B.E TI Nov-Dec-2011
Sem-I 2008 course

Total No. of Questions : 12] [Total No. of Pages : 3

P1143

[4064] - 602

B.E. (Information Technology)

INFORMATION ASSURANCE AND SECURITY

(2008 Course) (Sem. - I) (414441)

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

Instructions to the candidates:

1) ***Answers 3 questions from Section - I and 3 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.***
4) ***Figures to the right indicate full marks.***
5) ***Assume suitable data, if necessary.***

SECTION - I

Q1) a) Categories the different attacks. Illustrate, how passive attacks leads to business loss. **[9]**

b) Illustrate how to share and split the secret and its significance in some application. **[9]**

OR

Q2) a) What is the significance of Extended Euclidian algorithm with reference to RSA Algorithm. Illustrate. **[9]**

b) Draw AES block diagram and explain the steps in general. **[9]**

Q3) a) State different modes of operation. Compare these modes. **[8]**

b) How to solve the problem of Non-repudiation. Illustrate that availability of information assets may be hampered because of reliability or security threat. **[8]**

OR

Q4) a) How is the IPSEC helpful to implement Virtual Private Network? **[8]**

b) List and state any tools used for information security. **[8]**

P.T.O.

Q5) a) State the purpose of Needham Schroeder Symmetric Protocol & public key Protocol. Moreover state the purpose of Radius Server & Kerberos Server. [8]

b) Illustrate the Diffiee Hellman Key Exchange Protocol [8]

OR

Q6) a) How IT Law 2000 describes digital signature. [8]

b) Encryption does not solve all the security problems: Justify. [8]

SECTION - II

Q7) a) List and state the channels of Key distribution in Symmetric and Asymmetric Key systems. [8]

b) State different Identity ways and also state the attacks on Identity. [8]

OR

Q8) a) Explain SSL protocol interaction sequence diagram between client and server. [8]

b) Explain different IDS methods with one example each. [8]

Q9) Write short notes on : [18]

a) Industrial Espionage.

b) Phishing Attack.

c) Information Security Policy.

OR

Q10) Write short notes on : [18]

a) Cyber Terrorism.

b) Security by obscurity.

c) IT law awareness.

*Q11)*a) You know the 7 OSI layers. What are the layer wise security concerns? [8]

b) State the Chinese remainder theorem with example. [8]

OR

*Q12)*a) Using Euclidean algorithm calculate gcd (16,20) and gcd (50,60). [8]

b) Compare Linear Cryptanalysis and Differential Cryptanalysis. [8]

❖❖❖❖