H Roll No. ....

TIT–704

B. TECH. (CSE) (EIGHTH SEMESTER) END SEMESTER EXAMINATION, Dec., 2022

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 are **twenty**.

(iv) Each sub-question carries 10 marks.

1. (a) Explain the conventional encryption model with proper examples and diagrams. (CO1)

(b) Explain the following : (CO1)

(i) Classical encryption techniques

P. T. O.

(ii) Difference between a block cipher and a stream cipher

(c) Encrypt "Graphic Era" by Caesar Cipher where key = 3. (CO1)

2. (a) State the Chinese Remainder Theorem and find X for the given set of congruent equations : (CO2)

$X = 1 \bmod 5$

$X = 1 \bmod 7$

$X = 3 \bmod 11$

(b) Demonstrate the encryption of the message "ATTACK" using hill cipher with the following key matrix : (CO2)

{2 3
3 6}

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

3. (a) Write short notes on the following : (CO3)

(i) Pseudo-random number generator

(ii) Blum blumshub algorithm

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

(c) 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. (CO3)

4. (a) Explain IP security architecture and its components with a proper diagram. (CO4)

(b) Apply the mathematical foundations of the RSA algorithm. Perform encryption decryption for the following data : P = 17, $q = 7$, $e = 5$, $n = 119$, message = "6". Use Extended Euclid's algorithm to find the private key. (CO4)

(c) Write short notes on the following : (CO4)

(i) Cryptographic Hash Functions

(ii) Secure Hash Algorithm

5. (a) Explain the following : (CO5)

(i) Message Authentication Code (MAC)

(ii) IEEE 802.11 architecture with diagram

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

(c) Define Firewall. Explain its working with the help of diagram, advantages and its importance. (CO5)