1. (a) CIA stands for Confidentiality, Integrity, Authenticity or Availability

(b) (i) Phishing is an internet scam where are user convinced to give their valuble information.

(ii) phishing attacks can be done through mass messaging, mass mailing etc.

(c) Sniffing is a computer attack.

Sniffing is a process of monitoring and capturing all data packets passing through given network.

(d) Virus is a self duplicating program that produces its own code by attaching copies of itself into other executable codes.

1(c)

Authentication	Authorisation
(1) Verifies user's credentials	Validates user's permissions
(2) Checks a person's details to identify him	check a user's privileges to access resources

(2) (i) RSA :- It was developed by Rivest, Shamir, Adleman.

(ii) RSA is a block cipher

RSA algorithm is as follows:-

Step 1 Key generation:-

(a) Select two prime number p, q where p ≠ q & of equal length

(b) Calculate n

$n = pq$

(c) calculate Euler totient function.

(d) Select integer 'e' such that

$$\gcd(\phi(n), e) = 1$$

or

$$1 < e < \phi(n)$$

(e) Calculate d

such that

$$d = e^{-1} \bmod \phi(n)$$

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

(f) Now

The public key = $\{e, n\}$

private key = $\{d, n\}$

Step 2:- Encryption

Let the plain text is capital M such that $M < n$ so cipher text

$$\boxed{CT = M^e \bmod (n)}$$

Step 3:-

If CT = C then

Plaintext

PT = $C^d \bmod(n)$

We have given

CT = 11

e = 7

n = 33

Step 1 Key generation.

(a) Let P = 3

Q = 11

So, n = 33

(b) Euler totient function

$\phi(n) = (P-1)(Q-1)$

$= (3-1)(11-1)$

$= 2 \times 10$

$= 20$

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

$7d = 1 \bmod 20$

$\boxed{d = 3}$

(d) Key generation.

Public key = {e, n}

= {7, 33}

Private key = {3, 33}

we need to find key ~~decrea~~ decoption

So,

$PT = (CT)^d \bmod n$

$= (11)^3 \bmod 33$

$= 1331 \bmod 33$

$= 11$

PT = 11

(3) (i) Diffie-Hellman key exchange algorithm is a secure algorithm for public key cryptography.

(ii) The purpose of this algorithm is to enable two users to securly exchange their keys for encryption.

Diffie-Hellman algorithm :—

Step 1 ⓐ Global public element.

We take two no. q and α where q is prime number and α is an integer.

α is a primitive root of q.

if.

$\alpha^1 \bmod q = x$

$\alpha^2 \bmod q = y$

$\alpha^3 \bmod q = z$

$\alpha^n \bmod q = p$ where $n < q$.

Or $n = q - 1$

if we get distinct no number like x, y, z --- p then

[α is primitive root of q]

Step 2 :- Public key of User A.

User A select a random integer

$X_A < q$ as his private and find his public key.

$$y_A = \alpha^{X_A} \bmod q.$$

Step 3:- User B key generation

$X_B < q$

$$y_B = \alpha^{X_B} \bmod q$$

Step 4:

Now A & B exchanged their public key.

Step 5:- Generation of Secret key of User A

$$K = (y_B)^{X_A} \bmod q$$

Step 6:- Generation of Secret

$$K_A = (y_A)^{x_B} \bmod q$$

$$K_A = (\alpha^{x_A} \bmod q)^{x_B} \bmod q$$

$$K_A = (\alpha^{x_B} \bmod q)^{x_A} \bmod q$$

$$\boxed{K_A = (y_A)^{x_B} \bmod q.}$$

3.(a) To show 2 is the primitive root of 11

So,

$2^1 \bmod 11 = 2$

$2^2 \bmod 11 = 4$

$2^3 \bmod 11 = 8$

$2^4 \bmod 11 = 5$

$2^5 \bmod 11 = 10$

$2^6 \bmod 11 = 9$

$2^7 \bmod 11 = 7$

$2^8 \bmod 11 = 3$

$2^9 \bmod 11 = 6$

$2^{10} \bmod 11 = 1$

Hence, we get different value of mod 0 so, 2 is the primitive root of 11.

3(b) If $y_A = 9$. find x_A

$$y_A = \alpha^{x_A} \bmod q$$

$$9 = 2^{x_A} \bmod 11$$

$$\boxed{x_A = 6} \text{ ans.}$$

3(c) $y_B = 3$ then find shared secret key.

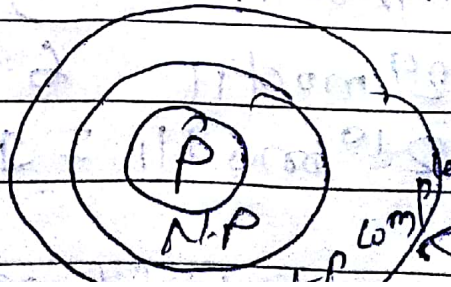
$$K = (y_3)^{x_A} \bmod q$$

$$= 3^6 \bmod 11$$

$$= 729 \bmod 11$$

$$= 3$$

(4) Knapsack crypto system is developed by Merkle Hellman use to solve n-p complete problem.



