2011-2012

**203.4447 – Foundations of Cryptography  
Semester ?** B

**Time:** Monday, 13-16, Room 714.

**Instructor:** Dr. Ronen Shaltiel

**Office Hours:** Thursday, 13-14, Jacobs 414, 8249952.

**Course Type:** Lecture

**Course Level**: M.Sc. and B.Sc.

**Pre-Requisites:** Basic Probability, Computational Models

**Course Overview:** The course covers definitions, constructions and analysis of basic cryptographic protocols. The focus is on rigorous mathematical treatment and provable security.

**Topics (tentative list):**

1. Symmetric Perfectly Indistinguishable Encryption.
2. Pseudorandom Generators and Computationally Indistinguishable Encryption.
3. Hard Bits, Hybrid Arguments and the Blum-Micali-Yao generator.
4. Commitment Schemes.
5. Zero Knowledge Proof Systems.
6. Secure Function Evaluation.

**Requirements:** Exam

**Grading:**

Exam – 100%

**Website:** <http://www.cs.haifa.ac.il/~ronen/courses/Crypto2012/Crypto2012.html>

**Reading List:**

Books:

* Jonathan Katz and Yehuda Lindell.  [*An Introduction to Modern Cryptography*](http://www.cs.umd.edu/%7Ejkatz/imc.html)*.*
* Oded Goldreich. [*Foundations of Cryptography.*](http://www.wisdom.weizmann.ac.il/%7Eoded/foc-book.html)

Lecture notes:

* Salil Vadhan. [Introduction to Cryptography.](http://people.seas.harvard.edu/%7Esalil/cs120/)
* Yehuda Lindell [Foundations of Cryptography](http://u.cs.biu.ac.il/%7Elindell/89-856/main-89-856.html).