No. of Printed Pages : **2**

Sl. No.

C8-R4 : INFORMATION SECURITY

NOTE :

1. **Answer question 1 and any FOUR from questions 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 Mono Alphabetic Cipher and Poly Alphabetic Cipher.

(b) What do you understand by Message Integrity ? How does Digital Signatures provide Message Integrity ?

(c) Explain Cipher Feedback (CFB) Mode and how it differs from Electronic Codebook (ECB) and Cipher block Chaining (CBC).

(d) Why do we need Pseudo Random Number Generator (PRNG) in Cryptography ?

(e) What is Message Authentication Code and briefly explain its uses.

(f) Briefly describe how "Chosen Cipher Text" attack is possible on RSA.

(g) Why Key Exchange is a problem in Symmetric Key Cryptography ? Explain Deffie Hellman Key Exchange Algorithm. **(7x4)**

2. (a) What is Extended Euclidian Algorithm ? Find the multiplicative inverse of 23 in Z_{100}.

(b) Define Fermat Little Theorem. Compute the remainder of 7103 when divided by 17 using Fermat Little Theorem.

(c) Discuss the significance of Prime Numbers in Cryptography and how are large prime numbers generated for RSA algorithm. **(6+6+6)**

3. (a) Differentiate between Asymmetric Key Cryptography over Symmetric Key Cryptography.

(b) Describe the role of Key Distribution Center (KDC) in Symmetric Cryptosystem. Differentiate between Flat Multiple KDCs and Hierarchical Multiple KDCs.

(c) What is Birthday Attack in Cryptography ? Explain in detail. **(6+6+6)**

4. (a) Can we use Secret Key (Symmetric Key) to both sign and verify the signature ? Give reasons for your answer. What is the main difference between Encryption and Digital Signatures ?

(b) Explain the working of Key Generation Round in Data Encryption Standard (DES). What is avalanche effect ?

(c) What is Hashing ? Explain Cryptographic Hash Function Criteria with neat diagrams. **(6+6+6)**

5. (a) Is Advanced Encryption Standard (AES) faster than Data Encryption Standard (DES) ? Write in detail about the working of Encryption in AES.

(b) What is Message Digest ? Explain MD5 algorithm which is used to generate the Message Digest for the given message. **(9+9)**

6. (a) Describe how Man in the Middle Attack can be performed on Diffie-Hellman Key Exchange algorithm using appropriate example.

(b) Explain Hash Based Message Authentication Code (HMAC) algorithm in detail.

(c) Explain Blum-Blum-Shub approach for generating secure Pseudo Random Numbers. **(6+6+6)**

7. (a) With appropriate example, explain the concept of ElGamal Public Key Cryptosystem.

(b) Solve the simultaneous congruencies using Chinese Remainder Theorem :

(i) $x \equiv 2 \bmod 3$

(ii) $x \equiv 4 \bmod 5$

(iii) $x \equiv 5 \bmod 7$

(9+9)

- o 0 o -