大学计算机教育国外著名教材系列（影印版）

PEARSON
Prentice Hall

CLASSICAL AND CONTEMPORARY CRYPTOLOGY

经典密码学与现代密码学

Richard J. Spillman 著

Pearson Education

清华大学出版社

大学计算机教育国外著名教材系列（影印版）

Classical and Contemporary Cryptology

经典密码学与现代密码学

Richard J. Spillman

Pacific Lutheran University Tacoma, WA

清华大学出版社
北京

图书在版编目(CIP)数据

经典密码学与现代密码学 = Classical and Contemporary Cryptology/(美)斯皮尔曼(Spillman, R. J.)著. —影印本. —北京：清华大学出版社，2005.7
(大学计算机教育国外著名教材系列)
ISBN 7-302-11156-1

Ⅰ.经…　Ⅱ.斯…　Ⅲ.密码—理论—高等学校—教材—英文　Ⅳ.TN918.1

中国版本图书馆 CIP 数据核字(2005)第 058945 号

出 版 者：清华大学出版社　　　地　　址：北京清华大学学研大厦
　　　　　http://www.tup.com.cn　邮　　编：100084
　　　　　社 总 机：010-62770175　客户服务：010-62776969
印 刷 者：北京市清华园胶印厂
装 订 者：三河市新茂装订有限公司
发 行 者：新华书店总店北京发行所
开　　本：148×210　印张：9.375
版　　次：2005 年 7 月第 1 版　2005 年 7 月第 1 次印刷
书　　号：ISBN 7-302-11156-1/TP·7372
印　　数：1~3000
定　　价：23.00 元

出 版 说 明

进入21世纪，世界各国的经济、科技以及综合国力的竞争将更加激烈。竞争的中心无疑是对人才的竞争。谁拥有大量高素质的人才，谁就能在竞争中取得优势。高等教育，作为培养高素质人才的事业，必然受到高度重视。目前我国高等教育的教材更新较慢，为了加快教材的更新频率，教育部正在大力促进我国高校采用国外原版教材。

清华大学出版社从1996年开始，与国外著名出版公司合作，影印出版了“大学计算机教育丛书(影印版)”等一系列引进图书，受到国内读者的欢迎和支持。跨入21世纪，我们本着为我国高等教育教材建设服务的初衷，在已有的基础上，进一步扩大选题内容，改变图书开本尺寸，一如既往地请有关专家挑选适用于我国高等本科及研究生计算机教育的国外经典教材或著名教材，组成本套“大学计算机教育国外著名教材系列(影印版)”，以飨读者。深切期盼读者及时将使用本系列教材的效果和意见反馈给我们。更希望国内专家、教授积极向我们推荐国外计算机教育的优秀教材，以利我们把“大学计算机教育国外著名教材系列(影印版)”做得更好，更适合高校师生的需要。

清华大学出版社

Preface

The goal of this book is to introduce you to the fascinating world of cryptography. It is a multifaceted world—for some, it is a world of spies and secrets. For others, it is a world of mathematics and computers. Anyway you look at it, cryptography has an air of mystery and adventure. It also transcends traditional academic disciplines. It is not just a computer-science topic—the study of cryptography involves history, political science, engineering, languages, military science, ethics, mathematics, and technology. No single text could cover cryptography from all these perspectives, so the true student of cryptography must be prepared to develop a broad educational background. This book will only serve as the starting point for a long and satisfying search for knowledge and understanding of this very complicated, yet rewarding, topic.

Two overall principles guided the writing of this book. The first is that cryptography did not begin with the invention of the computer. While contemporary ciphers are all computer based, they owe a lot to the early work of the developers of classical ciphers. These developers had to work by hand using paper and pencil to discover weaknesses in the classical ciphers. Without the aid of a computer or even a calculator, they had to train their minds to recognize patterns and to organize data. Hence, to learn how to "think" like a cryptographer, you need to understand and appreciate the cleverness and patience that underlie the classical systems.

