YMCA UNIVERSITY OF SCIENCE & TECHNOLOGY, FARIDABAD
B.TECH (CE), 7TH SEM EXAMINATION (UNDER CBS)
SECURITY OF INFORMATION SYSTEMS (CE-403)

60

Time: 3 hrs M. Marks: 60

Note: All questions in part-I are compulsory and attempt any four in part-II.

PART-I

Q. No. 1 (1) Differentiate between confusion and diffusion.
(2) Explain the concept of Kirchoff's principle.
(3) In the context of access control, what is the difference between a subject and an object?
(4) What is the difference between differential and linear cryptanalysis?
(5) Briefly describe AddRoundKey in AES.
(6) What is triple encryption?
(7) Write the participants in the SET protocol.
(8) Differentiate between threat and vulnerability.
(9) Explain the nature of inference threat to a RDBMS.
(10) Explain how cookies can be misused to invade people's privacy?
(10*2=20)

PART-II

Q.No. 2 (a) What are covert channels? Explain how storage and timing channels are created? (5)
(b) Explain how secure E-mails can be sent? Explain how "ring of trust" helps PGP to address key distribution problem. (5)

Q.No. 3 (a) Given the plain text in hexadecimal {0123456789ABCDEF0123456789ABCDEF} and the key in hexadecimal {02020202020202020202020202020202}. Show the original contents of state displayed as 4*4 matrix, after shift rows and after initial add round key (No need to show mix columns). (5)
(b) Explain the concept of biometric authentication. (5)

Q.No. 4 (a) What do you mean by virus signature? Explain how does boot sector virus attach and spread itself? (5)
(b) What do you mean by security planning? Differentiate between patents, copyrights and tradesecrets. (5)

Q.No. 5 (a) Decrypt the cipher text 10000001 using 8-bit DES having key K=11111111. (5)
(b) Discuss security features of trusted operating system. Also explain two operating system security policies. (5)

Q.No. 6 (a) Encrypt the following message using play fair matrix using key "Gymnastic"
Message-> " Exercise is good for health" (3)
(b) Write the X.509 structure of digital certificate. (4)
(c) Discuss some of the attacks on the network security. (3)

P.T.O

Q.No. 7 Write short notes on following:

(a) SSL Protocol
(b) Guard firewalls
(c) Kerberos authentication protocol
(d) End to end encryption (2.5*4)