

Chapter 1

Introduction

This text is an introduction to *cryptology*, whose objective is to provide various aspects of security in electronic transactions. It consists of *cryptography*—the art of making secure systems—and *cryptanalysis*—the art of breaking them.

The text consists of two parts, entwined with each other. The modern part, with chapters numbered numerically, explains some of the basic systems used today and some attacks on them. The historical part, with chapters numbered alphabetically, recounts some inventions and episodes from the rich history of this subject, sometimes amusing, sometimes dramatic.

Chapters 2 through 5 explain some of the basic tools of modern cryptology, namely the AES and RSA cryptosystems and cryptography in groups and elliptic curves. While algebraic and arithmetic methods of cryptanalysis (factoring integers and computing discrete logarithms) are interwoven with these chapters, Chapter 6 deals purely with (Boolean) cryptanalysis. The next two chapters describe hash functions and digital signatures. Chapter 9 presents a core topic of modern cryptology: security reductions. Such a reduction usually shows that if some computational problem is hard, then the cryptographic system at hand is secure, since a successful adversary would perform a computationally infeasible feat. This allows the design of cryptographic systems that withstand any possible attack, not just the known ones. In fact, reductions of various types are a central tool in this text.

After discussing identification and authentication (Chapter 10), we come to more advanced topics: pseudorandom generation (Chapter 11), zero knowledge proof systems (Chapter 12), and lattice-based cryptography (Chapter 13). All these rely heavily on the concepts introduced in Chapter 9. Chapter 14 explains the power of quantum computers: if

they could ever be built to scalable size, they would presumably devastate most cryptosystems discussed here, with the possible exception of AES, some hash functions, and the lattice cryptosystem in Section 13.13.

Chapter 15 at the end presents a toolbox, mainly of methods from computer algebra, that will be known to many but can be looked up at the reader's convenience.

A holistic view of cryptology includes its rich history. The historical parts provide a glimpse at this, sometimes amusing, sometimes scary. Chapter A begins with a general introduction and goes on to discuss frequency analysis. Chapter B deals with classical group cryptography, but in additive groups that are useless for modern methods. Chapter C explains a remarkable piece of cryptanalysis, namely, that of Kasiski on the “unbreakable” Vigenère system. Will anyone designing unbreakable systems heed this message? The codebooks of Chapter D were a staple of cryptography for over five centuries. Steganography—which survives today in attempts at digital watermarks and copyright protection—and transposition ciphers follow in Chapters E and F. Chapters G and H introduce some designers and some users of cryptography, from the Middle Ages to the nineteenth century. The last two historical Chapters I and J explain successes of British cryptanalysis over German cryptography, in the First and Second (hopefully last) World Wars. These played a prominent role in history, presumably saving countless lives—of Britons, Germans, and others.

Cryptology has a distinguished history of brilliant ideas and tools, some of which are described in this text. But for over two millennia, it was essentially confined to the *black chambers* of secret services, diplomacy, and the military.

The Diffie-Hellman revolution in 1976 brought public-key cryptography into power, with their key exchange, RSA, and most of the systems discussed here. But even more important than the technical advance was the sociological one: all of a sudden, leading researchers in mathematics and computer science realized the wealth of fascinating and difficult scientific questions whose answers could contribute to cryptology. The field remains deeply rooted in computer science, mathematics, and electrical engineering, but it has matured into a discipline of its own.

How to use this text. This book is suitable for one- or two-semester courses for graduate or advanced undergraduate students in computer science and mathematics, and also for students in computer engineering or security with a mathematical inclination. The prerequisite mathematical facts are minimal and largely explained in the toolbox of Chapter 15. What is required is the mental acceptance that rigorous proofs are more

desirable than hand-waving plausibilities, and the ensuing drudgery (better: joy) of going through those proofs. The basic ideas, protocols, and facts of modern cryptography that are presented try to challenge those who enjoy the thrill of convincing themselves of a stated truth rather than those who are willing to take someone's (like this author's) word for it. This is underlined by the more than 240 exercises, some of which deeply challenge the student's understanding of the material. The fun generated in class is visible in the various contributions of students, duly acknowledged, to this text.

A ubiquitous predicament of a conscientious instructor is that on the one hand, one would like to teach all details including proofs, but on the other hand, the material is too rich to do this in the allotted time. The usual way out is to point to the relevant literature. This is ok for some bright students, but many are confused by different notations and an embedding into other material that is not relevant to the purpose at hand.

This text, based on lecture notes from the author's many courses on *the art of cryptography*, tries to alleviate this predicament by presenting as many details as possible. It is then easy to look them up if the lecture time is insufficient. The necessary exceptions to this quest for completeness are duly noted in the text. The author has taught one-semester introductory courses covering parts of the first nine chapters, namely, Sections 2.1–2.8, 3.1–3.5, 3.10–3.13, 4.1–4.8, 5.1, 5.3–5.6, 7.1–7.3, 7.6, 8.1–8.2, and 9.1–9.6. For a second course, one or two of the following topics are appropriate: Chapters 6 and 10, Sections 9.7–9.10 with the background of Chapter 11, and Chapters 12, 13, or 14. This can be supplemented by suitable sections that were previously left out. Furthermore, the historical Chapters A–J make up a nice course on the history of cryptology, with fewer mathematical challenges (if any) and appealing to a wider audience.

The quest for completeness in treating the protocols presented here entails, given any reasonable page limitation, incompleteness in the list of tools described. Some references for further reading are given, but even those do not aim at encyclopedic coverage. The text is largely structured in a linear fashion, whereby all prerequisites for certain material have been discussed previously. A natural exception is the toolbox of Chapter 15, which is used throughout the book.

