UNIT-V

E-mail Security

* What is e-mail Security:-

as a platform for delivering viruses, spam. and phishing attacks, email is promient with attackers.

To manipulate users into disclosing personal information they use misleading texts, culminating in identity fraud. they tempt user to user register files(or) click URL's on users computer that allows like email malware.

for threats anyone wants to penetrate network archi-tecture. and hack sensitive customer information. e-mail is often a key entry point.

the characteristics of email security are often flexible and according to the user requirements

* pretty good privacy: (PGP)

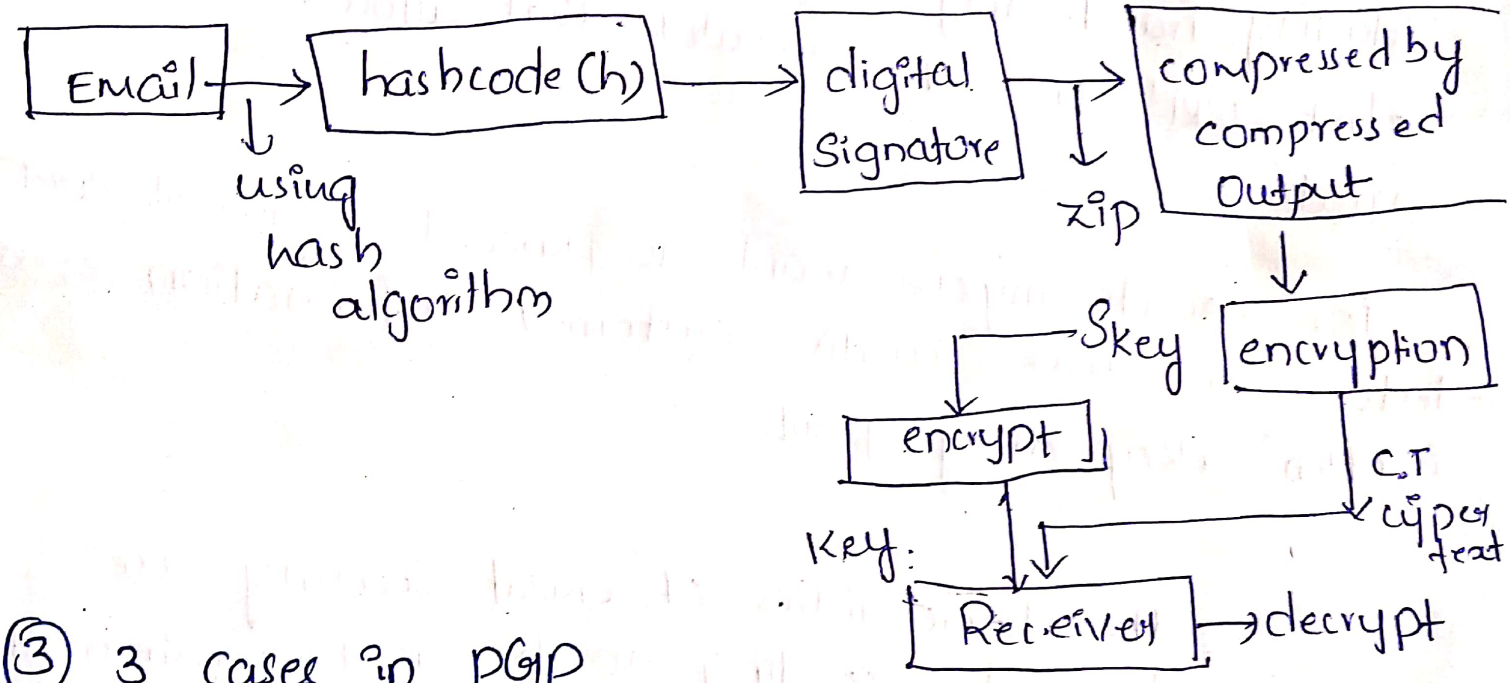
- provide email security.
- used for siging, encryption, decryption ... of texts, files, directories -- (data in emails)

