Théorie Algébrique des nombres et applications notamment à la cryptographie

Ecole CIMPA-ICTP, Abidjan 2017

Dates : du 10 avril au samedi 22 avril 2017

Lieu : UFR MI - Université Félix Houphouët Boigny

Listes des intervenants

Cours:

Alain TOGBE "*Application of the elementary number theory to cryptography*".

This course will use the basics of the elementary number theory to introduce cryptography. So the theory of congruences will be gently used to introduce cryptography. From the Caesar cipher, we will present the public-key cryptography. We will also discuss the knapsack cryptosystem (which is based on the difficult classic problem in combinatorics known as the knapsack problem) and the discrete logarithm problem.

Francesco PAPPALARDI "Elementary approach to elliptic curves".

Examples of elliptic curves, drawing elliptic curves, the set of rational points of an elliptic curve, intersection between a line and an elliptic curve, the point at infinity of an elliptic curve, singular points, the group law, Weierstrass equations and their classification, elliptic curves over finite fields and their properties, the Hasse bound, the structure of the group of points over finite fields.

François TANOE « *Décomposition cyclotomiques sur les corps finis* ».

This course aims to provide the necessary tools for the study of error-correcting codes, including that of HAMMING. This course uses basic arithmetic (multiplicative functions, including Mobius' multiplicative inversion formulas); modular arithmetic, and the Galois's theory.for cyclic groups, Galois' extension on finite field will be essential to study the decomposition into irreducible factors polynomials over finite fields. Such construction's examples for finite fields of small order are given. The cyclotomic's decomposition for polynomials over finite fields are detailed and many numerical examples are given and too, the main fundamental theorems.

Christophe DELAUNAY T.D. PARI.

The main goal of this course is to give an introduction to the PARI/GP software which is number theoretic computational software. We will illustrate several notions given in the courses of this school (modular arithmetic, cyclotomic fields, elliptic curves, L-functions, ...) with an emphasize on the explicit and experimental point of views. We will insist on the cryptographic aspects and, in particular, we will explain how to build explicitly some classical crypto-systems.

Adriana SALERNO *Lattices and cryptography*.

- Review on vector spaces and lattices.
- The shortest vector problem and the closest vector problem.
- Babai's algorithm for finding "good" bases.
- Cryptosystems based on hard lattice problems: The GGH Public Key Cryptosystem, The NTRU Public Key Cryptosystem.

Possible additional topics:

- Lattice-based digital signature schemes.
- Lattice reduction algorithms.
- Fully homomorphic encryption.

Michel WALDSCHMIDT "*Application of the elementary number theory to cryptography*"

This course will introduce some of the main basic tools from number theory which are essential for the modern cryptographic systems. Starting with the arithmetic of rational integers, divisibility and congruencies will be explained in connection with algebra (group theory, especially cyclic groups; rings, ideals, quotients; fields). The finite fields with a number of elements which is a prime number occur naturally in this context; hoverer they do not suffice for advanced purposes, and the general theory of finite fields will be developed. Such a theory has a lot of deep applications, some of which will be outlined.

Conférences :

Colonel Lucien Blegban N'GUESSAN	« Les besoins actuels en cryptographie »
Kouadio KIMOU :	« Cryptographie et sécurité du signal et/ou de l'information »
Sylvain DUQUESNE :	« Calcul d'indice sur les corps finis et applications aux couplages pour la cryptographie »
Christophe DELAUNAY	« *Introduction à la Cryptographie* »
Kolo Fousseni SORO	« Tableaux de Young et Cryptographie »

Exposés étudiants

1) **Sézare Abé GNAGNE**	Décomposition des Fractions Egyptiennes et tests de primalité
2) O. I. BADO	Démonstration du théorème de Sophie Germain
3) S. T. ATAMEWOUE	Hyperstructures and applications to the theory of codes
4) H. A. MOUFEK	Les codes convolutionnels et applications à la cryptographie
5) P. S. SANON	New vector spaces
6) A. DOSSAVI-YOYO	L'extension du *D(±k)-triplet {k ∓1,k,4k ∓1}*
7) S. E. RIHANE	Les ensembles diophantiens et les nombres de Fibonacci
8) J. ODJOUMANI	Pell factoriangular numbers
9) A. MAIGA	Fast computation of norm on unramified extension of $\boldsymbol{Q}_p$
10) B. FAYE	Extracting a uniform random bit-string over Jacobian of hyperellipic curves of genus 2
11) I. JERRARI	On the 2-class field towers of some imaginary quartic number fields of type *(2,2,2)*