Solution Cryptography held on 26/11/19
IT 7th sem

Ans 1 (a) → Antiphishing tool.

(b) → Virus is a Self-Replicating prog. that infect other prog. by modifying them.

(c) Sniffing allow individuals to capture data as it is transmitted over a n/w.

(d) A Brute-force attack consists of an attacker submitting many password. It's a process of guessing pwd by hit-and-trial method.

(e) Authentication means confirming your own identity while Authorization means granting access to the system.

Ans 2 ⇒ $P = 11$, $q = 13$, ~~$A = 77$~~ $e = 11$, $m = 7$

$n = pq = 11 \times 13 = 143$

$\phi(n) = (p-1)(q-1) = 10 \times 12 = 120$

$\Rightarrow ed = 1 \bmod \phi(n)$

$\Rightarrow 11 \cdot d = 1 \bmod (120)$

$\therefore d = 11$

Now

$M = C^d \bmod n$

$C = m^e \bmod n$

$\therefore [C = (7)^{11} \bmod 120]$

$\Rightarrow C = 1977326743 \bmod 120$

$\therefore C = 13$ Ans.

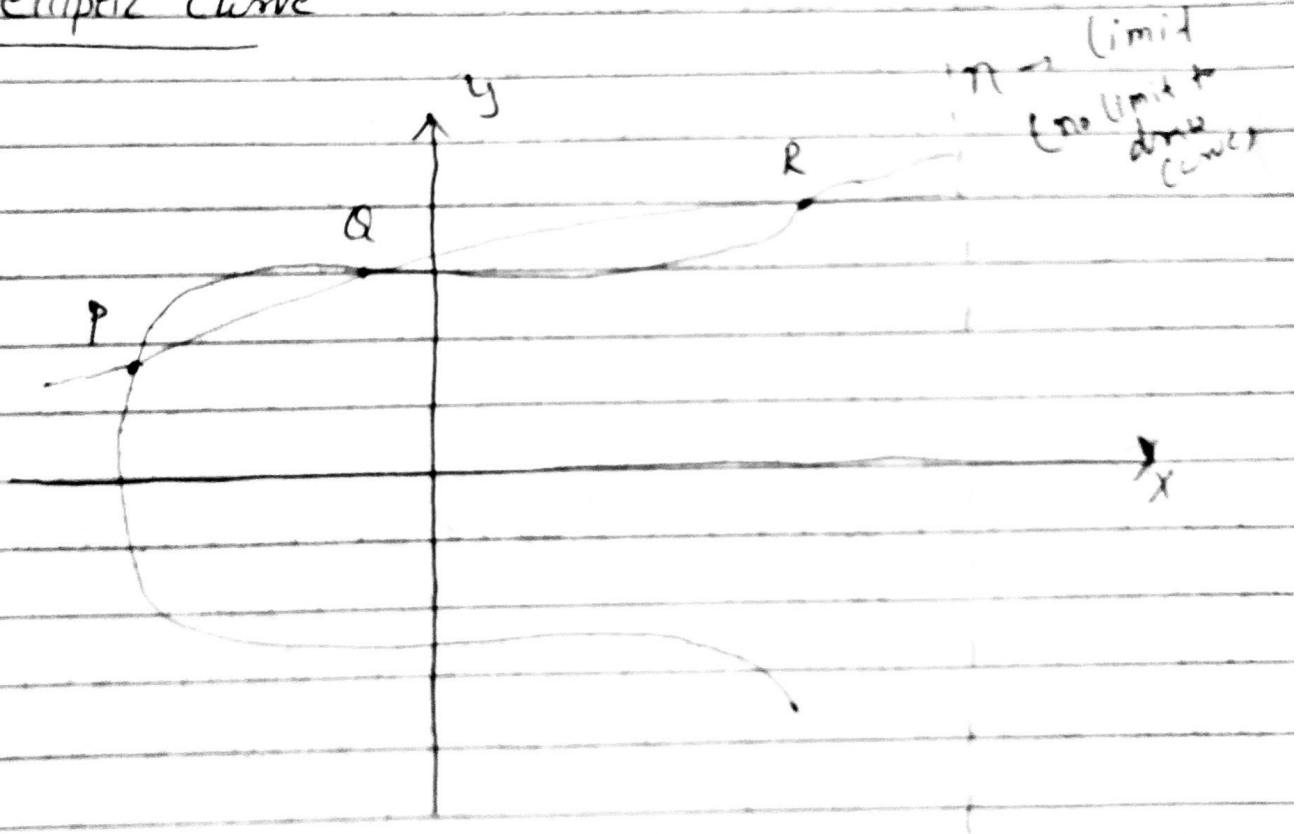
Now,

$M = (13)^{11} \bmod 120$ Ans

4=) Eliptic Curve Cryptography

=) Asymmetric / Public key cryptosystem
=) ECC provide equal security with Smaller key size
=) ECC makes use of Elliptic Curves
=) Elliptic Curves are defined by Mathematical function.
Cubic functions. → degree 3
