Cryptography 101: From Theory to Practice

Chapter 17 – Summary

Rolf Oppliger

April 6, 2022

Terms of Use

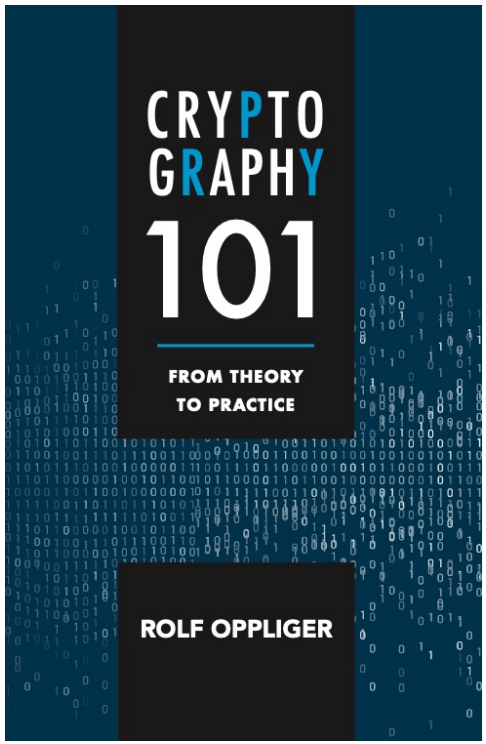
- This work is published with a CC BY-ND 4.0 license ()
  - CC = Creative Commons ()
  - BY = Attribution ()
  - ND = No Derivatives ()

whoami

rolf-oppliger.ch
rolf-oppliger.com

- Swiss National Cyber Security Centre NCSC (scientific employee)
- eSECURITY Technologies Rolf Oppliger (founder and owner)
- University of Zurich (adjunct professor)
- Artech House (author and series editor for information security and privacy)

Reference Book



ISBN 978-1-63081-846-3

`https://books.esecurity.ch/crypto101.html`

Challenge Me

Outline

17. Summary

17. Summary

17.1 Unkeyed Cryptosystems

- Random generators (→ Chapter 3)
- Random functions (→ Chapter 4)
- One-way functions (→ Chapter 5)
- Cryptographic hash functions (→ Chapter 6)

17. Summary

17.2 Secret Key Cryptosystems

- Pseudorandom generators ($\rightarrow$ Chapter 7)
- Pseudorandom functions ($\rightarrow$ Chapter 8)
- Symmetric encryption ($\rightarrow$ Chapter 9)
- Message authentication ($\rightarrow$ Chapter 10)
- Authenticated encryption ($\rightarrow$ Chapter 11)

17. Summary

17.3 Public Key Cryptosystems

- Key establishment ($\rightarrow$ Chapter 12)
- Asymmetric encryption ($\rightarrow$ Chapter 13)
- Digital signatures ($\rightarrow$ Chapter 14)
- Zero-knowledge proofs of knowledge ($\rightarrow$ Chapter 15)

17. Summary

17.4 Final Remarks

- In practice, unkeyed, secret key, and public key cryptosystems are combined to complement each other (e.g., hybrid systems)
- Public key cryptosystems are used for authentication and key distribution, whereas secret key cryptosystems are used for bulk data encryption and message authentication
- Consequently, applications typically combine all types of cryptosystems to come up with a design that can be implemented in an efficient and secure way
- Key management is the Achilles' heel

17. Summary

17.4 Final Remarks

- It is sometimes argued that public key cryptography is inherently more secure than secret key cryptography
- This argument is wrong
- There are secure and insecure public key and secret key cryptosystems
- If one has to decide what cryptosystem to use, then one has to look at the requirements from an application's point of view
- There is no single best cryptosystem to be used for all purposes and applications (i.e., no "one size fits all" solution)

Questions and Answers

Thank you for your attention