

Total No. of Questions :10]

SEAT No. :

**P3434**

**[5670]-710**

[Total No. of Pages : 2

**B.E. (Computer Engg.)**

**INFORMATION AND CYBER SECURITY**

**(2015 Course) (Semester - II) (410251) (End Sem)**

*Time : 2½ Hours]*

*[Max. Marks : 70*

*Instructions to the candidates:*

- 1) Answer Q1 or Q2, Q3 or Q4, Q5 or Q6, Q7 or Q8, Q9 or Q10.
- 2) Neat diagrams must be drawn whenever necessary.
- 3) Figures to the right indicate full marks.
- 4) Assume suitable data, if necessary.

**Q1)** a) Describe linear and differential cryptanalysis with suitable example [5]

b) Distinguish between Substitution and transposition ciphers [5]

OR

**Q2)** a) Explain Operational model of security in detail. [5]

b) What is Transposition Cipher? Use Transposition Cipher to encrypt the plain text "WE ARE THE BEST" use key "HEAVEN" [5]

**Q3)** a) Explain digital signature standard. [5]

b) Describe Elliptic Curve Cryptography [5]

OR

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

b) Write note on application and limitation of stenography. [5]

**Q5)** a) What is Backdoors and Key Escrow in PGP? [9]

b) Describe IPsec protocol with its components and security services. [8]

OR

**Q6)** a) Explain OAKLEY key determination protocol. [9]

b) Explain Secure Electronic Transaction in detail. [8]

**Q7)** a) Describe briefly how IPsec works and enlist its applications. Distinguish between tunnel and transport mode of IPsec [8]

b) Explain in detail password management practices. [9]

OR

**P.T.O.**

- Q8)** a) What are various types of firewall? Discuss limitations of firewall. [9]  
b) Explain need and challenges of intrusion detection system. Define signature based IDS. [8]
- Q9)** a) Discuss PII confidentiality safeguards. [8]  
b) What is cyber stalking? How to identify and detect cyber stalking. [8]

OR

- Q10)** a) Explain personally identifiable information PII. Describe PII impact levels with examples [8]  
b) Write note on Information Protection Law: Indian perspective [8]

