Devi Ahilya University, Indore, India Institute of Engineering & Technology				ME – I Year (Spl Digital Communication) Semester- B			
Subject Code & Name	**Instructions Hours per Week**			**Credits**			
DCP4E2 **Network Security**	**L**	**T**	**P**	**L**	**T**	**P**	**Total**
	3	**1**	**2**	**3**	**1**	**1**	**5**
Duration of Theory Paper: **3 Hours**							

Course Objectives:

Prerequisite(s):

COURSE CONTENT

UNIT –I:

Introduction: Attacks, Services and Mechanisms, Security attacks, Security services, A Model for Internetwork security.Classical Techniques: Conventional Encryption model, Steganography, Classical Encryption Techniques.

UNIT –II:

Modern Techniques: Simplified DES, Block Cipher Principles, Data Encryption standard, Strength of DES, Differential and Linear Cryptanalysis, Block Cipher Design Principles and Modes of operations.

Algorithms: Triple DES, International Data Encryption algorithm, Blowfish, RC5, CAST-128, RC2, Characteristics of Advanced Symmetric block cifers.

Conventional Encryption: Placement of Encryption function, Traffic confidentiality, Key distribution, Random Number Generation.

Public Key Cryptography: Principles, RSA Algorithm, Key Management, Diffie-Hellman Key exchange, Elliptic Curve Cryptography.

UNIT –III:

Number Theory: Prime and Relatively prime numbers, Modular arithmetic, Fermat's and Euler's theorems, Testing for primality, Euclid's Algorithm, the Chinese remainder theorem, Discrete alogarithms.

Message authentication and Hash Functions: Authentication requirements and functions, Message Authentication, Hash functions, Security of Hash functions and MACs.

UNIT –IV:

Hash and Mac Algorithms: MD File, Message digest Algorithm, Secure Hash Algorithm, RIPEMD-160, HMAC.

Digital signatures and Authentication Protocols: Digital signatures, Authentication ,Protocols, Digital signature standards.

Authentication Applications: Kerberos, X.509 directory Authentication service.Electronic Mail Security: Pretty Good Privacy, S/MIME.

UNIT –V:

IP Security: Overview, Architecture, Authentication, Encapsulating Security Payload, Combining security Associations, Key Management.

Web Security: Web Security requirements, Secure sockets layer and Transport layer security, Secure Electronic Transaction.

Intruders, Viruses and Worms: Intruders, Viruses and Related threats.

Fire Walls: Fire wall Design Principles, Trusted systems.

Books Recommended:

[1]. Cryptography and Network Security: Principles and Practice - William Stallings, Pearson

Education.
[2]. 1.Network Security - Private Communication in a Public World by Charlie Kaufman, Radia Perlman and Mike Speciner, Pearson/PHI.
[3]. Principles of Information Security, Whitman, Thomson.
[4]. Network Security: The complete reference, Robert Bragg, Mark Rhodes, TMH
[5]. Introduction to Cryptography, Buchmann, Springer.