Total No. of printed pages = 3

CSE 1818 PE 51

14/6/22

Roll No. of candidate

2022

B.Tech. 8th Semester End-Semester Examination

Computer Science and Engineering

CRYPTOGRAPHY AND NETWORK SECURITY

(New Regulation 2017-18)

(New Syllabus 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. Answer the following (choose the correct option) : $(10 \times 1 = 10)$

(i) The principle of ________ ensures that only the sender and the intended recipients have access to the contents of a message.

(a) Confidentiality (b) Authentication

(c) Integrity (d) Access control

(ii) The __________ attack is related to confidentiality.

(a) Interception (b) Fabrication

(c) Modification (d) Interruption

(iii) A _______ replicates itself by creating own copies, in order to bring the network to halt.

(a) Virus (b) Worm

(c) Trojan horse (d) Bomb

(iv) Caesar cipher is an example of

(a) Substitution cipher

(b) Transposition cipher

(c) Substitution as well as transposition cipher

(d) None of the above

[Turn over

(v) A clyptanalyst is a person who

(a) devises cryptographic solutions

(b) attempts to break cryptography solutions

(c) none of the above

(d) both of these

(vi) The matrix theory is used in the ———— technique.

(a) Hill cipher (b) Monoalphabetic cipher

(c) Playfair cipher (d) Vigenere cipher

(vii) DES encrypts blocks of ———— bits.

(a) 32 (b) 56

(c) 64 (d) 128

(viii) The Blowfish algorithm executes the ———— algorithm for subkey generation.

(a) Blowfish (b) IDEA

(c) Rijndal (d) RC4

(ix) If the sender encrypts the message with his/her private key, it achieves the purpose of ————.

(a) Confidentiality

(b) Confidentiality and authentication

(c) Confidentiality but not authentication

(d) Authentication

(x) ———— is a message — digest algorithm.

(a) DES (b) IDEA

(c) MD5 (d) RSA

2. (a) Encrypt the following using play fair cipher using the keyword MONARCHY.

"SWARAJ". (6)

(b) What is the OSI security architecture? (6)

(c) Find gcd (56, 86) using Euclid's algorithm. (3)

3. (a) Perform encryption mid decryption using RSA Algorithm, for the following.

$P = 7; q1 = 11; e = 17; M = 8.$ (12)

(b) What would be the transformation of a message "Happy birthday to you" using rail fence technique? (3)

4. (a) What is the difference between a block cipher and a stream cipher? (3)
   (b) Explain avalanche effect. (2)
   (c) Explain the main concept in DES. (10)

5. (a) Discuss the properties that are satisfied by Groups, Rings and Fields. Give examples of each. (9)
   (b) Differentiate between MD5 and SHA-1. (6)

6. (a) What types of attacks are addressed by message authentication? (7)
   (b) What requirements should a digital signature scheme satisfy? (6)
   (c) State Fermat Theorem. (2)

7. (a) What entities constitute a full-service Kerberos environment? What is Kerberos realm? (4)
   (b) What are the five principal services provided by PGP? (2)
   (c) Explain the format of the X.509 certificate. (9)
