(b) In Hill cipher, key matrix is $K = \begin{bmatrix} 19 & 25 \\ 8 & 11 \end{bmatrix}$. Find the inverse of given key matrix and decrypt the message "*AJHAWK*". Assume (A=0, B=1..., Z=25). (5)

[This question paper contains 6 printed pages.]

Your Roll No.....

Sr. No. of Question Paper : 4712 **E**

Unique Paper Code : 32347613

Name of the Paper : Information Security (DSE-3)

Name of the Course : **B.Sc. (H) Computer Science**

Semester : VI

Ramanujan College Library Kalkaji, New Delhi-110019

Duration : 3 Hours Maximum Marks : 75

Instructions for Candidates

1. Write your Roll No. on the top immediately on receipt of this question paper.
2. **All** questions are compulsory from **Section A**.
3. Please attempt any **four** questions from **Section B**.
4. Part of a question must be answered together.
5. Use of basic Calculator is allowed.

SECTION A

1. (a) What is Integer Overflow attack? (2)

(b) What is Traffic Analysis attack? (2)

(c) Explain the term watermarking. (2)

(d) What is Internet of Things (IoT)? (2)

(e) Differentiate between hamming weight and hamming distance. (3)

(f) Briefly explain the three key objectives of computer security. (3)

(g) Why general Caesar cipher (Shift cipher) substitution technique is vulnerable to brute-force attack? (3)

(h) What is Malware? Explain the differences between viruses and worms. (4)

(i) Explain encryption and decryption of Vigenere cipher with suitable example. (4)

(j) Describe the linear block codes and explain the systematic structure of codewords. (4)

(k) Differentiate between the following : (3+3)

(i) Symmetric and Asymmetric key cryptography.

5. (a) What is digital signature? Describe the various properties of digital signature and explain the generic model for constructing the digital signature. (7)

(b) Describe Steganography and its limitations. (3)

6. (a) Describe the Shannon's theory of *Confusion* and *Diffusion* for cryptography. (4)

(b) What is DES? Explain the DES encryption process with suitable diagram. (6)

7. (a) Explain RSA algorithm using suitable example. Why is it advisable to choose large prime numbers in RSA algorithm? (5)

(b) What are the limitations of Internet of Things (IoT) enabled products? (5)

8. (a) In a Diffie-Hellman Key Exchange, Alice and Bob have chosen prime value q = 17 and primitive root = 5. If Alice's secret key is 4 and Bob's secret key is 6, what is the secret key they exchanged? (5)

(ii) Unconditionally secure cipher and Computationally secure cipher.

SECTION B

2. (a) Write short note on the following : (2+2+2)

(i) Boot Sector virus.

(ii) Memory Resident virus.

(iii) Polymorphic virus.

(b) What is Buffer Overflow attack? Explain with suitable example. (4)

3. (a) What is the active attack? Explain different types of active attacks. (5)

(b) Encrypt the message "*I ONLY REGRET THAT I HAVE BUT ONE LIFE TO GIVE FOR MY COUNTRY*" by using given Playfair matrix : (5)

J/K	C	D	E	F
U	N	P	Q	S
Z	V	W	X	Y
R	A	L	G	O
B	I	T	H	M

4. (a) (i) Explain generator matrix and parity check matrix.

(ii) Describe minimum weight of codes.

(ii) How parity check matrix can be used to generate codewords? (2+1+2)

(b) Given the following generator matrix, what will be the encoded messages for the given words 1011 and 01011

$$G = \begin{bmatrix} g_0 \\ g_1 \\ g_2 \\ g_3 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix} \quad (5)$$