PC1740

[6353]-57

T.E. (AI&DS)

CYBER SECURITY

(2019 Pattern) (Semester - II) (317530)

Time : 2½ Hours]   *[Max. Marks : 70*

Instructions to the candidates:

1) *Answer Q1 or Q2, Q3 or Q4, Q5 or Q6, Q7 or Q8.*
2) *Neat diagrams must be drawn wherever necessary.*
3) *Draw neat figures wherever necessary.*
4) *Figures to the right indicate full marks.*
5) *Use of Calculator is allowed.*
6) *Assume suitable data if necessary.*

Q1) a) Evaluate encryption and decryption using RSA algorithm p=7, q=11, e=17 and M=8. **[8]**

   b) What is authentication? Explain various methods for authentication. **[9]**

OR

Q2) a) User A and B use the Diffie-Hellman Key exchange techniques with common prime q=71 and primitive root α=7. **[8]**

   i) If user A has private key X_A=5 what is A's public key Y_A?

   ii) If user B has private key X_b=12 what is B's public key Y_B?

   b) Distinguish between Kerberos and X.509 authentication service. **[9]**

Q3) a) Describe IPsec protocol with its components & security services. **[9]**

   b) What is PGP? Explain operation of PGP. **[9]**

OR

Q4) a) Explain Secure Socket Layer Protocol? **[9]**

b) Explain VPN architecture with its component. **[9]**

Q5) a) List and explain any two password management practices. **[9]**

b) What is IDS? Explain types of Intrusion detection systems (IDS). **[8]**

OR

Q6) a) Explain methods for intrusion detection system (IDS). **[8]**

b) Explain countermeasures that can be implemented in Cyber security. **[9]**

Q7) a) Define cybercrime? Explain it with its type? **[8]**

b) Write short note on following: **[10]**

i) Cyber stalking.

ii) Hacking.

OR

Q8) a) Define Hacking? Explain different types of hacking. **[8]**

b) Write short note on following: **[10]**

i) Information Protection Law.

ii) PII.

ⓘ ⓘ ⓘ ⓘ