2023

M.Sc.

4th Semester Examination

COMPUTER SCIENCE

PAPER : COS-402

(Cryptography and Steganography)

Full Marks : 50

Time : 2 hours

The figures in the right-hand margin indicate marks.

Candidates are required to give their answers in their own words as far as practicable.

Illustrate the answers wherever necessary.

Answer from **all** the Groups as directed.

GROUP—A

Answer *any* **four** questions from the following : 2×4=8

1. What is product cipher? List their two classes.

2. What is steganalysis?

3. Compare the round keys in DES and AES.

4. Define a cryptographic hash function.

5. What is key less cipher?

6. Differentiate between Digital Watermarking and Steganography.

GROUP—B

Answer *any* **four** questions from the following : 4×4=16

7. Distinguish between the following :

(a) Monoalphabetic and Polyalphabetic cipher

(b) Stream cipher and block cipher 2+2

8. What are the major challenges for steganographic research? 4

9. Encrypt the message "the house is being sold tonight" using Additive cipher with key = 20; ignore the space between words. 4

10. How to get cryptographic decryption key from encryption key? 4

11. Define P-box and its variation. 4

12. Describe active, passive and malicious type of attackers. 4

GROUP—C

Answer *any* **two** questions from the following : 8×2=16

13. *(a)* Consider image block

102	132	68
100	145	95
85	74	85

And secret data = 11011000111001100......
Weighted Matrix

1	2	3
4	0	5
6	7	8

Perform weighted matrix based data hiding (embedding and extraction) scheme and show the stego block and write the step by step procedure.

(b) What is play fair cipher? Find the play fair cipher of the word "VIDYASAGAR". 8

14. Distinguish between diffusion and confusion. Describe DES function. 8

15. *(a)* Consider the original pixel pair (129, 89) and Message Bits M = 10111101101011...... Perform Difference Expansion (DE) Method (embedding) and show stego pixel pair and write the algorithm. Also, perform extraction process of secret massage. Is this method reversible? Suggest any scheme to overcome the disadvantage of this scheme or embed more data bits within the pixel pair.

(b) Consider the original pixel pair (79, 52), Range Table [0-7, 8-23, 24-39,........ 255], Message Bits M = 10111101101011...... Perform Pixel Value Difference Method (PVD) (embedding) and show stego pixel pair. Also, perform extraction process of secret massage and write the algorithm. Is this method reversible? Suggest any scheme to overcome the disadvantage of this scheme. 8

16. Briefly explain the idea behind the AES cryptosystem. 8

[Internal Assessment : 10 marks]

★ ★ ★