H Roll No. ....

TIT–704

B. TECH. (CSE/IT)
(SEVENTH SEMESTER)
END SEMESTER
EXAMINATION, Dec., 2023

CRYPTOGRAPHY AND NETWORK SECURITY

Time : Three Hours

Maximum Marks : 100

Note : (i) All questions are compulsory.

(ii) Answer any *two* sub-questions among (a), (b) and (c) in each main question.

(iii) Total marks in each main question arc **twenty**.

(iv) Each sub-question carries 10 marks.

1. (a) Describe the advantages and disadvantages of symmetric and asymmetric key cryptography. (CO1)

P. T. O.

(b) State the Chinese Remainder Theorem and find X for the given set of congruent Equations : (CO1)

$X = 1 \bmod 3$

$X = 4 \bmod 5$

$X = 6 \bmod 7$

(c) Encrypt "LEETCODE" by VIGENERE Cipher where key = 3. (CO1)

2. (a) Let $q = 353$ and $\alpha = 3$, $Xa = 97$, $Xb = 233$. Use the Diffie Hellman Key exchange algorithm to find Ya, Yb and Secret key K. (CO2)

(b) Demonstrate the encryption of the message "GRAPHIC ERA" using Playfair Cipher with the following key "PLACEMENT". (CO2)

(c) Explain the AES algorithm, its steps and various modes with help of a suitable figure. (CO2)

3. (a) (i) What do you mean by message authentication function ?

(ii) Differentiate between SHA-1 and MD-5 algorithm.

(iii) Explain the MD-5 algorithm with the help of block diagram. (CO3)

(b) Explain Diffie Hellman Key Exchange Algorithm with an example. State its uses, advantages and disadvantages. (CO3)

(c) Discuss RSA with computations for public key cryptography. Also perform the encryption and decryption for $p = 7$, $q = 11$, $e = 17$ and $m = 8$. (CO3)

4. (a) Elaborate on the architecture of IP Security (IPsec) and its key components, and enhance your explanation with a suitable diagram. (CO4)

(b) Explain the following concepts : (CO4)

(i) Zombie program and Worm malware.

(ii) Steps involved in SET Transaction.

(c) Define a Firewall and discuss its importance in network security. Give a basic overview of how a firewall works.

(CO4)

5. (a) Provide a comprehensive explanation of the Advanced Encryption Standard (AES) algorithm, its steps, and various modes of operation, along with a suitable diagram. (CO5)

(b) Define wireless Network Security. Define different network security threats and their solutions. (CO5)

(c) Explain SSL version 3 and TLS along with the differences. (CO5)