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) What are goals (aspects) of Information Security? Comment on each one of its benefit in brief.

b) Enumerate and define the desired properties of a block cipher?

c) What is the purpose of Modes of Operations in symmetric – key encipherment and name its modes of operation.

d) Comment on Random numbers v/s Pseudo-random numbers.

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

f) Differentiate between a Private key and a Public key as asymmetric-key cryptography.

g) Which type of information might be derived from a traffic analysis attack?

(7x4)

2.

a) Differentiate between cryptanalytic attack and non-cryptanalytic attacks. Explain the non-cryptanalytic attacks after categorizing them into groups related to the security goals.

b) Use the extended Euclidean algorithm to find the inverse of $x^4 + x^3 + 1$ in $GF(2^5)$ using the modulus $x^5 + x^2 + 1$.

c) Assume that n is non-negative integer.

i) Find gcd (3n +1, 2n + 1)

ii) Using the result of **[Q.No. 2. c), i)]**, find gcd (301, 201) and gcd (121, 81).

(8+4+6)

3.

a) Comment on the solution of single variable equation of the form $ax \equiv b \pmod n$. Write algorithm to solve such equation and use this algorithm to solve the equations.

i) $14x \equiv 12 \pmod{18}$

ii) $4x + 6 \equiv 4 \pmod 6$

b) Draw the block diagram showing Encryption and Decryption with DES.

c) What are the weaknesses of DES in its design and in its cipher key? Explain them.

(8+4+6)

4.

a) Explain Chinese Remainder Algorithm and its use in Information Security.

b) Discuss the procedure to generate the pseudo random number. Explain linear congruential method. How are the random number generators evaluated? Is it possible to apply these evaluation tests to linear congruential method? Comment on it.

(7 +11)

5.

a) Explain MAC. Why is it needed? Comment on the security of it.

b) What is MDC? Explain it. How does it differ from MAC?

(10+8)

6.

a) What is the role of Cryptographic Hash function? What are the essential properties of Hash function? Explain them.

b) List the main features of SHA-512 Cryptographic Hash Functions? Explain what kind of compression function is used in SHA-512?

(10+8)

7.

a) Differentiate between conventional signature and digital signature.

b) Explain the digital signature process, the need for keys and advantages of signing the digest of the message.

c) Comment on the security services directly provided by digital signature.

(4+10+4)