eg → $y^2 = x^3 + ax + b$

An elliptic Curve



=) It is Symmetric to X-Axis
=) Cut Max^m of 3 points

→ Let $E_p(a,b)$ be the elliptic curve
→ Consider eqn" $Q = kP$
Where $Q, P \in E_p(a,b)$ and $k < n$
→ It should be easy to find Q given k and P.

- But should be extremly difficult to find given Q and P

⟶ ✓

⟵ ✗

→ It's a one way func" - trap door func"
→ Known as discrete logarithmic problem.

Algo

ECC - Key exchange

(a) Global public element
$E_q(a,b)$: Elliptic Curve with parameter a, b and q.
G : Point on elliptic curve whose order is large value n.

(b) USER A key Generation

Select Private key n_A : $n_A < n$
Calculate Public key P_A : $P_A = n_A \times G$

(c) USER B key generation

Select Private key n_B : $n_B < n$

Calculate public key P_B : $P_B = n_B \times G$

(d) Secret key calculation by user A,

$$K = n_A P_B$$

(e) Secret key calculation by user B,

$$K = n_B \times P_A$$

ECC - Encryption

- Let the message be M.
- First encode the message M into a point on the elliptic curve
- Let this point be P_m.
- Now this point is encrypted
- For encrypting choose a random positive integer k.
- Then

$C_m = \{kG, P_m + kP_B\}$ where G is the base point.

