## Network Security - I

### Security at application layer:

### PGP (PRETTY GOOD PRIVACY)

* PGP was designed to provide all four aspects of Security

  ie: • privacy
  • Integrity
  • Authentication
  &
  • Non-repudation

* It provides email Security.

* It is Used for • Signing
  • encrypting
  • decrypting of texts, files and directories. (ie data)

* It works through a Combination of Cryptography data Compression and hashing technique.

### PGP Notations:

* The growth of pretty good privacy (PGP) is available free worldwide in versions that run on varity of platforms.

* It has wide range of applications.

* It was not developed or Controlled by any government / Standard organization.

Ep - Public key encryption

Dp - Public key decryption

Ec - Symmetric encryption

Dc - Symmetric decryption

Ks - Session key Used in Symmetric encryption Scheme

PRa - Private key of User A, Used in public key encryption.

PUa - Public key of User A, Used in Private key encryption.

H - Hash function

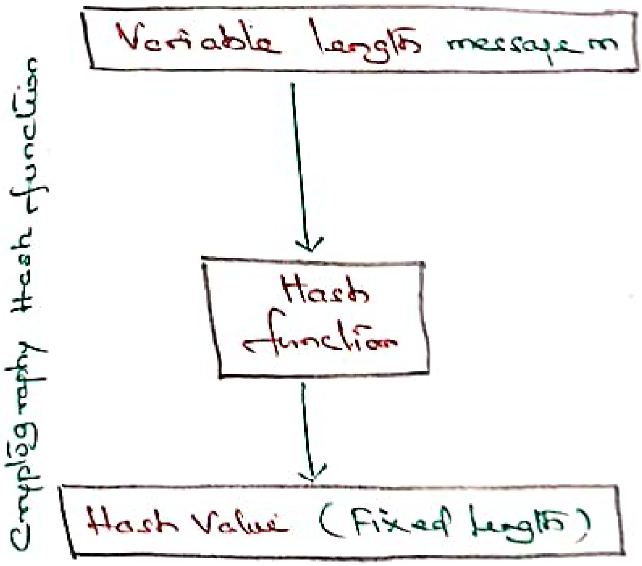
Z - Compression Using zip algorithm

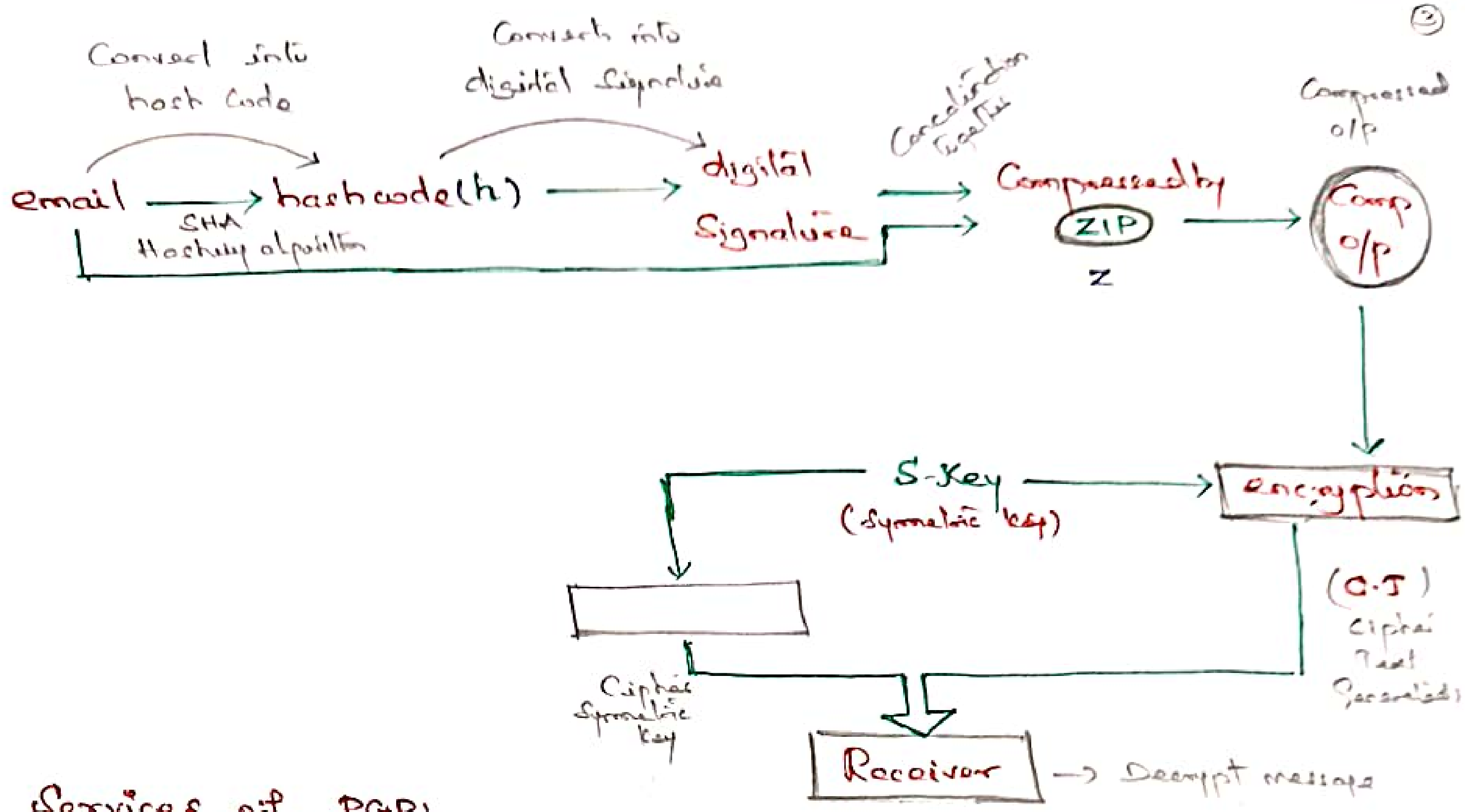
Techniques in PGP:

1. Hashing
2. Data Compression
3. Symmetric key
4. Asymmetric key

Hashing:

A Cryptographic hash function is a mathematical function that Converts a message of any length into a fixed-length string of numbers.