* Techniques used in PGP :-

1. Hashing :- MD5, SHA
2. Data compression
3. Symmetric key cryptography
4. Asymmetric key cryptography

* Services of PGP :-

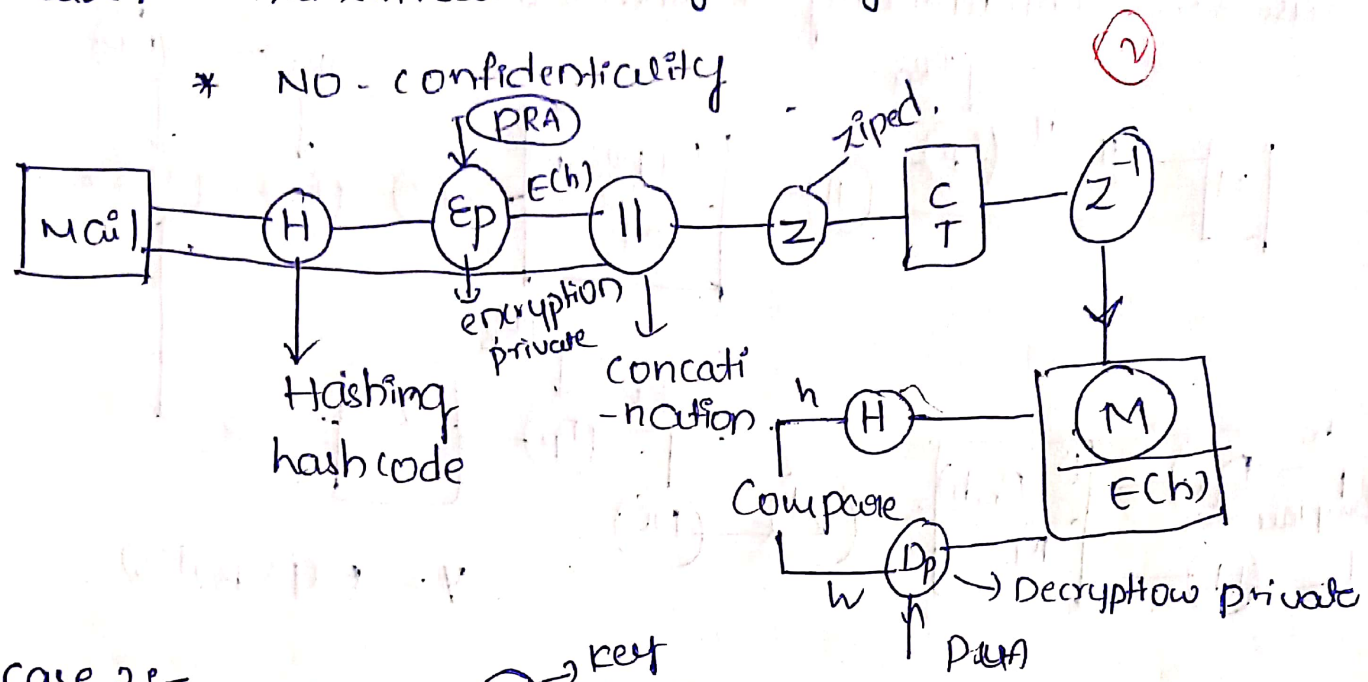
(i) Authentication
(ii) Confidentiality



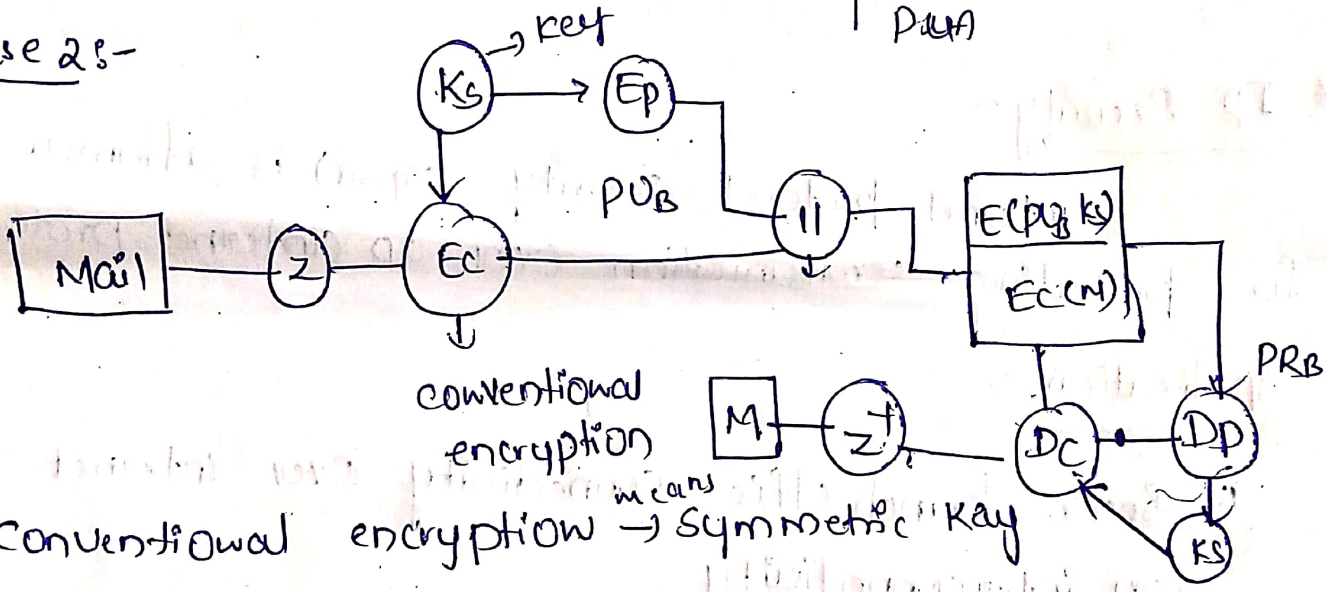
(3) 3 cases in PGP

(i) Authentication - only
2 confidentiality -
3. Authentication + confidentiality

Case 1:- Authentication + digital Signature.



Case 2:-



* Conventional encryption → means Symmetric Key

Z - zip u r information

EC - conventional encryption

Ks - Key for encryption with Ep using PU_B. (public key of B)

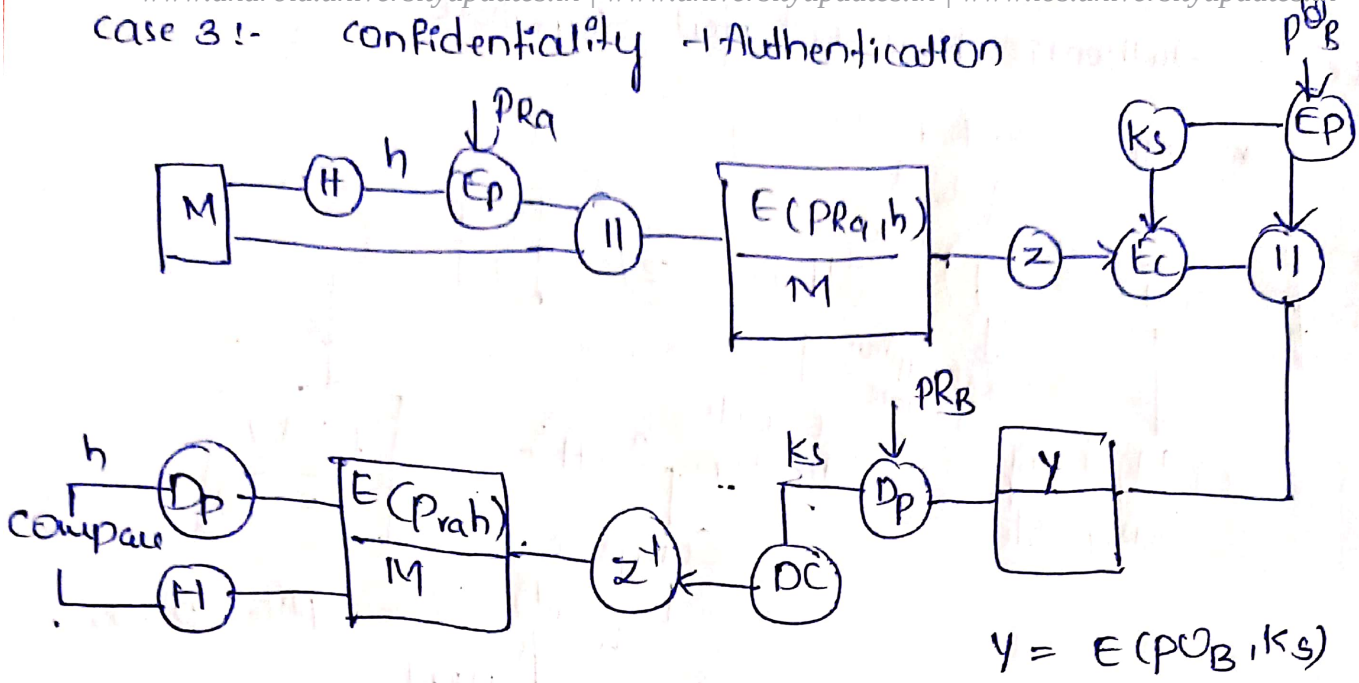
|| - concatination

Z^{-1} decompression of your data

In second case both data and key are encrypted

DC - conventional Decryption.

case 3 :- confidentiality + Authentication



* Ip Security :-

Internet protocol Security (IPsec) is a framework for protecting communication over IP (internet protocol)

Applications :-

1. Secure branch offic connecticity over internet. (or) interconnecticity

   Eg :- banks Sectors.

