Centre for Mathematical sciences (CMS)
Apaji Institute of Mathematics & Applied Computer Technology
Banasthali University
Banasthali 304022 (Rajasthan)

National Workshop

On

CRYPTOGRAPHY and NUMBER THEORY

May 03-06, 2012

Sponsored

by

Department of Science & Technology

Government of India, New Delhi

ADVISORY COMMITTEE

Prof. Aditya Shastri
Vice Chancellor, Banasthali University

Prof. B. K. Dass
Delhi University, New Delhi

CONVENOR
Prof. G. N. Purohit

COORDINATORS
Prof. Sarla Pareek and Dr. Deepa Sinha

ORGANIZING SECRETARIES
Mr. Prashant Kushwah and Mr. Pravin Garg

ORGANIZING COMMITTEE
Mrs. Amla Olkha, Mr. Piyush Kant Rai, Dr. Gauree Shanker, Ms. Nidhi Khandelwal, Ms. Mansi Khurana, Dr. Praveen Kumar Gupta

PROGRAM COMMITTEE
Dr. Narendra Thakur, Mrs. Swati Raj, Ms. Jyoti Sharma, Dr. Madhulika Kedawat, Ms. Kalpna, Ms. Geetanjali Sharma, Ms. Usha Sharma, Ms. Preeti Jain, Ms. Isha Sangal, Ms. Shinu, Ms. Ritu, Ms. Gargi, Ms. Firdos, Mrs. Nirupama

About the Workshop

At the present time, there is strong pressure to make academic studies more relevant. Number Theory provides generous evidence that topics pursued for their own intrinsic interest can later find significant applications. As the field of cryptography expands to include new concepts and techniques, the cryptographic applications of number theory have also broadened. In addition to elementary and analytic number theory, increasing use has been made of algebraic number theory (primality testing with Gauss and Jacobi sums, cryptosystems based on quadratic fields, the number field sieve) and arithmetic algebraic geometry (elliptic curve factorization, cryptosystems based on elliptic and hyperelliptic curves). A wide variety of applications of cryptography exist such as secure email, e-commerce and smart cards. The Workshop is intended for young faculty and researchers from Mathematical sciences and Computer Science who are interested in the field from in and out Banasthali. The participants are required to be familiar with basic concept of number theory and cryptography.

Eminent speakers in the field of who were resource persons:

1. Prof. S. A. Katre, University of Pune
2. Prof. R. Tandon, University of Hyderabad
3. Prof. R. K. Shyamasundar, TIFR, Mumbai
4. Prof. R. K. Sharma, IIT Delhi
5. Prof. Bhu Dev Sharma, JIIT, Noida
6. Prof. G. N. Purohit, Banasthali University

Participants: Participation was invited from all over the country by sending invitation to the Heads of the Departments of Mathematics/Statistics/Computer Science various Institutes/ Universities and Research Organizations and also announcing the workshop at the website of Banasthali University www.banasthali.org. More than hundred and twenty candidates from all over India applied for participation in the workshop. The advisory committee scrutinized the applications received and finally thirty-five candidates from these applications were short-listed and invited based on the relevance of the area of specialization with their research interest. Besides these participants, faculty members and students from Banasthali Vidyapith also participated.

Programme: The programme comprised of Lecture sessions in addition to Inaugural and Valedictory session. The detailed Program Schedule was as follows:

Centre for Mathematical Sciences (CMS)
Apaji Institute of Mathematics & Applied Computer Technology
Banasthali University
PROGRAM SCHEDULE

National Workshop on Cryptography and Number Theory

(May 03-06, 2012)

Sessions Date	**09:00 AM to 11.00AM**	**10.45 AM to 11:15AM**	**11.15 AM to 12:15 PM**	**12.15 PM to 01:15 PM**	**01.15 PM to 02.45 PM**	**02.45 PM to 3.45 PM**	**03.45PM to 04.00 PM**	**04.00 PM to 05.00 PM**
May 3, 2012	Registration (**09:00 AM to 10:00 AM**) Inaugural Session (**10:00 AM to 10:45 AM**)	High Tea	SAK	RT	Lunch	RKSS	Tea	RT

Sessions Date	**10:00 AM to 11.00 AM**	**11.00 AM to 11:15 AM**	**11.15 AM to 12:15 PM**	**12. 15 PM to 1.15 PM**	**1.15 PM to 02.45 PM**	**02.45 PM to 03.45 PM**	**03.45 PM to 04.00 PM**	**04.00 PM to 05.00 PM**
May 4, 2012	RKSS	Tea	SAK	RKSS	Lunch	RT	Tea	SAK
May 5, 2012	SAK	Tea	BDS	GNP	Lunch	RKS	Tea	GNP
May 6, 2012	RKS	Tea	BDS	RKS	Validictory followed by Lunch			

