CAA 23-24

Mini-project

29.11.2023

- Submit **your code** and **your report** on Cyberlearn.
- The **quality** of the cryptographic implementation will be graded.
- The grade 4 is obtained by a correct (and clear) modelling of the cryptography in a report.
- The remaining 2 points are obtained from a good implementation.
- The programming language is free (preferably among Rust, C/C++, Java, Python/Sage). If you would like to use another language, please ask first.
- Do not hesitate to ask questions.

1 An Encrypted File System

The goal of this laboratory is to implement a **shared encrypted network file system**. Here are the requirements:

- Users should be able to log into the system with a simple username/password.
- They should have to enter their password only once.
- Every file and folder should be protected against **active** adversaries. We don't consider DoS, though.
- File and folder names should also be confidential. Folders structure and file sizes can leak.
- We assume that the server is **honest but curious**.
- Clients should be able to connect to the file system from any computer and change device as they want.
- A **folder** can be **shared** with another user. We assume that the list of users can be known to the users of the system. When a folder is shared, all its sub-folder and files are also shared.
- Access to a shared folder can be **revoked** by anyone having access to the folder. Bonus points if only the original owner can revoke.
- A user should be able to **change their password**.
- A possible list of features is: `download file`, `upload file`, `create folder`, `share folder`, `unshare folder`, `change password`.

2 Deliverable

You have to deliver the following:

- A report describing your cryptographic architecture and explaining your choices (3/5). In particular, provide a scheme describing how the keys are managed. Explain and study the impact of your choices on **performances** (think huge file systems) and **security**.
- Your code (2/5). Note that we do **not** ask you to implement any networking. If you want, you can simulate everything locally. Only the cryptography will be evaluated.
- You do not have to do a GUI. Command line is fine.
- Bonus points will be given for any cool additional functionality (e.g. read/write access, more complex access rights, ...). **Describe them in your report!**