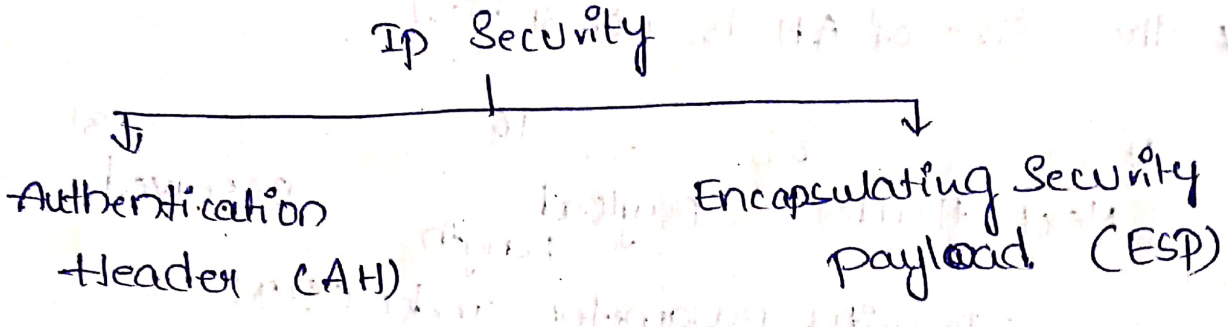
2. Secure remote access over internet

3. enchancing electronic commerce Security

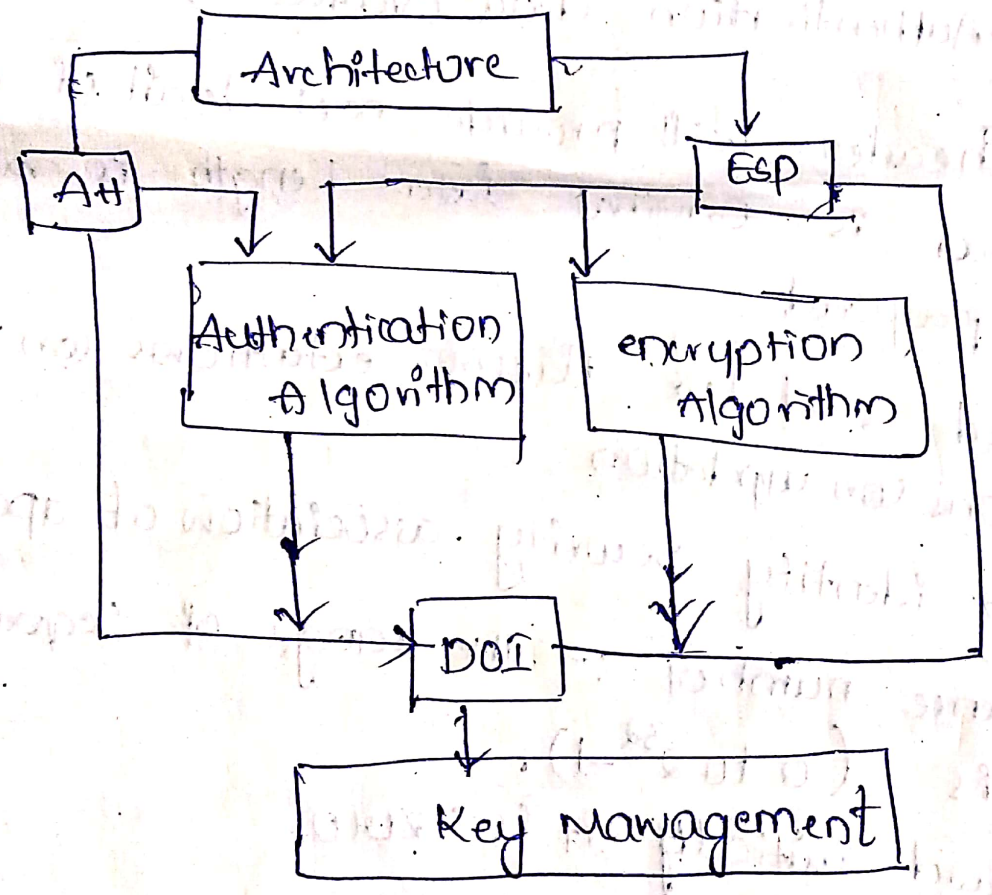
   Eg :- e-commerce Secure transactions

Ip Security architecture :- (5)

Ip Security architecture is combination of two protocols



Architecture :-

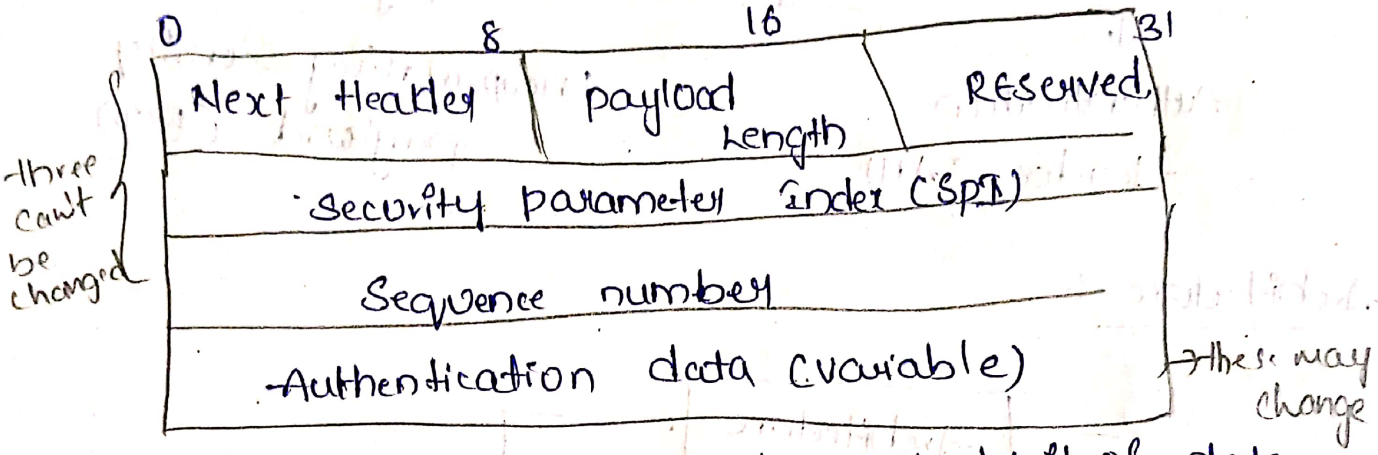


* DOI :- Domain of interpretation
  - it will have id's of all the approved authentication and encryption Algorithms

* Authentication Header :- (AH)

