UNIVERSITÀ
DEGLI STUDI DI MILANO-BICOCCA

SYLLABUS DEL CORSO

Teoria dei Numeri e Crittografia

2021-1-F4001Q073

Aims

In line with the educational objectives of the Degree in Mathematics, the course aims to provide the student with some of the fundamental concepts, methods and some techniques of Number theory, essential for understanding the main asymmetric Cryptographic systems based on modular arithmetic or on elliptic curves over finite fields.
The student is expected to have knowledge of main probabilistic and deterministic primality tests, of the structure of the group of elliptic curves over finite fields, with applications to the problems of discrete logarithm, of the digital signature, and of factorisation. It is also expected to have the ability to give proofs presented in the course, using given techniques to solve easy problems and the ability to study some more details of results presented during the course.

Contents

Some classical results in Number Theory are presented, with particular regard to factorizzation methods, primality tests and discrete logarithm , using modular arithmetic and Elliptic Curves.

Detailed program

- Integers and finite fields; Euler function; modular arithmetic

- Definition of a Cypher: public and private key
- Some topics about Prime numbers: Dirichlet's Theorem; Number Prime Theorem
- Prime numbers and factorization: pseudoprimes; primality tests (Fermat, Jacobj, Miller-Rabin AKS);

(p-1)-pollard method for factorization; complexity of the alghoritms.

- Some remark about Riemann's zeta function. Euler'sFactorization. Riemann's hypothesis. L(s,?) funcions and extended Riemann hypothesis; some consequence on primality tests.
- Diffie-Hellman cypher; discrete logarithm
- Elliptic curves; group of the points of an elliptic curve on a finite field (and rings).
- Endomorphisms.
- Torsion points and Weil pairing.
- Hasse Theorem
- Cryptosystems on elliptic curves.
- Discrete Logarithm on Elliptic Curves
- Digital Signature: DSA, ECDSA

Prerequisites

Basic Algebra: algebraic structure; abelian groups; finite fields.

Teaching form

The cours consists of Lectures for 8 credits. They will give knowledge of basic definitions, relevant results and theorems. On the other side, we intend to give skills to use results and knowledge in solving exercises and analysing problems

Because the evolution of Covid-19 health emergency, at the moment (A / A 2020/21) it is not possible to say if the lectures will be in presence; in any case the lectures of this course will be videotaped and will be available to students on the e-learning platform.

Textbook and teaching resource

- N. Koblitz, A course in Number Theory and Cryptography, volume 114 of Graduate texts in Mathematics, Springer-Verlag, second edition, 1994.
- A. Languasco, A. Zaccagnini, Introduzione alla Crittografia, Hoepli Editore, 2004.
- H.E. Rose, A course in Number Theory, II edizione, Oxford: Clarendon press, 1994
- Lawrence C. Washington, Elliptic Curves, Number Theory and Criptogtaphy CRCPress
- Maria Welleda Baldoni, Ciro Ciliberto, Giulia Maria Piacentini Cattaneo, Elementary Number Theory, Cryptography and Codes, 2009 Springer-Verlag Berlin Heidelberg

Semester

II term.

Assessment method

Pending the current health emergency, the oral exam will be held online through WebEx or analogous, with access made available on the e-learning website. The procedures for carrying out the written test will be established later on.

It will be possible to give oral and written exam not in presence, via webex or analogues platforms.

- Some exercises will be proposed in the lectures. If they will be uploaded on e-learning website (or sent by mail) they will be considered for the final valuation.
- The written part consists of exercises where the students show their ability in using methods and tools introduced in the course.
- The oral part consists of two parts:

- discussion about written part;
- the student may decide to have a classical oral exam, where he must show his competence about subjects considered in the lectures, also giving motivations for applications of theoretical topics; alternatively, one student may give a talk about a particular subject, which was considered not very deeply in the course. The final result is achieved considering the average between the mark obtained in written+discussion (together), and the mark obtained in the subsequent oral part.

Mark range: 18-30/30.

Office hours

By appointment. Due to the current health emergency, student reception will be carried out online through WebEx or analogous.