 Roll No. ……..

CEGCS–03

Cyber Attacks and Counter Measures : User Perspective

Certificate of E-Governance and Cyber Security
(CEGCS–16/17)

First Semester, Examination, 2017

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 do you understand by COBIT framework ? What are its key principles ?
2. Discuss in detail

   (a) Cyber War

   (b) Hacktivism

   Support your explanation with the real life cases in past or recent history.

3. What do you understand by Digital Forensics ? Explain the various steps involved in digital forensic investigation.
4. Explain the relation between threat and vulnerability. List out various types of threats in relation to the Information Security.

Section–B

(Short Answer Type Questions)

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

1. What is an Information Asset ? How can compromise of Information asset impact an organisation ?
2. What are User Access Controls ? Why are they required ?
3. Write short notes on the following :
   (a) Wireless Network Security
   (b) Password Security
   (c) Phishing
   (d) Viruses
4. What are the best practices for creating a strong password ?
5. What is cryptography and what are its objectives ?
6. What is the difference between POP3 protocol and IMAP protocol ? Which of the two is better in relation to Information Security and why ?
7. Explain various public key cryptography with examples.
8. Explain functioning of SSL (Secure Socket Layer).

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. A cyber-attack is initiated from a computer against :
   (a) A website
   (b) Computer Infrastructure
   (c) Individual Computer
   (d) All of the above

2. In Public Key cryptography, Public Key is used :
   (a) By others to encrypt the data for Key owner
   (b) As hash algorithm
   (c) For transmitting the data using own private key
   (d) None of the above

3. Process of identifying a user to verify whether he/she is what he/she claims to be is known as :
   (a) Authorization
   (b) Non repudiation
   (c) Authentication
   (d) Kerberos

4. File artefacts and meta-data can be used to identify :
   (a) the origin of a particular piece of data
   (b) to rebuild a database
   (c) the reverse of a hash value
   (d) All of the above

5. When a complete application is offered to the customer as a service on demand, it is called as :
   (a) Service on demand
   (b) Infrastructure as service
   (c) Application as service
   (d) Software as service

6. Project Athena at Massachusetts Institute of Technology gave birth to :
   (a) TCP/IP
   (b) SSL
   (c) Kerberos
   (d) Public key Cryptography

7. Cryptography not only protects the information, but also :
   (a) Verifies the Integrity of data
   (b) Facilitate a hacker in stealing the data
   (c) Provides secure method of offline financial transactions
   (d) All of the above

8. A denial of service attack will :
   (a) Only infect the data on a network
   (b) Incapacitate the infrastructure, hence no service will be available.
   (c) Only corrupt the data on an IT infrastructure
   (d) None of the above

9. Best practices for creating a password are :

   (a) Using a dictionary word with numeric characters

   (b) Using special characters with dictionary words

   (c) Write it on a piece of paper

   (d) Have a mix of capital, small, numeric and special characters

10. Digital Certificates are the files used for proving the authenticity :

   (a) Of the receiver

   (b) Of the sender

   (c) Of both sender and receiver

   (d) None of the above