Prof. S. A. Katre (SAK):	An introductory lecture on RSA Cryptography Waring's problem for matrices (i.e. writing matrices as sums of k-th powers) The zeta function of a projective curve. The cyclotomic polynomial and factorization of x^n-1
Prof. Rajat Tandon (RT):	Elliptic Curve Cryptology and factorization via elliptic curves
Prof. R. K. Shyamasundar (RKSS):	Combating Malware: Issue and Challenges Detection of Malware: A behavioral Approach Characterization of Metamorphic Virus as a regular expression De-centralized Information Flow Control: A strategy for protection
Prof. R. K. Sharma (RKS):	Group ring cryptography Algebraic aspect of Cryptography
Prof. G. N. Purohit (GNP):	Introduction to cryptography Post quantum cryptography
Prof. Bhu Dev Sharma (BDS):	From sufficiently advanced angle on Coding Theory: some open problems Some aspects of Number Theory

Venue for lectures: NLT, AIM & ACT

Report of the Program

The inaugural ceremony commenced with the lighting of the lamp by a group of dignified persons- Prof. S.A. Katre (University of Pune), Prof. Rajat Tandon (University of Hyderabad), Prof. G.N. Purohit (Dean, AIM &ACT, Banasthali University), Prof. Sarla Pareek (Head, Department of Mathematics and Statistics, Banasthali University) and Dr. Deepa Sinha, coordinator of the program. The programme was followed by Saraswati-Vandana.

Prof. Sarla Pareek formally welcomed the dignitaries on the dais and participants from various parts of the country, colleagues & students. She made the audience aware about the origin and significance of CMS and mentioned its achievements in terms of doctoral research. She wished for the comfortable and productive stay of the participants.

Prof. G.N. Purohit formally introduced both the dignitaries on the dais to the participants. Then he explained the topics of the workshop "Cryptography" and "Number Theory". He gave the brief development of cryptography and explained the new era of cryptography "Post Quantum Cryptography". He also encouraged everyone to take active participation and get benefited by the expert lectures to generate new ideas for future research.

Prof. Katre thanked the organizers of the workshop for the invitation and said that University has many facilities and was impressed by the research activities going on in CMS and felt very elated to know the way Mathematics is being promoted in the department. He appreciated that the Department of Mathematics & Statistics is working to create an interest in mathematics at the School level and Under Graduate level students by organizing in-house training program and MTTS program. He suggested organizing ATM schools in the University. He also told to the participants about various advance research programs.

Prof. Tandon told about the Cryptography. He said, nowadays cryptography has become a fascinating research topic and to develop a cryptographic protocol, one has the need of sophisticated knowledge of mathematics. He added it that to do application of various branches of mathematics in cryptography is not easy.

In the end, Dr. Deepa Sinha offered a vote of thanks to all including Prof. Aditya Shastri, Director CMS and Vice Chancellor, Banasthali University in absentia for his constant support and motivation. She thanked all the dignitaries for gracing the occasion by their solemn presence and all the participants of the workshop who are the main ingredient of this workshop. She also thanked DST for providing financial assistance to conduct such workshops in the centre.

The workshop went for four days and participants were benefited by the lectures of the eminent professors from across the country.

Prof. S. A. Katre delivered four lectures on 3-5 May 2012. In his first lecture he gave the talk on the RSA crytography, which is used in online purchases, banking, smart cards and

similar gadgets. He discussed some classical cryptosystems like Caeser's cipher and permutation ciphers, and showed that they can be broken using frequency analysis. He also explained the method of calculating powers in modulo system. In contrast to the first lecture his second lecture pertained to number theory, in which, he introduced the Waring's problem for matrices and showed the journey of this research problem from the beginning to its current state. In his third lecture, he explained the zeta function of a projective curve. He started with cyclotomic numbers for finite field and showed that the zeta functions of certain algebraic curves become simple in the case of uniform cyclotomy. In this case the formulae for the number of points on certain curves and surfaces over finite fields become extremely simple. He also told that in certain cases the density of primes satisfying the condition of uniform cycltomy is high, so these calculations are expected to be very helpful in applications to cryptography. One important thing about this lecture was he related his results with the Prof. R. Tandon lectures very beautifully. In his fourth and last lecture, Prof Katre gave an interesting method for the factorization of cyclotomic polynomial x^n-1. He also mentioned the importance of pattern recognition to prove a number theoretic result. He concluded his lecture with the brief introduction to coding theory.

