

## General Information

Time: Thursday 10:00-13:00.

Instructors: [Nir Bitansky](#) and [Iftach Haitner](#)

Reception (please coordinate in advance via email): Nir: Wednesday 13:00-14:00, Iftach: Tuesday 12:00-13:00.

Abstract: This is a graduate-level advanced course in Cryptography. Tentative list of subjects: fully-homomorphic encryption, functional encryption, obfuscation, applications of encrypted computation, black box impossibility results, black box impossibility results, computational notions of entropy.

Prerequisite: [Foundations of Cryptography I](#)

Requirements: 5-6 homework assignments (50-70%), final exam (30-50%).

## Tentative schedule

Week	Date	Class Topics
1	March 04	Fully-homomorphic encryption
2	March 11	Functional encryption
3	March 18	Obfuscation I
4	April 8	Obfuscation II
5	April 22	Applications of encrypted computation
6	April 29	Applications II
7	May 06	Black-box Impossibility results
8	May 13	Black-box Impossibility results
9	May 20	Black-box Impossibility results
10	May 27 (ends at 12, Student Day)	Computational Analogues of Entropy
11	June 03	Computational Analogues of Entropy
12	June 10	Computational Analogues of Entropy

