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) List different attack models. Name some active and passive attacks.

b) How a hash function can be used to provide message authentication without using a key?

c) Differentiate between Direct Digital Signature and Arbitrated Digital Signature.

d) Explain the factorization and discrete logarithm problems. Explain how those are used in cryptography?

e) Explain Meet-in-the-middle attack in Data Encryption Standard (DES).

f) Explain Next bit test and its use in Information Security.

g) Compute Euler's Totient function, φ(29791).

(7x4)

2.

a) Describe various Classical Encryption Techniques & also draw the simplified model of Conventional Encryption.

b) Explain how Pseudo Random Number Generator works?

c) Define linear congruence. What algorithm can be used to solve an equation of type $ax \equiv b \pmod{n}$? How can a set of linear equations be solved?

(8+5+5)

3.

a) State the difference between S-DES and DES. Explain S-DES in detail.

b) What is Diffie-Hellman key exchange algorithm? How does man-in-the-middle attack break the security of it? How this attack can be prevented?

(10+8)

4.

a) List and briefly define types of cryptanalytic attacks. How these are different from attacks on digital signatures.

b) Using the Euclidean algorithm, find the greatest common divisor of the following:

i) 24 and 320

ii) 401 and 700

c) What is difference between block cipher and stream cipher?

(6+6+6)

5.

a) Discuss various encryption algorithm modes for block ciphers.

b) What is Fast Exponentiation? Which cryptography algorithm requires fast exponentiation? Write steps of one fast exponentiation algorithm.

(9+9)

6.

a) Use Hill Cipher to decrypt the message:

"IUVAFSLDNNLDWMCOTKGMCHEZ" using key $\begin{bmatrix} 3 & 2 \\ 5 & 7 \end{bmatrix}$

b) List the main features of SHA-512 Cryptographic Hash Functions? Explain what are the applications of SHA-512?

(10+8)

7. Write short notes on the following:

a) Chinese Remainder theorem.

b) Principle and operation of RSA.

c) Finite Field Arithmetic.

(6+6+6)