DHARMSINH DESAI UNIVERSITY, NADIAD.
FACULTY OF TECHNOLOGY.
ONLINE SESSIONAL EXAMINATION

B. Tech (CE) Sem: 6th
Subject: NIS

Roll No: CE-107
Signature:

Date: 24/03/21
Time: 9:00 am to 10:15 am
Total Pages: 11

Q-1

a) Number of Padding bits required.

$L = 3000 + (107)^2$ Roll No = 107

$= 3000 + 11449$

$L = 14,449$

$|P| = (-14449 - 128) \bmod 1024$

$|P| = (-24153) \bmod 1024$

~~$|P| = 601$~~

$\boxed{|P| = 423}$

length of Padding required

$\boxed{|P| = 423}$

b> limitations of message Authentication Codes Compared to Digital Signature

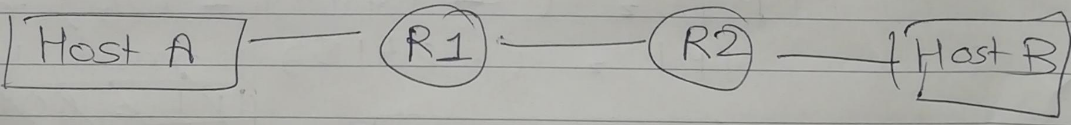
→ In Authentiation, if Data is received with modification then Integrity of Data will be violated, & in Digital signature it does not happen.

→ Where digital signature it selfc ~~so~~ Provide Authentication of message, Integrity & ~~Non-repuditio~~ Non-repudiation. So, ~~digi~~ It provide Integrity batterly.

→ Digital Signature works faster than Authentication.

→ Digital Signature provides confidentiality while Authentication do not

c>



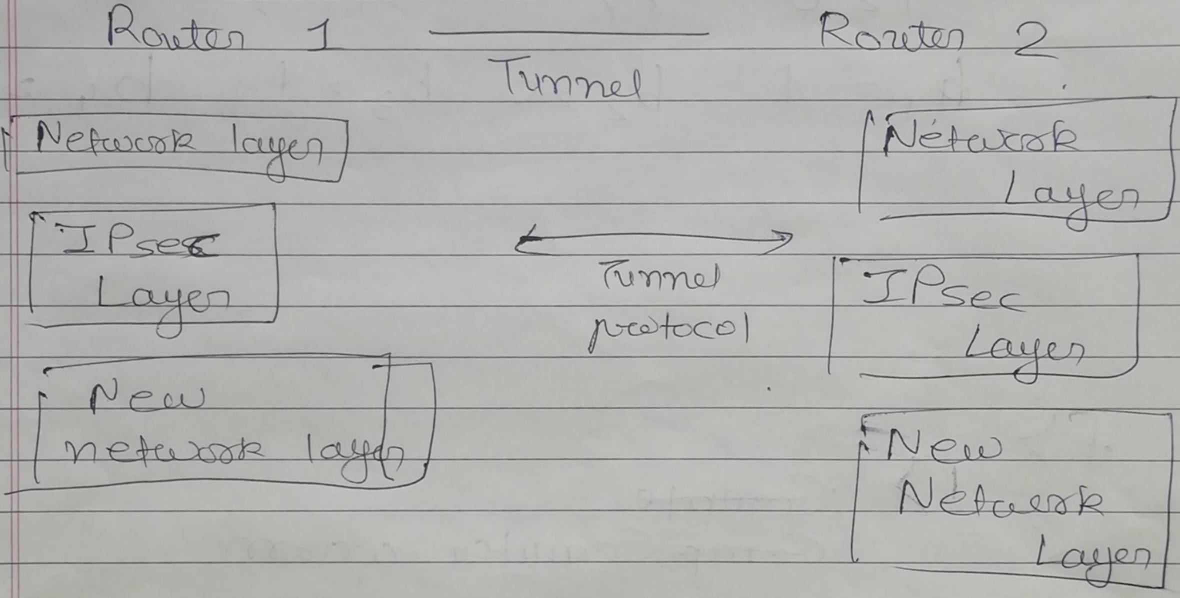
here IPsec Protocol will be In use.

It has two operation mode.