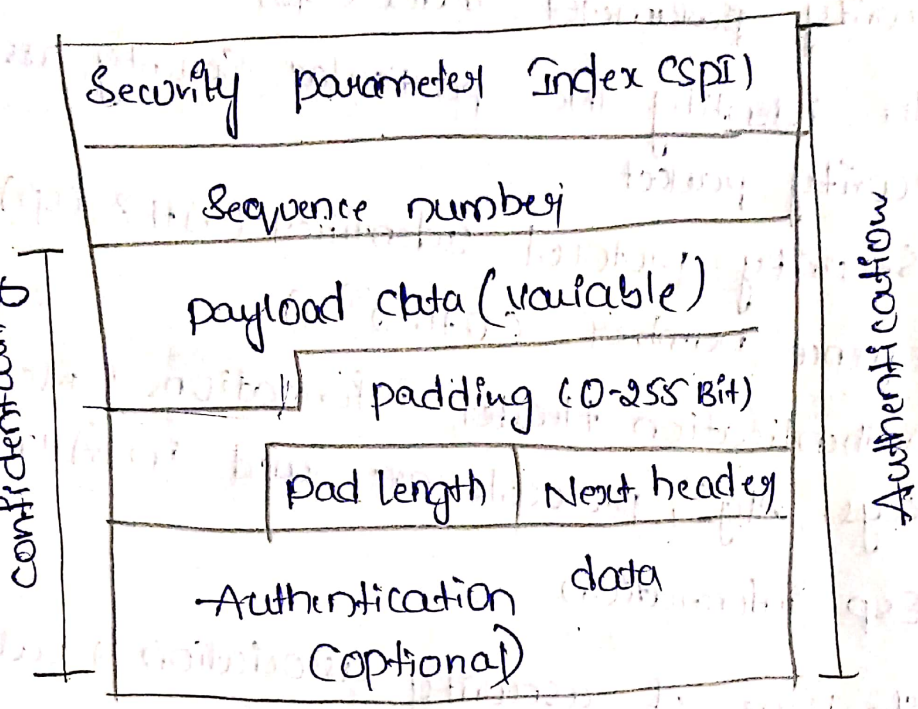
Authentication Header for Integrity and authentication

* the size of AH is (0-31 bits)



* Next header will provide next detail of data
* payload is original data length is maintained by payload
* Reserved used for future extentions or new versions or updation
* SPI → identify security association of a packet
* Sequence number :- the range of sequence number is (0 to $2^{32}-1$). and initially it is zero.
* Authentication (data) :- it contain ICV (or) MAC of packet
* ICV :- (Integrity check value) :- if there are any unwanted modification are changes done to data that determined.

* Encapsulating Security payload :-



* payload data → original data.
* padding means adding extra bit to original data
* pad length :- no. of bits at the end. how many bits are added
* Authentication data is (Optional)

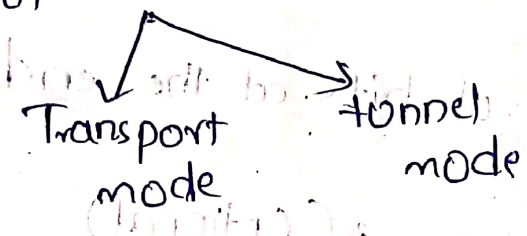
* Combining Security associations :-

* Security Associations :- (SA)

1. Security association is a contract shared between all the entities before the start of communication
2. SA specifies the protocols to be used in ipsec to ensure security.

1 Parameters of security associations:-

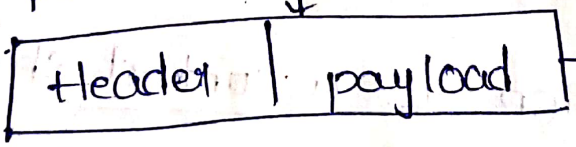
i. Security parameter Index (SPI):-
   ↳ to identify the particular security association of security packet
2. ↳ Security protocol Identifier (AH & ESP)
3. Sequence number (0 to $2^{32}-1$)
4. Authentication Header informations: means what are Keys, Alg's, protocols are used in (AHI)
5. Esp information
6. life time of security association → validity on life time of security
7. Ipsec protocol modes — 2 modes



① Transport mode :-

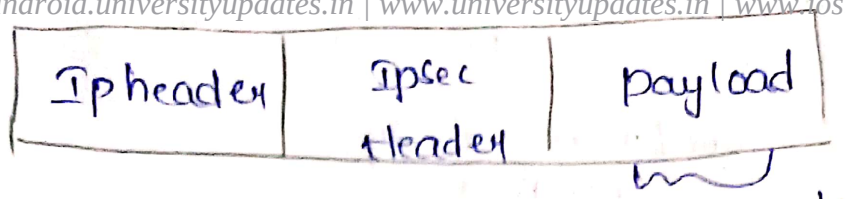
payload → encrypted
Header → not encrypted

* Initially packets are



* a packet will have both Header not encrypted payload is encrypted

later in transport mode we insert Ipsec header in b/w

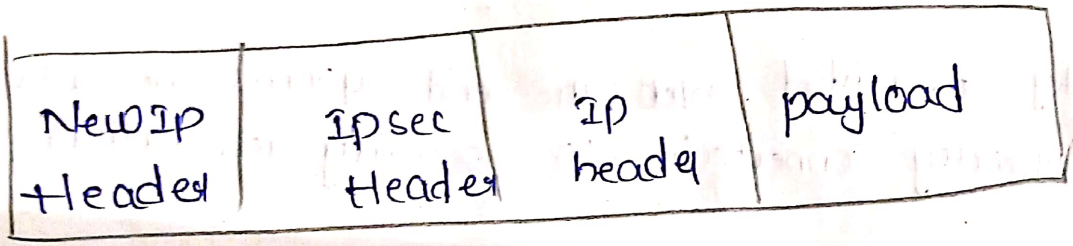


* direct host to host communication

* Tunnel Mode:-

payload } both are encrypted
Header

(i.e: entire packet is encrypted as a result, new IP header is generated)



- Gateway to gateway communication is done
  - for sender → Receiver.

