Course code: Course Title	Course Structure			Pre-Requisite
SE431: Data Security and Privacy	L	T	P	NIL
	3	1	0	

Course Objective: To become familiar with the fundamental concepts of data security and privacy mechanisms along with an understanding of hiding data in text and images.

S. NO	Course Outcomes (CO)
CO1	Understand and remember the basic concepts related to data security and different types of symmetric key ciphers.
CO2	Understand and apply the concepts of encryption standards.
CO3	Understand hash functions and to learn the basic concepts of hiding data in text and images.
CO4	Understand the concepts of privacy, authentication, web and email security.

S. NO	Contents	Contact Hours
UNIT 1	**Introduction to Security and Ciphers:** Introduction: Security goals, Cryptographic Attacks, Services and Mechanism, Techniques. Traditional Symmetric Key Ciphers: Introduction, Substitution Ciphers, Transposition Ciphers, Stream and Block Ciphers. Introduction to Modern Symmetric-Key Ciphers: Modern Block Ciphers, Modern Stream Ciphers.	10
UNIT 2	**Symmetric and Asymmetric Encryption Algorithms:** Data Encryption Standard (DES): Introduction, DES Structure, DES Analysis, Multiple DES, Security of DES. Advanced Encryption Standard (AES): Introduction, Transformations, Key Expansion, AES Ciphers, Analysis of AES. Asymmetric-Key Cryptography: Introduction, RSA Cryptosystem, Rabin Cryptosystem, Elgamal Cryptosystem, Elliptic Curve Crypto systems.	10
UNIT 3	**Hash Functions, Digital Signature and Data Hiding:** Cryptographic Hash Functions: Introduction, Iterated Hash function, SHA-512, WHIRLPOOL. Digital Signature: Comparison, Process, Services, Attacks on Digital Signature, Digital Signature Standard. Data Hiding in Text: Basic Features, Applications of Data Hiding, Watermarking, Intuitive Methods, Simple Digital Methods, Data Hiding in Text, Innocuous Text, Mimic Functions. Data Hiding in Images: LSB Encoding, BPCS Steganography, Lossless Data Hiding, Spread Spectrum Steganography, Data Hiding by Quantization, Patchwork, Signature Casting in Images, Transform Domain Methods, Robust Data Hiding in JPEG Images, Robust Frequency Domain Watermarking, Detecting Malicious Tampering.	12
UNIT 4	**Privacy, Legal and Ethical Issues:** Privacy Concepts, Privacy Principles and Policies, Authentication and Privacy, Data Mining, Privacy on the Web, E-Mail Security, Impacts on Emerging Technologies. Legal and Ethical Issues in Computer Security: Protecting Programs and Data, Information and the Law, Rights of Employees and employers, Redress for Software Failures, Computer Crime, Ethical Issues in Computer Security.	10
	TOTAL	42

REFERENCES

S.No.	Name of Books/Authors/Publishers	Year of Publication / Reprint
1.	Behrouz A. Forouzan, Dedeep Mukhopadhyay, "Cryptography and Network Security", TMH, 2nd Edition.	**2013**
2.	Charles P. Pfleeger, Shari Lawrence Pfleeger, Jonathan Margulies, "Security in Computing", PHI, 5th Edition.	**2015**
3.	Mark Stamp, "Information Security: Principles and Practice", Wiley Inter Science.	**2011**
4.	Matt Bishop, "Computer Security: Art and Science", Addison Wesley, 1st Edition.	**2002**
5.	William Stallings, "Cryptography and Network Security", Pearson Education, 7th Edition.	**2017**