Mathematical Methods for Cryptography
(Metodi Matematici della Crittografia)

Instructor: Davide Lombardo

2023-2024
(first semester)

1 Contents

The course is designed to provide an introduction to a wide range of cryptographic techniques. Modern public-key cryptography is an asymmetric problem: the goal is to find a way to encode information in such a way that it can be easily decrypted by someone in possession of a certain secret, while being inaccessible to anyone else (without the two communicating parties sharing a *common* secret!). Early attempts to achieve this were mostly based on two fundamental problems in arithmetic: the factorisation of (large) integers and the so-called discrete logarithm problem in finite fields. Over time, both the cryptosystems and the attacks on them have become more sophisticated, and much of modern cryptography instead relies on properties of elliptic curves to achieve both speed and secrecy.

The course will cover the fundamental cryptographic primitives (one-way hash functions, digital signatures, key exchange, public key cryptography...), discussing both the classical approaches (based on factoring or on the discrete logarithm problem) and more modern ones. On the classical side, we will look at methods for factoring integers, proving primality, and computing discrete logarithms. On the modern side, the course will include both a complete theoretical introduction to the mathematics of elliptic curves over finite fields and a description of their cryptographic applications. If time permits, we will also briefly touch upon the problem of *post-quantum* cryptography.

2 Highlights

How would you *convince* someone that $10^{60} + 7$ is a prime number? And how would you *prove* it (answer: using elliptic curves!)? Jul vf guvf n irel onq rapbqvat? Did you know that you can crack RSA encryption keys by listening to a CPU doing computations (article on pcworld.com)?

3 Practical information

The course lasts 42 hours and takes place in the first semester. Roughly half the lectures will focus on cryptography, with the other half providing the necessary theoretical background on elliptic curves. The final assessment will be a traditional oral examination. It will include questions on the course content and possibly some simple exercises.

Prerequisites for this course are some arithmetic (at the the level of the first year course, including e.g. the notion of congruence between integers, the theory of finite fields, and the notion of field extension), the basics of linear algebra, and some familiarity with polynomial rings. Some knowledge of algebraic geometry (at the level of the introductory course "Elements of Algebraic Geometry") is useful but not required. All relevant notions and results from algebraic geometry will be covered in the course (without proofs).

For enquiries, please contact davide.lombardo@unipi.it.