The second guiding principle is that a course in cryptography is not (and should not be) a programming course. While it may be helpful for students to write one or two programs that implement a cipher or an analysis tool, the time it would take learning how to write and debug code for all the important ciphers and tools would significantly reduce the time available to learn the real substance of cryptology. The task of writing cipher programs should be part of an algorithms or programming course. Hence, this book comes with a software package, Cryptographic Analysis Program (CAP), that provides access to both classical and contemporary ciphers. It also contains a set of tools for the analysis of those ciphers. The combination of the text and the software will give you real hands-on experience.

Beginning students, hobbyists, and advanced students should find something worthwhile in this text and its accompanying software program, CAP. Part One covers classical issues in cryptography and is a good place for those new to the field to begin their study. More advanced students may want to quickly scan this part for information on running CAP and perhaps spend more time on those classical ciphers or analysis techniques that are unfamiliar. Part Two covers contemporary ciphers including stream, block, and public key systems. This is the section that the more advanced students will find most useful. Part Three considers the future of cryptography and provides a short introduction to quantum systems. The world of quantum computing is so strange that it challenges our view of how the universe operates. This section is really for those who can abandon all common sense, be they beginning or advanced students.

There is a Web page for this book, which can be found at http://www.plu.edu/~spillmrj. (Follow the CAP pointers.) It contains a set of PowerPoint® files which are designed for lectures. Instructors also have access to answers to the problems in the book as well as additional problems and test questions.

The single most unique feature of this text is the accompanying software package, CAP. Together, CAP and the text are designed to create a complete learning environment. As you read about a particular cipher system, CAP allows you to explore the operation of that system. As you study an analysis technique, CAP allows you to experiment with it. CAP implements 30 different ciphers following a standardized interface so that once you become familiar with the implementation of one cipher you can easily run all the ciphers. CAP also provides a wide range of analysis tools that allow you to test the resistance of most CAP ciphers to cryptanalysis and to discover weaknesses that may be exploited in those ciphers. The usefulness of CAP is reflected in the problems at the end of each chapter. The problem sets are unique and, at times, challenging because they rely on your access to CAP. Above all, CAP is fun. It comes with a game feature so you can continue to test your cryptographic skills after you complete the text material. The CAP website (previously referenced) will contain additional challenges and post readers' high scores (if you will send in your game scores).

I hope you find the study of cryptography as interesting and rewarding as I found the writing of this book.

RICHARD J. SPILLMAN
Pacific Lutheran University,
Tacoma, WA

Contents

Chapter 1

Introduction to Cryptology

1.0 INTRODUCTION

We live in an exciting, fast-paced world and nothing is changing faster than the way we deal with information. Using the Internet, we can access and use information in ways that we never even dreamed of just a few years ago. Rather than going to the bank and standing in line waiting for a teller, we can pay bills, write checks, and shift money between accounts from home, 24 hours a day, 7 days a week. We can apply for and receive approval for loans without ever leaving home. We can buy books, food, gifts, and just about anything else over the Internet. Instead of running a garage sale in our front yard on a weekend, we can sell anything at anytime over the Net. We can buy and sell stock. We can post information for others to read and find information on just about any subject. With the advent of wireless technology, we can do all this and more from almost any location on earth using a cellular phone.

Sure, these are exciting times, but they also have a down side. The same technology that makes life so much easier has the potential to destroy our lives when used by criminals. For example, identity theft is one of the fastest growing crimes in the United States today. It thrives because the legal penalties have not caught up with the effects of the crime, besides the fact that it is easy to do. This is because most of the information "out there" about individuals is not protected. To enjoy the benefits while avoiding the pitfalls of new technology, we must have some method of protecting our identity and our personal information. How this can be done is precisely the subject matter of this book. It is about "secret writing," which has been around for centuries, but has now become a vital force for protecting and nurturing the growth of information technology. The field is called cryptography.

