End Term (Odd) Semester Examination December 2024

Roll no..............................

Name of the Course and semester: Bachelor of Technology and 3rd Semester
Name of the Paper: Introduction to Cryptography
Paper Code: TCS-392
Time: 3 hour

Maximum Marks: 100

Note:

(i) All the questions are compulsory.
(ii) Answer any two sub questions from a, b and c in each main question.
(iii) Total marks for each question is 20 (twenty).
(iv) Each sub-question carries 10 marks.

Q1. (2X10=20 Marks)

a. What is the OSI security architecture? List and briefly define categories of passive and active security attacks. (CO1)

b. State the differences between diffusion and confusion with examples. State its role in increasing the cryptographic strength of an algorithm. (CO1)

c. Explain with the help of suitable block diagram how Confidentiality, Authentication and Integrity is achieved in Message Authentication using Message Encryption (CO1,CO4)

Q2. (2X10=20 Marks)

a. Show the result of 3-bit circular left shift and circular right shift on word $(10011011)_2$. Explain, with the help of neat and clean diagram, the working of a single round of DES with key generation. (CO2)

b. Calculate the round keys(sub keys) K1, K2 from the key K= 1010101011 using S-DES algorithm. Given the values of P10= {3,5,2,7,4,10, 1,9,8,6} and P8={6,3,7,4,8,5,10, 9}. (CO2)

c. Explain the steps of Key scheduling, stream generation, Encryption and Decryption of RC4. (CO2)

Q3. (2X10=20 Marks)

a. In Symmetric Key Cryptography, How a KDC can create a session key K_{AB} between Alice and Bob (Simple protocol).
Find the Euler's totient function (φ) of φ(21) and φ(35). (CO4)

b. State the facts of Euclidean algorithm. Find the greatest common divisor of (3486, 10292) and (2740, 1760) using Euclidean algorithm. (CO4)

c. Find the multiplicative inverse of (3 mod 5) and (11 mod 26) using extended Euclidean algorithm. (CO4)

End Term (Odd) Semester Examination December 2024

Q4. (2X10=20 Marks)

a. Explain the Key generation, Encryption and decryption steps of RSA. In RSA, Given p = 19, q = 23, and e = 3, find n, φ(n), and d. (CO3)

b. What is message authentication? Explain the four possible ways in which a hash code is used to provide message authentication. (CO3)

c. Explain, with the help of diagram, the working of MD5 with compression function. (CO3)

Q5. (2X10=20 Marks)

a. What is the difference between statistical anomaly detection and rule-based intrusion detection? What is a honeypot? (CO5)

b. What is a DDoS? List four techniques used by firewalls to control access and enforce a security policy. (CO5)

c. Define three types of intellectual property. Describe a classification of computer crime based on the role that the computer plays in the criminal activity. (CO6)