Cryptography and Public Key Infrastructure on the Internet

Klaus Schmeh

Gesellsschaft für IT-Sicherheit AG
Bochum, Germany

Cryptography and Public Key Infrastructure on the Internet

Cryptography and Public Key Infrastructure on the Internet

Klaus Schmeh

Gesellsschaft für IT-Sicherheit AG
Bochum, Germany

Title of the German original: *Kryptografie und Publik-Key-Infrastrukturen im Internet.* ISBN: 3 932588 90 8

National 01243 779777
International (+44) 1243 779777
e-mail (for orders and customer service enquiries): cs-books@wiley.co.uk
Visit our Home Page on http://www.wileyeurope.com or http://www.wiley.com

Library of Congress Cataloging-in-Publication Data

(to follow)

British Library Cataloguing in Publication Data

A catalogue record for this book is available from the British Library

ISBN 0 470 84745 X
Translated and typeset by Cybertechnics Ltd, Sheffield
Printed and bound in Great Britain by Biddles Ltd., Guildford and Kings Lynn
This book is printed on acid-free paper responsibly manufactured from sustainable forestry
for which at least two trees are planted for each one used for paper production.

Contents

Foreword by Carl Ellison

Cryptography is variously a hobby, a pastime for children, a branch of mathematics, a tool for personal privacy, a hindrance for law enforcement or the salvation of media companies. It is also an area that has seen much conflict, often reported in the press. In the latter half of the 1990s, when the first edition of this book was published in Germany, the conflict was between law enforcement agencies and citizens who wanted to use cryptography for protecting their own privacy. More recently, the conflict has been between video, audio and software copyright holders, on the one hand, and cryptographers who choose to do research in the area of content protection, on the other. One would think they would work together, but part of research into cryptography is the breaking of cryptographic schemes of others, and legislative efforts in copyright protection try to make it illegal to perform and publish such breaks, threatening to bring research to a stop. We do not know yet how that conflict will be resolved, but when it is, we would be guilty of excessive optimism to assume that there will be no more conflicts over cryptography.

To some of us, cryptography is all in a day's work. To others it is a personal passion. To my average friend, cryptography is something intensely complex, somehow associated with spies and diplomats and clearly something impossible to understand.

Someday, strong cryptography may be so invisibly incorporated into everyday products that the average user would not need or want to understand it. Computer file system internals, networking protocols, SCSI bus commands, etc., are already in that category. They are details that the average user need never address. Even the average computer developer needs only a rudimentary understanding of such details.

That day is not yet at hand for cryptography. The US export rules have been relaxed and more engineers are using strong cryptography (although not always properly), but we are still at the beginnings of making the actual use of cryptography understandable and comfortable for the man in the street. If the end user of a computer system wants to use cryptography intelligently, then he or she will need to understand some of the details of this field.

To the student of cryptography, the field is no longer in its infancy, but neither is it in old age. Most likely it is in its adolescence: a time of growth spurts, identity crises, agonies over acceptance and a struggle to find its place in the mature world. This makes the present a time of real excitement for those of us developing and using cryptography and runs the risk of making it a time of great confusion for the average computer user.

Childhood

Cryptography's childhood was very long. David Kahn's history of cryptology [Kahn] follows its development for millennia. There was the potter 3500 years ago in Mesopotamia who invented and used a cipher in order to protect the secrecy of a new formula for glaze. There were the Hebrew scribes of the book of Jeremiah who used a cipher to hide various names. Medieval alchemists used ciphers to protect their secret formulas. Perhaps from association with the alchemists, cryptography in Europe acquired an aura of magic or even the occult. In India, on the other hand, the Kama Sutra listed cryptography among the 64 arts necessary for a well-rounded individual.

As David Kahn noted, 'It must be that as soon as a culture has reached a certain level, probably measured largely by its literacy, cryptography appears spontaneously – as its parents, language and writing-probably also did. The multiple human needs and desires that demand privacy among two or more people in the midst of social life must inevitably lead to cryptology wherever men thrive and wherever they write. Cultural diffusion seems a less likely explanation for its occurrence in so many areas, many of them distant and isolated' [Kahn, p. 84].

The examples over the years of uses of cryptography tend to be dictated by need. Those who needed to communicate securely at a distance, under the threat of interception, used cryptography for communications. These tended to be military and diplomatic personnel, tracing back to the ancient Greeks and Julius Caesar. Those, such as the Mesopotamian potter, who needed secure storage of information but who lacked the wealth to erect fortified buildings and hire guards, gave us examples of cryptography for storage. International bankers gave us examples of cryptography for authentication. These three areas continue to be relevant today and should be considered separately to be well understood.

Over the years, various inventions spurred rapid developments in cryptography. For the most part, these were the inventions that made communications easier and at the same time more easily intercepted: the telegraph, the radio and now the Internet.

One non-communication invention of the twentieth century has also spurred cryptographic developments, and appropriately so because it grew out of cryptography. That invention is the digital computer. The first digital computers were built to perform cryptanalysis during World War II. Now, of course, the computer is the enabling technology for the Internet, so it has crossed over into communications, but the biggest reason that it spurs development of cryptography is that cryptographic operations are inherently complex. Cryptographic operations

are designed to be intolerant of even the smallest mistake. Therefore, these complex operations must be executed perfectly. In the days before the computer, cipher clerks were hired to perform these mind-numbing tasks. Those clerks needed not only to be precise in their work; they also needed to be extremely trustworthy. This is clearly a job begging for a computer. A computer is not always flawless, but it easily beats a human in precision. A computer is not always trustworthy (if it is infected by a virus or plagued with bugs, for example), but it can be the total property of its user and the user is free to make his computer as trustworthy as it is humanly possible to do by locking it in a safe when it isn't being used, for example – something you would not do to a cipher clerk.

Adolescence

The knowledge of cryptography has always been generally available. With the invention of the personal computer, the cipher clerk is now also generally available. This opens up wonderful possibilities. Now, common everyday products can take advantage of the characteristics of cryptography, especially in the areas of authentication, fault tolerance, virus protection and privacy.

With all these possibilities has come public notice. Various law enforcement agencies expressed alarm over the possibility of widespread cryptography. Everyday communications of normal citizens had been laid bare by advances in technology (for example, the cellular telephone), and these agencies had taken advantage of their increased ability to eavesdrop. This ability amounts to power and an agency will preserve its power at all costs. A citizen needs to be aware of the realities of cryptography and its uses in order to be an informed voter and citizen when dealing with the issues of cryptography policy introduced by such agencies.

Another kind of notice has come from organizations and individuals pursuing money. Cryptography looks like a sure thing: something everyone will need, since everyone wants privacy. So, the number of product offerings and patents in cryptography is quite large. Here a citizen needs to be aware of cryptography just to be an informed buyer. Cryptographic products are especially prone to being described with inflated claims.

Today's uses

Today one uses cryptography to exchange 'secure' e-mail, to connect to a 'secure' web page, to use a virtual private network. There are new developments in the use of cryptography to permit a consumer to protect his or her personal data and resources, and hopefully to do so in a way that is simple to understand and easy to use correctly. We see developments using cryptography for Digital Rights Management and a corresponding policy debate over copyright law [Lessig]. There might also be legal actions involving cryptography – suing someone over a digitally signed message, backed by an open PKI – although that possibility looks more remote now than it did in 1998 because of the decline of PKI.

We don't know what will finally develop out of cryptography, but today's two principal classes of use are certain to remain: confidentiality and authentication. Confidentiality allows someone to encipher a message so that an intended recipient(s) can decipher it but no one else can. An intended recipient can be some other person, in which case we are dealing with communications, or it can be oneself at some time in the future, in which case we are dealing with enciphered storage. Authentication allows someone to prepare a message signature or MAC (message authentication code) by which to determine that the message has not been changed and that it originated with someone possessing the secret needed to make that signature or MAC.

Each of these areas of cryptography has witnessed a pitched battle in recent years.

Confidentiality

The battle over confidentiality generated much press coverage and inflamed deep passions. Does a citizen have the right to use cryptography to attempt to keep a secret from the government? If some government is to be permitted to overrule that citizen's right, then which government(s)? ... Germany, the USA, France, Russia, China? At the moment almost all governments have concluded that the citizens' needs for confidentiality are important for national security. However, in light of continual danger from terrorism, whose perpetrators are not localized in one physical country, there continues to be a desire to put entire populations under surveillance and confidentiality via cryptography might interfere with that surveillance.

As long as there are personal computers, compilers and cryptography books, the citizen will continue to have the ability to use cryptography no matter what controls are attempted. Will they continue to have the right?

This needs to be decided in appropriate political fora.

Authentication and authorization

The battle over authentication and authorization is different. There are battles of wills over privacy rights and over property rights. There is also a contest of definitions.

With regard to privacy, there rage debates between those who believe that all cryptographically authenticated remote operations should be backed up by a digital certificate revealing the user's identity and those who believe that one can authorize actions anonymously [Brands].

With regard to property rights, Digital Rights Management allows someone to attempt to enforce property rights in a way that was not available before, and from that ability comes unexpected consequences. Some DRM policies that can be and sometimes are specified violate provisions of copyright law (for example, 'fair use' provisions). Imagine a car that could read the current speed limit from the road, digitally, and absolutely enforced it. Our existing copyright law permits people to

use personal judgment and have the result adjudicated later. With DRM, rules are enforced by a mechanism with which one is not able to argue and which offers no room for personal judgment.

Perhaps more interesting is the contest over definitions.

Prior to the invention of public key cryptography, two people who wanted to communicate in secret had to have a secret key that only they knew. Given that shared key, not only would the two parties be able to communicate without fear of eavesdroppers, each party would know that an incoming encrypted message was from the other party. This provided a kind of authentication. For cases when privacy wasn't desired, there was developed a cryptographic operation yielding a MAC (message authentication code), in which the shared secret key was used with the message contents to produce a check value that could be made (or checked) only by someone having the secret key.

Since keys can be betrayed, these secret keys would have to be replaced by fresh ones periodically. Typically this was accomplished by use of a trusted courier, bringing keys from one party to the other. Then in 1976, Diffie and Hellman published the first practical public key cryptosystem, capable of securely delivering keys at a distance, over a non-confidential channel (although one that had to have integrity). In that paper, Diffie and Hellman proposed that one could replace trusted couriers with a kind of telephone book – except this telephone book would have a name and public key for each listed person. This telephone book would be a networked directory rather than a paper book, although one such paper book was actually printed [RJA Global Trust Directory]. To make it possible to operate when that directory was not available, Loren Kohnfelder proposed in 1978 that the line items from this directory be digitally signed and carried by the people who care about these entries. He called such a digitally signed line item a **certificate**.

The claim made by Diffie and Hellman was that if my key was in that directory, anyone could go to the directory and find my public key (via my name) and use my key to send me a message for my eyes only. What they overlooked was that names do not specify people uniquely. Granted, there may be some person who has a globally unique name, but John Smith is not one of those. A security system that works only for people who have globally unique names isn't very interesting. Nevertheless, there are digital signature laws in some countries and in some states of the United States that specify the legal meaning of digital signatures backed up by such certificates, and those laws assume that when a certificate binds a public key to a name, it is binding that key to a person.

Even though the names that serve us so well in our small communities in the physical world fall short for us on the net, we still need authentication and authorization. We need to know things about the people with whom we deal. However, the original assumption was wrong. We need more than just to trust the binding of a name to that other person. We need to know things about that person – usually not a name – and need to learn those facts from authorities on those facts. For example, the SET cardholder certificate provides a fact about a keyholder (permission to use a specific credit card), issued by the authority on that fact (the

bank issuing that credit card) without referring to the person's name. That certificate is used in the process of authorization (deciding if the keyholder is allowed to do something), not merely in establishing the name of that keyholder.

SET is just one example, from one limited (but important) area of daily life. SET looks unlikely to become ubiquitous but as more of our daily life moves to the Internet we will need to develop more such certificates and authorization procedures. These procedures in the physical world developed over centuries, by evolution in small steps. On the Internet, operating at 'web speed', the invention is likely to be in much larger steps and to have flaws with larger impacts. This calls for more people who can intelligently review such inventions.

The Internet is exciting. Relationships form, people fall in love, business is transacted, warfare is waged, and life in this world is just beginning to be developed. It is a new frontier for us, now that we have run out of dry land to explore. It is a land with its own rules. Some of those rules are disarmingly familiar while others are radically different. One thing we do know, however, is that cryptography will play a key role in many of these new rules and behaviors.

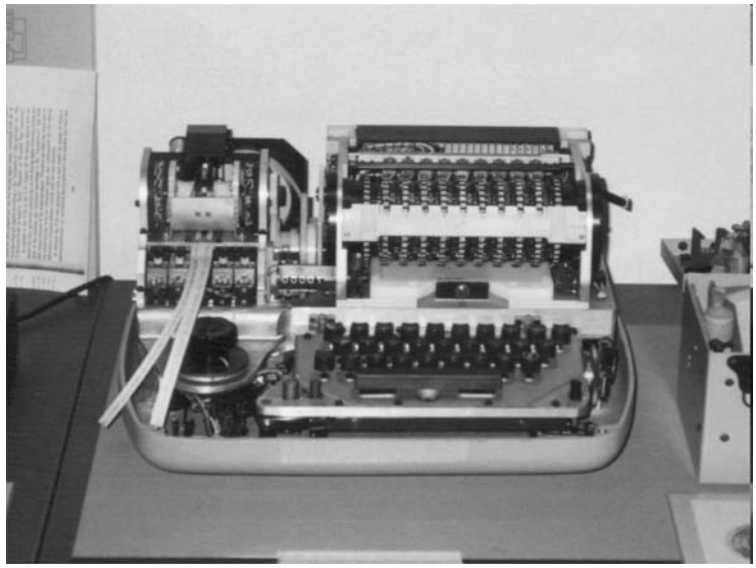
Happy exploring.

