Course Objectives:

Cryptography is the science or art of securing data. It is the study of information hiding and verification. Cryptography has crept into everything, from Web browsers and e-mail programs to cell phones, bank cards, cars and even into medical implants, voting system. The fundamental objective of this course is to provide an introduction to modern cryptography and cryptanalysis. A wide variety of basic cryptographic primitives will be discussed in this course. It will enable the participants to learn the use of Mathematics in Cryptology. The course will help to get the idea about the attacks on existing cryptosystems along with the possible preventions. In addition to that, some advanced topics like post-quantum cryptography, electronic voting, functional encryption, Blockchain, crypto-currency and two-party/multi-party computation.

Tentative Speakers:

- Dr. Sourav Mukhopadhyay, Associate Professor, IIT Kharagpur
- Dr. Ratna Dutta, Associate Professor, IIT Kharagpur
- Dr. Avishek Adhikari, Professor, Presidency University
- Dr. Tarni Mandal, Professor, NIT Jamshedpur
- Dr. Sumit Kumar Debnath, Assistant Professor, NIT Jamshedpur (Coordinator)
- Dr. Ratnesh Mishra, Assistant Professor, NIT Jamshedpur

Eligibility:

1. Faculty/UG/PG/Research Scholars from any Central/State/Private University or Institute.
2. Interested Participants from Industry.

Tentative Contents:

- Introduction to Classical Cryptography
- Block and Stream cipher
- Data Encryption Standard (DES) & Modes of operations
- Advanced Encryption Standard (AES)
- Introduction to PKC
- Provable Security: Security Reductions
- Secret Sharing
- Broadcast Encryption and Attribute-Based Encryption
- Functional Encryption
- Elliptic Curve Cryptography
- Stream Cipher Cryptanalysis
- Multi-party computation
- Obfuscator & Multilinear maps
- ID-based cryptosystems
- Code-based cryptography
- Lattice-based cryptography
- Multivariate Public Key Cryptography
- Blockchain and crypto-currency
- Block cipher cryptanalysis

Organizing Committee:

Patron: **Prof. Karunesh Kumar Shukla**
Director NIT, Jamshedpur

Chairperson: **Prof. Tarni Mandal,**
HOD, Dept. of Mathematics, NIT Jamshedpur

Coordinator: **Dr. Sumit Kumar Debnath**
Assistant Professor, Dept. of Mathematics, NIT Jamshedpur

A TEQIP-III Short Term Course on Introduction to Modern Cryptography (IMC-2019)

July 01-06, 2019

Last date of application: June 10, 2019

Organized by

Department of Mathematics
National Institute of Technology
Jamshedpur - 831014
Jharkhand, India

General Information:

Jamshedpur is the first well-planned industrial city of India, founded by the late Jamshedji Nusserwanji Tata and ranks 28th among the 35 million-plus cities and is also the 31st urban agglomeration in India according to the census 2001. Located in the East Singhbhum district of Jharkhand on the Chota Nagpur plateau, it is the district headquarters and is surrounded by the beautiful Dalma Hills. The rivers Subarnarekha and Kharkai border the North and West of the city, respectively. The institute is located in Adityapur town of the district which is at the border of Saraikela-Kharswan district and East Singhbhum district. Adityapur is a highly industrialized town having hundreds of small and medium scale industries.

Connectivity:

- **Railway:** The railway station of Jamshedpur is known as Tatanagar Junction. Tatanagar (Jamshedpur) is an important railway junction & a model station on the South Eastern Railway and is the most important railway junction of the state as it is connected directly to all the major cities of India. The institute is approximately 8 km from Tatanagar railway station.
- **Airways:** I. Birsa Munda Airport, Ranchi, Jharkhand is connected with Jamshedpur through NH-33. Road distance is about 140km. Numerous bus services are available between Ranchi and Jamshedpur.

  II. Netaji Subhash Chandra Bose Domestic & International Airport, Kolkata is 260km away from Jamshedpur. The best way of travelling is by train which will take 4-5 hours. By road it takes about 6 hours.

For further information please contact

Course Coordinator:

Dr. Sumit Kumar Debnath
Department of Mathematics,
NIT Jamshedpur,Jamshedpur-831014, Jharkhand, India.
Email: sdebnath.math@nitjsr.ac.in
Phone: +917001672827

Accommodation:

Limited accommodation in institute hostels is available without payment. It can be arranged on request for those participants who have remitted the registration fee before due date.

Registration Fee:

Overseas Participants	US $200
Faculty	INR 4000
Participants from Industry	INR 4000
Outside Students	INR 3500
NIT Jamshedpur Students (without food)	INR 1000

Note: (i) No TA and DA will be provided.

(ii) Registration Fee includes only Food and Kits for outside participants.

(iii) **Reduced registration fee for outside participants without food and without accommodation is INR 1000.**

(iv) Registration Fee has to be paid through direct fund transferred to the following bank account within due date.

(iv) Please mention "**IMC2019**" in the place of remark/comment at the time of online transfer.

(v) Duly signed application form along with the proof of online transfer/bank transfer should be emailed to sdebnath.math@nitjsr.ac.in.

BANK ACCOUNT DETAILS:

A/c. No: 38273724736
A/c. Name: SHORT TERM COURSE DEPARTMENT OF MATHEMATICS NIT JAMSHEDPUR
Bank Name: STATE BANK OF INDIA Branch: NIT, JMSHEDPUR

IFSC CODE: **SBIN0001882** MICR: 831002004
BRANCH CODE: 1882

APPLICATION FORM

A TEQIP-III Short Term Course

on

Introduction to Modern Cryptography

(IMC-2019)

July 01-06, 2019

Last date of application: June 10, 2019

Organized by

Department of Mathematics

National Institute of Technology Jamshedpur

(Scanned Copy of duly signed application form along with the proof of online transfer/bank transfer should be emailed to the Course Coordinator)

1. Name (Mr./Ms./Dr.)**:** ……....
2. Category**:** Academic/Industry/Student (Attach Institute/Company ID proof)
3. Affiliation**:** ….....
4. Address**:** ….....

5. Email**:**….....
6. Mobile No**:** ….....
7. Qualification**:** ….....
8. Payment Details**:**
   Amount….....
   Online Transaction ID…….....
   Date of Transaction .....

9. Accommodation Details*:
   Accommodation required (Yes/No)…….

Signature of the applicant

Signature of Head of the Institution/Head of the Department with seal