UNIVERSITÀ
DEGLI STUDI DI MILANO-BICOCCA

SYLLABUS DEL CORSO

Teoria dei Numeri e Crittografia

2627-1-F4002Q032

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, finite fields, and various tools from number theory.

Learning objectives and expected outcomes are as follows, formulated according to the five Dublin Descriptors:

Knowledge and understanding:
Students will acquire advanced knowledge in number theory, with emphasis on modular arithmetic, finite fields, probabilistic primality tests, and the mathematical foundations of public-key cryptographic systems. This knowledge will build upon a solid undergraduate background and will provide insight into the algebraic and arithmetic structures underlying modern cryptographic protocols.

Applying knowledge and understanding:
Students will be able to apply the learned techniques to critically analyze cryptographic algorithms based on number-theoretic problems (e.g., factorization, discrete logarithm), and to solve both theoretical and computational problems related to the topics covered in the course.

Making judgements:
Students will develop the ability to assess the mathematical soundness and security of cryptographic protocols, to interpret theoretical results and proofs independently, and to identify relevant hypotheses and methods for generalization.

Communication skills:
Students will be able to present theoretical concepts and techniques clearly and rigorously, both in written and oral form, using appropriate mathematical language suited to both scientific and applied contexts.

Learning skills:

Students will be capable of independently exploring related or more advanced topics, consulting the mathematical literature and understanding specialized texts and research articles in number nheory and cryptographic mathematics.

Contents

The course focuses on algebraic and number theoretic results that are of cryptographic interest, and their applications in cryptography. Special attention will be given to algorithmic aspects, and of computational complexity. Topics covered will include primality tests and factorization methods.

Detailed program

- Review of various topics on integers and modular arithmetic, with special attention to aspects of computational complexity.
- Introduction to cryptographic systems, both secret-key and public-key. Digital signatures.
- Prime numbers: discussion od some deeper results such as Dirichlet's Theorem on primes in arithmetic progressions and the prime number theorem.
- Finite fields and the quadratic reciprocity law.
- Deeper analysis of the RSA cryptosystem: risks and requirements.
- Primality: probabilistic primality tests (Fermat, Jacobj, Miller-Rabin), and deterministic tests in some cases.
- The discrete logarithm in a finite field, and applications (such as the Diffie-Hellmann cryptosystem).
- Factorization: Pollard's rho method, the factor bases method.
- Depending on time and interest, selected additional topics of cryptographic interest or consequences, such as: characters and Dirichlet series; character sum bounds; Riemann's zeta function; basics on elliptic curves; the AKS (deterministic) primality test.

Prerequisites

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

Teaching form

Lectures (8 credits). They will be of two different kind: 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

Periodic exercise sheets will be made available on the e-learning website to encourage participation. The solutions will be discussed in class on request, or during officie hours.

The course comprises a total of 56 one-hour in-class lectures (usually combined in pairs).

A hybrid teaching approach is used, that combines lecture-based teaching (DE) and interactive teaching (DI). DE involves detailed presentation and explanation of theoretical content. DI includes active student participation

through exercises and problems, short presentations, group discussions, and group or individual work. It is not possible to precisely determine in advance the number of hours dedicated to DE and DI, as these methods are dynamically intertwined to adapt to the course's needs and promote a participatory and integrated learning environment, combining theory and practice.

Lectures (56 hours) and practical sessions/tutorials are conducted in person and will be in Italian by default, and when necessary, in English.

Textbook and teaching resource

Lecture notes for the course are made available. They are partially inspired from the following textbook, which is recommended for further reading:

- N. Koblitz, A course in Number Theory and Cryptography, volume 114 of Graduate texts in Mathematics, Springer-Verlag, second edition, 1994.

Please see the notes for other recommended sources.

Semester

II term.

Assessment method

Written and oral examination.

- The written part requires solving a set of exercises, mainly of practical character.
- The oral examination will serve to demonstrate the knowledge of the topics of the course (including statements and proofs of theorems).

Admission to the (compulsory) oral exam requires obtaining a mark of at least 18/30 in the written exam.

Both the written and oral exam will contribute to the final mark for the course.

Office hours

By direct agreement.

Sustainable Development Goals

QUALITY EDUCATION