Total No. of printed pages = 3

7

CSE 1818 PE 51 20/6/23

Roll No. of candidate □□□□□□□□□□

2023

B. Tech. 8th Semester End-Term Examination

CSE

CRYPTOGRAPHY AND NETWORK SECURITY

(New Regulation (w.e.f. 2017-18) & New syllabus (w.e.f. 2018-19))

Full Marks – 70 Time – Three hours

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

Answer Question No. 1 and any *four* from the rest

1. Choose the correct answer : (10 × 1 = 10)

(i) Use Caesar's Cipher to decipher the message : HQFUBSWHG WHAW

(a) ABANDONED LOCK (b) ENCRYPTED TEXT

(c) ABANDONED TEXT (d) ENCRYPETED LOCK

(ii) The S-Box is used to provide confusion, as it is dependent on the unknown key.

(a) True

(b) False

(iii) MAC defences ———— properties of a message.

(a) Integrity (b) Authenticity

(c) Confidentiality (d) Both (a) and (b)

(iv) A small program that changes the way a computer operates:

(a) Worm (b) Trojan

(c) Bomb (d) Virus

[Turn over

(v) The man-in-the-middle attack can endanger the security of the Diffie-Hellman method if two parties are not

(a) Authenticated
(b) Encrypted
(c) Communicated
(d) Separated

(vi) Malware stands for

(a) Multipurpose Software
(b) Malfunctioned software
(c) Malicious Software
(d) None of the above

(vii) Which of the following is used for encrypting data at the network level

(a) HTTPS
(b) SMTP
(c) IPSec
(d) S/MIME

(viii) Identify the term which denotes the protection of data from modification by unknown users

(a) Authentication
(b) Confidentiality
(c) Integrity
(d) Non-repudiation

(ix) The certificate authority sings the digital certificate with

(a) User's public key
(b) User's private key
(c) Its own public key
(d) Its own private key

(x) Public Key System is useful because

(a) It uses two keys
(b) No key distribution problem as public key can be kept on a commonly accessible database
(c) Private key can be kept secret
(d) It's symmetric key system

2. (a) Explain the OSI security architecture. (7)

(b) What are the general approaches to attacking a cipher? Compare stream cipher with block cipher. (3)

(c) Encrypt the following using play fair cipher using the keyword MONARCHY. "SWARAJ IS MY BIRTH RIGHT". (3)

(d) Encrypt the plain text "MEET TOMORROW" using Rail fence Technique, where the secret key is 3. (2)

3. (a) What is traffic Padding? (2)

(b) What is the role of a key distribution center (KDC) in symmetric encryption? (3)

(c) Explain DES with proper diagram. What is Avalanche effect? (10)

4. (a) Using the RSA algorithm, encrypt message M where p=7, q=11, e=17, M=8. (5)

(b) Explain Diffie-Hellman key Exchange with example. State its merits and demerits. (10)

5. (a) Differentiate MAC and Hash function. (3)

(b) Explain the approaches for Digital Signatures based on Public Key Encryption. (4)

(c) Describe the MD5 algorithm with necessary block diagrams. (8)

6. (a) Define S/MIME. What is the role of Ticket Granting Server in Kerberos? (5)

(b) What are the security options PGP allows when sending an email message? (5)

(c) Describe the SSL Specific protocol – Handshake action in detail. (5)

7. (a) Explain the different phases a virus go through in its lifetime? (5)

(b) Explain any two approaches for intrusion detection. Explain different types of firewalls? (10)

8. Write a short note on (Any *three*). (15)

(a) Meet in the Middle Attack.

(b) X. 509.

(c) Blowfish.

(d) Kerberos.

(e) Public Key Encryption.