Roll No. ……..

CEGCS–02

Cyber Security Techniques

Certificate in e-Governance and Cyber Security

(CEGCS–16)

First Semester, Examination, 2017

Time : 3 Hours **Max. Marks : 70**

Note : This paper is of **seventh (70)** marks containing **three (03)** sections A, B and C. Learners are required to attempt the questions contained in these sections according to the detailed instructions given therein.

Section–A

(Long Answer Type Questions)

Note : Section 'A' contains four (04) long answer type questions of fifteen (15) marks each. Learners are required to answer *two* (02) questions only.

1. What are the various web security approaches ? Briefly explain them.
2. What is attack ? Explain its different modes in detail.
3. What do you mean by desktop security and malware ? Discuss the different aspect of Security policy.
4. Discuss about cyber law and explain the different cyber law in detail.

Section–B

(Short Answer Type Questions)

Note : Section 'B' contains eight (08) short answer type questions of five (05) marks each. Learners are required to answer *six* (06) questions only.

1. What do you understand by authentication ? State its requirements.
2. Discuss and explain the different types of viruses and its phases.
3. Write a note on e-Commerce. Also discuss its advantages.
4. With the neat block diagram explain assurance framework.
5. What is social engineering ? Also describe the tools of social engineering.
6. Discuss about the firewall. Explain its design principle.
7. What do you mean by cyber crises plan ? What are the different national cyber crises plans ?
8. Differentiate Viruses and Worms with suitable example.

Section–C

(Objective Type Questions)

Note : Section 'C' contains ten (10) objective type questions of one (01) mark each. All the questions of this section are compulsory.

1. Firewall is used to protect against ..... .
   (a) Data driven attacks
   (b) Fire attacks
   (c) Virus attacks
   (d) Unauthorized attacks

2. Message must be encrypted at sender site and decrypted at the :
   (a) Sender site
   (b) Site
   (c) Receiver site
   (d) Conferencing

3. In computer security ..... means that computer system assets can be modified only by authorized parities.
   (a) Confidentiality
   (b) Integrity
   (c) Availability
   (d) Authenticity

4. ..... programs can be used to accomplish functions indirectly that an unauthorized user could not accomplish directly.
   (a) Zombie
   (b) Worm
   (c) Trojan Horses
   (d) Logic Bomb

5. A message authentication is service beyond :
   (a) Message confidentiality
   (b) Message integrity
   (c) Message splashing
   (d) Message sending

6. VIRUS stand for :
   (a) Very Intelligent Result Until Source

(b) Very Interchanged Resource Under Search

(c) Vital Information Resource Under Siege

(d) None of the above

7. One-way to preserve integrity of a document is through use of a :

(a) Thumb impression

(b) Fingerprint

(c) Biometric

(d) X-rays

8. Which of the following is independent malicious program that need not any host program ?

(a) Trap doors

(b) Trojan horse

(c) Virus

(d) Worm

9. An attempt to make a computer resource unavailable to its intended users is called :

(a) Denial-of-service attack

(b) Virus attack

(c) Worms attack

(d) Botnet process

10. Encryption and decryption provide secrecy, or confidentiality, but not ..... .

(a) Authentication

(b) Integrity

(c) Keys

(d) Frames