VE475
Introduction to Cryptography

Project 1

Manuel — UM-JI (Summer 2019)

Goals of this project

- Improve research efficiency
- Develop teamwork and collaboration skills
- Organise and write clear documents
- Improve understanding by confronting acquired knowledge to new information

Cryptography being a vast field of study not all its subtopics can be properly considered in class. Therefore the goal of this project is to perform some personal study in order to acquire this extra knowledge while also improving major skills such as writing, collaboration, and public presentation.

As a team, discuss which subjects to investigate. In the case where everybody agrees on a topic not listed below please inform us of your choice.

This projects splits into two parts: (i) writing a report and (ii) presenting the result of your work to all the students. In particular the project report is to be submitted before the deadline and should provide a thorough presentation of the subfield of study. The presentation in front of all the students will be held at a later time and should provide a high level introduction on the chosen topic.

Any source of information can be used (internet, textbooks, research articles...). However, in any case, **do not recopy the materials** and always cite all your sources.

When reading new information, understand it, process it, consider how it relates to what you already know, and how you can reach conclusions beyond the ones offered in your source.

Available topics:

1. Public Key Infrastructure
2. The Random Oracle Model
3. Shannon's Theory and Cryptography
4. Error Correcting Codes and Cryptography
5. Steganography and Cryptography
6. Lattice-based Cryptography*
7. Multivariate Cryptography*
8. Message Authentication Code

*Those slightly more advanced projects will benefit from a softer grading policy.