Cryptography is the study of codes and ciphers. David Kahn, in what has to be called the "bible of cryptography," defines it as follows: "Cryptology is protection. It is to that extension of modern man—communications—what the carapace is to the turtle, ink to the squid, camouflage to the chameleon." It is centuries old yet it remains fresh, new, and exciting. It is a field that is constantly changing and discovering new challenges. As a result, this is more than just a dry textbook only covering topics of interest to computer scientists and mathematicians. It is also a book that delves into history, political science, language, military tactics, and even games. It covers a body of knowledge that has secretly shaped the world in which we live.

1.1 CRYPTOGRAPHY

This book is a soap opera in some ways. It is the story of three people: Alice, Bob, and Eve. (These are the three names traditionally used by cryptographers to illustrate the principles of both cryptography and cryptanalysis.) It seems that Alice and Bob are constantly sending messages to each other. Eve, on the other hand, for reasons that are clouded in the past, wants to keep tabs on what Alice and Bob are saying to each other. Since both Alice and Bob are aware of Eve's intentions, they try as best they can to prevent Eve from discovering the content of their messages. This little soap opera is pictured in Figure 1.1.

The messages that Alice and Bob send to each other are called *plaintext* because they are readable by anyone. When they first started their correspondence, Alice and Bob sent each other their plaintext without any protection. However, they quickly discovered that if they did nothing to protect the messages, anyone, including Eve, could read them. So, as a result of Eve's reading their plaintext messages, Alice and Bob decided to hide the message contents in such a way that they could recover the plaintext, but Eve could not. This process of disguising a message in such a way as to hide its substance is called *encryption.* The encrypted version of the message is called the *ciphertext.* The process of recovering the plaintext from the ciphertext is called *decryption.* The encryption and decryption processes are determined by an algorithm and are controlled by a single key that only Alice and Bob share. Alice will use the key to encrypt her plaintext and then send the ciphertext on to Bob. Bob will use the same key to decrypt the ciphertext back into plaintext. If Eve intercepts the ciphertext, it appears meaningless to her because she does not have the key. This new process is illustrated in Figure 1.2.

The problem that Alice and Bob face is that Eve is both intelligent and determined. Once they try a particular encryption method, it is only a matter of time before Eve discovers a method to break the cipher. That is, Eve finds a way to either recover the plaintext

