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) Distinguish between vulnerability, threat and control.

b) Preserving confidentiality, integrity and availability of data is a restatement of the concern over interruption, interception, modification, and fabrication. How do the first three concepts relate to the last four?

c) Can message confidentiality and message integrity protection be applied to the same message? Why or why not?

d) Does PKI use symmetric or asymmetric encryption? Explain your answer.

e) How can the same key be reused in triple DES?

f) Justify the inclusion of SSL layer in between application layer and transport layer.

g) Compare and contrast between challenge/response tokens and time-based token for user authentication.

(7x4)

2.

a) What parameters identify an Security Association (SA) and what parameters characterize the nature of a particular SA?

b) What is a firewall and what are its limitations? Why corporate houses implement more than one firewall for security?

c) Briefly explain the ESP protocol along with its different mode of operations.

(6+6+6)

3.

a) Describe in brief, the basic steps performed in simplified DES scheme.

b) What is the security purpose for the fields, such as sequence number, of an IPSec packet? Briefly explain.

c) How does Kerberos works?

d) State the advantages of using Cipher Block Chaining (CBC) mode over Electronic Code Book (ECB) mode.

(6+4+4+4)

4.

a) 'Virtually all symmetric block encryption algorithms are based on a structure referred to as a Feistel block cipher' State whether this statement is true or false. Justify your answer. Mention the basic parameters and design functions on which the exact realization of Feistel Chipher depends.

b) Describe in brief the basic steps performed in a simplified DES scheme.

c) Comment on the strength of the simplified DES scheme.

(9+6+3)

5)

a) Why do MD4, MD5 and SHA-1 require padding of messages that are already in multiples of 512 bits? What are minimal and maximal amount of padding in each of these cases?

b) What is S/MIME and how does it works? Briefly explain.

c) What is electronic money? Why is anonymous offline electronic money is dangerous? Discuss double spending problem.

(6+6+6)

6.

a) What are the typical contents of a digital certificate? Compare and contrast self-signed certificate and cross-certificate.

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

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

d) 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.

(5+5+4+4)

7. Write short notes on any **three** of the following:

a) Digital envelope

b) Intrusion detection

c) Security with XML

d) Pretty Good Privacy

e) AES

(3x6)