COURSE TITLE	**SECURITY ESSENTIALS**
COURSE CODE	**01CT0824**
COURSE CREDITS	**3**

Objective:

1 The Objective of this course is to give students an understanding of cryptography, various techniques of cryptography. Students will be able to apply the knowledge to protect sensitive information and ensure the integrity of industrial control processes that has placed a premium on cybersecurity skills in today's information technology market.

Course Outcomes: After completion of this course, student will be able to:

1 Understand the classical cryptosystems and concepts

2 Understand the various ciphers like monoalphabetic, polyalphabetic and Vigenère.

3 Apply the various mathematical functions such as GCD, Multiplicative inverse, Chinese remainder theorem

4 Understand the working of Block Cipher, DES

5 Understand and apply the Public Key Cryptography

Pre-requisite of course: Basic knowledge of OOP.

Teaching and Examination Scheme

Theory Hours	Tutorial Hours	Practical Hours	ESE	IA	CSE	Viva	Term Work
3	0	0	50	30	20	25	25

Contents : Unit	Topics	Contact Hours
1	**Module** Introduction to Cryptography, Codes and Ciphers, Cryptanalysis, Modern Guiding Principles in Cryptography, Types of Cryptanalytic Attacks, Frequency Analysis of Monoalphabetic Ciphers, Multi-Character Frequency Analysis, Frequency Analysis of Monoalphabetic Ciphers – Example, Key Length Determination in Polyalphabetic Ciphers, Example of Cracking a Vigenere Cipher, Divisibility, Primes, GCD, Modular Arithmetic, Multiplicative Inverses, Extended Euclidean Algorithm, Eulers Totient Function, Discrete Logarithms, Chinese Remainder Theorem, Block Cipher and DES, Double-DES and Meet-in-the-Middle Attack, Triple DES, Advanced Encryption Standard (AES), Cipher Block Chaining (CBC), Cipher Feedback (CFB), Output Feedback (OFB)Counter (CTR), Asymmetric Cryptography, Asymmetric Encryption for Message Confidentiality, RSA, Key Distribution and Management	42
Total Hours		**42**

MR. CHANDRASINH DHIRUBHA PARMAR
Digitally signed by (Name of HOD)

DR. RAJENDRASINH BAHADURSINH JADEJA
Digitally signed by (Name of Dean/ Principal)

Textbook :

1 Computer and Network Security Essentials, Kevin Daimi , Guillermo Francia , Levent Ertaul, Springer, 2017

References:

1 Cyber Security Essentials, Cyber Security Essentials, James Graham , Ryan Olson, CRC Press, 2010

Suggested Theory Distribution:

The suggested theory distribution as per Bloom's taxonomy is as follows. This distribution serves as guidelines for teachers and students to achieve effective teaching-learning process

Distribution of Theory for course delivery					
Remember / Knowledge	**Understand**	**Apply**	**Analyze**	**Evaluate**	**Higher order Thinking / Creative**
10.00	20.00	40.00	30.00		

Instructional Method:

1 Students may use supplementary resources such as online videos, NPTEL videos, e-courses, Virtual Laboratory, etc.

Supplementary Resources:

1 MOOC Course, NPTEL, COURSERA, Udemy, Infosys, Springboot, SWYAM etc. Online learning platform

MR. CHANDRASINH DHIRUBHA PARMAR
Digitally signed by (Name of HOD)

DR. RAJENDRASINH BAHADURSINH JADEJA
Digitally signed by (Name of Dean/ Principal)