

Total No. of Questions : 12]

SEAT No. :

P1472

[Total No. of Pages : 2

[4164] - 715

May - June 2012

**B.E. (Computer Engineering)
INFORMATION SECURITY**

(2008 Pattern) (Elective-IV) (Sem. - II)

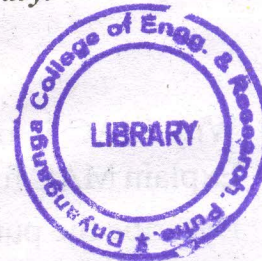
Time : 3 Hours]

[Max. Marks : 100

Instructions to the candidates :-

- 1) Answer any 3 questions from each section.
- 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) Assume suitable data, if necessary.

SECTION - I



- Q1) a) Explain OSI security architecture. [6]
b) Discuss in brief the "security life cycle" [6]
c) Define an active attack Explain any two active attacks with example. [6]

OR

- Q2) a) What is the need of Information security? Explain legal, ethical and professional issues associated with it. [8]
b) i) Construct a playfair matrix with the key largest.
ii) Construct a playfair matrix with the key occurrence. Make a reasonable assumption about how to treat redundant letters in the key.
iii) Using the following playfair matrix encrypt this message.

"Must see you over Cadogan West. Coming at once."

M	F	H	I/J	K
U	N	O	P	Q
Z	V	W	X	Y
E	L	A	R	G
D	S	T	B	C

[10]

- Q3) a) What is the Feistel Cipher structure? Explain in detail. [8]
b) Why RC 5 is suitable for smart card like devices? Explain the working of RC 5. [8]

OR

P.T.O.

