CAA 2021

Lab #2

27-4-2021

- 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 by a good implementation.
- The programming language is free (preferably among C/C++, Rust, Java, Python/Sage). If you would like to use another language, please ask first.
- Do not hesitate to ask questions.

1 An Encrypted Vault

The goal of this laboratory is to implement an online vault storing encrypted files. Here are the requirements:

- The authentication should be performed by password and we want a **challenge-response** protocol.
- When the client is **not authenticated**, neither files nor filenames should be readable by the server.
- When the client **authenticates**, he receives an encrypted list of filenames. He can then select which file he wants.
- The selected file is sent by the server (still encrypted).
- Every file should be encrypted with a **different key**.
- The server should **never** see the documents in clear and should not be able to recover them (assuming a "good" password).
- The client should not have to enter more than **one password**.
- If a document's encryption key leaks, one should not be able to decrypt all documents.

2 Bonus

Bonus points will be given for additional cool functionalities. Examples:

- Multi-user software with server not able to distinguish which files belong to which user.
- File sharing among users.
- Multi-factor authentication
- Use of TPM to secure secrets
- Any other cool idea...

3 Deliverable

You have to deliver the following:

- A report describing your cryptographic architecture and explaining your choices (3/5)
- Your code (2/5). Note that we do **not** ask you to implement the networking part if you do not want to. You also do not have to use a real database. You can simulate everything with a local file if you prefer.