VASAVI COLLEGE OF ENGINERING (Autonomous)
DEPARTMENT OF MATHEMATICS

BASICS OF CRYPTOLOGY

Open Elective(for B.E., IV semester)- (CBCS)(2018-19)

Name of the Faculty: Mr. R. Hari Kishore

Instruction:	1 hr Per week	**Semester End Exam Marks :**	60	**Subject Reference Code :**	OE420MA
Credits:	1	**Sessional Marks :**	40	**Duration of Semester End Exam :**	hours

COURSE OUTCOMES

The objective of this course is to familiarize the prospective engineers from various disciplines with the basic concepts and techniques of cryptography and cryptanalysis.

At the end of the course he students shall be able to:

1. Account for the Basics of cryptology, principles and techniques that are used to establish security properties and encipher/decipher using Monoalphabetic substitution ciphers.
2. Aanalyze and use methods viz., Monoalphabetic and Polyalphabetic substitution ciphers for cryptography, exponentiation cipher and public key cryptography in enciphering and deciphering.

UNIT- I (6 classes)

Introduction and Terminology -Monoalphabetic Substitution Ciphers-The Additive (or shift) Cipher - Modular Arithmetic - The Multiplicative Cipher - The Affine Cipher.

UNIT –II (7 classes)

Polyalphabetic Substitution Ciphers - Integer Matrices - The Hill Digraph Cipher - The Hill Trigraph Cipher - The Vigenère Square Cipher -The Permutation Cipher – Exponentiation cipher- Public Key Cryptography.

Text Book:

Elementary Number Theory , Kenneth H. Rosen, Pearson India Education services Pvt.Ltd, 6th edition.

Reference Book :

A Course in Number Theory and Cryptography by Neal Koblitz, Springer, New York.

Online Resources:

1. https://onlinecourses.nptel.ac.in/noc16_cs21
2. www.mastermathmentor.com