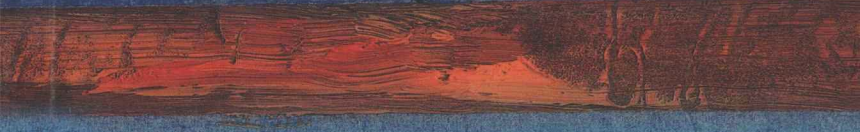
斑斓阅读 · 外研社英汉双语百科书系

密码术的奥秘

Cryptography

A Very Short Introduction

Fred Piper & Sean Murphy 著
冯绪宁 袁向东 译



外语教学与研究出版社
FOREIGN LANGUAGE TEACHING AND RESEARCH PRESS

斑斓阅读·外研社英汉双语百科书系

密码术的奥秘

Cryptography

A Very Short Introduction

Fred Piper & Sean Murphy 著
冯绪宁 袁向东 译

外语教学与研究出版社
FOREIGN LANGUAGE TEACHING AND RESEARCH PRESS
北京 BEIJING

京权图字：01－2006－6862

图书在版编目(CIP)数据

密码术的奥秘：英汉对照／(英)派珀(Piper, F.)，(英)墨菲(Murphy, S.)著；冯绪宁，袁向东译．— 北京：外语教学与研究出版社，2009.5
(斑斓阅读·外研社英汉双语百科书系)
书名原文：Cryptography: A Very Short Introduction
ISBN 978－7－5600－8588－3

Ⅰ．密… Ⅱ．①派… ②墨… ③冯… ④袁… Ⅲ．①英语—汉语—对照读物 ③密码—理论 Ⅳ．H319.4：TN

中国版本图书馆CIP数据核字(2009)第070709号

出 版 人：于春迟
项目负责：姚 虹 周渝毅
责任编辑：文雪琴
美术编辑：牛茜茜
版式设计：袁 璐
出版发行：外语教学与研究出版社
社 址：北京市西三环北路19号(100089)
网 址：http://www.fltrp.com
印 刷：北京市鑫霸印务有限公司
开 本：787×980 1/32
印 张：8.75
版 次：2009年5月第1版 2009年5月第1次印刷
书 号：ISBN 978－7－5600－8588－3
定 价：18.00元

* * *

物料号：185880001

Contents

目录

Chapter 1
Introduction

Most people seal the envelope before posting a letter. If asked why, then some immediate responses would probably include comments like 'I don't know really', 'habit', 'why not?' or 'because everyone else does'. More reasoned responses might include 'to stop the letter falling out' or 'to stop people reading it'. Even if the letters do not contain any sensitive or highly personal information, many of us like to think that the contents of our personal correspondence are private and that sealing the envelope protects them from everyone except the intended recipient. If we sent our letters in unsealed envelopes then anyone who gained possession of the envelope would be able to read its contents. Whether or not they would actually do so is a different issue. The point is that there is no denying that they would be able to if they wanted to. Furthermore, if they replaced the letter in the envelope then we would not know they had done so.

For many people the use of email is now an alternative to sending letters through the post. It is a fast means of communication but, of course, there are no envelopes to protect the messages. In fact it is often said that sending email messages is like posting a letter without an envelope. Clearly anyone wanting to send confidential, or maybe even just personal, messages via email needs to find some other means of protecting them. One common solution is to use cryptography and to encrypt the message.

If an encrypted message falls into the hands of someone other than its intended recipient then it should appear unintelligible. The use of encryption to protect emails is not yet particularly widespread, but it is spreading and this proliferation is likely to continue. Indeed in May 2001 a group of European MPs recommended that computer users across Europe should encrypt all their emails, to 'avoid being spied on by a UK–US eavesdropping network'.

Cryptography is a well-established science that has been a significant historical influence for more than 2,000 years. Traditionally its main users were governments and the military, although it is worth noting that *The Kama Sutra of Vatsyayana* contains a recommendation that women should study 'the art of understanding writing in cypher' (full details of all works cited are given in References and further reading).

The impact of cryptography on history is well documented. The tome on the subject is undoubtedly *The Codebreakers* by David Kahn. This book has over 1,000 pages and was first published in 1967. It has been described as 'the first comprehensive history of secret communication' and makes absorbing reading. More recently Simon Singh has written a shorter book called *The Code Book*. This is an easy-to-read account of some of the most significant historical events. It is not as comprehensive as Kahn's book, but is intended to stimulate the layman's interest in the subject. Both are excellent books that are highly recommended.

