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) Explain the active security attacks.

b) Find the inverse of given matrix under modulo 29:

$$\begin{bmatrix} 12 & 16 \\ 2 & 28 \end{bmatrix}$$

c) Calculate phi(240) using Euler's phi-function.

d) Calculate 5^{23} mod 33 using fast exponentiation method.

e) Find the inverse of 30 in the modulus of 1033 using extended Euclidean algorithm.

f) Explain the round key structure of DES.

g) Explain Interactive Proofs and Zero-Knowledge Proofs.

(7x4)

2.

a) List out the properties of ring and field structures using suitable example.

b) Let G = Z_{12}*. Show that the group is cyclic group. Find out the primitive elements in it.

c) Calculate $z = x + y$ where $x = 123$ and $y = 334$, assume that system accepts only numbers less than 100.

(6+5+7)

3.

a) Explain AES transformation functions.

b) What is trap-door one-way function? Explain the Four possible approaches to attack the RSA algorithm.

(9+9)

4.

a) What is digital signature? Explain ELGAMAL digital signature scheme.

b) List out the problem arises while distributing symmetric key and asymmetric key. Explain how X.509 has standardized the asymmetric key distribution.

(9+9)

5.

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

b) What is Kerberos? What are the roles of authentication and ticket granting server in it? List the Drawbacks and limitations of Kerberos.

c) What is Man-in-the-middle attack in Diffie-Hellman algorithm? How it can be prevented?

(4+6+8)

6.

a) How does a birthday attack on a hashing algorithm work?

b) What is Cipher Block Chaining (CBC) Mode? Explain the security issues and error propagation in CBC.

c) List and explain the requirements for a Cryptographic Hash Function.

(4+6+8)

7.

a) What are Pseudorandom number generator (PRNG) and Pseudorandom function (PRF)? Define two criteria used to validate that a sequence of numbers is random.

b) Differentiate Differential Cryptanalysis and Linear Cryptanalysis.

c) Find the result of $(x^7+x+1) \otimes (x^6+x^4+x^2+1)$ in GF(2^8) with irreducible polynomial $(x^8+x^4+x^3+x+1)$ using polynomial representation only.

(5+5+8)