0368.4162: Foundations of Cryptography

Fall 2014

Dan David 204, Thursdays 10:00am - 1pm

Instructor: Ran Canetti. Office Hours: please coordinate. Email: canetti@tau.ac.il

Syllabus: The course will provide an in-depth introduction to the foundations of cryptography. The goal is to give students a taste of the main concepts, abstractions, algorithms, and techniques. The target audience is graduate students who wish to get acquainted with the magic of cryptography and consider doing research in it. Throughout, the course will alternate between the foundational viewpoint and the applied one. Here is a tentative list of topics, by week:

- **Week 1: Overview of cryptography; perfect encryption**
- **Week 2: Hard problems; one way functions; hardness amplification**
- **Week 3: Stream ciphers, computational indistinguishability, pseudorandom generators**
- **Week 4: Pseudorandom generators from one-way functions; hard-core predicates**
- **Week 5: Block ciphers; pseudorandom functions and permutations**
- **Week 6: Message authentication codes; collision resistant hashing**
- **Week 7: Digital signatures**
- **Week 8: Symmetric encryption**
- **Week 9: Trapdoor permutations; key exchange, public key infrastructure**
- **Week 10: Public-key encryption: CPA, CCA**
- **Week 11: Homomorphic and functional encryption, program obfuscation**
- **Week 12: Commitment schemes; interactive proofs; Zero knowledge**
- **Week 13: Secure distributed computation**

Pre-requisites:

Basic probability theory, basic complexity (the classes P, NP, BPP, NP-completeness). Some prior informal-level knowledge of cryptography, such as the undergraduate course 0369.3049, is recommended but not required. Perhaps the most important pre-requisite

is mathematical maturity: The ability to read, understand, complete, and generate mathematical proofs.

This is a graduate course. Undergraduate students are encouraged to take 0369.3049. In some special cases, however, undergraduates who receive personal permission of the instructor can take the course.

Course requirements: There will be weekly problem sets (around 10 altogether). Each problem set is due in class the following week. You are encouraged to collaborate and consult external resources in solving the homework problems. However, you should write the solution on your own, and list all external resources and collaborators. In addition, there will be a final exam.

Reading material: We will not follow any single textbook. Still, practically all the material that will be presented in class is covered by one or more of the resources listed below, as well as many others that are available online. Beware, however, that conventions, notations and definitions may differ from lecture. See the syllabus of the class of fall 2010 for a more detailed description of the two books below, as well as several other useful ones.

Books:

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

Lecture notes:

- Ran Canetti. Introduction to Cryptography
- Leo Reyzin: Fundamentals of Cryptography
- Salil Vadhan: Introduction to Cryptography
- Luca Trevisan. Cryptography.
- Yehuda lindell Foundations of Cryptography.
- Dan Boneh. Introduction to Cryptography.
- Mihir Bellare and Shafi Goldwasser: Lecture Notes on Cryptography
- Jonathan Katz: Introduction to Cryptography (undergraduate and graduate)
- Ronitt Rubinfeld: On Chernov and Chebichev bounds.

Additional material:

- Victor Shoup. A Primer on Algebra and Number Theory for Computer Scientists.