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 statements:

a) The concept of product cipher is based on confusion and diffusion function.
b) Symmetric key cryptography does not provide no-repudiation.
c) Chaining mode makes block cipher safer.
d) The Diffie-Hellman technique was the first practical public key crypto algorithm.
e) AH in IPsec is responsible to prevent replay attack.
f) Packet filter is able to control flow between internal and potentially hostile networks.
g) Meet-in the middle attack can be prevented by 3-DES encryption.

(7x4)

2.

a) Compare symmetric and asymmetric key cryptography on the basis of their performance.
b) State some typical situations where public key techniques can be used effectively.
c) 'Attack against RSA exploit mathematical properties of messages and the keys that encrypt them' – Explain using examples of these attacks.

(6+6+6)

3.

a) What is a replay attack? How can this be prevented?
b) Discuss the properties required of a hash function to produce a secure message digest. Considering a brute force attack on a digitally signed message of length n bits, determine the time complexities of the computational properties of the hash function.
c) Compare the distinct features of SHA-1 and MD-5 algorithms.

(5+[4+4]+5)

4.

a) In a Secured Socket Layer (SSL) connection, is the session key chosen by the client or the server? How is it communicated to the other party?
b) Preety good Privacy (PGP) uses the following approach for generation the session keys that are used in encrypting the body of the e-mail message. A random secret key is generated by the sender, which is used for encrypting the message body. The sender then encrypts this secret key using receiver's public key and the result is appended to the encrypted message.

   An alternative approach would be to use an iterative protocol, such a Diffie-Hellman exchange, to decide the session keys. Explain why this approach would be inappropriate in the context of secured e-mail application.
c) 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 three.

(6+6+6)

5.

a) How will you justify the need of IP security along with other security measures?

b) What types of protection are provided by transport and tunnel modes?

c) What are the characteristics of Bastion Hosts? How are Bastion Hosts used in firewalls?

(6+6+6)

6.

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

b) 'Strength of DES depends on the S-boxes in DES' – Comment on the statement.

c) Justify – 'Man in the middle attack can be prevented by 3-DES encryption'.

(6+6+6)

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

a) Network Vulnerability

b) Message Digests

c) Digital envelope

d) Pseudo-random sequences

(3x6)