B.E. IT. Sem - I
May - June - 2012

Total No. of Questions : 12]

SEAT No. : □

✓

P1473

[Total No. of Pages : 2

[4164]-721
B.E. (Information Technology)
INFORMATION ASSURANCE AND SECURITY
(2008 Pattern) (Sem. - I)

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

Instructions to the candidates:

1) *Answer question 1 or 2, 3 or 4, and 5 or 6 from Section - I and question 7 or 8, 9 or 10 and 11 or 12 from Section - II.*
2) *Answers to the two sections should be written in separate books.*
3) *Neat diagrams must be drawn wherever necessary.*
4) *Figures to the right indicate full marks.*
5) *Use of logarithmic tables slide rule, Mollier charts, electronic pocket calculator and steam tables is allowed.*
6) *Assume suitable data, if necessary.*

SECTION - I

Q1) a) What are the different types of ciphers? Explain in detail. **[10]**

b) Differentiate between Active attacks & Passive attacks. **[8]**

OR

Q2) a) Enlist the Security goals and mechanism in detail. **[10]**

b) State Euclid's Algorithm with example? **[8]**

Q3) a) What are the possible attacks on DES? Explain double DES and triple DES. **[10]**

b) Explain the working of MD5 in detail. **[6]**

OR

Q4) a) Write working of AES algorithm in detail. **[10]**

b) Calculate Cipher text using RSA algorithm. Given data is as follows :- Prime numbers P, Q as 7, 17 respectively & the plain text is to be send is 10. **[6]**

Q5) a) What is PKI? Explain the different PKI Architectures. **[8]**

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

OR

P.T.O.

Q6) a) Explain the Needham/Schroeder Protocol for secret key distribution. [8]

b) How the Digital Certificate creation takes place? Enlist the contents of digital certificate. [8]

SECTION - II

Q7) a) What is IPSEC? How does AH and ESP differs while working under Tunnel Mode and Transport Mode? [10]

b) What is IDS? Explain working of Honeypots as Intrusion detection system. [6]

OR

Q8) a) What is SSL? Explain the SSL architecture in detail. [10]

b) Explain the different phases in IKE-Internet Key Exchange Protocol. [6]

Q9) a) Which are the key participants in SET? How does SET protect payment information from the merchant? Explain the SET model. [10]

b) Write a note on Smart Cards and Chip Cards transaction. [6]

OR

Q10) a) What are the possible attacks on the E-Transaction using cards. [4]

b) Explain the steps to carry out Payment over the Internet. [6]

c) Write a note on Electronic Cash. [6]

Q11) a) Explain in detail about Information Security Policy. [8]

b) What are different methods of Industrial Espionage? How can we prevent Industrial Espionage? [10]

OR

Q12) Write Short Notes on : [18]

a) Indian IT Act.

b) Security by obscurity.

c) Computer Forensics.

✷✷✷