2015

MCA

5th SEMESTER EXAMINATION

PAPER—504

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.

Elective-II

Answer *Q. No. 1* and any *six* questions taking at least *two* from each group.

Group—A

(CRYPTOGRAPHY & STAGNOGRAPHY)

1. Answer any *five* questions : 5×2

(a) Define cryptanalysis and brute-force attack.

(b) What are S-box and P-box operations ?

(c) Differentiate between RSA and DES.

(d) What is digital signature ? Give example.

(e) What is authentication ?

(f) Differentiate between spatial domain and frequency domain steganography.

(g) Differentiate between symmetric and asymmetric techniques.

(h) What is message digest ?

Group — A

2. (a) Describe DES algorithm and explain its key structure.

(b) Define session key. Give an example. 5+5

3. Define Diffusion and Confusion. What is product cipher ? Draw a diagram of product cipher made of two rounds. What is Feistel ciphers, explain. 2+4+4

4. (a) What is message digest ? Generate a message digest of the number 7195379 using any suitable algorithm.

(b) Write down MD5 algorithm with a block level simulation and explanation. (2+3)+5

5. (a) What is digital certificate ? Write down an algorithm to generate digital certificate along with its verifications.

(b) Describe special domain steganography. Encode "10110111" into following image matrix using (LSB+2) steganography :

10110110	11110001	10101010	11011010
10110111	11001100	11000010	11001110

(2+3)+(2+3)

Group — B

6. (a) What are the basic differences between spatial and frequency domain stegonagraphy ?

(b) What is the utility of hash function in embedding ? What is handle ? Why do we go for handle ?

(c) Embed '1011' using hash function I * J MDO 4, where starting values of I and J are 101 and 110 respectively into the following image matrix :

250	100
110	120

2+(2+2+2)+2

7. (a) Define frequency domain Steganography. Account for reversibility of transform based steganography.

(b) Write down generalized equations of DFT. What is the basis of selecting 2×2 mask ? Explain with example.

(c) Embed first nibble of 'C' in the following manner using DFT :

No embedding	1-bit embedding
1-bit embedding	2-bit embedding

Also extract the embedded message. Show detailed steps. Use image matrix of question no. 5.

(2+2)+3+3

8. (a) Write down transform equation pair of DCT.

(b) Normally imaginary part in DCT is ignored. Why ? Explain with example.

(c) Embed 9 into transform coefficient of a 2×2 DCT using following matrices. Show detailed steps for decoding also :

90	120
110	100

3+2+5

9. (a) Discuss PVD method. What are basic difference between LSB and PVD methods ?

(b) Structure of PVD methods with principle of no. of bits embedding in each division.

(c) Embed 'a' into the following image matrix :

10	15	11
05	12	14
09	00	20

2+3+5

10. (a) Discuss document authentication. Why it is necessary for digital document ?

(b) What is legal document authentication? How it is done ?

(c) Describe a method of legal document authentication.

3+3+4

11. (a) What is wavelet transform ? How it is differ from DFT ? Write transform equation pair of wavelet.

(b) What are various types of wavelets ? What are scaling functions ?

(c) How Outputs are characterized in wavelets ? What is its utility ?

4+3+3

[*Internal Assessment*] 30

(ADVANCED NETWORKING)

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

1. Answer any *five* questions : 5×2

(a) What is the function of routed protocol? Give an example of routed protocol.

(b) What is plaintext and cyphertext?

(c) What is segmentation? Which layer of OSI ref. model is responsible for segmentation?

(d) What is administrative distance?

(e) What is autonomous system?

(f) What are the metric of RIP and OSPF?

(g) What is gateway?

(h) What is datagram?

2. (a) Describe any shortest path algorithm.

(b) Briefly describe header format of IPV_6. 6+6

3. (a) What is symmetric key and asymmetric key cryptography?

(b) What is private key and public key?

(c) Describe about various types of Cypher. 3+3+6

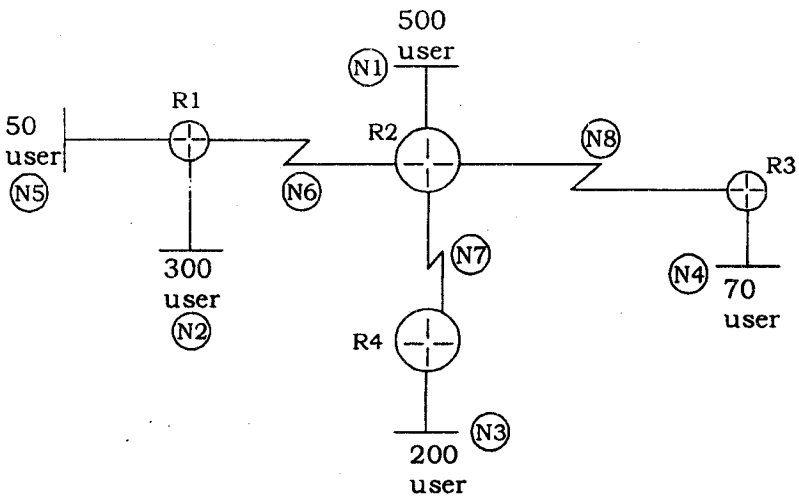
4. (a) Briefly explain the compression rule of IPV_6 with a suitable example. 6

(b) Discuss about RSA algorithm. 6

5. (a) What is VLSM? What are the advantages of VLSM over subnetting? 2+3

(b) You are given 172.16.0.0 IP address and plan to deploy VLSM to the networks, which are shown in the

figure below : 7



Assign IP address to the every network.

6. (a) Briefly explain about a 3-way hand shaking and 4-way hand shaking. 3+3

(b) Describe TCP header format. 6

7. (a) Briefly explain about Token bucket algorithm. 6

(b) Describe about various types of satellite. 6

8. Write short notes on any *three* : 3×4

(a) ICMP ; (b) VLAN ; (c) NAT and PAT ; (d) SMTP ;

(e) Firewall.

[*Internal Assessment*] 30