Cryptography 101: From Theory to Practice

Lead and Chapter 1 – Introduction

Rolf Oppliger

February 1, 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

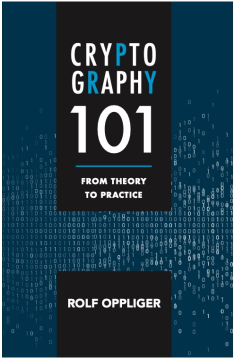
- Swiss National Cyber Security Centre NCSC (scientific employee)
- eSECURITY Technologies Rolf Oppliger (founder and owner)
- University of Zurich (adjunct professor)
- Artech House (author and series editor for information security and privacy)

Guiding Principle

If you want to build a ship, dont drum up the men to gather wood, divide the work, and give orders. Instead, teach them to yearn for the vast and endless sea.

— Antoine de Saint-Exupéry

Reference Book



© Artech House, 2021
ISBN 978-1-63081-846-3

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

Leading Quotes (1)

Necessity is the mother of invention, and computer networks are the mother of modern cryptography.

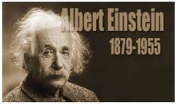
— Ronald L. Rivest

Any sufficiently advanced technology is indistinguishable from magic.

— Arthur C. Clarke

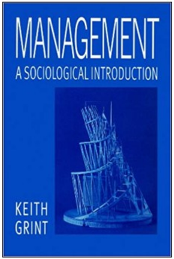
- James L. Massey (2001), Cryptography – Science or Magic?
- Dieter Gollmann (2011), Cryptography - Magic, Science, or Science Fiction?

Leading Quotes (2)



In theory, theory and practice are the same. In practice, they are not.

— Albert Einstein



Theory is when you know everything and nothing works;
Practice is when everything works and nobody knows why;
Here we combine Theory with Practice: Nothing works and nobody knows why.

— Keith Grint

Disclaimers (1)

- The slides are relatively simple, down-to-earth, and not visually stimulating
- Mathematical fundamentals are not addressed here (cf. appendixes A, B, C, and D)
- Alice, Bob, Carol, Dave, Eve, and the rest of the gang are posted as missing (cf. *Disillusioning Alice and Bob*, IEEE Security & Privacy, Vol. 15, No. 5, 2017, pp. 82–84)

© https://xkcd.com/1323/

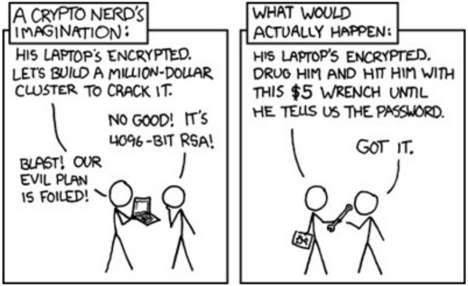
ALICE SENDS A MESSAGE TO BOB SAYING TO MEET HER SOMEWHERE.
UH HUH.
BUT EVE SEES IT, TOO, AND GOES TO THE PLACE.
WITH YOU SO FAR.
BOB IS DELAYED, AND ALICE AND EVE MEET.
YEAH?

I'VE DISCOVERED A WAY TO GET COMPUTER SCIENTISTS TO LISTEN TO ANY BORING STORY.

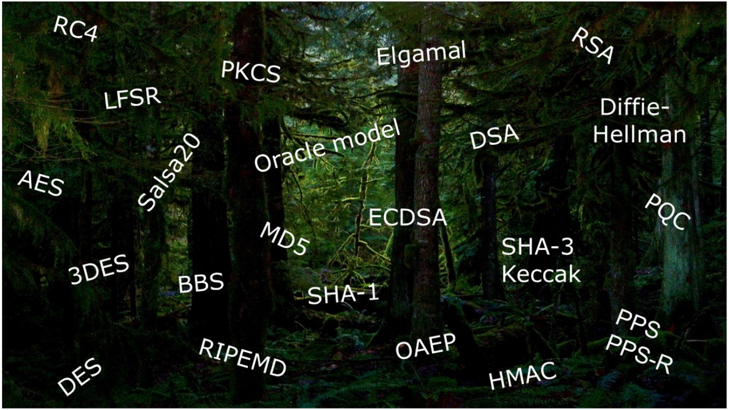
Disclaimers (2)

