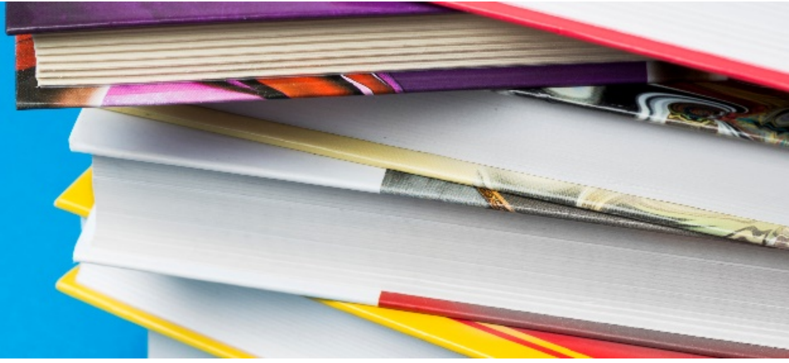
TEL AVIV אוניברסיטת
UNIVERSITY תל אביב



Full Syllabus

Course Title

Introduction to Modern Cryptography

Lecturer

Omer Paneth

Semester

2020/1 A

Course requirements

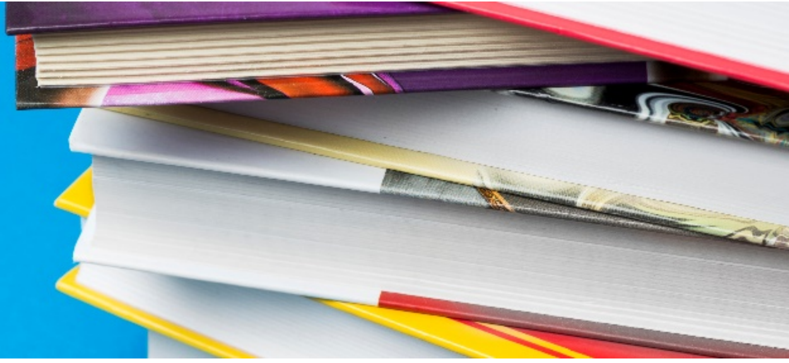
8-10 homework assignments and a final exam. Half and the assignments will be theoretical and half will involve programing.

Final grade components

20-30% homework, 70-80% final exam.

Course schedule

Class no. / Date	Subject and Requirements (assignments, reading materials, tasks, etc.)
1	Course overview, perfect security. Recommended reading: Lecture 1 in Barak's notes. Sections 2.1 and 2.2 in the Boneh-Shoup. Chapters 1 and 2 in Katz-Lindell.
2	Computational security, pseudorandom generators. Recommended reading: Lectures 2 and 3 in Barak's notes. Sections 2 and 3 in the Boneh-Shoup. Chapters 3.1-3.4 in Katz-Lindell.
3	Encrypting multiple messages, chosen plaintext security, pseudorandom functions. Recommended reading: Lectures 4 and 5 in Barak's notes. Sections 4 in the Boneh-Shoup. Chapters 3.5,3.6,5 in Katz-Lindell.
4	Authentication, Collision Resistant Hash functions Recommended reading: Lectures 4 and 7 in Barak's notes. Sections 6,7,8 in Boneh-Shoup. Chapter 4 in Katz-Lindell.
5	Diffie–Hellman key exchange, group theory and number theory background. Recommended reading: Lecture 9 in Barak's notes. Sections 10,11 in Boneh-Shoup. Chapters 8,10 in Katz-Lindell.
6	Public-key encryption, RSA. Recommended reading: Lecture 10 in Barak's notes. Sections 10,11 in Boneh-Shoup. Chapter 11 in Katz-Lindell.
7	Digital signatures.



	Recommended reading: Lectures 9,13 in Barak's notes. Sections 13,14 in Boneh-Shoup. Chapter 12 in Katz-Lindell.
8	Zero-Knowledge Proofs. Recommended reading: Lecture 14 in Barak's notes. Chapter 4 in Pass-Shelat.
9	Coin flipping, oblivious transfer. Recommended reading: Lecture 17 in Barak's notes. Chapter 6 in Pass-Shelat.
10	Multiparty computation, Yao’s Garbled Circuit Recommended reading: Lecture 17 in Barak's notes. Chapter 6 in Pass-Shelat. Lindell's simulation tutorial.
11	Consensus, blockchain, cryptocurrency. Lecture 7 in Barak's notes.
12	Fully homomorphic encryption. Lectures 16 and 17 in Barak's notes.
13	Software Obfuscation. Lectures 22 and 23 in Barak's notes.

Required course reading

Optional course reading

- Introduction to Modern Cryptography / Katz and Lindell.
- An Intensive Introduction to Cryptography / Barak.
- A graduate course in applied cryptography / Boneh and Shoup.
- Foundations of Cryptography / Goldreich.
- A course in cryptography / Pass and Shelat.

Comments