COURSE CONTENT

CRYPTOGRAPHY AND NETWORK SECURITY								
VI Semester: CSE								
Course Code	**Category**	**Hours / Week**			**Credits**	**Maximum Marks**		
		L	**T**	**P**	**C**	**CIA**	**SEE**	**Total**
2460516	**Foundation**	3	1	0	4	40	60	100
Contact Classes: 45	**Tutorial Classes: Nil**	**Practical Classes: Nil**				**Total Classes: 45**		
Prerequisites: Computer Networks								

Course Overview:

This course focuses on techniques and protocols used to protect information and communication systems from unauthorized access, attacks, and misuse. The course combines mathematical foundations of cryptography with practical network security mechanisms used in real-world systems.

Course Objectives:

1. Understand security threats, attacks, and countermeasures
2. Apply cryptographic algorithms to protect data
3. Analyze and design secure communication protocols
4. Understand network security architectures and standards
5. Evaluate real-world security systems and vulnerabilities

Course Outcomes: After Completion of the Course, Students should be able to

1. Understand basic cryptographic techniques and models of internetwork security.
2. Apply symmetric and asymmetric cryptographic techniques to secure data and understand their algorithmic principles
3. Analyze the role of cryptographic hash functions and authentication mechanisms in ensuring data integrity and security in key distribution systems
4. Implement email and IP layer security protocols and analyze their effectiveness in protecting communication.
5. Apply system security concepts to configure web security protocols, identify threats, and design security infrastructure like firewalls and IDS.

UNIT – I: Security Attacks (Interruption, Interception, Modification and Fabrication), Security Services (Confidentiality, Authentication, Integrity, Non-repudiation, access Control and Availability) and Mechanisms, A model for Internet work security, 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.

UNIT- II: Symmetric key Ciphers: Block Cipher principles, DES, AES, Blowfish, RC4, Block cipher operation, Stream ciphers, Asymmetric key Ciphers: Principles of public key cryptosystems, RSA algorithm, Elgamal Cryptography, Diffie – Hellman Key Exchange, Knapsack Algorithm.

UNIT - III: Cryptographic Hash Functions: Message Authentication, Secure Hash Algorithm (SHA512), 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: E mail privacy: Pretty Good Privacy (PGP) and S/MIME. IP Security: Over view, IP Security Architecture, Authentication Header, Encapsulating Security Payload, Combining Security Association and Key Management.

UNIT - V: Web Security: Requirements, Secure Socket Layer (SSL) and Transport Layer Security (TLS), Secure Electronic Transaction (SET). Intruders, Viruses and related threats, Firewall Design principles, Trusted Systems, Intrusion Detection Systems.

TEXT BOOKS:

1. Cryptography and Network Security by Atul Kahathe MC Graw Hill, 2nd edition.
2. Cryptography and Network Security by Will I am Stallings 6th Edition, Pearson Education.

REFERENCE BOOKS:

1. Cryptography and Network Security by Behrouz A.Forouzan.
2. Applied Cryptography‖ by Bruce Schneier

ELECTRONIC RESOURCES:

1. https://www.nptelprep.in/courses/106105031
2. https://www.getyoureducation.net/course/cryptography-and-network-security-
3. https://wizape.com/English/Cryptography-and-Network-Security/
4. **https://www.tutorialsduniya.com/notes/cryptography-network-security-notes/**
5. **https://www.cse.iitm.ac.in/~shwetaag/notes/Lec1.pdf**

MATERIALS ONLINE:

1. Course template
2. Tutorial question bank
3. Tech talk and Concept Video topics
4. Open-ended experiments
5. Definitions and terminology
6. Assignments
7. Model question paper – I
8. Model question paper – II
9. Lecture notes
10. E-Learning Readiness Videos (ELRV)