**Techno India NJR Institute of Technology**



**Course File**

**Information Security System (6CS4- 03)**

 Akhilesh Arya

(Assistant Professor)

**Department of CSE**

****

**Course Overview:**

To study concepts related to Security Attacks, Encipher Techniques, Block Cipher & Its methods, Public Key Cryptosystems & Its Types, Cryptographic Hash Functions & their applications, Key Management & their distribution etc. which is vital to excel in the field of information security domain.

**Course Outcomes:**

|  |  |  |
| --- | --- | --- |
| **CO. NO.** | **Cognitive Level** | **Course Outcome**  |
| 1 | Synthesis | Develop a basic understanding of cryptography, how it has evolved and some key encryption techniques used today, Develop an understanding of security policies. |
| 2 | Synthesis | To master and implement different encryption algorithms |
| 3 | Synthesis | To master fundamentals of secret and public cryptography |
| 4 | Synthesis | Students will be able to understand message authentication protocols and hash functions. |
| 5 | Synthesis | To master protocols for security services |

**Prerequisites:**

1. Elementry knowledge of Data Communications
2. Basic Concepts of Information & Networking
3. Good Problem Solving Skills

**Course Outcome Mapping with Program Outcome:**

|  |  |
| --- | --- |
| **Course Outcome**  | **Program Outcomes (PO’s)** |
| **CO. NO.** | **Domain Specific (PSO)** | **Domain Independent (PO)** |
|  | **PO1** | **PO2** | **PO3** | **PO4** | **PO5** | **PO6** | **PO7** | **PO8** | **PO9** | **PO10** | **PO11** | **PO12** |
| CO1 | 2 | 2 | 2 | 2 | 1 | 0 | 1 | 1 | 0 | 0 | 0 | 0 |
| CO2 | 3 | 2 | 3 | 2 | 1 | 0 | 1 | 1 | 0 | 0 | 0 | 0 |
| CO3 | 3 | 3 | 3 | 2 | 2 | 0 | 1 | 1 | 0 | 0 | 0 | 0 |
| CO4 | 2 | 2 | 2 | 2 | 1 | 0 | 1 | 1 | 0 | 0 | 0 | 0 |
| CO5 | 2 | 2 | 2 | 2 | 2 | 1 | 1 | 1 | 0 | 0 | 0 | 0 |
| 1: Slight (Low) , 2: Moderate (Medium), 3: Substantial (High)  |

**Course Coverage Module Wise:**

|  |  |  |
| --- | --- | --- |
| **Lecture No.** | **Unit** | **Topic** |
|  | 1 | **Introduction to Objective, Scope & outcome of Information Security System** |
|  | 2 | Introduction to security attacks |
|  | 2 | Services and mechanism |
|  | 2 | Classical encryption techniques- substitution ciphers |
|  | 2 | Transposition ciphers |
|  | 2 | Cryptanalysis |
|  | 2 | Stream and block ciphers |
|  | 3 | Modern block ciphers, Block Cipher structure |
|  | 3 | Data Encryption standard (DES) with example, strength of DES |
|  | 3 | Design principles of block cipher |
|  | 3 | AES with structure, its transformation functions, key expansion, example and implementation. |
|  | 3 | Multiple encryption and triple DES |
|  | 3 | Electronic Code Book, Cipher Block Chaining Mode, Cipher Feedback mode, Output Feedback mode, Counter mode |
|  | 4 | Public Key Cryptosystems with Applications |
|  | 4 | Requirements and Cryptanalysis |
|  | 4 | RSA cryptosystem |
|  | 4 | Rabin cryptosystem |
|  | 4 | Elgamal cryptosystem |
|  | 4 | Elliptic curve cryptosystem |
|  | 5 | Cryptographic Hash Functions their applications |
|  | 5 | Hash functions based on Cipher Block Chaining |
|  | 5 | Message Authentication Codes |
|  | 5 | Digital Signature |
|  | 5 | Various digital signature schemes (Elgamal and Schnorr), NIST digital Signature algorithm |
|  | 6 | Key management and distribution, symmetric key distribution using symmetric and asymmetric encryptions |
|  | 6 | Distribution of public keys, X.509 certificates, Public key infrastructure |
|  | 6 | Remote user authentication with symmetric and asymmetric encryption |
|  | 6 | Kerberos Web Security threats and approaches, SSL architecture and protocol, Transport layer security, HTTPS and SSH |

