[This question paper contains 7 printed pages]

Your Roll No.	: ....
Sl. No. of Q. Paper	: **6132** **F-9**
Unique Paper Code	: 2341702
Name of the Course	: **B.Tech. Computer Science**
Name of the Paper	: CS-702 Information Security
Semester	: VII

Time : 3 Hours ***Maximum Marks : 75***

Instructions for Candidates :

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

(b) **Section - A** is compulsory.

(c) Attempt any **4** questions from **Section - B**. Parts of a question must be answered together.

Section - A

1. (a) What is the difference between vulnerability and exposure ? 2

P.T.O.

(b) Define linear congruence. Solve the questions $3x + 4 \equiv$ (mod 13). 3

(c) Find the multiplicative inverse of 132 in Z_{180}. 3

(d) Differentiate between block ciphers and stream ciphers. 3

(e) Use affine cipher to encrypt the message "Today is our IS exam" with the key pair (7.2). 2

(f) Explain the concept of Fiestal Network. Also prove that the mixer in Fiestal Cipher is self-invertible. 5

(g) Why does a round key generator need a parity drop table ? 3

(h) What is a honeypot ? How is it different from a honeynet ? 2

(i) Describe the legal issues in Security. 2

(j) What would be the code word corresponding to the message (1101). The generator matrix, is given below : 2

$$G = \begin{vmatrix} g_0 \\ g_1 \\ g_2 \\ g_3 \end{vmatrix} = \begin{vmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{vmatrix}$$

(k) Explain Man in the middle attack with a suitable example. 3

(l) Explain the Public key Infrastructure. 5

Section - B

2. (a) Use the Playfair Cipher to encipher the message "Information need to be secure". The secret key can be made by filling the matrix diagonally from top left corner. Consider alphabets 'Y' and 'Z' together in one cell of the matrix. 5

(b) A Vigenere Cipher is a combination of m additive ciphers. Justify with an example. 5

3. (a) Consider a symmetric (8,4) code whose parity – check equations are. 6+4=10

$V_0 = u_1 + u_2 + u_3$

$V_1 = u_0 + u_1 + u_2$

$V_2 = u_0 + u_1 + u_3$

$V_3 = u_0 + u_2 + u_3$

Where u_0 u_1 u_2 and u_3 are message digits and V_0 V_1 V_2 and V_3 are parity-check digits. Find the generator and parity-check matrices for this code. Determine the minimum distance of this code.

(b) Determine the weight distribution of the (8,4) linear code given in above problem. Assume the transition probability of a BSC be $p = 10^{-2}$. Compute the probability of an undetected error of this code.

4. If generator g = 2 and p = 11, use Diffie-Hellman algorithm to solve the following for User A and User B. 1+4+4+1

(a) Show that 2 is primitive root of 11.

(b) If A has public key 9 then what is A's private key.

(c) If B has public key 3 then what is B's private key.

(d) Calculate the shared secret key.

5. (a) Using the S-box below find out the result of passing strings.

(i) 110111

(ii) 001100

(iii) 111111

S-Box Table

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	10	00	09	14	06	03	15	05	01	13	12	07	11	04	02	08
1	13	07	00	09	03	04	06	10	02	08	05	14	12	11	15	01
2	13	06	04	09	08	15	03	00	11	01	02	12	05	10	14	07
3	01	10	13	00	06	09	08	07	04	15	14	03	11	05	02	12

(b) Briefly describe the components of DES including key generation. 7

6. Briefly explain Rabin Key Generation Algorithm. Assume the private key pair is (23, 11). Calculate the Cipher text if the plain text is 24.Also calculate all four possible plain text for the corresponding cipher text. 10

7. Write a short notes on (any **five**) :

2×5=10

(a) Honey pots

(b) Digital Signature

(c) E-mail Security

(d) Threats

(e) Transposition Cipher

(f) One Time Pad