Devi Ahilya University, Indore, India Institute of Engineering &Technology				**IV Year B.E. (Electronics & Instrumentation Engg)**			
Subject Code & Name	**Instructions Hours per**			**Credits**			
8EIRE1	**L**	**T**	**P**	**L**	**T**	**P**	**Total**
NETWORK SECURITY	**3**	**1**	**2**	**3**	**1**	**1**	**5**
Duration of Theory Paper:3Hours							

Course Objectives:

1. To impart the knowledge and in-depth reference to current information and network security standards and procedures.
2. This course provides an overview of data and computer security and concentrates in technical and continuity management issues.
3. Student motivated 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

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.

Course Outcome:

Students earned credits will develop ability to

CO. No.	Course Outcome	Program Outcomes
CO1	Students will be able to understand the fundamental need for security in computer networks, identify various security approaches and principles governing security services and their application contexts.	PO1, PO2, PO12
CO2.	Define symmetric key cryptography and its basic principles. Analyze possible types of attacks on symmetric encryption. Compare and contrast symmetric and asymmetric cipher models.	PO1, PO2, PO3
CO3	Understand the RSA algorithm and its significance in public key cryptography. Compare asymmetric and symmetric key cryptography approaches. Explain the concept of digital envelopes and digital signatures, digital certificates i.e public key infrastucture (PKI) in secure communication and message authentication.	PO2, PO4, PO5, PO12
CO4	Explain the architecture and functioning of Secure Socket Layer (SSL), Secure Hypertext Transfer Protocol (SHTTP), Time Stamping Protocol (TSP), email security and Kerberos protocol.	PO2, PO3, PO8
CO5	Describe the role and functioning of firewalls in network security. IP Security (IPsec), Virtual Private Networks (VPNs) and its use in securing IP communications.	PO3, PO6, PO8, PO12

CO-PO Relationship

CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	3	3		2								1

CO2	3	2	1									
CO3		2		2	3							1
CO4		2	3					3				
CO5			2			3		3				1

CO-PO Relationship

1. * CO (rows) mention nil/very small/insignificant contribution to the PO(column)
2. 1→ relevant and small significance 2 → medium or moderate and 3 →strong

Books Recommended:

[1] Williams Stallings; Cryptography & Network Security; 3rd Edition, Pearson Education.
[2] Bernard Menezes;Network Security and Cryptography;Cengage Learning India Pvt Ltd.
[3] Atul kahate ; Cryptography & Network Security, Third edition ,McGraw hill education,
[4] Behrouz A. Forouzan, Cryptography & Network Security, Tata McGraw hill, 2007.

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.