

# National Workshop on Cryptology (NWC 2023)

An event of Cryptology Research Society of India (CRSI)



**LNMIIT**   
The LNM Institute of  
Information Technology

@  
LNMIIT Jaipur

August 01–05, 2023

Dr. Jayaprakash Kar

## **Brief Summary**

The LNM Institute of Information Technology, Jaipur, in association with Cryptology Research Society of India (CRSI) shall be hosting National Workshop on Cryptology (NWC) 2023 in Campus from 1st to 5th August 2023. The event shall have invited talks by eminent researchers and practitioners working in the area of Cryptology in various organizations and academic institutes across the country. Subject areas of the invited talks shall include Post-Quantum Cryptography, Light-Weight Cryptography, Homomorphic Encryption and other advanced areas in Applied Cryptology. Workshop participants' profile is expected to be a mix of students working in the area of cryptology; Data Security, cryptography products' users from various defense and security agencies and cryptology product developers from organizations and companies across the country.

The event is expected to increase collaboration amongst cryptology researchers within the National Community. It shall also help expose students and other workshop participants to the cutting-edge frontiers of research and development in Cryptology and Data Security. The event shall help the LNMIIT to create more collaboration opportunities with academia as well as industry partners for carrying out National Projects in the areas of Cryptology and Data Security.

## **About the Event**

## Event Overview

**Date:** August 01–05, 2023  
**Venue:** Lecture hall 17, RIEP building, the LNMIIT Jaipur.  
**Organizers:** The LNMIIT Jaipur,  
**General Chair** Jayaprakash Kar, LNMIIT Jaipur  
Avisekh Adhikar, Presidency University Kolkata

## Resource Person/s:

1. Bimal Roy, ISI Kolkata
2. Mridul Nandi, ISI Kolkata
3. Somitra Kumar Sanadhya , IIT Jodhpur
4. Avishek Adhikari, Presidency University Kolkata
5. Arpita Maitra, TCG Crest
6. Suchetna Chakraborty, IIT Jodhpur
7. C Pandu Rangan, IIT Madras
8. Jayprakash Kar, The LNMIIT Jaipur

## Organization

**Chief Patron** Rahul Banerjee LNMIIT Jaipur, India  
**General Chair** Jayaprakash Kar, LNMIIT Jaipur  
Avisekh Adhikar, Presidency University Kolkata

## Organizing Committee

Shweta Bhandari, LNMIIT Jaipur, India  
awan Kumar LNMIIT Jaipur, India  
Ashish Kumar Dwivedi LNMIIT Jaipur, India  
Sakthi Balan, LNMIIT Jaipur, India  
Subrat Dash, LNMIIT Jaipur, India  
Sandeep Saini, LNMIIT Jaipur, India

## Program Committee

Bimal Roy Indian Statistical Institute Kolkata, India  
C Pandu Rangan Indian Institute of Technology Madras, India  
Avishek Adhikari Presidency University Kolkata  
Debdeep Mukhopadhyay Indian Institute of Technology Kharagpur, India  
Deepak Garg Bennett University, India  
Sourav Mukhopadhaya Indian Institute of Technology Kharagpur, India  
Somitra Sandhya Indian Institute of Technology Jodhpur, India  
Deepak Kumar Dalai National Institute of Science Education and Research (NISER)  
Bhubaneswar, India  
Jayaprakash Kar The LNM Institute of Information Technology Jaipur, India  
Mridul Nandi Indian Statistical Institute Kolkata, India  
N V Narendra Kumar IDRBT Team, India  
Rajesh Pillai DRDO, India

Ratna Dutta	Indian Institute of Technology Kharagpur, India
S P Suresh	Chennai Mathematical Institute Madras, India
Santanu Sarkar	Indian Institute of Technology Madras, India
Subhamoy Maitra	Indian Statistical Institute Kolkata, India
Sumit K. Pandey	Indian Institute of Technology Jammu, India
Sushmita Ruj	Indian Statistical Institute Kolkata, India
Vishal Saraswat	Bosch Engineering and Business Solutions, India
Bhupendra Singh	DRDO Bengaluru, Karnataka, India
Migrignka Mandal	Indian Institute of Technology Jodhpur
Bimal Mondal	Indian Institute of Technology Jodhpur

