You have to develop a simple Python app that integrates well-know cryptographic tools in a coherent and secure manner (within the scope of the course). The objective is that you learn how the cryptographic tools studied in theory are implemented and integrated in real projects, even if it is a "small" project.

This activity is designed to be done in groups (2 students per group).

Requirements for the app:

- The app must be capable of dealing with more than one user
- Users can register in the app (sign up)
- Users can login in the app (login)
- (Optional) Users can modify its account data (username, password, etc...)
- The app must store and process some data for providing the app's functionality.
- Data stored by the app must be protected (using authenticated encryption) in a coherent and secure manner (giving the scope of the app). Note that this requirement does not mean that ALL data must be protected.

Additionally, the users and/or the system must have the capability of generating digital signatures on some information and verify such signatures. A simple public key infrastructure (Root_CA) needs to be deployed and all the public keys of the users and/or the system must be certified by Root_CA or its subordinate CA.

Assessment criteria:

a) You must submit a short report describing your app, the cryptographic design (key management, selection of algorithms, etc.) and how you have integrated the cryptographic tools within it. It is expected that you include snapshots of code snippets and terminal interactions.

b) You'll have to defend your app in person, explaining its main features (mostly the cryptographic ones) and answer the teacher's questions about the cryptographic design.

c) Grade distribution:

User authentication	0,5 over 4,0
Key management	0,5 over 4,0
Authenticated encryption of user's data (OR Symmetric encryption and MAC)	0,75 over 4,0
	(OR 0,4 + 0,35 over 4,0)
Generation and verification of digital signatures	0,75 over 4,0
Mini-PKI (public key certificates)	1,0 over 4,0
BONUS (extra) Asymmetric encryption	(+ 0,5 over 4,0)
Report	0,5 over 4,0
TOTAL	4,0 (+0,5 extra)

Last modified: Tuesday, 25 November 2025, 1:11 PM

© Universidad Carlos III de Madrid

Get the mobile app

?