1> Transport mode

2> ~~In~~ Tunnel mode

⇒ we will use Tunnel mode here, now, In this, Entire packet is protected from Intrusion between the sender & receiver, as whole packet go through ~~that~~ imaginary tunnel.



d) to detect virus, "Hashing" will be use
at sending time & receiving time hash values are being compared.
So, if there exist any virus then, Hash value will be different.
So, ~~Value~~ Hash value at Sending & receiving time will differ & virus will be detected.

e) Roll NO = 107
Hexa = 6B.

6 → 0110
B → 1011

$a_1 = 0$ $a_2 = 1$ $a_3 = 1$ $a_4 = 0$

$b_1 = 1$ $b_2 = 0$ $b_3 = 1$ $b_4 = 1$

f) 1) ~~Compte~~
~~Comp~~ Comuter worm

2) Adware

Q-2

a) $p = 283$

$q = 47$

$e_0 = (\text{RollNO} + 2)$, $e_0 = 107+2$

$e_0 = 109$

$d = 24$

$M = 21 \Rightarrow h(M) = 21$

$r = 15$

now $e_1 = e_0^{(P-1)/q}$

$= (109)^{(282)/47}$

$= (109)^6$

~~11236 x 11236 x 11236~~

$\boxed{e_1 = 1677099910841}$

$e_2 = e_1^{d} \bmod p$

$= (16770999110841)^{24} \bmod (283)$

$\boxed{e_2 = 207}$

private key $d = 24$

public key $= (16770999110841, 207, 283, 47)$

$S_1 = (e_1^{r} \bmod p) \bmod q$

$= ((16770999110841)^{15} \bmod 283) \bmod (47)$

$= (181) \bmod (47)$

$\boxed{S_1 = 40}$

$S_2 = (((h(M) + d S_1) r^{-1}) \bmod q$

$= ((21 + 24 \cdot 40)(15)^{-1}) \bmod 47$

$(((981)(15)^{-1}) \bmod 47)$

$S_2 = (981)(22) \bmod 47$

$\boxed{S_2 = 9}$

$$V = \left[P_{283}^{\cancel{mx}} \times 47 + 283^{x} \right] \bmod 283$$

$V =$

$$\boxed{V = .40}$$

Q-3

a) Services provides by SSL to uper layer payload

→ fragmentation of Data: SSL fragment received data into 2 ^ 14 bytes

→ ~~Compa~~ Compression of Data: SSL compresses each block of data using loseless compression method between client & server

→ ~~Confied~~ Confidentiality: data & ~~Ma~~ MAC are encrypted by symmetric key cryptography.

→ Message Integrity: SSL creates MAC by using keyed-~~a~~ hash function for data Integrity

→ ~~for s~~

for session establishment between client & server in SSL,

1> Client send message, it has clients SSL ~~number~~ version number & cipher settings.

~~2> Client first verifies the server's SSL~~

2> now, server's ~~reesponsce data~~ responce data include, SSL certificate with public key

3> now, client verify server's SSL Certificate from certificate Authority & Authenticate.

4> now, if ~~Suc Succeed then Succes~~ above step succeeds, then, client Creates session key, encrypt it with server's public key & send to Server, now if server has requested client Authentication then client sends own ~~cce~~ certificate to server

5> now, server decrypt the session key with private key & sends acknowledgment to client

(b) (10)

b) C = client
AS = Authentication server
TGS = Ticket Granting Server
V = server to which client wants to request

TGT = Ticket granting Ticket

Ticket for V = The combination of user's ID, networkID & Server's ID, which is encrypted by secret key shared by AS & Server & send to client as Ticket to use Server

Authentication Protocols:

→ client requests a Ticket-granting ticket on behalf of user by sending its ~~use~~ ID & password to AS, with ~~TG~~ TGS ID.

→ AS responds with ticket that is encrypted with key that is derived from User's password. When ~~th~~ this response arrives at the client, the client prompts the user for ~~his~~ ~~e~~ password, generates key and attempts to decrypt the ~~time~~ incoming message. if the c~~orrect~~ password is correct then ticket is recovered

→ client requests a service-granting ticket on behalf of user. client transmits message to the TGS containing user's ID & ticket.

→ TGS decrypts the incoming ticket & verifies the success of the decryption by ID.

→ The client requests access to the service on behalf of the user. & clients transmits message to Server containing ID & service granting ticket. Server authenticate by using the contents of the ticket.

X—— end ——X