SWARNANDHRA
COLLEGE OF ENGINEERING AND TECHNOLOGY
(AUTONOMOUS)

SEETHARAMPURAM, NARSAPUR-534280, WG- DT, AP

DEPARTMENT OF MASTER OF COMPUTER APPLICATIONS

## TEACHING PLAN

| Course Code | Course Title | Year/ Sem | Branch | Contact Hrs/ Week | Academic Year |
|---|---|---|---|---|---|
| 20MC3T03 | PRINCIPLES OF CRYPTOGRAPHY AND NETWORK SECURITY | II/III | MCA | 6 | 2024-25 |

### COURSE OBJECTIVES:

1. To learn various cryptographic algorithms including secret key cryptography, hashes and message digests, public key algorithms.
2. To Familiar in design issues and working principles of various authentication protocols and various secure communication standards including Kerberos, IPsec, and S/MIME.

**COURSE OUTCOMES (CO):** Students are able to

| Course Outcomes | | Knowledge Level (K)# |
|---|---|---|
| CO1 | Explain Basic Principles, different security threats, countermeasures, foundation course of cryptography mathematics and Symmetric Encryption. | K2 |
| CO2 | Classify the basic principles of Asymmetric key algorithms and operations of asymmetric key cryptography. | K4 |
| CO3 | Design Cryptographic Hash Functions as SHA-3 and Digital Signatures as Elgamal | K6 |
| CO4 | Explain the concept of Revise Key Management and Distribution and User Authentication | K3 |
| CO5 | Determine the knowledge of Network and Internet Security Protocols such as S/MIME | K5 |

