Total No. of printed pages = 7

END SEMESTER REGULAR/RETEST EXAMINATION, JULY 2023

Branch : (Computer)

Semester : 6th

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 :

(i) *All* questions of PART – A are compulsory.

(ii) Answer any *five* questions from PART – B.

PART – A

Marks – 25

1. Fill in the blanks : 1×5=5

(a) _____ is the science and art of transforming messages to make them secure and immune to attacks.

(b) The acronym DES stands for _____.

[Turn over

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

(d) The _____ is the original message before transformation.

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

2. Write True or False : 1×5=5

(a) Protocols referrers to only rules.

(b) Integrity allows the assets to be modified only in authorized ways.

(c) The Worm – a malicious program needs not any host program.

(d) Hacking refers to only accessing data without permission.

(e) KDC stands for Key Distribution Code.

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

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

(i) Corrupting data (ii) Secret writing

(iii) Open writing (iv) Closed writing

(b) Encryption Strength is based on

(i) Length of key

(ii) Secrecy of key

(iii) Strength of algorithm

(iv) All of the above

(c) Symmetric key encryption is also called as

(i) Public key encryption

(ii) Private key encryption

(iii) Both (i) and (ii)

(iv) None of the above

(d) The keys used in cryptography is/are

(i) Private Key (ii) Public Key

(iii) Secret Key (iv) All of these

(e) In cryptography, the order of letters in a message is rearranged by

(i) Transpositional ciphers

(ii) Substitution ciphers

(iii) Both (i) and (ii)

(iv) Quadratic ciphers

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

(i) block of packets (ii) block of slots

(iii) block of signals (iv) block of symbols

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

(i) Identification (ii) Authentication

(iii) Access control (iv) Lock

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

(i) Authentication (ii) Identification

(iii) Validation (iv) Verification

(i) In public key encryption, if A wants to send an encrypted message

(i) A encrypts message using B's public key

(ii) A encrypts message using his private key

(iii) A encrypts message using B's private key

(iv) A encrypts message using his public key

(j) The _____ method provides a one-time session key for two parties.

(i) Diffie-Hellman (ii) RSA

(iii) DES (iv) AES

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

(a) What do you mean by Network Security ?

(b) What do you mean by Message Integrity ?

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

(d) What is the Full form of PKI ?

(e) What do you mean by Kerberos ?

PART – B
Marks – 45

5. Define any *six* of the following : 1½×6=9

(a) Cryptography

(b) Cryptology

(c) Cryptanalysis

(d) Plain text

(e) Cipher text

(f) Encryption

(g) Decryption

(h) Steganography

(i) Phishing

(j) Pharming

(k) Hash Function.

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

(a) Explain the need for security.

(b) What do you mean by CIA Triad ?

(c) What is the working principle of Cookies ?

(d) Discuss the substitution Cipher.

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

(f) What are the criterion of cryptographic hash function ?

7. (a) Write the differences between AES and DES. 4

(b) Briefly explain the various operation modes of DES. 5

8. Differentiate between any *two* : 4½×2=9

(a) Active Attacks and Passive Attacks.

(b) Symmetric and Asymmetric Encryption.

(c) Message integrity and Message authentication ?

(d) Block Cipher and Stream Cipher.

9. Compare Substitution and Transposition techniques with examples. 9

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

11. Define digital signature. What requirements should a digital signature scheme should satisfy ? 2+7=9

12. (a) Write down the features of RSA algorithm 3

(b) Write short notes on any *two* : 3×2=6

(i) Digital signature

(ii) Message digest

(iii) Secure hash algorithm.