

Report on National Workshop on Cryptography (NWC-2015)
Conducted by
Department of Mathematics
The LNM Institute of Information Technology
Deemed University, Jaipur-302031, India

The Department of Mathematics, The LNM Institute of Information Technology, Jaipur, organized a *National Workshop on Cryptography (NWC-2015)* during **December 14-20, 2015**.

The workshop was co-sponsored by NBHM, IBM and LNMIIT. All Speakers in the Workshop were from eminent Institutes of India such as IIT Kharagpur, IIT Roorkee, ISI Kolkata, DRDO and IIIT Delhi. Participants attended the workshop are from across the India.

Conveners: Dr. Manish Garg, Dr. Vikas Gupta, Dr. Dheerendra Mishra.

The workshop started with a welcome address by Dr. Manish Garg. He briefly introduced the theme of the workshop, mission, vision and activities of NWC-2015. Prof S. S. Gokhale, Director, LNMIIT Jaipur, emphasized on the key attributes of the workshop. Dr. P. K. Saxena, Former Director, SAG DRDO and Chief Guest of the Workshop discussed the role of cryptography in secure communication and stressed on the ongoing research on various topics connected with security.

First two days of the workshop: Dr. Shanta Laisaram from ISI Delhi and Dr. Sourav Sen Gupta from ISI Kolkata taught the Basics of Number Theory and Finite Field respectively. Dr. Sourav Sen Gupta also took Lab session of 3 hours on SageMath Software, which is a free open-source mathematics software system licensed under the GPL.

Third day of the workshop: Third day was the excursion. Participated visited to some historical places of Jaipur like Amer Fort, City place, Hawa Mahal and Jantar Mantar and enjoy a lot.

Fourth and Fifth day of the workshop: Dr. Ratna Dutta from IIT Kharagpur and Dr. Somitra Sanadhya from IIIT Delhi have delivered the lectures on the 3rd and 4th day of the workshop. Dr. Ratna Dutta has delivered the lectures on Public Key Cryptography (PKC) and elliptic curve cryptography(ECC). She discussed PKC in details also discussed different issues related to PKC. Dr. Somitra Sanadhya delivered the lectures on Hash Function, Secret Sharing and Entropy and Symmetric Key Cryptography.

Last Two days of the workshop: Prof Subhmoy Maitra, ISI Kolkata gave the nice lectures on Quantum and post quantum Cryptography. He also discussed the future scope of research in this area. Dr. Manisg Garg, LNMIIT Jaipur delivered a talk on basic of Cryptographic Boolean functions. Dr. Sugata Gangopadhyay from IIT Roorkee discussed the Linear Feed Back Shift Register and advanced research on Cryptographic Boolean Functions. Dr. Dheerendra Mishra, LNMIIT delivered a talk on authentication and key agreement protocol.

At the closing ceremony of the workshop Dr. Ajit Patel told about the department of Mathematics also about the over upcoming M.Sc Program. At last Dr. Dheerendra Mishra has encapsulated the outcome of the workshop and concluded the workshop with a vote of thanks.