**TEXT/REFERENCE BOOKS**

1. William Stallings: Network Security Essentials Applications Standards, Pearson Education India
2. Atul Kahate: Cryptography & Network Security, The McGraw Hill Companies
3. Mark Rhodes - Ousley: Information Security – The Complete Reference, The McGraw Hill Companies
4. Michael E. Whitman, Herbert J. Mattord: Principles of Information Security, MindTap from Cengage

|  |  |
| --- | --- |
| **CO.NO.** | **Problem description** |
| **1** | 1. Understanding the introductory concepts of Security Attacks, Services & Mechanisms
2. Understanding the Concepts Encryption Techniques, Various Cipher Techniques
 |
| **2** | 1. Understanding the concepts Modern Block Ciphers
2. Conceptualizing the variation in various Block based Encryption Techniques & Encryption Modes
 |
| **3** | 1. Conceptualizing the need of Public Key Cryptosystems
2. Understanding the various Public Key Cryptosystems with their applications
 |
| **4** | 1. Understanding the need of Hash Functions as key entity in Security
2. Understanding the various Cryptograhic Hash Functions & their Applications
 |
| **5** | 1. Understanding the concepts of Key Management, Certificates, Web Security Threats & its approaches
 |

**Assessment Methodology:**

1. Assignments one from each unit.
2. Final paper at the end of the semester subjective.

**Teaching and Learning resources unit-wise:**

**Unit-1**

A. Introduction to Information Security System

Video Tutorials: <https://www.youtube.com/watch?v=FBxO5FJxllY&ab_channel=ComputerandNetworkSecurity>

Theory concepts: <https://www.geeksforgeeks.org/what-is-information-security/>

Sample Quiz: <https://mcqslearn.com/cs/computer-networks/mcq/network-security-multiple-choice-questions-answers.php>

**Unit-2**

1. Introduction to Security Attacks

Video Tutorials: <https://www.youtube.com/watch?v=yIm0Ol9Dg4Y&ab_channel=NesoAcademy>

Theory concepts: <https://www.sciencedirect.com/topics/computer-science/security-attack>

Sample Quiz: <https://mcqslearn.com/cs/computer-networks/mcq/cryptography-multiple-choice-questions-answers.php>

**Unit-3**

1. Modern Block Ciphers

Video Tutorials: <https://www.youtube.com/watch?v=scBXZbVV_zg&ab_channel=ReemaThareja>

Theory concepts: <https://www.tutorialspoint.com/cryptography/block_cipher.htm>

Sample Quiz: <https://www.includehelp.com/cryptography/mcq-modes-of-operations-in-block-cipher.aspx>

1. Encryption Techniques & Cipher Modes

Video Tutorials: <https://www.youtube.com/watch?v=QjSWXj4gKBw&ab_channel=EasyEngineeringClasses>

Theory concepts: <https://www.geeksforgeeks.org/data-encryption-standard-des-set-1/>

Sample Quiz: <https://mcqslearn.com/cs/db/data-encryption-standard-multiple-choice-questions.php>

**Unit-4**

1. Cryptanalysis Requirements

Video Tutorials: <https://www.youtube.com/watch?v=pPqfU2_KByE&ab_channel=ChiragBhalodia>

Theory concepts: <https://searchsecurity.techtarget.com/definition/cryptanalysis>

Sample Quiz: <https://mcqslearn.com/cs/computer-networks/mcq/cryptography-multiple-choice-questions-answers.php>

1. Public Key Cryptosystems

Video Tutorials: <https://www.youtube.com/watch?v=rLiEA06Bcic&ab_channel=AndroidAuthority>

Theory concepts: <https://www.globalsign.com/en-in/ssl-information-center/what-is-public-key-cryptography#:~:text=Public%2Dkey%20cryptography%2C%20or%20asymmetric,key%20performs%20a%20unique%20function>.

Sample Quiz: <https://www.sanfoundry.com/digital-communications-questions-answers-public-key-crypto-systems-1/>

**Unit-5**

1. Cryptographic Hash Functions

Video Tutorials: <https://www.youtube.com/watch?v=KqqOXndnvic&ab_channel=MITOpenCourseWare>

Theory concepts: <https://www.synopsys.com/blogs/software-security/cryptographic-hash-functions/#:~:text=A%20cryptographic%20hash%20function%20is,used%20to%20verify%20the%20user>.

Sample Quiz: <https://www.sanfoundry.com/cryptography-questions-answers-hash-functions/>

B. Message Authentication Code

Video Tutorials: <https://www.youtube.com/watch?v=Iy9mXkUyklQ&ab_channel=ChiragBhalodia>

Theory Concepts: <https://www.investopedia.com/terms/m/message-authentication-code.asp#:~:text=A%20message%20authentication%20code%20(MAC,request%20sent%20by%20the%20user>.

Sample Quiz: <https://mcqslearn.com/cs/computer-networks/message-authentication-multiple-><choice-questions.php>

**Unit-6**

1. Key Management & Distribution

Video Tutorials: <https://www.youtube.com/watch?v=Roti8qzbk3U&ab_channel=ChiragBhalodia>

Theory concepts: <https://www.geeksforgeeks.org/easy-key-management-in-cryptography/>

Sample Quiz: <https://quizplus.com/quiz/80010-quiz-14-key-management-and-distribution>

Previous Year Question Papers:







