B.E. (Computer Engineering) Seventh Semester (C.B.S.)

Information Assurance & Network Security

P. Pages : 2 **NRT/KS/19/3595**

Time : Three Hours *0281* 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. Due credit will be given to neatness and adequate dimensions.
9. Assume suitable data whenever necessary.
10. Illustrate your answers whenever necessary with the help of neat sketches.

1. a) State & explain the various security services and mechanisms in details. **9**

b) Explain the substitution and transposition cipher ? Convert the following given sentences into encrypted form : (Caesar cipher) "Welcome to our college party". **5**

OR

2. a) Explain the Chinese Remainder Theorem & find X = ? **8**
where $x \equiv 2 \pmod 5$; $x \equiv 3 \pmod 7$, $x \equiv 4 \pmod 9$

b) Explain about discrete logarithm. **4**

c) Define steganography ? **2**

3. a) Differentiate between differential and linear cryptanalysis. **4**

b) Explain AES algorithm in details. **9**

OR

4. a) Explain MDS algorithm in details. **5**

b) Explain RSA algorithm with key generation. Perform Encryption and Decryption using RSA algorithm for the following values **8**
p = 5, q = 11, e = 3 and M = 9

5. a) Define KDC ? Explain how the digital signature utilize in key management. **5**

b) Explain X 509 certificates with its format. **7**

c) Define one way authentication. **1**

OR

6. a) Describe Diffie-Hellman key exchange algorithm in details. What are the weakness of algorithm. **7**

b) Explain Kerberos V_5 in details. **6**

7. a) Explain in details Handshake protocol with the help of diagram. **6**

b) Explain SSL protocol with role of record layer protocol. **6**

c) Define IPsec. **1**

OR

8. a) Write short notes on : **6**
ESP protocol in both modes.

b) Explain anomaly based intrusion detection system. **7**

9. a) Explain firewall configuration in details. **6**

b) What is viruses ? What are the general phases of a virus. **4**

c) To whom we called a trusted system & explain purpose of it. **4**

OR

10. a) Explain about electronic cash. **6**

b) Explain about chip-card transaction and attacks. **8**

11. a) What is computer forensics ? Explain the use of computer forensics in law enforcement. **7**

b) Discuss about cyber stalking. **6**

OR

12. a) Explain about different online investigation tools used in cyber crimes. **7**

b) Write short notes on : **6**
Cyber Terrorism.

****