6KSO4 CRYPTOGRAPHY [L-3,T-0,C-3]

Course Prerequisite: Discrete Structure & Graph Theory, Data Communication and Networking, Introduction to Cyber security

Course Objectives: Throughout the course, students will be expected to demonstrate their understanding of Cryptography by being able to do each of the following:

1. Understand Security Concepts.
2. Know about various encryption techniques.
3. Understand the concept of public key cryptography.
4. Study about message authentication and hash functions.
5. Impart knowledge on Network security, Internet Security Protocols.

Course Outcomes (Expected Outcome): On completion of the course, the students will be able to

1. Classify the symmetric encryption techniques
2. Illustrate various public key cryptographic techniques
3. Evaluate the authentication and hash algorithms.
4. Discuss authentication applications
5. Summarize the intrusion detection and its solutions to overcome the attacks.
6. Understand basic concepts of system level security

Unit I: Hours: 6

Attacks on Computers and Computer Security: Introduction, Need for Security, Security Approaches, Principles of Security, Types of Attacks. Cryptography: Concepts and Techniques Introduction, Plain Text and Cipher Text, Substitution and Transposition Techniques, Encryption and Decryption, Symmetric and Asymmetric Key Cryptography, Stenography, Key Range and Key Size, Possible Types of Attacks

Unit II: Hours: 6

Symmetric Key Algorithms and AES: Introduction, Algorithm Types and Modes, An Overview of Symmetric Key Cryptography, Data Encryption Standard(DES), International Data Encryption Algorithm(IDEA), RC4, RC5, Blowfish, Advanced Encryption Standard(AES).

Unit III: Hours:6

Asymmetric Key Algorithms, Digital Signatures and RSA: Introduction, History and Overview of Asymmetric Key Cryptography, The RSA Algorithm, Symmetric and Asymmetric Cryptography, Digital Signatures, Knapsack and other Algorithms.

Unit IV: Hours:6

Digital Certificates and Public Key Infrastructure (PKI): Introduction, Digital Certificates, Private Key Management, The PKIX Model, Public Key Cryptography Standards (PKCS), XML,PKI and Security, Creating Digital Certificate.

Unit V: Hours:6

Internet Security Protocols: Introduction, Concepts, Secure Socket Layer(SSL), Transport Layer Security(TLS), Secure Hypertext Transport Protocol(SHTTP), Time Stamping Protocol(TSP), Secure Electronic Transaction(SET), SSL Versus SET, 3-D Secure Protocol, Electronic Money, Email Security, Wireless Application Protocol(WAP)Security, Security in GSM, Security in 3G.

Unit VI: Hours:6

User Authentication and Kerberos: Introduction, Authentication Basics, Passwords, Authentication Tokens, Certificate-based-Authentication, Biometric Authentication, Kerberos, Key Distribution Center(KDC), Security Handshake Pitfalls, Single Sign On (SSO) Approaches.

Text Book:

[1] Atul Kahate, “ Cryptography and Network Security”, McGraw Hill, Second Edition.

Reference Books:

[1] William Stallings, “Cryptography and Network Security, Principles and Practice”, PHI Fourth Edition.
[2] Behrouz A. Forouzan and Debdeep Mukhopadhyay, “Cryptography and Network Security”, McGraw Hill, Second Edition.
[3] Matt Bishop, “Computer Security Arts and Science”, Pearson Education.
[4] Douglas R Stinson, “Cryptography, Theory and Practice” CRC Press.
[5] Keith M Martin, “Everyday Cryptography, Fundamental Principles and Applications”, Oxford University Press, Second Edition.