Herein you can read a tentative planning of what we will see in each of the lab sessions.

First, I copy of the schedule; see in green the lab sessions.

Detailed Planning (tentative)

	Large Group		Small Group
8.sep.25	M0: Presentation + Introduction	10.sep.25	M1: Mathematical Foundations I
15.sep.25	M1: Mathematical Foundations II	17.sep.25	M2: Classical Crypto I
22.sep.25	M2: Classical Crypto II	24.sep.25	M3: Fund. Crypto Concepts (Encryption, Randomness, Security Notions)
29.sep.25	M4: Symmetric Encryption I	1.oct.25	LAB 0: Intro to Python I
6.oct.25	M4: Symmetric Encryption II	8.oct.25	LAB 0: Intro to Python II + LAB I start
13.oct.25	M4: Symmetric Encryption III	15.oct.25	LAB I: Symmetric Encryption
20.oct.25	M5: Key Distribution & Asymmetric Encryption I	22.oct.25	M5: Key Distribution & Asymmetric Encryption II
27.oct.25	M5: Key Distribution & Asymmetric Encryption III	29.oct.25	LAB II: Key Distribution & Asymmetric Encryption
3.nov.25	**MIDTERM I (25%)**	5.nov.25	M6: Hash Functions & MAC
10.nov.25	M6: Authenticated Encryption	12.nov25	LAB III: Hash Functions, MACs, AE & Digital Signatures
17.nov.25	M7: Digital Signatures	19.nov.25	M8: PKI I
24.nov.25	M8: PKI II	26.nov.25	LAB IV: PKI
1.dec.25	M9: User Authentication	3.dec.25	**MIDTERM II (25%)**
8.dec.25		10.dec.25	**Research & Tell Presentations (10%)**
15.dec.25			

Description of the concepts and achievements related to a specific session:

1. Lab session on 01/10/2025: Introduction to lab tasks. Overview of suggested simple architecture. Discussion on challenges and impact of the functionality on key management. Overview of how to store a "super hash" of the pwd instead of the password to authenticate users. Discussion on the need to encode byte-like sequences to more robust text-based encodings.
2. Lab session on 08/10/2025: In this session ideally you should have a basic idea of your app and utopically :D you should have a minimal implementation of a Python script that, via a text-based menu, allows to register users (storing the username and pwd in cleartext), and to authenticate users (just by checking that the provided password is equal to the one stored in the system). Not needed persistence (JSON files) at this moment. We review in more detail how to generate the super hash of the pwd and verify a pwd against this token when authenticating a user.
3. Lab session on 15/10/2025: At this point you should have the design of your app and its implementation quite advanced (without crypto algorithms). You should have shared with me the functionality and basic design of your app. We will focus on designing the key management aspects and implementing the authenticated encryption of the data that needs protection.
4. Lab session on 29/10/2025: We will see how asymmetric keys are generated and how you can generate and verify a digital signature on some data extracted from your system.
5. Lab session on 12/11/2025: We will deal with digital certificates and how to use them in your processes of signature generation and verification. We'll introduce the use of OpenSSL to generate a mini-PKI.
6. Lab session on 26/11/2025: We will review again certificates and PKI. You still have some time after this last session to complete your code, as the assessment sessions will be allocated after the lectures finish. However, if some group is ready for assessment before this week, we can arrange previous dates for the lab assessment.

Notice that you'll have to share with me a short report (I'll provide you with some guidelines for its structure and contents) and the code (copying the source code in the folder that I'll create for your lab group or by writing the link to your GitHub repo in a text file and sharing with me the repository).

Last modified: Tuesday, 7 October 2025, 7:55 PM