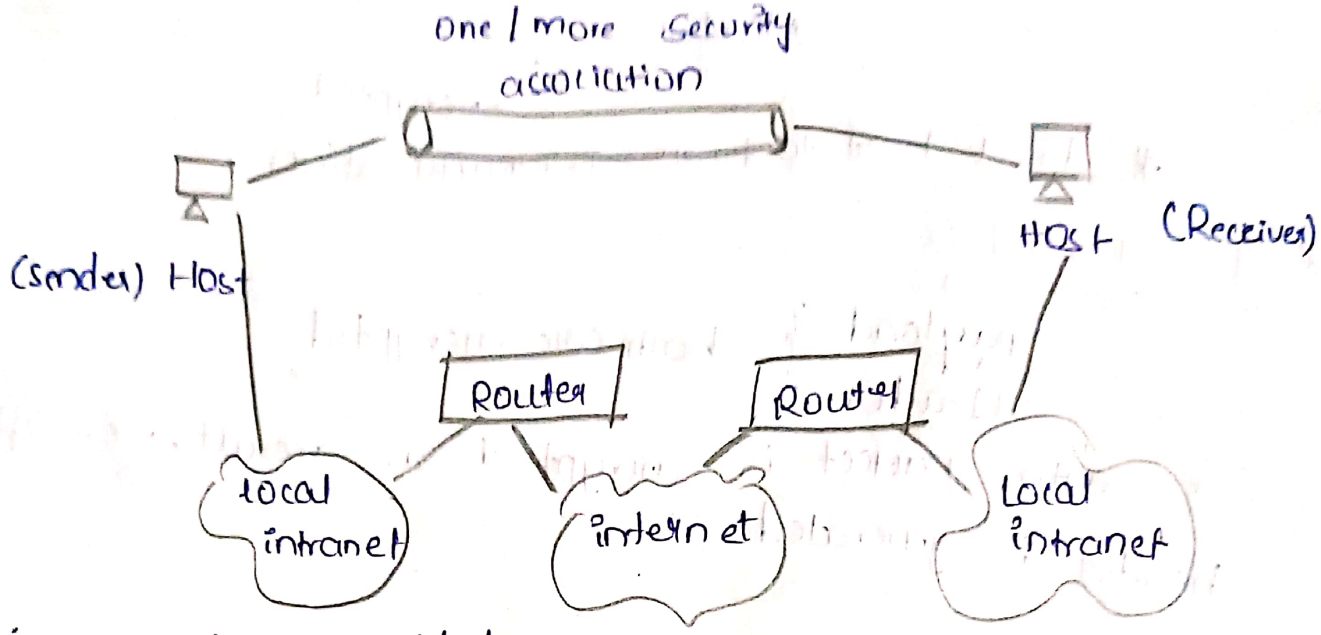
* Combining Security associations :-

with an individual SA's we can implements either (AH/ESP) but not both.

* when both are required we need to combine multiple SA's.

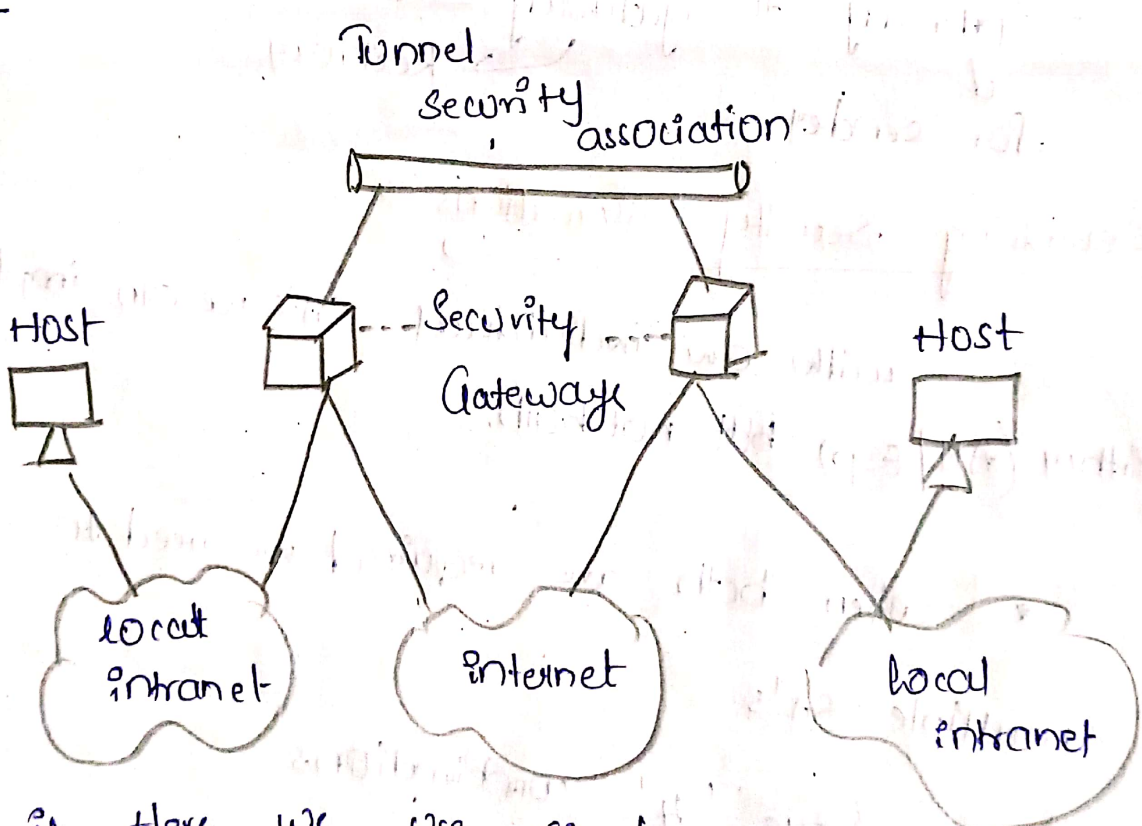
* we have '4' combinations

Case 1 :-



(i) Security provided bleo the end systems, because host is directly connected to security association.

