Total No. of Questions : 12]

SEAT No. :

P3445

[Total No. of Pages : 3

[4959]-222
B.E. (Computer Engg)
d:INFORMATION SECURITY
(2008 Pattern) (Semester - II) (Elective - IV)

Time : 3 Hours] *[Max. Marks : 100*

Instructions to the candidates:

1) ***Answer three questions from section I and three questions from section II.***
2) ***Answers to the two sections should be written in separate answer books.***
3) ***Neat diagrams must be drawn wherever necessary.***

SECTION - I

Q1) a) Enlist and explain different standards to information security. **[6]**

b) What is cryptography? discuss different kinds cryptography in brief. **[6]**

c) Which crytography is called as classical cryptography?

Explain any one classical cryptography in short. **[6]**

OR

Q2) a) What are professional issues of information security? Discuss it in brief. **[6]**

b) Explain standard security architecture in detail. **[6]**

c) What types of security are need for information in computer? Explain in short. **[6]**

Q3) a) What is IDEA? Explain the working principle of IDEA in the form of algorithm. **[8]**

b) Explain RC5 encryption algorithm in details. **[8]**

OR

P.T.O.

Q4) a) Discuss different mechanisms of key distribution in detail. **[8]**

b) Explain block ciphering modes operations with suitable diagram. **[8]**

Q5) a) What is public key cryptography? Explain any one algorithm of public key cryptography. **[8]**

b) Write and explain the algorithm of ECC cryptography. **[8]**

OR

Q6) a) Differentiate Mac and Hash functions with suitable examples. **[8]**

b) What is PKI? Explain PKI with suitable examples. **[8]**

SECTION - II

Q7) a) Differentiate Mac and Hash functions with suitable examples. **[6]**

b) What is PKI? Explain PKI with suitable examples. **[6]**

c) What are the responsibilities of X.509 standard? **[6]**

OR

Q8) a) What is digital signature? Why is a need of it? Discuss any algorithm of digital signature. **[6]**

b) Explain working principles of HMAC? **[6]**

c) Compare all authentication functions with suitable parameters. **[6]**

Q9) a) Differentiate TLS and SSI with suitable parameters. **[8]**

b) What are the firewall-design principles? Discuss in short. **[8]**

OR

Q10)a) What is intrusion prevention? How can prevent network from intrusions. **[8]**

b) Differentiate Intrusion detection and intrusion prevention system. **[8]**

Q11)a) Discuss Electronic commerce security in detail. **[8]**

b) Explain PEm in details. **[8]**

OR

Q12)Write short notes of the following (Any Two) **[16]**

a) S/MIME

b) PGP

c) Web Security