Project 1: Topic 1

Encrypt your data

Luca Campa

Department of Computer Science
Universität Innsbruck

13 March, 2025

Topics

- Introduction
- Task Description
- Learning Objective
- Dates
- Evaluation

Introduction

If someone steals your device, it can always read the content of your hard disk, unless...

- you encrypt your hard drive and you protect your data with a password or more authentication factors.

Common modus operandi:

- encrypt your entire hard drive (e.g. VeraCrypt,LUKS), even the `boot` partition.
- encrypt specific folders, files, non-system partitions (e.g. VeraCrypt)

How the encryption works (at high level):

- uses standardized algorithms, like AES (you can also choose the Mode of operation)
- the user chooses a password from which the system derives a key for the encryption algorithm. We will discuss about key derivation functions in the last lecture. **For the purpose of this project you can generate the key as you prefer**.

Task description

Using Python and the encryption systems we have discussed, develop a simple tool that:

- Asks the user for the path of the folder it wants to encrypt or decrypt
- Asks the user for the type of operation (encryption or decryption)
- Asks the user for a password
- Encrypt (or decrypts) the target folder (the choice of the mode of encryption is up to you, but you must justify it).

Note: you can choose to encrypt the entire folder or to encrypt the contained files. Feel free to make your own implementation choices.

Task description

Your project must be structures in the following way:

- it must contain a `src` folder where the tool will be located
- it must contain a `README.txt` file that contains the detailed usage instructions with a small justification of the implementation choices.

Learning objective

- Understanding how to protect your device and the data on it.
- Understanding the usage of the cryptographic schemes we have tackled during the lecture.

Dates

- **Deadline for submission**: 30 March 2025 at 23:59
- **Oral presentation**: 03 April 2025

Evaluation

The project will count as the 20% of the final grade, in particular:

- 10% Implementation:
    - 2% if the code is running
    - 8% if the code returns correct results on all the test inputs (we will provide you with some of them, but not all)
- 10% Oral presentation

It is not mandatory, you can do the project in groups of **maximum 2** students.