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) How are cryptographic system characterized? Explain each characteristic in one line.
b) Explain encrypt-decrypt-encrypt variant of DES.
c) Explain Blum-Blum-Shub approach for generating secure pseudo random numbers.
d) Explain a situation in cryptography in which an attack based on birthday paradox is possible.
e) Perform an attack on RSA algorithm when $\varnothing(n)$ is known.
f) Find the multiplicative inverses of all nonzero elements of Z_7.
g) Write an algorithm to test the primality of integer n where $n=2^k q$, k, q are integers $k > 0$, q is odd.

(7x4)

2.

a) What do you mean by cryptanalysis? Explain differential cryptanalysis attack on DES.
b) Explain output feedback mode of DES. Compare it with cipher feedback mode.
c) What do you mean by 'confusion' and 'defusion'?

(8+8+2)

3.

a) Explain ANSI X 9.17 PRNG standard. What are the factors responsible for the strength of the method?
b) Write the algorithm for ElGamal encryption and decryption.
c) How 'main-in-the-middle' attack can be performed on Diffie-Hellman key exchange algorithm?

(6+8+4)

4.

a) What are characteristics of cryptographic hash function?
b) What is RIPEMD-160? Write pseudo-code for it.
c) Write the four stages in AES. Explain each to the point.

(4+8+6)

5.

a) Define digital signatures. Explain digital signature standard based on RSA algorithm
b) Give the steps for constructing $GF(2^m)$ and hence give the elements of $GF(2^4)$.
c) Where do we use random numbers in cryptography? Write the criteria used to validate a sequence of numbers to be random.

(8+6+4)

6.

a) What is Message Authentication Code? Write four situations where it is used.
b) Explain Message Authentication Code based on DES.
c) Write a hash function giving rise to a hash value having effectiveness of 2^{-128}.

(6+8+4)

7.

a) Explain RC-4 stream cipher, also giving the algorithm.

b) Explain the key distribution scenario in which each user shares a unique master key with the key distribution centre.

(9+9)