiver.




▶ step 4 :-

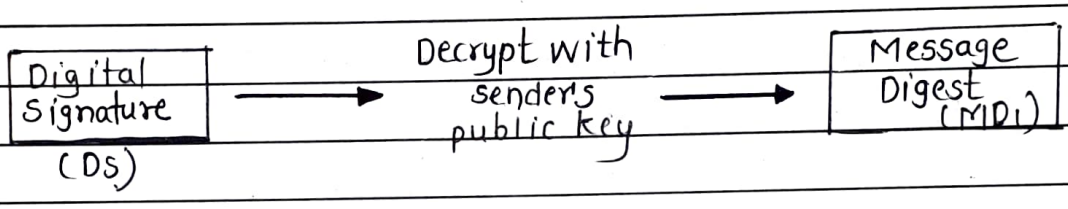
once the receiver receives the original message M & the sender's digital signature, he uses the same message digest algorithm which was used by sender & calculates the new message digest MD2.



Experiment No. Date :

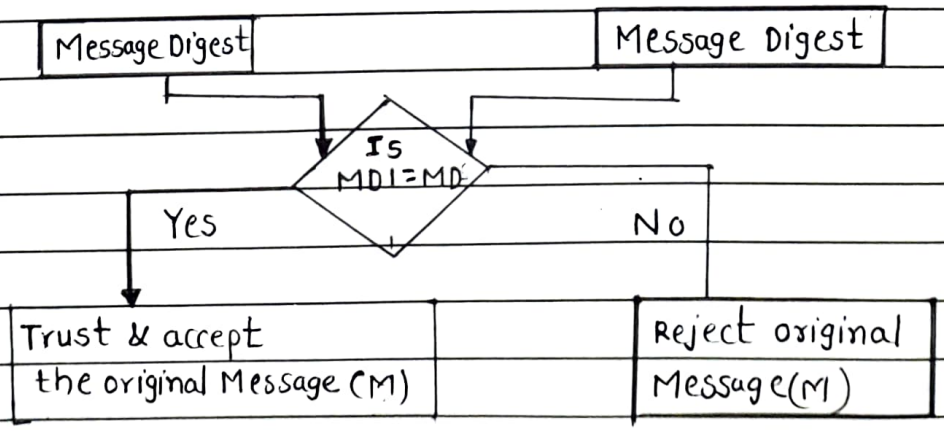
▶ Step 5 :- Decryption

The receiver now uses the sender's public key to decrypt the digital signature ($DS^e \bmod n$). Only sender's public key can be used to decrypt it.




▶ Step 6 :- Verification

Receiver now compares MD2 (calculated in step 4) & MD1 (retrieved from sender's digital signature in step 5)
If MD1 = MD2 then receiver accepts the original Message (M) as the correct, unaltered message from sender.



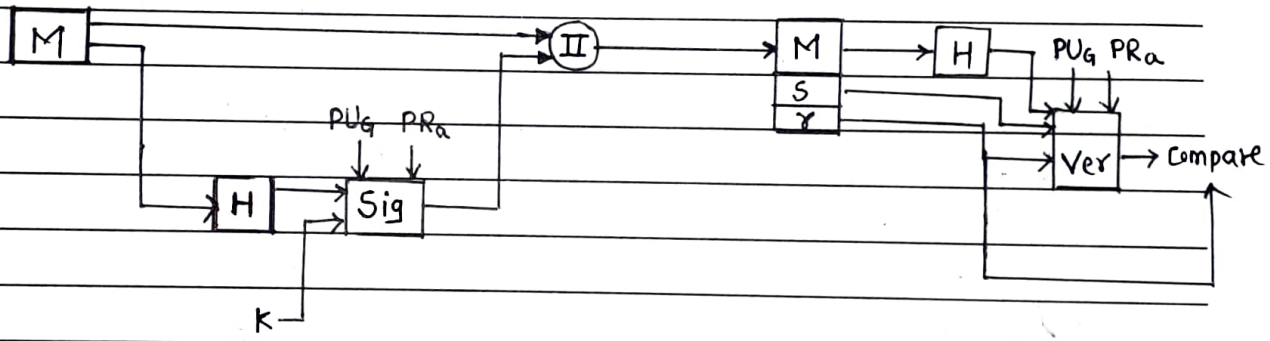
## II) ElGamal Digital Signature scheme :-

- The ElGamal digital signature scheme stems from the ElGamal cryptosystem based upon the security of the one-way function of expomentiation.
- The Elgamal encryption scheme is designed to enable encryption by a receiver's public key & decryption by the receiver's private key.
- The ElGamal scheme involves the use of the private key of sender for encryption & the public key of sender for decryption. This scheme uses the same keys but the algorithm is different. The algorithm creates two digital signatures, these two signatures are used in the verification phase.

Q.11 Explain Digital signature standard ?

→ • Digital signature standard (DSS) is a FIPS which defines algorithms that are used to generate digital signatures with the help of SHA for the ~~Key~~ authentication of electronic documents.

• Unlike RSA, it cannot be used for encryption or key exchange. However it is a public-key technique.




DSS Approach.

• The signature function also depends on the sender's private key (PRa) and a set of parameters known to a group of communicating principals.
We can consider this set to constitute a global public key ($PU_G$). The result is a signature consisting of two components, labelled as s & r.

• At the receiving end, the hash code of the incoming message is generated. This hash code & the signature is input to a verification function.

• The verification function is also depend on the global public key (PUG) as well as the sender's public key (PUa) which is paired with the sender's private key.

- The output of the verification function is compared with the signature component $r$. If the signature is valid that is equal to the signature component $r$.
- The signature function is such that only the sender, with knowledge of the private key, could have produced the valid signature.

Q.12 What is meant by IP spoofing ?

→ IP Spoofing or IP address spoofing, refers to the creation of Internet Protocol (IP) packets with a false source IP address to impersonate another computer system.

IP spoofing allows cyber criminals to carry out malicious actions, often without detection. This might include stealing our data, infecting our device with malware or crashing our server.

Q.13 How does PGP achieve confidentiality and authentication in emails ?