↓

Cipher point

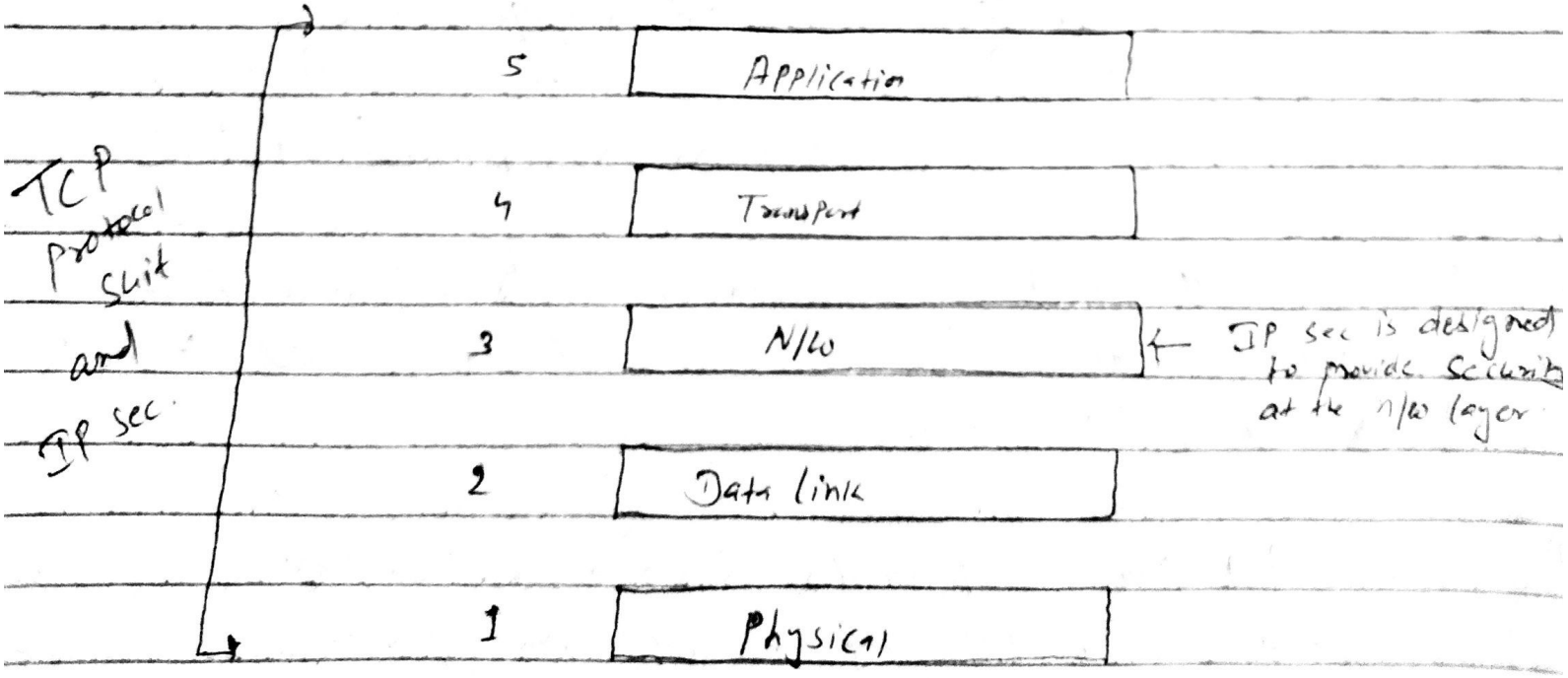
5(a)

IP Sec =)

* Stands for Internet protocol Security.
* It's an Authentication protocol works at n/w layer.
* IP Sec is a collection of protocol designed by IETF (Internet engineering task force) to provide Security for a packet at the n/w level.
* IP sec helps to create an Authenticated and Confidential packets for IP layer.

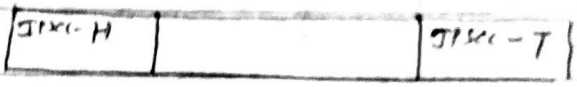
Note :=) As per CERT (Computer emergency Response Team) More than 52,000 incedents of Internet Scam in Cu Most incedents were from IP Spoofing where the attacker creates false IP address.

Thats why,
IAB (Internet architecture Board) introduces "CIA" and Encryption are necessary Security features in next generation IP ie. IPv6.



IP Sec operates at one of the two different modes ie.
(a) Transport Mode
(b) Tunnel "

→ IP sec in transport mode doesnot protect the IP header, it only protects the Information coming from the transport layer.