Case 2 :-

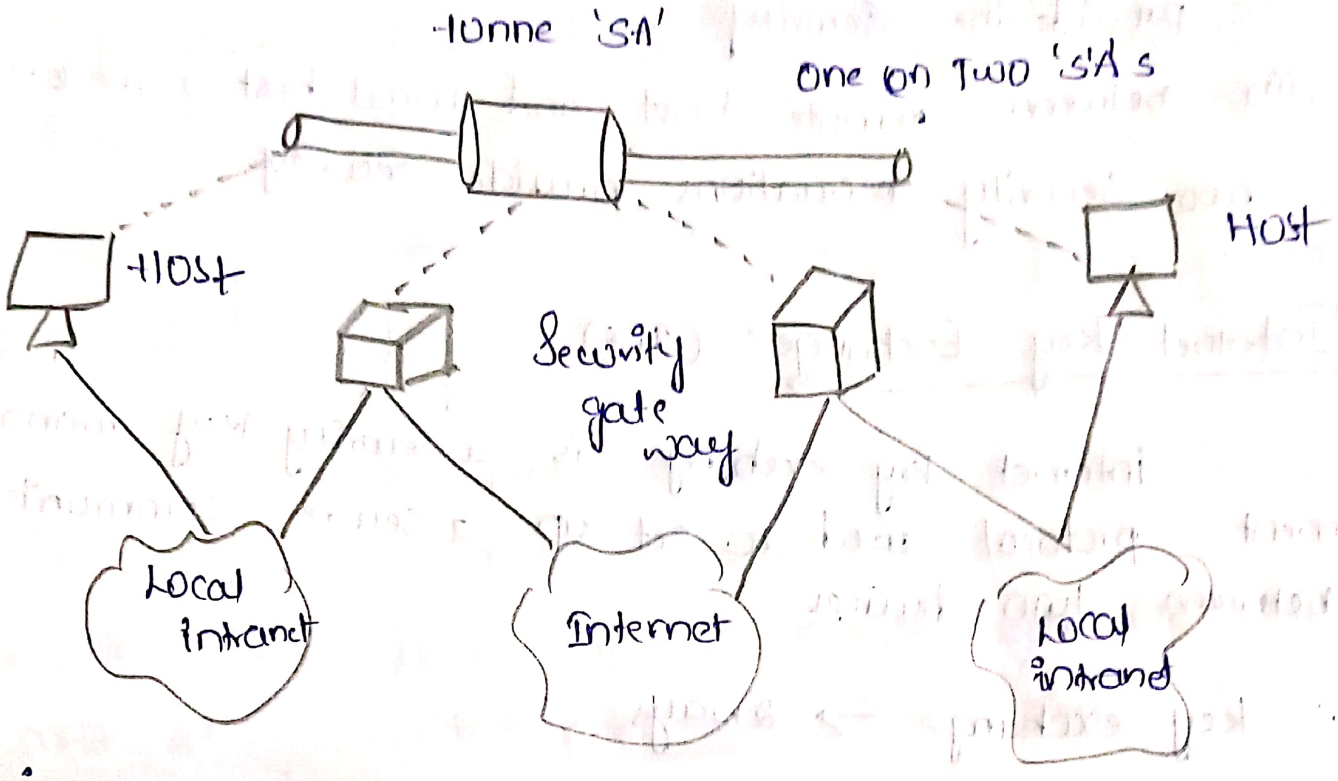


(ii) Here we use single tunnel Security association

But here 'SA' connected to the gateways connected to host local (intranet)

(iii) mostly used in VPN

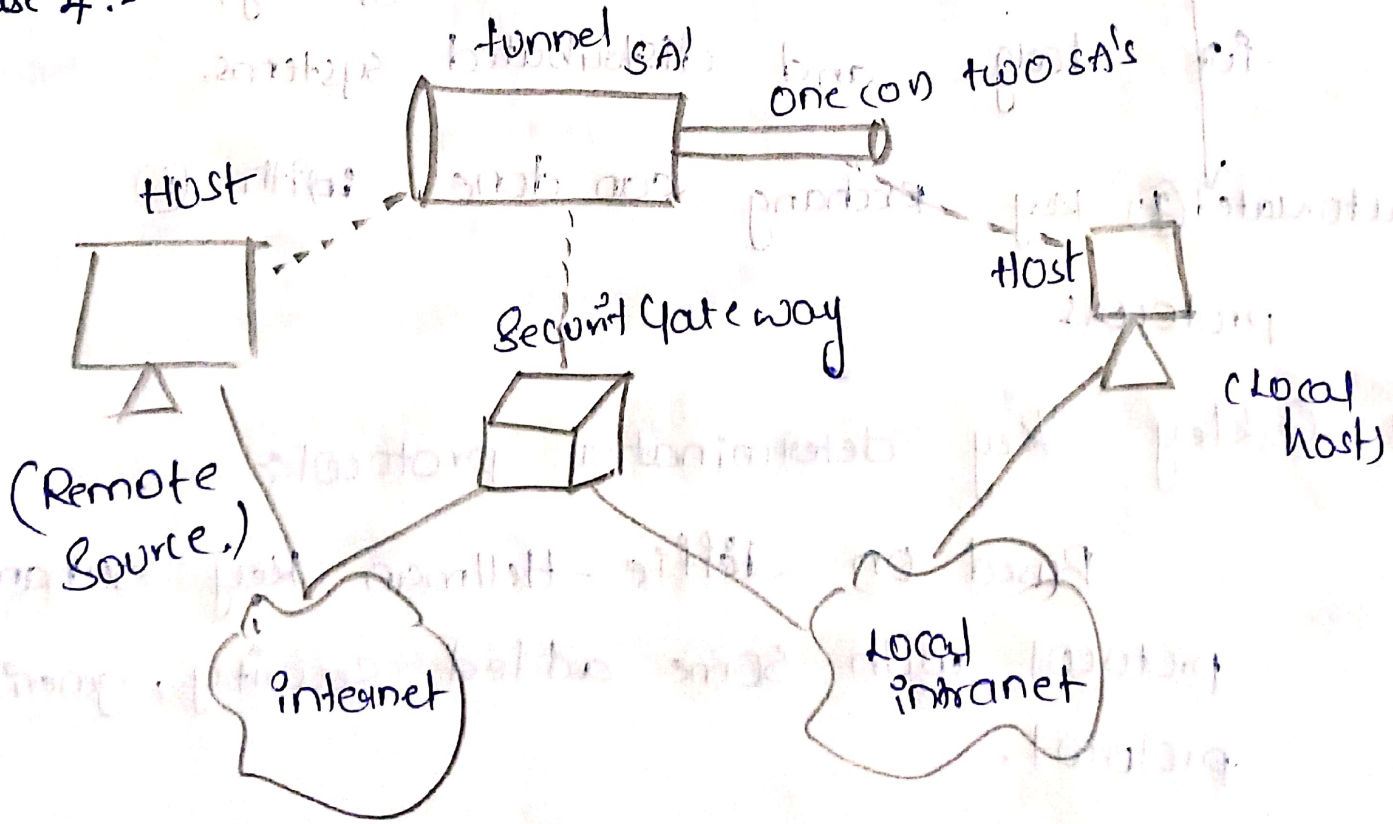
Case 3 :-



(ii) combination of case 1 and case 2

(ii) tunnel security for Gateways + Security association to end to end systems also

Case 4 :-



(i) used in remote sensor's

(ii) between remote host and Gateway → tunnel mode provide the security

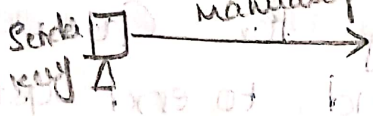
(iii) between remote host and local host → one on two security associations provide security.

* Internet Key Exchange :- (IKE)

Internet key exchange is a security key management protocol used to set up a secure communication between two devices

* Key exchange → 2ways

(i) Manual :- manually configure each system, small, and static.



→ system admins can do

(ii) Automated :-

for large and distributed systems.

on demand creation of keys

automated (2) Key Exchang can done with: (2)

protocols

(i) Oakley Key determination protocol :-

Based on diffie-Hellman Key exchange protocol with some added security, generic protocol.

② ISAKMP :- (internet security association key management protocol) :- ④

- provide a framework for key exchange and provides protocols specific support

* ISAKMP is done in two phases

phase 1 :-

(i) exchange of proposals for security services. (encryption algorithm, authentication alg etc)
- when both ends of the tunnel agree to accept a set of security parameter then phase ① .

* In phase ① we have two modes those are
  (i) main mode
  (ii) aggressive mode

phase ②

once participants established a secured channel in phase ① they move to phase ② - here security association are negotiated

- decided to use 'AH'/Esp and also select with algorithm to use
- phase ② always operates in ② quick mode.

