

NATIONAL INSTRUCTIONAL WORKSHOP ON CRYPTOLOGY (NIWC)-2015

18-22 MAY, 2015

Organized by:



Department of Mathematics & Statistics
Himachal Pradesh University, Shimla
&
Cryptology Research Society of India

Venue:

Himachal Pradesh University,
Summer Hill, Shimla-171005 (H .P.)

Prof. P. L. Sharma

Organizing Secretary

E -mail: plsharma1964@gmail.com

Mobile: 94180-03066

Prof. Joginder Singh Dhiman

Convener, NIWC-2015

&

Chairman, Deptt. of Mathematics & Statistics



ABOUT THE UNIVERSITY

The Himachal Pradesh University was founded on July 22, 1970. It is located at Summer Hill which is at a distance of 5 kms from the main town, Shimla. The University is nestled amidst tall and lush green trees of deodars, oaks, pines and rhododendrons. The campus where one half bathes in the fresh sun towards the east and another half in the grandeur of unique sunset on the West. Its salubrious climate and calmness presents congenial atmosphere to pursue higher studies. The University campus occupies an area of 200 acres and has been designed to possess a distinctive architectural style. Himachal Pradesh University is the only multi-faculty and affiliating University in the state. It firmly believes in what India's first Prime Minister Jawaharlal Lal Nehru said in his oft. Cited convocation address at the University of Allahabad, "A University stands for humanism, for tolerance, for region, for progress, for the adventure of ideas and for the search for truth. It stands for the onward march of the human race towards even higher."

ABOUT THE DEPARTMENT

The Department of Mathematics and Statistics started in 1971 under the dynamic leadership of **Padma Bhusan Professor P. L. Bhatnagar**. Over the years the department has made its mark in the academic world. **Professor M. B. Banerjee** of the department was awarded the Shanti Swaroop Bhatnagar Award in 1988, Professor S. N. Dube, Professor M. B. Banerjee and Professor R. C. Sharma have been conferred F.N.A.Sc. Over the years more than 100 students have completed their Ph.D. Degree in Mathematics from the University. In recognition of large number of National and International research publications by the faculty members and other academic initiatives, the department has been selected by the UGC for Special Assistance

Program (SAP,DRS-I) in 2009 and after the assessment of the research work done in the previous phase of the project, the department has been again awarded the DRS-II level w. e. f. April 2015 to March 2020.

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.

OBJECTIVE OF THE WORKSHOP

The subject of cryptology (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, Faculties, 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.

TRAVELLING ALLOWANCE AND ACCOMMODATION

Local hospitality including stay and meal; and AC-III train fare of participants will be provided by the CRSI and HP University.

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
- Dr. P. K. Saxena, Former Director, DRDO, Delhi
- Prof. R. K. Sharma, IIT Delhi.
- Prof. R. C. Mittal, IIT Roorkee.
- Dr. Debdeep Mukhopadhyay - IIT Kharagpur
- Dr. Nitin Saxena, IIT Kanpur
- Dr. Indivar Gupta, DRDO Delhi.
- Dr. M. Prem Laxman, SETS, Chennai
- Dr. Sahadeo Padhye, MNNIT Allahabad.
- Dr. Vishal Saraswat, C.R. Rao AIMSCS, Hyderabad
- Dr. Rajeev Anand Sahu, C.R.Rao AIMSES Hyderabad.

TOPICS TO BE COVERED

The following are some of the main topics:

- Overview of Cryptology
- Mathematics for Cryptology
- Classical Cryptosystems
- Modern Block Ciphers and Stream Ciphers
- Public Key Cryptosystems.
- Hash Functions and Digital Signature
- Elliptic Curve Cryptography
- Pairing Based Cryptography
- Lattice-Based Cryptography
- Steganography, Speech Secrecy
- Quantum and Post-Quantum Cryptography
- ID-Based Cryptography, Visual Cryptography
- Implementation of some Cryptosystems
- Hardware Security
- Network and Internet Security Overview
- Anonymous Signature.