## REGISTRATION PROCESS

There is no cost for attending the workshop for students, professionals from industry and government organizations and faculty members doing thesis/ research/ projects in cryptology & allied areas. However, prior registration is mandatory. Request for registration can be given below

### Note for students interested in attending the workshop:

A limited Number of Student Travel Grants are sponsored by CRSI and IEEE Communications Society-Delhi Chapter for PhD/ PG/ Final year UG students working in the area of cryptology and other allied areas in network security. As part of the student travel grants, round-trip AC 3 Tier fares of Indian Railways from student's place of study to Jaipur can be reimbursed subject to presenting the proof of travel and full attendance in NWC on all the 5 days. Interested students may give request for registration ASAP

### Registration details

- (i) CRSI student member : full waiver
- (ii) CRSI life member not student : INR 1200
- (iii) Other : INR 2000

o pay the registration amount, please transfer the amount to the following account and then share the transaction details on the registration link.

### Areas of interest include applied cryptology such as (but are not limited to) the following topics-

- Introduction to Cryptography
- Symmetric Key Cryptography
- Cryptanalysis
- Public Key Cryptography
- Hash function
- Secret Sharing
- Multi Party Computation
- Internet of Things

## **Details of Participants:-**

No. of Internal Faculty :- 19

No. of External Students :- 64

## **Invited Talks**

### **Some recent advances in Cryptology**

Dr. Bimal Roy

ISI Kolkata

bimal@isical.ac.in

1 August 2023 - 10:30AM -12:30 PM

### **Attacks on Symmetric Key Designs**

Dr. Mridul Nandi

ISI Kolkata

mridul.nandi@gmail.com

1 August 2023 - 02:00PM - 03:30 PM

### **An Introduction to Secret Sharing Schemes for Secure Data Sharing**

Dr. Avishek Adhikari

Presidency University Kolkata

avi@psych.ucla.edu

2 August 2023 - 10:00AM - 12:30 PM

### **Mathematical Hard Problems- Assumption and Cryptanalysis, Cryptographic Primitives**

Dr. Jayprakash Kar

The LNMIIT Jaipur

jayprakashkar@lnmiit.ac.in

2 August 2023 - 03:00PM - 04:30 PM

### **Few Open Issues Related to Secret Sharing**

Dr. Avishek Adhikari

Presidency University Kolkata

avi@psych.ucla.edu

3 August 2023 - 10:00AM - 11:30 PM

### **Selected Topics in Quantum Cryptography**

Dr. Arpita Maitra

TCG Crest

3 August 2023 - 12:00PM - 01:30 PM

### **Cybersecurity Threat Modeling using Meta Attack Language**

Dr. Ashish Kumar Dwivedi  
The LNMIIT Jaipur  
3 August 2023 - 03:00PM - 04:30 PM

**DeFI Security**  
Dr. Mohit Gupta  
The LNMIIT Jaipur  
4 August 2023 - 10:00AM - 11:30 PM

**Pairing based Cryptography**  
Dr. Somitra Sanadhya  
IIT Jodhpur  
4 August 2023 - 12:00PM - 01:30 PM

**Hands-on: Cybersecurity Threat Modeling using Meta Attack Language**  
Dr. Ashish Kumar Dwivedi  
The LNMIIT Jaipur  
4 August 2023 - 03:00PM - 04:30 PM

**Trust in Sensory Data: Case studies for IoT and CP**  
Dr. Suchetana Chakraborty  
IIT Jodhpur  
5 August 2023 - 12:00PM - 01:30 PM

**Blockchain trilemmas - past, present and future**  
Dr. Pandurangan Chandrasekaran  
IIT Madras  
prangan55@gmail.com  
5 August 2023 - 03:00PM - 04:30 PM

### **Few snaps:**

Some of the pictures of the NWC are shown below:





Nation



