Cryptography

B.E., VII Semester, Electronics & Communication Engineering

[As per Choice Based Credit System (CBCS) scheme]

Subject Code	15EC744	IA Marks	20
Number of Lecture Hours/Week	03	Exam Marks	80
Total Number of Lecture Hours	40 (08 Hours / Module)	Exam Hours	03

CREDITS – 03

Course Objectives: This Course will enable students to:

- Enable students to understand the basics of symmetric key and public key cryptography.
- Equip students with some basic mathematical concepts and pseudorandom number generators required for cryptography.
- Enable students to authenticate and protect the encrypted data.
- Enrich knowledge about Email, IP and Web security.

Modules

Module-1	**RBT Level**
Basic Concepts of Number Theory and Finite Fields: Divisibility and the divisibility algorithm, Euclidean algorithm, Modular arithmetic, Groups, Rings and Fields, Finite fields of the form GF(p), Polynomial arithmetic, Finite fields of the form $GF(2^n)$(Text 1: Chapter 3)	L1, L2
Module-2	
Classical Encryption Techniques: Symmetric cipher model, Substitution techniques, Transposition techniques, Steganography (Text 1: Chapter 1) **SYMMETRIC CIPHERS:** Traditional Block Cipher structure, Data Encryption Standard (DES) (Text 1: Chapter 2: Section1, 2)	L1, L2
Module-3	
SYMMETRIC CIPHERS: The AES Cipher. (Text 1: Chapter 4: Section 2, 3, 4) **Pseudo-Random-Sequence Generators and Stream Ciphers:** Linear Congruential Generators, Linear Feedback Shift Registers, Design and analysis of stream ciphers, Stream ciphers using LFSRs (Text 2: Chapter 16: Section 1, 2, 3, 4)	L1, L2, L3
Module-4	
More number theory: Prime Numbers, Fermat's and Euler's theorem, Primality testing, Chinese Remainder theorem, discrete logarithm. (Text 1: Chapter 7) **Principles of Public-Key Cryptosystems**: The RSA algorithm, Diffie - Hellman Key Exchange, Elliptic Curve Arithmetic, Elliptic Curve Cryptography (Text 1: Chapter 8, Chapter 9: Section 1, 3, 4)	L1, L2, L3
Module-5	

One-Way Hash Functions: Background, Snefru, N-Hash, MD4, MD5, Secure Hash Algorithm [SHA],One way hash functions using symmetric block algorithms, Using public key algorithms, Choosing a one-way hash functions, Message Authentication Codes. Digital Signature Algorithm, Discrete Logarithm Signature Scheme (Text 2: Chapter 18: Section 18.1 to 18.5, 18.7, 18.11 to 18.14 and Chapter 20: Section 20.1, 20.4)	L1, L2, L3

Course Outcomes: After studying this course, students will be able to:

- Use basic cryptographic algorithms to encrypt the data.
- Generate some pseudorandom numbers required for cryptographic applications.
- Provide authentication and protection for encrypted data.

Question paper pattern:

- The question paper will have 10 full questions carrying equal marks.
- Each full question consists of 16 marks with a maximum of Three sub questions.
- There will be 2 full questions from each module covering all the topics of the module
- The students will have to answer 5 full questions, selecting one full question from each module.

Text Books:

1. William Stallings , "Cryptography and Network Security Principles and Practice", Pearson Education Inc., 6th Edition, 2014, ISBN: 978-93-325-1877-3
2. Bruce Schneier, "Applied Cryptography Protocols, Algorithms, and Source code in C", Wiley Publications, 2nd Edition, ISBN: 9971-51-348-X

Reference Books:

1. Cryptography and Network Security, Behrouz A. Forouzan, TMH, 2007.
2. Cryptography and Network Security, Atul Kahate, TMH, 2003.

D.V.

H. O. D.
Dept. Of Electronics & Communication
Alva' : Institute of Engg. & Technology
Mijar, MOODBIDRI - 574 225