Devi Ahilya University, Indore, India Institute of Engineering & Technology				IV Year B.E. (Electronics & Instrumentation Engg.)			
Subject Code & Name	**Instructions Hours per Week**			**Credits**			
EIR8E1	**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 network system & OSI model, concept of security- approaches and principles , attacks, cryptography technique, encryption & decryption, substitution & transport technique, symmetric & asymmetric cryptography,

Unit II

An overview of symmetric key cryptography algorithm types and modes, data encryption standard (DES), Advanced encryption standard(AES)-criteria, transformation , International data encryption algorithm (IDEA).

Unit III

Asymmetric key cryptography, RSA cryptosystem-, Digital signature -process ,service &scheme, Knapsack algorithm, ElGamal algorithm, public key exchange, attacks on RSA, attacks on digital signature.

Unit IV

Digital certificates ,private key management, public key cryptography standards, XML ,PKI & security,, internet security protocols, SSL,TSL,SHTTP, secure electronic Transaction, email, security, security in 3G, GSM,IEEE802.11,

Unit V

User authentication mechanism, Biometric authentication, Kerberos, Password, Authentication tokens, IP security overview & policy, Firewall characteristic, VPN, Malicious software,Intruder, Email security.

Books Recommended:

[1]. Williams Stallings; Cryptography & Network Security; 3rd Edition, Pearson Education.Pearson Education, 2006.
[2]. Atul kahate ; Cryptography & Network Security, Third edition ,McGraw hill education
[3]. Behrouz A. Forouzan, Cryptography & Network Security, Tata McGraw hill, 2007.
[4]. Matt Bishop ,"Computer Security art and science ", Second Edition, Pearson Education, 2002.

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.