Course 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.

Tentative Faculty:

IIT Kharagpur and ISI Kolkata faculty will deliver the lectures.

Eligibility:

Category A:

I. Teachers of TEQIP-III approved degree level engineering colleges

Category B:

II. Teachers of Non-TEQIP-III degree level engineering colleges
III. Engineers/Researchers from Govt. Labs/Industry
IV. Research Scholars (PhD students) from IIT Kharagpur/ Other Institution
V. IIT non-faculty

Tentative Contents:

1. Introduction to Classical Cryptography
2. Block and Stream cipher
3. Data Encryption Standard (DES) & Modes of operations
4. Advanced Encryption Standard (AES)
5. Introduction to PKC
6. Provable Security: Security Reductions
7. Secret Sharing and Visual Cryptography
8. Broadcast Encryption and Attribute-Based Encryption
9. Functional Encryption
10. Elliptic Curve Cryptography
11. Stream Cipher Cryptanalysis
12. Multi-party computation
13. Obfuscator & Multilinear maps
14. ID-based cryptosystems
15. Lattice-based cryptography
16. Code-based cryptography
17. Multivariate Public Key Cryptography
18. bitcoin and crypto-currency
19. Block cipher cryptanalysis
20. Introduction to Quantum Cryptography

Course Website:
http://www.facweb.iitkgp.ac.in/~ratna/confi.htm

A TEQIP-III Short Term Course
on
“Modern Cryptography”

September 17-21, 2018

Last date of application September 5, 2018

A Continuing Education Programme of Indian Institute of Technology Kharagpur

INDIAN INSTITUTE OF TECHNOLOGY KHARAGPUR.
भारतीय प्रौद्योगिकी संस्थान खड़गपुर
1951
योगः कर्मसु कौशलम्

Organized by

Department of Mathematics
Indian Institute of Technology
Kharagpur - 721302
West Bengal, India

General Information:

Kharagpur is situated at a distance of 130 km from Kolkata and is unique with its green, calm and quiet campus. Historically, IIT Kharagpur started its journey in the "Hijli detention camp" which presently houses a science and technological museum known as the Nehru Museum of Science and Technology.

Connectivity:

Kharagpur is an important junction and is well-connected to all parts of the country by rail service (SER). Numerous local and express trains are available from Howrah. The institute is approximately 7 km from Kharagpur railway station. Auto-rickshaws (Rs. 100) and taxis (Rs. 150) are available from the railway station for reaching IIT Campus.

Course Coordinators:

Prof. Ratna Dutta
Department of Mathematics,
IIT Kharagpur, Kharagpur-721302,
West Bengal, India.
Email:
ratna@maths.iitkgp.ernet.in
Phone: +91-3222-282858(O)
09836215016(Mob)
FAX : 03222-255303

Accommodation and Food:

Limited shared accommodation is available in institute guest houses for TEQIP-III affiliated faculty members without payment. Shared accommodation for other participants is available on a payment basis (Rs. 1000/- per day in TGH A/C single room or Rs. 1500/- for double occupancy). On prior intimation, we will try to arrange accommodation with the above charges. *Course fee includes food and snacks.*

Course Fee:

Category A

TEQIP-III faculty	NO FEE*

*TEQIP-III Faculties should send an account payee cheque of **Rs: 2000** only in the name of "**CEP- ISWT**" during their application, without which the application will not be entertained. The cheque will be sent to the address:
Prof. Ratna Dutta
Department of Mathematics, IIT Kharagpur, Kharagpur -721302, West Bengal, India (by 5th September)
(The same cheque will be handed over at the time of certificate distribution.)

Category B

Overseas Participants	US $400
Self-sponsored Participants	INR 8000
IIT-KGP student	INR 4000
Sponsored Industry/ Research Organizations	INR 12000
Outside student	INR 5000

For category A, course material, accommodation and food will be provided with no fee. For Category B, course fee includes course material and food. The fee is inclusive of GST.

How to Apply:

Procedure for applying in IIT Kharagpur online Course Registration portal
Use the link: https://erp.iitkgp.ernet.in/CEP/courses.htm

Step to be followed:

1. Sign-Up
2. Verify your email-id (link will be send to your e-mail)
3. Login
4. Edit Profile(Fill up all the mandatory fields, upload photo and signature)
5. Click on 'APPLY NOW' button.
6. Upload your pdf format id-card.

An e-mail will be communicated from the Continuing Education Program, IIT Kharagpur to the shortlisted applicants stating the payment details.

** *This is one time sign up process in apply to IIT Kharagpur online Course Registration portal*. You can apply to other courses using the same credential.