* S/MIME protocols:-

* Mime protocol :- "multipurpose internet mail extention"
* previously. emails could be sent only in NVT - 7bit ascii format.
  cie: audio, /video / images etc could not be sent)
  ∴ mime is introduced.
  ↓
  add on which allows us to transfer non-Ascii data over mail (other types of data)

Smime :- Secure mime, extention to mime protocol.

1) encrypts emails and provide security
2) allows us to digitally sign on our email
3) Uses asymmetric key cryptography

functions of S/mime

i) Authentication ii) message integrity
iii) non-Repodiation - can't deny the message
iv) privacy
v) data security

* Security services of S/Mime :-

1) Security of services of S/Mime are

   i) Digital Signature

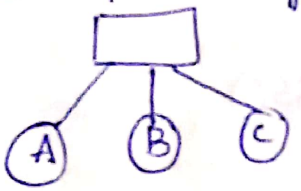
   ii) Message encryption. → (write in detail about both for exam)

* Case Studies On Cryptography and Security :-

i) Secure Multiparty calculation →

when data is distributed in network, it provides a protocol : so that no individual can see other parties data

In General it enable data scientists and analysis to compute data privately without exposing it.



Example :- if we want calculate the average salary of (3) employees then

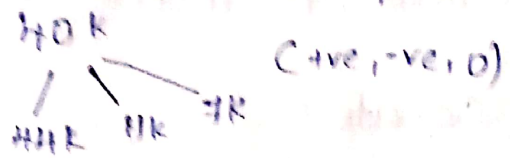
without - this protocol - data should be revealed

with this protocol - data need not be reveled

functionally F(A,B,C) = Average (A,B,C)

We have calculate average salary of A,B,C without divided into three parts.

If A's salary is 40K then using additive sharing 40K is divided into (3) parts



and B & C also same process

	A	B	C	
A	(44)	-11	7	40K
B	-6	(32)	24	50K
C	20	0	(40)	60K
	58	21	71 → cipher	

original → (40+50+60) = 150

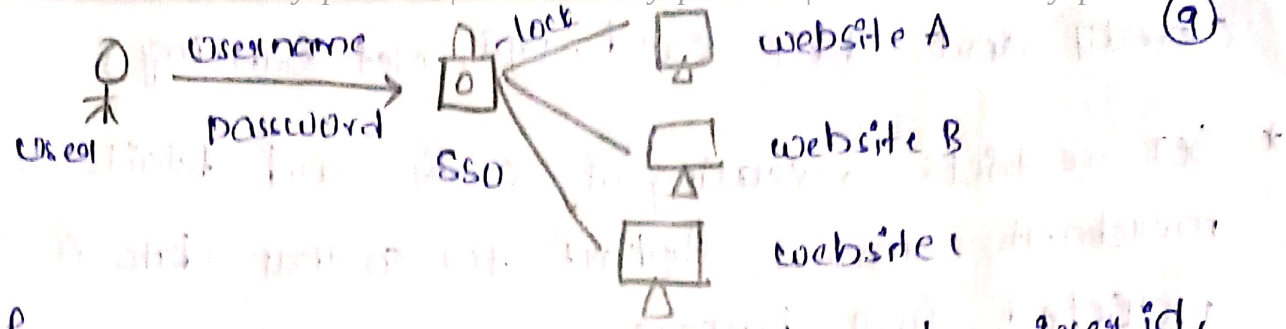
total salary = 58 + 21 + 71 = 150

average = 150/3 = 50

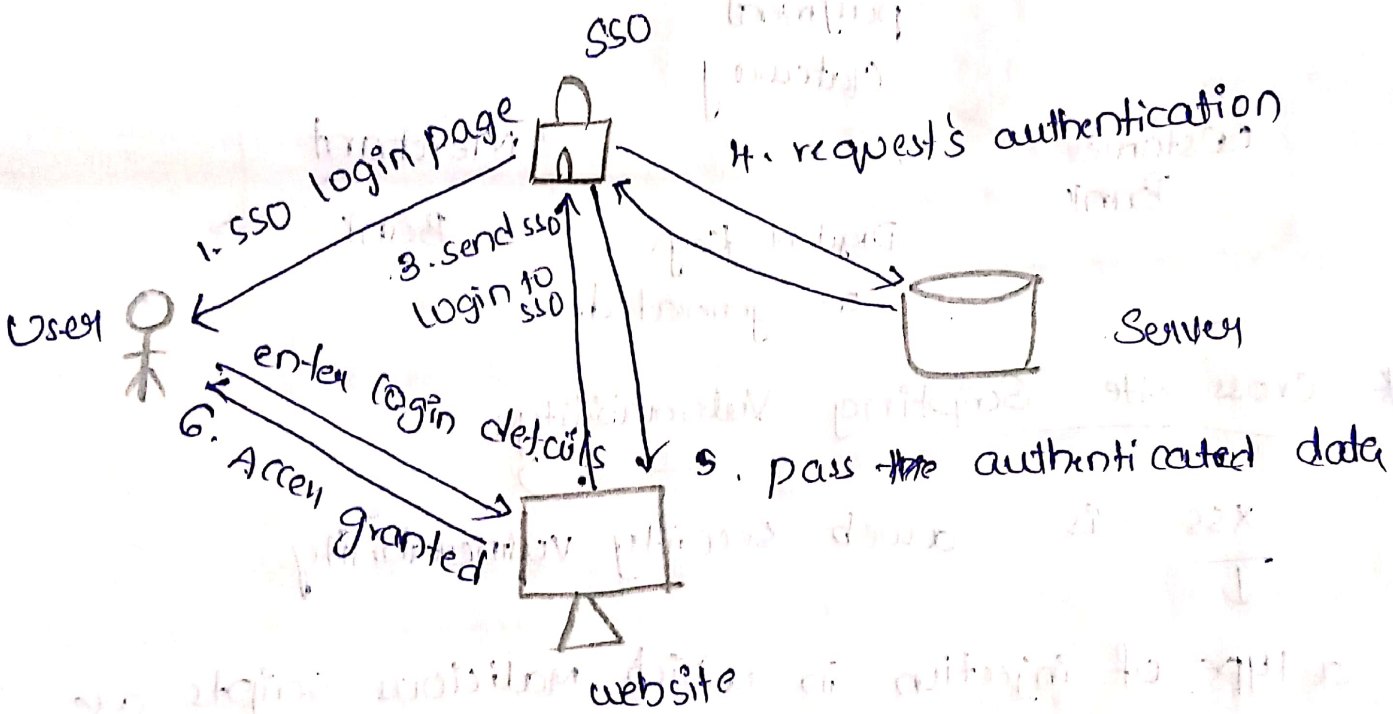
* Single Sign On :- (SSO)

- SSO in an authentication scheme where users can securely gain access to multiple applications and website only with single user name and password.

Example :- One Google account it provide services like Gmail, docs, drives etc.