Prof. Rajat Tandon delivered three lectures on 3-4 May 2012. On 3rd May, he took two lectures. His lectures are on elliptic curves and its application to cryptography. He started with the introduction of elliptic curves and showed how we can define a group of points on elliptic curve. He discussed how to add two points on an elliptic curve. He proved the associativity property in the Elliptic curve group using Bezout's theorem. He continued results on elliptic curves in his second lecture. He discussed how to find the number of points on an elliptic curve over the finite field. He also explained the Messey-Omura Cryptosystem based on elliptic curves. In his third lecture, He explained how to embed a message unit to a point of elliptic curves.

Prof. R. K. Shyamasudar gave three lectures on 3-4 May 2012. His lectures were oriented to computer security. In his first lecture, he spoke on malware. He told why there is an acute need for detecting and controlling the spread of malware. He discussed various types of malware: viruses, worm, adware, spyware, trojon horses and others. He gave an example of virus. He also showed the comparison of biological viruses and computer viruses. After that, he discussed metamorphic viruses which rewrite themselves and polymorphic virus which infects files with an encrypted copy of itself. In his second lecture, He discussed about code obfuscation and how we can detect and analyze obfuscation. He explained various threats due to SQL injection, obfuscation, PDF exploitation. He briefly discussed about cyber war and SCADA attacks. He also told India got rank second in spam industry by Geographic distributor of spam senders-2010. Third lecture of Prof. Shyamasundar was related to application of cryptography to data security. He mainly talked about access control.

Prof. G. N. Purohit's first lectures on 4th May 2012 were on the basics of cryptography. He briefly explained three types of cryptography: symmetric key cryptography, asymmetric key cryptography and hash function. He told that the search for public key cryptosystems has gone into many different directions and there are many important classes of cryptographic systems beyond RSA and DSA i.e. hash based cryptography, code based cryptography and lattice based cryptography, multivariate-quadratic equation cryptography. In his second lecture he raised the issue about cryptography when the quantum computers are available. He

told that the quantum computer will destroy the RSA, DSA and El-Gamal but there are other important classes of cryptography beyond these. Then he discussed about post quantum cryptography.

Prof. R. K. Sharma delivered three lectures on 5-6 May 2012. He started his first lecture with explaining the importance of units in cryptography. He defined the group ring of a group over integers. He discussed how to find the units in a group ring by considering an example. In his second lecture, he discussed some open problems regarding Lie centrally metabelian ring. His results were more related to algebraic aspects of cryptography. The third lecture of Prof. R. K. Sharma contained some public key cryptosystems based on group structure for example Deffie-Hellman key exchange, RSA encryption scheme, El-Gamal encryption scheme. He also showed that how to convert these cryptosystems on group ring structure.

Prof. Bhu Dev Sharma delivered two lectures on 5-6 May 2012. In his first lecture, He talked about the evolution of the coding theory and briefly outline the basic concepts of coding theory. He explained Hamming distance, Hamming weight, length of the code; generator matrices and parity check matrices which are the tools in construction and study of error correcting codes. In the second lecture, he discussed about product codes and duality property. He also discussed his paper "Partitioned Product of Matrices and Construction of Efficient Product Codes".

At the end in the **Valedictory Session,** the coordinator, Dr. Deepa Sinha gave a brief of the proceedings and seminar statistics, the sessions and contribution of resource persons and the participants. Prof. G.N. Purohit expressed his satisfaction on the arrangements of the seminar and cooperation from the participants from outside instrumental in the success of the academic activity. He appreciated the fact that Banasthali University enthusiastically participates in research activities, necessary for the promotion of research in Mathematical Sciences. Few participants presented their views about the workshop on behalf of all, where they expressed that the quality of all the lectures was par excellence.

At last, Dr. Deepa Sinha on behalf of organizing committee thanked the University staff, DST and all other involved in the managing of the workshop.

Lecture notes: The soft copy of the lecture notes procured from experts has been provided to the participants.

Inclusion of a book in the folder: A book entitled **"Elementary Number Theory"** by ***David M. Burton*** published by Mc Graw Hill private limited, New Delhi, 2011 was also included in the folder.

Conclusion: The seminar, sponsored by DST, under CMS had very positive outcomes as follows:

It has given a chance to the faculty and students to interact with the distinguished experts from the field of Cryptography and Number Theory.

It established the fact that Centre for Mathematical Sciences, Banasthali University organizes activities for the promotion of research in Mathematical Sciences thereby providing a platform for the researchers. It introduced and exposed the participants to the range of support for various academic initiatives by DST.