Total No. of printed pages = 6

END SEMESTER EXAMINATION – 2022

Semester : 6th

Branch : Computer

Subject Code : Co-602

CRYPTOGRAPHY AND NETWORK SECURITY

Full Marks – 70

Time – Three hours

The figures in the margin indicate full marks for the questions.

Instructions :

1. *All* questions of PART – A are compulsory.
2. Answer any *five* questions from PART – B.

PART – A

Marks – 25

1. Fill in the blanks : 1×5=5

   (a) Any action that compromises the security of information owned by an organization is called _____.

   (b) _____ is a weakness in the security system.

[Turn over

(c) When one entity pretends to be a different entity, we call it _____.

(d) _____ cannot protect against forgery by a recipient, since both sender and recipient share a common key.

(e) Encrypted e-mail messages always carry a _____, so the authenticity and non-reputability of the sender are assured.

2. Write True or False : 1×5=5

(a) Integrity allows that assets to be modified only in authorized ways.

(b) Cryptography is the art of secret reading.

(c) The encrypted text is also called plain text.

(d) Cipher text depends on the original plaintext message, the algorithm, and the key-value.

(e) DES stands for Data Encryption System.

3. Choose the most suitable option : 1×10=10

(i) In symmetric-key cryptography, the key locks and unlocks the box is

(a) same (b) shared

(c) private (d) public

(ii) The keys used in cryptography are

(a) secret keys (b) private keys

(c) public keys (d) all of them

(iii) Cryptography, a word with Greek origins, means

(a) corrupting data (b) secret writing

(c) open writing (d) closed writing

(iv) A transposition cipher reorders (permutes) symbols in a

(a) block of packets

(b) block of slots

(c) block of signals

(d) block of symbols

(v) Which is not an objective of network security ?

(a) identification (b) authentication

(c) access control (d) lock

(vi) The process of verifying the identity of an user

(a) authentication (b) identification

(c) validation (d) verification

(vii) Which of these is a part of network identification ?

(a) user id (b) password

(c) otp (d) fingerprint

(viii) The process of transforming plain text into unreadable text is called

(a) decryption

(b) encryption

(c) network security

(d) information hiding

(ix) A process of making the encrypted text readable again is called

(a) decryption

(b) encryption

(c) network security

(d) information hiding

(x) A person who enjoys learning details about computers and how to enhance their capabilities is known as

(a) cracker (b) hacker

(c) app controller (d) site controller.

4. Answer the following in a word/sentence each : 1×5=5

(a) What is CIA triad ?

(b) Which can change the normal way of a computer operation ?

(c) What do you mean by non-repudiation ?

(d) What do you mean by VPN ?

(e) Is a firewall hardware ?

PART – B

Marks – 45

5. Answer any *three* of the following : 3×3=9

(a) What is the role of S-Box in DES ?

(b) What are the criteria of cryptographic hash function ?

(c) What are the requirements of Kerberos ?

(d) What is the difference between message integrity and message authentication ?

(e) What is meant by PKI ?

6. Briefly define the monoalphabetic cipher. What is the difference between a monoalphabetic cipher and a polyalphabetic cipher ? 9

7. Differentiate between : $4\frac{1}{2}\times2=9$

(a) Active attacks and Passive attacks.

(b) Symmetric and Asymmetric Encryption.

8. Write about Block Cipher Design principles. 9

9. Compare Substitution and Transposition techniques with examples. 9

10. Write about Security Mechanisms in cryptography. 9

11. How a man-in-middle attack can be performed in Diffie Hellman algorithm ? 9

12. What is a digital signature ? What requirements should a digital signature scheme should satisfy ? 2+7=9

13. Explain the key generation Technique of RSA. Suppose Alice uses Bob's RSA public key (7, 143) and sends the Cipher Text 5 to Bob. Then perform a factorization attack to find the Plain Text. 5+4=9