

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 National Institute of Technology fully funded by Government of India. The Institute now offers nine B.Tech., nineteen M.Tech. Degree Programmes, MCA, MBA, M.Sc. (Mathematics and Scientific Computing) and Master of Social work (M.S.W.) programmes and also registers 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

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 undergraduate level and several advanced courses at post graduate level. The department also enrolls candidates for Ph.D. programme. There is a wide spread interaction between mathematics department and various engineering departments in the field of teaching and research. The department of Mathematics started full time M.Sc. in Mathematics & Scientific Computing program since 2008 and admission is done through JAM (Joint Admission test for M.Sc) conducted by IIT.

ABOUT CRYPTOLOGY RESEARCH SOCIETY OF INDIA

Set up in 2001, CRSI is a scientific assembly made up of academicians, researcher, 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. for motivating and guiding the young Indian researchers in the field of cryptology and data security.
- Organizing the annual events INDOCRYPT- the International Conference on Cryptology and Security and the National Workshop on Cryptology.

ADVISORY COMMITTEE

- Prof. Rajeev Tripathi, Director, MNNIT Allahabad.
- Prof. Bimal Roy, ISI Kolkata & General Secretary of CRSI
- Prof. R. Balasubramanian, IMSC, Chennai & President of CRSI
- Prof. C. Pandurangan, IIT Chennai
- Prof. M.M. Gore, Dean, P & D, MNNIT Allahabad
- Prof. Haranath Kar, MNNIT Allahabad
- Prof. Sunita Agarwal, MNNIT Allahabad
- Prof. Ramji Lal, Retd. Prof. University of Allahabad
- Prof. Kalyan Chakraborty, HRI, Allahabad

ORGANIZING COMMITTEE

- Prof. Rajeev Tripathi (Patron)
- Prof. Haranath Kar, Head, Deptt. of Mathematics
- Prof. Shiv Datt Kumar (Chairman)
- Dr. Sahadeo Padhye (Convener)
- Dr. Pitam Singh (Coordinator & Treasurer)
- Dr. S.N. Pandey, Member
- Dr. Pramod Kumar Yadav, Member
- Dr. Garakh Nath, Member
- Dr. B. Vasu, Member
- Dr. Mukesh Kumar, Member
- Dr. Surabhi Tiwari, Member
- Dr. Shashank Srivastava, Member

STUDENT WORKING COMMITTEE

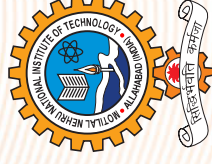
- Ms. Sonika Singh
- Ms. Swati Rawal
- Mr. Abhishek Juyal
- Ms. Deepika Agarwal
- Mr. Atul Kumar Tiwari
- Mr. Digvijay Singh
- Mr. Atul Kumar Ray
- Ms. Ankita Dubey
- Ms. Sneha Jaiswal
- Ms. Sumita Singh
- Mr. Jaykant Yadav

National Instructional Workshop

on

CRYPTOLOGY (NIWC-2018) (6-10 June, 2018)

Organized by



Department of Mathematics

Motilal Nehru National Institute of Technology Allahabad

Cryptography Research Society of India

Venue

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

Dr. Sahadeo Padhye
Convener

Prof. Shiv Datt Kumar
Chairman

Dr. Pitam Singh
Co-ordinator



Department of Mathematics

Motilal Nehru National Institute of Technology
Allahabad

National Instructional Workshop on Cryptology
(NIWC-2018)
(6-10 June, 2018)

APPLICATION FORM

Name.....
Designation.....
Department.....
Area of Interest and Specialization.....
Institute/Organization.....
CRSI Member (Yes/No)..... Membership No.
Address.....
.....
.....
Contact (Phone/Mobile).....
Email.....
Mode of travel: Air/train/bus.....
Accommodation Required: Yes/No.....
Accompanying person (on payment basis, if any, with name(s) & relationship).....
.....

Signature of Participant
Signature of Head of Department/Institute

WFOZ
1. Please send your CV through email.
2. DD/NEFT in favor of NIWC-2018, MNNIT Allahabad payable at Allahabad should be send after notification of confirmed participants to:

Dr Sahadeo Padhye

Convener, NIWC-2018
Department of Mathematics
Motilal Nehru National Institute of Technology
Allahabad-211004
Email-sahadeomathru@gmail.com
Contact- +91-9453256043, 0532 - 2271257

TOPICS TO BE COVERED

The following are some of the main topics-

- Basics of Number Theory - Modular arithmetic, Primality Testing, Factoring, DLP etc.
- Basic Algebra-Finite Field, Galois field etc.
- Some Mathematical Problems and their Applications in Cryptography
- Classical Cryptosystems
- Modern Block Ciphers and Stream Cipher
- Public Key Cryptosystems: RSA, ElGamal, ECC etc.
- Hash Function and Digital Signature
- Secret Sharing
- ID-based Cryptography
- Post-quantum Cryptography
- Lattice-based Cryptography

REGISTRATION FEE

Industry Executive/Officer/Faculty: ₹ 2000/-

Student / Research scholar : ₹ 1000/-

(Registration fee is waived 50% for CRSI members)

Registration fee may be paid through DD/NEFT payable at Vijaya Bank, MNNIT Allahabad drawn in favor of NIWC-2018 after notification of the confirmed participants. A/c No. for NEFT will be communicated to the selected participants.

TRAVELLING ALLOWANCE AND ACCOMMODATION

Boarding, Lodging and AC III train fare to participants will be provided.

IMPORTANT DATES

Last date for receipt of application: 24-03-2018

Notification of Accepted Participants: 30-03-2018

Last Date of Confirmation/Registration: 15-04-2018

OBJECTIVE OF THE WORKSHOP

The subject of cryptography (mathematical techniques related to aspects of information security and crypt analysis) 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 the 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, Network Security and other information security related issues and applications.

ELIGIBILITY

Students, faculty, Industry Executives. Participants familiar in the area of Algebra/Number Theory/Cryptography/ Information Security are preferred. A reference/ recommendation letter is required for the P.G. students and research scholars.

RESOURCE PERSONS

Resource persons from various IIT's, ISI, DRDO and other reputed organizations will be delivering the expert lectures. List of confirmed speakers are :

- Prof. Bimal Roy, ISI Kolkata
- Prof. R Balasubramanian, IMSC Chennai
- Prof. C. Pandu Rangan, IIT Chennai
- Dr. Debdeep Mukhopadhyay, IIT Kharagpur
- Dr. Vishal Saraswat, R.C. Bose Center for Cryptography and Security, ISI Kolkata
- Dr. Sartaj Ul Hasan, IIT Jammu
- Dr. Somitra Kumar Sanadhya, IIT Ropar
- Dr. Nitin Saxena, IIT Kanpur
- Dr. Dhyanjay Day, Scientist F, SAG DRDO New Delhi
- Dr. Rajesh Pillai, Scientist G, SAG DRDO New Delhi
- Dr. Ashish Choudhary, IIT Bangalore
- Dr. Shashank Singh, IIT Kanpur

LIST OF SPEAKERS FROM MNNIT, ALLAHABAD

- Prof. Shiv Datt Kumar, Department of Mathematics
- Dr. Sahadeo Padhye, Department of Mathematics
- Dr. Pitam Singh, Department of Mathematics
- Dr. Shashank Srivastava, Computer Science & Engineering Department