[6180]-284
T.E. (Artificial Intelligence and Machine Learning)
INFORMATION SECURITY
(2019 Pattern) (Semester - I) (318545 C) (Elective - I)

Time : 2½ Hours]   *[Max. Marks : 70*
Instructions to the candidates :
1) *Answer Q1 or Q2, Q3 or Q4, Q5 or Q6 and Q7 or Q8.*
2) *Neat diagrams must be drawn wherever necessary.*
3) *Figures to the right side indicate full marks.*
4) *Assume Suitable data if necessary*

Q1) a) Write a note on Diffie- Hellman key exchange. **[6]**

b) Explain in detail Elliptic Curve Cryptography **[6]**

c) Explain El Gamal algorithm in detail. **[6]**

OR

Q2) a) What is the Chinese remainder theorem & how is it used in public key cryptography? **[6]**

b) How do Fermat and Euler theorems contribute to the RSA algorithm? **[6]**

c) What are the different types of Cryptography. Explain Public Key Cryptography in detail. **[6]**

Q3) a) Explain Secure Hash Algorithm (SHA) in detail. **[6]**

b) Explain Hash Functions Based on Cipher Block Chaining in detail. **[6]**

c) How are digital signatures used to verify the authenticity of digital documents? **[5]**

OR

Q4) a) Write a short note on PKI X.509 Certificate. **[6]**

b) What are message authentication codes & how do they ensure message authentication? **[6]**

c) Which are the different Web Security issues? **[5]**

Q5) a) What are the different types of access control mechanisms and how are they used in network security? **[6]**

b) Explain the need of firewall and its characteristics. **[6]**

c) Explain the concepts of trusted system & Trusted computing. **[6]**

OR

Q6) a) Draw & explain OSI Security architecture. **[6]**

b) Write a note on Host based and network based Honeypot **[6]**

c) What are types of Firewall, and also explain Intrusion prevention system: Host based in detail. **[6]**

Q7) a) What is mean by Proxy servers and Anonymizer? Explain with its categories **[6]**

b) Write a note on Social Engineering. **[6]**

c) Explain Cybercrime Scenario in India. **[5]**

OR

Q8) a) State the Amendments in Indian IT Act. **[6]**

b) Write a note on Phishing. **[6]**

c) State the Classification of Cybercrimes. Write a note on Cybercrime. **[5]**

▶◀ ▶◀ ▶◀