Like most natural sciences, cryptology combines theoretical and practical aspects. In its theory, we have well-defined models, and claims are proven with mathematical rigor, under clearly stated assumptions.

An interesting new result usually either proposes a new direction or improves in a clear sense on previous results. Much of this text works within this framework. Some protocols such as AES and practical hash

functions seem—in principle—not amenable to such an analysis, but may still be deemed secure.

The vibrancy and attraction of this theory are largely due to its multitude of practical applications, of central importance in today’s digital world. The secure cryptosystems described here provide excellent building blocks for such applications. But beware! It is easy (and such has happened time and again) to build insecure systems based on secure sub-routines. There are many dangers outside of the models considered here: bad secret keys—from passwords stuck on a screen or handed to a fake website to RSA moduli with a common factor, virus-installed key loggers, fault attacks, attacks on the operating system (“cold boot”), denial of service, and many others.

However, this seems the best we can do at this time, and it is a comfort to have secure cryptographic building blocks which will thwart any attack in the standard computational model. Then one “only” has to worry about the mortar holding the blocks together, and unwanted entry into the system through a back door.

The origins. In this text, we use the word *cryptography* for the art and science of making cryptosystems, *cryptanalysis* for breaking them, and *cryptology* for both together. The words come from the Greek κρυπτός (kryptos), meaning *hidden* or *secret*, together with γράφειν (graphein) *to write*, λύσις (lysis) *solution*, and λόγος (lógos), which is *word*, *science*, and also has other meanings.

Webster’s dictionary defines cryptography as *the act or art of writing in or deciphering secret characters*, and also *secret characters or cipher, or a system of writing with them*. *Cryptology* is a *secret or enigmatic language*, or simply *cryptography*. *Cryptanalysis* is the *art or science of deciphering a code or coded message without a prior knowledge of the key*. The word *cipher* comes from the Arabic صفر (sifr) *zero*, from صَفَر (safara), *to be empty*. One of its meanings is *a secret or disguised manner of writing meant to be understood only by the persons who have the key to it; a code; also, the key to such a code*.

Thanks. Martina Kuhnert, Daniel Loebenberger, and Konstantin Ziegler have contributed substantially to the production of this book, always in a cheerful and supportive manner. Many thanks for help in many ways go to Michael Nüsken, and other present and former members of my research group: Raoul Blankertz, Jérémie Detrey, Nihal Dip, Laila El Aimani, Michael Heußen, Claudia Jakob, Cláudia Oliveira Coelho, Dejan Pejić, Alexander Pfister, Yona Raekow, Deniz Sarier, Ayush Sharma, Jamshid Shokrollahi, Damien Vergnaud, and Marianne Wehry.

The work was supported by the B-IT Foundation and the Land Nordrhein-Westfalen.

I am indebted to David Kahn, Pascal Paillier, and Igor Shparlinski for substantial insights into various aspects of cryptography, and also to the other instructors at our annual `crypt@bit` summer school: Joan Daemen, Max Gebhard, Gary McGuire, Dennis Hofheinz, Marc Joye, Alexander May, Phong Nguyễn, Valtteri Niemi, Kenny Paterson, Chris Peikert, Bart Preneel, Charles Rackoff, Vincent Rijmen, Gadiel Seroussi, and Hoeteck Wee. I am also grateful for help on various matters to Frank Bergmann, Klaus Lagally, Sihem Mesnager, and Werner Schindler.

I owe my introduction to the subject to some “early” cryptographers, including Shafi Goldwasser, Russell Impagliazzo, Mike Luby, Silvio Micali, and Charlie Rackoff, whose presentations and courses in the 1980s opened a new field for me.

The *Notation* section towards the end of this book explains some of the symbols used. The web page <https://cosec.bit.uni-bonn.de/cryptoschool/> of the book contains additional material and corrections if necessary (sigh). Readers are encouraged to send their comments to the address on that web page.

Bonn, July 2015
Joachim von zur Gathen



The *Characters* used to express *Numbers* by are either ...
The Ten Numeral *Figures* of the *Arabians*:
... 0 *Nothing or a Cypher*.
WILLIAM JONES (1706)

Real mathematics has no effects on war.
No one has yet discovered any warlike purpose
to be served by the theory of numbers as relativity,
and it seems very unlikely that anyone will do so for many years.
GODFREY HAROLD HARDY (1940)

It may well be doubted whether human ingenuity can construct
an enigma of the kind which human ingenuity may not,
by proper application, resolve.
EDGAR ALLAN POE (1843)

There is, the cryptographic experts assure us,
no unbreakable cipher.
RICHARD WILMER ROWAN (1934)

It is extremely probable that an insoluble cipher
could be produced by mathematical means today.
FLETCHER PRATT (1939)

[The NSA's stranglehold on cryptography] ended abruptly
in 1975 when a 31-year-old computer wizard
named Whitfield Diffie came up with a new system,
called 'public-key' cryptography, that hit the world of cyphers
with the force of an unshielded nuke.
STEVEN LEVY (1993)

Solange ein Wissenszweig Überfluß an Problemen bietet,
ist er lebenskräftig; Mangel an Problemen bedeutet
Absterben oder Aufhören der selbstständigen Entwicklung.¹
DAVID HILBERT (1900)

¹As long as a branch of science offers an abundance of problems, so long it is alive; a lack of problems foreshadows extinction or the cessation of independent development.

CryptoSchool

von zur Gathen, J.

2015, XII, 876 p. 186 illus., 97 illus. in color., Hardcover

ISBN: 978-3-662-48423-4