H: HEADER
T: TRAILER

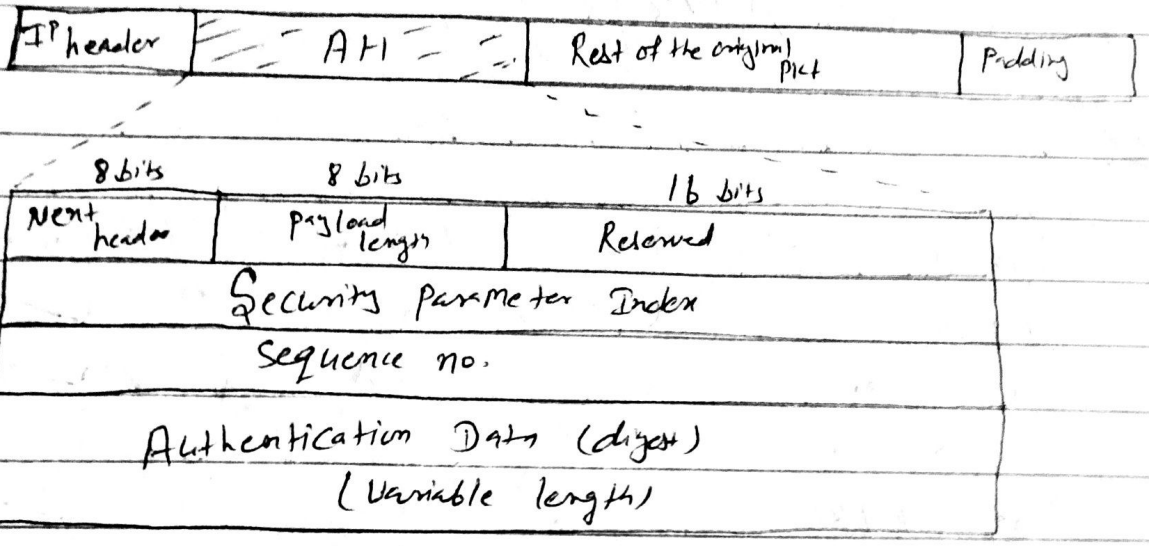
→ IP Sec in tunnel Mode protect the original IP header or both Header and Trailer is protected.

NOW

IP sec defines two Security protocols
(a) Authentication Header (AH)
(b) Encapsulating Security payload (ESP)

AH is designed to authenticate the source host and to ensure the Integrity of the payload carried in the IP packet.

The AH protocol provides source authentication and data Integrity, but not privacy.



Next header → defined the type of Payload
Like TCP, UDP, ICMP etc

Payload length → defines the length of Authentication
doesn't define the length of payload.

SPI → act as Virtual Ckt identifier

Seq. no → providing ordering info. of datagrams

Authentication Data → provide TTL (Time to live)

SSL ⇒ (Secure Socked layer)

→ It's a mechanism invented by Netscape Inc.

→ It Provide Secure Communication b/w browser and a server

→ When an information is encrypted by browser, the whole process is hidden from a user Private.

→ With SSL, a browser can encrypt a message so the contents remain

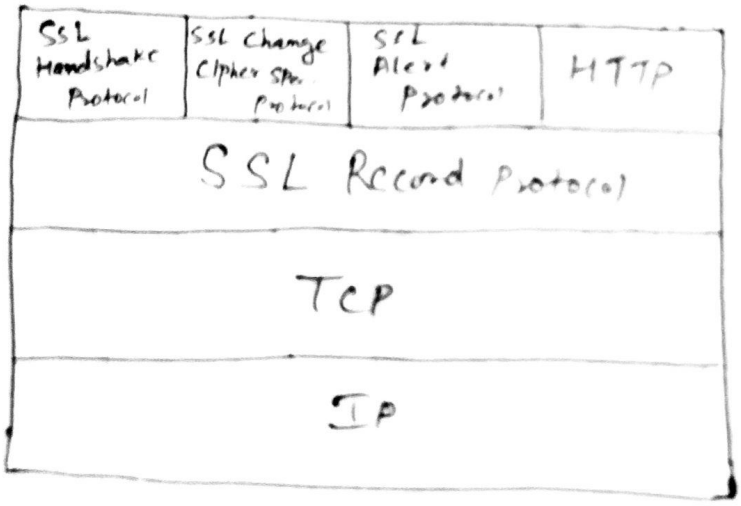
Architecture :

→ SSL is designed to make use of TCP to provide a reliable end-to-end Secure Service.

→ SSL is not a single Protocol but rather two layers of protocols

→ The SSL record Protocol provides basic Security Services to various higher layer Protocols.

→



→ Provide msg. confidentiality & integrity

PT2XDR4N