(c) login credentials (eg: FB, EMail, GMail).

IP Security:

=> Internet Protocol Security.

=> It's job is to secure the communication of two parties when they are communicating our a IP network - Secure the communication includes confidentiality, integrity and authentication.

=> Here for that we use two protocols:-

1):- Authentication Header (AH)

2):- Encapsulating Security payload

Authentication Header: responsible for providing security to the message / data packets.

Encapsulating Security payload: responsible for providing confidentiality / using encryption algo. so that no-one can read it.

=> IP security also have an DOI (Domain of interpetation) which has identifiers that identify the algos. that are used and approved to use.

Date:

Security Association:

=> It is a set of rules relationship that is established b/w two parties and they describe how the security services is utilized so that the two parties communicate securely.

=> There are 7 parameters regarding to it:

i):- **Security Parameter Index:-** This is the type of identifier that is use to uniquely identify the Security Association(SA) from many SA's.

ii):- **Security Protocol Identifier:-** If we take one SA into consediration and init we can implement which of the protocol e.g:- either it is AH or ESP, the security protocol identifier is used for that identification

iii):- **Sequence number Counter:-** A 32-bit value used to generate the sequence number field in AH or ESP headers.

iv):- AH information:- Authentication algo, keys, key lifetime and related parameters being used with AH.

v):- **ESP information:-** Encryption and authentication algo, keys, initialization values, key lifetime and related parameters being used with ESP.

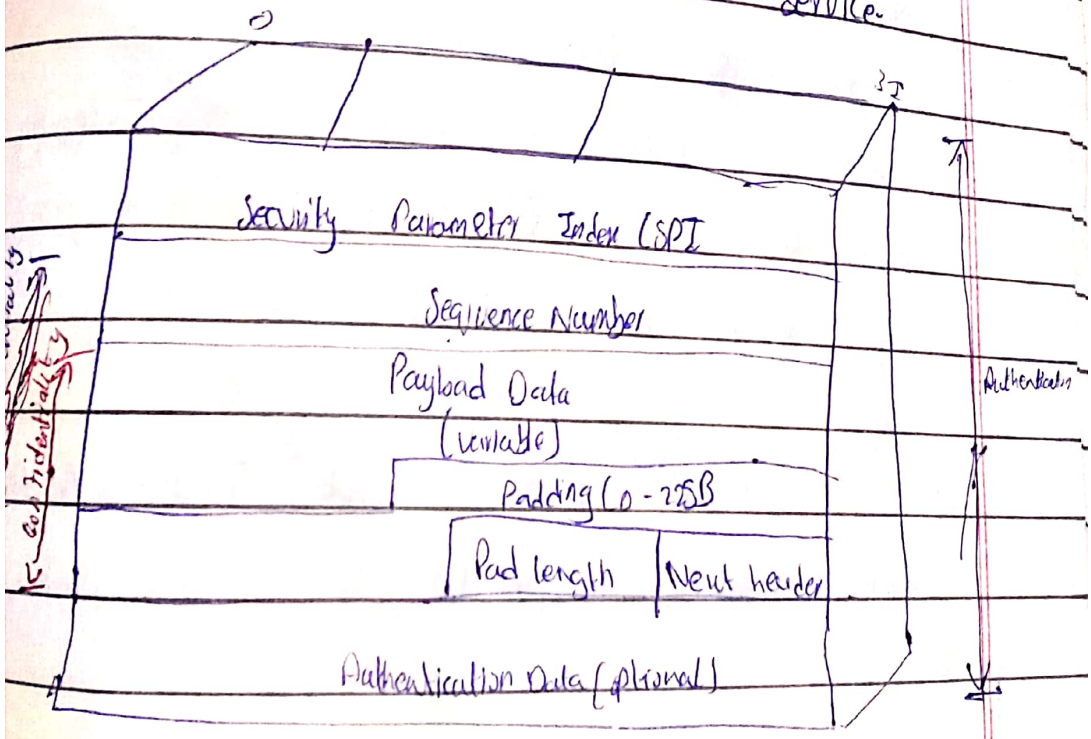
Day: M T W T F S

lifetime of this SA: A time interval or byte count after which an SA must be replaced with a new SA (and new SPI) or terminated.

IPSec Protocol Mode: Transport and Tunnel Mode.

ENCAPSULATING SECURITY PAYLOAD:

The ESP provides confidentiality services including confidentiality of message. As an optional feature ESP also provide an authentication service.



SPI: Identifies a security association

Sequence Number: A monotonically increase counter value.

Payload Data (variable): It is the data that is being encrypted before sending it is of the variable length.

Day: M T W T F S

Date: / /20

:: **Padding (0-255B):** Suppose we have an encryption algo that takes plainText as block and every block size of 64B but we have the plain text of 62B so, to that we use the padding to convert it into 64-B. Similarly we can do if for multiple blocks.

:: **Pad length:** Numbers of bytes used for padding, we can write here.

:: **Next Header:** Tells what type of data we have in the payload data field.

:: **Authentication Data:** In it we use Integrity check value that will chk weather there is any undesired modification or not.

TRANSPORT Mode and TUNNEL Mode:

Transport Mode: provide protection to upper layers protocols That is.

Read from Book.