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

Computer System Security

P. Pages : 2 **NRJ/KW/17/4638**

Time : Three Hours * 0 4 7 6 * Max. Marks : 80

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

1. a) Explain Active and Passive attacks in detail. **6**

b) Explain play-fair substitution technique. Convert following text to cipher text using. 'ENGINEERING' as a keyword "Welcome to computer system security". **7**

OR

2. a) Explain any three block cipher modes of operation with neat diagram. **6**

b) Explain simple DES algorithm with neat diagram. **7**

3. a) Explain linked and end-to-end encryption in detail. **7**

b) Write short note on Pseudorandom number generator. **6**

OR

4. a) Explain characteristics of advanced symmetric block ciphers. **7**

b) Explain Chinese Remainder theorem with example. **6**

5. a) Explain RSA algorithm in detail. Perform encryption and decryption using RSA algorithm for the following. **8**
P = 3, q =11, d = 7. m = 5.

b) Explain Hash function authentication requirements. **6**

OR

6. a) Explain Diffie-Hellman Key exchange-algorithm in detail. **8**

b) Differentiate between conventional and public key encryption system. **6**

7. a) Describe secure Hash algorithm (SHA-1) in detail. **7**

b) Explain concept of Digital signature. **6**

OR

8. a) What are the uses of Kerberos? Explain Kerbero's version V4. **6**

b) Explain X-509 directory authentication service. Describe its format. **7**

9. a) Explain data compression using ZIP-in detail. **6**

b) Explain Radix-64 algorithm with example. **8**

OR

10. a) Explain the architecture of Authentication Header and encapsulating security payload in detail. **9**

b) Write a short note on PGP (Pretty Good Privacy). **5**

11. a) Explain Secure Electronic Transaction in detail. **8**

b) Write a note on transport layer security. **5**

OR

12. a) Write notes on **any three.** **13**

i) Intruders
ii) Trusted systems.
iii) DOS
iv) Firewall

****