Solution Information Security (ME/EE)
06-1505

Ans 1 (a) Confidentiality, Integrity, Authenticity

(b) Phishing is an internet scam where the user is convinced to give Valuable Information.

(c) Sniffing is a data interception technology.
Objective of sniffing is to steal (i) Password (ii) Email text (iii) Files in transfer

(d) An attack is any action that Violates Security.

(e)

Authentication	Authorization
→ Verifies you are who you say you are	→ Decides if you have permission to access a resource
→ Methods	→ Method:
a) Login form	a) Access controls for URLs
b) HTTP authentication	b) Secure objects and methods
c) HTTP digest	c) Access control lists (ACLs)
d) Custom authentication method	

Ans 2 ⇒ $C = 11$, $e = 7$, $n = 33$

$$n = pq$$

$$\therefore p = 3, \; q = 17$$

$$\phi(n) = (p-1)(q-1) = 2 \times 10 = 20$$

$$ed = 1 \bmod \phi(n) \Rightarrow 7 \cdot d = 1 \bmod 20$$

$$\therefore d = 3$$

Now

$$M = C^d \bmod n$$

$$\Rightarrow M = (11)^3 \bmod 33$$

$$\Rightarrow M = 1331 \bmod 33$$

$$\Rightarrow M = 11 \text{ Ans}$$

Ans 3 =) (a) $2^1 \bmod 11 = 2$

$2^2 \bmod 11 = 4$ $\quad\because$ all the values are unique

$2^3 \bmod 11 = 8$ $\quad\therefore$ 2 is the primitive root of 11.

$\vdots$

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

(b) $q = 11, \quad \alpha = 2$

$y_A = 9, \quad x_A = ?$

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

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

$$\therefore x_A = 6 \text{ Ans}$$

(c) $q = 11, \quad \alpha = 2$

$y_B = 3$

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

$$= (3)^6 \bmod 11$$

$$= (729) \bmod 11$$

$$K = 3 \text{ Ans}$$

Ans 4 =) Knapsack Cryptosystem was developed by Merkle-Hellman.
The Merkle-Hellman Knapsack Cryptosystem is based on NP-Complete problem.
Used for providing secure public key Cryptography.

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

where $a \rightarrow$ Item

$w \rightarrow$ weight, $\quad S =$ Sum

eg =) Suppose the weights are :=)

85, 13, 9, 7, 47, 27, 99, 86

designated Sum $(S) = 172$

$\therefore$ Sol^n is $a = (a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7) = (11001100)$

$\therefore S = 85 + 13 + 47 + 27 = 172$ An

Ans 5 (a) IP Sec is an authentication protocol works at N/w layer

Services :-) (a) Access Control

(b) Connetionless integrity

(c) Data origin Authentication

(d) Rejection of Replayed packed

(e) Confidentiality (encryption)

(f) limited traffic flow Confidentiality.

(b) $C = KP \bmod 26$ 	$a=0$ $b=1$ $c=2$ $d=3$ $e=4$ $f=5$

me et me 	$g=6$ $h=7$ $i=8$ $j=9$ $k=10$ $l=11$

12 4 4 19 12 4 	$m=12$ ---- $z=25$

for me,

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

$$= \begin{bmatrix} 108+16 \\ 60+28 \end{bmatrix} \bmod 26 = \begin{bmatrix} 124 \\ 88 \end{bmatrix} \bmod 26 = \begin{bmatrix} 20 \\ 10 \end{bmatrix} = \begin{matrix} u \\ K \end{matrix}$$

for et

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

$$= \begin{bmatrix} 36+76 \\ 20+133 \end{bmatrix} \bmod 26 = \begin{bmatrix} 112 \\ 153 \end{bmatrix} \bmod 26 = \begin{bmatrix} 8 \\ 23 \end{bmatrix} = \begin{matrix} i \\ x \end{matrix}$$

Similary me = (u, k)

∴ Meet me = [ukix uk] Ans

(C) Hash function =)

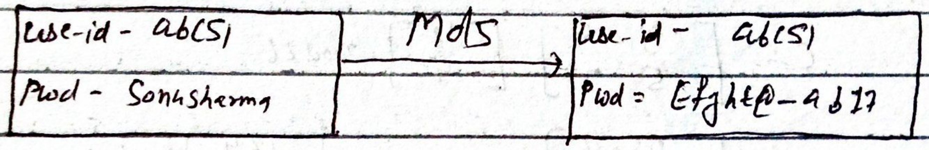
- It's a function that takes Variable-length input String called (called pre-image) and Converts it to a fixed length (generally Smaller) o/p String (called hash Value).
- A Simple has function would be a function that takes pre-image and returns a byte Consisting of the XOR of all the i/p bytes.

$$h = H(m)$$

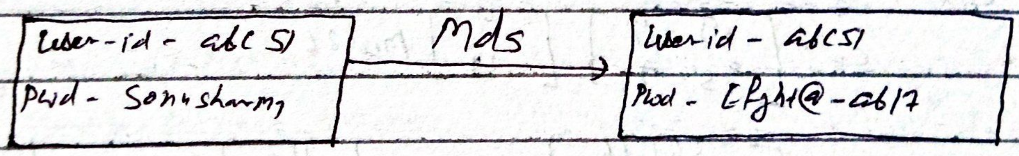
Where M is Variable length msg.
H(M) is the fixed length hash Value.

Signup

eg=)



Signin :=)



Encryption of Pwd will Save at the Server of Website or Service provider Company.