| Week No | Outcomes | Blooms Level | TOPIC/ACTIVITY | | Text Books | Contact Hours | Delivery Method |
|---|---|---|---|---|---|---|---|
| 1<br>2<br>3 | Basic Principles, different security threats, countermeasures, foundation course of cryptography mathematics and Symmetric Encryption. | K2 | | **Unit I** | | | Chalk & Board & Demonstration of Cryptography Algorithms |
| | | | 1.1 | Security Goals, | T1 | 1 | |
| | | | 1.2 | Cryptographic Attacks, | T1 | 1 | |
| | | | 1.3 | Security Services | T1 | 1 | |
| | | | 1.4 | Security Mechanisms | T1 | 1 | |
| | | | 1.5 | Mathematics of Cryptography | T1 | 2 | |
| | | | 1.6 | Traditional Symmetric key ciphers | T1 | 1 | |
| | | | 1.7 | Mathematics of Symmetric Key Cryptography | T1 | 1 | |
| | | | 1.8 | Introduction to Modern Symmetric Key Ciphers | T1 | 1 | |
| | | | 1.9 | Transposition Ciphers | T1 | 1 | |
| | | | 1.10 | Data Encryption Standard | T1 | 1 | |
| | | | 1.11 | DES Structure | T1 | 1 | |
| | | | 1.12 | DES Analysis | T1 | 1 | |
| | | | 1.13 | Security of DES | T1 | 1 | |
| | | | 1.14 | Advanced Encryption Standard | T1 | 1 | |
| | | | 1.15 | Transformations | T1 | 1 | |
| | | | 1.16 | Key Expansion | T1 | 1 | |
| | | | 1.17 | AES Ciphers | T1 | 1 | |
| 4<br>5<br>6 | Classify the basic principles of Asymmetric key algorithms and operations of asymmetric key cryptography. | K4 | | **Unit II** | | | Chalk & Board & Demonstration of Cryptographic Algorithms |
| | | | 2.1 | Mathematics of Asymmetric Key Cryptography | T1 | 1 | |
| | | | 2.2 | Primes | T1 | 1 | |
| | | | 2.3 | primality Testing | T1 | 1 | |
| | | | 2.4 | Factorization | T1 | 1 | |
| | | | 2.5 | Asymmetric Key Cryptography | T1 | 1 | |
| | | | 2.6 | RSA Cryptosystem | T1 | 1 | |
| | | | 2.7 | Rabin Cryptosystem | T1 | 1 | |
| | | | 2.8 | ElGamal Cryptosystem | T1 | 1 | |
| | | | 2.9 | Elliptic Curve Cryptosystem | T1 | 1 | |
| | | | | **Unit III** | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 7 | | K6 | 3.1 | Applications of Cryptographic Hash Functions | T1 | 1 | Chalk & Board PPT Presentation & Demonstration of Cryptographic Algorithms |
| 8<br>9 | Design Cryptographic Hash Functions as SHA-3 and Digital Signatures as Elgamal. | | 3.2 | Two Simple Hash Functions Requirements Hash Functions | T1 | 1 | |
| | | | 3.3 | Security Hash Functions | T1 | 1 | |
| | | | | **MID Exam-I** | | | |
| | | | 3.4 | Cipher Block Chaining | T1 | 1 | |
| | | | 3.4 | Secure Hash Algorithm (SHA), SHA-3. | T1 | 1 | |
| | | | 3.5 | **Digital Signatures:** Elgamal Digital Signature Scheme | T1 | 1 | |
| | | | 3.6 | Schnorr Digital Signature | T1 | 1 | |
| | | | 3.7 | NIST Digital Signature Algorithm | T1 | 1 | |
| | | | | **UNIT-IV** | | | |
| 10<br>11<br>12 | Concept of Revise Key Management and Distribution and User Authentication | K3 | 4.1 | Symmetric Key Distribution Using Symmetric Encryption | T2 | 1 | Chalk & Board & Demonstration of Cryptographic Algorithms |
| | | | 4.2 | Symmetric Key Distribution Using Asymmetric Encryption | T2 | 1 | |
| | | | 4.3 | Distribution of Public Keys | T2 | 1 | |
| | | | 4.4 | X.509 Certificates | T2 | 1 | |
| | | | 4.5 | X.509 Architecture | T2 | 1 | |
| | | | 4.6 | **User Authentication:** User Authentication | T2 | 1 | |
| | | | 4.7 | Remote User-Authentication Principle | T2 | 1 | |
| | | | 4.8 | Remote User-Authentication Using Symmetric Encryption | T2 | 1 | |
| | | | 4.9 | Kerberos | T2 | 1 | |
| | | | 4.10 | Remote User-Authentication | T2 | 1 | |
| | | | 4.11 | Using Asymmetric Encryption | T2 | 1 | |
| | | | | **Unit V** | | | |
| 13<br>14 | Determine the knowledge of Network and Internet Security Protocols such as S/MIME | K5 | 5.1 | Network Security Overview | T2 | 1 | Chalk & Board PPT Presentation |
| | | | 5.2 | Network Access Control | T2 | 1 | |
| | | | 5.3 | Cloud Security | T2 | 1 | |
| | | | 5.4 | Electronic Mail Security | T2 | 1 | |
| | | | 5.5 | Internet Mail Architecture | T2 | 1 | |
| | | | 5.6 | Email Formats | T2 | 1 | |
| | | | 5.7 | Email Threats | T2 | 1 | |
| | | | 5.8 | Comprehensive Email Security | T2 | 1 | |
| | | | 5.9 | S/MIME. | T2 | 1 | |

|  |  |  |  |  |  |  |  |
|---|---|---|---|---|---|---|---|
|  |  |  | 5.10 | **IP Security** | T2 | 1 |  |
|  |  |  | 5.11 | IP Security Overview | T2 | 1 |  |
|  |  |  | 5.12 | IP Security Policy | T2 | 1 |  |
|  |  |  | 5.13 | Encapsulating Security Payload | T2 | 1 |  |
|  |  |  | 5.14 | Combining Security Associations | T2 | 1 |  |
|  |  |  | 5.15 | Internet Key Exchange | T2 | 1 |  |
|  |  |  | 5.16 | Cryptographic Suites | T2 | 1 |  |
| **Course Beyond Syllabus** |  |  |  | Projects for Teaching Cryptographic and Network Security |  | **1** |  |
|  |  |  |  | **MID Exam-II** |  |  |  |
|  | **TOTAL CLASSES** |  |  |  |  | **62** |  |

**Recommended Text Books for Reading:**

T1: Behrouz A Forouzan, Deb deep Mukhopadhyay, Cryptography and Network Security, McGraw Hill, 3rd Edition, 2015

T2: William Stallings, Cryptography and Network Security, Global Edition, 7e Pearson, 2017

**Reference Text Books:**

R1: Bernard Meneges, Network Security and Cryptography, Cengage Learning, First Edition, 2018

**Faculty** **Head of the Department** **Principal**