

		Tulsiramji Gaikwad-Patil College of Engineering and Technology Wardha Road, Nagpur-441 108 NAAC Accredited (A+ Grade)			
Third Year (Semester-V) B. Tech. Information Technology					
BIT33525: - Secure Computation					
Teaching Scheme				Examination Scheme	
Theory	3 Hrs/week			CT-I	15 Marks
Tutorial	-			CT-II	15 Marks
Total Credits	3			CA	10 Marks
				ESE	60 Marks
		Total	100 Marks	Duration of ESE: 3 Hrs	
Course Objectives:					
1.	To introduce the mathematical foundations of secure computation and the fundamental secret sharing schemes.				
2.	To explain linear and general secret sharing schemes, access structures, secure message transmission, and the foundational principles of Multi-Party Computation.				
3.	To develop an understanding of the BGW protocol for perfectly secure MPC, including gate evaluation, degree reduction, and general adversary models.				
4.	To explain Oblivious Transfer and the GMW protocol for secure computation under semi-honest and malicious adversary models.				
5.	To introduce Yao's garbled circuit protocol for secure two-party computation and modern mixed-protocol MPC frameworks with real-world applications.				
Course Contents					
Unit I	Foundations of Cryptography and Secure Computation: Motivation for Secure Computation and Real-World Applications. Dimensions of Secure Computation. Review of Cryptographic Concepts. Basic Mathematical Foundations: Groups, Rings, and Fields. Introduction to Secret Sharing. Shamir Secret Sharing Scheme. Additive Secret Sharing. Replicated Secret Sharing				
Unit II	Secret Sharing and Secure Message Transmission: Linear Secret Sharing Schemes (LSSS). General Secret Sharing Schemes. Access Structures and Threshold Schemes. Applications of Secret Sharing. Secure Message Transmission. Security Goals: Privacy, Correctness, and Fairness. Introduction to Multi-Party Computation (MPC)				
Unit III	BGW Protocol and Perfectly Secure MPC: Ben-Or Goldwasser Wigderson (BGW) Protocol. Secure Evaluation of Addition and Multiplication Gates. Security Analysis of BGW Protocol. Degree Reduction Problem and Its Solutions. MPC in the Pre-processing Model. Perfectly Secure MPC with General Adversaries. Secure Three-Party Computation (3PC)				
Unit IV	Oblivious Transfer and GMW Protocol: Introduction to Oblivious Transfer (OT). 1-out-of-2 OT Protocol. Construction of OT from Cryptographic Assumptions. Goldreich-Micali-				

	Wigderson (GMW) Protocol. Security Analysis of GMW Protocol. Semi-Honest and Malicious Adversary Models. GMW Protocol in the Pre-processing Model. OT Extension Techniques
Unit V	Yao's Protocol and Advanced MPC Frameworks: Secure Two-Party Computation (2PC). Garbled Circuits and Yao's Protocol. Security Analysis of Yao's Protocol. Optimizations of Yao's Protocol. Mixed-World MPC Protocols. Arithmetic and Boolean Computation Models. ABY Framework for Secure Computation. Applications of MPC in Privacy-Preserving Machine Learning, Secure Voting, and Healthcare Data Sharing
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	Illustrate the working of Shamir, additive, and replicated secret sharing schemes.	2	9
BIT32425 .2	Interpret linear and general secret sharing schemes, access structures, secure message transmission, and the principles of Multi-Party Computation	2	9
BIT32425.3	Classify the BGW protocol for secure evaluation of gates and evaluate solutions to the degree reduction problem.	2	9
BIT32425.4	Analyze Oblivious Transfer and the GMW protocol under semi-honest and malicious adversary models.	2	9
BIT32425.5	Evaluate Yao's garbled circuit protocol and mixed-protocol MPC frameworks for privacy-preserving applications.	5	9