→ Pretty Good Privacy (PGP) is secure email program that provides a confidentiality and authentication service that can be used for electronic email & file storage applications. PGP achieve confidentiality and authentication by the following steps.

1. The sender creates a message M.
2. SHA-1 is used to generate a 160-bit hash code of the message.
3. The hash code is then encrypted with the original message & with RSA using sender's private key.
4. The result is concatenated with the original message

Confidentiality :-

5. Also a 128-bit number is generated which is going to be session key for the current session only.
6. The message from the step 4 is encrypted using CAST-128 & the session key.
7. The session key is then encrypted with RSA using the recipient public key.
8. Message is tranfered through the medium.
9. The receiver uses RSA to with its private key to decrypt and recover session key.
10. Now since the session key is obtained, the remaining message is decrypted using sender's public key & RSA.
11. The receiver then generates a hash code for the message & compares them it with the decrypted hash code. If they match, the message is considered as authentic.

Q.14 Describe Intrusion Detection System ?

→ An intrusion detection system (IDS) is a software application or device that monitors network traffic or anamalous patterns.

- These patterns indicate potentially suspicious activity.
- An IDS also monitors for violations of established network policy

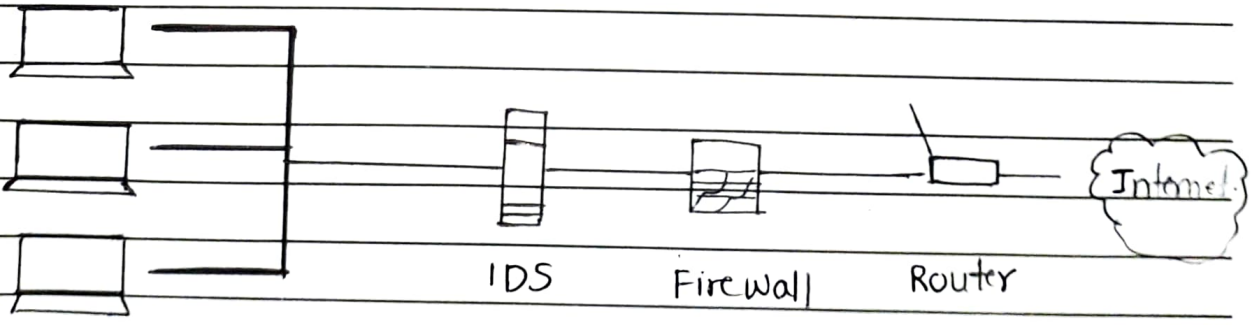
IDS has two possible responses.

1. Send alerts :-

Passive IDS solutions respond by raising alerts through email or text. They may also notify a security information & event management (SIEM) system.

2. Defensive action :-

Active IDS also known as instrusion prevention (IPS) not only sends alerts but has extra security features. These features give active IDS solutions the ability to modify access control lists on firewalls to block the suspicious traffic



Functions of IDS :-

- It keeps an eye on the functions of routers, firewalls, key management servers, & files.
- It provides continuous support to the users.
- Arrange the various audit trails & other logs.

Q.15 Explain firewall characteristics with configurations.

→ Characteristics :-

1. Service control :-

Determines whether inbound or outbound Internet resources can be accessed. The firewall can filter traffic based on IP address, protocol or port number; provide proxy software that receives & interprets each service requests befor passing it on.

2. Direction control :-

Determine the path in which specific service requests are permitted to be initiated & flow through the firewall.

3. User control :-

Controls access to a service based on the customer who is trying to use it.

4. Behavioral control :-

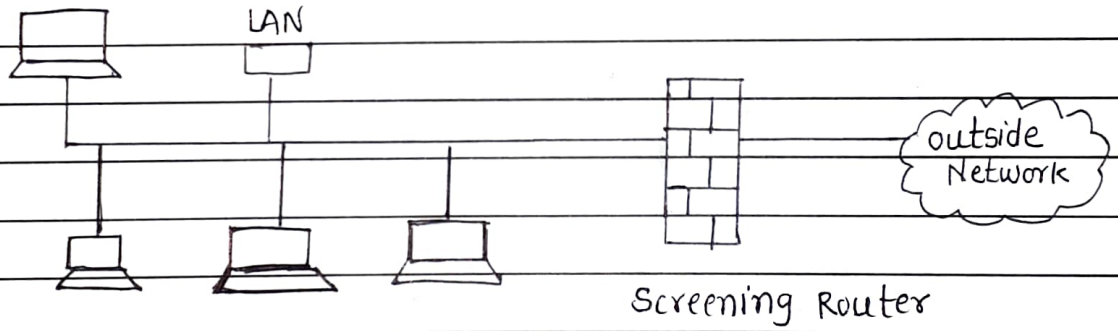
Controls how specific programs are used. The firewall for ex. many filter e-mail to prevent

spam, or it may allow external access to only a portion of the information on a local Web server.

## Different configurations of Firewalls :-

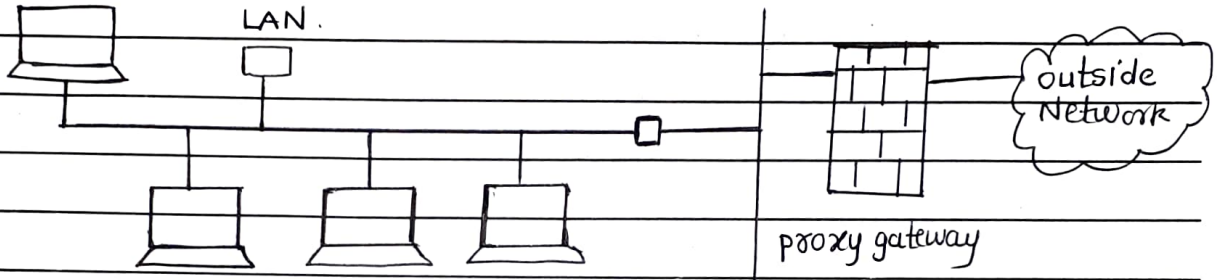
1. Firewall with screening router.
2. Firewall on Separate LAN.
3. Firewall with Proxy & Screening Router.

### 1. Firewall with screening Router :-



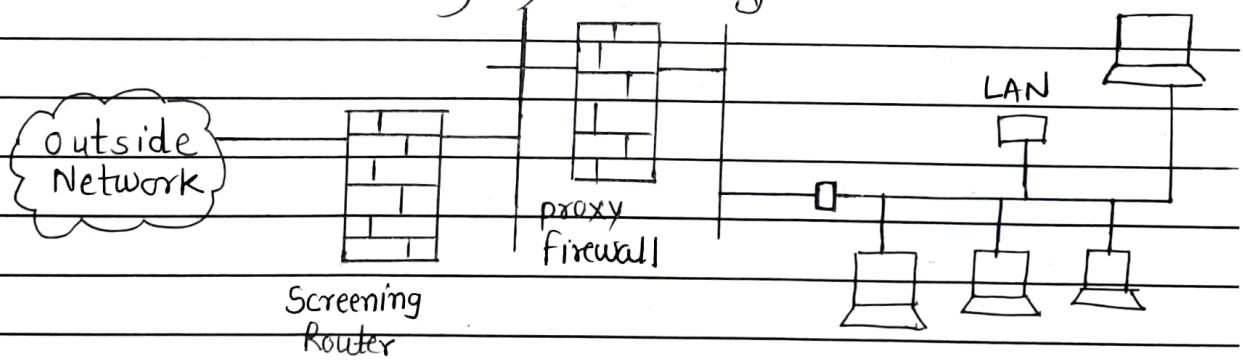

Screening Writer is placed in between intranet & extranet. Another name for screening router firewall is network level or packet-filter firewall.

## 2. Firewall on separate LAN




Unauthorized internet users from accessing private networks connected to the internet are prevented by firewall, especially intranet.

## 3. Firewall with Proxy & Screening Router :-




If screening Router is ~~ist~~ installed behind the proxy firewall, then it ensures the correct address to proxy firewall. In other words it is a double guard protection If anyone fails LAN is not exposed.

Q.16 Classify types of firewalls.

→

1. Packet filtering gateways or screening routers :-

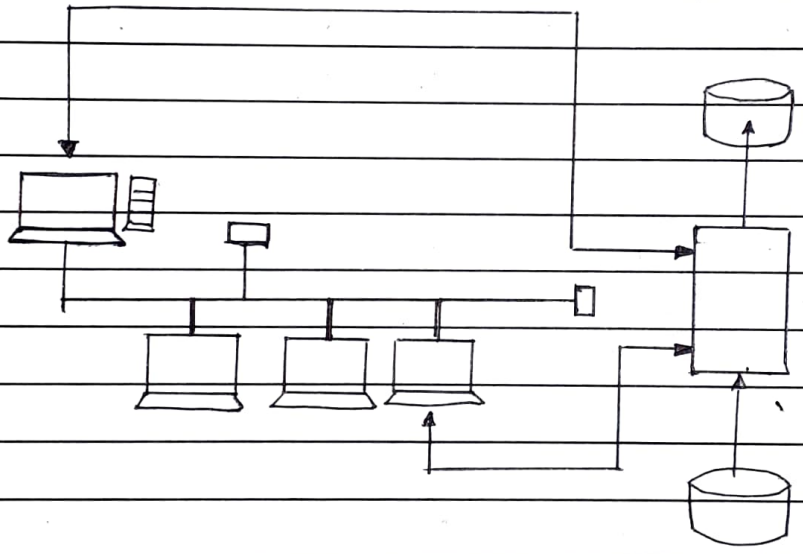
- It is the most simple & easy to impliment firewall.
- Packet filtering is done on the basis of packets source or destination address or based on some protocol. type like HTTP or HTTPS.
- If the firewall is placed behind the router then the traffic can be analyzed easily.

2. Stateful inspection Firewall

- Packet filtering is done one packet at a time. Sometimes attacker use this technique for their attack. Attacker can split the script of attack into different packets so that the complete script of attack cannot be identified by packet filtering firewall.
- To avoid this stateful inspection firewall keeps record of states of the packets from one packet to another. Thus sequence of packets and conditions within the packet can be identified easily..

## 3. Application Proxy :-

- Packet filters cannot see inside the packets, From the packet headers they just get IP addresses for filtering.
- Application proxy is also known as bastion



## 4. Guard :-

- A guard is a kind of complex firewall. It works similar to proxy firewall. Only difference is that guard can detect & decide what to do on the behalf of the user by using available knowledge.
- It can use knowledge of outside users identity, can refer previous interactions, blocked list etc.

Q.17 How Firewall can be placed in a network & be trusted?

→ A firewall acts as a gatekeeper. It maintains & monitors attempts to gain access to your operating system & blocks unwanted unrecognized source.

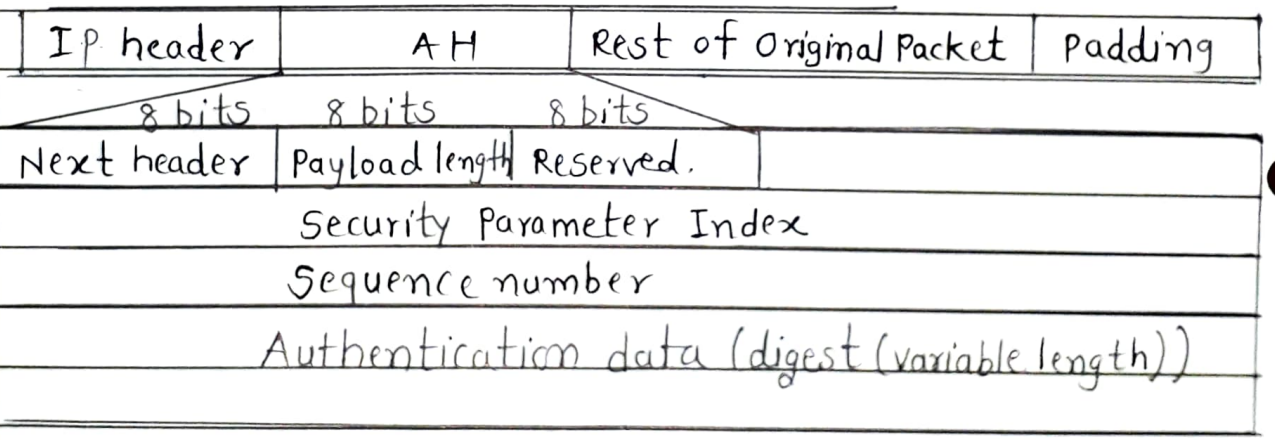
2) It helps to protect your network & information by managing your network traffic.