- The world of cryptography is restricted and does not properly take into account human aspects and the subtleties of machine-user interaction (cf. YouTube video)

© https://xkcd.com/538/


A CRYPTO NERD'S IMAGINATION:
HIS LAPTOP'S ENCRYPTED. LET'S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.
NO GOOD! IT'S 4096-BIT RSA!
BLAST! OUR EVIL PLAN IS FOILED!
WHAT WOULD ACTUALLY HAPPEN:
HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.
GOT IT.

See the wood for the trees



Do not worship a golden calf (e.g., PKI, blockchain, . . .)

© Nicolas Poussin, 1634

Challenge Me

Outline

1. Introduction
2. Cryptographic Systems
3. Random Generators
4. Random Functions
5. One-Way Functions
6. Cryptographic Hash Functions
7. Pseudorandom Generators
8. Pseudorandom Functions
9. Symmetric Encryption
10. Message Authentication
11. Authenticated Encryption
12. Key Establishment
13. Asymmetric Encryption
14. Digital Signatures
15. Zero-Knowledge Proofs of Knowledge
16. Key Management
17. Summary
18. Outlook

1. Introduction

1.1 Cryptology

1.2 Cryptographic Systems

1.3 Historical Background Information

1.4 Outline of the Book

1. Introduction

- Kryptos (Jim Sanborn, 1990) located at the CIA Headquarter in Langley, Virginia
- Section IV (97 characters)

```
OBKRUOXOGHULBSOLIFBBWFLRV
QQPRNGKSSOTWTQSJQSSEKZZWA
TJKLUDIAWINFBNYPVTTMZFPKW
GDKZXTJCDIGKUHUAUEKCAR
```

- Hints
  - NYPVTT = BERLIN (2010)
  - MZFPK = CLOCK (2014)
  - QQPRNGKSS = NORTHEAST (2020 and final)

1. Introduction

1.1 Cryptology

- The term **cryptology** is derived from the Greek words "kryptós," meaning "hidden," and "lógos," meaning "word"
- Consequently, the term can be paraphrased as "hidden word"
- This refers to the original intent of cryptology, namely to hide the meaning of words and to protect the confidentiality and secrecy of data accordingly
- Today, the term is more broadly used for many other security-related purposes and applications (in addition to the protection of the confidentiality and secrecy of data)

1. Introduction

1.1 Cryptology

More specifically, the term **cryptology** refers to the mathematical science and field of study that comprises both cryptography and cryptanalysis

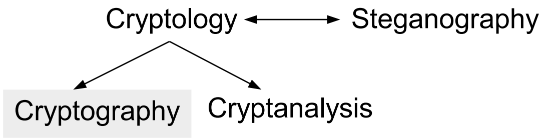
- The term **cryptography** is derived from the Greek words "kryptós" and "gráphein," meaning "to write" (≈ "hidden writing")
- The term **cryptanalysis** is derived from the Greek words "kryptós" and "analýein," meaning "to loosen" (≈ "to loosen the hidden")

1. Introduction

1.1 Cryptology

It is sometimes also used to include steganography

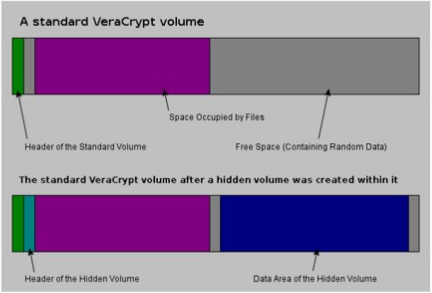
- The term **steganography** is derived from the Greek words "steganos," meaning "impenetrable," and "gráphein" (≈ "impenetrable writing")
- It includes digital watermarking and digital fingerprinting



1. Introduction

1.1 Cryptology

Cryptographic and steganographic techniques are not mutually exclusive and can be combined at will (e.g., VeraCrypt hidden volumes)


