

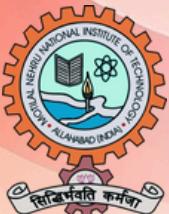
NATIONAL INSTRUCTIONAL WORKSHOP

ON CRYPTOLOGY

LATTICE BASED CRYPTOGRAPHY

(1-5 July 2024)

Organized by



Department of Mathematics
Motilal Nehru National Institute of Technology
Allahabad
&
Cryptology Research Society of India

Venue

Motilal Nehru National Institute of Technology
Allahabad, Prayagraj-211004 (U.P.)



ABOUT THE INSTITUTE

Motilal Nehru National Institute of Technology, Allahabad (MNNIT) was established as one of the seventeen Regional Engineering Colleges of India in the year 1961. On June 26, 2002 MNREC was transformed into the National Institute of Technology fully funded by Government of India. The Institute now offers nine B.Tech., twenty four M.Tech. Degree Programmes, MCA, MBA, M.Sc. (Mathematics and Scientific Computing) and Master of Social Work (M.S.W.) programmes also register candidates for the Ph.D. degree. The Institute has been recognized by the Government of India as one of the centers for the Quality Improvement Programme for M.Tech. and Ph.D. It is an institute with total commitment to quality and excellence in academic pursuits and is among one of the leading institutes in India.

ABOUT THE DEPARTMENT

The Department of Mathematics came into existence w.e.f., 1st April 2003; prior to this, it constituted a section of the Department of Applied Sciences & Humanities. The department offers core courses at the undergraduate level and several advanced courses at post graduate level. The department also enrolls candidates for the Ph.D. programme. There is widespread interaction between the Mathematics department and various Engineering departments in the field of teaching and research. The Department of Mathematics started a full-time M.Sc. in Mathematics & Scientific Computing program since 2008 and admission is done through JAM (Joint admission in M.Sc.) conducted by IIT.

ABOUT CRYPTOLOGY RESEARCH SOCIETY OF INDIA

Set up in 2001, CRSI is a scientific assembly made up of academicians, researchers, specialists, students, and institutions who are interested in promoting the science and technology of Cryptology and Data security and related theory and applications in India. The CRSI has been founded for:

- Supporting and promoting research activities in cryptology and data security in India.
- To arrange lectures, discussions, workshops, seminars, conferences, etc. to motivate and guide the young Indian researchers in the field of cryptology and data security.
- Organizing the annual events INDOCRYPT- the International Conference on Cryptology and Security, the National Workshop on Cryptology and National Instructional Workshop on Cryptology.

OBJECTIVE OF THE WORKSHOP

The subject of Cryptology (mathematical techniques related to aspects of information security and cryptanalysis) is developing rapidly and its popularity is increasing day by day in information sciences, particularly in network, banking, mail, and information security-related activities. CRSI (Cryptology Research Society of India) organizes this workshop every year, in co-operation with an Indian institution, to reach students all across the country and provide them with a platform to explore the opportunities in Cryptology and related fields of study and research. The objective of this workshop is to systematically expose the students and faculties of Mathematics and Engineering to the basic understanding of Cryptology, Post Quantum Cryptography, Lattice based Cryptography, Network Security and other information security-related issues and applications.

ELIGIBILITY

Students, Faculty, and Industry Executives. Participants familiar with the area of Algebra / Number Theory / Cryptography / Information Security are preferred.

RESOURCE PERSONS

Resource persons from various IITs, ISI, DRDO and other reputed organizations will be delivering the expert lectures.

List of tentative speakers are

- Prof. Bimal Roy, ISI Kolkata, General Secretary CRSI
- Dr. N Rajesh Pillai, Scientist H, Director SAG, DRDO New Delhi
- Dr. Bhupendra Singh, Scientist F, CAIR, DRDO, Bangalore
- Dr. Indivar Gupta, Scientist F, SAG DRDO, New Delhi
- Dr. Dhananjay Day, IIIT Lucknow
- Dr. Angshuman Karmakar, IIT Kanpur
- Dr. Vishal Saraswat, Bosch Cybersecurity and Global Software Technologies, Bosch, India
- Dr. Rajeev Anand Sahu, Bosch Cybersecurity and Global Software Technologies, Bosch, India
- Dr. Mahaveer Jhawar, Ashoka University
- Dr. Shashank Singh, IISER Bhopal
- Dr. Sonika Singh, CMP Degree College, University of Allahabad
- Prof. Shiv Datt Kumar, MNNIT Allahabad
- Dr. Sahadeo Padhye, MNNIT Allahabad
- Dr. Shashank Srivastava, MNNIT Allahabad