Total No. of Questions: 8]

SEAT No. : □

P278

[Total No. of Pages : 2

[6003]-357
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) What are the different types of attacks possible on RSA? Explain in brief. **[6]**

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

c) Consider a Diffie-Hellman scheme with a common prime q = 71 and a primitive root α = 7 **[6]**

i) If user A has private key $X_A = 5$, what is A's public key Y_A?

ii) If user B has private key $X_B = 12$, what is B's public key Y_B?

iii) What is the shared secret key K?

OR

Q2) a) Explain Chinese reminder theorem. **[6]**

b) Differentiate betwen Asymmetric key cryptography and symmetric key cryptography. **[6]**

c) Perform encryption and decryption using RSA algorithm for the following: P=3; q=11; d=7; M=5 **[6]**

Q3) a) List and describe the contents of the Authentication header in IPSec with diagram. **[6]**

b) Explain the working of IPSec. What are the benefits of IPSec? **[5]**

c) What is Message Digest? Compare MD-5 with SHA-1. **[6]**

OR

P.T.O.

Q4) a) Discuss two modes of IPSec. **[6]**

b) Discuss web security issues. **[5]**

c) Discuss the basic requirements for a cryptographic hash function. What is the difference between a strong and a weak collision resistance? **[6]**

Q5) a) Explain the needs and challenges of intrusion detection systems. **[6]**

b) What is Denial of Service (DoS) attack? How does it affects the network performance? **[5]**

c) Discuss Application-level security in detail. **[6]**

OR

Q6) a) Compare Anomaly based and Signature based intrusion detection system. **[6]**

b) Explain access control and its types in detail. **[5]**

c) Discuss the concept of multilevel security. **[6]**

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

a) Botnets

b) Types of cyber crimes

c) Information Security Life Cycle

d) Cyber Stalking

OR

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

a) Cyber Terrorism

b) Anonymizers

c) Types of Cyber stalkers

d) Aims and objectives of IT act 2000