Crypto Rulez

The Rules

The exams will be composed of three parts:

- Oral exam
- Written exam
- Project

In each part you can get up to 11 points.

The final mark for this module will be the sum of the points.

The final mark for the course will be the average of the two modules.

Team implementation of a project

The students will be divided randomly in groups of 2 people each and they will be given the same project to implement *using MAGMA*.
The implementation must be completely written in the MAGMA language, without calling any external programme. The code must be well-commented in English.
The teams will receive the same official document describing the project, composed of 5 different assignments.

The projects will be tested and evaluated in the 24/05/2022 lecture.
If the programme fails to work correctly and the problems are not fixed before the end of the lecture, then **all team members will fail** and they will have to **attend again the whole lab session** in Spring 2023.

Bonus point for the fastest project

When testing the projects, we will evaluate the speed of each algorithm. The group with the overall fastest algorithms will get an extra point in the final mark.

In case of dispute, we will consider the hierarchy of the exercises. This will be explained in the next slides.

Personal report on the project

Assuming that a team has passed the first phase, then each team member must submit an individual report on the project. The report must be written in English and not more than 15 pages.
The report must include the following:

- your personal contribution to the team project (0-2 points)
- a complete overview of the mathematical problems behind the algorithms (0-4 points)
- an in-depth explanation of the implementative choices (0-4 points)

You must also submit the code of the project. This may include some improvements that you personally added after the project submission.

Mark: 0/10 (+1 for the bonus)
(that is, the evaluation of the report constitutes one third of the exam's mark)

Crypto Project 2022

Crypto Projects 2022

There are 5 different assignments to implement.

1. Signature scheme: ECDSA (2000 TV)
2. ECDLP: Pohlig-Hellman (500 TV)
3. DLOG: Index calculus (1000 TV)
4. Primality test: Solovay-Strassen (3000 TV)
5. Factorisation: Lehman (1000 TV)

This ordering corresponds to the hierarchy (in case of dispute for the bonus point).

Crypto Groups 2022

Crypto Groups 2022

You have been divided into five groups:

1. Baby K: Fregona, Di Muzio;
2. Sfera Ebbasta: Salvatori, Astore;
3. Elettra Lamborghini: Di Domenico, Sorbera;
4. Miss Keta: Selvaggini, Errati;
5. Bello FiGo: Borin, Maddaloni.