crypto attacks & defenses RELOADED

JP Aumasson, Philipp Jovanovic

ringzerø

introduction

Welcome

Thank you for registering to our class!

You will…

- Learn the **core concepts** of cryptography, but without too much theory
- Discover real **crypto engineering** problems and solutions
- Solve **challenges** inspired from real crypto failures
- Have fun! 😎

Our Approach

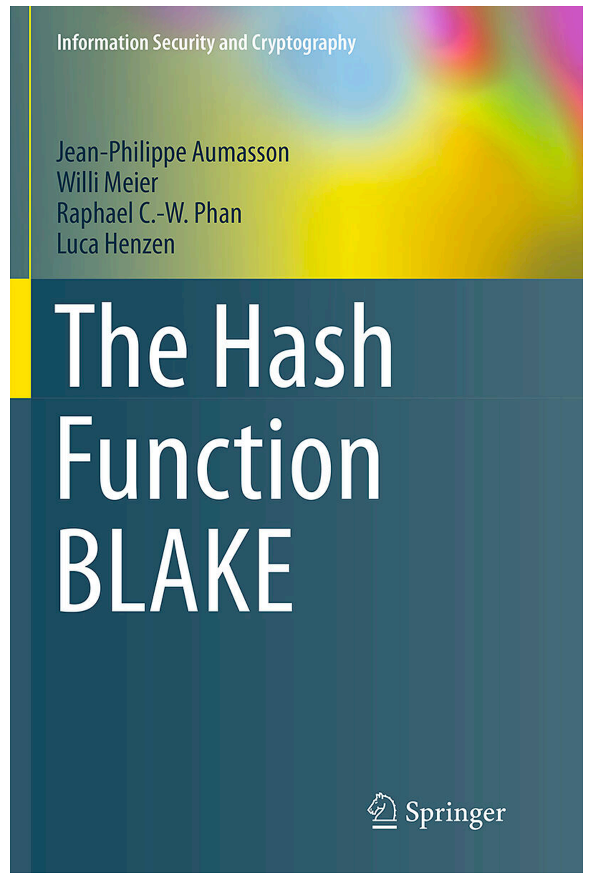
We’ve been teaching crypto since 2013, and like to follow these principles:

- Focus on **real-world** crypto
- Teach the **what** (concepts and ideas) more than how (tools, commands, etc.)
- Describe **attacks** to learn defenses
- Focus on **modern** crypto algorithms and applications
- Make the class **interactive**, encouraging questions and interruptions

About Us

JP - @veorq - aumasson.jp

- Co-founder, CSO @ **Taurus**, CH
- Doing crypto since 2006, PhD 2009
- Academia, industry, consulting, start-ups
- Design algorithms SipHash, BLAKE2