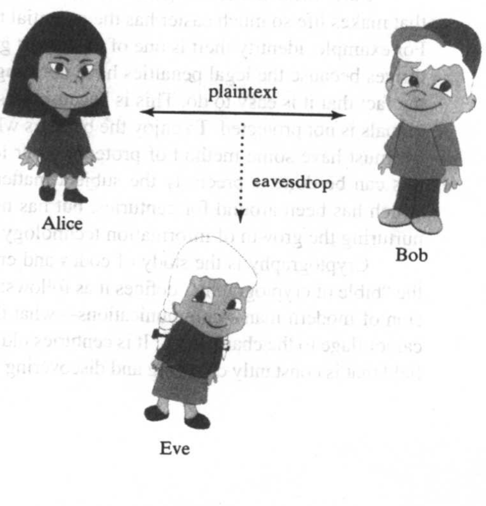

Figure 1.1: Typical communication model

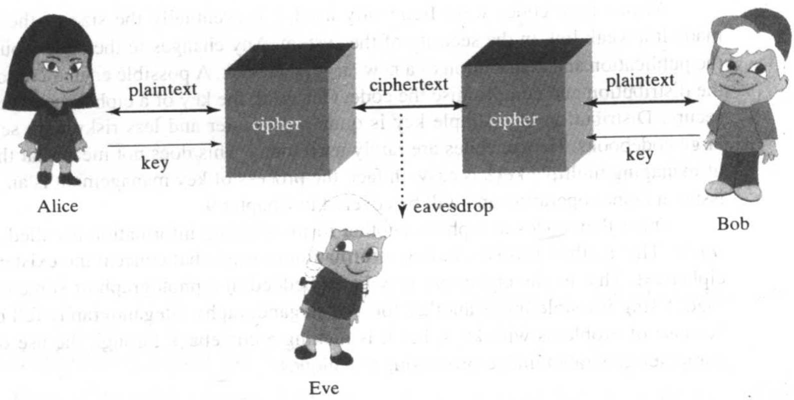

Figure 1.2: Typical communication model

without the key or a way to recover the key from the ciphertext. This forces Alice and Bob to try an even more complicated encryption method. So, the story of Alice, Bob, and Eve is a never-ending one. Alice and Bob are always trying to stay one step ahead of Eve, who is becoming increasing clever in her approach to breaking new ciphers. This book will allow you to follow this exciting story and watch as Alice and Bob develop new ciphers and Eve discovers new tools to allow her to break them. Before we can pick up the beginning of this story, however, it is necessary to define some basic terms.

1.2 IMPORTANT TERMS

Cryptology is the science (and to some extent the art) of building and analyzing different encryption–decryption methods. There are really two parts to this science. *Cryptography* is the science of building new more powerful and efficient encryption–decryption methods. This is the job of Alice and Bob. *Cryptanalysis* is the science of discovering weaknesses in existing methods so that the plaintext can be recovered without knowledge of the key. This is Eve's job. This book is about both subjects. You will learn how to protect data and how to discover weaknesses in current data-protection methods. Studying both processes will make you better at each. Understanding the different approaches to encryption will make it easier to detect weaknesses in specific ciphers. In addition, it is only through the understanding of cryptanalysis that you can ultimately judge the usefulness of any proposed encryption method. That is, every good cryptologist must spend some time in Eve's shoes in order to judge the security of their own favorite encryption algorithm.

An initial distinction must be drawn between *codes* and *ciphers* because sometimes they are mistakenly used to describe the same process. Both are methods used to hide information, but they do it in distinctly different ways. A code will substitute words, phrases, or numbers for plaintext. That is, the word "bomb" might appear in a message as the number sequence 1508. There is no algorithm or simple key that allows plaintext to be recovered from the codetext. The process of creating codetext or recovering plaintext requires a codebook that lists all the numbers (or substitution symbols) and their corresponding plaintext word, phrase, or letter. A cipher uses an algorithm and a key to hide information.

At one time codes were frequently used, but eventually the size of the codebook made it a weak link in the security of the system. Any changes in the code would require the publication and distribution of a new large codebook. A possible enemy could intercept the distribution and compromise the code. Changing the key of a cipher, however, is more secure. Distribution of a simple key is quite a bit easier and less risky than sending out large codebooks. Hence, codes are rarely used today. This does not mean that the process of managing multiple keys is easy. In fact, the process of key management is an important issue in cipher operation and will be covered in Chapter 9.

Other than codes or ciphers, another form of hiding information is called *steganography*. This method involves hiding information in ways that conceal the existence of the ciphertext. That is, the ciphertext may be embedded in a photograph or some other message. Using invisible ink is another form of steganography. Steganography fell out of use because of problems with keys, but it is making a comeback through the use of modern computer-generated image-processing techniques.

1.3 CIPHER EVALUATION

Throughout this book, the issue of what actually makes a good cipher will be continually explored. In part, you will learn what makes a good cipher by watching how Alice and Bob discover what works and what doesn't work as they continue to try to stay ahead of Eve. Each success on the part of Eve and each failure on the part of Alice and Bob will expose a weakness that will become a test for cipher quality. Each chapter will end with a summary of the current principles of good cipher design that can be derived from the plight of Alice, Bob, and Eve.

