Nov-Dec-2012

[Total No. Of Questions: 12]

Seat No. :
Total No. of Pages : 02

[4264] – 710A
B.E. Computer Engineering
Information Security
(2008 Pattern) (Sem, II)

Time : 3 Hours *Max. Marks : 100*

Instructions to the Candidates :

1) *Answer to the two sections should be written in separate answer books*
2) *Neat Diagrams must be drawn wherever necessary*
3) *Figures to the right indicate full marks*
4) *Assume suitable data , if necessary*
5) *Solve Q1 or Q2 , Q3 or Q4, Q5 or Q6 , Q7 or Q8, Q9 or Q10, Q11 or Q12*

SECTION - I

Q1.a) List and explain attributes of security 08

b) Explain OSI security architecture 08

OR

Q2. a) List and briefly define categories of passive and active security attacks. 08

b) Briefly define Caesar cipher, monoalphabetic Cipher, play fair cipher and transposition cipher 08

Q3. a) Explain with neat diagram DES algorithm 08

b) Explain with example meet-in-middle attack. 08

OR

Q4. a) List important design considerations for Stream cipher. 08

b) Discuss issues in key distribution with respect to secret key cryptography. 08

Q5. a) Explain in details public-key cryptosystems 08

b) Explain in general terms an efficient procedure for picking a prime number. 08

c) What is key generation issue in public-key cryptography ? 02

OR

Q6.a) Explain RSA algorithm 08

b) Explain Diffie-Hellman key exchange algorithm and man-in-the-middle attack. 10

SECTION-II

Q7.a) Explain basic arithmetic and logical functions used in MD5 and SHA-1 operation. 08

b) What is the purpose of the X.509 standard? How is an X.509 certificate revoked. 08

OR

Q8.a) Enlist HMAC design objectives and explain HMAC algorithm with structure. 08

b) Explain how message authentication code (MAC) ensures the integrity of message. Why private and public keys cannot be used in creating a MAC ? 08

Q9. a) Explain the difference between Packet Filtering router and Stateful inspection firewall. 08

b) What services are provided by IPSec ? Explain various applications of IPSec with examples. 08

OR

Q10.a) Explain the architecture of SSL. Differentiate between SSL and TLS. 10

b) What are different types of intruders in the system ? Explain with examples. 06

Q11.a) List and define the principle categories of SET participants. 08

b) What are the Five principal services provided by PGP ? 10

OR

Q12. Write short notes on (Any Three) : - 18

a) Digital Signatures
b) PEM
c) Trusted Systems
d) S/MIME