Carl Ellison
Portland, OR

Carl M. Ellison is a Senior Security Architect with the Corporate Technology Group of Intel Corporation. His current research is devoted to delegatable, distributed, public-key authorization. His concentration on security has been a side-effect of a more general career focus on the design of distributed and fault-tolerant systems.

Part 1

Why cryptography on the Internet?



Encryption machine HX-63, 1963 Model
(from the IT-Security Teaching & Study Collection of the BSI)

1

Introduction

If the automobile had followed the same development as the computer, a Rolls-Royce would today cost $100, get a million miles per gallon, and explode once a year killing everyone inside.
ROBERT CRINGELY

Key experience no. 1
In the mid-1990s, network-pioneer Bob Metcalf was one of the more important Internet-pessimists. When, during a lecture, he once again forecast the early collapse of the Internet, he let himself be drawn into making a bet: should his forecast not come true, then he would eat the manuscript of his lecture. Since no such collapse occurred in the meantime, Metcalf finally had to admit defeat. However, he dispensed with the pleasure of eating paper. Instead, while at a WWW Conference, he ate his words in the form of icing-sugar words piped on a cake.

1.1 If the Internet were a car ...

The development of the car was unlike that of the computer

A car for 100 US dollars, that needs filling up only once in its lifetime? According to Robert Cringely, such a super-car would have been a reality long since if the development of the automobile had proceeded at anything like the speed of computer development. Each new car model would have had twice the top speed of its predecessor, and even small cars would have a luggage compartment the size of a gymnasium. The glove compartment of a medium -class limousine would swallow the baggage for a two-week holiday without even a hiccup. Naturally, such developments would bring concomitant disadvantages. In the latter years, baggage size would have increased enormously and correspondingly. A simple shopping bag would long ago have reached the size of a single family house. Naturally, it would be especially annoying if pieces of luggage went missing as the result of a 'baggage compartment crash' before we had made a 'baggage compartment backup'. Equally exasperating would be the mandatory requirement to change the engine and all interior furnishings and fittings at frequent intervals.

The development of the car also differed from that of the Internet

In view of the scenario just described, it is perhaps just as well that car development did not parallel that of the computer. But does this conclusion also follow for the Internet ? If car development had followed that of the Internet then we would today have 60 mph motorways with 10-lane 3000 mph access roads. There would be no way of knowing whether the quickest way from London to Bristol was via Bath or via New York! The disappearance of a car without trace would be just as much an everyday event as an unpredictable change in the car's content. One of the worst consequences, however would be that someone could burgle a car travelling at full tilt down the motorway without the driver even noticing.

1.2 Security on the Internet

The Internet displays a considerable lack of security

The comparison with a car that can be burgled while travelling at top speed demonstrates at least one thing quite clearly: the Internet exhibits a substantial array of security failings. Naturally these stand in the way of serious commercial use. How is a bank supposed to offer online banking on the Internet if hackers cannot be prevented from gaining access to the accounts of others? How can business be conducted on an insecure Internet?

Such a lack of security is incomprehensible at first glance. Studying the history of the Internet, however, makes some things clear. The gaps in security are not unrelated to the fact that, for a long time, commercial use of the Internet was not even considered. For a few years the Internet was just a scientists' toy to which scarcely anyone gave a thought. Hardly anyone thought of making money on the network of networks. The Internet continued its cloistered existence until just a few years ago, when the monastery gates were flung wide open.

The Internet was not created for commercial use

What happened then astonished everyone. User numbers increased with explosive speed and the Internet became a mass medium. The '@' generation was born – honest citizens became 'netizens' and the verb 'to surf' gained a completely new meaning. However, not only home users were impressed by the Internet. Business enterprises also profited enormously from the new opportunities. A 'net' or 'com' in the company name was often the only necessary requirement to become a rising star on the Stock Exchange. In just a few years, firms such as Netscape and Amazon achieved growth that would have taken generations in other branches of industry. Internet euphoria was such that one might easily have imagined that the entire world would soon be completely carpeted with Internet cables.

