

Programme Schedule
(NIWC-2018, June 06-10, 2018)

June 06, 2018 (Day-1)

8.30 – 9.30 A.M.
9.30 – 10.00 A.M.
11:00-11:30 A.M.

Registration (Venue: LH2, SMS Building)*
Inauguration
Tea Break

Tea Break 11.30 – 11.45 A.M., **LUNCH**- 01.00 – 3.00 P.M., **Tea Break** 4.15 – 4.30 P.M.

Lightning talk by interested participants: 5 : 15- 5 : 45 PM

Session	Lectures	Time	Topic/Speaker
Session – 1	Lecture 1	10:00 – 11:00 A.M	Some important issues in current day Cryptology Prof. Bimal K Roy, ISI Kolkata
	Lecture 2	11.30– 12.45 PM	Block Cipher Design: DES & AES Prof. Debdeep Mukhopadhyay, IIT Kharagpur
Session – 2	Lecture 3	3.00 –4.00 P.M.	Block Cipher Cryptanalysis: Linear & Differential Cryptanalysis Prof. Debdeep Mukhopadhyay, IIT Kharagpur
	Lecture 4	4.15 – 5.15 P.M.	Lattice Based Signature Dr. Vishal Saraswat, IIT Jammu
June 07, 2014 (Day-2)			
Session – 1	Lecture 1	9.30 – 10.30 A.M.	Code Based Cryptography Dr. Vishal Saraswat, IIT Jammu
	Lecture 2	10.30 – 11.30 A.M.	Mathematical Foundation Prof. Shiv Datt Kumar , MNNIT Allahabad
	Lecture 3	11:45 - 12.45 PM	Stream Cipher Dr. Sartaj UI Hasan, IIT Jammu
Session – 2	Lecture 4	03.00 –4.00 P.M.	Public key Cryptography Dr. Amit Awasthi, Goutam Buddha University, Greater Noida
	Lecture 5	4.15 – 5.15 P.M.	Cryptographic Hash Function Dr. Sahadeo Padhye, MNNIT Allahabad
June 08, 2014 (Day-3)			
Session – 1	Lecture 1	9.30 – 10.30 A.M.	Digital Signatures Ms. Swati Rawal, MNNIT Allahabad
	Lecture 2	10.30 – 11.30 A.M.	Elliptic curves and cryptology Prof. R Balasubramanian, IIT Bombay
	Lecture 3	11:45 - 12.45 PM	Secure Multi-party Computation Dr. Ashish Choudhury, IIIT Banglaore
Session – 2	Lecture 4	03.00 –4.00 P.M.	Block Chain and Crypto Currency Dr. Ashish Choudhury, IIIT Banglaore
	Lecture 5	4.15 – 5.15 P.M.	Primality Testing & Prime Number Generation Dr. Nitin Saxena, IIT Kanpur
June 09, 2014 (Day-4)			
Session – 1	Lecture 1	9.30 – 10.30 A.M.	Network Security using Cryptography Dr Shashank Srivastava, MNNIT Allahabad
	Lecture 2	10.30 – 11.30 A.M.	Advancement of Number Field Sieve Algorithm and its Effect on Pairing Based Cryptography Dr. Shashank Singh, IIT Kanpur
	Lecture 3	11:45 - 12.45 PM	Practical Cryptography Dr. N Rajesh Pillai, SAG DRDO, New Delhi
Session – 2	Lecture 4	03.00 –4.00 P.M.	Role of Cryptography in Cyber Crime S.K. Vishwakarma, Sr. Cyber Security Analyst, IBM India PVT LTD – Bangalore
	Lecture 5	4.15 – 5.15 P.M.	Introduction to Quantum and Post-Quantum Cryptography Dr. Dhananjay Dey, SAG DRDO, New Delhi
June 10, 2014 (Day-5)			
Session – 1	Lecture 1	9.30 – 10.30 A.M.	NTRU Cryptosystem Ms. Sonika Singh, MNNIT Allahabad
	Lecture 2	10.30 – 11.30 A.M.	Group Based Cryptography Prof Ramji Lal
	Lecture 3	11:45 - 12.45 PM	Integer factorization using GNFS Prof. Kalyan Chakraborty, HRI Allahabad
Velidictory Function		12.45 P.M.-1.00	

* Note: Venue of the Workshop is LH2, School of Management Studies (SMS) building, MNNIT Allahabad.