→ Knapsack is used to provide secure public key system.

→ And knapsack problem started that if we have given set of n weight $w_0, w_1, w_2 \ldots w_{n-1}$ and a sum S we have to find $a_0, a_1, a_2 \ldots a_{n-1}$ where $a \{0, 1\}$

$$S = a_0 w_0 + a_1 w_1 + a_2 w_2 + \ldots + a_{n-1} w_{n-1}$$

where

S = sum

a → itemset

w → weight

→ Generally knapsack is very difficult to used so, we are using super increasing knapsack.

A super increasing knapsack is similar to general knapsack except that where the weight are arranged from least to greatest each weight

Teacher's Signature .....

is greater than the sum of all previous weight.

Example

If the given weight are (1, 6, 8, 15, 24) and the given sum as
(a) S = 40 Find the item sets.

ans: S = 40

{1, 6, 8, 15, 24}
0 1 2 3 4

S > 24

S 24 = 8

S = S - 24
= 40 - 24
= 16

S > 15

93 = 1

S = S - 15
= 16 - 15
= 1

S < 8

$S < 6$

$a_1 = 0$

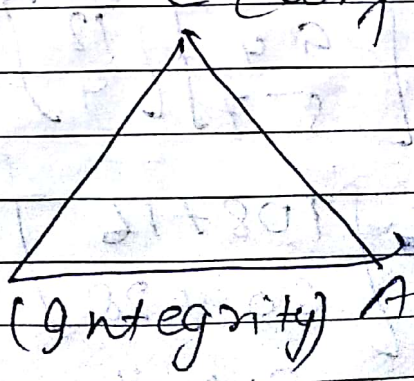
$S \geq 1$

$a_0 = 1$

So, item sets = $\{1, 0, 0, 1, 1\}$

5. (a) Internet protocol Security uses cryptographic security services to protect communication over Internet protocol network.

IPsec supports network-level peer authentication, data origin authentication, data integrity, data confidentiality and delay protection



5(b) Meet me

$$K = \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix}$$

$C = K p \bmod 26$

ME

ET

ME

A	B	C	D	E	F	G
0	1	2	3	4	5	6

H	I	J	K	L	M	N
7	8	9	10	11	12	13

O	P	Q	R	S	T	U
14	15	16	17	18	19	20

V	W	X	Y	Z
21	22	23	24	25

$$\begin{bmatrix} M \\ E \end{bmatrix} = \begin{bmatrix} 12 \\ 4 \end{bmatrix}$$

$$C = \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix} \begin{bmatrix} 12 \\ 4 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 108+16 \\ 60+28 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 124 \\ 88 \end{bmatrix} \bmod 26$$

Teacher's Signature .....

$$\begin{bmatrix} 20 \\ 10 \end{bmatrix}$$

$$\begin{bmatrix} U \\ K \end{bmatrix}$$

$$\begin{bmatrix} E \\ T \end{bmatrix} = \begin{bmatrix} 4 \\ 19 \end{bmatrix}$$

$$C = Kp \bmod 26$$

$$= \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix} \begin{bmatrix} 4 \\ 19 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 36 + 76 \\ 20 + 133 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 112 \\ 153 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 8 \\ 1 \end{bmatrix}$$

$$= \begin{bmatrix} I \\ B \end{bmatrix}$$

$$\begin{bmatrix} M \\ E \end{bmatrix} = \begin{bmatrix} 12 \\ 4 \end{bmatrix}$$

$$C = Kp \bmod 26$$

$$= \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix} \begin{bmatrix} 12 \\ 4 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 124 \\ 88 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 20 \\ 10 \end{bmatrix}$$

$$= \begin{bmatrix} U \\ K \end{bmatrix}$$

Meet me → UKIBUK

(c) A hash function is a function that takes variable length input string which is called pre-image and converts it into a fixed length output called hash value.

For example:—

SHA-1 one of the most widely used cryptographic hash function, produces a 160 bit value. In this case their size which is called block size is much bigger than the size of the hash value.

(6) (a) A firewall examines all the traffic related between the two network to see if it meet certain criteria.

(b) It routes packets between the network inbound as well as outbound activity

(c) It filters both inbounded and outbound traffic

Types of firewall:—

(1) Packet filtering firewall
(2) Network filtering firewall

Firewall	IDS
① firewall is a network security device that filters incoming and outgoing network based on predetermined rules	An Intrusion detection System is a device or a software application that monitors a traffic for malicious activ
② Block the traffic	Alarms on detection of anomaly.
③ Not analysed	Analysed