3) This includes blocking unsolicited incoming network traffic & validating access by accessing network traffic for anything malicious like hackers & malware.

Q.18 Explain IPsec Authentication Header & Encapsulating security Payload ?

→ 1) Authentication Header :-

The Authentication Network & Transport layer



The various field of AH Header are explained below :-

1. Next header :-
It is an 8-bit field that identifies the type of the next payload after the Authentication Header.

2. Payload length :-
Specifies length of AH in 32 bit words.

3. Reserved :-
16-bits field is reserved for future use. It must be set to zero.

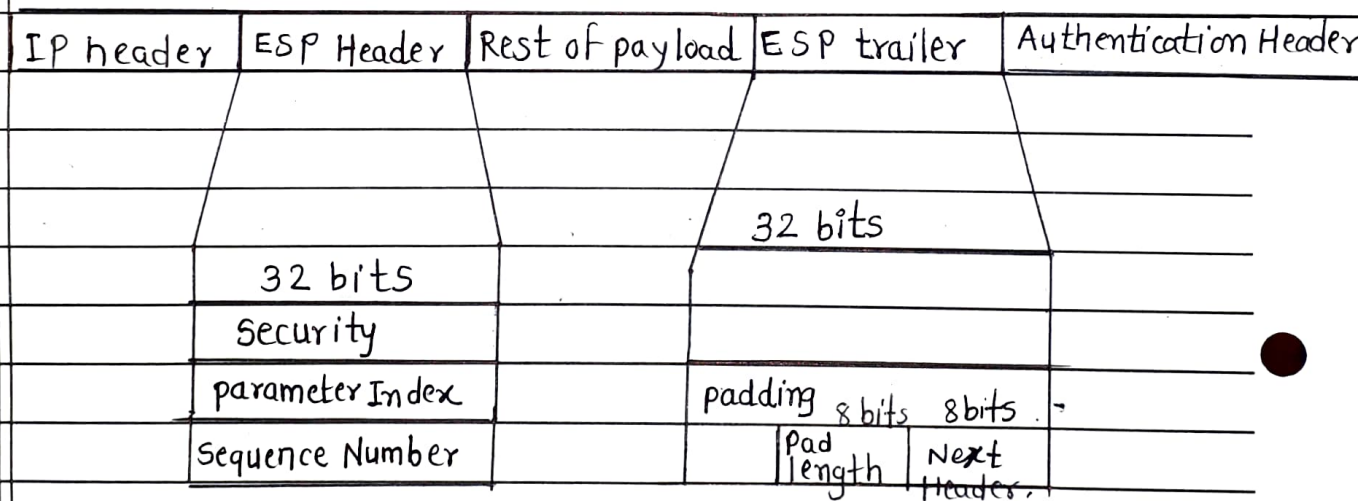
4. Security Parameters Index (SPI) :-
The SPI is an arbitrary 32 bit value that in combination with destination IP address & security protocol (AH) uniquely identifies the security Association for this datagram.

5. Sequence Number field :-
This contains 32-bit field a monotonically increasing counter value. It is mandatory and is always present even if the receiver does not elect-to enable the anti-reply service for a specific SA.

6. Authentication Data :-
This is a variable length field that contains the integrity check value (ICV) for this packet.

## 2. Encapsulating Security Payload - ESP

1) IPsec uses an encryption which provides the encapsulating security payload (ESP).
2) ESP is used to encrypt the entire payload of an IPsec packet.
3) It accomplish this by adding 3 seperate components.
   1. ESP Header
   2. An ESP trailer &
   3. An ESP Authentication block.
4) The combination of this overlapping provide good security.




- ESP Header

It consists of two fields, namely security parameters Index & Sequence Number.

1) Security Parameter Index :-

The SPI is an arbitrary 32-bit value that, in combination with the destination

IP address & security protocol (ESP), uniquely identifies the security Association for this datagram.

2) Sequence Number :-

This unsigned 32-bit field contains a monotonically increasing counter value.

• ESP Trailer :-

1) Padding (for encryption) :-

This field ranges from 0 to 2040 bits. It takes different values depending upon the encryption algorithm used.

2) Pad length :-

This is a 8-bit field which indicates the number of pad bytes immediately preceding it.

3) Next header :-

The next header is an 8-bit field that identifies the type of data contained in the payload data field.

• ESP Authentication :-

The authentication data is a variable length field that contains the integrity check value (ICV) computed over ESP packet minus the Authentication Data.

Q.19 Explain Malicious & Targeted Malicious Codes ?

→ Malicious :-

Malicious software is a software where an attacker can get partial or full control of the program. Thus attacker is free to do anything that he/she want to do.

Malware is currently the major source of attacks & fraudulent activities on the Internet. Malware is used to infect computers. Malware, short form is malicious software or also called as malicious software.

Targeted Malicious Code :-

This is a computer code which is written to attack a particular system, a particular application & for a particular purpose.

Example :-

- An intruder can enter into the system by bypassing all security services or mechanisms. Thus intruder knows the flaws or loopholes in the system & get these loopholes to gain access to the computer.
- Trapdoors are the entry points which are not documented but still inserted during code development for testing purpose, for future extensions or for an emergency access if software fails. These loopholes are purposely kept in the system with good intension.

Q.20 Compare Virus & worm.

| | Virus | Worm. |
|---|---|---|
| 1) | Types : stealth virus, polymorphic, metamorphic etc. | Types :- Email Worm, IRC worm, file sharing worm etc. |
| 2) | Mode of spreading :- Need host program to spread. | It does not need host, it spreads by itself. |
| 3) | It is a software program that can be copy itself & infect the data or information without the knowledge. | It is self-replicating spreads through networks. |
| 4) | Inception :- 'Creeper' virus first known virus spread through ARPANET in 1970. | The name originated by the shock wave rider a novel of science fiction in 1975. from where name is adapted. |
| 5) | Prevalence : More than 100,000 known computer virus have been there through only few have attacked system | Worm existance is moderate as compare to virus. |

Q.21 Explain Virus Countermeasure ?

