END SEMESTER EXAMINATION,MAY-2020
Semester: Sixth
Subject Code:CO-602
Subject: Cryptography and Network Security
Full Marks: 70 (Part A =25 + Part B = 45)
Duration: 3 hours
Instructions:
1. **Questions on Part A are compulsory**
2. **Answer five questions from part B**

PART – A
(Marks– 25)

1) Fill in the blanks 1x10=10

a) Every encryption and decryption process has two aspects : the algorithm and the _____ used for encryption and decryption

b) The principle of _____ ensures that only the sender and the intended recipients have access to the contents of a message

c) If the same key is used for encryption and decryption, we call the mechanism as ____ key Cryptography

d) Caesar Cipher is an example of _____

e) There are ____ rounds in DES

f) In AES, the 16-byte key is expanded into _____ bytes

g) Each communicating party needs a key pair in _____ key cryptography

h) RSA can be used both for encryption and _____.

i) In Kerberos _____ shares a unique password with every user in the system

j) A ____ stands like a sentry on the main door between the internal network and the external Internet

2) Write true or false 1x10=10

a) Non-repudiation does not allow the sender of a message to refuse the claim of not sending that message.

b) Trojan horse attempts to reveal confidential information to an attacker.

c) An algorithm mode defines what size of plain text should be encrypted in each step of the algorithm.

d) Steganography is a technique that facilitates hiding of a message that is to be kept secret inside other messages.

e) Cryptography is the technique of transforming plain text into cipher text by encoding plain text messages.

f) RSA is very popular symmetric key cryptographic algorithm

g) A Certification Authority is a trusted agency that can issue digital certificates

h) DES encrypts data in blocks of size 64 bits each

i) An application gateway works at Network Layer

j) A firewall cannot protect the internal network from virus threats

3) Choose the correct answer 1x5=5

a) Virus is a
   A) Hardware device
   B) Computer program
   C) Client
   D) Network

b) The process of writing the text as diagonals and reading it as sequence of rows is called as
   A) Rail Fence Technique
   B) Caesar Cipher
   C) Mono-alphabetic Cipher
   D) Homophonic Substitution Cipher

c) If the number of parties involved in a lock-key mechanism is 4, the number of keys needed is
   A) 2
   B) 4
   C) 6
   D) 8

d) The actual algorithm in AES encryption scheme is
   A) Blowfish
   B) IDEA
   C) RC4
   D) Rijndael

e) To verify a digital signature, we need the
   A) Sender's private key
   B) Sender's public key
   C) receiver's private key
   D) receiver's public key

PART – B

(MARKS – 45)

Answer any three questions (from Q.N. 4 to Q.N.7)

4) a) What are the key principles of security 3

b) Discuss the concept of Phishing 5

c) Discuss any one passive attack 4

5) a) Differentiate between 5
   i) Symmetric Key Cryptography and Asymmetric Key Cryptography
   ii) Worm and Virus

b) Using Playfair cipher, convert the following plain text to corresponding cipher text 7
   Keyword: PLAYFAIR EXAMPLE
   Plain Text: MY NAME IS ATUL

6) a) Explain the Diffie-Hellman Key Exchaneg/Agreement Algorothm 5

b) Discuss the VPN mechanism. 4

c) What are the limitations of firewall? 3

7) a) State the key advantages and disadvantages of various algorithm modes 5

b) Explain RSA algorithm with the help of one example 7

Answer any one question (from Q.N. 8 to Q.N.9)

8) a) Define the terms – i) plain text, ii) cipher text 2

b) What is IP address spoofing? 2

9) a) What is Certification Authority? 2

b) What is relay attack? 2

Answer any one question (from Q.N. 10 to Q.N. 12)

10) Explain the primary steps in the Kerberos Protocol 5

11) Write short notes on (any two) 5

a) History of asymmetric key cryptography

b) Steganography

c) Password

12) Explain the working of Application Gateway. 5

****