

Preface

Computers are indispensable in today's world and many individuals spend substantial amounts of time using them. Most users consider the computer a tool for communications (email, Web browsing, and file transfers) and entertainment (playing games, listening to music, and watching movies). However, when the first modern electronic computers were developed, during and after World War II, their designers had other applications in mind. They were interested in a fast, reliable calculating machine to solve immediate practical problems such as creating and breaking secret codes, constructing accurate firing tables for cannons, and simulating complex physical processes such as weather forecasting and nuclear reactions. Thus, cryptography is one of the oldest computer applications.

Cryptography is the stuff of spy novels, action comics, and thriller movies. Some of us may remember how as kids we saved up bubble-gum wrappers to send away for Captain Midnight's secret decoder disk. On television and in the movies we commonly watch a nondescript gentleman in a gray flannel suit carrying a briefcase, presumably full of secrets, handcuffed to his wrist.

And what about you, gentle reader, sitting in your office, trying to email a confidential company memo to a colleague; a common, boring, but responsible task. You have to guarantee that your coworker is the only recipient of the message, you want to be sure that the recipient has actually received it, and is convinced that you, and no one else, were the sender. Considering how easy it is to intercept email messages, and taking into account the sophistication of computer hackers and commercial spies, sending this memo is no trivial task. If you are like most, you use cryptography. Specifically, you use a modern cryptographic technique to encrypt your message with the recipient's public key on your computer and you send it directly from your computer to its destination. The recipient has a private key to decrypt the message.

Cryptography is an old science (some may consider it an art). The timeline following the appendixes lists developments in this field since 1900 B.C.. Today, these developments are considered *classical cryptography*. With the advent of the computer in the mid twentieth century, new cryptographic methods have been developed that are referred to as *modern cryptography*.

One of the earliest computers, the Colossus, was built in England during World War II for the specific purpose of deciphering German military codes. Early in the war, the German military used the Enigma machine to encrypt messages. The story of the Enigma and how its code was broken is told in Chapter 5. Later in the war, the British discovered that the Germans had started using another cipher, dubbed the Lorenz, that was far more complex than the Enigma. Breaking the Lorenz code required a sophisticated machine, a machine that could perform statistical analyses, data searching, and string matching, and that could easily be reconfigured to perform different operations as needed. Max Newman, one of the mathematicians employed in Bletchley Park on breaking the Enigma code, came up with a design for such a machine, but his superiors were convinced that constructing it, especially during the war, was beyond their capabilities.

Fortunately, an engineer by the name of Tommy Flowers had heard about the idea and believed that it was workable. He worked for the British Post Office in North London, where he managed to convert Newman's design into a working machine in 10 months. He finished the construction and delivered his machine to Bletchley Park in December 1943. It was called Colossus, and it had two important features; it was completely electronic, using 1500 vacuum tubes and no mechanical relays, and it was programmable. It used paper tapes for input and output. Today, the Colossus is one of several candidates for the title "the first modern electronic computer," but for a long time it was kept secret.

After the war, Colossus was dismantled, and its original blueprints destroyed by Flowers obeying government instructions. This is why for many years, others were credited with the invention of the modern computer.

Cryptography is important and popular because it scrambles our data, making them unreadable and thereby providing privacy. There is, however, another approach to privacy. Data can be *hidden* instead of being encrypted. Data hiding, also called *steganography*, is different from cryptography but achieves the same goal, namely privacy and security of our data.

This book is about keeping data private, which is why it covers classical cryptography, modern cryptography, and steganography. Each of the three topics is illustrated and explained by presenting and describing various methods and techniques.

Modern cryptographic methods are mathematical and are based on concepts such as binary numbers, the modulo function, prime numbers, factoring large numbers, and permutations. Yet I believe that when this material is presented with an adequate introduction to each topic and with enough examples, anyone with even a little exposure to mathematics and computer algorithms can grasp the main ideas. The use of mathematics is kept to a minimum and the stress is on examples, diagrams, and clear descriptions. Instead of trying to be rigorous and prove every claim, the text often says "it can be shown that ..." or "it can be proved that"

An important feature of the book is the exercises, which are generously sprinkled throughout. Most of them encourage the reader to better understand a topic by doing

<p>Cryptography is the mathematical consequence of paranoid assumptions.</p>
--

<p>—Unknown</p>

a bit of work. The rest tempt the reader to try to come up with a new idea or a novel principle. It is important to try to work out the exercises, but the answers are provided and can always be consulted as a last resort.

