Semester: 6th			
Paper code: OAE310T	**L**	**T/P**	**Credits**
Subject: Cryptography and Network Security	**4**	**0**	**4**

Marking Scheme

1. Teachers Continuous Evaluation: As per university examination norms from time to time
2. End term Theory Examination: As per university examination norms from time to time

INSTRUCTIONS TO PAPER SETTERS: Maximum Marks: As per university norms

1. There should be 9 questions in the end term examination question paper.
2. Question No. 1 should be compulsory and cover the entire syllabus. This question should have objective or short answer type questions.
3. Apart from Question No. 1, the rest of the paper shall consist of four units as per the syllabus. Every unit should have two questions. However, students may be asked to attempt only 1 question from each unit.
4. The questions are to be framed keeping in view the learning outcomes of course/paper. The standard/ level of the questions to be asked should be at the level of the prescribed textbooks.
5. The requirement of (scientific) calculators/ log-tables/ data-tables may be specified if required.

Course Objectives:

1.	To understand the fundamentals of cryptography
2.	To acquire knowledge on standard algorithms used to provide confidentiality. Integrity and authenticity
3.	To analyze concepts, issues, principles of security related properties and validate using model checking
4.	To apply knowledge of a range of computer security technologies as well as Design techniques to achieve differential privacy for linear queries

Course Outcomes:

CO1	Understand the knowledge about security services, data privacy and mechanisms.
CO2	Analyse about Symmetrical and Asymmetrical cryptography.
CO3	Analyse and Understand about the concept of Data integrity, Authentication, Digital Signatures.
CO4	Investigate Various network security applications and Design mechanisms for query release problem using online learning algorithms.

Course Outcomes (CO) to Programme Outcomes (PO) Mapping

(Scale 1: Low, 2: Medium, 3: High)

CO/PO	PO01	PO02	PO03	PO04	PO05	PO06	PO07	PO08	PO09	PO10	PO11	PO12
CO1	3	1	-	-	-	1	1	-	-	2	-	-
CO2	3	3	3	3	3	-	-	-	-	2	-	-
CO3	3	3	3	2	2	-	-	-	-	2	-	-
CO4	3	3	3	2	3	2	1	-	-	2	-	-

Course Overview:

Cryptography and Network Security is a comprehensive course covering the fundamentals of secure communication and information protection in computer networks. Students will explore encryption techniques, cryptographic algorithms, and protocols used to ensure confidentiality, integrity, and authentication. The course also delves into network security concepts such as firewalls, intrusion detection systems, and secure network design. Practical applications and case studies are included to enhance understanding of securing data transmission, securing network infrastructure, and addressing emerging security challenges.

UNIT - I **[12]**

Security Concepts: Introduction, The need for security and Data Privacy, Security approaches, Principles of security, Types of Security attacks, Security services and mechanisms, A model for Network Security, Social Aspects of Privacy, Legal Aspects of Privacy and Privacy Regulations, Database Security, Statistical Database security, Inference Control, Hippocratic databases.

Cryptography Concepts and Techniques: Introduction, plain text and cipher text, substitution techniques, transposition techniques, encryption and decryption, symmetric and asymmetric key cryptography, steganography, key range and key size, possible types of attacks.

UNIT - II **[8]**

Symmetric key Ciphers: Block Cipher principles, DES, AES, RC5, IDEA, Block cipher operation, Stream ciphers, RC4.

Asymmetric key Ciphers: Principles of public key cryptosystems, RSA algorithm, Elgamal Cryptography, Diffie-Hellman Key Exchange.

UNIT-III **[10]**

Cryptographic Hash Functions: Message Authentication, Secure Hash Algorithm (SHA-512), Message authentication codes: Authentication requirements, HMAC, CMAC, Digital signatures, Elgamal Digital Signature Scheme.

Key Management and Distribution: Symmetric Key Distribution Using Symmetric & Asymmetric Encryption, Distribution of Public Keys, Kerberos, X.509 Authentication Service, Public – Key Infrastructure

UNIT-IV **[10]**

Anonymization: Linkage and re-identification attacks, k-anonymity, I-diversity, t-closeness, implementing anonymization, Anonymizing complex data, Privacy and anonymity in mobile environments, Database as a service, Privacy in Cloud infrastructure

Differential Privacy (DP): Formalism and interpretation of DP, Fundamental DP mechanisms and properties, Interactive and non-interactive DP, DP for complex data Local Differential Privacy (LDP)

Text Books:

1. Cryptography and Network Security - Principles and Practice: William Stallings, Pearson Education, 6th Edition
2. Cryptography and Network Security: Atul Kahate, Mc Graw Hill, 3rd Edition
3. C. Dwork and A. Roth, The Algorithmic Foundations of Differential Privacy, now Publishers, 2014.

Reference Books:

1. Cryptography and Network Security: C K Shyamala, N Harini, Dr T R Padmanabhan, Wiley India, 1st Edition.
2. Cryptography and Network Security: Forouzan Mukhopadhyay, Mc Graw Hill, 3rd Edition
3. Information Security, Principles, and Practice: Mark Stamp, Wiley India.
4. Charu C. Aggarwal, Privacy-Preserving Data Mining: Models and Algorithms, 1st Edition, Springer, 2008.