The first Internet boom years are over

Today, some five years after the start of the big boom, we are again a bit further on. Rumours that years would soon be termed 'before the Internet' and 'after the Internet' have not been confirmed. In the industry, the euphoria of some enthusiasts has been replaced by the cool consideration of corporate enterprise decision takers, who ask themselves if, and how, cash can be wrested from the Internet. The investment favourites of the early days have become (pro tem?) the whipping boys of Stock Exchange investors. Internet users are no longer a

progressive elite, but people like you and me – even bowling clubs and local league football clubs have their own home page these days. Already, the first Internet Luddites have appeared, and hold themselves to be especially progressive because they want to know nothing more of this new technology. Meanwhile, the younger brother of the Internet, the intranet, has reached school age. But it is rumoured that the intranet is not the solution to all problems, but 'only' a useful tool.

The gold-rush mood on the Internet has calmed down

The gold-rush mood has thus cooled down. However, the boom is still not long past – on the contrary, the Internet is only at the start of its triumphal procession through our everyday life. A procession that will see online shopping, online banking, online apparatus control, and much more, taken for granted.

During the rapid development of the Internet from a scientists' toy to a mass communication medium, it is no wonder that security came a poor second. I have already mentioned that this is a disadvantage, in light of new applications like online trading and online banking. Security had therefore to be added later. Hackers and spies had to be prevented from playing their little games on the network.

Such a belated change in the design naturally comes with problems. Even after adding wings and enlarging it ten-fold, a car is still a car and not a jet-plane. Just as little can the Internet, which was not even designed to be a secure system, be transformed by some patchwork design measures into a suitable medium for confidential business letters, financial transactions or contract closures.

Security had to be built into the Internet belatedly

What therefore was to be done? Since the Internet could not be reinvented from scratch, the existing technology had to be amended. And so people tried to furnish the existing Internet with the corresponding additions and changes that would put a stop to the games of criminally-minded users. This process has now been going on for some years. It is still not finished by far, and will probably never be finished completely. Nevertheless, there has been progress, which has led to an increasing acceptance of the Internet for applications where security is critical.

It is possible to eavesdrop on the Internet

One of the largest dangers on the Internet arises from the fact that it is quite simple to tap into the data that flows through the network. The only way to counter these security gaps reliably is provided by a thousand-year-old science which, because of the present lack of security in computer networks, is experiencing an unforeseen boom: the science of data encryption, known also as 'cryptography'.

Cryptographic procedures were built into the Internet as an afterthought

In recent years, great efforts have been made to introduce cryptographic processes into the existing Internet. These efforts have given rise to so many methods that it is difficult to keep abreast of them. To enable you to find your way around the gigantic field of cryptography on the Internet, I have written this book, which describes the means that modern cryptography makes available, and how these are used on the Internet to confound hackers and snoopers. You will also learn why e-mails are encoded differently from Web pages, how money is transferred over the Internet, and at which points on the network encryption can apply. Naturally, I also tell you about encryption products – about those that have taken the Internet by storm, about others that flopped despite immense effort, and yet others that still have their future before them. Finally, mention must be made of government activities in the field, which often have the unfortunate goal of limiting the application of cryptography.

1.3 The second edition

The present book is a second edition

The book you hold in your hands is the second edition of this work. The first edition appeared in October 1998 under the name *Safer Net – Kryptografie im Internet und Intranet* (*Safer Net – Cryptography in the Internet and intranet*) [Schm98/1]. After the first edition sold encouragingly well, in mid-1999 I undertook a complete revision, which is now finished. As in the first edition, it has been my goal to write more than a dry reference book. Attractive presentation and reading enjoyment seem to me just as important as the factual content.

The first edition of the book evoked many positive comments

Reactions to the first edition were mostly positive. Again and again it was confirmed that a book about the practical side of cryptography on the Internet – and in particular a description of the numerous standards on the market – had been missing, and that my book closed this gap. Also, the idea of imparting technical knowledge through attractive presentation and readability was well received, as I was often informed. 'That Klaus Schmeh in his book *Safer Net – Cryptography in the Internet and intranet* actually succeeds in keeping boredom at bay for the reader lies in his easy writing style and the personal case examples', wrote *Card Forum* magazine. The magazine *Internet Professionell* rated *Safer Net* as a 'profound, well written and entertaining work covering all aspects of encryption'.

Critical comments, though happily rare, were naturally also in evidence. Most points of criticism concerned various themes that had been covered in insufficient detail, or even not at all. In some cases (such as S/MIME) criticism was surely justified; basically, however, a book such as this is always incomplete. Still, I have done my best to cover everything of importance in the new edition. Apart from the errors of omission in the first edition, there were naturally also some factual errors (for example, there actually is an Internet AG), numerous misprints, and various inconsistencies, mostly brought to my attention by attentive readers. Everyone who advised me on such failings is included in the list of acknowledgements at the end of the chapter.

