[This question paper contains 5 printed pages.]

Your Roll No.....

Sr. No. of Question Paper : 1175 **A**

Unique Paper Code : 32347613

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

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

Semester : VI

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) Differentiate between symmetric key encryption and asymmetric key encryption. (3)

P.T.O.

(b) Explain the CIA Triad. (3)

(c) Which cryptosystem (cipher) is referred to as perfect secrecy and why? (3)

(d) Briefly explain OSI security architecture. (3)

(e) What are the limitations of Internet of Things (IoT) in the field of medicine? (3)

(f) Differentiate between Vernam cipher and Vigenere cipher with the help of suitable examples. (4)

(g) Differentiate between mono-alphabetic and poly-alphabetic substitution ciphers using suitable examples. (4)

(h) What is the difference between active and passive security attacks? (4)

(i) Write a short note on the following malicious codes :

- Trojan Horse
- Worms
- Rabbit
- Logic Bomb (4)

(c) Explain syndrome decoding with suitable example. (4)

7. (a) What is a digital signature? Describe the various attacks possible on the digital signature? (4)

(b) Briefly explain zero - day attack. (2)

(c) Differentiate among resident virus, transient virus, boot sector virus and polymorphic virus. (4)

8. (a) Briefly explain hill cipher. Encrypt the message "SECURITY" using the hill cipher with the given

$$2\text{x}2 \text{ key} = \begin{bmatrix} 7 & 3 \\ 2 & 5 \end{bmatrix}. \quad (6)$$

(b) What is stack smashing? How can we protect our stack from being overwritten by the attacker? (4)

(j) What are the various parameters of the hamming code? (4)

SECTION – B

2. (a) Differentiate between substitution cipher and transposition cipher with the help of suitable examples. (4)

(b) How do you identify whether a given cipher text is based on substitution or transposition? (2)

(c) Decrypt the following message using rail-fence cipher with key = 3: (4)

"CTAAERCTRPORP YNNTOKEUIYYGHDWSR".

3. (a) Explain the Feistel cipher structure in detail. (6)

(b) Perform the encryption of plain text (m) = 2 and decryption of the generated cipher text (c) using the RSA Algorithm. (Given: p=3,q=11) (4)

4. (a) Explain the steps of Diffie - Hellman key exchange protocol. What is the most common attack on this protocol? (6)

(b) Encrypt the following message using playfair cipher :

Keyword: PLAYFAIR

Plain Text: INFORMATIONSECURITY (4)

5. (a) What is Buffer Overflow attack? Explain with suitable example. (5)

(b) Explain various techniques of viruses gaining control over a program with the help of suitable diagrams. (5)

6. (a) What are the error detecting and error correcting capabilities of a block code? (2)

(b) What is a parity check matrix? Consider the generator matrix of the (7, 4) linear code as given below :

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

Determine the corresponding Parity Check Matrix. (4)