- The Introduction tells the story of the Zimmermann telegram to illustrate the effect secret codes and code breaking can have on important historical events. The main terms used in this field, such as cryptography, cryptanalysis, and steganography, are defined. The Introduction continues with a discussion of Kerckhoffs' principle which claims that the important part of a secret code is not the encryption algorithm but the cryptographic key. The Introduction concludes with a list of important cryptographic resources.
- Chapter 1 discusses monoalphabetic substitution ciphers, where each symbol is replaced by another symbol and the replacement (substitution) rule does not vary. Section 1.2 illustrates how a knowledge of the letter frequencies of a language can be used to break a monoalphabetic cipher. Section 1.4 discusses the Polybius monoalphabetic cipher, Section 1.6 explains the Playfair cipher, and Section 1.7 introduces homophonic substitution ciphers.
- Chapter 2 is devoted to transposition ciphers. Such a cipher replaces the entire alphabet with a permutation of itself. The topics covered in this chapter are transposition by turning template (Section 2.3), transposition with a key (Section 2.4), and the two-step ADFGVX cipher (Section 2.6).
- Polyalphabetic substitution ciphers are the topic of Chapter 3. In such a cipher, the substitution rule is varied each time a character is encrypted. The main encryption methods covered in this chapter are the Trithemius cipher (Section 3.4), the Vigenère cipher (Section 3.5) and how it was broken, the index of coincidence (Section 3.17), and Polybius's polyalphabetic cipher (Section 3.16).
- A polyalphabetic substitution cipher can be made absolutely secure through the use of a one-time pad based on random numbers, so Chapter 4 is a survey of random numbers, methods for generating both true and pseudo-random numbers, and statistical tests for randomness.
- The last word in encryption, before the computer age, was mechanical (or electromechanical) rotor encryption machines. Chapter 5 is devoted to these machines, specifically to the most famous of them, the German Enigma. The principles of rotor machines are explained, followed by a discussion of the Enigma, its history, principles of operation, and how its code was broken before and during World War II.
- Chapters 6, 7, and 8 discuss modern cryptography. Both symmetric-key and public-key encryption methods are discussed, with emphasis on block ciphers and stream ciphers.
- Does the future belong to quantum cryptography? This question is the topic of Chapter 9, where the principles of this esoteric field are explained.

x Preface

- Steganography, the topic of Chapters 10 through 12, represents a different approach to privacy. Instead of being encrypted, the data are hidden. These chapters include an overview of steganographic techniques and descriptions of many methods for embedding data, watermarks, and fingerprints in text, image, video, and audio files.
- The appendixes present auxiliary material such as convolution, hash functions, cyclic redundancy code (CRC), and finite fields.
- Both a cryptography timeline and a glossary of important terms follow the appendixes. The former provides a bird's-eye view of the main stages in the development of cryptography, while the latter is a summary of important terms.
- The index caters to those who have already read the book and want to locate a familiar item, as well as to those new to the book who are looking for a particular topic. I have included any terms that may occur to a reader interested in any of the topics discussed in the book (even topics that are just mentioned in passing). As a result, even a quick glancing over the index gives the reader an idea of the topics and subtopics included in the book. A special effort was made to include full names (first and middle names instead of initials) and dates of all persons mentioned in the book.

Currently, the book's Web site is part of the author's Web site, which is located at <http://www.ecs.csun.edu/~dxs/>. Domain name BooksByDavidSalomon.com has been reserved and will always point to any future location of the Web site. The author's email address is dsalomon@csun.edu, but it is planned that any email sent to [\(anyname\)@BooksByDavidSalomon.com](mailto:(anyname)@BooksByDavidSalomon.com) will be forwarded to the author.

Consumer electronics maker JVC and games developer Hudson Soft say they've found a way to fight CD-ROM software piracy.

The companies said Wednesday they've developed a new anti-copying technology, called "Root," that they claim will prevent CD-ROM discs from being duplicated. The technology is just one part of the computer industry's ongoing efforts to control software piracy.

The Root technology—which prevents illegal copying “from the roots up,” the company says—uses encryption keys, an established method of protecting data. The technology encrypts a disc's contents so it cannot be read without a key, which is also located on the disc. The key is hidden in such a way that it can be read by any CD-ROM drive, but cannot be written by a CD-R/RW drive—so that a copied version of the disc would be unreadable. The key is different for each disc and is hidden in a different place each time.

From Cnet news.com August 29, 2002, 4:01 PM PT

Audience, level, and treatment—a description of such matters is what prefaces are supposed to be about.

—Paul R. Halmos, *I Want To Be A Mathematician* (1985)

Northridge, California

David Salomon

Data Privacy and Security

Salomon, D.

2003, XIV, 465 p. 45 illus., Hardcover

ISBN: 978-0-387-00311-5