Credit for the popularization and increase in public awareness of the historical importance of cryptography is not restricted to literature. There are a number of museums and places of historic interest where old cipher machines are exhibited. High on the list of such venues is England's Bletchley Park, considered by many to be the home of modern cryptography and computing. It was here that Alan Turing and his team broke the Enigma cipher and their working environment has been preserved as a monument to their incredible achievements. Many recent films on the Second World

War have stressed the importance of code-breaking. Events that have received special attention are the impact of the breaking of the Enigma ciphers and the breaking of encrypted messages immediately prior to Pearl Harbor. There have also been a number of TV series devoted to the subject. All this means that millions of people worldwide have been exposed to the concept of encrypting messages to keep them secret and to the effect that breaking these ciphers can have. However, for many of them, the precise meaning of the terms used remains a mystery and their understanding is limited. The aim of this book is to rectify this situation by presenting a non-technical introduction to cryptology; the art and science of code-making and code-breaking. Readers will then be able to revisit these books, films, and TV series with extra knowledge which should make them more understandable and, as a result, more enjoyable.

Prior to the 1970s, cryptography was a black art, understood and practised by only a few government and military personnel. It is now a well-established academic discipline that is taught in many universities. It is also widely available for use by companies and individuals. There have been many forces that have influenced this transition. Two of the most obvious have been the move towards automated business and the establishment of the Internet as a communications channel. Companies now want to trade with each other and with their customers using the Internet. Governments want to communicate with their citizens via the Internet so that, for example, tax returns may be submitted electronically.

Whilst there is no doubt that e-commerce is becoming increasingly popular, fears about security are often quoted as being one of the main stumbling blocks for its complete acceptance. We have already focused on the problems associated with confidential information, but confidentiality is frequently not the main concern.

If two people are communicating over a public network and cannot see each other then it is not immediately obvious how either of them

can establish the identity of the other. However, it is clear that anyone receiving a message over a network may need to be able to convince themselves that they know the identity of the sender, and that they are confident that the message they have received is identical to the one that the originator sent. Furthermore, there may be situations where the receiver needs to be confident that the sender cannot later deny sending the message and claim to have sent a different one. These are important issues that are not easy to solve.

In traditional non-automated business environments hand-written signatures are frequently relied on to provide assurances on all three of these concerns. One of the main challenges that security professionals have faced recently is to find 'electronic equivalents' to replace the social mechanisms, such as face-to-face recognition and the use of hand-written signatures, that are lost in the migration to digital transactions. Despite the fact that there is no obvious relation to the need to keep certain information secret, cryptography has become an important tool in meeting this challenge. In a 1976 paper that was appropriately entitled *New Directions in Cryptography*, Whitfield Diffie and Martin Hellman proposed a way in which cryptography might be used to produce the electronic equivalent to the hand-written signature. It is impossible to overstate the impact of that paper. Prior to their work, cryptography was being used to make users confident that their messages had not been altered during transmission. However, it relied on mutual trust between the communicating parties. This was not a problem for the financial institutions, which were probably the main users in the 1960s and 1970s, but environments where it could be employed were certainly limited.

Modern cryptography has evolved considerably over the past three decades. Not only has the technology changed, but there is a wider range of applications. Furthermore, everyone is likely to be either a direct user or be affected by its use. We all need to understand how it works and what it can achieve.

Using this book

This book provides an introductory overview of cryptography. It is non-technical and is written primarily for the layman. Mathematicians and computer scientists who wish to study the technical aspects of cryptography are already spoilt for choice. The basic theory of the design and analysis of encryption algorithms is well documented and there are numerous textbooks on the topic. (We regard the standard reference as being the *Handbook of Applied Cryptography* by Alfred Menezes, Paul van Oorschot, and Scott Vanstone.) This book is not meant to be another. It is not concerned with the technical issues associated with algorithm design, but concentrates on how algorithms are used and what they are used for. If it inspires readers with suitable mathematical backgrounds to read more specialized technical textbooks then it will have achieved one of its objectives. However, its primary objective is to try to remove the mystique that surrounds cryptography and to remove the fear with which many non-mathematicians regard it.

This book is based on a course in the M.Sc. in Information Security at Royal Holloway, University of London. The course was called 'Understanding Cryptography' but its title has been changed to 'An Introduction to Cryptography and Security Mechanisms'. The interests and backgrounds of the students on the course are varied but most of them have ambitions to become practising security professionals including, for instance, IT security managers or security consultants. Most of them do not wish to become professional cryptographers. In fact they enter the course regarding cryptography as a necessary evil that must be endured in order for them to obtain an Information Security qualification. While we, the authors, cannot regard the subject as 'evil', it is certainly true that cryptography should be studied within the context of providing secure systems, rather than as an independent subject in its own right. It is this attitude that justifies the assertion that it is generally more important for security practitioners to understand key

management than to be able to analyse cryptographic systems mathematically.

For those who have no desire to be security professionals the aim of this book is to present cryptography as an interesting, important topic. It should enable the reader to understand the terminology in the numerous historical books and films on cryptography, and also to appreciate the impact cryptography has had on our history and is likely to have on our future. It should also facilitate understanding of the problems which the increased availability of cryptography causes for governments and law enforcement agencies.

