Course Announcement

Cryptography
(Advanced Computer Science)


Instructor(s): Krzysztof Pietrzak
Teaching Assistant: Georg Fuchsbauer

Description:
This course offers an introduction to the theory and practice of modern cryptography, the science of computer security. We will cover basic topics such as encryption (secret-key and public-key), message authentication, digital signatures, identification, cryptographic hashing and zero-knowledge proofs.

The course is self-contained, however a basic understanding of probability theory will be helpful.

Textbook:
Introduction to Modern Cryptography by J. Katz and Y. Lindell.

Requirements and Exams:
Lectures and recitations (homework and exams TBA)

Schedule:
2 weekly 75min lectures Fridays, 10:45AM-12:00PM and 1:00-2:15PM, recitations Fridays, 2:30-3:20PM

Academic Credits:
3 ECTS

Website: [http://pub.ist.ac.at/courses/AY1314/Cryptography_F13/](http://pub.ist.ac.at/courses/AY1314/Cryptography_F13/)

This course starts on Friday, November 29, 2013 (10:45AM-12:00PM & 1:00-2:15PM)
Seminar Room Mondi 3, IST Austria Central Building, 1st floor

The registration deadline for this course is Monday, November 18, 2013 via IST Austria’s online registration tool: [http://ist.ac.at/graduate-school/courses/registration/](http://ist.ac.at/graduate-school/courses/registration/).

This announcement is valid as a ticket for the IST Shuttle bus (#242) from and to Heiligenstadt Metro Station. Please find a schedule of the IST Shuttle on our webpage (note that the IST Shuttle times are marked in dark green): [https://ist.ac.at/fileadmin/user_upload/pdfs/IST_shuttle_bus.pdf](https://ist.ac.at/fileadmin/user_upload/pdfs/IST_shuttle_bus.pdf).

The IST Shuttle bus is marked “IST Shuttle” and has the Institute logo printed on the side.