Course program and reading list

Semester 2 Year 2021

School: Efi Arazi School of Computer Science M.Sc.

Cryptography

Lecturer:

Prof. Alon Rosen alon.rosen@runi.ac.il

Teaching Assistant:

Ms. Noa Oved Noa.Oved@post.runi.ac.il

Course No.:	Course Type :	Weekly Hours :	Credit:
159	Elective	3	3

Course Requirements :	Group Code :	Language:
Final Exam	212015901	Hebrew

Prerequisites

Prerequisite:

52 - Calculus I
53 - Calculus II
54 - Linear Algebra I
55 - Linear Algebra II
56 - Discrete Mathematics
59 - Data Structures
69 - Logic And Set Theory
77 - Algorithms
417 - Introduction To Computer Science
643 - Automata And Formal Languages

Course Description

Cryptography is the science of designing algorithms and protocols that guarantee privacy, authenticity, and integrity of data when parties are communicating or computing in an insecure environment. The recent explosion of electronic communication and commerce has expanded the significance of cryptography far beyond its historical military role into all of our daily lives. For example, cryptography provides the technology that allows you to use your credit card to make on-line purchases without allowing other people on the internet to learn your credit card number.

The past 35 years have also seen cryptography transformed from an ad hoc collection of mysterious tricks into a rigorous science based on firm complexity-theoretic foundations. It is this modern, complexity-theoretic approach to cryptography that will be the focus of this course. Specifically, we will see how cryptographic problems can be given **precise mathematical definitions**. Then we will construct algorithms which **provably** satisfy these definitions, under precisely stated and widely believed **assumptions**. For example, we will see how to prove statements of the flavor "Encryption algorithm X hides all information about the message being transmitted, under the assumption that factoring integers is computationally infeasible."

Topics that we will cover include ``classical" cryptographic methods, Shannon's theory of secrecy (and how to get around its limitations using computational assumptions), one-way functions, private-key and public-key encryption, digital signatures, pseudorandom generators. If time permits, we will also cover higher-level protocols such as zero-knowledge and secure computation, electronic cash, and the role of cryptography in network and systems security.

Course Goals

On completion of the course, students will be able to explain and apply the basic concepts underlying the science of modern cryptography. In particular, they will be able to use these methods to develop secure systems and/or to assess the security of given cryptographic constructions. The course is designed to expose students to the state of the art of modern cryptography and should serve as a solid starting point for scientific research in the area.

Grading

Final exam (90% of the course grade).

Homework (10% of the course grade).

Learning Outcomes

What can you hope to learn from this course?

- **Definitions:** Why it is important to precisely define cryptographic problems, and how to do so for several important problems (encryption, authentication, digital signatures, etc.). What are the kinds of subtleties that arise in such definitions, and how to critically evaluate and interpret cryptographic definitions.
- **Constructions and Proofs of Security:** Examples of general and concrete solutions to various cryptographic problems, and how to prove that they satisfy the definitions mentioned above (based on precisely stated assumptions).
- **Foundations:** The assumptions on which modern cryptography is based, and their implications.
- **Theory vs. Practice:** This course will focus on theory, but we will discuss how the theory relates to what is actually done in practice.
- **Applications:** If time permits, we will see one or two examples of how to address cryptographic issues in higher-level protocol problems, such as auctions, voting, or electronic cash.
- **Security:** This is not a course on security, but if time permits, we will discuss how cryptography fits into the broader contexts of network and systems security.

What this course will NOT teach you

- **Acronyms:** There are many different cryptographic algorithms, protocols, and standards out there, each with their own acronym. It is not the aim of this course to cover these specific systems, which may come and go, but rather the general principles on which good cryptography is based. Understanding these principles will enable you to evaluate the specific systems-you encounter outside this course, on your own. (This is not to say that the course will be without exa

---

Lecturer Office Hours

Tuesdays 14:00-15:00.

Reading List

The course will loosely follow the book *Introduction to Modern Cryptography* by Jonathan Katz and Yehuda Lindell. A more advanced (graduate-level) exposition of the material can be found in Oded Goldreich's *Foundations of Cryptography (Volumes I and II)*. More application-oriented crypto books are (note that these books take a much less careful approach to definitions and security proofs than we do in the course):

- A.J. Menezes, P.C.van Oorschot, and S.A. Vanstone. *Handbook of Applied*

Cryptography.

- D.R. Stinson. *Cryptography: Theory and Practice.*
- B. Schneier. *Applied Cryptography.*
- R.Anderson. *Security Engineering*.