GANPAT UNIVERSITY

FACULTY OF ENGINEERING & TECHNOLOGY

Programme	Bachelor of Technology	Branch/Spec.	Computer Engineering (Artificial Intelligence)
Semester	VI	Version	2.0.0.0
Effective from Academic Year	2021-22	Effective for the batch Admitted in	July 2019
Subject code	2CEIT6PE3	Subject Name	Cryptography and Network Security

Teaching scheme						Examination scheme (Marks)			
(Per week)	Lecture (DT)		Practical (Lab.)		Total		CE	SEE	Total
	L	TU	P	TW					
Credit	3	0	1	-	4	Theory	40	60	100
Hours	3	0	2	-	5	Practical	30	20	50

Pre-requisites:

Concept of Computer Networks, Discrete Mathematics, and programming

Objectives of the course:

- To introduce fundamental concepts of symmetric and asymmetric cipher models
- To acquire knowledge on standard algorithms used to provide confidentiality, integrity and authenticity
- To introduce network security and web security protocols

Theory syllabus:

Unit	Content	Hrs
1.	**Introduction to Cryptography and Network Security:** Need of Security, Principles of Security, Types of Attacks, Techniques for security goals implementation, OSI Security Architecture, Possible Cryptanalysis Attacks, Basic Terminology.	05
2.	**Traditional Symmetric Key Cryptography:** Symmetric key and Asymmetric key cryptography, Substitution Techniques, Transposition Techniques, Key range and Key Size, Symmetric key and Key Distribution Problem, Diffie-Hellman Key Exchange/Key Agreement Algorithm, Man in the Middle Attack.	06
3.	**Modern Symmetric Key Cryptography Techniques:** Stream Cipher, Block Cipher, Product Cipher, Claude Shannon's concept of Confusion & Diffusion, Algorithm types and modes, Two classes of product ciphers (Feistel Ciphers and Non-Feistel Ciphers), Data Encryption Standards (DES), Advanced Encryption Standards (AES).	10
4.	**Asymmetric key Cryptography:** Difference between Symmetric key and Asymmetric key cryptosystems, RSA Algorithm, Security of RSA.	03
5.	**Symmetric and Asymmetric Key both together:** Digital Envelope, Digital Signature, Digital Signature Schemes, Message Digest (MD), SHA, Message Authentication.	04
6.	**Network Security:** Kerberos, Key Management, PKI, Security at the Network Layer – IPSec, Security at the Transport Layer – SSL, Security at the Application Layer- PGP and S/MIME, Firewall, Network Vulnerabilities.	09
7.	**Mathematics for Cryptography:**	08

Practical content:

- Experiments/ Practicals /Simulations would be carried out based on syllabus

Text Books:

1.	'Cryptography and Network Security' by Behrouz A Forouzan, Debdeep Mukhopadhyay (Latest Edition).

Reference Books:

1.	'Cryptography and Network Security' by Atul Kahate (Latest Edition).
2.	'Cryptography and Network Security' by William stallings (Latest Edition).

3.	'Cryptography and Network Security' by Prakash C. Gupta (Latest Edition).
4.	'Network Security and Cryptography' by Bernard Menezes (Latest Edition).
ICT/MOOCs Reference:	
1.	https://nptel.ac.in/courses/106/105/106105031/
2.	https://www.coursera.org/learn/crypto
Course Outcomes:	
COs	Description
CO1	Understand the concepts related to the Cryptography and Information security
CO2	Importance of Network Security and Challenges in Network Security
CO3	Deduce the mechanisms to be employed while trying to satisfy any of the security services
CO4	Apply the concept of security services and mechanisms from the application developers and network administrator's perspective
CO5	Finding the importance of Security tools
CO6	Implementing Security services in an organization
CO7	Apply security principles to system design
CO8	Conduct research in Network Security

Mapping of CO and PO:

COs	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	3	3	1	2	3	2	3	3	0	0	0	3
CO2	3	3	1	2	2	2	2	2	0	0	0	3
CO3	3	3	1	2	3	2	2	2	0	0	0	2
CO4	3	3	3	2	2	2	2	3	0	0	0	3
CO5	3	3	2	2	3	1	1	3	0	0	0	3
CO6	3	3	2	2	2	1	3	2	0	0	0	2
CO7	3	3	3	2	2	3	3	3	0	0	0	3
CO8	3	3	2	2	3	3	3	3	0	0	0	3