

Total No. of Questions : 6]

SEAT No. :

**P74**

[Total No. of Pages : 2

**APR-17/BE/Insem.-85**

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

**CYBER SECURITY**

**(Elective - III(d)) (Semester - II) (2012 Pattern)**

*Time : 1 Hour]*

*[Max. Marks : 30*

*Instructions to the candidates:*

- 1) *Answer Q1 or Q2, Q3 or Q4, Q5 or Q6.*
- 2) *Neat diagrams must be drawn wherever necessary.*
- 3) *Figures to the right indicate full marks.*
- 4) *Assume suitable data if necessary.*

**Q1)** a) List and explain categories of information security. **[5]**

b) What are the various security services. **[5]**

OR

**Q2)** a) Draw and explain operational model of security. **[5]**

b) What is cryptanalysis? Explain various attacks performed by cryptanalysis. **[5]**

**Q3)** a) What is steganography? What are applications and limitations of steganography? **[5]**

b) Use transposition cipher to encrypt message "WE ARE THE BEST" use key "HEAVEN". **[5]**

OR

**Q4)** a) What is block cipher? Explain counter mode of block cipher. **[5]**

b) Explain operation of DES algorithm in detail. **[5]**

**P.T.O.**

**Q5) a)** What is public key cryptography? Explain RSA algorithm used for public key cryptography. [5]

b) What are different approaches of public key distribution? Explain any one. [5]

OR

**Q6) a)** What is Message digest? Compare MD5 with SHA-1. [5]

b) What is digital signature? Explain digital signature standard. [5]

