Total No. of Questions : 8]

SEAT No. :

P-457

[Total No. of Pages : 1

[6003]-564

T.E. (Honour in Cyber Security)

INFORMATION AND CYBER SECURITY

(2019 Pattern) (Semester - I) (310401)

Time : 2½ Hours] *[Max. Marks : 70*

Instructions to the candidates:

1) ***Answer Q1 or Q2 , Q3 or Q4,Q5 or Q6, Q7 or Q8.***
2) ***Neat diagram must be drawn wherever necessary.***
3) ***Figures to the right side indicate full marks.***
4) ***Assume suitable data if necessary.***
5) ***Use of Scientific Calculator is permitted.***

Q1) a) Explain RSA algorithm step by step in detail with example. **[9]**

b) What is Chinese remainder theorem? What is it implication in cryptography? Explain with example. **[9]**

OR

Q2) a) Explain Diffie Hallman in detail. Solve if p=7, q=17 using Diffie Hellman algorithm, select a=6, b=4. **[9]**

b) Explain operation of MD5 Message digest algorithm. **[9]**

Q3) a) What are the challenges in Social Engineering? Explain cyber stalking. **[8]**

b) Describe different categories of cybercrime with example. **[9]**

OR

Q4) a) List the steps for risk identification and assessment in risk management for Information Security. **[8]**

b) What are the objectives and pros and cons of Quantitative and Qualitative risk Assessment? **[9]**

P.T.O.

Q5) a) What services are provided by IPSec? Give difference between Transport mode and Tunnel mode. **[9]**

b) What protocols comprise SSL with neat diagram? What is the difference between SSL connection and SSL session? **[9]**

OR

Q6) a) What problem was Kerberos designed to address? Explain its working. **[9]**

b) Define firewall and explain following details about firewall. **[9]**

i) Roels of firewall

ii) Design goal of firewall

iii) Different types of firewall

iv) Limitation of firewall

Q7) a) Define, list and explain different types of viruses. **[8]**

b) Explain Password Cracking and types of Password Cracking. **[9]**

OR

Q8) a) Explain Intrusion detection system with its types limitations and challenges. **[8]**

b) What is DoS and DDoS attack? Explain with suitable example. **[9]**

◆◆◆