May 2017

Total No. of Questions : 10]

SEAT No. :

P3120

[5154]-687

[Total No. of Pages :2

B.E. (Computer Engineering)
CYBER SECURITY (Elective - III)
(2012 Pattern)(Semester - II) (End Sem) (410451D) (Elective - III)

Time : 2½ Hours] *[Max. Marks : 70*

Instructions to the candidates:

1) *Answer Q1 or Q2, Q3 or Q4, Q5 or Q6, Q7 or Q8 and Q9 or Q10.*
2) *Neat diagrams must be drawn wherever necessary.*
3) *Figures to the right indicate full marks.*
4) *Use of logarithmic tables, slide rule, Mollier charts, electronic pocket calculator and steam tables is allowed.*
5) *Assume suitable data, if necessary.*

Q1) a) What is cryptanalysis? Expalin various cryptanalysis techniques. [5]

b) Using Playfair cipher encrypt message. "We live in a world full of beauty" use key "ANOTHER" [5]

OR

Q2) a) Draw and explain operational model of network security. [5]

b) Explain the operation in key Expansion process in AES algorithm. [5]

Q3) a) Explain Ciper Feedback Mode(CFB) Block cipher. [5]

b) What is weak key in DES algorithm? Explain with example. [5]

OR

Q4) a) Use RSA algorithm to encrypt the plaintext "3" use following parameters p = 11, q = 3, e = 13 [5]

b) What is authentication? Explain various methods for authentication. [5]

Q5) a) Explain working of PGP algorithm in detail. [9]

b) Explain the operation of Secure Socket Layer(SSL) protocol in detail. [8]

OR

Q6) a) Explain ISAKMP protocol of ISPEC. [6]

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

c) List and explain various participants involved in Secure Electronic Transaction(SET). [5]

P.T.O.

Q7) a) What are the challenges of intrusion detection. [6]

b) List and explain any two password management practices. [6]

c) What are the various characteristics of firewall. [5]

OR

Q8) a) Explain various types of firewall. [6]

b) Explain anomaly-based intrusion detection system. [6]

c) What is Trusted System. [5]

Q9) a) What is War dialing for remote connectivity? Explain software used for war dialing. [8]

b) Explain attacks and counter measures on application and data with examples. [8]

OR

*Q10)*a) What is VOIP hacking? What are the counter measures for it? [8]

b) Explain various hacking devices used for hacking. [8]

♦ ♦ ♦