→ 1. Detection :-

Once the infection has occured, determined that it has occured & locate the virus.

2. Identification :-

Once detection has been achieved, identify the specific virus that has infected a program.

3. Removal :-

Once the specific virus has been identified remove all traces of the virus from all infected systems so that the disease cannot spread further.

Advanced Antivirus Techniques :-

1) Generic Decryption :-

GD technology enables the antivirus program to easily detect even the most complex polymorphic viruses, while maintaining fast scanning speeds.

CPU emulator :-

Instruction is an executable file are interpreted by the emulator rather than executed on the underlying processor.

Virus Signature Scanner :-

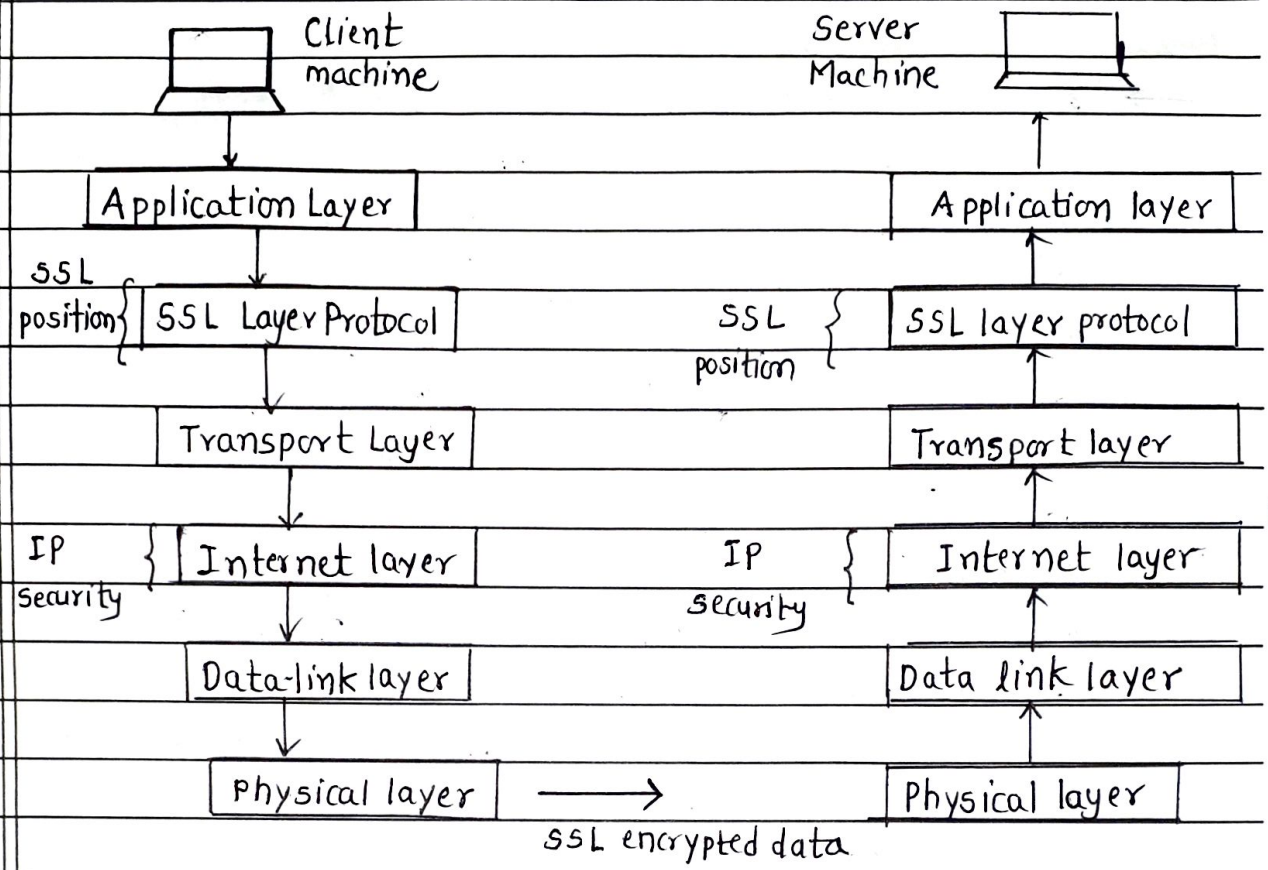
A module that scans the target code looking for known virus signature.

Q.22 Explain SSL & TLS?

→ • Secure socket layer invented by Netscape communications in 1994. Secure Socket layer is an internet protocol used for securely exchanging the information between client's web browser & the web server.
• SSL ensures the authentication, data integrity & data confidentiality between web browser & web server i.e. it creates a secure tunnel between client & server. The main role of SSL is to provide the security to web traffic in all the way.
• The current version of SSL is 3.0. The position of SSL in TCP/IP protocol suite is shown.
• SSL is works between application layer & transport layer the reason is also called as Transport Layer Security (TLS)

• Transport Layer Security :-

• It is used to ensure between communicating applications and their users on the Internet.
• Main function of transport layer protocol is to protect attacker when a server & client communicate, it ensures that attacker or third party should not modify or tamper with any message.
• TLS is the successor to the Secure Socket Layer (SSL).




Q.23 Explain DoS & DDoS.

→ • DoS Attacks :-

• In this attack attacker keeps sending or makes the network or bandwidth overflow by e-mails or spam mail by depriving the victim to access services.

• It is a continuous effort of attacker to make victim unable to use any internet service or resources.

A Dos attack does the following actions :-

1. Flood whole network with unnecessary traffic
2. Damage connection between two system so that communication cannot occur.
3. Disrupt services to legitimate users.

