GANPAT UNIVERSITY									
FACULTY OF ENGINEERING AND TECHNOLOGY									
Programme	Bachelor of Technology					Branch/ Spec.	Computer Science & Engineering (CS)		
Semester	V					Version	1.0.0.0		
Effective from Academic Year			2022– 23			Effective for the batch Admitted in			June 2020
Subject code	2CSE50E24		Subject Name			CRYPTOGRAPHY			
Teaching scheme						Examination scheme (Marks)			
(Per week)	Lecture (DT)		Practical (Lab.)		Total		CE	SEE	Total
	L	TU	P	TW					
Credit	3	0	1	0	4	Theory	40	60	100
Hours	3	0	2	0	5	Practical	30	20	50

Pre-requisites:

Programming Language, Basics of Communication System

Objectives of the Course:

After learning the course the students should be able to:

- Understand the principles and practices of cryptographic techniques.
- Understand information security goals for designing secure systems.
- Apply security algorithms in solving real-life security problems in communicating systems.
- Apply security to information over the network and world wide web.

Theory syllabus

Unit	Content	
1	**Basics of Cryptography** Information Security understanding, Security goals, Security attacks, Security services, security mechanisms	**4**
2	**Cryptographic Mathematics** Modular arithmetic, linear congruence, Algebraic structure, checking of primeness, quadratic congruence	**4**
3	**Classical Ciphers** Symmetric cipher model, substitution ciphers, transposition ciphers, steganography	**5**
4	**Modern symmetric key ciphers** Modern block ciphers, modern stream ciphers, Data Encryption standard, advanced encryption standard, Electronic code book mode, CBC, cipher feedback mode, output feedback mode	**7**
5	**Public key cryptography** RSA, RSA proof, RSA attacks, Rabin cryptosystem, Key management: Diffie Hellman Key Exchange Algorithm	**6**
6	**Message Authentication and Hash functions** Authentication requirements, functions, Message authentication codes (MAC), Hash functions, security of Hash functions	**6**
7	**Hash algorithms, Digital Signatures** SHA- 512, Basics, digital signature standards	**6**

8	**Network and System Security** Understanding of Worms, Virus, Trojan Horse, Malwares, IP and Network Security ,Web security Email Security, System Security, tools	**7**

Practical content:

Practicals will be based on performing web security attacks to understand security goals, Perform Substitution Techniques for Encryption, Perform Block Cipher Encryptions, Implement Digital Signature Algorithm, Perform Asymmetric Key Encryptions, Implement MAC.

Text Books:

1.	William Stallings: "Cryptography and Network Security – Principles and Practice",Pearson Education.

Reference Books:

1.	Bruce Scheneir: "Applied Cryptography", John Wiley.
2.	Behrouz Forouzan: "Cryptography & Network Security", TMH.

Course Outcomes:

COs	Description
CO1	Understand the principles and practices of cryptographic techniques.
CO2	Understand a variety of generic security threats and vulnerabilities, and identify & analyze particular security problems for given applications.
CO3	Apply security algorithms in solving real-life security problems in communicating systems.
CO4	Apply security to information over the network and world wide web.

Mapping of CO and PO:

COs	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	3	2	2	0	0	0	0	0	3	0	0	0
CO2	3	2	2	0	0	0	0	0	3	0	2	0
CO3	3	2	2	0	0	0	0	0	3	0	3	0
CO4	3	2	3	0	0	0	0	0	3	0	0	0