Modern Cryptography Primer

Czesław Kościelny • Mirosław Kurkowski •
Marian Srebrny

Modern Cryptography Primer

Theoretical Foundations and Practical Applications

Springer

Czesław Kościelny
Faculty of Information Technology
Wrocław School of Information Technology
Wrocław, Poland

Mirosław Kurkowski
Inst. of Computer and Information Sciences
Czestochowa University of Technology
Czestochowa, Poland
and
European University of Information
Technology and Economics
Warsaw, Poland

Marian Srebrny
Institute of Computer Science
Polish Academy of Sciences
Warsaw, Poland
and
Section of Informatics
University of Commerce
Kielce, Poland

ISBN 978-3-642-41385-8 ISBN 978-3-642-41386-5 (eBook)
DOI 10.1007/978-3-642-41386-5
Springer Heidelberg New York Dordrecht London

Library of Congress Control Number: 2013955235

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Preface

For centuries, the need to ensure confidentiality of some gathered or transmitted information got a lot of attention in various political or military contexts. Nowadays, in the era of a general necessity for privacy, and the conscious awareness of one's rights to it, cryptography is found useful in a wide range of practical applications. For the most part, it is used for securing confidentiality in interpersonal computerized communication. The turn of the 21st century is sometimes called the Internet age, computer era; communication takes place instantly and without hindrance. Obviously, no one can imagine the functioning of various types of communication and telecommunication networks without the appropriate security measures against undesirable listening in on our information.

Modern cryptography would not exist without solid mathematical foundations, especially in number theory. The recent and most advanced security algorithms are built on such arithmetic constructs as integer arithmetic divisibility, modulo operations, prime numbers, or the Euler function.

Today's societies depend to a large extent on computers which process huge amounts of information, often transferred via telecommunication networks, and stored in databases. This information often needs adequate security protection against being read by unauthorized users of computer systems and networks, particularly illegal users. Cryptography provides economical means that enable this protection. The experts in cryptography work on more and more efficient methods of ensuring the secrecy of information and electronic documents which require it. Striking advances in the proliferation of electronic data storage, linkage, and transmission have created significant new challenges in maintaining confidentiality and developing adequate methods of authentication. The ambition of cryptanalysis and cryptanalysts is to break the security codes and forge encrypted messages in such a way that they look authentic.

Until quite recently, cryptography was applied only in the area of military forces and diplomacy. This is also why cryptographers usually worked in agencies dealing with state security, and all research work concerning cryptography, as well as cryptanalysis, was classified. It was not until the late 1960s that a multinational group of scholars, who were not controlled by security agencies, became interested in the

problems of cryptology and started to publish their research papers on this subject, thanks to which cryptographic data protection was found useful also in various civilian fields. The new paradigm requires that the cryptographic algorithms be publicly known, whereas only the private keys must be secret. Nowadays, the public access to the algorithms is treated as a safeguard of their security, assurance that there are no flaws due either to poor, unprofessional work by their designers or to deliberate insertion of so-called hidden backdoors (e.g., collecting copies of private keys).

Cryptographic methods are the most efficient ways of secure protection of modern telecommunication network users against computer break-ins, which have by now become a plague. That is why business promotes the use of cryptography since a basic requirement for worldwide economic growth is the development of secure worldwide computer networks underlying the information society economic infrastructure. In this context, possible administrative limitations on the use of cryptography are considered responsible for a substantial decline in a country's attractiveness in the eyes of foreign investors. Cryptographic security means are inevitable in order to improve trading and legal proceedings in the electronic economy, as well as to ensure at least the minimum of civil privacy and freedom.

The aim of this book is to introduce the currently most interesting and most important issues of modern applied cryptography in the technological practice of telecommunication networks, along with the necessary basic mathematics. Cryptography is an area on the edge of mathematics and practical software engineering. Like no other, it combines immense, challenging unsolved mathematical problems with the issues of authentic use in practical security tools in currently deployed vital data communication systems.

We present all the best known and most often used technologies, algorithms and protocols, and methods of their design and analysis. The algorithms are presented in readable pseudocode; i.e., written in English with some mathematical or programming symbols, or simple graphics and diagrams. We will not go into details on finding implementation bugs or methods of program engineering depending on the features of a particular programming environment, specification and implementation in any favorite programming language.

We bring particular attention in this book to performance analysis of the presented algorithms and protocols because since the late 1980s efficiency has essentially become the central concept to understanding modern cryptographic mechanisms, their usage, and many related problems, especially the problems of breaking the codes.

There are many very good publications on the market devoted to cryptography and/or its usage. However, only very few of them can serve as course textbooks. The material they present seems to us either extensively broad or too narrow for a graduate course, often too mathematical, and therefore very difficult for the majority of student readers with no deep mathematical background.

This book is written at the level of a graduate lecture course textbook for students of any technical university in the European Union or North America. As prerequisites it requires only some very basic elementary mathematical experience in algebra, number theory, probability, data structures, as well as the design and efficient

analysis of algorithms. The material presented in the book can constitute a one-year graduate course, as well as providing material for shorter courses on selected topics to be used without the need to search other parts of the book. Each chapter contains all the necessary background information concerning the problems being discussed. Selected chapters can constitute a reasonable basis for further studies of the subject, e.g., in the form of seminar or term credit papers, etc. The references provided will definitely be of help in completing such tasks. For the same reason, this book can be treated as a useful source of information in the field of data and network transactions security for practitioners and researchers just after their studies.