4. Prevent individuals to access network services.

The types of DoS attacks :-

1) Flood attack :-

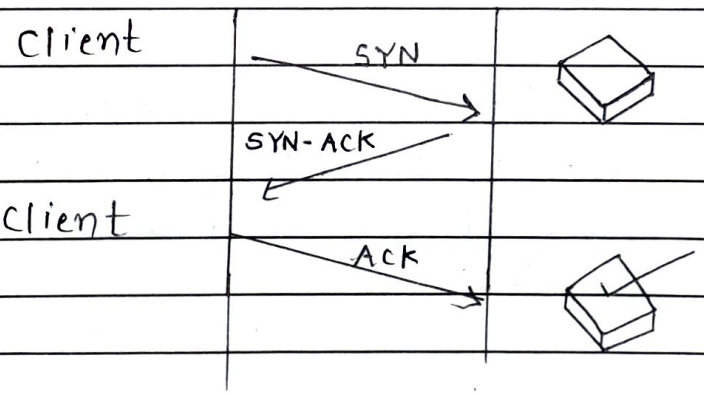
It is very simple to launch & difficult to handle.

2) Ping of Death Attack :-

sending huge ICMP packet

The attacker sends this huge oversize packet to the victim's system which causes victim's system to crash or freeze resulting in DOS.

3) SYN Attack :-




3 way handshake

- It is a TCP SYN flooding attack, a denial of service attack. In TCP handshaking of network connection is done between sender & receiver through synchronous and acknowledgement (ACK) messages.

DDoS - Distributed Denial of service Attacks :-

- It is a attack in which multiple compromised computer system attack a target such as a server website or other network resource, & a cause a denial of service for users of the targeted resource.
- DDoS, it is when an attacker uses your own computer to attack on another computer.
- It takes advantage of loopholes & security vulnerability to take control on for computer to send vulnerability spam or send huge data to other computers.
- The system which are used for attacking victim computer are called as Zombie systems.
- Various tools to launch DDoS attack are Trinoo, Tribe flood, shaft etc.
- A deniel of service Attack is characterized by explicit attempt by an attacker to prevent legitimate users of service from using the desired resources. -

Measures to protect from DoD/DDoS attack are :-

- Implementing filters on routers
- Disable unused network services.
- Examine the physical security routinely
- Maintain regular backup schedules & policies.
- Maintain password policies.
- Using fault tolerent network configuration
- Tools for detecting DoS/DDoS attacks zombie Zapper, find-DDoS, remote intrusion detector (RID).

Page No:

Q.24 What is Denial of service attack ? What are the different ways in which an attacker can mount a DOS attack on a system ?

→ • Deniel of service & distributed deniel of services is a type of attack that causes legitimate users unable to use services on the resources, or services become unavailable to the legitimate users.

• In this attack, the attacker keeps on sending or marks the network or bandwidth overflow by e-mails or spam mail by depriving the victim to access services.

• The attacker's main target for websites or services which include financial site bank or credit card gateway systems.

• The targeted network which are root for DOS are mobile phone network or credit card, gateway network.

• The different ways in which an attacker can mount DoS attacks are :-

1) SYN Flood Attack :-

Attacker keeps on flooding or overloading victim's system with 'n' numbers of ping packets which result into huge traffic which the victim itself cannot handle.

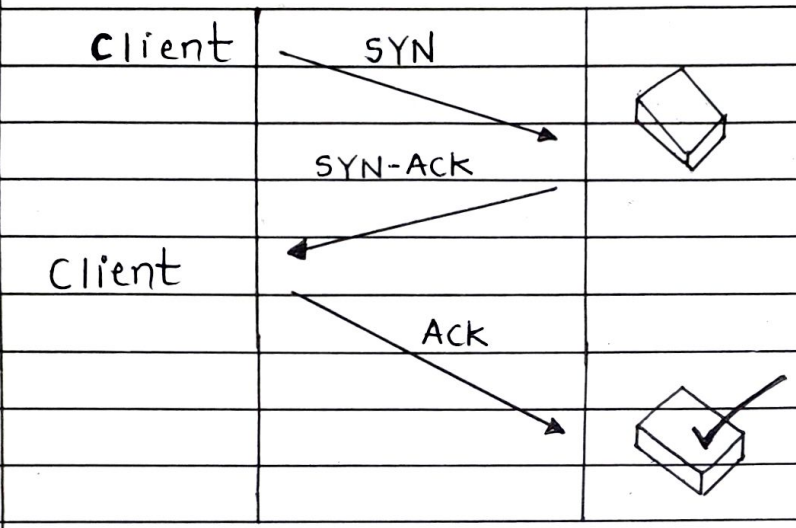
It is very simple to launch & difficult to handle.

