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

UNIVERSITY OF PUNE

[4364]-781

B. E. (*Computer & Electronics***)/ Examination - 2013**

Information Security(2008 Course)

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

Instructions:

1 ***Answer any 3 questions from each Section.***

2 *Answers to the* ***two sections*** *should be written in* ***separate answer-books****.*

3 *Black figures to the right indicate full marks.*

4 *Neat diagrams must be drawn wherever necessary.*

5 *Assume suitable data, if necessary.*

SECTION -I

Q.1 A List and explain OSI security services. 8

B Explain the following OSI security mechanisms: 10
(i)Digital signature
(ii)Access control
(iii)Data Integrity
(iv)Authentication exchange

OR

Q.2 A Explain the significance of information security from legal,ethical and professional point of view in an organization. 8

B Differentiate between a block cipher and a stream cipher.What are two general approaches to attack a cipher? 10

Q. 3 A Explain differential and linear cryptanalysis with suitable examples. 8

B Explain block cipher modes of operation. 8

OR

Q. 4 A Explain 3-DES algorithm with example. 8

B Explain AES algorithm with example. 8

Q. 5	A	What are the three broad categories of applications of public key cryptosystems?	8
	B	Explain RSA algorithm and its application.	8
		OR	
Q. 6	A	List four general categories of schemes for the distribution of public keys?	8
	B	Explain Diffie-Hellman key exchange.	8

SECTION II

Q. 7	A	What is message authentication code?	8
	B	What types of attacks are addressed by the message authentication?What is the difference between a message authentication code and a one way hash function?	8
		OR	
Q. 8	A	Explain MD5 algorithm with suitable example.	8
	B	What are the properties of digital siganatures?What requirements should a digital signature satisfy?	8
Q. 9	A	Describe the Transport and Tunnel modes of IPSec.	8
	B	Describe the difference types of Intrusion detection system.	8
		OR	
Q. 10	A	What are differences in SSL and TLS? Explain in detail?	8
	B	What services are provided by IPSec? Explain the ESP header format used in IPSec?	8
Q. 11		Write a short note on any three. (i)PEM & PGP (ii)S/MIME (iii)Radix 64 (iv)Electronic commerce security	18
		OR	
Q. 12	A	Write a short note on secure electronic transaction with a neat diagram show secure electronic commerce components.	8
	B	What is Radix 64 (R64) conversion? Explain with suitable example.	10