

Tutorial Workshop in Cryptology

March 10–11, 2012

Seminar Hall, Chennai Mathematical Institute

Chennai Mathematical Institute (CMI), in association with Centre of Excellence in Cryptology (CoEC), Indian Statistical Institute (ISI), will host a two-day tutorial workshop on cryptology at CMI on March 10 and 11, 2012. The lectures at the workshop will be aimed at the BSc and MSc students at CMI and MStat students at ISI Chennai. No prior background in cryptology is assumed or required.

Schedule of the Workshop

Saturday, 10 March 2012 [Day 1]	
10:00 – 11:00	Introduction to Basics of Cryptology and Block Ciphers - Prof. R.L. Karandikar (CMI)
11:00 – 13:00	Introduction to Public Key Cryptosystems - Mr. S. Sen Gupta (CoEC, ISI)
13:00 – 14:00	Lunch
14:00 – 15:00	Cryptology and its National Perspective - Dr. P.K. Saxena (SAG, DRDO)
15:00 – 17:00	Advances in Public Key Cryptography - Prof. R. Balasubhramanian (IMSc)

Sunday, 11 March 2012 [Day 2]	
10:00 – 11:00	Introduction to Cryptology from a Security Perspective - Dr. S. Burman (CAIR, DRDO)
11:00 – 13:00	Introduction to Stream Ciphers - Prof. S. Maitra (ISI Kolkata)
13:00 – 14:00	Lunch
14:00 – 16:00	Introduction to Provable Security - Prof. C. Pandurangan (ISI Chennai)

Logistics

The participants will be provided lunch and transportation arrangements for ISI/IMSc students will be made. Interested students/faculty at ISI/CMI/IMSc/IIT should register by March 2, 2012, by filling out the form at the following website: <http://www.cmi.ac.in/~spsuresh/crypto>.