Roll No. ....

D–1017

M. Sc. (Fourth Semester) (Main/ATKT)

EXAMINATION, May-June, 2020

COMPUTER SCIENCE

Paper Second

(Network Security and Cryptography)

Time : Three Hours] [*Maximum Marks : 100*

[*Minimum Pass Marks : 40*

Note : Attempt all Sections as directed.

Section—A 1 each

(Objective/Multiple Choice Questions)

Note : Attempt all questions.

Choose the correct answer :

1. Which is not an objective of network security ?

   (a) Identification

   (b) Authentication

   (c) Access control

   (d) Lock

2. An algorithm in encryption is called _______.

   (a) Algorithm

   (b) Procedure

   (c) Cipher

   (d) Module

3. A small program that changes the way a computer operates :

   (a) Worm

   (b) Trojan

   (c) Bomb

   (d) Virus

4. An attack it which the site is not capable of answering valid request :

   (a) Smurfing

   (b) Denial of service

   (c) E-mail bombing

   (d) Ping storm

5. A unique piece of information that is used in encryption :

   (a) Cipher

   (b) Plain Text

   (c) Key

   (d) Cipher

6. An indirect form of surveillance :

(a) Honey pot

(b) Logical

(c) Security

(d) Intrusion

7. A malicious code hidden inside a seemingly harmless piece of code :

(a) Worm

(b) Bomb

(c) Trojan Horse

(d) Virus

8. An encryption technique with 2 keys is ________.

(a) Monoalphabetic cipher

(b) Cryptography

(c) Private key cryptography

(d) Public key cryptography

9. Triple-DES has _______ keys.

(a) 1

(b) 2

(c) 5

(d) 4

10. DES stands for :

(a) Data Encryption Standard

(b) Data Encryption Statistics

(c) Data Encryption System

(d) Data Encryption Sequence

11. Firewalls can be of_______ kinds.

(a) 1

(b) 2

(c) 3

(d) 4

12. Which of the following is not a software firewall ?

(a) Windows Firewall

(b) Outpost Firewall Pro

(c) Endian Firewall

(d) Linksys Firewall

13. _____________ perform automated DoS (Denial of Service) attacks on a targeted web address.

(a) DDoS-Trojan

(b) Backdoor Trojan

(c) Trojan-Banker

(d) Trojan-Downloader

14. Public key encryption/decryption is not preferred because :

(a) it is slow

(b) it is hardware/software intensive

(c) it has a high computational load

(d) All of the mentioned

15. Which system uses a trusted third party interface ?

(a) Public-Key certificates

(b) Public announcements

(c) Publicly available directories

(d) Public-Key authority

16. Another name for Message authentication codes is :

(a) cryptographic codebreak

(b) cryptographic codesum

(c) cryptographic checksum

(d) cryptographic checkbreak

17. For a 100 bit key and a 32 bit tag, how many possible keys can be produced in the 3rd round ?

(a) 2^4

(b) 2^{32}

(c) 2^{16}

(d) 2^{64}

18. For an n-bit tag and a k-bit key, the level of effort required for brute force attack on a MAC algorithm is :

(a) 2^k

(b) 2^n

(c) min $(2^k, 2^n)$

(d) $2^k/2^n$

19. What is the value of ipad in the HMAC structure ?

(a) 00111110

(b) 00110010

(c) 10110110

(d) 01110110

20. In affine block cipher systems if f(m) = Am + t, what is f (ml+m2) ?

(a) f (m1) + f (m2) + t

(b) f (m1) + f(m2) + 2t

(c) f (ml) + t

(d) f(ml) + f (m2)

Section—B 2 each

(Very Short Answer Type Questions)

Note : Attempt all questions.

1. Define cryptography.

2. Name the *two* Signature schemes that are used in cryptography.
3 What is Hash function ?
4. What is OAEP ?
5. What are worms ?
6. List out different types of encryption algorithms.
7. List down some Hashing Algorithms.
8. What is honeypots ?
9. What is firewall basing ?
10. Define crypt analysis.

Section—C 3 each

(Short Answer Type Questions)

Note : Attempt all questions. Give Answer in less than 75 words.

1. Define cryptography in your own way along with its benefits.
2. Write few major applications of cryptography in the modem world.
3. What is decryption ? What is its need ?
4. How Hash Functions are different from Public Key Cryptography a Secret Key Cryptography ?
5. What are the prime objectives of modern cryptography ?
6. What is Digital Signature Algorithm ?
7. Give Classification of virus.
8. What is birthday problem ?

9. What is Feistel Ciphor structure ?
10. What is digital signature ?

Section—D 6 each

(Long Answer Type Questions)

Note : Attempt all questions.

1. Explain a model of network security and security mechanism.
2. What is the Advanced Encryption Standard (AES) ?
3. Explain in details the application of public key cryptosystem.
4. Explain Intruders and Intruder behavior patter and detection by audit records.
5. Discuss cyber security policy and domain of cyber security policies.