This book covers a complex subject

Naturally, the task of writing a cryptology book has not become easier over the past two years. Much has happened since the deadline for the first edition, and an already complex theme has become even more complex.

In this second edition, I hope I can impart to you some of the fascination that cryptography can engender. This centuries-old art, to hide information from prying eyes, has become through the computer an even more fascinating science than it already was. It is waiting for you to discover. This book should be your gateway to it.

1.4 Why yet another cryptography book?

There are numerous other cryptography books on the market

Two years before the first edition of this book appeared, there were already numerous books about cryptography on the market. Naturally, others have appeared in the meantime. One could long ago have filled a whole library with books on this subject. Many may ask: is not the present book superfluous? Weren't

there already more than enough other works that treat everything of interest in the field of cryptography? My answer to this is 'no'. While the quality and quantity of the presently available books on cryptography leave a little to be desired (see Section 31.2), I still think that this book has its place in cryptographic literature.

This book should fill a gap

About three years ago I noted that there was still a gap in the cryptography book market. At that time there was no book that covered both cryptographic processes and their comprehensive practical application in computer networks. I felt that this was a big cap, for from my experience it was exactly this practical application that was of interest. To close this gap, I wrote the first edition of my book.

Two years after the appearance of the first edition, the gap in the market has become smaller (not only because of my book). Many aspects that I missed three years ago have been covered by other authors in the meantime. Thus, *Safer Net* appeared almost simultaneously with the book *Internet Cryptography* by Richard Smith, which likewise was concerned mainly with the application of cryptography on the Internet. Despite everything, numerous aspects are to be found in my book that readers will look for in vain in most other crypto books. Here is a selection:

The central theme of this book is the integration of cryptography in the Internet

- The central theme of the book, the integration of cryptography in the Internet, is treated here more comprehensively than in any other book I know. Terms like SSL, IPSec, PGPS, S/MIME, SET, HBCIS, DNSSec and many others are covered.
- Other cryptography books are concerned mostly with solutions. The problem – namely the susceptibility to hacking of the Internet and other networks – is mostly treated only peripherally.
- How cryptography can be integrated into the different OSI layers, and whether hardware or software is the right means to achieve it, is described in this book in detail.
- Smart cards are ideal for the implementation of cryptographic processes. Their importance is growing all the time. Nevertheless, smart cards are treated shabbily in most cryptography books – but not in this one.

Even biometrics is a subject in this book

- Biometrics is of course not part of cryptography, but there are numerous points of contact. These are described in this book.
- The theme of public key infrastructures (PKI) and Trust Centres continues to gain in importance, and is therefore treated especially comprehensively.
- Additionally, in this book you find a survey of the more important crypto publishers.
- I have placed particular value on readability and attractive presentation. So you certainly have anything but a dry reference book in your hands.

Reading enjoyment and attractive layout play an important role in this book

Long on words, short on content: I have tried not to write a book for the ivory tower. Instead, practical usability, easy intelligibility and, not least, readability have been given priority. By contrast, in other books you will find more cryptographic processes and more theory.

1.5 My regrets, my requests and my thanks

Constructive criticism of this book is welcome

Despite all our efforts, errors, inaccuracies or other defects will have crept into my book. This was true of the first edition and the second can hardly be different. This regrettable, but unavoidable, fact should be no reason for frustration, but rather an incentive: phone, write or e-mail your comments to me. I am grateful for each pointer, just as for any inspiration or criticism. Since there will surely be a third edition of this book, your communications will not land in the waste bin (and certainly not before I have read them conscientiously). Please send your comments to Wiley, or better still via e-mail to schmeh@wiley.com. In this way I gained dozens of valuable hints on the first edition, which have helped me greatly with the new version. Errata and additional information on the book are always available on the World Wide Web under the address www.dpunkt.de/buch/krypto.html.

Besides the author, many others have contributed to the success of a book such as this. At this point I would like to thank all those people most cordially, even if I cannot mention all of them by name. I offer particular thanks to the following people:

My thanks to numerous people

- Dr Michael Barabas of dpunkt.verlag for his support in the realisation of this book.
- Carl Ellison for his remarks on the themes of SDSI and SPKI, as well as for his outstanding foreword.
- Gerald Volkmann, Kai-Uwe Konrad, Susanne Gehlen, Marco Breitenstein, Matthias Niesing and Bernhard Esslinger for their comprehensive comments.
- Fred Fischer for his support in connection with the encoding machine photos.

