Mathematics Study Resources 4

Olaf Manz

Encrypt, Sign, Attack

A compact introduction to cryptography

Springer

Mathematics Study Resources

This series comprises direct translations of successful foreign language titles, especially from the German language.

Powered by advances in automated translation, these books draw on global teaching excellence to provide students and lecturers with diverse materials for teaching and study.

Olaf Manz

Encrypt, Sign, Attack

A compact introduction to cryptography

Springer

Olaf Manz
Worms, Germany

ISSN 2731-3824 ISSN 2731-3832 (electronic)
Mathematics Study Resources
ISBN 978-3-662-66014-0 ISBN 978-3-662-66015-7 (eBook)
https://doi.org/10.1007/978-3-662-66015-7

This Springer imprint is published by the registered company Springer-Verlag GmbH, DE, part of Springer Nature.
The registered company address is: Heidelberger Platz 3, 14197 Berlin, Germany

Preface

Have you ever wondered whether mobile phones can be used to confide even the most secret secrets? Or whether online banking is really secure these days? Or whether an electronic signature on contracts sent by e-mail meets legal requirements? All of this has something to do with the **encryption –** or **ciphering –** of data, which is sent or stored on data carriers every day in large and ever-increasing quantities via data highways or "wireless".

Textbooks and reference books take a more scientific approach to the topic of data encryption under the title of **cryptography.** They deal with the mathematical theories of the common procedures, describe their algorithms and program-technical realizations, and also deal with many topics of the organizational implementation. As a basis for lectures or seminars, it must in the first instance be the goal to introduce students to scientific work and to introduce them to areas of current research. Practitioners working in the subject also need a correspondingly comprehensive presentation. On the other hand, there are also numerous popular science publications that aim at a generally understandable level. This works very well in this case, since simple ciphering methods can easily be brought to the attention of interested laymen and can be substantiated with examples from everyday practice. The mathematics behind it, however, usually remains hidden.

This book aims to be a balancing act between the two. It is a fact that cryptography can be understood quite comprehensively with very little mathematics. Our goal is therefore, without a theoretical superstructure, to deal specifically with the most important procedures of **encryption, signing** and **authentication,** and to present them in a compact and mathematically understandable manner, which is reflected in many practical examples.

- We focus first on symmetric ciphers, where anyone who knows the cipher procedure can decode it. The procedures go back to antiquity to the **Caesar cipher,** in which each letter in the alphabet is replaced by the letter three places further down. The **Vigenère cipher** from the sixteenth century does this much more subtly, while more modern methods such as the **Triple DES** (Data Encryption Standard) and especially today's standard method **AES** (Advanced Encryption Standard) are considerably more complex.

- But how is it supposed to work that you can encrypt but can't decrypt even with the help of the biggest and most modern computers? The keyword is **public key.** We will learn about the standard methods: **RSA** relies on the difficulty of decomposing large natural numbers into factors, and **Diffie-Hellman** and **ElGamal** exploit the problem that "discrete logarithms" cannot be computed efficiently enough. Here, we even run into "elliptic curves" with **ECDH.**
- Ciphering would certainly be unnecessary if there were not rogues and especially also professional attackers who would expect political, military or economic advantage from the knowledge of secret data and therefore try to "crack" the encryption. In addition to classical attacks using **statistical analysis** and **Friedman's coincidence index,** we learn about **Pollard's** methods for effectively factorizing large natural numbers to potentially "crack" RSA. Finally, we also attack the "discrete logarithm" with **Baby-Step-Giant-Step** and **Pohlig-Hellman**.
- Particularly fatal, however, is an attack in which an unauthorized person not only passively listens in but also actively engages in the message traffic and changes it in their own way. In this case, the recipient of a message is completely unaware of whether the information received in this form really originates from exactly the sender specified. In order to prevent this situation, **digital signatures** are used, for example the **RSA, DSA** or **ECDSA** procedure, thus giving a **man-in-the-middle attack** no chance.
- Of course, we will always deal with practical applications. Historically interesting are, for example, the **Illuminati** cipher and the **Enigma** machine. The **Internet** with **HTTPS** is perhaps the most prominent modern application for secure data transmission, but wireless **WLAN** networks and the **Bluetooth** radio interface are also well protected today. The **PGP Pretty Good Privacy** method is widely used for **e-mails**, while **mobile communications** with **GSM** are only partially secure against eavesdropping, but those with **UMTS/LTE** are much more secure. Another focus is on **online banking, credit cards** and **Bitcoins.** Finally, **e-passports** with their biometric data are also designed to be forgery-proof. Last but not least, data stored on **hard disks**, and thus **passwords** in particular, must be protected against unauthorized access.

The target audience for this book is basically anyone who is enthusiastic about the topic; in particular, it is also intended as an introduction to more advanced literature. We will have to do relatively little, but nevertheless some mathematics. We will need arithmetic with binary numbers (bits) and with remainders modulo a natural number, as well as an understanding of permutations, both for the conceptual background and for one or the other formal derivations. However, we will build this up piece by piece, with special emphasis on the plausibility of the relationships. So, let's plunge into the adventure – and have fun.

As a guide, here is a brief reading guide for the four chapters of this book in advance:

- Chapter 1 is intended as a "warm up", with an overview of important historical ciphers.
- Chapter 2 examines **symmetric ciphers S** (standard methods: **Triple-DES** and **AES**). These cipher procedures depend on a parameter to be kept secret, the so-called **key k,** with the help of which decryption can also be performed. Thus, participant **T** encrypts a secret message **m** as follows:
  - **S**(**m**, **k**).
- But how does participant **T** deliver the comparatively short key **k** to the authorized recipient of the secret message **m,** also by secret means? Chapter 3 introduces the concept of **public-key ciphers E** (standard methods **RSA, (EC)DH, ElGamal**). In these methods, which however require much more computation time than symmetric ciphers, one cannot decrypt **e** from the knowledge of their **key** alone. Participant **T** therefore encrypts **k** using **E** and sends the concatenation as a whole:
  - **E**(**k**, **e**)‖ **S**(**m**, **k**).
- But wait: How can the recipient be sure that the received message really comes from participant **T** in exactly this form? In Chap. 4, this problem is solved by means of **digital signatures sig** (standard methods **RSA, (EC)DSA**). Participant **T** signs the message **m,** more precisely a **digital fingerprint h**(**m**) of **m** (standard procedure **SHA**), and additionally sends the signature **sig**(**h**(**m**)) in the following concatenation:
  - **E**(**k**, **e**)‖ **S**(**m** ‖ **sig**(**h**(**m**)), **k**).
- Sometimes, however, a more conventional method, the **checksum MAC**, is used as an alternative to the digital signature (standard procedures **CBC-MAC, HMAC**):
  - **E**(**k**, **e**)‖ **S**(**m** ‖ **MAC**(**m**), **k**).
- Before sending a secure message, participant **T** usually has to log on to a system (e.g., mobile phone, computer network, bank server) and legitimize himself. As explained at the end of Chap. 4, this can be done "classically", for example by entering a PIN or password, but also with the aid of modern **public key** procedures and in particular with a **digital signature**:
  - **T** ►… **E**(**k**, **e**)‖ **S**(**m** ‖ **sig**(**h**(**m**)), **k**).

Worms, Germany Olaf Manz

Contents