A standard VeraCrypt volume
Space Occupied by Files
Header of the Standard Volume
Free Space (Containing Random Data)
The standard VeraCrypt volume after a hidden volume was created within it
Header of the Hidden Volume
Data Area of the Hidden Volume

1. Introduction

1.2 Cryptographic Systems

- According to RFC 4949, the term **cryptographic system** (or **cryptosystem**) refers to "a set of cryptographic algorithms together with the key management processes that support use of the algorithms in some application context"

Definition 1.1 (Algorithm)

A well-defined computational procedure that takes a value as input and turns it into another value that represents the output

An algorithm can be deterministic or probabilistic (randomized)

1. Introduction

1.2 Cryptographic Systems

Definition 1.2 (Protocol)

A distributed algorithm in which two or more entities take part

Definition 1.3 (Cryptographic Algorithm)

An algorithm that employs and makes use of cryptographic techniques and mechanisms (→ single-entity cryptosystem)

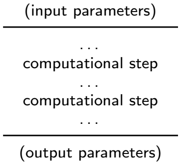
Definition 1.4 (Cryptographic Protocol)

A protocol that employs and makes use of cryptographic techniques and mechanisms (→ multiple entities cryptosystem)

1. Introduction

1.2 Cryptographic Systems

Algorithm notation

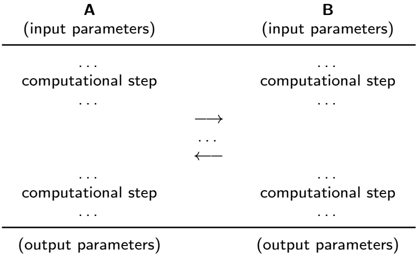


(input parameters)

...
computational step
...
computational step
...

(output parameters)

Protocol notation



A
(input parameters)

B
(input parameters)

...
computational step
...

...
computational step
...

⟶
...
⟵

...
computational step
...

...
computational step
...

(output parameters)

(output parameters)

1. Introduction

1.2 Cryptographic Systems

Definition 1.5 (Unkeyed Cryptosystem)

Cryptographic system that uses no secret parameter

Definition 1.6 (Secret Key Cryptosystem)

Cryptographic system that uses secret parameters that are shared among the participating entities

Definition 1.7 (Public Key Cryptosystem)

Cryptographic system that uses secret parameters that are not shared among the participating entities

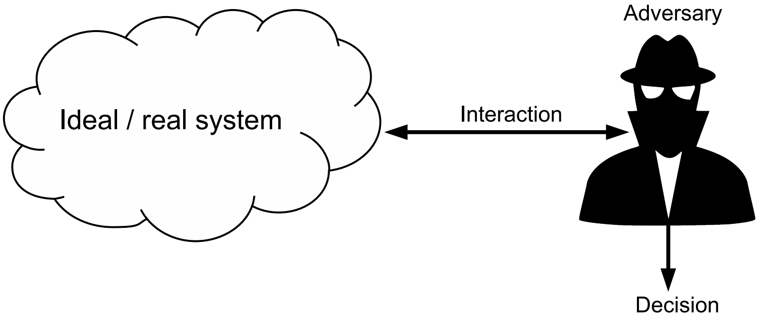
1. Introduction

1.2 Cryptographic Systems

- The goal of cryptography is to design, implement, and employ cryptographic systems that are **secure**
- To make precise statements about the security of a cryptosystem, one must formally define the term **security**
- In theory, this requires the definition of an adversary (→ threats model) and a task the adversary has to solve in order to be successful
- The second point is often addressed with a **security** or **(in)distinguishability game** in the **ideal/real simulation paradigm**

1. Introduction

1.2 Cryptographic Systems



1. Introduction

1.2 Cryptographic Systems

Definition 1.8 (Secure cryptographic system)

A cryptographic system is secure if a well-defined adversary cannot break it, meaning that he or she cannot solve a well-defined task

A strong security definition assumes an adversary that is as powerful as possible and a task that is as simple to solve as possible

Examples

- Security of a safe
- Football game
- ...

