About IIT Kharagpur

Kharagpur - a dusty town tucked away in the eastern corner of India, famous until 1950 as home to the longest railway platform in the world - became the nursery where the seed of the IIT system was planted in 1951. IIT Kharagpur started its journey in the old Hijli Detention Camp in Eastern India, where some of the country's great freedom fighters toiled and sacrificed their lives for India's independence. Spurred by the success of IIT Kharagpur, four younger IITs sprouted around the country in the two following decades, and from these five came thousands of IITians, the brand ambassadors of modern India. It was the success of this one institution at Kharagpur that wrote India's technological odyssey.

The Institute takes pride in its relentless effort to provide the best platform for both education as well as research in the areas of science and technology, infrastructure designs, entrepreneurship, law, management, and medical science and technology. IITKGP is not just the place to study technology, it is the place where students are taught to dream about the future of technology and beam across disciplines, making differences enough to change the world.

Program Features/ Structure

Classroom lectures – **70%**

Class participation, discussion-**10%**

Numerical/ Problem solving, Case study and Activity – **20%**

Program Schedule and Venue

10 – 14 February 2020(9:30 AM – 6 PM)

IIT Kharagpur – Department of Mathematics

Program Fee

Nil for TEQIP-III sponsored participants

For others - INR 10,000/- (Ten thousand) **+ GST** @18% per participant

Who will benefit (Eligibility)

Teachers of TEQIP-III approved degree level engineering colleges

Teachers of Non-TEQIP-III, Research Scholars, Ph.D, U.G., P.G. students

Last day of Registration

31

January 2020

Accommodation

Accommodation will be provided to the TEQIP-III sponsored participants at the campus Guesthouse. For other participants, the same will be provided on chargeable basis as per rule.

How to Apply

Use the link: **https://erp.iitkgp.ac.in/CEP/courses.htm** to apply ONLINE.

Signup → Login → Profile Fillup → Choose a Program → Apply Now

Payment if applicable is to be done **ONLINE** after getting short listed for the program.

Contact Us:

Dr. Ratna Dutta, Principal Co-ordinator
Department of Mathematics
Indian Institute of Technology Kharagpur
Phone: +91 - 3222 - 282858
Email: ratna@maths.iitkgp.ac.in

NPIU

TEQIP-KIT

NPIU - A Unit of MHRD, Govt of India for Implementation of World Bank Assisted Projects in Technical Education

Indian Institute of Technology Kharagpur

ADVANCED TOPICS IN CRYPTOGRAPHY

10 – 14 February 2020

Introduction / Overview

Cryptography is the science of using mathematics to encrypt and decrypt data. Cryptography enables you to store sensitive information or transmit it across insecure networks (like the Internet) so that it cannot be read by anyone except the intended recipient. While cryptography is the science of securing data, cryptanalysis is the science of analyzing and breaking secure communication. Classical cryptanalysis involves an interesting combination of analytical reasoning, application of mathematical tools, pattern finding, patience, determination, and luck. Cryptanalysts are also called attackers.

Program Objectives

The aim of this course is to introduce the areas of cryptography and cryptanalysis to the participants. This course develops a basic understanding of the algorithms used to protect users online and addresses some of the design choices behind these algorithms. One of the major focus in this course is to build a workable knowledge of mathematics used in cryptology. The course emphasizes to provide a basic understanding of previous attacks on cryptosystems with the aim of preventing future attacks. A wide variety of basic cryptographic primitives will be discussed along with recent developments in some advanced topics like functional encryption, two-party/multi-party computation, bitcoin and crypto-currency and post quantum cryptography..

What you will learn

Program Content

- Introduction to Classical Cryptography
- Block and Stream cipher
- Data Encryption Standard (DES) & Modes of operations
- Advanced Encryption Standard (AES)
- Generic attacks on Symmetric Ciphers
- Introduction to Public Key Cryptography
- Elliptic Curves and Pairings
- Multilinear maps
- ID-based cryptosystems
- Broadcast Encryption
- Attribute-Based Encryption
- Homomorphic Encryption
- Functional Encryption
- Obfuscator
- Constrained PRF
- Witness encryption
- Commitment schemes
- Zero-Knowledge proofs - SNARK, SNARG
- Distributed PRF and Threshold Authenticated Encryption
- Construction of Trapdoor Function from CDH
- Homomorphic Secret Sharing
- Cloud computing - Private Anonymous Data Access
- Multi-party computation
- Introduction to Post-Quantum Cryptography – lattice-based, code-based and multivariate
- Bitcoin and crypto-currency

About the Faculty

Dr. Sourav Mukhopadhyay

Sourav Mukhopadhyay is an Associate Professor, Department of Mathematics at Indian Institute of Technology Kharagpur. He has completed his B.Sc (Honours in Mathematics) in 1997 from University of Calcutta, India. He has done M.Stat (in statistics) and M.Tech (in computer science) from Indian Statistical Institute, India, in 1999 and 2001 respectively. He worked with Cryptology Research Group at Indian Statistical Institute as a PhD student and received his Ph.D. degree in Computer Science from there in 2007. He was a Research Assistant at the Computer Science department of School of Computing, National University of Singapore (NUS). He visited Inria Rocquencourt, project CODES, France and worked as a post-doctoral research fellows at the School of Computer Engineering, Nanyang Technological University (NTU), Singapore. He was a post-doctoral research fellows with School of Electronic Engineering, Dublin City University (DCU), Ireland.

Course Coordinator

Dr. Ratna Dutta

Ratna Dutta is an Associate Professor, Department of Mathematics at Indian Institute of Technology Kharagpur. She worked with Cryptology Research Group at Indian Statistical Institute as a PhD student and received his Ph.D. degree in Computer Science from there in 2006. She worked as post-doctoral research fellow, Claude Shannon Institute, NUIM, Maynooth, Co. Kildare, Ireland and worked as research fellow, Institute for Infocomm Research, 21 Heng Mui Keng Terrace, Singapore. Her research interests include attribute based encryption, broadcast encryption, functional encryption, traitor tracing, witness encryption and lattice based cryptography.

Tentative lecturers from IIT Kharagpur and ISI Kolkata