(Please write your Exam Roll No.) *Exam Roll No. .....*

END TERM EXAMINATION

SEVENTH SEMESTER [B.TECH] FEBRUARY 2023

Paper Code: ETIT-403 ***Subject: Cryptography and Network Security***

Time: 3 Hours ***Maximum Marks: 75***

Note: Attempt five questions in all including Q. No.1 which is compulsory. Select one question from each unit. Assume missing data, if any.

Q1 (a) Differentiate between monoalphabetic and polyalphabetic cipher. Generate the cipher text of the plain text "Decryption" using the key as DATA. **(4.5)**

(b) Find gcd(a(x), b(x)) for $a(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$ and $b(x) = x^4 + x^2 + x + 1$. **(3)**

(c) Explain the methods of Steganography. **(4)**

(d) Generate the cipher text of text "Transportation" using rail fence with depth 3. **(4.5)**

(e) What is the difference between confusion and diffusion? **(3)**

(f) What is the role of compression in the operation of a virus? **(3)**

(g) Briefly explain traffic confidentiality. **(3)**

UNIT-I

Q2 (a) Explain in brief the block diagram of single round of DES Algorithm and also explain the function of E-box and S-Box. The input to S-box 8 is 100010. What is the output? **(6.5)**

S_8																
	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

(b) Using Play fair encrypt the following message using key committee: **(6)**
"Possessivenessleadscheerfulness1000"

Q3 (a) Explain S-DES in detail and in S- DES 10-bit key is 1000100010. Find the subkey K1 and K2 if **(6)**
P10 = 3 5 2 7 4 10 1 9 8 6
P8 = 6 3 7 4 8 5 10 6

(b) Draw the block diagram of AES and explain shift rows and mix columns in detail? **(6.5)**

UNIT-II

Q4 (a) Explain two methods of Triple DES and its applications? **(6.5)**

(b) Perform encryption and decryption using the RSA algorithm for p=5, q=11, e=3, M=9? **(6)**

Q5 (a) Briefly Explain Diffie-Hellman key exchange? **(6.5)**

(b) What is elliptical curve? **(6)**

P.T.O.

UNIT-III

Q6 Explain the working of SHA-2 algorithm in detail. Differentiate between SHA-2 and MD5. **(12.5)**

Q7 (a) How does PGP provide authentication and confidentiality for email services and for file transfer applications? Draw the block diagram and explain the components. **(7.5)**

(b) Write short notes on **any one** of the following:- **(5)**

(i) Light Weight Cryptography

(ii) Light Weight Cryptography

UNIT-IV

Q8 (a) Differentiate between intrusion detection (IDS) and intrusion prevention system (IPS). **(6)**

(b) Describe the various types of firewalls along-with their advantages and disadvantages. **(6.5)**

Q9 (a) Analyze the Cryptographic algorithms used in S/MIME and Explain S/MIME certification processing. **(7.5)**

(b) What is a Digital Immune System? **(5)**

****