CE4-R3: NETWORK SECURITY AND CRYPTOGRAPHY

NOTE:

> **1. Answer question 1 and any FOUR questions from 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 security attacks classified?

b) Which statistical distribution do pseudo-random numbers follow? What are characteristics features of these numbers?

c) What are the basic steps involved in elliptic curve cryptography?

d) What are the requirements for a Hash function?

e) Illustrate two-way authentication procedure in X.509.

f) If P is a set of all prime numbers then any positive integer can be written uniquely, how?

g) Define a finite field of order p. Discuss arithmetic operations in GF(2).

(7x4)

2.

a) How are polyalphabetic ciphers implemented and how are they superior to monoalphabetic ciphers?

b) Explain Euclid's algorithm.

c) Given polynomials $f(x)=x^3+x^2+2$ and $g(x)=x^2+x-1$. Is g(x) a factor of f(x)? Show all your calculations.

(6+6+6)

3.

a) Show and explain Feistel encryption and decryption algorithms.

b) How is double DES achieved? Under what condition the above is reduced to single encryption?

(10+8)

4.

a) Explain key generation, encryption and decryption in the RSA algorithm?

b) What is the difficulty posed to an opponent when Diffie-Hellman Key exchange algorithm is used in public key cryptography? Show necessary steps to support your answer.

(9+9)

5.

a) Discuss basic requirements for Kerberos services.

b) Illustrate various kinds of exchanges amongst clients, Authentication server, Ticket Granting Server and service providing server in Kerberos.

(8+10)

6.

a) How are transport and tunnel nodes used in IPsec Encapsulating Security Payload (ESP) service?

b) What are the various controls used by a firewall?

c) Differentiate between circuit-level and Application-level firewalls.

(8+5+5)

7.

a) Show and explain HMAC structure.

b) How is Authentication achieved in Pretty Good Privacy?

c) What are the various techniques for password checking?

(7+6+5)