COURSE CODE	COURSE TITLE	L	T	P	C
1152CS156	MODERN CRYPTOGRAPHY THEORY	3	0	0	3

Course Category: Program Elective

A. Preamble:

This course introduces to the concepts of IFP-based cryptographic systems and protocols, Discrete Logarithm Based Cryptography, Quantum Resistant Cryptography; Block Chain Technology and emphasizes their significance in modern cryptography.

B. Prerequisite Courses:

Sl. No	Course Code	Course Name
1	1152CS148	Modern Number Theory

C. Related Courses:

Sl. No	Course Code	Course Name
1	1152CS158	Cyber Security
2	1156CS601	Minor Project
3	1156CS701	Major Project

D. Course Outcomes:

Upon successful completion of the course, the students shall attain the abilities to

CO Nos.	Course Outcomes	Knowledge Level (Based on revised Bloom's Taxonomy)
CO1	Applythe concepts of integer factorization to solve simple cryptographic problems	K3
CO2	Apply the concepts of discrete logarithms to solve simple cryptographic problems	K3
CO3	Apply the concepts of elliptic curve discrete logarithms to solve simple cryptographic problems	K3
CO4	Summarizethe concepts of Quantum computational number theory to solve simple cryptographic problems	K2
CO5	Outlinebasic concepts of Block Chain Technology in Crypto currencies.	K2

E. Correlation of COs with POs:

Cos	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CO1	M		H										M		
CO2	H		H		L	L					L		M		
CO3	M		H		L	L					L		M		
CO4	H		H	L		L		M	L					M	L
CO5	M	H	L	L							L	M			L

H- High; M-Medium; L-Low

F. Course Content:

UNIT I: INTEGER FACTORIZATION BASED CRYPTOGRAPHY 9

RSA Cryptography- Cryptanalysis of RSA- Rabin Cryptography- Residuosity Based Cryptography- Zero-Knowledge Proof.

UNIT II: DISCRETE LOGARITHM BASED CRYPTOGRAPHY 9

Diffie Hellman Merkle Key Exchange Protocol- ElGamal Cryptography- Massey Omura Cryptography- DLP Based Digital Signatures

UNIT III:ELLIPTIC CURVE DISCRETE LOGARITHM BASED CRYPTOGRAPHY 9

Basic Ideas- Elliptic Curve Diffie Hellman Merkle Key Exchange Scheme- Elliptic Curve Massey Omura Cryptography- Elliptic Curve ElGamal Cryptography- Elliptic Curve RSA Cryptosystem.

UNIT IV: QUANTUM COMPUTATIONAL NUMBER THEORY 9

Quantum Algorithms for Order Finding- Quantum Algorithms for Integer Factorization- Quantum Algorithms for Discrete Logarithms- Quantum Algorithms for Elliptic Curve Discrete Logarithms- Coding Based Cryptography- Lattice-Based Cryptography- Quantum Cryptography

UNIT V:INTRODUCTION TO BLOCK CHAIN TECHNOLOGY 9

Block Chain Technology- Working of Block Chain Technology- Finanacial and Non-Financial applications, and implementation

Total: 45 Periods

G. Learning Resources

i. Text Books:

1. Song Y. Yan, "Computational Number Theory and Modern Cryptography", John Wiley (ISBN 978-1-118-18858-3), 2013.

2. Narayanan A, Bonneau J, Felten E, Miller A, and Goldfeder S, Bit coin and Cryptocurrency Technologies- A Comprehensive Introduction, Princeton University Press, 2016.

ii. Reference:

1. William Stallings, "Cryptography and Network Security: Principles and Practice", Seventh edition, Pearson, 2016
2. Jonathan Katz and Yehuda Lindel,"Introduction to ModernCryptography" CRC PRESS,2007.
3. Gilles Van Assche, "Quantum Cryptography and Secret-Key Distillation", Cambridge University Press,2006.
4. https://www.chatreddaccountantsanz.com/ The Future of Block Chain: Applications and Implementations of Distributed Ledger Technology.