Cryptography Hash function
Variable length message m
Hash function
Hash Value (Fixed length)



## Services of PGP:

(i) Authentication

(ii) Confidentiality

(iii) Compression

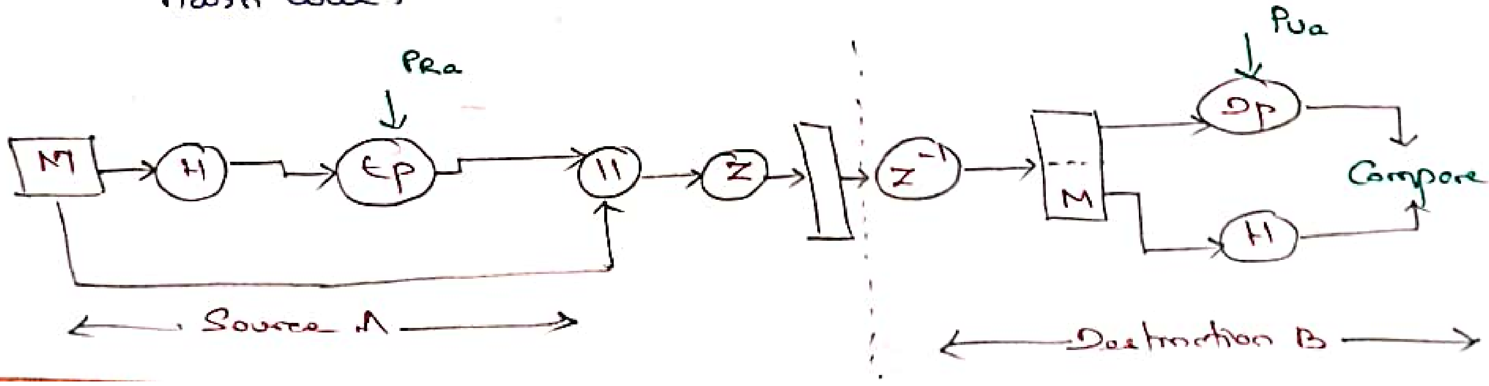
(iv) email Competibility

## (i) Authentication :-

- * Sender Creates a message, SHA-I, Used to generate 160-bit hash Code of message.

- * Hash Code is encrypted with RSA Using Sender private Key and result is attached to message.

- * In the other end receive Uses RSA or DSS with Senders public Key to decrypt to recover hash code.



- Receiver generates new hash Code for message and Compare with decrypted hash Code, if match the message is accepted as authentic.

(ii) Confidentiality:-

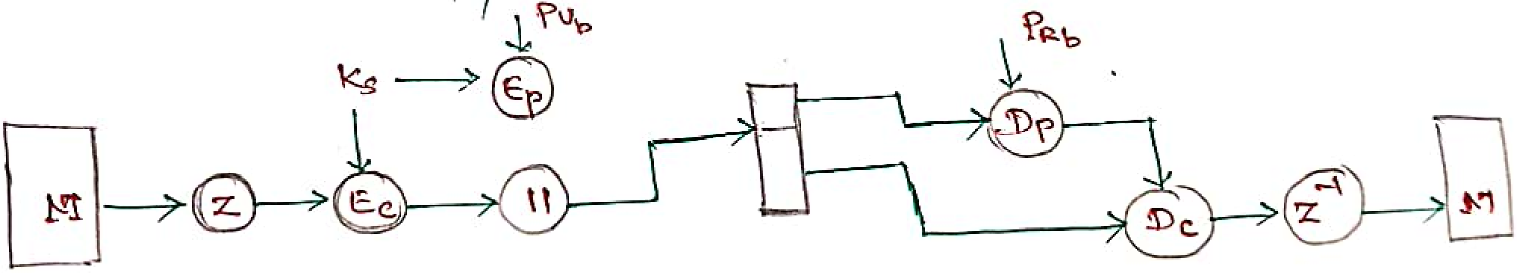
- Sender generates message and random 128 bit number to be Used as Session key for this message only.

- Message is encrypted Using CAST-128/IDEA/3DES with Session key.

- Session key is encrypted Using RSA with recipient's public key then attached to message.

- Receiver Uses RSA with private key to decrypt and recover Session key (Ks)

Session key (Ks) is Used to decrypt message.



(iii) Compression:-

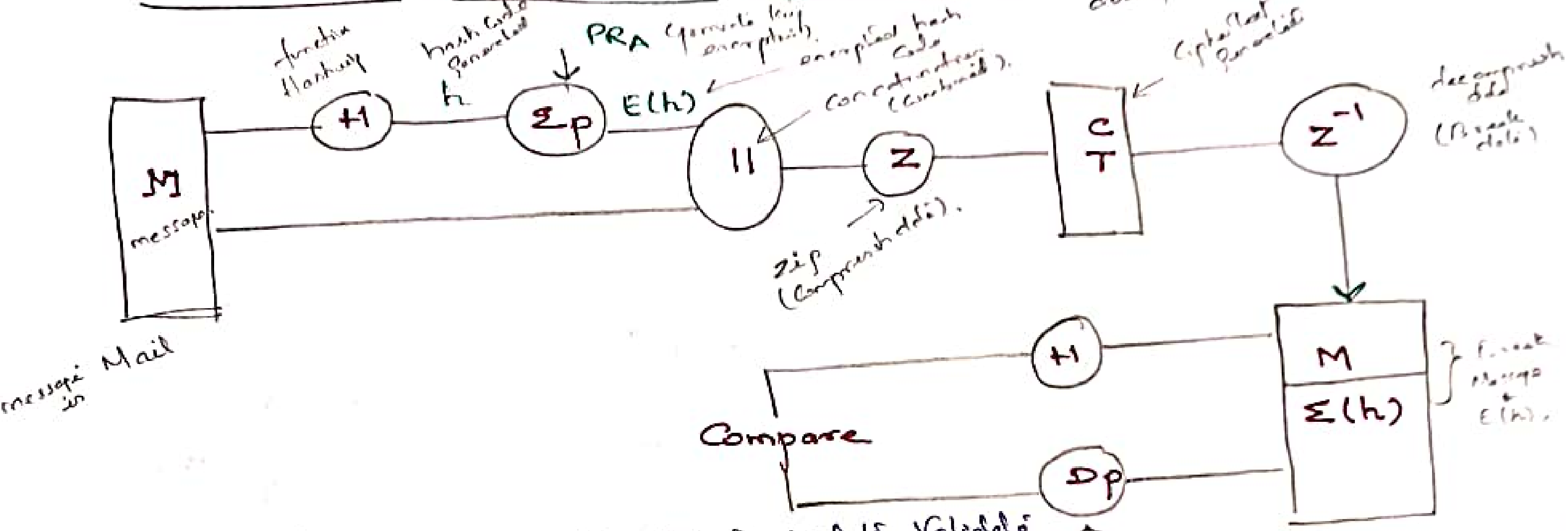
- The PGP Compresses the message after applying the Signature, but before encryption.

- This has the benifit of Saving Space both for email-transmission and for the purpose of file-Storage.

## Case 1:

## Authentication + digital Signature:.

No Confidentiality → because we are not doing encryption. X



* Authentication basically that is used to validate something as true or real. Ex: login email.