2) Ping of Death Attack :-

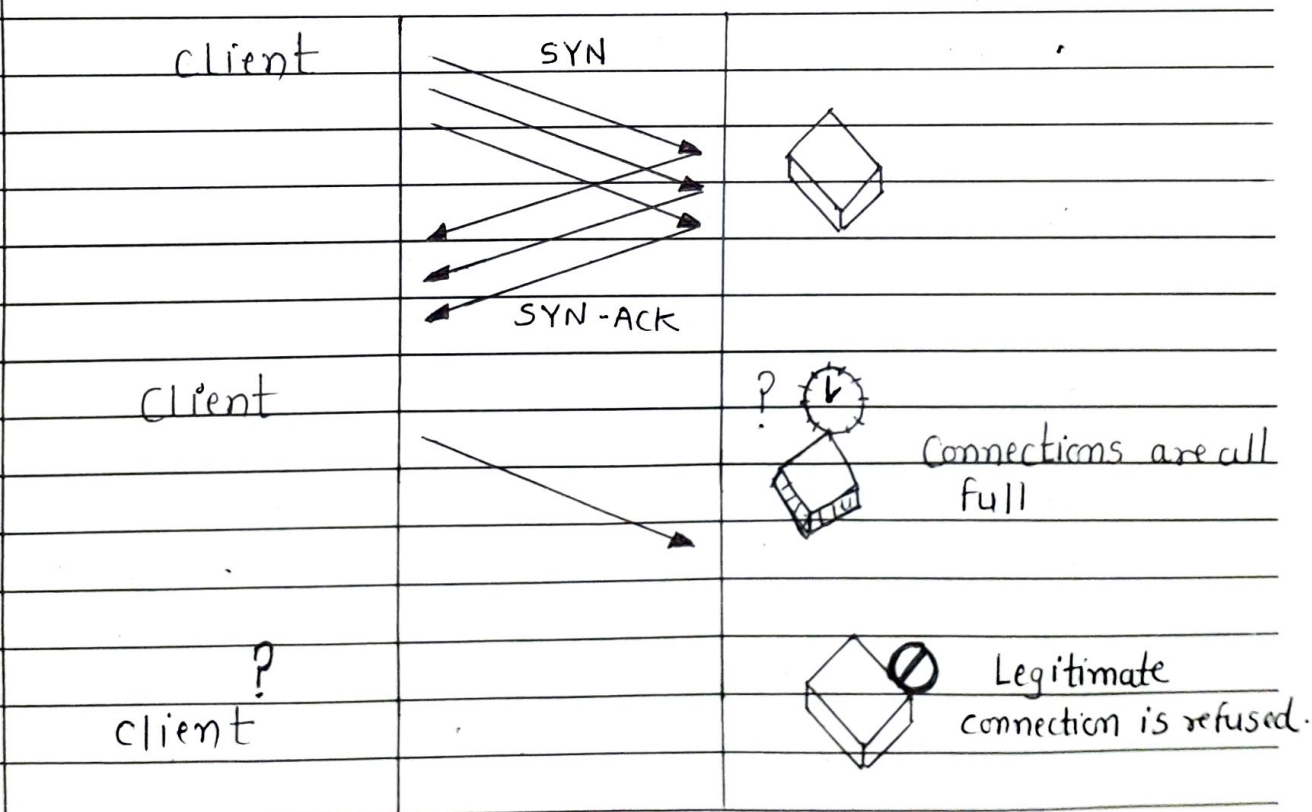
sending huge ICMP packet (These packets are used in IP layer or network layer for indicating error message) The attacker sends this huge oversize packet to the victim's system which causes victim's system to crash or freeze resulting in DOS.

3) SYN Attack :-

- It is a TCP SYN flooding attack, a deniel of service attack. In TCP handshaking of network connection is done between sender & receiver through synchronous (SYN) & acknowledgement (ACK) messages.
- An attacker initiates a TCP connection with server with a SYN message. The server in reply sends an acknowledgement message (SYN-ACK) message.
- The client (attacker) does not respond back with acknowledgement which causes server to wait.
- Due to which it is unable to connect with other client. This fills up the buffer space for SYN message preventing other for communicate.




3 way Handshake.



4. Teardrop Attack :-

It is an attack when packets are developed & overlapped with each other & the receiver is not able to reassemble them, usually corrupted packets are send by attacker to hang or freeze the system.

5. Nuke :-

It is an attack of sending invalid ICMP packet to the target which slow down the affected computer till it is completely stop.

6. smurf attack :-

It is an attack in which IP address broad casting is done. A smurf program is used to make network inoperable. It builds a packet which seems to originate from another address. This packet contains ICMP ping. The echo responses are sent back to victim. Maximum ping & echo make network unusable.

The various tools for DOS attack are Jolt2, Nemesy, Targa etc.

Q.25 What is session Hijacking & Spoofing ?

→ Session Hijacking :-

- TCP session Hijacking is a security attack on a user session over a protected network. The most common method of session hijacking is called IP spoofing.
- When an attacker uses source-routed IP packets to insert commands into an active communication between two nodes on a network & disguising itself as one of the authenticated users. This type of attack is possible because authentication typically is only done at the start of a TCP session.
- Another type of session Hijacking is known as a man-in-the middle attack, where the attacker using a sniffer, can observe the communication between devices & collect the data that is transmitted.

Spoofing :-

- Spoofing is a type of scam in which a criminal disguises an email address, display name, phone number, text message or website URL to convince target that they are interacting with known trusted source. Spoofing often involves changing just one letter, number or symbol of the communication so that it looks valid a quick glance. For example, you could receive an email that

appears to be from Netflix using the fake domain name.

Q. 26. Define

i) Phishing :-

Phishing is a cybercrime in which a targets are contacted by email, telephone or text message by someone posing as a legitimate intitution to lure individuals into providing sensitive data such as personality identifiable information banking & credit card details & passwords.

ii) Buffer overflow :-

Buffers are memory storage regions that temporarily hold data while it is being transferred from one location to another A buffer. A buffer overflow occurs when the volume of the data exceeds the storage capacity of the memory buffer.

iii) Format strings Attack :-

A format string is a way of telling the C compiler how it should format numbers & other values when it prints them or store to the buffer.

iv) SQL Injection :-

It is a source code injection technique in which malicious SQL statements are inserted into entry field of database to dump database content.

Q.27 Differentiate Firewall & IDS.

| Parameter | Firewall | IDS |
|---|---|---|
| Definition | Firewall is a network security device that filters incoming & outgoing network traffic based on predetermined rules. | IDS is a device or software application that monitors a traffic for malicious activity or policy violations & sends alert on detection. |
| Principle of working. | Filters traffic based on IP address & port numbers. | Detects real time traffic & looks for traffic parameters or signatures of attack & then generates alerts. |
| Configuration mode | Layer 3 mode or transparent mode. | Inline or as end host for monitoring & detection. |
| Placement. | Inline at the perimeter of the network. | Non-Inline through port span. |
| Traffic patterns | Not analyzed. | Analyzed. |

| Parameter | Firewall | IDS |
|---|---|---|
| Placement wrt to each other. | should be 1st Line of defence. | should be placed after firewall. |
| Action on Unauthorized traffic detection | Block the traffic | Alerts/alarms on detection of anomaly. |
| Related Technologies. | • Stateful packet filtering<br>• permits & blocks traffic by port/protocol rules. | • Anomaly based detection<br>• signature detection<br>• Monitoring<br>• Alarm. |

Q.28 Differentiate between the transport mode & tunnel mode of IP sec & Explain how authentication & confidentiality are achieved in using IP sec.

