B5.3-R4: NETWORK MANAGEMENT & INFORMATION SECURITY

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) Explain Encapsulating Security Payload (ESP).

b) What is perfect secrecy? Explain why it is not achievable.

c) What are confusion and diffusion? How are they achieved in cipher?

d) What are the differences between the AES encryption algorithm and the DES encryption algorithm?

e) In the CTR mode, it was mentioned that if any plaintext block that is encrypted using a given counter value is known, then the output of the encryption function can be determined easily from the associated ciphertext block. Show the calculation.

f) What is PRNG? What is the difference between statistical randomness and unpredictability?

g) Find the inverse of 3 in Z^*_{79} using extended Euclidean algorithm.

(7x4)

2.

a) What is stream cipher? Why it is not desirable to reuse a stream cipher key if once it is used? What RC4 key value will leave S-array unchanged during initialization?

b) List and explain types of attacks on encrypted messages.

c) What is the purpose of HTTPS? Explain the session state parameters defined in SSL protocol.

(6+5+7)

3.

a) Draw a possible firewall configuration that uses the screened subnet architecture of firewall.

b) What is SMIME? Explain the different CMS content types related to SMIME.

c) Which parameters and design choices determine the actual algorithm of a feistel cipher? Explain the avalanche effect.

(6+7+5)

4.

a) What are Block cipher modes of operation? Compare the various block cipher modes of operations.

b) Explain three protocols of SSH that typically run on top of TCP.

c) What is security policy? Describe the types of security policy. Differentiate threats and vulnerabilities.

(5+6+7)

5.

a) List and explain the chosen cipher text attack on RSA using appropriate example.

b) Solve 12^{416} mod 516 using the fast modular exponentiation algorithm.

c) What is Diffie-Hellman key exchange algorithm? How does man-in-the-middle attack break the security of it?

(6+7+5)

6.

a) Explain the Elgamal cryptographic system. Compare the Elgamal cryptographic system with RSA.

b) What is cryptographic hash function? What is the difference between weak and strong collision resistance?

c) For SHA-512, show the equations for the values of W16, through W19 (inclusive). State the value of the padding field and length in SHA-512 if the length of the message is

i) 1
ii) 897
iii) 1024

(6+6+6)

7.

a) What are the properties a digital signature should have? In what order should the signature function and the confidentiality function be applied to a message, and why?

b) What is Public-Key Infrastructure (PKI)? What are the requirements for the user in the public-key certificate scheme?

c) What four requirements were defined for Kerberos? What entities constitute a full-service Kerberos environment? In the context of Kerberos, what is realm?

(6+6+6)