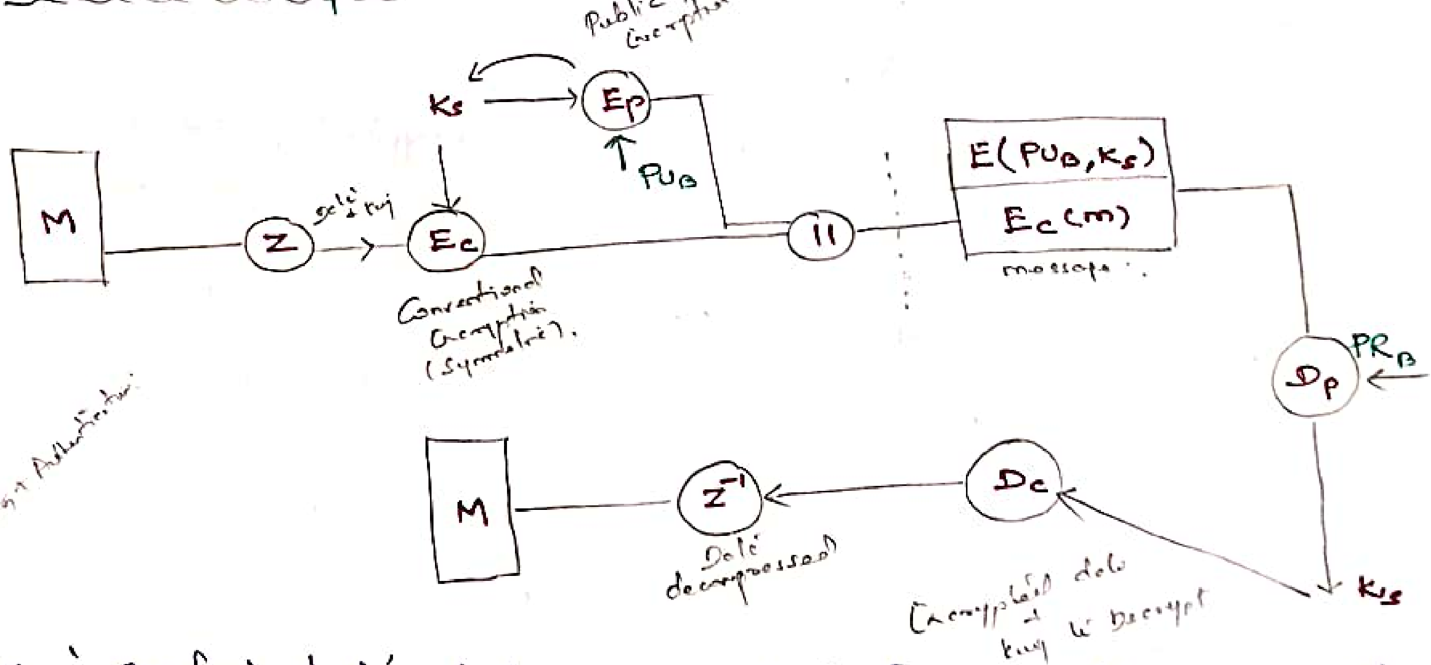
* Hash function (H) calculate the Hash values of the message, for the hashing purpose. SHA-1 is used and it produces a 160 bit output hash value. Then using the sender's private key (Kpa) it is encrypted is called Digital signature.

* The msg is compressed to reduce the transmission overhead and is sent over to the receiver.

* The signature is then encrypted using the sender's public key (PUa) and hash value is obtained.

## Case : 2 :-

## Confidentiality :.



Case 3: Confidentiality + Authentication

* 'Confidential' which means that those package are not meant for all the people and only selected person's can see them.

* The same applies to the email confidentiality as well as.

* In email service only sender and receiver should be able to read the message.

Note:- Hash function is a mathematical algorithm that converts a variable number of characters into a fixed number of characters.

- Here, the Session Key (Ks) itself gets encrypted through public encryption (Ep) Using receiver public key (KUb)

- The Original message was Compressed and then encrypted intially. Even if any one could get hold of the traffic. They Cannot read the contents.

- They Can read if they had the Session key (Ks)

- Session key (Ks) is transmitted to the receiver and it is to encrypted form and only the receiver's private key (Kpb) can be Used to decrypt.

Email Compatibility:

- When PGP is Used, at least part of the block to be transmitted is encrypted. If the only Signature (Security purpose) Service is Used.

- Then the msg digest is encrypted. If the Confidentially Service is Used, the msg + Signature are encrypted.

- Thus, part or the entire resulting block Consists of a Stream of arbitary 8-bits.

- However, many electronic mail systems only permit the Use of blocks Consisting of ASCII text.

## S/MIME :-

First we have to know about SMTP.
[S]imple [M]ail [T]ransfer [P]rotocol.

SMTP :- * In SMTP transfer the ASCII data which is nothing but Text format.

* By Using SMTP we can send only Text message, we cannot send videos, images and audio's etc.
* SMTP send the text that is written in english only no other languages are not supported like Telugu, Hindi, Malayalam, Kannada etc.
* SMTP has a very simple structure. To overcome this MIME is introduced.

## MIME:

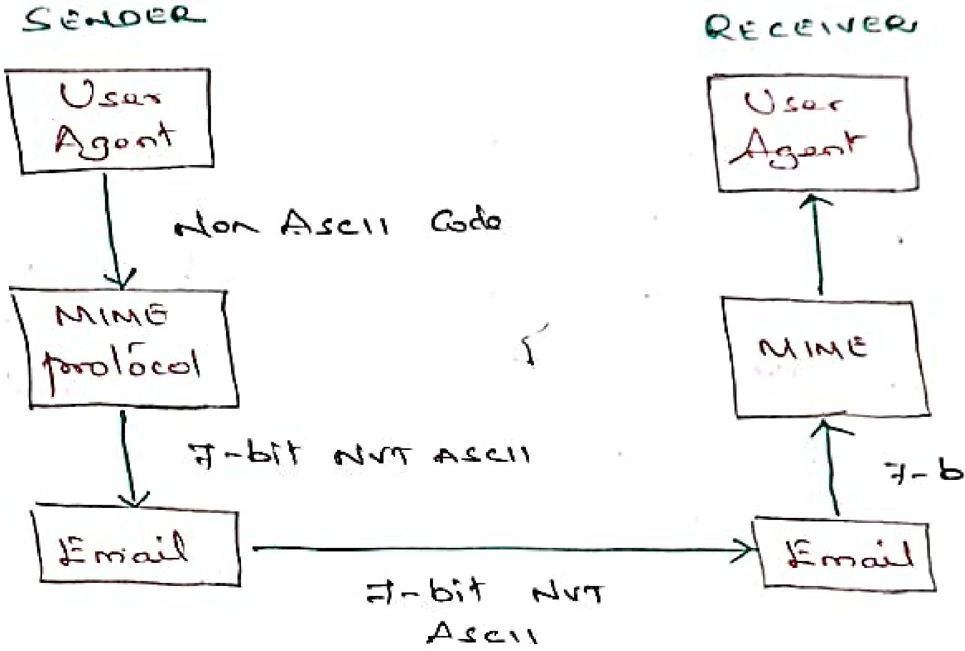
* MIME stands for Multipurpose internet Mail Extension
* MIME is a kind of add-on or a Supplimentry protocol that allows non-ASCII data to be send through SMTP.

It allows the Users to, exchange different kinds of data like Audio, Video, image through internet.

## Working of MIME:

* Suppose a User wants to send an email to the receiver through User agent.
* The data is Non-ASCII format. So there is a MIME protocol that Convert it into 7-bit ASCII through Network Virtual Terminals (i.e: NVT format)
* In the receiver side the MIME protocol

receives the 7-bit ASCII and 7-bit format Convert it back into non-ASCII Code and then now the receiver reads it.



MIME Header:

MIME header provides important details about the Content of a message.