However, any discussion of what makes a good cipher must begin with the First General Principle of Cryptography—that is, it will always be assumed that ***the eavesdropper has knowledge of the underlying algorithm used to encrypt data***. This means that data are never secure just because the algorithm is new or unknown. Data are secure only if the key to the cipher algorithm remains secure. Never count on the hope that the enemy does not know how you encrypt your data. Always assume that they know every detail of the algorithm. This is sometimes called Kerckhoffs's law, and it is one of the six requirements of any cipher system that Flemish cryptographer Auguste Kerckhoffs listed in his 19th-century work *La Crypthographie Militaire*. All six are still considered to be fundamental to any cryptographic algorithm:

1. The system should be unbreakable in practice if not theoretically unbreakable.
2. Compromise of the system should not inconvenience the correspondents.
3. The key should be easy to remember without notes and should be easy to change.
4. The cryptograms should be transmissible by telegraph.
5. The apparatus or documents should be portable and operable by a single person.
6. The system should be easy, neither requiring knowledge of a long list of rules nor involving mental strain.

Claude Shannon devised another general evaluation concept in the late 1940s. He took the position that a good cipher will involve both *confusion* and *diffusion*. The confusion property means that the cipher should hide any local pattern—that is, any identifying characteristics of the language should be obscured by the cipher. The cipher should hide features of language that might give away the key to the cipher. The diffusion property requires that the cipher mix up different segments of the plaintext so that no character is left in its original position. Many of the classical ciphers that we will encounter early in this text fail on one or both of these properties. Often it is their failure to satisfy both of Shannon's conditions that allows them to be broken through the process of cryptanalysis.

As with most technologies, the evaluation of a cipher system all comes down to economics in the end. A cipher does not have to be "unbreakable" to be secure. (With one exception, it is doubtful that any cipher is truly unbreakable.) If the value of the information to be obtained is less than the cost of breaking the cipher, the data are secure. Or, if the time required to break the cipher is longer than the useful lifetime of the information, the data are secure. Hence, the ultimate security of any cipher is based on the principle that it is "more work than it is worth" to try and break it.

1.4 CRYPTANALYSIS

While Alice and Bob are faced with the challenge of creating a safe and secure cipher, Eve has to come up with ways to compromise their work. Eve will be attacking the intercepted ciphertext using all the tools and auxiliary information she can gather. This book will follow the exploits of Eve and teach you how to discover weaknesses in ciphers, which is the goal of cryptanalysis. However, it is important to understand that cryptanalysis is a classical double-edged sword. The knowledge you gain can be used for good or for evil. There are important reasons to learn about cryptanalysis—it is a necessary tool for the evaluation of new ciphers and it plays a vital role in preserving our national security. On the other hand, it can become a tool for compromising the privacy of others. Eve has no business attacking the communications between Alice and Bob. No matter how intelligent or skilled she appears to be, ultimately she is evil. You need to commit yourself to using the knowledge you gain to protect and not to harm.

There are three ways that Eve will attack the ciphers of Alice and Bob. The first is called a *ciphertext-only* attack. When all that Eve can get her hands on is the transmitted ciphertext, she will use any information she can gain from the ciphertext alone to try to produce the plaintext. The second is a *known-plaintext* attack. In this case, Eve has both the ciphertext and all or part of the plaintext available. Perhaps she has discovered that Alice and Bob always start or end their messages with the same sentence. Using this information and the ciphertext, Eve might be able to discover the key. Knowledge of the key for one set of plaintext–ciphertext may help her pry into other communications between Bob and Alice. The third is a *chosen-plaintext* attack. In this case, Eve has managed to influence the nature of the message between Alice and Bob. Perhaps she has given Alice some juicy information that she knows Alice will send to Bob. She has chosen the information so that the plaintext and the ciphertext have some important properties that make the job of discovering the key easier. Eve can use the information plus Alice's ciphertext to try and discover Alice's key.

Obviously, the ciphertext-only attack is the most difficult, while the chosen-plaintext attack is the easiest. Throughout this book, different ciphers will be compromised using one or more of these attack methods. As you learn how to break ciphers, it is important that you maintain a moral and ethical perspective. I understand that only a few paragraphs earlier this same subject was broached, but it is too important to leave to just one comment. There are only two good reasons to use cryptanalysis skills to break a particular ciphertext: for reasons of national security or to support law-enforcement efforts. Even then it should be done only with specific and lawful authority. On the other hand, there is very good reason to study the