Foundation of Cryptography (0368-4162-01), Lecture 0

Adminstration + Introduction

Iftach Haitner, Tel Aviv University

November 1, 2011

Part I

Administration and Course Overview

Section 1

Administration

Important Details

1. Iftach Haitner. Schriber 20, email iftachh at gmail.com

Important Details

1. Iftach Haitner. Schriber 20, email iftachh at gmail.com
2. Reception: Sundays 9:00-10:00 (please coordinate via email in advance)

Important Details

1. Iftach Haitner. Schriber 20, email iftachh at gmail.com
2. Reception: Sundays 9:00-10:00 (please coordinate via email in advance)
3. Who are you?

Important Details

1. Iftach Haitner. Schriber 20, email iftachh at gmail.com
2. Reception: Sundays 9:00-10:00 (please coordinate via email in advance)
3. Who are you?
4. Mailing list: 0368-4162-01@listserv.tau.ac.il
    - Registered students are automatically on the list (need to activate the account by going to https://www.tau.ac.il/newuser/)
    - If you're not registered and want to get on the list (or want to get another address on the list), send e-mail to: listserv@listserv.tau.ac.il with the line: subscribe 0368-3500-34 <Real Name>

Important Details

1. Iftach Haitner. Schriber 20, email iftachh at gmail.com
2. Reception: Sundays 9:00-10:00 (please coordinate via email in advance)
3. Who are you?
4. Mailing list: 0368-4162-01@listserv.tau.ac.il
   - Registered students are automatically on the list (need to activate the account by going to https://www.tau.ac.il/newuser/)
   - If you're not registered and want to get on the list (or want to get another address on the list), send e-mail to: listserv@listserv.tau.ac.il with the line: subscribe 0368-3500-34 <Real Name>
5. Course website: http://www.cs.tau.ac.il/ iftachh/Courses/FOC/Fall11/main.html (or just Google iftach and follow the link)

Important Details

1. Iftach Haitner. Schriber 20, email iftachh at gmail.com
2. Reception: Sundays 9:00-10:00 (please coordinate via email in advance)
3. Who are you?
4. Mailing list: 0368-4162-01@listserv.tau.ac.il
   - Registered students are automatically on the list (need to activate the account by going to https://www.tau.ac.il/newuser/)
   - If you're not registered and want to get on the list (or want to get another address on the list), send e-mail to: listserv@listserv.tau.ac.il with the line: subscribe 0368-3500-34 <Real Name>
5. Course website: http://www.cs.tau.ac.il/ iftachh/Courses/FOC/Fall11/main.html (or just Google iftach and follow the link)

Grades

1. Grading: Please add your name and email through the course website
    1. Class exam 60%

Grades

1. Grading: Please add your name and email through the course website
   1. Class exam 60%
   2. Homework 30%: 3-5 exercises. Recommend to use use LaTex (see link in course website) Exercises (separate email per question) should be sent to foc.exc@gmail.com; Title: Question #, Name, Id

Grades

1. Grading: Please add your name and email through the course website
    1. Class exam 60%
    2. Homework 30%: 3-5 exercises. Recommend to use use LaTex (see link in course website) Exercises (separate email per question) should be sent to foc.exc@gmail.com; Title: Question #, Name, Id
    3. Self grading 10 %
        - Please register following the link on the course website, and email foc.exc@gmail.com; Title: Grader #: Name, ID
        - Submit your solution to the question using Latex (I'll check it)
        - Within two weeks after the submission time. The grader should send the checked exercises to foc.exc@gmail.com and to the authors, and send a single excel file (columns: Id, Name, grade) to foc.exc@gmail.com, Title: Checked Exe # ,

and..

1. Slides

and..

1. Slides
2. English

Course Prerequisites

1. Some prior knowledge of cryptography (such as 0369.3049) might help, but not necessarily
2. Basic probability.
3. Basic complexity (the classes P, NP, BPP)

Course Material

1. Books:
   1. Oded Goldreich. Foundations of Cryptography.
   2. Jonathan Katz and Yehuda Lindell. An Introduction to Modern Cryptography.
2. Lecture notes
   1. Ran Canetti. Foundation of Cryptography (The 2008 course)
   2. Salil Vadhan. Introduction to Cryptography.
   3. Luca Trevisan. Cryptography.
   4. Yehuda lindell Foundations of Cryptography.

Section 2

Course Topics

Course Topics

Basic primitives in cryptography (i.e., one-way functions, pseudorandom generators and zero-knowledge proofs).

- Focus on *formal* definitions and *rigorous* proofs.
- The goal is not studying some list, but to understand cryptography.
- Get ready to start researching

Part II

Foundation of Cryptography

Cryptography and Computational Hardness

1. What is Cryptography?

Cryptography and Computational Hardness

1. What is Cryptography?
2. Hardness assumptions, why do we need them?

Cryptography and Computational Hardness

1. What is Cryptography?
2. Hardness assumptions, why do we need them?
3. Does $\mathrm{P} \neq \mathrm{NP}$ suffice?

$\mathrm{P} \neq \mathrm{NP}$: i.e., $\exists L \in \mathrm{NP}$, such that for any polynomial-time algorithm A, $\exists x \in \{0,1\}^*$ with $\mathrm{A}(x) \neq 1_L(x)$

polynomial-time algorithms: an algorithm A runs in polynomial-time, if $\exists p \in$ poly such that the running time of $A(x)$ is bounded by $p(|x|)$ for any $x \in \{0,1\}^*$

Cryptography and Computational Hardness

1. What is Cryptography?
2. Hardness assumptions, why do we need them?
3. Does $\mathrm{P} \neq \mathrm{NP}$ suffice?

   $\mathrm{P} \neq \mathrm{NP}$: i.e., $\exists L \in \mathrm{NP}$, such that for any polynomial-time algorithm A, $\exists x \in \{0,1\}^*$ with $\mathrm{A}(x) \neq 1_L(x)$

   polynomial-time algorithms: an algorithm A runs in polynomial-time, if $\exists p \in$ poly such that the running time of $A(x)$ is bounded by $p(|x|)$ for any $x \in \{0,1\}^*$
4. Problems: hard on the average. No known solution

Cryptography and Computational Hardness

1. What is Cryptography?
2. Hardness assumptions, why do we need them?
3. Does $\mathrm{P} \neq \mathrm{NP}$ suffice?

   $\mathrm{P} \neq \mathrm{NP}$: i.e., $\exists L \in \mathrm{NP}$, such that for any polynomial-time algorithm A, $\exists x \in \{0,1\}^*$ with $\mathrm{A}(x) \neq 1_L(x)$

   polynomial-time algorithms: an algorithm A runs in polynomial-time, if $\exists p \in$ poly such that the running time of $A(x)$ is bounded by $p(|x|)$ for any $x \in \{0,1\}^*$
4. Problems: hard on the average. No known solution
5. One-way functions: an efficiently computable function that no efficient algorithm can invert.