Today's cryptography is a very broad and lively field. We are aware that many areas need much broader treatment. For example, the elliptic curve algorithms, quantum cryptography, secret sharing, and various cryptanalytic techniques. Cryptographic hash algorithms are limited in this book to signaling the basic approaches and challenges, with no coverage of the most recent very interesting advances. These areas have got a lot of attention in the last few years, with many different methods and their own challenges. These topics will be covered in full detail in our follow-up textbook to appear soon.

This book consists of nine chapters discussing today's actual practice in applied cryptography from the very basics to strong state-of-the-art security algorithms and protocols.

The first chapter introduces the basic concepts of cryptography. The general diagram of encryption/decryption, as well as the notion of a cryptographic algorithm and the definition of cryptographic keys are discussed. The rules for building strong cryptographic codes are introduced. The chapter also presents the fundamental notions of theoretical and practical computational complexity, and discusses its meaning for determining the difficulty of breaking cryptosystems. Next, we introduce codes known from history such as Caesar's ancient code, and Playfair and Enigma, which were applied during the World Wars.

Modern cryptography would not exist without solid mathematical foundations, therefore in Chap. 2 we recollect and present mathematical concepts and properties required for continuing the course. Elements of the theory of algebraic structures, as well as elements of number theory, are presented. Also, we present simple arithmetic algorithms applied in cryptography. The chapter ends with a discussion on currently applied algorithms for testing integer primality, and computationally hard problems in number theory.

In Chap. 3 the most important symmetric ciphers are presented, among them the standards of symmetric encryption applied in widespread practice today. The DES (Data Encryption Standard) algorithm, its modifications and modes of operation are given and discussed in detail. A lot of attention is focused on the most recent American standard for symmetric cipher, the AES (Advanced Encryption Standard) algorithm. The IDEA algorithm, as well as the algorithms of the RC family are presented. As an interesting detail illustrating the resistance of encryption algorithms against attempts to break them, we present the process of the global competition in breaking RC algorithms, and the results.

In Chap. 4 the reader will find exact descriptions of asymmetric algorithms, beginning with the Diffie-Hellman scheme, through the ElGamal algorithm. Next, the

well known RSA algorithm, and various issues concerning unceasing attempts to break it are discussed. An interesting detail is the discussion on the results of the RSA factorization challenge, illustrating the cryptographic power of the RSA code.

Chapter 5 presents one of the most important modern applications of cryptography, namely the electronic signature. The general scheme, as well as several of the currently most essential and most interesting applied algorithms for generation and verification of the validity of e-signature are covered. We present various algorithms of digital signature and hash functions. We discuss the current issues concerning the usage of these functions, and their security.

In Chap. 6 the reader will find the exact description of the popular cryptosystem PGP (Pretty Good Privacy). The overall scheme of the system and the algorithms used in it are surveyed. The installation and the usage of PGP are described, encryption and signing documents (messages, e-mails, files) among others. In this chapter, the authors introduce other, non-commercial solutions enabling the application of strong cryptography by any computer user.

Chapter 7 is devoted to the public key infrastructure as a solution enabling application of the electronic signature for business and legal proceedings in the form required by legislation in most countries. The role of the so-called trusted third party in contemporary solutions, as well as the issues concerning certification of cryptographic keys, are presented.

Another important feature of cryptography in day-to-day reality is the cryptographic protocols applied often in mass scale in all kinds of communication via computer networks, especially for entity authentication and preventing identity theft. The goals to be achieved by the cryptographic protocols, as well as their examples, are presented. Issues and problems of their specification, design and application, methods of complexity analysis as well as methods of verification of correctness, and the security of cryptographic protocols are introduced and covered more broadly than in any other textbook available so far.

In Chap. 9 the remaining aspects of the application of cryptography in data and transaction security are taken up. The problems and solutions of preserving the secrecy and privacy of electronic mail, as well as secure exchange of documents in electronic form are discussed. The commonly applied SSH (Secure SHell) and SSL (Secure Socket Layer) protocols are also studied.

Like every book, ours is surely not flawless. In case of any errors, mistakes or inaccuracies in this publication, we would appreciate if the reader could kindly submit them to us via e-mail at cryptobook@icis.pcz.pl. Any feedback will be appreciated. In return, we promise an up-to-date list of corrections, a constantly revised corrigendum.

Our thanks for help and support in various stages of the process of writing and editing this book are due to many of our friends and collaborators, as well as our students, audience and participants in lectures and seminars given by each of us. Our special thanks must be given to Professor Leonard Bolc (1934–2013) of the Institute of Computer Science of the Polish Academy of Sciences, without whose kind and gentle but tenaciously ongoing systematic encouragement this book would most definitely never have come into existence. Very special acknowledgments go

to Professor Andrzej Borzyszkowski for his fruitful cooperation on the early versions of the materials for the chapter on the security protocols, their specification and verification of correctness. Similarly to Maciej Orzechowski. The third author gratefully acknowledges many useful conversations and discussions with Professors Paweł Morawiecki, Stanisław Spież, and Jerzy Urbanowicz (1951–2012). The latter was entirely responsible for dragging the third author in a friendly manner into the world of cryptologic research and practice, and for educating him on the field's special beauty and problems, splendors and shadows. The first author acknowledges support from Wrocław School of Information Technology. The second author acknowledges support from Czestochowa University of Technology and the European University of Information Technology and Economics, Warsaw. We would also like to thank Kasia Grygiel, Gosia Berezowska, Ewelina Gajek and Janek Jay Halicki for their help in the preparation of the English version of our book. Last but not least, the authors thank the copyeditor for his excellent careful work, and Springer's Ronan Nugent for successfully and nicely driving us through the whole editorial and production process.

Poland
August 2013

Czesław Kościelny
Mirosław Kurkowski
Marian Srebrny

Contents