(1) MIME Version : Defines the Version of MIME protocol

(2) Content type : Type of data is being transmitted like. text, image, Videos

(3) Content type Encoding:- It defines the method Used for encoding the message like 7-bit encoding.

(4) Content id : It is Used for the purpose of Uniquely identifying the Message.

## S/MIME Protocol:

- * It is Secure/MIME , ie: extension to MIME
- * It encrypts emails and provide security
- * It allows us to digitally sign on our email.
- * Finally which uses asymmetric key Cryptography.
- * MIME is introduced addon which allows to transfer non ASCII data over mail and now S/MIME is secure for other types of data.

## Functions of S/MIME:

1. Authentication – Data received by authenticate user.
2. Message Integrity – protect from modification
3. Non-Repudiation – protect against repudiation on both
4. Privacy – Data cannot be caused by the 3rd party
5. Data Security – protect data being transmitted

## Services of S/MIME:-

1. Digital Signature
2. Message Encryption – write

## 1. Digital Signature:-

* A digital signature is a mathematical technique used to validate the authenticity and integrity of a message, software or digital document.

* Digital signature in S/MIME protect against email spoofing attacks that involves sending an email with a fack sender address.

## Support for S/MIME:

The most popular email programs that Support S/MINE are as follows.

1. iphone ios Mail
2. Apple mail
3. GMail IBM Notes
4. Cipher Mail
5. Outlook on the Web.

## Security of Transport Layer:

### Secure Socket Layer: (SSL)

* SSL provide Security for Communication between two users.

* SSL ensures three Concepts that,

Integrity
authentication
&
Confidentiality

* SSL lies between application layer and transport layer of TCP/IP.

TCP/IP - 4 layer
OSI - 7 layer

Application Layer

⟶ SSL

Transport Layer

### Protocol stack of SSL:

<table>
<tr><td>SSL Handshake protocol</td><td>SSL change Cipher</td><td>SSL alert protocol</td><td>http</td></tr>
<tr><td colspan="4">SSL Record protocol</td></tr>
<tr><td colspan="4">TCP</td></tr>
<tr><td colspan="4">IP</td></tr>
</table>

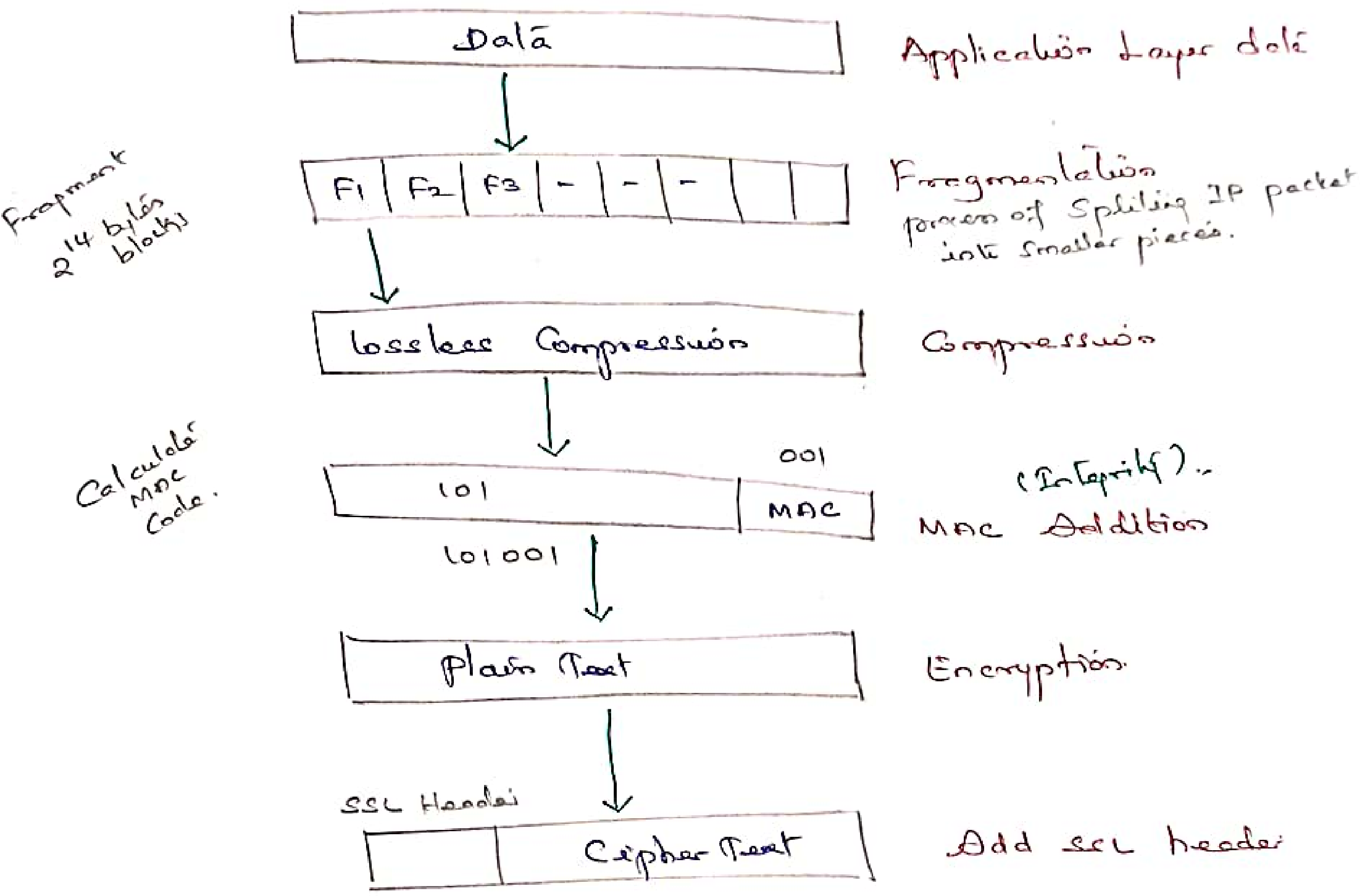
### SSL Record protocol:

It has two Services.

(i) Confidentiality ⇒ by encryption.

(ii) Message Integrity ⇒ by MAC

⑫



## SSL Handshake protocol :-

- ✱ It ensures Authentication
- ✱ It Can be solve most Complicated part in SSL.
- ✱ It Can do key exchange between client and Server.

procedure :-

1. It's Connection establishment with Server.
2. Makes key exchange from client to Server
3. Make's key exchange from Server to client

} authentication

4. Handshake done from Server.

Handshake protocol in Cryptography is a process that establishes a secure connection between a Client and a Server.

# TLS (Transport layer Security)

- TLS was proposed by the "Internet Engineering Task force" [IETF] an international standard organization.

- TLS was derived from "Secure Socket layer" (SSL)

- The first Version of TLS was published in 1999.

- The most recent Version of TLS 1.3 which was published in 2018.

