1.   Answer the following :

(a) What is substitution cipher ? (3 marks)

(b) What is rail fence cipher ?   (3 marks)

(c) What are the various components of key management process? Briefly explain all of them ?   (9 marks)

2.   Briefly explain OSI model of Internetworking and function of the various layers.

3.   Enumerate and explain various phases involved in penetration testing. Briefly explain each of them.

4.   What do we understand by active and passive attacks ? What are the various techniques used for carrying out these attacks?

5.   Answer the following :

(a) What do you understand by foot printing and reconnaissance in respect of Penetration testing / Hacking ?

(b) Explain three way handshake using a diagram.

(c) Explain Null, FIN and Xmas scan.

Section - B
(Short-Answer-Type Questions)

Note - Section 'B' contains Eight (08) short-answer-type questions of Seven (07) marks each. Learners are required to answer any Five (05) questions only.
                                        $(5 \times 7 = 35)$

1.   Explain the various components of CIA Triad. What is it used for ?

2. Answer the following :

(a) What are the four modes of cryptography operations for DES ?

(b) What type of stream cipher cryptosystem is considered "unbreakable"?

3. Discuss the implementation of Kerberos for Key distribution ?

4. Explain the process of key generation.

5. Explain the purpose and type of subnetting.

6. What are client side attacks ? Enumerate the techniques used for carrying out such attacks ?

CEGCS-04/PGDCS-04/ MIT (CS) - 104

Information System

Certificate of E-Governance and Cyber Security / P. G. Diploma/ M. Sc. Cyber Security

(CEGCS-16/17/PGDCS-17/MSCCS)

First Semester, Examination - 2019

Time : 3 Hours   Max. Marks : 80

_____

Note - This Paper is of Eighty (80) marks divided into two (02) Sections A and B. Attempt the Questions contained in these sections according to the detailed instructions given therein.

Section - A
(Long-Answer-Type Questions)

Note - Section 'A' contains Five (05) long-answer-type questions of Fifteen (15) marks each. Learners are required to answer any Three (03) questions only.

$(3 \times 15 = 45)$

7. Discuss the strategy to improve crack re-
    sistivity of a key.

8. What is 'Meet in the middle attack'?