* If no SSO then every time you enter user id, and password every-time
* with SSO we no need to give (or enter id & password different web sites
- it is very important to protect SSO. for that we we used MFA (multifactor authentication)



* Secure inter branch payment transactions :-

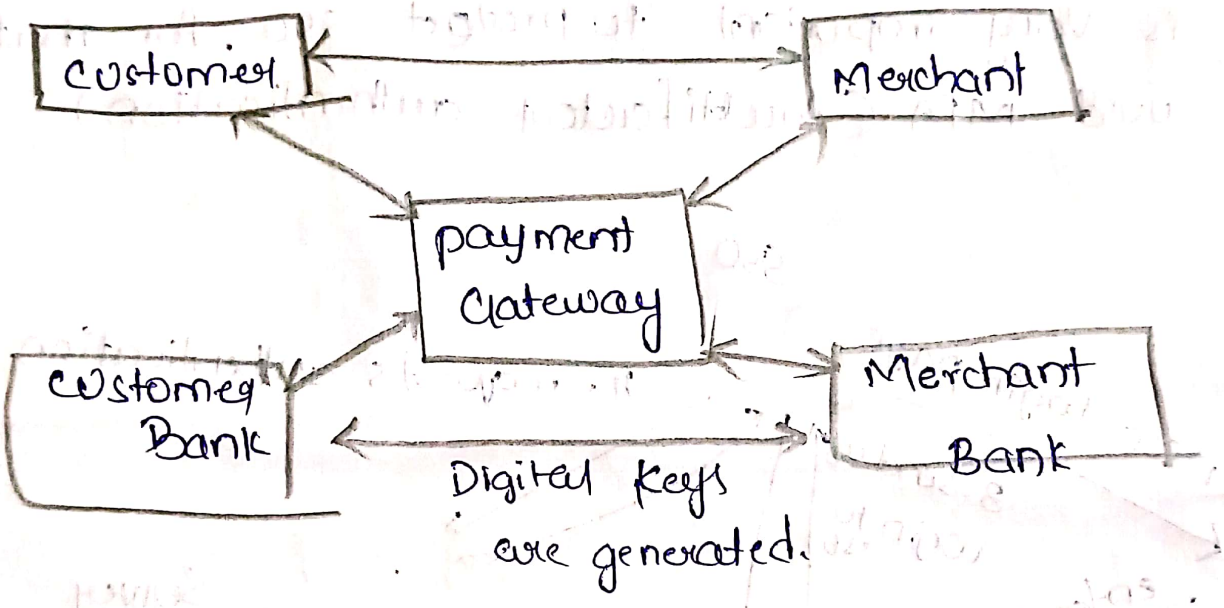
done with the help of Secure electronic transaction (SET)

SET protocol :- this protocol ensures security and integrity of electronic transactions

(credit and debit card, UPI, Net banking)

* SET restricts revealing of credit card details to merchants (amazon, flipkart etc) so that data is protected from hackers.

- implemented with help of digital signature.



* Cross site Scripting Vulnerability :-

XSS is a web security vulnerability

↓

a type of injection in which malicious scripts are injected into trusted websites

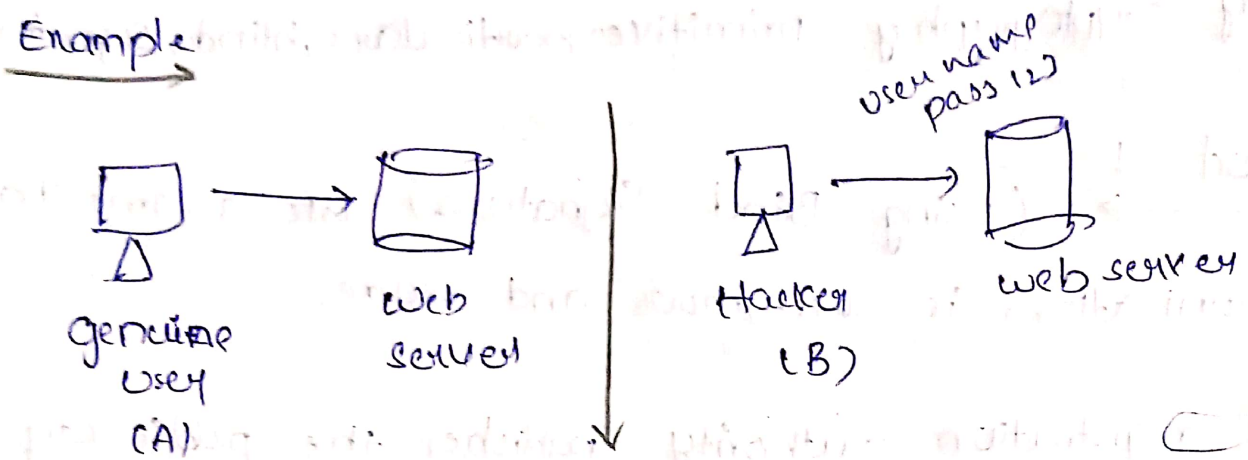
examples :- Data enters into website / application through an untrusted source (in form of a web request)

↓

(javascript, html, etc)

- xss vulnerabilities are easy to spot and they have high impact on your website.

Example:



* Electronic voting :-

An electronic voting system work as follows before voting a voter must first communicate with a registration authority. who provides the voter with a token. this token is used to vote.

Goals of electronic voting

1) correctness :-

1. only authorized parties can vote ie; registed voters.
2. no voters vote more than once
3. no voter can replace other votes
4. the party in charge of tabulation cannot change the outcome

(ii) Verifiability :- universal (or) private

(iii) Uses anonymity 4. Receipt Freeness

using cryptography primitive particulars, blind, signatures

Method 1 → (using Blind Signatures) We assume that communication is anonymous and secure.

(i) registration authority publishes the public key 'PK'

(ii) voter picks a random number that become their ID, and appends the candidate.

(iii) voter sends their personal information along with blinded versions of the tokens.

(iv) the voter unblinds all the signatures.

* Method (2) cryptography counters

If A and B are cryptographic counters consists of three algorithms

(i) Gen: generates $(PK, SK, S_0) \in \{0,1\}^* \times S_0$ is the initial state of the encrypted counter

(ii) Decrypt: Dec (S, SK) outputs one of $0, \ldots, B$ and $Dec(S_0, SK) = 0$

(iii) Increment : Inc (s) satisfies

Dec (Inc(s)) = Dec(s) + 1 (pk, sk) have been omitted for clarity

Definition :- A B-counter is (t, ϵ)-secure if for all t-time algorithm A.

$$Pr[A[pk, s) = Dec(s, sk) | (pk, sk, s_0)$$

Method 3 Mix nets:

In this scheme, each user encrypts their vote (using the public key of a decryption authority) and gives the to it to a mixer

the mixer then outputs a permutations of the encrypted votes along with a proof that it has been mixed correctly

for extra security, several mixers can be used ie: the first mixer passes its output to a second mixer who, passes its output to a third, mixer and so on

using a Neff mix, the proof requires about 8n exponentiations, where 'n' is the no. of voters