LECTURE PLAN OF B. TECH (CSE) and DD (CSE)

Course Type	Course Code	Name of Course	L	T	P	Credit
	CSH17101	Cryptography	3	0	0	9

Course Objective

The objective of the course is to present an introduction to Cryptography, with an emphasis on how to protect the information security from unauthorized users.

Learning Outcomes

Upon successful completion of this course, students will:

- have a broad understanding of Cryptography course.
- have a high-level understanding of cryptographic based different applications and their functionality.
- be able to model secure applications based on the knowledge of cryptography.

Unit No.	Topics to be Covered	Lecture Hours	Learning Outcome
1	Introduction to Cryptography and Its Applications, Mathematical Tools for Cryptography	3	• Comprehensive introduction about the course content will be delivered. • We will also discuss the possible application areas of Cryptography. • We will also introduce the necessary mathematical concepts to understand the course content.
2	Classical Cryptosystems, Cryptanalysis of Classical Ciphers	3	• To understand working procedure of cryptography through the example of Classical Cryptosystems and their cryptanalysis process.
3	Private-Key Cryptosystems: Feistel Cipher, DES, Differential Cryptanalysis	4	• To understand the internal structure Feistel networks. This will help students to understand the design process of DES, which is very helpful for understanding the evolution of modern cryptography. • The students also learn the security analysis on DES algorithm.
4	AES, IDEA, CAST, RC4, RC5, Blowfish; Mode of operations;	6	• This unit will help student to understand some popular private key cryptosystems. • In addition, they will learn the most important modes of operation for block ciphers in practice.
5	Public Key Cryptosystems: Knapsack cryptosystems, RSA; Attacks on RSA, Diffie-Hellman Key Exchange, Discrete Logarithm problem, ElGamal cryptosystems, Elliptic Curve cryptosystems;	12	• To understand the need of Public Key Cryptosystems. Practical aspects of different Public key cryptosystems. Protocols that can be realized with Public key cryptosystems.
6	Cryptographic Hash functions: MD5, SHA-1, SHA-512, Birthday Attack	4	• To understand important properties of hash functions and to get an overview of different families of hash functions. The students also learn the security threat on this particular topics.
7	Message Authentication Codes, HMAC	2	• To understand the principles of Message Authentication Codes
8	Digital Signatures: RSA Signatures, ElGamal Signature, DSA, Blind Signatures	3	• To understand principle of digital signatures and their different variants.
9	Key Establishment: Kerberos, X.509 Certificates.	2	• The students will learn several mechanisms for establishing keys between remote parties.

Text Books:

1. W. Trappe and L. Washington, “Introduction to Cryptography with Coding Theory”, Pearson Prentice Hall.

Reference Books:

1. B. Forouzan and D. Mukhopadhyay, “Cryptography and Network Security”, McGraw Hill Education.
2. D. Stinson, “Cryptography: Theory and Practice”, Chapman and Hall/CRC.