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.

a) Why can't a symmetric cipher be used for a digital signature?

b) A hard disk is to be encrypted sector by sector. A suitable cryptographic algorithm with a 512-byte block size is chosen. What are some of the characteristics to be considered when choosing modes of operation?

c) Why session keys are required? What are the advantages?

d) What is a fingerprint in PGP system? How to import a public key of a person into your key ring?

e) Compare and contrast between SSL and SET?

f) S/MIME allows messages to be signed and encrypted. Should information be signed or encrypted first? What would be the difference?

g) List four techniques used by firewalls to control access and enforce a security policy.

(7x4)

2.

a) Consider an ideal (only brute force attack possible) cryptographic algorithm using a *k* bit key. What is the complexity of the brute force attack? How can you increase the complexity of attack without changing the size of the key?

b) If a bit error occurs in the transmission of a cipher-text character in 8-bit CFB mode, how far does the error propagate?

c) What is *avalanche* effect? Why is it an important criterion for encryption?

(8+5+5)

3.

a) What are the different ways of distributing keys? Describe the Diife-Hellman Key Exchange Algorithm.

b) What primitive operations are used in RC5?

c) Why Blowfish is not suitable for smartcard-based applications?

(10+5+3)

4.

a) Perform encryption and decryption using the RSA algorithm using the following parameters: p=7,q=11,e=17; M=8

b) What is a replay attack? Explain with an example. Discuss its consequent ices.

(10+8)

5.

a) Consider two nodes A and B in a WAN apart by multiple hops. If both of them know each other's public keys, suggest a method to establish a communication between them that provides confidentiality, and message authenticity.

b) What is the birthday attack? How does it relate to a security problem?

c) Why MD5 is used to compute digital signatures of huge documents instead of simply encrypting it using RSA? How can the receiver of this document check on the digital signature and make sure it was really signed by the person who sent it?

(8+4+6)

6.

a) How SSL and IPSEC perform authentication and key exchange?

b) How do you prevent IP address spoofing and source routing attacks using a Packet filtering router?

(10+8)

7. Write short notes on the following:

a) Kerboros authentication service

b) PGP

c) Security Associations in IPSEC

(6+6+6)