Dr. Ambedkar Institute of Technology, Bengaluru-56

Department of Computer Science & EngineeringSchemeand Syllabus-NEP – 2023 -2024

CourseTitle	**CRYPTOGRAPHY AND NETWORK SECURITY**						
CourseCode	**21CST7033**						
Category	**Professional Elective Courses - II (PEC-II)**						
Scheme andCredits	No.of Hours/Week					Total teachinghours	Credits
	L	T	P	SS	Total		
	03	00	**00**	00	**03**	**42**	**03**
CIE Marks: 50	**SEEMarks: 50**		**TotalMax. marks=100**		**DurationofSEE:03Hours**		

COURSEOBJECTIVES

1. The students could able to recognize the different terminologies of cryptography
2. Able to understand the working of cryptographic algorithms.
3. Study the concept of Public key cryptosystem.
4. Acquire the knowledge of IP Security concepts.
5. Apply the knowledge in web Security applications

UNIT I **09 Hours**

Introduction: OSI Security Architecture, Security Attacks, Security Services, Security Mechanism, Model for Network Security.

Classical Encryption Technique: Symmetric Cipher Model, Substitution Techniques, Transposition Techniques

UNIT II **08 Hours**

Block Ciphers, Data Encryption Standard and Advanced Encryption Standard: Simplified DES, Block Cipher Principles, DES, and Differential and Linear cryptanalysis, Modes of operation.

AES. Evaluation Criteria for AES, AES Cipher-Encryption and Decryption, Data Structure, Encryption Round, Triple DES, Blowfish

UNIT III **09 Hours**

Public Key Cryptography and Key Management: Principles of Public Key Cryptosystem, RSA algorithm, Key management, Diffie Hellman Key Exchange, Elliptic curve cryptography..

UNIT IV **08 Hours**

IP Security: IP Security Overview; IP Security Architecture; Authentication Header; Encapsulating Security Payload; Combining Security Associations; Key Management.

UNIT V **08 Hours**

Web Security: Web security Considerations; Secure Socket layer (SSL) and Transport layer Security (TLS); Secure Electronic Transaction (SET).

System security

Intruders, Viruses and related threats

TEACHINGLEARNINGPROCESS:ChalkandTalk,powerpointpresentation,animations,videos

COURSEOUTCOMES: Oncompletionofthecourse,studentshouldbeableto,

CO1:Analyze different terminology of cryptography.
CO2: Write algorithm for cryptographic algorithms.
CO3: Describe Public key cryptosystem.
CO4: Understand IP security architecture and key management techniques.
CO5: Summarize Web Security and System security concepts

TEXT BOOK:

1. William Stallings, "Cryptography and Network Security – Principles and Practices", 6th Edition, Pearson Education 2014 ISBN13: 9780133354690

REFERENCE BOOKS/WEBLINKS:

ONLINERESOURCES

1. https://www.youtube.com/playlist?list=PLBlnK6fEyqRgJU3EsOYDTW7m6SUmW6kII
2. **https://archive.nptel.ac.in/courses/106/105/106105162/**

MAPPING of Cos with POs

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	3	1	3	3	-	3	-					
CO2	3	3	3	2	1	3	2					
CO3	2	3	2	2	1	3	-					
CO4	3	3	2	3	-	3	-					
CO5	3	3	3	3	3	-	-					
Strengthofcorrelation: Low-1, Medium-2, High-3												

Faculty In-charge
1.Dr.MADHU B