**19ECS707: CRYPTOGRAPHY AND NETWORK SECURITY**

**L T P C**

**3 0 0 3**

*The course is concentrated on the study of network security using various cryptographic algorithms. As a part of cryptanalysis we will study several attacks on these algorithms as well as their remedies. We will also study the usage of digital signatures and its variations for authentication. The concepts of securing computer network protocols, based on the application of cryptographic techniques.*

**Course Objectives:**

* This course purpose is to introduce the arithmetic topics, both ancient and very modern, which have been at the center of interest in applications, especially in cryptography.
* For this reason, we take an algorithmic approach, emphasizing estimates of the efficiency of the techniques that arise from the theory.
* Enable the student to learn basic knowledge in cryptographic various algorithms.
* Demonstrate the handling of variety of threats during transmission of information over network and also how to overcome it.
* Understand various block cipher and stream cipher models.
* Train the student to convert algorithm logic into any programming language code.

.

**Unit I 8 L**

Number theory: Divisibility and the Euclidean algorithm. Modular Arithmetic, Finite field arithmetic, prime numbers, testing of primality,Fermat’s and Euler’s Theorems, Chinese Remainder Theorem Discrete Logarithms.

**Learning Outcomes**

After completion of this unit the student will be able to

* **Learn basic Algebra and Discrete Mathematics.**
* Know to find the greatest common divisor of two numbers (which is an incredibly important problem by itself), but its extended version also gives an efficient way to solve Diophantine equations and compute modular inverses.
* Understand the Chinese remainder theorem which gives a unique solution to simultaneous linear congruence’s with co-prime moduli.

**Unit II 8 L**

Modern Cryptosystems: Block ciphers Principles –Data Encryption Standard (DES), Triple DES, Strength of DES,block cipher operation, AES structure and strength, Rc4.

**Learning Outcomes**

After completion of this unit the student will be able to

* Learn the environment that led to the development of the Data Encryption Standard (DES).
* Identifying, describing, and explaining the purpose of each stage of the DES algorithm.
* Explaining why the input and output permutation in DES do not improve the security.
* Enumerating the weaknesses of the DES algorithm.
* Ability to understand the current legal issues towards information security in Rc4.

**Unit III 10L**

Principles of Public-Key Cryptosystems, RSA Cryptosystem, bit security of RSA, Elgamal Cryptographic System, The Diffie–Hellman Key Agreement Protocol, Pseudorandom Number Generation Based on an Asymmetric Cipher.

**Learning Outcomes**

After completion of this unit the student will be able to

* Defining key expressions and terminology including multiplicative inverse, relatively prime, and the totient function.
* Describing the steps required to perform the RSA (Rivest, Shamir, and Adleman) encryption algorithm.
* Performing the RSA algorithm on a given number by hand.
* Using the RSA algorithm to encrypt and decrypt data.
* Describing a key exchange algorithm or protocol (e.g. Diffie­ Hellman).

**Unit IV 8 L**

Data integrity: Applications of Cryptographic Hash Functions, Sha512, SHA 3, Message Authentication Requirements, Message Authentication Functions, HMAC, CMAC. Digital signatures, RSA and Elgamal Digital signature.

**Learning Outcomes:**

After completion of this unit the student will be able to

* How the Hash Function is aimed to generate outputs from input.
* As the Hash Function, HMAC is also aimed to be one way, easy to generate output from input but complex the other way round.
* It aims at being less effected by collisions than the hash functions.
* HMAC reuses the algorithms like MD5 and SHA-1 and checks to replace the embedded hash functions with more secure hash functions, in case found.
* Examine how to handle the keys in more simple manner.

**Unit V 8L**

Network and internet security: Web Security, Secure Socket Layer and Transport Layer Security, IEEE 802.11 Wireless LAN, Wireless Application Protocol, IEEE 802.11i Wireless LAN Security, IP Security

**Learning Outcomes**

After completion of this unit, the student will be able to

* To provide data integrity and communication privacy.
* Know how SSL/TLS protocols allow the connection between two mediums (client-server) to be encrypted.
* Learn the IEEE 802.11i wireless networking standard with respect to data confidentiality, integrity, mutual authentication, and availability.

**Text Book(s):**

1. Cryptography and network Security, William Stalling, 5th edition.

2. Neal Koblitz, A Course in Number Theory and Cryptography, 2/e, Springer,2002. 2. William Stallings, 3. Mainiri & Valdmis Itri Frinovich, Introduction to quantum computers, 1st Edition, World Scientific, Singapore,1998. 5. Jonathan Katz, Yehuda Lindell, Introduction to Modern Cryptography, Principles and Protocols,2nd Edition, CRC Press,2014.

**Course Outcomes:**

After completion of the course, students would be able to:

* Understand the most common type of cryptographic algorithm.
* Analyze network security threats and determine efforts to counter them.
* Write code for relevant cryptographic algorithms.
* Sign and verify messages using Digital Signatures.
* Understand the Public-Key Infrastructure.
* Understand security protocols for protecting data on network security.
* Apply security principles to system design.
* Be able to provide data integrity and communication privacy.