## Concept of TLS:-

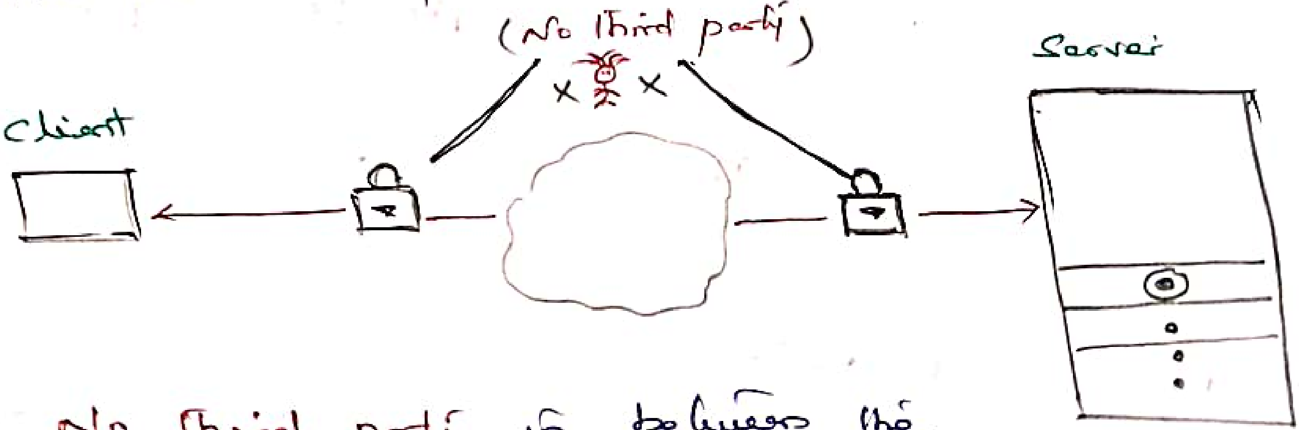
→ Transport layer Security (TLS) is designed to provide Security of Transport Layer.

→ It is derived from SSL

→ It is defined in RFC 2246

→ It provides a Secured Connection between client and server.

→ TLS is Used by http, smtp



→ No Third party is between the Clients and Server Secured Connection.

## Work of TLS:

→ TLS ensures

Encryption
Authentication
&
Integrity

→ **Encryption:** hides the data being transmitted from third parties.

Eg: Plain text to Cipher text.

→ **Authentication:** Ensures that the parties exchanging information are who they claim to be.

→ **Integrity:** Verifies that the data has not been changed or Tampered with.

## Protocol Stack:

* The architecture of TLS involves several Components and processes that work together to establish secure Communication between client and Server.

<table>
<tr><td>Hand Shake Protocol</td><td>change Cipher spec</td><td>Alert protocol</td></tr>
<tr><td colspan="3">TLS Record protocol</td></tr>
</table>

## TLS Record protocol:

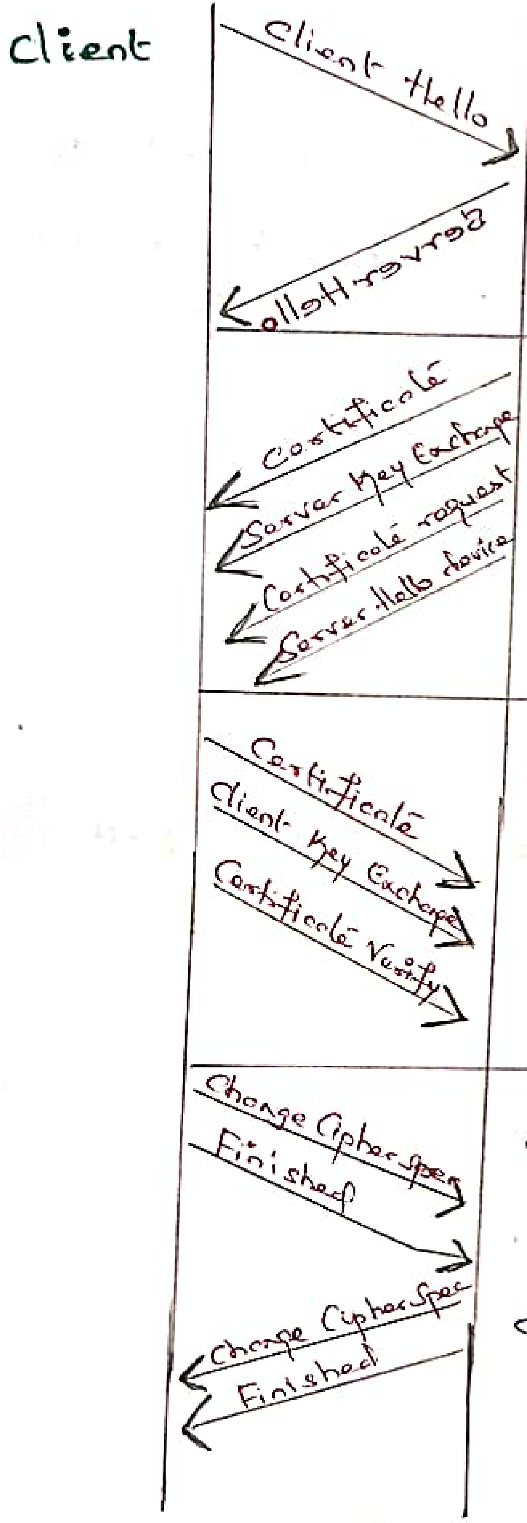
→ TLS Record protocol provides two services to it

1. Confidentiality — write about it
2. Integrity — write about it.

## Hand Shake Protocol:

This protocol allows the Client and Server to authenticate each other by Sending a Services of message to each other.

It uses four phases to Complete its Cycle:



Server

**Phase:1**

Establish Security Capabilities including protocol version session ID, Cipher suite Compression method.

**Phase:2**

Server may send Certificate Key exchange and request for Certificate Server Signals end of hello message phase

**Phase:3**

Client Sends Certificate if requested Client send key exchange client may send Certificate Verification.

**Phase:4**

Change Cipher Suite and finish hand shake protocol.

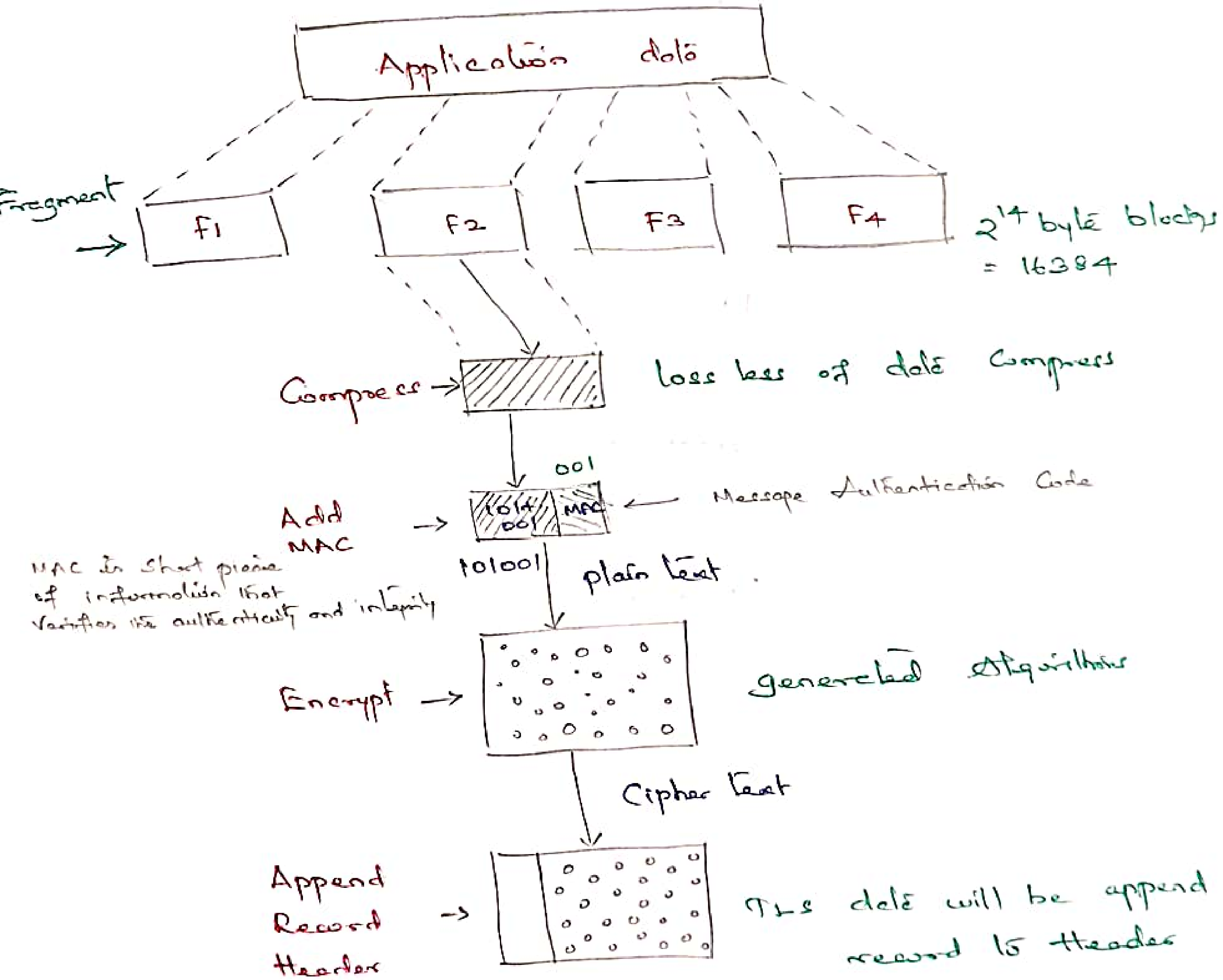
## 1. Confidentiality:

* Principle of Security which ensure that only the Sender & the receiver of a message Come to know about the "Content of message"

Ex: o/p of Banking transaction Secure.

## 2. Integrity:

* principle of Security which ensure that the Content of message must not be modified during it's "transmission" from Sender to receiver.


Application data
Fragment
F1
F2
F3
F4
$2^{14}$ byte blocks
= 16384
Compress
loss less of data Compress
001
1014
001
MAC
Message Authentication Code
Add MAC
MAC is Short piece of information that verifies the authenticity and integrity
101001
plain text
Encrypt
generated Algorithms
Cipher text
Append Record Header
TLS data will be append record to header

## Change Cipher Spec Protocol:-

→ Change Cipher protocol Consists of a Single message which is 1 byte in length and can have only one value.

→ This protocol purpose is to cause the pending state to be copied into the Current state.

## Alert Protocol:-

→ Alert protocol is used to convey TLS-related alerts to the peer entity.

→ Each message in this protocol Contain 2 bytes

→ In first byte :- Has 2 levels:

Level 1:-

* This alert has no impact on the Connection between Sender and receiver.

Ex:- Certificate Expired
No Certificate.

Level 2:-

* This alert breaks the Connection between Sender and receiver.

Ex:- Bad record MAC
handshake failure.

* Second byte in the alert protocol describes the error.

M. ANBARASU., M.Sc., (Maths)., M.S., (SS)., M.Tech., (CSE)., (PhD).,

## Security at Network Layer:

### IP Security:-

Internet protocol Security (IPSec) is a framework for protecting Communication over IP.

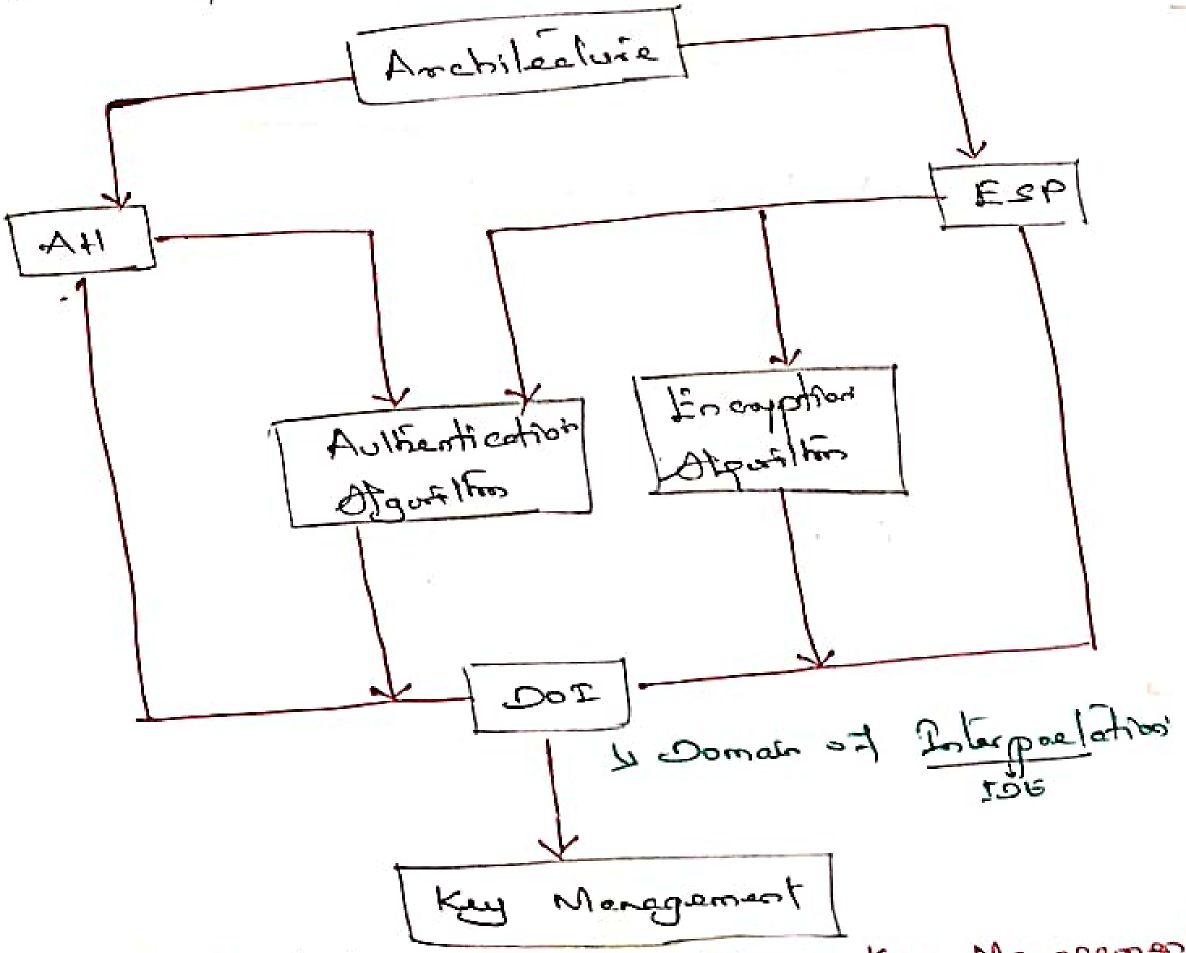
### Application of IPSec:

- ★ Secure branch office Connectivity over network.
- ★ Secure remote access over Internet
- ★ Enhancing electronic Commerce Security

### IP Security Architecture:-

- It is the Combination of two protocol

1. Authentication Header (AH)
2. Encapsulating Security payload. (ESP)

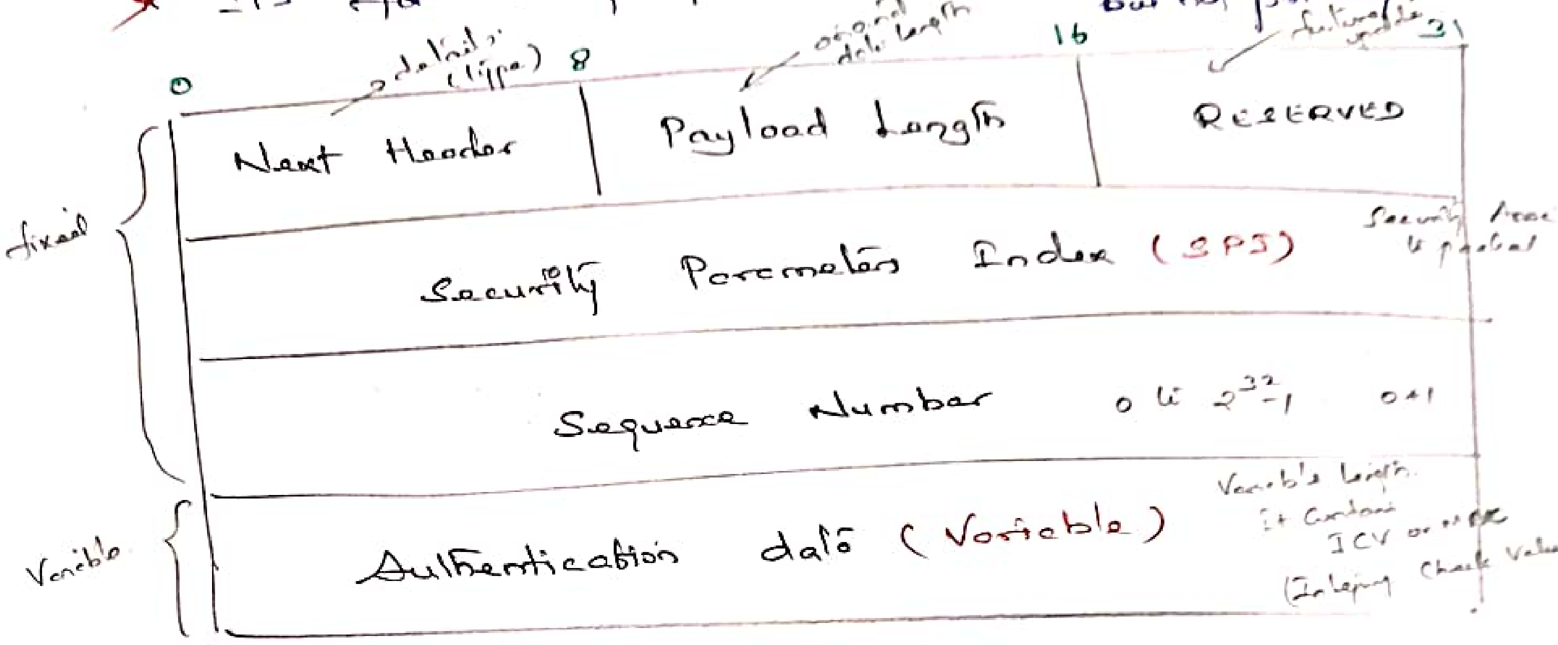


→ Internet Key Exchange (IKE) or Key Management provides message Content protection and also an open frame for implementing standard algorithms.

(20)

## (1) Authentication Header :- (AH)

* It's for integrity and authentication, but not privacy



— 32 bits.

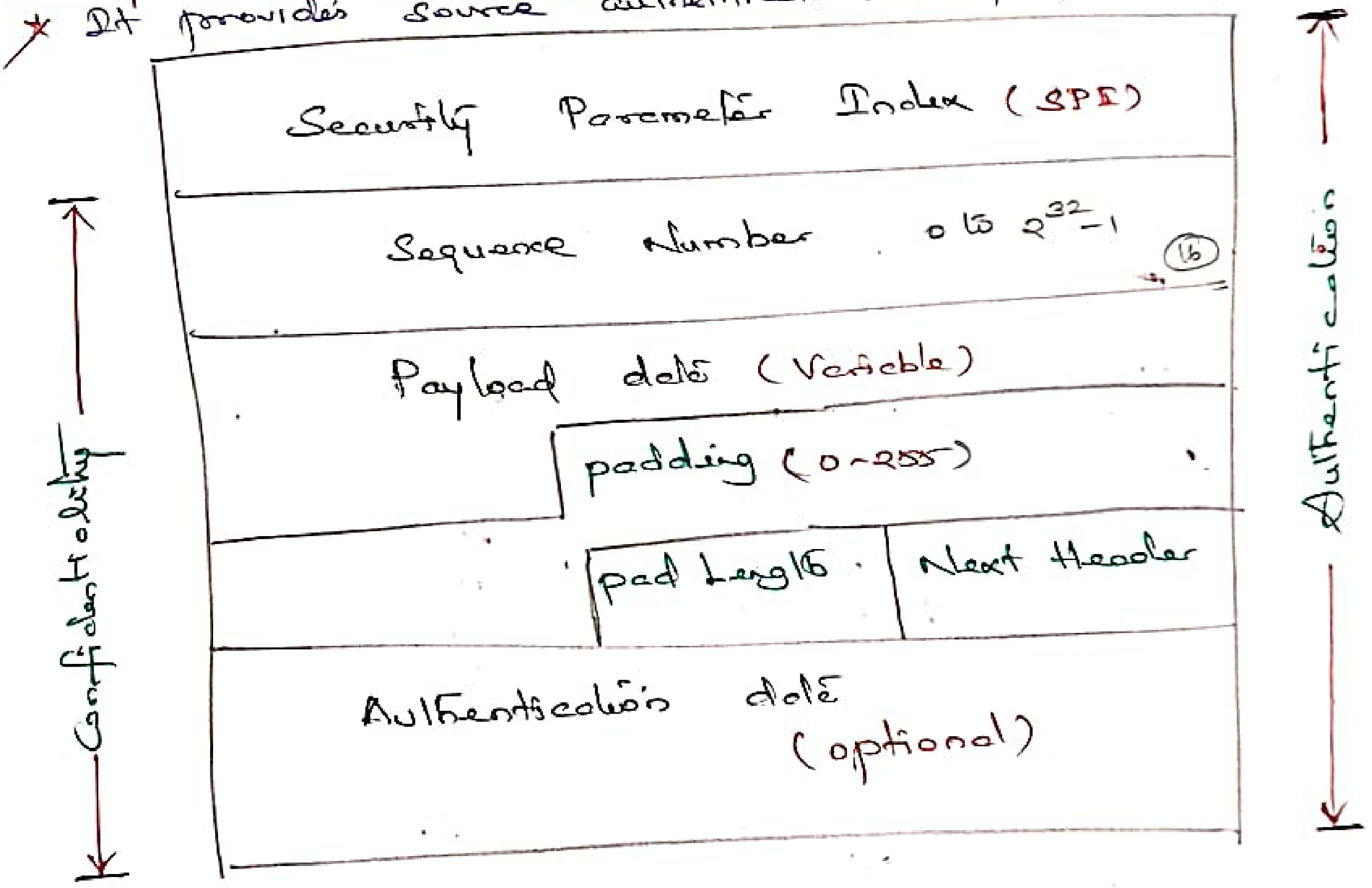
(0-31 bits)

