Cryptography

Course Overview

Gil Segev
What is Cryptography?

Cryptography is an ancient art

- For many centuries focused mainly on secret communication
- Consumers were military and intelligence organizations
- Relied on creativity and personal skill
- 500BC – 20th century: Design $\rightarrow$ break $\rightarrow$ repair $\rightarrow$ break $\rightarrow$ repair $\rightarrow$ …
What is Cryptography?

Cryptography is an ancient art
- For many centuries focused mainly on secret communication
- Consumers were military and intelligence organizations
- Relied on creativity and personal skill
- 500BC – 20\textsuperscript{th} century: Design $\rightarrow$ break $\rightarrow$ repair $\rightarrow$ break $\rightarrow$ repair $\rightarrow$ …

This course: Modern Cryptography
- Radical change in the late 20\textsuperscript{th} century: Cryptography as a science
- Much more than secret communication
- Consumed by everyone!
- Relies on rigorous models, definitions & proofs!
What is Cryptography?

The scientific study of techniques for designing systems that withstand adversarial behavior.
Course Objectives

Introduce the basic paradigms and principles of cryptography
• Explore a variety of cryptographic tools & systems
• Learn how to reason about their security
• Learn how to use them correctly
Course Objectives

Introduce the basic paradigms and principles of cryptography
• Explore a variety of cryptographic tools & systems
• Learn how to reason about their security
• Learn how to use them correctly

At the end of this course you will
• Be an educated crypto consumer
• Know why it is dangerous to assume you are a “crypto expert”
• Be able to learn more about cryptography
# Tentative Course Structure

<table>
<thead>
<tr>
<th>Weeks</th>
<th>Course Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-5</td>
<td>Private-key cryptography</td>
</tr>
<tr>
<td>6-10</td>
<td>Public-key cryptography</td>
</tr>
<tr>
<td>11-13</td>
<td>Zero-knowledge proofs &amp; secure computation</td>
</tr>
</tbody>
</table>
Recommended Resources


• Coursera’s *Cryptography* course (Prof. Jonathan Katz) https://www.coursera.org/learn/cryptography
Organization & Evaluation

• **Time & place:** Mon 15:10-17:55, Rothberg B221

• **Course webpage:** http://moodle2.cs.huji.ac.il/nu16/course/view.php?id=67531

• **Evaluation method:** $N \in \{5,6\}$ home assignments & final exam

Final grade = $\frac{1}{5} \times \text{(average of best } N-1 \text{ assignments)} + \frac{4}{5} \times \text{(exam grade)}$

Must pass the exam in order to pass the course
Contact Details

• **Lecturer:** Dr. Gil Segev (Rothberg A531, Wed 15:00-16:00 by appointment)

• **Please contact us via Moodle’s “Personal Forum” feature**
  (students can see their own posts only)