REGISTRATION FEE

Industry Executive/Officer/Faculty: Rs. 2000/-

Student / Research scholar: Rs. 1000/-

(Registration fee is waived for CRSI members)

Registration fee may be paid through DD/NEFT payable at State Bank of India, Summer Hill, Shimla, drawn in favour of NIWC-2015 or can be deposited in the following bank account only after **notification of the confirmed participants list.**

Bank Name : State Bank of India

Branch Name : Summer Hill, Shimla

Name of the Account Holder: Organizing Secretary (NIWC-2015)

Account No.: 34800062261

IFSC Code: SBIN002490

MICR Code: 171002004

IMPORTANT DATES

Last date for receipt of application: 7-04-2015

Notification of Accepted Participants: 09-04-2015

Last Date of Confirmation/Registration: 14-04-2015

ADVISORY COMMITTEE

- Prof. A. D. N. Bajpai, Vice Chancellor, Himachal Pradesh University, Shimla.
- Prof. Bimal Roy, Director, ISI Kolkata & General Secretary of CRSI
- Prof. R. Balasubramanian, Chairman, NBHM; Director, IMSc Chennai & President of CRSI
- Dr. P. K. Saxena, Former Director, SAG, DRDO, New Delhi
- Prof. R. K. Sharma, IIT Delhi
- Prof. Subhamoy Maitra, ISI Kolkata
- Prof. B. K. Dass, Delhi University, Delhi
- Prof. U. C. Gupta, IIT Kharagpur
- Prof. V. Vetrivel, IIT Madras
- Prof. R. C. Mittal, IIT Roorkee
- Prof. M. S. Chauhan, Dean, Faculty of Physical Sciences, H.P.U., Shimla
- Prof. M. G. Gorla, H.P.U., Shimla
- Prof. Joginder Singh Dhiman, Chairman, Department of Mathematics, H. P. U., Shimla
- Prof. R. P. Sharma, H.P.U., Shimla
- Prof. Veena Sharma, H.P.U., Shimla

ORGANIZING COMMITTEE

- Prof. A. D. N. Bajpai, Vice Chancellor, H.P. University, Shimla: **Chief Patron**
- Prof. R. S. Chauhan, Pro Vice Chancellor, H. P. University, Shimla: **Patron**
- Prof. M. S. Chauhan : **Dean, Faculty of Physical Sciences**
- Prof. Joginder Singh Dhiman : **Chairman & Convener of the Workshop**
- Prof. P. L. Sharma : **Organizing Secretary**
- Prof. M. G. Gorla : **Member**
- Prof. R. P. Sharma : **Member**
- Prof. (Mrs.) Veena Sharma : **Member**
- Prof. Rajesh Sharma : **Member**
- Prof. Khem Chand : **Member**
- Dr. Jyoti Prakash : **Member**

STUDENT WORKING COMMITTEE

- Mrs. Mansi Rehan
- Mr. Sada Ram
- Ms. Shabnam Sharma
- Mr. Ravinder Kumar
- Ms. Neetu Dhiman
- Mrs. Kiran Devi
- Mr. Sanjeev Kumar
- Mrs. Nivedita Sharma
- Ms. Shaloo Devi
- Ms. Bharti
- Ms. Minakshi
- Ms. Asha Singh
- Mrs. Reena
- Mrs. Purnima
- Mr. Arun Kumar
- Ms. Priyanka

Department of Mathematics & Statistics,
Himachal Pradesh University, Shimla-5

National Instructional Workshop on Cryptology (NIWC-2015) (18-22 May, 2015)

REGISTRATION FORM

Please fill and send this Registration Form before
7th April, 2015

Name

Designation.....

Department.....

Area of Interest and Specialization

Institute / Organisation

CRSI Member (Yes / No).....

Membership No.....

Address

Contact (Phone / Mobile).....

E-mail.....

Model of Travel (Air / Train / Bus).....

Accommodation required (Yes / No)

Accompanying person (on payment basis, if any, with name(s) and relationship

.....

.....

Signature of Participant

Signature of Head
of Department /
Institute

Note: (1) Please send your CV through email along with the scanned copy of the registration form. (2) DD/NEFT in favor of NIWC-2015, H. P. University, Shimla payable at State Bank of India, Summer Hill, Shimla should be sent only after notification of confirmed participants to:

Prof. P. L. Sharma

Organizing Secretary, NIWC-2015
Department of Mathematics & Statistics
Himachal Pradesh University, Shimla-171005
Email: plsharma1964@gmail.com
Contact- +91-9418003066