I would also like to thank the following for their support: Jacques Basmaji, Dr Rainer Baumgart, Hans Joachim Bickenbach, H. Bork, Marco Breitenstein, Dr Jörg Cordsen, Dr Jean-Christophe Curtillet, Dr Frank Damm, Bernd Degel, Karsten Dewitz, Manja Diering, Hans Peter Dittler, Prof. Hans Dobbertin, Peter Ehrmann, Oliver Ferreau, Helge Fischer, Carsten Gäbler, Thomas Garnatz, Thomas Gawlick, Stefan Haferbecker, Dirk Heuzeroth, Frank Hoherz, Detlef Hühnlein, Robert Joop, Markus Jünemann, Robert Jung, Dr Wolfgang Kahnert, Paul Knab-Rieger, Andreas Knöpfle, Stephanie Kopf, Andreas Krügel, Willi Mannheims, Stefan Milner, Ilja Ohliger, Prof. Christof Paar, Peter Pahl, Sachar Paulus, Gunnar Porada, Holger Reif, Prof. Dr Helmut Reimer, Stefan Reuter, Thomas Rolf, Prof. Christoph Ruland, Matthias Sakowski, Tahar Schaa, Patrick Schäfer, Christoph Schlenker, Volker Schmeh, Dr Michael Sobirey, Jochen Stein, Malte Sussdorf, Dr Uwe Tafelmeier, Dr Hubert Uebelacker, Boris Ulrich, Rüdiger Weis, Dominik Witte, Reinhard Wobst, Oliver Wolf, Zeljko Zelic, Dr Volker Zeuner, Stephanie Zeutschler, Ursula Zimpfer.

2

What is cryptography and why is it so important?

There is no security, only more or less insecurity.
JOSEF MAIER

Key experience no: 2
One of the oldest known examples of the use of cryptography stems from 1500 BC. About that time a Mesopotamian potter used secret characters to record the formula for a glaze on clay tablets. Even as long as 3500 years ago, there were industrial secrets that had to be hidden from competitors.

2.1 The name of the game

This book is not just (but also) aimed at the expert

'What is cryptography?' Perhaps you asked yourself this as you read the title of this book. Or are you someone who already knows about it? This does not matter; my book is addressed to both groups and I think even the professionals will find something here for them. If you have already worked with a computer, if you know how many bits make a byte, and have already heard something about the Internet, you need not find this book too much of a challenge. As you will see, a little mathematics cannot be avoided, but I have tried to make that part as easy to follow as possible. If you are a professional cryptographer you can certainly bypass the first chapters, but when we come to standards, protocols and products you will hopefully find things that engage your interest. But enough of the preamble, let's get straight to the point and begin answering the question contained in the title: what is cryptography and why is it so important?

2.1.1 What is cryptography?

There are has two answers: one short and one long.

The short answer

Cryptography is the science of data encryption

Cryptography is the science of data encryption.

The long answer

Cryptography is the science concerned with methods of data protection through encryption and related processes. Given that mathematics is an important aid in cryptography, then only through mathematical knowledge and mathematical thought processes can it be possible to develop the procedures necessary for secure data encryption. The other important aid is the computer. It performs the encryption procedures and renders another important service by testing for weaknesses in cryptographic methods.

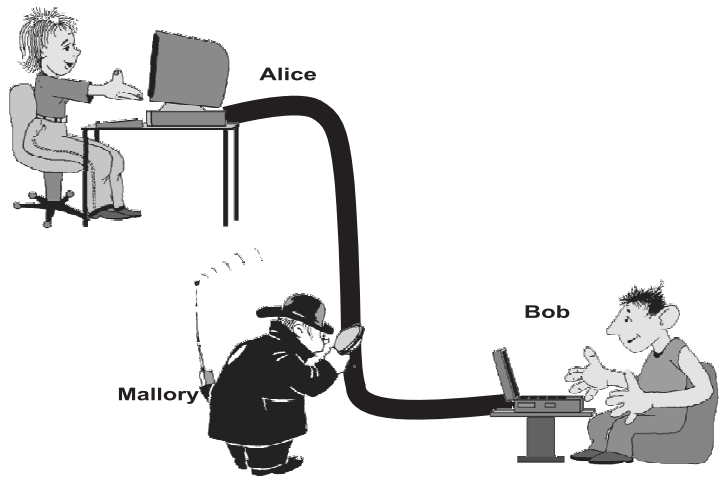


Figure 2.1 Alice and Bob exchange messages that Mallory can read and manipulate. This simple theme forms the basis of this book.

