COURSE CODE	COURSE TITLE	L	T	P	C
1152IT105	MODERN CRYPTOGRAPHY	3	0	0	3

Course Category:
~~Foundation (0)~~ / ~~Program Core (1)~~ /**Program Elective (2)** ~~/ Allied Elective (3) / University Elective (4) / Value Education Elective (5) / Independent Learning (6) / Industry – Higher Learning Institute Interaction (7).~~

a.Preamble :

This course provides an introduction to Modern Cryptography is an introductory-level treatment of cryptography written from a modern, computer science perspective.

a. Prerequisite Courses:

Introduction to cryptography , Cryptography and network security

b. Related Courses:

Network security
Principles and protocols

c. Course Educational Objectives :

Students undergoing this course are expected:

- Know about Classical encryption techniques
- Understand Block ciphers and pseudorandom functions

d. Course Outcomes :

Upon the successful completion of the course, students will be able to:

CO Nos.	Course Outcomes	Knowledge Level (Based on revised Bloom's Taxonomy)
CO1	Classical cryptography.	K1
CO2	Modern cryptography, symmetric and asymmetric ciphers.	K2
CO3	Symmetric ciphers. Key length, brute force attack.	K2
CO4	Examples of symmetric ciphers. Feistel, DES, modes of operation.	K2
CO5	Typical application of symmetric cryptograph	K2

e. Correlation of COs with POs :

COs	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	M		L		L							
CO2	M		L		M							
CO3	M		M		M							
CO4	M				M							
CO5	M				M							

H- High; M-Medium; L-Low

f. Course Content :

UNIT I **L-9**

Classical Cryptography-The Shift Cipher, The Substitution Cipher, The Affine Cipher Cryptanalysis-Cryptanalysis of the Affine Cipher ,Cryptanalysis of the Substitution Cipher, Cryptanalysis of the Vigenere Cipher, Shannon's Theory.

UNIT II **L-9**

Block Cipher and the Advanced Encryption Standard-Substitution -Permutation Netrworks, Linear Cryptanalysis, Differential Crypto analysis , The Data Encryption Standard, The Advanced Encryption Standard, Modes of Operation ,Cryptography Hash Function- Hash Function and Data Integrity,Security of Hash Function ,Iterated Hash Functions, Message

UNIT III **L-9**

The RSA Cryptosystem and Factoring Integer- Intoduction to Public –key Cryptography, Number theory,The RSA Cryptosystem ,Other Attacks on RSA,The ELGamal Cryptosystem,Shanks' Algorithm,Finit Fields,Elliptic Curves over the Reals, Elliptical Curves Modulo a Prime,Signature Scheme –Digital Signature Algorithm.

UNIT IV **L-9**

Identification Scheme and Entity Attenuation-Challenge – and – Response in the Secret-key Setting,Challenge – and – Response in the Public key Setting,The Schnorr Identificataon Scheme,Key distribution-Diffie-Hellman Key, Predustribution,Unconditionaly Secure key Predistribution,Key Agreement SchemeDiffie-Hellman Key agreement,Public key infrastructure-PKI,Certificates.

UNIT V **L-9**

Secret Sharing Schemes-The Shamir Threshold Scheme,Access Structure and General Scret key sharing,Informataion Rate and Construction of Effcient Schemes,Multicast Securuty and Copyright production-Multicast Security,Braodcast Encryption ,Multicast Re-keying,Copyright Protection ,Tracing Illegally Redistribution keys.

h. Learning Resources

i)Text Book

1. Introduction to Modern Cryptography Jonathan Katz and Yehuda Lindell,Chapman & Hall/CRC Press, Second or third edition

ii) Reference Books

1. Menges A. J , Oorschot P, Vanstone S.A,"Handbollk of Appliled Cryptography" CRC Press,1997.

2. William Stallings, "Cryptography and Network Security: Principles and Practices", Third Edition, Pearson Education,2006.

3. Wenbo Mao, "Modern Cryptography – Theory and Practice", Pearson Education, First Edition, 2006.

4. Charles B. Pfleeger, Shari Lawrence Pfleeger, "Security in Computing", Fourth Edition, Pearson Education, 2007. 14

5. Wade Trappe and Lawrence C. Washington, "Intrduction to Cryptography

iii) Online Learning:

- www.amazon.com/**Modern** **cryptography**-Applications.../dp/1852333081
- www.myreaders.info/01_Introduction_to_**modern cryptography**.pdf