CE4-R3: NETWORK SECURITY & 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. Critically comment on the following:

a) Hybrid crypto system is preferred over symmetric and public key encryptions systems.

b) Message authentication using Hash function.

c) Public key authentication in the growth of e-commerce.

d) Three-way handshake is a security threat.

e) Security policy of any organization.

f) Digital signature generation in DSS.

g) Chinese Remainder Theorem and its application.

(7x4)

2.

a) What is a replay attack? How can this be prevented?

b) Describe a Brute Force attack on a digitally signed message. Discuss the complexity of the brute force attack. How can the complexity of the attack be increased without changing the size of the key?

c) Compare the distinct features of SHA-1 and MD-5 algorithms.

(6+6+6)

3.

a) Explain the basics of Encrypted Key Exchange (EKE) protocol. How is the EKE protocol implemented with the Diffie-Hellman protocol? Describe the disadvantages of the EKE protocol and explain, how the augmented EKD (A-EKE) protocol can be used to overcome these disadvantages.

b) Kerberos uses three different kinds of secret keys: the login key, the ticket-granting key and session key. Explain the need for each of these keys. In particular, how the security offered by Kerberos is weakened if we made use of just the login key or just the session key and login key, instead of the three keys.

(10+8)

4.

a) What types of attacks are addressed by message authentication? What are some approaches to produce message authentication and what is a message authentication code?

b) What are the general guidelines of an efficient procedure for prime number generation?

c) In RSA-public key encryption scheme, each user has a public key, p and a private key, r. Suppose Sachin leaks his private key. Instead of generating a new modulus, he decides to generate a new public and a new private key. Is this safe? Justify.

(6+6+6)

5.

a) A pseudorandom process is a process that appears random but it is not. What is a pseudorandom sequence in a pseudorandom process? What is a cryptographically secured pseudorandom sequence?

b) Comment on the ways of protection an internal network using firewalls from the following attacks:
   i) SMTP Server Hijacking
   ii) Denial of Service

c) Given a speed of a current ordinary computer, estimate the amount of time necessary to crack a DES encryption by testing all possible 2^{56} possible keys.

(6+6+6)

6.

a) Discuss five benefits of IPSec as a security protocol.

b) Briefly explain, how Netscape Navigator and Internet Explorer implemented SSL technology.

c) Compare and contrast S-MIME and PGP protocols.

(6+6+6)

7.

a) What is the difference between authentication and non-repudiation?

b) Discuss two security mechanisms applied at the application layer. Are they safer than those applied at the lower network layer? Justify your answer.

c) Explain why the product of two relatively simple ciphers, such as a substitution and a transposition, can achieve a high degree of security.

d) Are DES and AES streams block ciphers? Give reasons.

(5+5+5+3)