B.E. (Information Technology) Seventh Semester (C.B.S.)

Computer System Security

P. Pages : 2 NRT/KS/19/3583

Time : Three Hours Max. Marks : 80

Notes :
1. All questions carry marks as indicated.
2. Solve Question 1 OR Questions No. 2.
3. Solve Question 3 OR Questions No. 4.
4. Solve Question 5 OR Questions No. 6.
5. Solve Question 7 OR Questions No. 8.
6. Solve Question 9 OR Questions No. 10.
7. Solve Question 11 OR Questions No. 12.
8. Assume suitable data whenever necessary.
9. Illustrate your answers whenever necessary with the help of neat sketches.

1. a) Distinguish between Monoalphabetic Ciphers and Polyalphabetic Ciphers. Explain example of each. **7**

b) Explain the various types of cryptanalytic attacks on security. **6**

OR

2. a) Explain the modes of operation of DES algorithm. **7**

b) Explain Play-fair substitution technique convert the following text to Cipher text using "MONARCHY" as a keyword "It was disclosed yesterday". **6**

3. a) Write short note on Pseudorandom number generator. **7**

b) Discuss IDEA encryption algorithm. **6**

OR

4. a) Explain Chinese Remainder theorem. **7**

b) Explain characteristics of advanced symmetric block Ciphers. **6**

5. a) Draw and explain MD-5 Hash algorithm in detail. **7**

b) Describe Diffie-Hellman key exchange algorithm in detail what are its weaknesses. **6**

OR

6. a) Write short notes on security of Hash functions and MACS. **7**

b) How confidentiality and authentication are provided with public key cryptography. Support your explanation with proper diagrams. **6**

7. a) Explain in detail about X509 directory authentication service. Describe the format of X.509 Certificate and certificate revocation. **8**

b) Describe Kerberos version 5 with the help of suitable diagram. **5**

OR

8. a) What are the design objectives of HMAC, explain the algorithm. **7**

b) What is digital signature? Explain various properties and its need. **6**

9. a) Explain the ESP protocol of IP Sec in both modes. **8**

b) Explain the general format of PGP message. **6**

b) How confidentiality and authentication are provided with public key cryptography. Support your explanation with proper diagrams. **6**

7. a) Explain in detail about X509 directory authentication service. Describe the format of X.509 Certificate and certificate revocation. **8**

b) Describe Kerberos version 5 with the help of suitable diagram. **5**

OR

8. a) What are the design objectives of HMAC, explain the algorithm. **7**

b) What is digital signature? Explain various properties and its need. **6**

9. a) Explain the ESP protocol of IP Sec in both modes. **8**

b) Explain the general format of PGP message. **6**

OR

10. a) Explain with diagrams the PGP message generations and message reception process. Also mention the importance of public and private key rings in the process. **8**

b) Write short note on S/MIME. **6**

11. a) What are viruses and worms? Describe the virus spreading mechanism. **7**

b) Write short note on firewall. **7**

OR

12. a) Explain secure electronic transaction protocol in detail. **8**

b) Explain the features of Oakley key protocol. **6**

****

B.E. (Information Technology) Seventh Semester (C.B.S.)

Computer System Security

P. Pages : 2 **NIR/KW/18/3583**

Time : Three Hours Max. Marks : 80

Notes : 1. All questions carry marks as indicated.

2. Solve Question 1 OR Questions No. 2