SEAT No. :

P3985

[Total No. of Pages : 2

[5561]-689

B.E. (Computer Engineering)
INFORMATION AND CYBER SECURITY
(2015 Pattern) (Semester - II) (410251)

Time : 2½ Hours]

[Max. Marks : 70

Instructions to the candidates:

1) *All questions are compulsory.*

2) *Figures to the right side indicate full marks.*

Q1) a) List and explain various elements of Information security. **[5]**

b) Using Hill Cipher encrypt the message 'ESSENTIAL'. The key for encryption is 'ANOTHERBZ'. **[5]**

OR

Q2) a) What is steganography? What are the applications and limitations of steganography? **[5]**

b) Use Transposition Cipher to encrypt plain text 'I Love my India' and use the key 'HEAVEN'. **[5]**

[Use single columnar transposition]

Q3) a) Discuss elliptic curve cryptography in detail. **[5]**

b) What is block Cipher? Explain counter mode of block Cipher. **[5]**

OR

Q4) a) What is authentication? Explain various methods authentication. **[5]**

b) Explain working of AES in detail. **[5]**

Q5) a) Discuss the working of IPSec. What are the benefits of IPSec. **[6]**

b) What is VPN? Explain types of VPN. **[6]**

c) Compare PGP, MIME and S/MIME. **[6]**

OR

P.T.O.

Q6) a) Differentiate between IP-V4 and IP-V6. **[4]**

b) Explain secure socket layer handshake protocol in detail. **[7]**

c) Explain ISAKMP protocol of IPSec with header format. **[7]**

Q7) a) What are the various types of firewall. Discuss limitations of firewall. **[8]**

b) Explain any two password management practices. **[4]**

c) What is trusted system. **[4]**

OR

Q8) a) Explain need and challenges of intrusion detection system. Define signature based IDS. **[8]**

b) What is access control security services. **[4]**

c) Explain packet filtering firewall. **[4]**

Q9) a) Explain personally identifiable information PII. Describe PII impact levels with examples. **[8]**

b) What is cyber stalking? How to identify and detect cyber stalking. **[8]**

OR

Q10) a) What are different phases of cyber forensics? Explain with suitable diagram. **[8]**

b) Discuss PII confidentiality safeguards. **[8]**

⌘⌘⌘