| **Devi Ahilya University, Indore, India Institute of Engineering & Technology** | | | | **IV Year B.E. (Electronics and Telecommunication Engg.)** | | | |
|---|---|---|---|---|---|---|---|
| **Subject Code & Name** | **Instructions Hours per Week** | | | **Credits** | | | |
| **8ETRE1 NETWORK SECURITY** | **L** | **T** | **P** | **L** | **T** | **P** | **Total** |
| | **3** | **1** | **2** | **3** | **1** | **1** | **5** |
| **Duration of Theory Paper: 3 Hours** | | | | | | | |

## Course Learning Objective:

- To impart the knowledge and network security standards and procedures.
- To understand the fundamentals of cryptography.
- To understand the various key distribution.
- To learn the application in field of information technology.

## Prerequisite:

Basic fundamentals of Network System.

## COURSE CONTENT

**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. | CO | PO |
|---|---|---|
| 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 |

## 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 Experiments: