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) 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) “Set of all integers is not a field”, give your comments.

c) Practical public-key cryptography schemes use suitable trap-door one-way function, how?

d) How are digital signatures generated in DSS?

e) Distinguish between signed data and clear-signed data in context of S/MIME.

f) Illustrate interconnection of various components in secure electronic commerce.

g) How are pseudo random numbers generated? Specify the algorithm.

(7x4)

2.

a) Define finite field of order p. Show arithmetic in GF(7) i.e. addition modulo 7, multiplication modulo 7 and additive and multiplicative inverses modulo 7.

b) Encrypt the message “meet me at the usual place at seven o clock rather than eight o clock” using the Hill Cipher with the key $\begin{pmatrix} 9 & 4 \\ 5 & 7 \end{pmatrix}$. Show your calculations and the result.

(9+9)

3.

a) Describe the DES encryption algorithm. What is avalanche effect in DES decryption?

b) How are confusion and diffusion achieved in IDEA?

(10+8)

4.

a) What are the important features of advanced encryption standard (AES)? How does AES differ from DES?

b) State the prove Euler’s theorem.

(10+8)

5.

a) How is RSA algorithm implemented? What are various approaches to attack RSA?

b) How is public key distribution of secret keys incorporated to maintain confidentiality and authentication?

(9+9)

6.

a) What are the properties which must be satisfied by a Hash function?

b) How are public-key certificates generated in X.509 authentication service? What do you understand by forward and reverse certificates in X.509?

(8+10)

7.

a) Discuss the various components of IPSec architecture. What is antireply mechanism in context of IPSec?

b) What are the design goals for a firewall? What is the tiny fragment attack in packet filtering firewall?

c) How does SSL use TCP to provide end-to-end secure service? What is the record protocol operation in SSL?

(6+6+6)