Lecture Series Introduction

Notes for *Serious Cryptography*

Jeffrey Goldberg
jeffrey@goldmark.org

April 2024 (Revised August 26, 2024)

Origins and directions

In the beginning

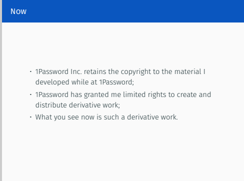
- 1Password Security Team Book Club;
- Sessions led by me, Jeffrey Goldberg;
- The book: *Serious Cryptography*, [Aum17];
- Sessions often digressed from the book;
- Sessions often riffed off of one or two things in a chapter.

Now

- 1Password Inc. retains the copyright to the material I developed while at 1Password;
- 1Password has granted me limited rights to create and distribute derivative work;
- What you see now is such a derivative work.

2024-08-26

Lecture Series Introduction
└Origins and directions
└Now



Now

- 1Password Inc. retains the copyright to the material I developed while at 1Password;
- 1Password has granted me limited rights to create and distribute derivative work;
- What you see now is such a derivative work.

1. A consequence of this is that anyyone seeking to republish or make deriviate works based on what I have here will need to get persion from 1Password, Inc.

Who is this for?

Who is this for?

> *The book doesn't require any coding skills, and is accessible to anyone who understands the basics of computer science and college-level math (notions of probabilities, modular arithmetic, and so on).* [Aum17, *Preface*]

My goal is to make this accessible to those without the basics of computer science and only requiring high-school level math.

(Re-)teaching the math

- Modular arithmetic
- Logarithms
- Probability

(Re)-teaching the Computer Science

- XOR
- bigO
- Complexity
- Notation

Not all at once

- Some background will be taught early;
- Some will be taught when needed;
- Some will be taught in bits and pieces, often indirectly;
- Notation may be introduced by example instead of full definitions.

Partial credit

- It is not necessary to understand all the math and CS;
- It is not necessary to understand concepts when they are first introduced;
- Many concepts will become clearer over time;
- You must be willing to try to get the gist of something even when the details are unclear.

A pack of lies

- I will leave things out of definitions and discussions when I feel that those may be distracting;
- Some things that may appear to be distractions may be meant to foreshadow things.

Resources

Resources

- These slides
- Sources

References I

[Aum17] Jean-Philippe Aumasson. *Serious cryptography: a practical introduction to modern encryption.* No Starch Press, 2017.