S-241 Roll No. …………………..

CEGCS–03

Cyber Attacks and Counter Measures : User Perspective

Certificate E-Governance and Cyber Security

(CEGCS-16/17)

First Semester, Examination, 2018

Time : 3 Hours **Max. Marks : 80**

Note : This paper is of **eighty (80)** 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 nineteen (19) marks each. Learners are required to answer *two* (02) questions only.

1. What is Cyber Espionage ? What Information Security controls can be employed to mitigate Cyber Espionage ?

2. What are the various categories of Computer Security controls ? Enumerate all of them and discuss Technical controls in detail.

3. Explain Password Authentication Protocol (PAP) process in detail.

4. What is Symmetric or Secret Key Cryptography ? How does it function ? Discuss *three* applications of this method of encryption.

Section–B

(Short Answer Type Questions)

Note : Section 'B' contains eight (08) short answer type questions of eight (8) marks each. Learners are required to answer *four* (04) questions only.

1. What are the three access control models ? Briefly discuss all of them.
2. What is Cloud Computing ? In what form a Cloud Provider, provides the services to an end user ? Discuss briefly.
3. What are the major differences ISO 27001 : 2005 and ISO 27001 : 2013 ?
4. What are the three master categories into which Computer Security is categorized ?
5. What are smart cards ? Explain how smart cards can contribute towards safe and secure electronic transactions.
6. What are the best practices to ensure protection from malicious attacks ?
7. What is an Intrusion Detection Systems ? Explain its functioning.
8. What do you understand by risk management process in relation to Information Security ? Enumerate the activities involved in Risk Management Process.

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. Hash functions are :

   (a) Two-way cryptographic functions

   (b) Example of PKI

   (c) Example of symmetric key cryptography

   (d) One-way cryptographic functions

2. Attack against an asset can be averted by implementing :

   (a) Antivirus

   (b) Firewall

   (c) Controls

   (d) All of the above

3. OTP is used for :

   (a) Two step authentication

   (b) Only financial transaction

   (c) Only G-mail verification

   (d) All of the above

4. Cloud computing utilizes a large pool of systems connected in public or private network to provide :

   (a) support to metrological departments

(b) support for distributed databases

(c) dynamically scalable infrastructure for application data and file storage

(d) None of the above

5. MAC filtering is the :

(a) Part of configuring IPv4 address of device

(b) Part of configuring IPv6 address of a device

(c) Most secure way of configuring a wireless router

(d) All of the above

6. MAC address of a card is :

(a) Uniquely assigned

(b) Assigned on demand

(c) User defined

(d) All of the above

7. Computer network is defined as :

(a) All the computers in a LAN

(b) All the computers and peripherals in a LAN

(c) Collection of nodes which is used for data communication

(d) All of the above

8. Biometrics provides effective method of :

(a) AADHAR linking of bank accounts.

(b) Monitoring of transactions by large population

(c) Authentication of users

(d) All of the above

9. A Ransomware is a malware which will render :

   (a) the session hijacking

   (b) the Operating System but data can be used

   (c) no harm to the system

   (d) The complete data unusable by encrypting the drives / data

10. WIPS stands for :

   (a) Windows Internal Password System

   (b) Wireless Intrusion Prevention System

   (c) Windows Interrupts Power System

   (d) Wireless Integrated Power Systems