Workshop on

Number Theory and Cryptography

IISc Mathematics Initiative

Department of Mathematics, Indian Institute of Science, Bangalore

January 23 - February 11, 2006

Venue : Lecture Hall I, Department of Mathematics

23.01.2006 Monday **8.30 - 9.30 : Registration**

	9.30 - 11.00	11.00 - 11.30	11.30 - 13.00	13.00 - 14.30	14.30 - 16.00	16.00 - 16.30	16.30 - 17.30
23.01.2006 Monday	**C. R. Pradeep** Rings and Fields	Tea	**Dilip P. Patil** Field extensions	Lunch	**C. E. Veni Madhavan** Symmetric and Public Key Cryptography	Tea	Open discussion
24.01.2006 Tuesday	**C. R. Pradeep** Euclidean domains and PIDs	Tea	**Dilip P. Patil** Splitting fields	Lunch	**C. E. Veni Madhavan** Computational Complexity	Tea	Open discussion
25.01.2006 Wednesday	**C. R. Pradeep** Factorization in Rings	Tea	**Dilip P. Patil** Automorphisms	Lunch	**Kumara Swamy** Public Key Primitives and Algorithms-1	Tea	Open discussion
26.01.2006 Thursday	**C. R. Pradeep** Polynomial Rings	Tea	**Dilip P. Patil** Normal Extensions	Lunch	**Kumara Swamy** Public Key Primitives and Algorithms-2	Tea	Open discussion
27.01.2006 Friday	**C. R. Pradeep** Noetherian Rings	Tea	**Dilip P. Patil** Separable Extensions	Lunch	**Kumara Swamy** Public Key Primitives and Algorithms-3	Tea	Open discussion
28.01.2006 Saturday	**C. R. Pradeep** Integral Extensions	Tea	**Dilip P. Patil** Galois Extensions	Lunch	-	-	-
30.01.2006 Monday	**C. R. Pradeep** Algebraic Integers	Tea	**Dilip P. Patil** Galois Theory	Lunch	**Gagan Garg** Public Key Cryptosystems-1	Tea	Open discussion
31.01.2006 Tuesday	**C. R. Pradeep** Norm, Trace, Bases	Tea	**Dilip P. Patil** Dedikind Domains	Lunch	**Gagan Garg** Public Key Cryptosystems-2	Tea	Open discussion
01.02.2006 Wednesday	**C. S. Yogananda / R. Thangadurai** Number Field Sieve-1	Tea	**C. S. Yogananda / R. Thangadurai** Number Field Sieve-2	Lunch	**Gagan Garg** Quadratic Sieve	Tea	Open discussion
02.02.2006 Thursday	**C. S. Yogananda / R. Thangadurai** Number Field Sieve-3	Tea	**C. S. Yogananda / R. Thangadurai** Number Field Sieve-4	Lunch	**Gagan Garg** Number Field Sieve Factoring	Tea	Open discussion

	9.30 - 11.00	11.00 - 11.30	11.30 - 13.00	13.00 - 14.30	14.30 - 16.00	16.00 - 16.30	16.30 - 17.30
03.02.2006 Friday	**Dilip P. Patil** Class Group	Tea	**Dilip P. Patil** Minkowski Theory	Lunch	**C. E. Veni Madhavan** Number Field sleve Factoring	Tea	Open discussion
04.02.2006 Saturday	**Dilip P. Patil** Finiteness of Class Number	Tea	**Dilip P. Patil** Dirichlet Unit theorem	Lunch	-	-	-
06.02.2006 Monday	**C. S. Yogananda / R. Thangadurai** Number Field Sieve-5	Tea	**C. S. Yogananda / R. Thangadurai** Number Field Sieve-6	Lunch	**Kumara Swamy** Index Calculus heuristics for Discrete Log	Tea	Open discussion
07.02.2006 Tuesday	**Dipendra Prasad** Elliptic Curve for Factorization-1	Tea	**B. Sury** Algorithms in Number Theory -1	Lunch	**Kumara Swamy** Elliptic Curve Group Law and Algorithms	Tea	Open discussion
08.02.2006 Wednesday	**Dipendra Prasad** Elliptic Curve for Factorization-2	Tea	**B. Sury** Algorithms in Number Theory -2	Lunch	**Rana Barua** Pairing based Cryptography-1	Tea	Open discussion
09.02.2006 Thursday	**Dipendra Prasad** Elliptic Curve for Factorization-3	Tea	**B. Sury** Algorithms in Number Theory -3	Lunch	**Rana Barua** Pairing based Cryptography-2	Tea	**Andreas Enge** Algorithmic Advances in Algebraic Curve Crptology
10.02.2006 Friday	**Dipendra Prasad** Elliptic Curve for Factorization-4		**B. Sury** Algorithms in Number Theory -4	Lunch	**Rana Barua** Pairing based Computations	Tea	**Prabhakar Vaidya** Chaos and Cryptography
	9.30 - 10.30	**10.30 - 11.00**	**11.00 - 12.00**	**12.00 - 12.15**	**12.15 - 1.15**	**1.15 - 14.30**	
11.02.2006 Saturday	**J. Pasupathy** Quantum Cryptography	Tea	**K. Ramachandra** Primes between n and $2n$	Break	**R. Balasubramanian** Smooth Numbers	Lunch	-

Contact Address

The Secretariat
IISc Mathematics Initiative (IMI)
Department of Mathematics
Indian Institute of Science
Bangalore - 560 012
Phone : +91-80-22933217, 22933218, 23605390
Fax: +91-80-23605390, 23600146
E-mail: imi@math.iisc.ernet.in

C. R. Pradeep, Convener (IISc, Bangalore)
C. E. Veni Madhavan (IISc, Bangalore)