Online Short Term Course on "Mathematics of Cryptography"

17-21 August, 2020
Centre for Continuing Education (CCE)
Indian Institute of Science, Bangalore, India - 560012

Overview of the short course:

Cryptography is a method of protecting information, especially during communication of information, by encrypting it using codes. Modern digital society cannot function without codes and encryptions. Internet banking, emails, mobile phones need highly secure encryptions.

The course will give an introduction to cryptography with an emphasis on the mathematics used for it. After introducing some classical cryptosystems we will develop the mathematical tools needed for their construction and security analysis. The mathematical topics will include elementary combinatorics, modular arithmetic and prime numbers. Cryptographic constructions will include Deffie-Hellman key exchange, discrete logarithm based cryptosystems, RSA cryptosystems and DES type algorithm.

Suggested books are:

- Introduction to cryptography with coding theory by Wade Trappe and Lawrence Washington.
- An Introduction to mathematical cryptography by Jeffery Hoffstein, Jill Pipher, Joe Silverman.

Minimum Qualification Required:

Bachelors degree in mathematics, Computer Science or Engineering

Prerequisites:

Background in elementary number theory, linear algebra and abstract algebra. Familiarity with computer programming is desirable

Course Coordinators:

- Prof. Mahesh Kakde, Department of Mathematics, Indian Institute of Science, Bangalore - 560012
  email: maheshkakde@iisc.ac.in

Registration: This course can be attended only by registration. The number of participants is limited to 50. The registration will be accepted on a first-come first-served basis.

Apply online at: http://cce.iisc.ac.in/ssp-stc.html

The registration fee is INR 10,000 +18% GST **Last Date to Apply: 15 July 2020**