MA2825
Algebra and cryptology

Professor: Damien Vergnaud

Language of instruction: French – **Number of hours**: 36 – **ECTS**: 3

Prerequisites: None

Period: S8 Elective 11 March to June IN28IE4, SEP8IE4

Course Objectives

This theoretical course covers fundamental concepts and tools of commutative algebra, from the perspective of modern cryptology. Particularly, some elements of number theory are introduced (finite fields, law of quadratic reciprocity, elliptic curves).

Cryptography is a set of skills which provides security of information systems. This field, at the frontier of Mathematics, Computer Science and Electronics, enables confidentiality of data to be preserved, for their access control or for documents identification.

In addition to fundamental mathematical concepts, this course will introduce algorithmic tools required for applications. Basic notions of algebra will be presented and certain algebraic structures will be studed in detail, notably those useful for public key cryptology (rings Z/nZ, rings of polynomials, finite fields, ...). Notions of algorithmic number theory will also be presented, for applications in the field of cryptology.

On completion of the course, students should be able to

In addition to the basic elements of modern cryptology, this course will provide a solid culture in algebra and number theory. It is an important foundation cours for students hoping to follow an MSc in the field.

Course Contents

- Groups, rings, fields.
- Arithmetics. Law of quadratic reciprocity.
- Basic algebraic algorithms.
- Cryptosystems with public key. Primality tests.
- Rings of polynomial with one or several variables. Finite fields.
- Error correcting codes. Cyclic codes
- Elliptic curves on finite fields.

Course Organization

Course 22 hr, Tutorials 9.5 hr.

Teaching Material and Textbooks

Course reader and correction of exercises.

Evaluation

Mid-term written exam 1.5 hr (without any support) + Final written exam 3 hr (without any support)