Devi Ahilya University, Indore, India Institute of Engineering & Technology				IV Year B.E. (Computer Engineering) (Full Time)			
Subject Code & Name	**Instructions Hours per Week**			**Credits**			
CER8C2	**L**	**T**	**P**	**L**	**T**	**P**	**Total**
Network & Information Security	**3**	**1**	**2**	**3**	**1**	**1**	**5**
Duration of Theory Paper:3 Hours							

Learning Objectives:

1. To impart the knowledge and in-depth reference to current information and network security standards and procedures.
2. This course provides you with an overview of data and computer security and concentrates in technical and continuity management issues.
3. Allow the student to gain expertise in some specific areas of information security such as the design and providing security to individual networks.

Prerequisites :

Basic knowledge of programming and Computer Networks

COURSE CONTENTS

Unit I

Introduction: The need for security, security approaches, principles of security services, mechanisms and attacks, a model for network security. substitution & transposition techniques, steganography, key range & key size.

Unit II

Symmetric Cipher: An general idea of symmetric key cryptography, classical symmetric ciphers, Algorithm types & modes, possible types of attacks, Symmetric & asymmetric cipher model, Data Encryption Standard (DES), Advanced Encryption Standard (AES).

Unit III

Asymmetric Cipher: RSA algorithm, asymmetric & symmetric key cryptography together, digital envelopes, digital signatures & digital certificates & Public key infrastructure (PKI).

Unit IV

Information Security Protocols: Secure Socket Layer, Secure Hyper Text Transfer Protocol (SHTTP), Time Stamping Protocol (TSP), 3- D Secure Protocol, Email Security, and Kerberos.

Unit V

Network Security: Deffie-Hellman key exchange, Firewalls, IP Security, Virtual Private Networks, Intrusion detection system, IP spoofing, DNS spoofing. Introduction to blockchain technology and cryptocurrency.

Learning Outcomes:

After completing this course the student must demonstrate the knowledge and ability to:

1. Acquire a practical overview of the issues involved in the field of information security.
2. Demonstrate a basic understanding of the practice of IS, especially in the evaluation of information security risks across diverse settings including the Internet and WWW-based commerce systems, high bandwidth digital communications and funds transfer services.
3. The learning outcome is students shall be able to understand what are the common threats faced today, what are the foundational theory behind information security, what are the basic principles and techniques when designing a secure system, how to think adversarial, how today's attacks and defenses work in practice, how to assess threats for their significance, and how to gauge the protections and limitations provided by today's technology.
4. Familiarity with the basic protocols of Information Security, and how they can be used to assist in network security design and implementation.

Books Recommended:

1. Douglas R. Stinson; Cryptography Theory and Practice; 2nd Edition, Chapman & Hall/CRC
2. Williams Stallings; Cryptography & Network Security; 3rd Edition, Pearson Education
3. Bernard Menezes; Network Security and Cryptography; Cengage Learning India Pvt Ltd.
4. Neal Krawetz; Introduction to Network Security; 2nd Edition, Thomson Learning Inc.

List of Practical Assignments:

During learning, of course, students need to do assignments:

1. Implementation of various symmetric key algorithms.
2. Implementation of various asymmetric key algorithms.
3. Implementation of Algorithm types and modes (Electronic Code Book (ECB), Cipher Block Chaining (CBC), Cipher Feedback (CFB), Output Feedback (OFB)).
4. Study of Pretty Good Privacy open source security tool for email security.
5. Implementation of digital certificates.
6. Study of IP Tables.
7. Implementation of various open source security tools (Wireshark, Nmap, tables, pretty good privacy, Snort, LC5, OpenVPN, TrueCrypt, THC Hydra).