[This question paper contains 4 printed pages.]

Your Roll No.....

Sr. No. of Question Paper : 3033 **H**

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. Attempt any **four** questions from **Section B**.
4. Parts of a question must be answered together.
5. Use of basic Calculator is allowed.

Section A

1. (a) What is confidentiality, authentication, and availability in context of information security? (3)

   (b) Consider the following C code: (3)

```
unsigned int x = 65535;
unsigned int y = 2;
unsigned int z = x + y;
printf ("The value of z is %u", z);
```

What is the value of z when

(i) This code is executed on 16-bit compiler?

(ii) This code is executed on 32-bit compiler?

(c) How is public key cryptography used to achieve the following security objectives? (3)

(i) Only Authentication

(ii) Only Confidentiality

(iii) Authentication and Confidentiality simultaneously

(d) Describe any 2 security threats to mobile devices security. How can they be mitigated? (3)

(e) Write short notes on **(Any two)** : (4)

(i) Root Kits

(ii) Trojan Horse

(iii) Logic Bomb

(f) What is the difference between the Vigenere Cipher and the One-Time Pad Cipher? Which one provides stronger security, and why? (4)

(g) What is syndrome decoding in the context of error-correcting codes, and how is it used to correct errors in a received message? (5)

(h) What is a columnar cipher, and how does it work? Encrypt the message "DEFENDTHEEASTWALL OFTHECASTLE" using a columnar cipher with the keyword "13524". (5)

(i) Explain any three active attacks with suitable examples. Which type of attack is more difficult to detect - active or passive and why? (5)

Section B

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

$$2\times2 \text{ key} = \begin{bmatrix} 7 & 3 \\ 2 & 5 \end{bmatrix}. \quad (5)$$

(b) List the security services provided under X.800 standard. Briefly describe any four services. (5)

3. (a) Using RSA algorithm, encrypt and decrypt a message with the following parameters: p=3, q=11, e=7, and M=5. Show all of your steps. (5)

(b) What is buffer overflow vulnerability? How can an attacker use stack smashing to overwrite stack memory in a purposeful manner? (5)

4. (a) Briefly describe the working of Data Encryption Standard (DES) algorithm with the help of a suitable diagram. What is "avalanche effect" in DES algorithm? (5)

(b) What is steganography and how is it different from cryptography? Give an example of a situation

where steganography would be a more suitable than cryptography for secure communication. (5)

5. (a) Explain how man-in-the-middle attack works. Provide an example to illustrate your answer. (5)

   (b) What is a digital signature and digital certificate? Explain the working of it. (5)

6. (a) Alice and Bob agree to use Diffie-Hellman Algorithm to exchange the secret key. They decided to use 23 as the prime number and 5 as the primitive root of 23. Alice chooses a private key of 6 and Bob chooses a private key of 15. What is the shared secret key that they can use for secure communication? (6)

   (b) How do digital watermarking techniques protect against intellectual property theft in the music industry? (4)

7. (a) Consider a (6,3) linear block code defined by the generator matrix (5)

$$G = \begin{matrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{matrix}$$

   (i) Determine if the code is a Hamming code?

   (ii) What is the minimum distance of the code?

   (iii) How many errors can the code detect?

   (iv) How many errors can the code correct?

   (v) Find the decoding table for the linear block code.

   (b) Differentiate between confusion and diffusion with suitable examples in context of cryptography. (5)