| 0 — 8 | 8 — 16 | 16 — 31 |
|---|---|---|
| Next Header | Payload Length | RESERVED |
| Security Parameters Index (SPI) | | |
| Sequence Number 0 to $2^{32}-1$ 0+1 | | |
| Authentication data (Variable) | | |

details (type)
original data length
future use
Security Assoc. to packet
Variable length. It contains ICV or MAC (Integrity Check Value)
fixed
Variable

## (2) Encapsulating Security Payload :-

* It provides source authentication, Integrity and privacy.



| | |
|---|---|
| Security Parameter Index (SPI) | |
| Sequence Number 0 to $2^{32}-1$ | |
| Payload data (Variable) | |
| padding (0-255) | |
| pad Length | Next Header |
| Authentication data (optional) | |

| Layer | Communication protocols | Security protocol |
|---|---|---|
| Application | HTTP FTP SMTP | PGP, S/MIME, HTTS |
| Transport | TCP/ UDP User data gram protocol | SSL, TLS, SSH, Secure Shell. |
| Network | IP | IPSec |

- The popular framework developed for ensuring security at network layer is Internet Protocol Security (IPSec)

- IPsec works from one n/w entity to another n/w entity.

- Security can be adopted without requiring changes to individual user/ computers/ applications.

- The most common use of IPsec is to provide a Virtual Private Network (VPN).

- It is widely used to provide secure communication between network entities, IPsec can provide host - to - host security as well.

- IPsec protects the entire packet presented to IP layer including higher layer header.

## AH Protocol:

* AH provides both Authentication and integrity Service.
* AH is implemented in one-way only.
* Authentication along with integrity AH covers the packet format and General issues.

## ESP Protocol:

* ESP provides a Confidentiality Service.
* ESP is implemented in two ways.
  - → ESP with optional Authentication
  - → ESP with Authentication.

Sequence Number:- Unique Sequence numbers are allotted to every packet so that on the receiver side packets can be arranged properly.

Security parameter Index:- It is used to give a Unique number to the Connection built between the client and Server.

payload data:- payload data means the actual data or the actual message. It is an encrypted format to achieve Confidentiality.

Padding:- Extra bits of space are added to the original message in order to ensure the Confidentiality.

Next Header:- It means the next payload or next actual data.

Authentication Data:- Authentication data field is optional in ESP protocol packet format.

## System Security at Network Layer :-

Mainly we have to notice three Concepts:

(i) System Security

(ii) Types of attacks

(iii) How we secure the system from those type of attacks.

Defn: System Security:-

* System Security is to Secure the system from the cyber attacks.

* In these malware play the key role.

* Malware means, it is a piece of software that can be designed for system damage (or) hacking the data (or) disturb the system and these can be harm the system in Multiple ways.

Types of attacks :

There are 8 types of attack, we can call as malicious software (or) man-in-the-middle attacks.

1. Worms
2. Virus
3. Bots + Botness
4. Trojen Horse
5. Rrand some ware
6. Adware + Scams
7. Spyware
8. Spam + phishing

## ① Worms :

It's Using FACK webbrowsers to hacking the System.

Eg: Phishing attack

It destroy systems & destroy the whole network.

Ex:. By Using facky web browsers Can hack the data and gaining Sensitive information [BANK].

impacts of worms:

① modify and delete files

② Inject malicious softlware into Computers

③ steel your data

④ Replicate themselves over.

## 2. Virus:

Eg:. Virus on your device [mobile] damage the system through the Code.

→ Repelion :- That means no: of times Code Can be Send to your device by these impect the System is healed and damage that System.

→ Viruses are typically attached to an executable file (or) Word document,

→ Most people aware that a $\boxed{.exe}$ file extension Could leads to issues.

→ It hacks your application and uses your own device apps to sneeze all over any one sending. out infected files to your friends (or) Clients

→ These Virus form from System to System.

## 3. Bots & Botness :

**Bots:**

→ After hacking the information that System Can operate through the remote, by Hackers.

→ By these million of Systems Can be Hacked.

→ It is popularly Used by the Hackers.

**Botness:**

→ It means Some bogus request Can be Send by Hackers, repeatedly, by this, System Can be damaged by repeating working of device.

Ex:. Key logging,
Screen shots
4
web Cam access.

## 4. Trogen Horse:

* it doesn't have replicate like Virus.
* These Can be Used for steal the information and Can be Used for.

→ Delete & Modify and Capture data

→ Spy on your device

→ Gain access to your network.

## 5. Randsom Ware :-

Initially Hacker hack the data (or) files and Hacker's demand the people, for wanting this files you pay money to me.

To reduce the risk (or) Randsomeware attack.

→ Always keep your operating Systems upto date.

→ Keep your antivirus Software upto date.

→ Back-up your most important files.

→ Don't open unknown browsers (or) files.

## 6. Adware & Scams:

→ Adds displays:

Ex: You choose any youtube (or) Movie downloading during that time some adds will displays.

Suppose we can click on that links (or) adds by this type of adds that particular channel gives money to the youtubers.

## 7. Spyware:

→ While Using internet explorer the Spyware's can be installed automatically

Ex: Sonic Music,

T. Amaranathu. M.Sc.,(Maths)., M.S.,(Software Systems)., M.Tech., (CSE)., (PhD).,

→ due to the installation, they can notice user's online activities, data & personal information.)

These Spyware works at the background that user never notice.

## 8. Spam & phising:-

→ It is a common method of cyber attack

→ phising is successful, since the emails sent, text message and web links created look like from trusted source

→ These are sent by criminals to fradulently aquire personal (or) financial information

→ Generally these malware enter to the system through these spam.

→ If you have noticed any of the following its confirmed to be that your device is attacked (or) malware is spreaded in your device.