REFRESHER COURSE IN MATHEMATICS

(Coding Theory, Cryptography and Discrete Mathematics)

2–14 December 2002

sponsored by

INDIAN ACADEMY OF SCIENCES, BANGALORE

organized by

PANJAB UNIVERSITY, CHANDIGARH

at

Department of Mathematics, Panjab University, Chandigarh 160 014

Applications are invited from University/College teachers and Research Fellows for participation in the Refresher Course on Coding Theory, Cryptography and Discrete Mathematics to be held at Department of Mathematics, Panjab University, Chandigarh from 2 to 14 December 2002. About 30 persons will be selected to attend.

Outline of the Course:

1. Error-correcting codes, linear codes, generator matrix, parity check matrix, dual codes, syndrome decoding, Hamming codes, perfect codes, BCH codes, cyclic codes, idempotents of cyclic codes, quadratic residue codes, Golay codes.
2. Simple cryptosystems, block ciphers, enciphering matrices, elementary cryptoanalysis, public key cryptography, RSA, discrete log and knapsack cryptosystems, primality testing and factoring, introduction to elliptic curve cryptography.
3. Pigeon-hole principle, basic counting arguments, inclusion–exclusion principle, recurrence relations, generating functions, elementary graph theory, Eulerian paths and cycles, trees, planar graphs, chromatic number.

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 Chandigarh.

Those who wish to participate may send their brief curriculum vitae containing name, date of birth, postal and e-mail address, qualifications, teaching experience, courses taught, positions held, etc. to:

Professor Madhu Raka
Convener, Organizing Committee
Refresher Course in Mathematics
Centre for Advanced Study in Mathematics
Panjab University
Chandigarh 160 014

Research Fellows who wish to participate should also submit a letter of recommendation from their supervisors.

Last date for receipt of applications: 7 September 2002.