Alice and Bob are the main characters in this book

In cryptography in general, and in this book in particular, we start with a model that is as simple as possible: two people (let's call them **Alice** and **Bob**) exchange data over a channel that can be intercepted. In this book, the channel is usually the Internet, but sometimes it can be a phone line, a wireless radio connection, or a floppy disk being transported in someone's trouser pocket. What matters is that it should be technically possible to intercept the transmitted data, whether by tapping a phone line or stealing the floppy disk. In this book, 'intercept' should always be understood in a general sense. It can mean 'listen in on', 'read', or even 'analyse'.

The villain in this book is called Mallory

To keep our model as simple as possible, we will start from the worst-case assumption, that a villain (let's call him **Mallory**) can intercept and control the transmission channel at will. In our case then, Mallory can intercept, manipulate and retransmit the data that Alice and Bob exchange over the Internet in any way he likes. On the basis of this model, the use of cryptographic encryption and similar measures can preclude that

- Mallory can affect the intercepted data
- Mallory can change the transmitted data without it being detected
- Mallory might pretend to Alice that he is really Bob (and vice versa)
- Without being detected, Alice can claim that a message from her might in reality be a forgery by Mallory.

Mallory can intercept communications between Alice and Bob

Of course, Mallory can also do things that cannot be prevented by cryptographic means. Such things include that

- Mallory can change messages (only he cannot avoid detection)
- Mallory might intercept data (only it will be to little avail if the message is well encrypted)
- Mallory might block the line, bring down a router, or blow up a data processing centre (in which case he would scarcely be able to access any data).

You may well think that the prerequisites for this model are not always realistic. That someone might have the same possibilities as Mallory is, however, far more frequently the case on the Internet than you might suppose. Above all, it is mostly very difficult to estimate correctly the danger of eavesdropping. Therefore it has proven wiser to take Mallory into consideration from the start and to rate him as a very dangerous opponent, just to be on the safe side. If the dangers seem rather exaggerated to you, just wait until Chapter 3. There I will examine the danger of interception and manipulation more closely and show that it is actually a formidable problem. From the outset, therefore, we will bear in mind Murphy's first law of cryptography: Mallory is always more dangerous than you think (see also Section 32.5).

Mallory is always more dangerous than you might think

At this point I will take this early opportunity to throw the first definitions in this book at you. I have just described in detail what cryptography is. The word comes from the Greek, where *kryptein* means 'hide' and *gráphein* means write. Along with cryptography there is also **cryptanalysis**. This is concerned, not with the encryption, but with the decryption of data already encrypted.

Cryptology covers both cryptography and cryptanalysis

Both cryptography and cryptanalysis are contained within the term **cryptology**, which is thus the more commonly used term in the field. As so often happens, the use of such terminology is not uniform in this case either. Since cryptography is worthless without cryptanalysis, one does not normally distinguish between cryptology and cryptography. In this book also, cryptography includes cryptanalysis, and I am speaking here not about cryptology but about cryptography.

2.1.2 Cryptography – an important branch

Cryptography is a branch of computer security

Cryptography belongs to a branch of information technology called **computer security** or **IT security** (in this book usually termed **security**). Cryptography is hence widely connected since computer security is a very large field that embraces many branches. The theme of computer safety is closely connected with that of computer security. The two terms have the following meaning:

- Computer safety is concerned with the guarding against accidental damage. This covers technical defects, accidental deletion, transmission errors, hard disk crashes, lightning strikes, floods, bad servicing, faulty diskettes, and the like.

- Computer security is concerned with guarding against intentional damage. This includes hardware sabotage, hacker intrusion, peeking at secret data, and the like.

Networked computers present dangerous security problems

This book deals exclusively with security. Security can be further divided: first there is the area of the security of individual computers (regarded as isolated units or systems) and, secondly, the security of networked computers (this area is also termed **network security**). Naturally, the former are not in as much danger as the latter. Therefore, and because this is a book about the Internet, I will not go into isolated computers in any detail. We are much more interested in computers connected to a network (namely the Internet), which give rise to two security questions in particular:

- How can a networked computer be protected against an unauthorised person gaining access via the network (i.e. against **hacking** or **cracking**)?

- How can messages that leave the computer be protected against an eavesdropper or manipulator (Mallory in our case) (i.e. **communications security**)?

Cryptography can be regarded as a branch of network security

Now we have finally got to where we actually wanted to be: cryptography. This is of course the science of encryption and consequently an important tool in communications security. Suitable methods of encryption can be used to prevent Mallory from understanding or changing the data he intercepts. Of course, encryption also gives protection against hackers and crackers, if only as a last line of defence when other security measures have failed and an intruder has already gained unauthorised access to sensitive data. However, since this is much less important in practice than the protection of data during transmission, we shall treat cryptography in this book as a branch of communications security. Of course, at the back of your mind you should always keep the idea that encryption can be applicable to other areas.