There is little doubt that trying to break simple codes enhances one's understanding of cryptography. It can also be fun. So, although this is not a textbook, there are a number of 'exercises', in the sense that the reader is invited to break some algorithms. Failure to do so should not prevent the reader from completing the book. Nevertheless a serious attempt at solving them is probably worthwhile. The exercises are usually letter substitutions and solving the exercises requires no mathematics.

Despite the fact that there are essentially no mathematical prerequisites for understanding this book, there is no denying that modern cryptographic systems almost always involve mathematical processes. Furthermore most modern algorithms operate on binary digits (bits) rather than alphabetic characters. In recognition of this we include a short appendix to Chapter 3 with some of the relevant elementary mathematics. Once again readers are encouraged to try to understand them, but are assured that they are not crucial for the latter parts of the book.

Chapter 2
Understanding Cryptography

Introduction

In this chapter we introduce the basic terminology and concepts of cryptography. Our aim is to be informal and to give as general an overview as possible.

The basic concepts

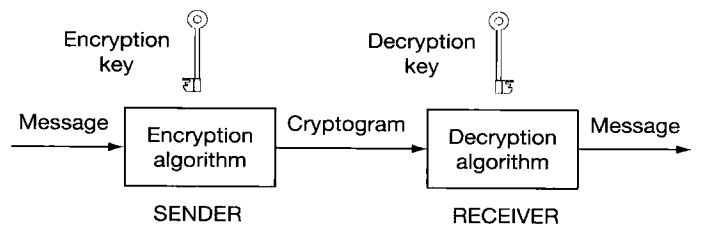
The idea of a cipher system is to disguise confidential information in such a way that its meaning is unintelligible to an unauthorized person. The two most common uses are, probably, to store data securely in a computer file or to transmit it across an insecure channel such as the Internet. In either scenario the fact that the document is encrypted does not prevent unauthorized people gaining access to it but, rather, ensures that they cannot understand what they see.

The information to be concealed is often called the *plaintext* and the operation of disguising it is known as *encryption*. The encrypted plaintext is called the *ciphertext* or *cryptogram* and the set of rules used to encrypt information plaintext is the *encryption algorithm*. Normally the operation of this algorithm depends on an *encryption key*, which is input to the algorithm together with the message. In order that the recipient can obtain the message from the

cryptogram there has to be a *decryption algorithm* which, when used with the appropriate *decryption key*, reproduces the plaintext from the ciphertext.

In general the set of rules that constitute one of these *cryptographic algorithms* is likely to be very complicated and they need careful design. However, for the purpose of this book, the reader may regard them as 'magic formulae' that, with the assistance of keys, transform information into an unreadable form.

The figure provides a diagrammatic description of the use of a *cipher system* to protect a transmitted message.



Any person who intercepts a message during transmission is called, not surprisingly, an *interceptor*. Other authors use different terms, including 'eavesdropper', 'enemy', 'adversary', or even 'bad guy'. However, it must be recognized that, on occasions, the interceptors may be the 'good guys'; more about them later. Even if they know the decryption algorithm, interceptors do not, in general, know the decryption key. It is this lack of knowledge that, it is hoped, prevents them from knowing the plaintext. *Cryptography* is the science of designing of cipher systems, whereas *cryptanalysis* is the name given to the process of deducing information about plaintext from the ciphertext without being given the appropriate key. *Cryptology* is the collective term for both cryptography and cryptanalysis.

It is very important to realize that cryptanalysis may not be the only means by which an attacker can gain access to the plaintext.

Suppose, for instance, that someone stores encrypted data on their laptop. Clearly they need to have some way of recovering the decryption key for themselves. If this involves writing it down on a piece of paper which they stick to the lid of the laptop, then anyone who steals the laptop automatically has the decryption key and has no need to perform any cryptanalysis. This is just one simple illustration of the fact that there is certainly more to securing data than using a good encryption algorithm. In fact, as we emphasize repeatedly, the security of the keys is critical for security of cryptographic systems.

In practice most cryptanalytic attacks involve trying to determine the decryption key. If successful, the attacker then has the same knowledge as the intended recipient and is able to decrypt all other communications until the keys are changed. However there may be instances where an attacker's sole objective is to read a particular message. Nevertheless when authors refer to an algorithm as being *broken*, they usually mean that an attacker has found a practical way of determining the decryption key.

Of course, the attacker is only able to break an algorithm if they have sufficient information to enable them to recognize the correct key or, more frequently, to identify incorrect keys. It is important to realize that this extra information is likely to be crucial to the attacker. Suppose, for instance, that they know the plaintext was English text, and that the decryption of some ciphertext using a guessed key does not give meaningful English plaintext. In this case, the guessed key must be incorrect.

