18ECPE809	NETWORK SECURITY	L	T	P	C
		3	0	0	3

Course Objectives:

1.	To understand network security, architecture and algorithms.
2.	To study various encryption and decryption standards for network security.
3.	To familiarize with necessary approaches and techniques to build protection mechanisms in order to secure computer networks.

Unit I	INTRODUCTION	9	+	0

Security Goals - Services, Mechanisms and attacks - OSI security architecture - Model of network security - Security trends - Legal, Ethical and Professional Aspects of Security - Need for Security at Multiple levels – Mathematics of Cryptography.

Unit II	SYMMETRIC CRYPTOGRAPHY	9	+	0

Encryption and Decryption – Substitution techniques – Transposition techniques - Block ciphers - Data Encryption Standard - Differential and Linear Cryptanalysis - Block Cipher modes - Advanced Encryption Standard - Triple DES - RC5 - RC4 stream ciphers.

Unit III	PUBLIC KEY ENCRYPTION	9	+	0

Introduction to Number Theory - Public Key cryptography – Rivest_Shamir_Adleman Algorithm (RSA) - Key management - Diffie-Hellman key exchange – Elliptic curve cryptography.

Unit IV	MESSAGE AUTHENTICATION AND INTEGRITY	9	+	0

Authentication requirements and functions – MAC – Hash functions – Security of hash functions and MAC – Secure Hash Algorithms - Digital signature and authentication protocols – Digital Signature Standard.

Unit V	NETWORK AND SYSTEM SECURITY	9	+	0

Authentication applications - E-mail Security - IP security - Web security – Intruders - Malicious Software - Firewalls.

Total (L+T)= 45 Periods

Course Outcomes:

At the end of the course, the student should be able to:

CO1	:	Understand the fundamentals of networks security, security architecture, threats and vulnerabilities
CO2	:	Apply the different cryptographic operations of symmetric cryptographic algorithms and public key cryptography.
CO3	:	Apply the various Authentication schemes to simulate different applications.
CO4	:	Understand various Security practices and System security standards.

Text Books:

1.	William Stallings, “Cryptography and Network Security”, 6th Edition, Principles and Practice”, PHI, 2013.
2.	AtulKahate, “Cryptography and Network security”, 3rd Edition, Tata McGraw-Hill, 2017.

Reference Books:

1.	C K Shyamala, N Harini and Dr. T R Padmanabhan, “Cryptography and Network Security”, Wiley India Pvt.Ltd, 2011.
2.	Behrouz A Forouson, “Cryptography & Network Security”, 3rd Edition, Tata McGraw hill, 2015.
3.	Charlie Kaufman, Radia Perlman, and Mike Speciner, “Network Security: PRIVATE Communication in a PUBLIC World”, 2nd Edition Prentice Hall, 2002.
4.	Roberta Bragg, Mark Phodes-Ousley, Keith Strassberg,“Network Security: The Complete Reference”, Tata Mcgraw-Hill, 2003.

E-References:

1.	https://nptel.ac.in/courses/106105162/
2.	https://nptel.ac.in/courses/106106178/10
3.	https://nptel.ac.in/courses/106105031/39