1. Introduction

1.2 Cryptographic Systems

Two reasons why an adversary cannot solve a task (according to Definition 1.8) lead to two different notions of security

Unconditional security: An adversary with infinite computing power is not able to solve the task within a finite amount of time (**information-theoretic security**) → probability theory and information theory

Conditional security: An adversary is in principle able to solve the task within a finite amount of time, but doesn't have the computational resources to do so (**computational security**) → computational complexity theory

1. Introduction

1.2 Cryptographic Systems

- The distinction between unconditional and conditional security is at the core of modern cryptography
- Interestingly, there are cryptosystems known to be secure in the strong sense (i.e., unconditionally secure), but there are no cryptosystems known to be secure in the weak sense (i.e., conditionally secure)
- **Provable security** refers to another notion of (conditional) security
- It goes back to the early days of public key cryptography (Diffie-Hellman key exchange)

1. Introduction

1.2 Cryptographic Systems

- Analogy
  - How can one prove that squaring a circle with compass and straightedge is impossible?
  - One reduces the problem of squaring a circle to the problem of finding a non-zero polynomial $f(x) = a_n x^n + \ldots + a_1 x + a_0$ with rational coefficients a_i for $i = 0, 1, \ldots, n$, such that π is a root, i.e., $f(\pi) = 0$
  - Because π is not algebraic (it is transcendental), such a polynomial does not exist and cannot be found either
  - This suggests that a circle cannot be squared with a compass and straightedge

1. Introduction

1.2 Cryptographic Systems

- Formally, let problem P_1 be the problem of squaring a circle with compass and straightedge and P_2 be the problem of finding a non-zero polynomial $f(x)$ with $f(\pi) = 0$
- Because $P_1 \leq_P P_2$ and P_2 cannot be solved, it seems that P_1 cannot be solved either
- To be precise, however, one has to show that $P_1 \leq_P P_2$ and $P_2 \leq_P P_1$, meaning that P_1 and P_2 are computationally equivalent, i.e., $P_1 \equiv_P P_2$
- A cryptographic system is provably secure if breaking it can be shown to be computationally equivalent to solving a hard (mathematical) problem

1. Introduction

1.2 Cryptographic Systems

- There are situations in which a security proof requires an additional assumption, namely that a cryptographic primitive (typically a cryptographic hash function) behaves like a random function
- This leads to a new paradigm and methodology to design cryptographic systems that are provably secure in the **random oracle model**
- This is in contrast to the **standard model**
- The random oracle methodology and the random oracle model are discussed controversially (→ Chapter 8)

1. Introduction

1.2 Cryptographic Systems

If it's provably secure, it probably isn't.

— Lars Knudsen

- The whole notion of provable security (in cryptography) must be taken with a grain of salt
- In practice, a (theoretically and/or provably secure) cryptosystem must be implemented in one way or another

1. Introduction

1.2 Cryptographic Systems

- Many things can go wrong here
  - Social engineering attacks (e.g., phishing)
  - The cryptographic keys may be extracted from memory (e.g., using a cold boot attack)
  - Compromising emanation (→ TEMPEST)
  - Side-channel attacks (see below)
  - . . .

1. Introduction

1.2 Cryptographic Systems

- Mind experiment (attributed to Artur Ekert)
  - Two rooms - one with 3 light switches and one with 3 light bulbs
  - The wiring of the light switches and bulbs is unknown
  - The adversary has to find out the wiring but can enter each room only once
- A mathematically-minded person can prove that the task is impossible to solve
- And yet, a physically-minded person can solve the task (e.g., by exploiting the temperature of the light bulbs as use it as a side-channel)

1. Introduction

1.2 Cryptographic Systems

- Side-channel attacks come in many flavors (e.g., Spectre and Meltdown)
    - Timing attacks
    - Power analysis attacks
    - Fault analysis attacks
    - Attacks that exploit protocol failures
    - Attacks that exploit the sounds generated by a computation
    - . . .

