CE4-R3: NETWORK SECURITY & CRYPTOGRAPHY

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) "Strong primes" are prime numbers with certain properties that make their product difficult to factor by specific factoring methods. Explain the properties to be satisfied by the strong prime numbers.
b) Describe linear congruential generators. Explain their limitations in cryptography.
c) Discuss the role of Ticket Granting server in inter realm operations of Kerberos?
d) Why is SHA more secure than MD5?
e) Discuss the purpose of Diffie-Hellman algorithm?
f) What are the differences between Stream Cipher and Block Cipher?
g) How does IPSec offer the authentication and confidentiality service?

(7x4)

2.

a) Draw the general structure of DES and explain encryption decryption process.
b) Discuss the advantages of AES over DES algorithm.
c) Write a note on 3DES approach.

(8+5+5)

3.

a) How does PGP provide confidentiality and authentication service for e-mail and storage applications? Draw the block diagram and explain its components?
b) What are the functions provided by S/MIME? Explain in detail.

(12+6)

4.

a) What is an Euler phi function? Explain how to use it to compute inverse of an element modulo n? Find $(11)^{-1}$ mod 7.
b) What is a firewall and what are its limitations? Why do corporate houses implement more than one firewall for security?

(10+8)

5.

a) Explain briefly about MD5 message digest algorithm.
b) Explain RSA algorithm? What is its use? Discuss with example.

(10+8)

6.

a) Discuss two security mechanisms applied at the application layer. Are they safer than those applied at the lower network layer? Justify your answer.
b) Discuss about the X.509 framework for the provision of Authentication Service.
c) How is an X.509 certificate revoked?

(6+8+4)

7.

a) What is Digital Signature? Discuss about the RSA approach and the DSS approach of Digital Signature.
b) Explain the Electronic Code Book (ECB) encryption mode which allows block ciphers to provide confidentiality for message of arbitrary length.

(10+8)