No. of Printed Pages : **2**

Sl. No.

C8-R4 : INFORMATION SECURITY

NOTE :

1. **Answer question 1 and any FOUR questions from 2 to 7.**
2. **Parts of the same question should be answered together and in the same sequence.**

Time : 3 Hours **Total Marks : 100**

1. (a) Differentiate between Symmetric Key and Asymmetric Key Cryptography.

(b) Enumerate and define the desired properties of a blocks in block cipher.

(c) Define second preimage resistance.

(d) What is perfect security ? How can an encryption algorithm become perfectly secure ?

(e) Encrypt the message "the house is being sold tonight" using Autokey cipher to get cipher text. Ignore the space between words. Consider the key = (7).

(f) Encipher your message "Move forward" by play fair technique and MONARCHY as key.

(g) The encryption key in a transposition cipher is (3, 1, 5, 2, 6, 4). Find the decryption key. **(7x4)**

2. (a) What is birthday attack ? How it is used in cryptography ? Explain in detail.

(b) What is Kerberos ? What problem was Kerberos designed to address ? In Kerberos, when Bob receives a Ticket from Alice, how does he know it is genuine ? **(9+9)**

3. (a) List the main features of the SHA-512 cryptographic hash function. What kind of compression function is used in SHA - 512 ?

(b) Explain output feedback mode of DES. Compare it with cipher feedback mode. **(9+9)**

4. (a) Which type of information might be derived from a traffic analysis attack ?

(b) What is message integrity ? Does integrity differ from secrecy or confidentiality or is it implied ?

(c) What is the Diffie-Hellman Key exchange algorithm and give detail explanation of the algorithm ? **(5+4+9)**

5. (a) RIPEMD-160- a variant of MD5 algorithm, explain and give its pseudo code.

(b) Explain in brief RC4 stream cipher, also giving the algorithm. **(9+9)**

6. (a) Explain the importance of prime numbers in the field of cryptography.

(b) What are the requirements of public key cryptography system ? Explain the characteristic of public key cryptography.

(c) Distinguish between message integrity and message authentication. **(6+6+6)**

7. (a) What are the limitations of message authentication ? Explain properties and requirements of digital signature.

(b) Explain in detail about the followings :

(i) Fermat's theorem

(ii) Euler's theorem

(iii) Chinese Remainder theorem **(9+9)**

- o 0 o -