Tulsiramji Gaikwad-Patil College of Engineering and Technology
Wardha Road, Nagpur-441 108
NAAC Accredited (A+ Grade)

Second Year (Semester-IV) B. Tech. Information Technology

BIT32425 :- Foundations of Cryptography

Teaching Scheme	
Theory	**3 Hrs/week**
Tutorial	**-**
Total Credits	**3**

Examination Scheme	
CT-I	15 Marks
CT-II	15 Marks
CA	10 Marks
ESE	60 Marks
Total	100 Marks
Duration of ESE: 3 Hrs	

Course Objectives:

1.	**To study** the principles of cryptography and the evolution of symmetric-key encryption techniques.
2.	**To classify** the design and security of stream and block ciphers, CPA-secure encryption, pseudorandom functions, and modes of operation of block ciphers.
3.	**To explore** symmetric cryptosystems and data integrity mechanisms such as DES, AES, message authentication codes, and cryptographic hash function constructions.
4.	**To analyze** hash-based applications, authenticated encryption schemes, key-exchange problems, and trapdoor function-based cryptographic primitives.
5.	**To apply** public-key cryptographic concepts including Diffie–Hellman, RSA, El Gamal, elliptic-curve cryptography, digital signatures, and secure communication protocols.

Course Contents

Unit I	**Foundations of Symmetric-Key Cryptography**: Course Overview and Security Goals, Symmetric-key Encryption, Historical Ciphers, Perfect Security and Its Limitations, Computational Security, Semantic Security, Pseudorandom Generators (PRGs)
Unit II	**Stream and Block Cipher Constructions:** Stream Ciphers, Provably-secure Instantiation of PRGs, Practical Instantiation of PRGs, CPA-Security, Pseudorandom Functions (PRFs), CPA-secure Ciphers from PRFs, Modes of Operation of Block Ciphers, Theoretical and Practical Constructions of Block Ciphers
Unit III	**Symmetric Cryptosystems and Hash Functions**: Data Encryption Standard (DES), Advanced Encryption Standard (AES), Message Authentication Codes (MACs), Information-theoretic Secure MACs, Cryptographic Hash Functions, Ideal Cipher Model, Davies–Meyer Construction, Merkle–Damgård Paradigm
Unit IV	**Hash Applications and Authenticated Encryption**: Birthday Attacks on Hash Functions, Applications of Cryptographic Hash Functions, Random Oracle Model, Authenticated Encryption, Generic Constructions of Authenticated Encryption Schemes, Key Exchange Problem, One-way and Trapdoor Functions, Cyclic Groups

Unit V	**Public-Key Cryptography and Secure Protocols**: Discrete Logarithm Problem, Computational and Decisional Diffie–Hellman Problems, Elliptic Curve Cryptography, Public-Key Encryption, ElGamal Encryption Scheme, RSA Assumption and RSA Cryptosystem, KEM–DEM Paradigm, CCA-security in Public-key Domain, CCA-secure Hybrid Encryption Schemes, Digital Signatures, RSA Signatures, Schnorr Identification and Signature Scheme, Overview of TLS/SSL, Basics of Number Theory, Interactive Protocols
Text Books	
T.1	Introduction to Modern Cryptography by Jonathan Katz and Yehuda Lindell
Reference Books	
R.1	Cryptography Theory and Practice by Douglas Stinson
Useful Links	
1	https://onlinecourses.nptel.ac.in/noc26_cs18/preview

	Course Outcomes	CL	Class Sessions
BIT32425.1	**Describe** the working principles of symmetric-key encryption schemes	2	9
BIT32425 .2	**Illustrate** the design principles and working of stream ciphers and their role in symmetric-key cryptography.	2	9
BIT32425.3	**Explain** the structure and working principles of symmetric cryptosystems	2	9
BIT32425.4	**Classify** the random oracle model and its significance in the security analysis of cryptographic schemes.	2	9
BIT32425.5	**Analyze** the working principles of secure communication protocols	4	9