Practical Cryptography in Python

Learning Correct Cryptography by Example

Seth James Nielson
Christopher K. Monson

Apress®

Practical Cryptography in Python: Learning Correct Cryptography by Example

Seth James Nielson
Austin, TX, USA

Christopher K. Monson
Hampstead, MD, USA

ISBN-13 (pbk): 978-1-4842-4899-7
ISBN-13 (electronic): 978-1-4842-4900-0
https://doi.org/10.1007/978-1-4842-4900-0

Managing Director, Apress Media LLC: Welmoed Spahr
Acquisitions Editor: Susan McDermott
Development Editor: Laura Berendson
Coordinating Editor: Rita Fernando

Cover designed by eStudioCalamar

Distributed to the book trade worldwide by Springer Science+Business Media New York, 233 Spring Street, 6th Floor, New York, NY 10013. Phone 1-800-SPRINGER, fax (201) 348-4505, e-mail orders-ny@springer-sbm.com, or visit www.springeronline.com. Apress Media, LLC is a California LLC and the sole member (owner) is Springer Science + Business Media Finance Inc (SSBM Finance Inc). SSBM Finance Inc is a **Delaware** corporation.

For information on translations, please e-mail rights@apress.com, or visit http://www.apress.com/rights-permissions.

Apress titles may be purchased in bulk for academic, corporate, or promotional use. eBook versions and licenses are also available for most titles. For more information, reference our Print and eBook Bulk Sales web page at http://www.apress.com/bulk-sales.

Any source code or other supplementary material referenced by the author in this book is available to readers on GitHub via the book's product page, located at www.apress.com/9781484248997. For more detailed information, please visit http://www.apress.com/source-code.

Printed on acid-free paper

For Saige, who hopes to be a Computer Scientist like Daddy.
—Seth

To Mom and Dad, who valued good writing
and never settled for less than my best.
—Chris

Table of Contents

About the Authors

Seth James Nielson is the Founder and Chief Scientist of Crimson Vista, Inc., a boutique computer security research and consulting company. He is also an adjunct professor at Johns Hopkins University where he teaches network security and has also served as the Director of Advanced Research Projects in the Information Security Institute. As part of his Hopkins work, he co-founded the https://cryptodoneright.org knowledge base, through a generous grant from Cisco.

Christopher K. Monson has a PhD in machine learning and has spent over a decade at Google in various engineering, machine learning, and leadership roles. He has broad experience writing and teaching programming courses in multiple languages and has worked in document password recovery, malware detection, and large-scale secure computing. He is serving as the Chief Technology Officer at Data Machines Corp. and teaches Cloud Computing Security at the Johns Hopkins University Information Security Institute.

About the Technical Reviewer

Mike Ounsworth is a Software Security Architect at Entrust Datacard. He holds an undergraduate degree in computer science with concentrations in mathematics and physics and an MSc in computer science in robotics and artificial intelligence. Professionally, his day job is mainly application security architecture and penetration testing, with some research side projects in cryptography and post-quantum cryptography. Outside of work, he mentors teams competing in the high-school-age FIRST Robotics Competition.

Introduction

The interconnected world of the current era has drastically changed everything, including banking, entertainment, and even statecraft. Despite differences in users, purposes, and security profiles, these digital applications have at least one thing in common: they all require properly applied cryptography to work correctly.

Informally, cryptography is the mathematics of secrets. We need secret codes to make messages unreadable to unauthorized eyes, to make messages unchangeable, and to know who sent the message. Practical cryptography is the design and use of these codes in real systems.

This book is primarily for computer programmers with little or no previous background with cryptography. Although mathematics makes brief appearances in the book, the overall approach is to teach introductory cryptography concepts by example.

Our journey begins with some introductory components, including hashing algorithms, symmetric encryption, and asymmetric encryption. Next, we go beyond encryption and into the realm of digital certificates, signatures, and message authentication codes. The final chapters show how these various elements come together in interesting and useful combinations, such as Kerberos and TLS.

Another important part of cryptography by example is cryptography by bad example! In this book we will break things on purpose to help the reader appreciate what motivates accepted best practices. Exercises and examples include walk-throughs of real vulnerabilities that have afflicted the Internet. The bad examples will help the reader gain a greater intuition of what goes wrong in cryptography and why.