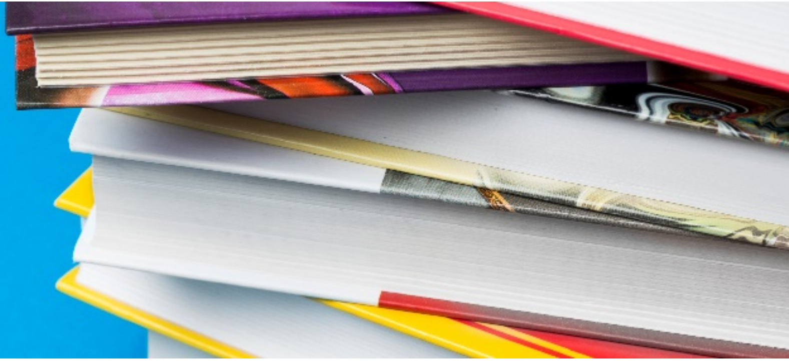
TEL AVIV UNIVERSITY אוניברסיטת תל אביב



Full Syllabus

Course Title

Foundations of Cryptography

Lecturer

Iftach Haitner and Omer Paneth

Semester

2020/1 A

Course requirements

5-6 homework assignments and a final exam.

Final grade components

20% homework, 80 final exam.

Course schedule

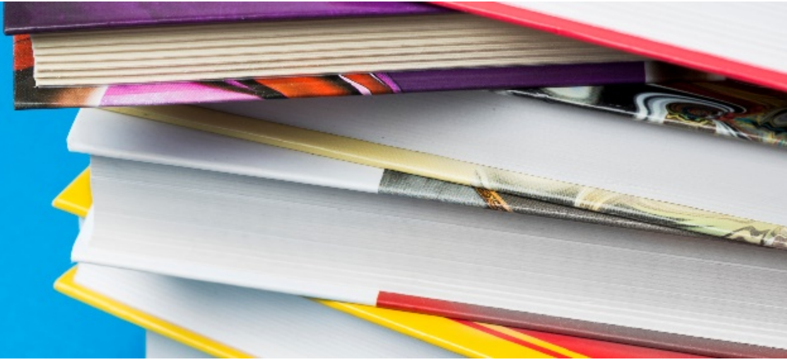
Class no. / Date	Subject and Requirements (assignments, reading materials, tasks, etc.)
1	Course overview, one-way functions.
2	One-way functions, pseudorandom generators.
3	Hardcore predicates.
4	Pseudorandom functions.
5	MACs, signature schemes.
6	Interactive proofs, zero knowledge.
7	Zero knowledge, commitment schemes.
8	Zero Knowledge, non-interactive zero knowledge.
9	Non-interactive zero knowledge, proof of knowledge.
10	Encryption schemes
11	Secure multi-party computation.
12	Non black-box zero-knowledge
13	Advanced topics

Required course reading

Optional course reading

Books:
- Jonathan Katz and Yehuda Lindell. An Introduction to Modern Cryptography.
- Oded Goldreich. Foundations of Cryptography.

Other crypto courses and notes:
- Benny Applebaum and Iftach Haitner (form the last time I gave this course with Benny)
- Boaz Barak



- Nir Bitansky
- Ran Canetti
- Benny Chor (The Undergraduate Course)
- Yevgeniy Dodis
- Yehuda lindell
- Rafael Pass and Abhi Shelat
- Gil Segev
- Salil Vadhan
- Daniel Wichs

Comments

Slides and materials from previous years are available on Moodle.