



Information and Announcements

Refresher Course in Mathematics – Cryptology

May 2 – 14, 2005

at Cochin University of Science and Technology, Cochin 682 022

sponsored by Indian Academy of Sciences, Bangalore 560 012

Applications are invited from University/College teachers, Research Fellows and BTech/MSc (Mathematics) degree holders for participation in the Refresher Course on Cryptology to be held at Department of Mathematics, Cochin University of Science and Technology, Cochin. About 40 persons will be selected to attend.

Outline of the Course: Some topics in elementary number theory, congruences, finite fields, quadratic residues, some simple cryptosystems, enciphering matrices, PKC, RSA, discrete log, pseudo primes, the rho method, elliptic curve crypto systems, discussion based on "A course in Number Theory and Cryptography" by N Koblitz, Springer II Ed. (1994).

Classical encryption techniques, block ciphers and DES, AES, confidentiality using symmetric encryption, message authentication and hash functions, digital signatures, discussion based on 'Cryptography and network security', W Stallings, PHI, III Ed. (2004).

Recent trends in cryptology research.

There will be formal lectures, general talks, problem sessions and discussions.

Pre-requisites: Knowledge of elementary number theory and first course in algebra.

Selected participants will be provided local hospitality and round trip train fare (first class or three-tier A/C) to and fro by the shortest route between their place of stay and Cochin.

Those who wish to participate may send by email, their brief curriculum vitae containing name, date of birth, postal and e-mail address, qualifications, teaching experience, courses taught, positions held, and a brief write up on your academic activities etc.. Research Fellows who wish to participate should also submit a letter of recommendation from their supervisors.

Dr Ambat Vijayakumar, Coordinator, Refresher course in Cryptology, Department of Mathematics, CUSAT, Cochin 682022, Email: vijay@cusat.ac.in, ambatvijay@rediffmail.com

Last date for receipt of applications: 31 March 2005.