One important fact that should already be clear from our introduction is that knowledge of the encryption key is not necessary for obtaining the message from the cryptogram. This simple observation is the basis of the seminal Diffie–Hellman paper. It has had a dramatic impact on modern cryptology and has led to a natural division into two types of cipher systems: symmetric and asymmetric.

A cipher system is called *conventional* or *symmetric* if it easy to deduce the decryption key from the encryption key. In practice, for symmetric systems, these two keys are often identical. For this reason, such systems are frequently called *secret key* or *one-key* systems. However, if it is practically impossible to deduce the decryption key from the encryption key, then the system is called *asymmetric* or *public key*. One reason for distinguishing between these two types of system should be clear. In order to prevent an interceptor with knowledge of the algorithm from obtaining the plaintext from intercepted ciphertext it is essential that the decryption key should be secret. Whereas for a symmetric system this necessitates that the encryption key should also be secret, if the system is asymmetric then knowledge of this key is of no practical use to the attacker. Indeed it can be, and usually is, made public. One consequence of this is that there is no need for the sender and receiver of a cryptogram to share any common secrets. In fact there may be no need for them to trust each other.

Although the statements made in the last paragraph may appear to be simple and self-evident, their consequences are far-reaching. Our diagram above assumes that the sender and recipient have a 'matching pair' of keys. It may, in practice, be quite difficult for them to reach this situation. If, for instance, the system is symmetric then there may be a need to distribute a secret key value before secret messages can be exchanged. The problem of providing adequate protection for these keys should not be underestimated. In fact the general problem of key management, which includes key generation, distribution, storage, change, and destruction, is one of the most difficult aspects of obtaining a secure system. The problems associated with key management tend to be different for symmetric and asymmetric systems. If the system is symmetric then, as we have seen, there may be a need to be able to distribute keys while keeping their values secret. If the system is asymmetric then it may be possible to avoid this particular problem by distributing only the encryption keys, which do not need to be secret. However it is then replaced by the problem of guaranteeing

the authenticity of each participant's encryption key, that is, of guaranteeing that the person using a public encryption key value knows the identity of the 'owner' of the corresponding decryption key.

When we were introducing the difference between symmetric and asymmetric systems we assumed that the attacker knew the algorithm. This, of course, is not always true. Nevertheless it is probably best for the designer of a cipher system to assume that any would-be attacker has as much knowledge and general intelligence information as possible. There is a famous principle of cryptography which asserts that the security of a cryptographic system must not depend on keeping secret the cryptographic algorithm. Thus the security should depend only on keeping secret the decryption key.

One of the objectives of studying cryptography is to enable anyone wishing to design or implement a cipher system to assess whether or not that system is secure enough for the particular implementation. In order to assess the security of a system we make the following three assumptions, which we refer to as the *worst-case conditions.*

(WC1) The cryptanalyst has a complete knowledge of the cipher system.

(WC2) The cryptanalyst has obtained a considerable amount of ciphertext.

(WC3) The cryptanalyst knows the plaintext equivalent of a certain amount of the ciphertext.

In any given situation it is necessary to attempt to quantify realistically what is meant by 'considerable' and 'certain'. This depends on the particular system under consideration.

Condition WC1 implies that we believe there should be no reliance on keeping details of the cipher system secret. However this does

not imply that the system should be made public. Naturally the attacker's task is considerably harder if he does not know the system used and it is now possible to conceal this information to a certain extent. For instance, with modern electronic systems, the encryption algorithm may be concealed in hardware by the use of microelectronics. In fact it is possible to conceal the entire algorithm within a small 'chip'. To obtain the algorithm an attacker needs to 'open up' one of these chips. This is likely to be a delicate and time-consuming process. Nevertheless it can probably be done, and we should not assume that an attacker lacks the ability and patience to do it. Similarly, any part of the algorithm that is included as software within the machine can be disguised by a carefully written program. Once again, with patience and skill, this can probably be uncovered. It is even possible that, in some situations, the attacker has the precise algorithm available to him. From any manufacturer's or designer's point of view, WC1 is an essential assumption, since it removes a great deal of the ultimate responsibility involved in keeping a system secret.

It should be clear that WC2 is a reasonable assumption. If there is no possibility of interception, then there is no need to use a cipher system. However, if interception is a possibility then, presumably, the communicators are not able to dictate when the interceptions takes place and the safest option is to assume that all transmissions can be intercepted.

WC3 is also a realistic condition. The attacker might gain this type of information by observing traffic and making intelligent guesses. He might also even be able to choose the plaintext for which the ciphertext is known. One 'classic' historical example of this occurred in the Second World War when a light buoy was subjected to a bombing attack merely to ensure that the distinctive German word *Leuchttonne* would appear in plaintext messages that were to be enciphered using the Enigma encryption machine. (See the BBC publication *The Secret War* by B. Johnson.)