SEAT No. :

P2348

[Total No. of Pages : 2

[5254]-681

B.E. (Information Technology) (Semester - I)

INFORMATION AND CYBER SECURITY

(2012 Pattern)

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 wherever necessary.*

3) *Figures to the right side indicate full marks.*

4) *Assume suitable data if necessary.*

Q1) a) Explain Passive attacks and Active attacks in detail. **[6]**

b) State the Euclids algorithm with example. **[4]**

OR

Q2) a) Draw AES block diagram and state the general steps in detail. **[6]**

b) Distinguish between linear cryptanalysis and differential cryptanalysis.**[4]**

Q3) a) Enlist the requirement of hashfunction and explain working of MD5 algorithm In detail. **[6]**

b) What is Needham Schroeder protocol? Explain with sequence diagram.**[4]**

OR

Q4) a) Define Fermat's theorem with example. **[3]**

b) What is Kerberos? **[2]**

c) Explain Diffie- Hellman Key exchange algorithm with example. **[5]**

Q5) a) Explain SSL hand shake and SSL Record protocol in detail with neat sketch. **[8]**

b) Explain different IDS methods with one example each. **[8]**

OR

Q6) a) Define IKE protocol and explain its aggressive mode and quick mode in brief. **[8]**

b) Describe briefly how IPSec works and enlist its applications? Distinguish between tunnel and transport mode of IPSec. **[8]**

Q7) a) Describe the Indian and global legal perspective oncyber-crime. **[6]**

b) Explain the types of cyber-crime in detail. **[10]**

OR

Q8) a) What is cyber stalking? Explain the types of stalkers. **[10]**

b) Address security issues in cloud computing. **[6]**

Q9) a) Write short note on. **[12]**

i) Indian IT Act 2000 and its challenges.

ii) SQL injection

b) Define and differentiate phishing and pharming? Describe key loggers and Spywares in brief. **[6]**

OR

Q10) Write short note on following

a) Host based Malicious programs: Trap Door, Logic Bombs and Trojan Horse. **[6]**

b) Virus and Worm. **[6]**

c) Proxy server and an anonymizer. **[6]**

○○○