Total No. of Questions : 8]

SEAT No. :

P-7548

[Total No. of Pages : 2

[6180]-56

T.E. (Computer Engineering)

INFORMATION SECURITY

(2019 Pattern) (Semester - II) (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) ***Neat diagram must be drawn wherever necessary***
3) ***Assume suitable data if necessary.***

Q1) a) Explain Diffie-Hellman key exchange algorithm. **[6]**

b Determine the value of x using the Chinese remainder theorem. **[6]**

$x \equiv 2 \bmod 3$

$x \equiv 3 \bmod 5$

$x \equiv 2 \bmod 7$

c) What are the different types of attacks possible on RSA? Explain in brief. **[6]**

OR

Q2) a) Explain the "Man in the middle" attack in Diffie Hellman Key Exchange algorithm with the help of an example. **[6]**

b) Perform encryption and decryption using RSA algorithm for the following : **[6]**

P = 5; q = 11; e = 3; M = 9

c) Explain El-Gammal Algorithm in detail. **[6]**

Q3) a) Compare between IPSec and TLS. **[6]**

b) Explain the steps to create the digital certificate with diagram. **[5]**

c) Define hash function. List the requirements of hash function. **[6]**

OR

P.T.O.

Q4) a) List and describe the contents of the Encapsulating Payload header in IPSec with diagram. **[6]**

b) Explain the contents of X.509 format of certificate with diagram. **[5]**

c) What is a message authentication code? What is the difference between a message authentication code and a one-way hash function? **[6]**

Q5) a) Explain any two types of Intrusion detection systems? **[6]**

i) Network based IDS

ii) Host based IDS

iii) Anomaly based IDS

iv) Signature based IDS

b) Explain packet filtering firewall in detail. **[5]**

c) Discuss operating system security in detail. **[6]**

OR

Q6) a) Write a short note on any one : **[6]**

i) Honeypot

ii) Distributed DOS attack

b) What are the capabilities and limitations of Firewall? **[5]**

c) Explain access control and its types in detail. **[6]**

Q7) Write short note on any three : **[18]**

a) Cyber Terrorism

b) Examples of Cyber Crime

c) Social Engineering

d) Types of cyber stalkers

OR

Q8) Write short note on any three : **[18]**

a) Phishing attack

b) Keyloggers and Spywares

c) Aim and objectives of IT act

d) Password Cracking

□□□