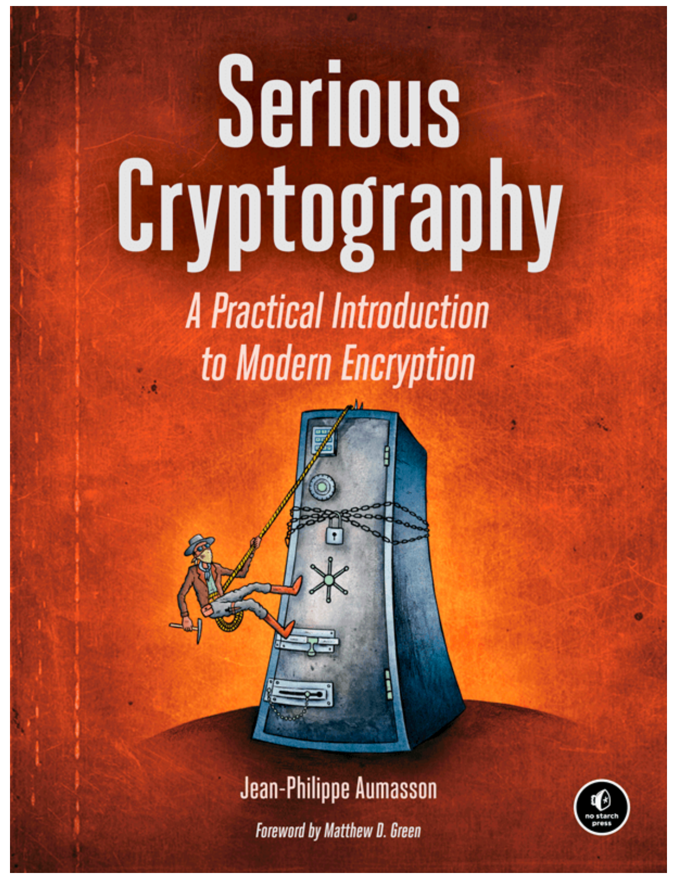


Information Security and Cryptography

Jean-Philippe Aumasson
Willi Meier
Raphael C.-W. Phan
Luca Henzen

The Hash Function BLAKE

Springer

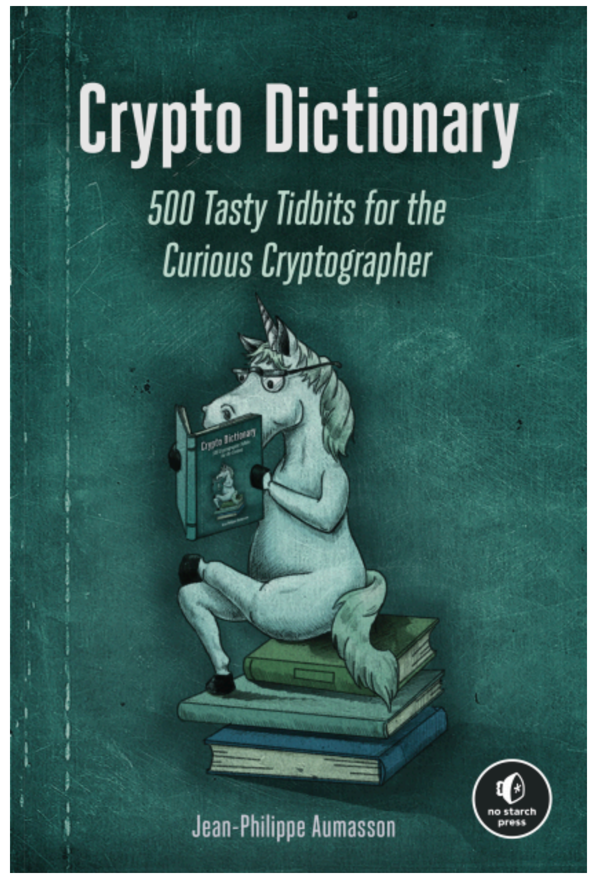


Serious Cryptography

A Practical Introduction to Modern Encryption

Jean-Philippe Aumasson

Foreword by Matthew D. Green



Crypto Dictionary

500 Tasty Tidbits for the Curious Cryptographer

Jean-Philippe Aumasson

Philipp - @daeinar - philipp.jovanovic.io

- Professor @ **University College London**, UK
- Co-founder at ZKV, advisor at various blockchain orgs
- Doing crypto since 2010, PhD 2015
- Designing crypto algorithms (NORX, MEM-AEAD) and distributed systems (ByzCoin, OmniLedger, drand, ARKE)

Round Table

Agenda

Monday	Tuesday	Wednesday	Thursday	Friday
Introduction	Secure Channels	Key Management	Secure Coding	Decentralized Randomness
Randomness	TLS	Passwords	Blockchains	Post-Quantum Crypto
Symmetric	E2EE	Libraries & API	Multi-Party Computation	Zero-Knowledge Proofs
Public-key	Exercises	Exercises	Exercises	Exercises

Roughly 1h per item (45 min talk + 15 min break)

Logistics

- Please use **Discord for discussions** about the class and exercises
- **Slides** (PDFs) and **exercises** available at the beginning of each day
- **Videos** and all exercises solutions available after the training
- If you have **questions** during the lectures, please don't hesitate to **interrupt us**, and if you'd prefer not to, post your question on **Discord**

Exercise Sessions 👨🏽‍💻

Environment: 2 options…

- Docker
  - Install: https://www.docker.com/products/docker-desktop
  - Run: `docker run -it veorq/cryptotraining:v0 /bin/bash`
- Your own system (Linux or macOS), with python3, openssl (prior to v3.0), gnupg, gcc, and ssss

We'll be hanging out on Discord when we can, feel free to ask for hints, or for the solution to verify that you have the right one, or if you're really stuck 🙃

Final Introductory Thoughts

- Crypto is more exciting today than it's ever been, in part thanks to blockchain security challenges, it can open many job/research opportunities

- Becoming an expert takes time and practice, but anyone can get there 😊

- Our goals are to help you understand what crypto can and cannot do, the underlying **ideas** and concepts, rather than **recipes** (which you can search for online for your specific use case)

We hope you'll enjoy the class! 😎 🚀

crypto attacks & defenses RELOADED

JP Aumasson, Philipp Jovanovic

ringzerø

introduction ✓