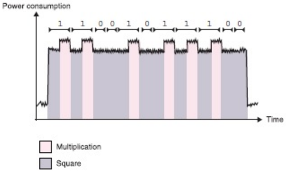


Figure 13.5 Some cryptographic algorithms leak so much information via their power consumption that a simple power analysis of a single power trace (a measure of the power consumed in time) can leak the private key of the algorithm. For example, this figure represents a trace of an RSA exponentiation (the message being exponentiated to the private exponent; see chapter 6). The RSA exponentiation is implemented with a square-and-multiply algorithm that iterates through the bits of the private exponent; for each bit it applies a square operation followed by a multiply operation only if the bit is set. In this example, multiplication is obviously consuming more power; hence, the clarity of the power trace.

© David Wong, *Real-World Cryptography*, Manning Publications Co., Shelter Island, NY, 2021, page 292

1. Introduction

1.2 Cryptographic Systems

- In theory, people are looking into **physically observable cryptography** or **leakage-resilient cryptography** to mitigate side-channels and respective attacks
- For example, constant-time programming may help to mitigate timing attacks
- But writing code that runs in constant time is not trivial (e.g., avoid branches) and must withstand compiler optimization
- Consequently, the results achieved so far in leakage-resilient cryptography are not particularly encouraging

1. Introduction

1.2 Cryptographic Systems

- In the past, there have been many examples in which people have tried to improve the security of a cryptographic system by keeping secret its design and internal working principles
- This approach is known as **security through obscurity**
- Many of these systems do not work and can be broken trivially
- In contrast, the **Kerckhoffs' principle** states that a cryptographic system should be designed so as to remain secure, even if the adversary knows all the details of the system, except for the keys
- In some areas, the Kerckhoffs principle is not strictly followed and even discussed contraversially (e.g., pay TV)

1. Introduction

1.2 Cryptographic Systems

- Cryptosystems should be as
  - secure
  - usable
  - boring

  as possible
- Formal verification and testing tools are increasingly important (e.g., Google Project Wycheproof)
- Existing cryptographic libraries should be used whenever possible (e.g., Bouncy Castle, OpenSSL/LibreSSL, Google Tink, NaCl, libsodium, cryptlib, . . .)

1. Introduction

1.3 Historical Background Information

- Cryptography has a long and thrilling history
- Until World War II, it was considered to be an art (rather than a science) and was primarily used in military and diplomacy
- Two major developments and scientific achievements changed the scene forever
  - In the late 1940s, Claude E. Shannon proposed **information theory** to argue about the secrecy of encryption systems
  - In the 1970s, Whitfield Diffie and Martin E. Hellman proposed the use of one-way functions to implement **public key cryptography** (prior work was done at the Government Communications HeadQuarters in the UK)

1. Introduction

1.3 Historical Background Information

- Since the early 1990s (and the rise of the Internet), there has been a wide deployment and massive commercialization of cryptography
- Many companies develop, market, and sell cryptographic techniques, mechanisms, products, and services
- There are cryptography-related conferences (e.g., hosted by the IACR) and trade shows (e.g., RSA conferences)
- The field fastly evolves and there are many use cases and applications for cryptography
- This includes **post-quantum cryptography (PQC)**

1. Introduction

1.3 Historical Background Information

- There is a lot of snake oil
- Warning signs (due to Bruce Schneier)
    - Pseudo-mathematical gobbledygook
    - New mathematics
    - Proprietary cryptography
    - Extreme cluelessness
    - Ridiculous key lengths
    - One-time pads
    - Unsubstantiated claims
    - Security proofs
    - Cracking contests

1. Introduction

1.3 Historical Background Information

- There are products that are worse than snake oil
  - Spyware
    - State trojans
    - Pegasus (NSO Group, 2021)
  - Backdoored standards and products
    - Crypto Wars I, II (1990s), and III (ongoing)
    - DUAL_EC_DRBG (2013)
    - Cryptoleaks (2020)
    - ANOM (2021)
- Human skepticism remains important (→ Chapter 18)

Questions and Answers

Thank you for your attention