Subject Code	Subject Name	Credits
22CS602	CRYPTOGRAPHY	04

Course Objectives

1. To get to know the latest security trends and the security architecture
2. To learn about encryption and the various algorithms associated with it
3. To get to know Number theory and how it helps in cryptography
4. To understand IP Security and various concepts associated with it.

Learning Outcomes

To learn various security related cryptography concepts

Unit 1 – Introduction (12 hrs.)

Introduction, Security trends, OSI Security Architecture, Security attacks, Security services, A Model for Internetwork security. Classical Techniques: Conventional Encryption model, Steganography, Classical Encryption Techniques. Modern Techniques: Simplified DES, Block Cipher Principles, Data Encryption standard, Strength of DES, Differential and Linear Cryptanalysis, Block Cipher Design Principles and Modes of operations. Algorithms: Triple DES, International Data Encryption algorithm, Blowfish, RC5, RC4, Characteristics of Advanced Symmetric block ciphers.

Unit 2 - Conventional Encryption (12 hrs.)

Placement of Encryption function, Traffic confidentiality, Key distribution, Random Number Generation. Public Key Cryptography: Principles, RSA Algorithm, Key Management, Diffie-Hellman Key exchange, Elliptic Curve Cryptography.

Unit 3 - Number theory (12 hrs.)

Number theory: Prime and Relatively prime numbers, Modular arithmetic, Fermat's and Euler's - Theorems, Testing for primality, Euclid's Algorithm, the Chinese remainder theorem, discrete logarithms. Message authentication and Hash functions: Authentication requirements and functions, Message Authentication, Hash functions, Security of Hash functions and MACs.

Unit 4 - Hash and Mac Algorithms (12 hrs.)

MD File, Message digests Algorithm, Secure Hash Algorithm, RIPEMD- 160, and HMAC. Digital signatures and Authentication protocols: Digital signatures, Authentication Protocols, Digital signature standards. Authentication Applications: Kerberos, X.5012 directory Authentication service, Electronic Mail Security: Pretty Good Privacy, S/MIME.

Unit 5 - IP Security (12 hrs.)

IP Security: Over view, Architecture, Authentication, Encapsulating Security Payload, Combining security Associations, Key Management, Web Security: Web Security requirements, secure sockets layer and Transport layer security, Secure Electronic Transaction. Intruders, Viruses and Worms: Intruders, Viruses and Related threats, Fire Walls: Fire wall Design Principles, Trusted systems.

References:

1. William Stallings, Cryptography & Network Security: Principles and Practice, Pearson.
2. Stallings William, Network Security Essentials (Applications and Standards), Pearson Education.
3. Menezes Alfred J., Van Oorschot Paul C., Vanstone Scott A., *Handbook of Applied Cryptography*, CRC Press
4. Aumasson Jean-Philippe, *Serious Cryptography: A Practical Introduction to Modern Encryption*, No Starch Press.
5. Paar Christof, Pelzl Jan, *Understanding Cryptography: A Textbook for Students and Practitioners*, Springer