

Total No. of Questions : 8]

SEAT No. :

PD4251

[Total No. of Pages : 2

[6403]-46

T.E. (Computer Engineering)
INFORMATION SECURITY

(2019 Pattern) (Semester - VI) (310254 (A)) (Elective - II)

Time : 2½ Hours]

[Max. Marks : 70

Instructions to the candidates:

- 1) Attempt Q1 or Q2, Q3 or Q4, Q5 or Q6, Q7 or Q8.
- 2) A Neat diagram must be drawn wherever necessary.
- 3) Assume suitable data if necessary.
- 4) Figures to the right indicate full marks.

Q1) a) Differentiate between Asymmetric key cryptography and symmetric key cryptography? [8]

b) What are the different types of attacks possible on RSA? Explain in brief? [8]

c) Explain Chinese reminder Theorem? [6]

OR

Q2) a) Explain ECC for the finite field with points $y^2 = x^3 + ax + b$? [8]

b) Perform encryption and decryption using RSA algorithm for the following: [8]

$P = 3; q = 11; d = 7; M = 5$

c) Explain El-Gemmal Algorithm in detail? [6]

Q3) a) What services are provided by IPSec? What is the difference between transport mode and tunnel mode in IPSec? [8]

b) Explain the MD5 algorithm in brief? [8]

OR

P.T.O.

Q4) a) What is Message Digest? Compare MD-5 with SHA-I? [8]

b) Explain the contents of X.509 format of certificate with diagram? [8]

Q5) a) Write a short note on : [8]

i) Honeypot

ii) Distributed DOS attack

b) What are the capabilities and limitations of Firewall? [8]

OR

Q6) a) What are Intrusion Prevention policies? Explain in brief? [8]

b) Discuss operating system security in detail? [8]

Q7) a) Write short note on : [8]

i) Cyber Terrorism

ii) Social Engineering

b) Write short note on : [8]

i) Keyloggers and Spywares

ii) Password Cracking

OR

Q8) a) Write short note on Amendments of IT ACT in India? [8]

b) Write short notes on keyloggers and spyware? Also explain the severity of the incident? [8]

