Devi Ahilya University, Indore, India Institute of Engineering & Technology				**IV Year B.E. (Electronics and Telecommunication)**			
Subject Code & Name	**Instructions Hours per Week**			**Credits**			
ETR8E2	**L**	**T**	**P**	**L**	**T**	**P**	**Total**
NETWORK SECURITY	**3**	**1**	**2**	**3**	**1**	**1**	**5**
Duration of Theory Paper: 3 Hours							

Learning Objectives:

- To understand the fundamentals of Cryptography.
- To acquire knowledge on standard algorithms used to provide confidentiality, integrity and authenticity.
- To understand the various key distribution and management schemes.
- To understand how to deploy encryption techniques to secure data in transit across data networks
- To design security applications in the field of Information technology

Prerequisite: Computer Network

COURSE CONTENTS

UNIT I -
An Overview of Computer Security-Security Services-Security Mechanisms-Security Attacks-Access Control Matrix, Policy-Security policies, Confidentiality policies, Integrity policies and Hybrid policies.

UNIT II-
Classical Cryptography-Substitution Ciphers-permutation Ciphers-Block Ciphers-DESModes of Operation- AES-Linear Cryptanalysis, Differential Cryptanalysis- Hash Function - SHA 512-Message Authentication Codes-HMAC - Authentication Protocols.

UNIT III-
Introduction to Public key Cryptography- Number theory- The RSA Cryptosystem and Factoring Integer- Attacks on RSA-The ELGamal Cryptosystem- Digital Signature Algorithm-Finite Fields-Elliptic Curves Cryptography- Key management – Session and Interchange keys, Key exchange and generation-PKI.

UNIT IV -
Design Principles, Representing Identity, Access Control Mechanisms, Information Flow and Confinement Problem Secure Software Development: Secured Coding - OWASP/SANS Top

Vulnerabilities - Buffer Overflows - Incomplete mediation - XSS - Anti Cross Site Scripting Libraries - Canonical Data Format - Command Injection - Redirection - Inference – Application Controls.

UNIT V -
Secret Sharing Schemes-Kerberos- Pretty Good Privacy (PGP)-Secure Socket Layer (SSL)-Intruders – HIDS- NIDS - Firewalls - Viruses

Learning Outcomes:

At the end of this course, students will be able to:

- Implement basic security algorithms required by any computing system.
- Analyze the vulnerabilities in any computing system and hence be able to design a security solution.
- Analyze the possible security attacks in complex real time systems and their effective countermeasures.
- Identify the security issues in the network and resolve it.
- Evaluate security mechanisms using rigorous approaches, including theoretical derivation, modeling, and simulations.
- Formulate research problems in the computer security field.

BOOKS RECOMMENDED:

[1]. William Stallings, "Cryptography and Network Security: Principles and Practices", Third Edition, Pearson Education, 2006.
[2]. Matt Bishop ,"Computer Security art and science ", Second Edition, Pearson Education, 2002.
[3]. Wade Trappe and Lawrence C. Washington, "Introduction to Cryptography with Coding Theory" Second Edition, Pearson Education, 2007.
[4]. Jonathan Katz, and Yehuda Lindell, Introduction to Modern Cryptography, CRC Press, 2007.
[5]. Douglas R. Stinson, "Cryptography Theory and Practice", Third Edition, Chapman & Hall/CRC, 2006.

List of Practical Assignments:

1) Design and implementation of a simple client/server model and running application using sockets and TCP/IP.
2) To make students aware of the insecurity of default passwords, printed passwords and password transmitted in plain text.
3) To teach student how to use SSH for secure file transfer or for accessing local computer using port forwarding technique.
4) Comparison between Telnet and SSH for Secure Connection