VRK/KS/14/3209

Faculty of Engineering & Technology
Eighth Semester B.E. (Computer Science) Examination
COMPUTER SYSTEM SECURITY (NEW)
Sections—A & B

Time—Three Hours] [Maximum Marks—80

INSTRUCTIONS TO CANDIDATES

(1) All questions carry marks as indicated.

(2) Answer **THREE** questions from Section A and **THREE** questions from Section B.

(3) Due credit will be given to neatness and adequate dimensions.

(4) Assume suitable data wherever necessary.

(5) Illustrate your answers wherever necessary with the help of neat sketches.

SECTION—A

1. (a) Distinguish between mono alphabetic and poly alphabetic ciphers. State why poly alphabetic is more secure than mono alphabetic ciphers with the help of an example. 6

(b) What is Cryptanalysis ? Explain the various types of cyptanalysis attacks based on amount of information known to cryptanalyst. 7

2. (a) Define the functioning of DEs algorithm in detail and also explain output feedback mode and counter code mode of operation in DES. 7

(b) Consider the keyword : ZEBRAS. The order for given keyword is "632415". The message is "WE ARE DISCOVERED FLEE AT ONCE". In an irregular columnar transposition encrypt the message using double transposition method. Make use of different key as STRIPE and keyword order 564231 for second step. 7

3. (a) Distinguish between Conventional Encryption and Public Key Encryption. 5

(b) Describe Diffie-Hellman key exchange algorithm in detail. What are the weaknesses of algorithm ? 8

4. (a) Perform encryption and decryption using RSA algorithm for the following :

$P = 3 \quad Q = 11 \quad E = 7 \quad M = 5$ 7

(b) Give properties of Digital Signature. 6

5. (a) Explain DSA algorithm with suitable example. 6

(b) Identify the application areas of MD-5 algorithm and state the difference between MD5 and SHA-1 algorithm. 7

SECTION—B

6. (a) Explain X.509 certificate revokation mechanism in detail. Also provide X.509 format. 7

(b) Explain S/MIME functionality in detail. 7

7. (a) Describe PGP message generation and message reception. 7

(b) What protocol comprises SSL ? State the difference between SSL Connection and SSL Session. 6

8. (a) Differentiate between SHTTP and HTTP based on their functionality. 6

(b) List and briefly define the principal categories of SET participant. Also define three classes of intruders and state two common techniques used to protect a password file. 7

9. (a) Explain Honey-pot of system of intrusion detection. 4

(b) State three types of firewall and give their configuration clearly stating their advantages one over the other. 9

OR

10. (a) What is Intruder ? Explain intrusion detection techniques. 6

(b) What is Virus ? Explain various types of Virus. 7