3/12/2016 Morning

Saturday

This question paper contains **4** printed pages]

Roll No.

S. No. of Question Paper : **1492**

Unique Paper Code : **2341702** **F-7**

Name of the Paper : **CS-702 Information Security**

Name of the Course : **B.Tech. Computer Science**

Semester : **VII**

Duration : **3 Hours** Maximum Marks : **75**

(Write your Roll No. on the top immediately on receipt of this question paper.)

Section A is compulsory.

Attempt any *four* questions from Section B.

Parts of a question must be answered together.

Section A

1. (*a*) List the different layers of an organization where security must be implemented to protect its operations. 3

(*b*) Assume a hacker hacks into a network, copies a few files, defaces the Web page, and steals credit card numbers, how many different threat categories does this attack fall into ? 2

(*c*) What measures can individuals take to protect against shoulder surfing ? 1

(*d*) Differentiate between Honeynet, Honeypot and Padded cell systems. 3

(*b*) (*i*) Show the P-Box for the following table :

8	1	2

(*ii*) A message has 2000 bits. It is supposed to be encrypted using a block cipher of 64 bits, find the size of padding and the number of blocks. 3+2

4. (*a*) Explain Data Encryption standard with the help of a diagram. 7

(*b*) (*i*) Give a list of possible items, which could be stored on a smart card, for authentication and encryption of connections.

(*ii*) How are those items stored on the smart card ? 2+1

5. (*a*) Explain Public Key Infrastructures (PKI) along with the types of models. 5

(*b*) Given the following Generator matrix, what will be the encoded message for the word (0101) ? 3

$$G = \begin{bmatrix} g_0 \\ g_1 \\ g_3 \\ g_4 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

(*c*) Explain Syndrome Decoding. 2

6. (*a*) What do you mean by Intrusion Detection and Prevention System ? Explain any *two* types of IDPS. 5

(*b*) Explain vulnerability scanner. How is it used to improve security ? 2

(*c*) Define network footprinting and network fingerprinting ? How are these two related ? 3

7. (*a*) Explain the different phases of security systems development Life Cycle. 6

(*b*) List and explain any *four* types of deliberate software attacks. 4

(*b*) Assume a language with 8 letters : A, B, C, K, L, O, T, Y, where A is 0, B is 1, C is 2, K is 3, L is 4, O is 5, T is 6, Y is 7. In order to encrypt a word in this language, we convert the letters into binary form, apply the scheme shown in the diagram given below and convert them back to corresponding letters. Using the above algorithm, encrypt the word : KAL. 5

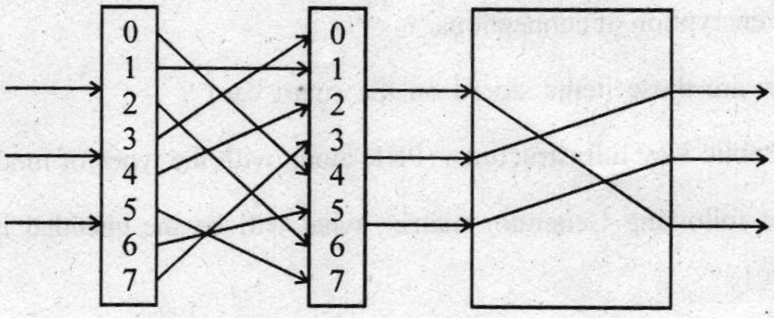

Fig. for question 2(*b*)

3. (*a*) (*i*) Describe Playfair Cipher encryption.

(*ii*) Encrypt the plaintext "This is Good" using playfair cipher and the following key :

secret key =

L	G	D	B	A
Q	M	H	E	C
U	R	N	I/J	F
X	V	S	O	K
Z	Y	W	T	P

3+2

P.T.O.

(*e*) (*i*) Define Generator and Parity Check Matrix.

(*ii*) How can parity check matrix be used to generate codeword ?

(*iii*) Define minimum weight of the code. 2+2+1

(*f*) Describe linear block code. Explain the difference between hamming distance and hamming weight. 3

(*g*) Define congruence and compare with equality. 2

(*h*) Explain modulo operator along with its application. Also define residue classes with an example. 2

(*i*) Explain whether the following cipher is monoalphabetic or not. Given reason also.

Plain text : Frittata

Ciphertext : LTOHHQJQ 2

(*j*) Use the Additive cipher to encrypt the message "HelloAbraham" with key = 10. 3

(*k*) Explain transposition cipher with a suitable example. 3

(*l*) How many permutation tables are used in Data Encryption Standard cipher ? 2

(*m*) Differentiate between the following : 2+2

(*i*) Digital Signature and conventional signature

(*ii*) Public key and Private key.

Section B

2. (*a*) Explain the steps of Diffie-Hellman Key exchange protocol. What is the most common attack on this protocol ? 5