→

| Transport Mode | Tunnel Mode |
|---|---|
| • Provide protection mostly for upper-layer protocols eg. TCP or UDP segment ICMP Packet. | Provide protection to the entire IP packet. |
| • Typically used for end-to-end communication between two hosts. | Used when one or both ends of a security association (SA) are a security gateway. |
| • ESP in transport mode encrypts & optionally authenticates the IP payload but not the IP header. | ESP in tunnel mode encrypts, can authenticate entire inner IP packet including inner IP header. |
| • AH in transport mode authenticates the IP payload & selected portions of the IP header. | AH in tunnel mode authenticate the entire inner IP packet & selected portions of outer IP header. |

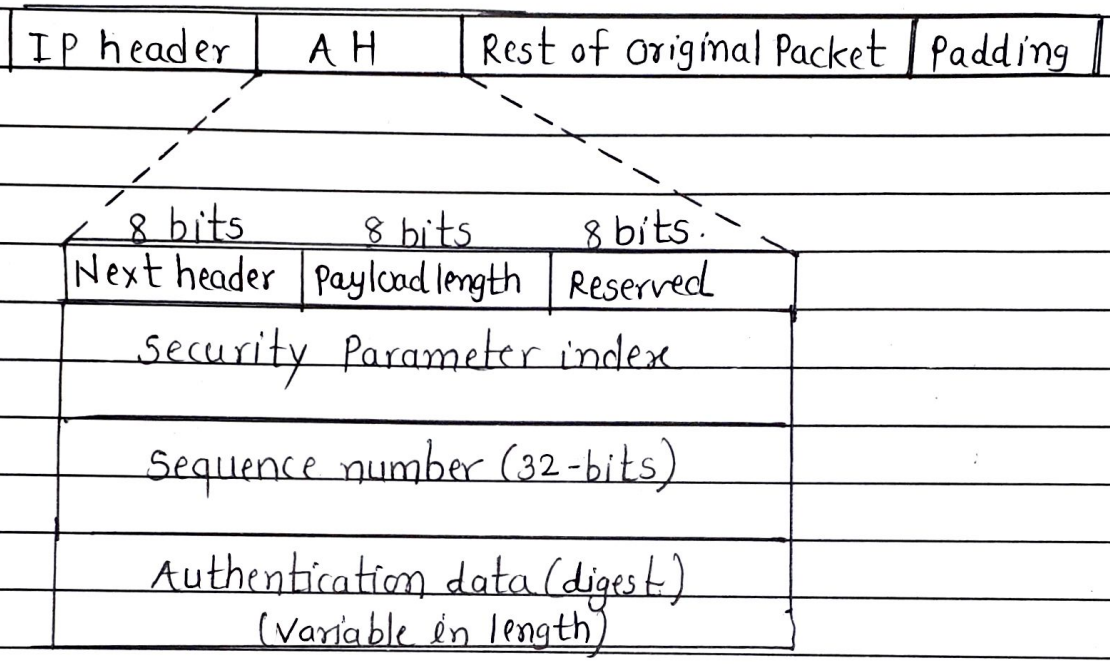
IPSEC :-

- It is a protocol to provide security for a packet at a network layer which is often referred to as the internet protocol or IP layer.

IPSec defines two protocols :-
a. The authentication Header (AH)
b. Encapsulation Security Payload (ESP)
to provide authentication & for encryption for the packets, at the IP level.

a. Authentication Header (AH) :-

- Provide source authentication & data integrity but not privacy.
- AH protocol is designed to authenticate the source host & to ensure the integrity of payload carried in the IP packet.
- This protocol was a hash function & a symmetric key to create a message digest, the digest is inserted via the authentication header.
- The AH is then placed on the appropriate header based on the model i.e. transport or tunnel.




Authentication Header (AH) protocol.

b. Encapsulating Security Protocol :-

- As all protocol does not provide privacy IPSEC comes up with ESP protocol.
- It provides source authentication, integrity & privacy.
- It adds a header & trailer.
- ESP's authentication data are added at the end of the packet which makes its calculation easier.

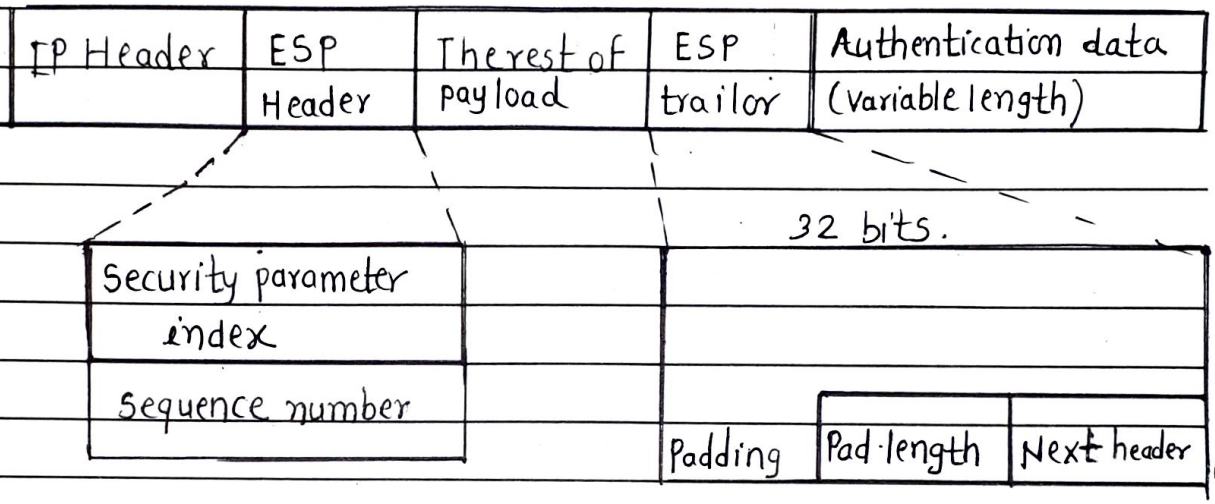

IP Header
ESP Header
The rest of payload
ESP trailor
Authentication data (Variable length)
32 bits.
Security parameter index
Sequence number
Padding
Pad length
Next header

fig: ESP