UNIVERSITY OF PUNE

[4364]-791

B. E. Information Technology – 2013

Information Assurance and Security

(2008 Pattern)

Total No. of Questions : 12 **[Total No. of Printed Pages :2]**

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

Instructions :

(1) Assume suitable data, if necessary.

(2) Figures to the right indicate full marks.

SECTION-I

Q1a) Illustrate the idea of securing the software code (Writing & distribution) [12]

Q1b) Illustrate Chinese remainder theorem [6]

OR

Q2a) What is mean by Modular arithmetic & Exponentiation? [12]

Q2b) What is the difference between block and stream cipher? [6]

Q3a) Explain Counter mode of operation. [8]

Q3b) Draw block diagram of SHA-1 and state the general step in the process. [8]

OR

Q4a) Describe the advantages and disadvantages of symmetric and asymmetric key cryptography. [8]

Q4b) Explain permutation and substitution steps in DES [8]

Q5a) List the certifying authorities in India and worldwide. Also list the steps to acquire the digital certificate. [8]

Q5b) Explain role of key distribution centre in symmetric system [8]

OR

Q6a) Draw sequence diagram of Neeham Schroeder protocol and explain [8]

Q6b) Explain how key storage and usage is managed in practice [8]

SECTION – II

Q7a) Illustrate **application programming** level security solution for Peer to Peer chat application which should support authentication, integrity and secrecy. [12]

Q7b) State threats in physical layer [6]

OR

Q8a) Explain SSL authentication protocols. [12]

Q8b) Explain the usage of any tool for instrusion Detection System [6]

Q9a) Write short note on ISO 27001 standard. [8]

Q9b) Explain importance of Security audit of "abc bank of india" [8]

OR

Q10a) Explain and draw a model for ISMS (Information security management system) of PDCA cycle (Plan, DO, Check, Act Phase). [8]

Q10b) What is mobile payment? How it works? [8]

Q11a) Explain in your own words what you understand about the global cooperation required in fighting against cybercrime. [8]

Q11b) Which types of data and techniques used for computer forensics [8]

OR

Q12a) Illustrate Industrial Espionage in IT industry. [8]

Q12b) List some of the cyber crime and respective penalties [8]