Faculty of Science & Technology

Seventh Semester B.Tech. (Computer Science & Engineering/C.E./C.T.) (CBCS) Examination

CRYPTOGRAPHY AND NETWORK SECURITY

Time : Three Hours] [Maximum Marks : 70

INSTRUCTIONS TO CANDIDATES

(1) All questions carry marks as indicated.

(2) Solve Question No. **1 OR** Question No. **2**.

(3) Solve Question No. **3 OR** Question No. **4**.

(4) Solve Question No. **5 OR** Question No. **6**.

(5) Solve Question No. **7 OR** Question No. **8**.

(6) Solve Question No. **9 OR** Question No. **10**.

(7) Due credit will be given to neatness.

(8) Assume suitable data wherever necessary.

(9) Diagrams should be given wherever necessary.

(10) Illustrate your answers wherever necessary with the help of neat sketches.

(11) Use of non-programmable calculator is permitted.

1. (a) What do you mean by network security ? Explain the model of network security in detail. 7

(b) What are different types of attack ? Explain all categories and its subtypes of attack in detail. 7

OR

2. (a) Explain monoalphabetic Cipher in detail and generate Ciphertext for text :

"HAVE A GOOD DAY". 7

(b) Encrypt the message "Money helps to build infrastructure" using Hill Cipher with the key $\begin{pmatrix} 9 & 4 \\ 5 & 7 \end{pmatrix}$.

Show your calculations and results in detail. 7

3. (a) Explain in detail DES, Double DES Triple DES with diagram. 7

(b) Describe the process of key generation in AES. 7

OR

4. (a) Differentiate Block Ciphers and Stream Ciphers. 7

(b) Explain in detail Blowfish algorithm with suitable diagram. 7

5. (a) Explain Fermat's little theorem in detail. 7

(b) Discuss Chinese remainder theorem with suitable example. 7

OR

6. (a) Perform encryption using RSA Algorithm for given data P = 07; 9 = 17; plaintext : 10. Also write steps of the Algorithm. 7

(b) Generate key K_1 and K_2 for Alice and Bob using Diffie-Hellman key exchange Algorithm. Given data : n = 11; g = 7 x = 3 and y = 6. 7

7. (a) What is MAC ? Why it is needed ? What are its types ? Explain in detail. 7

(b) What do you mean by message digest ? Explain MD5 Algorithm with suitable diagram. 7

OR

8. (a) Explain Kerberos version 4 in detail. Also explain its working. 7

(b) Explain requirement of a good hash function in detail. How such requirements can be achieved ? 7

9. (a) Explain in detail the concept and application of VPN in networking. 7

(b) Explain IPsec ESP and AH in detail. Draw suitable diagram. 7

OR

10. (a) Write short notes on the following :

(i) Firewall

(ii) PGP

(iii) Web Security. 7

(b) Explain Intrusion detection and various types of viruses in detail. 7