2011

MCA

5th SEMESTER EXAMINATION

ELECTIVE—II

PAPER—3504

Full Marks : 100

Time : 3 Hours

The figures in the margin indicate full marks.

Candidates are required to give their answers in their own words as far as practicable.

Illustrate the answers wherever necessary.

Cryptography and Steganography

Group—A

(Cryptography)

Answer Q. No. *1* and any *three* from the rest

1. Answer any *two* : $2\times2\frac{1}{2}$

(a) What is Non-Repudiation ?

(b) What do you mean by masquerade attack ?

(c) What is product cipher ?

(d) Name three wordwide certification authority.

2. (a) What do you mean by attacks on network system ? Briefly describe several types of passive attacks. 1+4

(b) Encrypt the following message using Playfair cipher encryption scheme. 5

Message : VIDYASAGAR UNIVERSITY

Keyword : CRYPTOSYSTEM

3. (a) With suitable example, describe Diffie-Hellman key exchange algorithm. 5

(b) Discuss the problem associated with Diffie–Hellman key exchange algorithm. 5

4. (a) What is S-Box substitution in DES? 5

(b) What are the key requirements of message digest? 2

(c) Discuss, how padding is performed at the initial stage of MD5. 3

5. (a) Write down the RSA algorithm to demonstrate the public and private key-pair generation. 5

(b) Briefly discuss the concept of digital certificate. 5

6. Write short note (any *two*) : 2×5

(a) Access Control;

(b) Caesar Cipher;

(c) X·509.

Group—B

(Steganography)

Answer any *five* question 5×7

7. What is steganography? What are the differences and similarities of steganography with digital water marking? How reganography differ from cryptography?

$2+1\frac{1}{2}+1\frac{1}{2}+2$

8. What is steganalysis ? Define the role of passive, active and malicious steganalysts. 1+2+2+2

9. Write an algorithm for encoding and decoding of any message using Hide & Seek randomized technique. $3\frac{1}{2}+3\frac{1}{2}$

10. Explain J-steg algorithm for encoding and decoding of any message. What are the disadvantage of this algorithm. 3+3+1

11. Explain outguess 0.1 algorithm for encoding and decoding any message. Why is it much secure than Hide & Seek and J-steg algorithms.

12. Explain F3 algorithm of encode any message. What are the weaknesses of F3. 5+2

13. Briefly write F4 algorithm to encode message in the cover. Also decode the same using F4. $3\frac{1}{2}+3\frac{1}{2}$

14. Write short note on (any *two*) : $3\frac{1}{2}\times2$

(a) Visual attacks ;

(b) Structural attacks ;

(c) Statistical attacks ;

(d) Histogram attacks.

Hybrid System

Answer Q. No. *1* and any *five* from the rest.

1. (a) What is a Hybrid System? 5×2

(b) What do you mean by population in Genetic algorithm?

(c) What is 'Fizzy logic'?

(d) What do you understand by a threshold value in neural network.

(e) State some encoding techniques of Genetic Algorithm.

2. (a) Why do we need Hybrid system. 2

(b) In how many ways can Hybrid system be classified. Explain each of them with suitable examples. 7

(c) What do you understand by Fizzy-Genetic Hybrids. 3

3. (a) How would you relate chance versus fuzziness? 6

(b) What is a Partition and covering set. Give example. 6

4. Consider the given fuzzy set :

$$\tilde{I} = \{(F, 0{\cdot}4), (E, 0{\cdot}3), (X, 0{\cdot}1), (Y, 0{\cdot}1), (I, 0{\cdot}9), (T, 0{\cdot}8)\}$$

$$\tilde{F} = \{(F, 0{\cdot}99), (E, 0{\cdot}8), (X, 0{\cdot}1), (Y, 0{\cdot}2), (I, 0{\cdot}5), (T, 0{\cdot}5)\}$$

Find the following :

(a) (i) $\tilde{I} \cup \tilde{F}$, (ii) $\tilde{I} - \tilde{F}$, (iii) $\tilde{F} \cup \tilde{F}^c$ 6

(b) Verify De Morgan's Law, $\left(\tilde{I} \cup \tilde{F}\right)^c = \tilde{I}^c \cap \tilde{F}^c$ 3

(c) How would you apply Fuzzy within Neural Network. Briefly explain. 3

5. (a) What is composition of relations.

Consider $\tilde{R} =$

	y_1	y_2
x_1	0.5	0.1
x_2	0.2	0.9
x_3	0.8	0.6

$\tilde{S} =$

	z_1	z_2	z_3
y_1	0.6	0.4	0.7
y_2	0.5	0.8	0.9

Find $R \circ S$. 2+4

(b) Under what conditions of P and Q is the implication $P \longrightarrow Q$ a tautology? Derive the truth table to show the tautology. 4

(c) What do you understand by approximate reasoning in Fuzzy logic. 2

6. (a) How many types of fuzzy quantifiers present. Explain. 4

(b) If X = {a, b, c, d} Y = {1, 2, 3, 4}

$\tilde{A}$ = {(a, 0) (b, 0·8) (c, 0·6) (d, 1)}

$\tilde{B}$ = {(1, 0·2) (2, 1) (3, 0·8) (4, 0)}

$\tilde{C}$ = {(1, 0) (2, 0·4) (3, 1) (4, 0·8)}

Determine the implication relation

(i) If x is $\tilde{A}$ THEN y is $\tilde{B}$

(ii) If x is $\tilde{A}$ THEN y is $\tilde{B}$ ELSE y is $\tilde{C}$ 8

7. (a) What are the different types of defuzzification methods. Briefly explain. 6

   (b) What is a fuzzy rule based system ? How many types of them an available ? Give example. 6

8. (a) Demonstrate with an example to show how a crisp value is being fuzzified to generate its membership value within a fuzzy set. 4

   (b) Draw the block diagram of fuzzy system and explain the flow of information. 6

   (c) What do understand by Generalized Modus Tollens (GMT) ? 2

Internal Assessment — 30