Roll No. ....

CEGCS–04

Information System

Certificate of 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. Answer the following :

   (a) Explain the sequence of three way handshake. 12

   (b) Name any *two* application layer protocols based on TCP and UDP. 3

2. Answer the following

   (a) Define a hashing function and what are their properties with respect to cryptography ? 7

   (b) Explain Secure Hashing algorithm and MD5 algorithm. 4

   (c) What is a birthday attack in the context of cryptography ? 4

3. Answer the following :

   (a) In the context of cryptography, what is the significance of KEYS ? What are the various methods in key generation, key distribution and key management ? 8

   (b) Discuss elaborately how 'Kerberos' provides the different authentication services with necessary diagrams. 7

4. Answer the following :

   (a) What is Secure Multipurpose Internet Mail Extensions (S/MIME) and how does it enhance security in today's e-Mail communication ? 7

   (b) What is Pretty Good Privacy (PGP) ? Explain in detail its role in e-Mail security. 8

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 is the relevance of subnetting ? In theory, how many valid hosts are available per subnet ?
2. What is meet in the middle attack ?
3. What is a reply attack ? As an administrator, what are the countermeasures would you take to prevent a reply attack in an enterprise network ?
4. What is a Digital Signature ? Explain its usage in computer security. Differentiate digital signature from digital certificate.

5. Define encryption. What is the importance of Encryption on a PC and on a network ?
6. Explain with examples, Cross site Scripting (XSS) and SQL injection web application attacks.
7. What is the role of DNS in internet ? What happens when you navigate to the website www.uou.ac.in [UTTARAKHAND OPEN UNIVERS1TYsite] from a DNS perspective ?
8. Differentiate between http and htpps.

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. What is the attack called "evil twin" ?

   (a) MAC spoofing

   (b) ARP poisoning

   (c) Rogue access point

   (d) Session hijacking

2. A PKI certificate is being issued by :

   (a) IT Ministry

   (b) Certificate authority

   (c) Resource Access Control Facility

   (d) Self-Signed

3. Which of the following is private IP address ?

   (a) 12.0.0.1

   (b) 168.172.19.39

   (c) 172.15.14.36

   (d) 192.168.24.43

4. Which protocol does Ping use ?

   (a) TCP

   (b) ARP

   (c) ICMP

   (d) Boot P

5. You are running a web server that supports secure (HTTPS) connections. What is the best way to ensure that client will not accidentally request a page over non-secure HTTP connection ?

   (a) Redirect all requests for port 80 to port 443

   (b) Completely close port 80

   (c) Use HTTP Strict-Transport-Secutify

   (d) None of the above

6. In Digital Payment Context, what does UPI stand for ?

   (a) Unified Payment Interface

   (b) Unified Payments in India

   (c) United Payment Industry

   (d) None of the above

7. What is the first hacking phase that hackers perform to gather information about a target prior to launching an attack ?

   (a) Reconnaissance

   (b) Scanning

   (c) Gaining Access

   (d) Maintaining Access

8. An enterprise network have the best IDS, firewall with strict rules and routers with no configuration errors. Which of the following techniques practiced by an attacker exploits human behaviour to make your network vulnerable to attacks ?

   (a) Buffer overflow

   (b) Social Engineering

   (c) Denial of Service

   (d) SQL injection

9. Which of the following is a symptom of a DoS attack ?

   (a) Unavailability of a particular website

   (b) Decrease in the amount of spam e-mails received

   (c) Automatic increase in network bandwidth

   (d) Automatic increase in network performance

10. Which of the listed is not a DNS resource record ?

   (a) CNAME

   (b) PTR

   (c) MX

   (d) NAT