Chapter 1

Introduction

We live in a world where information and its exchange play central roles, and yet it's only the beginning of the information age. It will become increasingly important to protect information which, in turn, requires knowledge in cryptology. **Cryptology** encompasses two fields: **cryptography**, which is, roughly speaking, the science of data protection by encryption, and **cryptanalysis**, which is the art of obtaining information on secret data without knowing the key. Though people have been dealing with cryptology for several thousands of years, it is still somewhat mystery-mongered. It is also a difficult field. First, every cryptologist needs to have sound mathematical knowledge. Second, a cryptologist is often hindered by the fact that he's either bound to confidentiality, or that research findings are kept secret. Cryptology still hasn't rid itself of its reputation of being a playground for national intelligence agencies, diplomats, and militaries, though it has meanwhile made its way into everyday use—think only of your bank card's PIN, or digital cell phones. On the other hand, for example in the United States up into the 1990s, good (secure) encryption algorithms had been banned from export. They were classified as 'ammunition'. In France, cryptography was thought of as the second most dangerous type of weapon, and its use had to be approved by the Prime Minister (explicitly excluding criminals and alcoholics). Meanwhile, the regulations have loosened up in France, too.

Knowledge of good cryptographic methods and mainly their correct use is still not widely disseminated. We often use bad or unpublished algorithms, or

Cryptology Unlocked Reinhard Wobst

algorithms whose security we know little or nothing about. ‘Security’ means almost always: we haven’t found a vulnerability so far, but who knows whether somebody found one long ago and just didn’t tell us about it. Security that is both theoretically provable and practically usable is still the pipe-dream of all cryptologists today, even though we may quite reasonably trust modern, thoroughly studied algorithms.

In contrast, interested outsiders encounter problems with the large choice of algorithms, theoretical findings from analyses, and difficult cryptographic protocols. The significance of good methods cannot be appreciated enough. The ‘information society’ needs to have a totally new security awareness; the risks are different and sometimes even much greater than in the physical world. One thing is for sure: not knowing about cryptology can only make things worse. You will find plenty of hair-raising examples in this book.

All the mystery-mongering, the imponderabilities and their particular significance make cryptology very different from other fields of knowledge. Cryptology is an adventure we will try to unlock in this book.

1.1 Should You Read This Book?

This is not a textbook. It is by no means complete, and it isn’t particularly mathematical either (at least not more than absolutely necessary). If you have some background knowledge and want to delve deeper into cryptology, I recommend the seminal work of Schneier [SchnCr], but this is a hefty tome of more than 800 pages. Nevertheless, the author refers to the literature frequently enough when it comes to the details (more than 1653 quotations!). Or perhaps you are looking for an easier way to first get to grips with the basics in cryptology: What does it actually research? What is known so far? What is it good for? How can I benefit from it? If you are intrigued by these questions, you may want to have a go at this book. If you make it to the very end, you will hopefully have found answers to these questions. And you should have a rough idea of how the security of methods and protocols is evaluated, and what to think of the findings. You will know how many fields belong to cryptology (and which don’t), how much inventiveness cryptanalysts put into their work, and how little we know in spite of it all; many statements in this book are only suppositions.

Cryptological knowledge can prove very useful in practice. With basic knowledge, if somebody tries to talk you into buying a product by simply stating that ‘nobody will reveal the data because they are encrypted’, you will not buy it. Modern ciphering devices and ciphering programs should have freely usable interfaces for a customer's cryptographic components, or they should at least offer reproducible methods. But only a qualified customer can force vendors to do this. This customer could be you, for example. The triumphant success of the free PGP program shows *one* possible way toward 'cryptological justice'.

You will find reading this book easier if you have some IT knowledge—people who know the C programming language will have a home advantage—and if you are not too hostile toward mathematics. But you don't have to be a professional programmer. *Cryptology Unlocked* is meant to be a book for practitioners who want to get a rough idea of this fascinating field without having to delve deeply into its theory. I'll spare you the nitty-gritty, like formulas, to the widest possible extent. Many things can be explained verbally just as well. Sometimes, however, there is no way around formulas. After all, cryptology is a field where each side uses mathematical ingenuity to trick the other side. This is why not everything can be explained without using some background knowledge. But it's not a math book for sure.

You will find only a few ready-made programs on the Web site to this book (`www.wileyeurope.com/go/cryptology`). Conversely, you will find plenty of C source texts 'to play' with, and many documents that go far beyond the things discussed here. The Web site to this book, the list of references, and information sources on the Internet will help you if you want to deal with cryptology more deeply.

1.2 Why Busy Ourselves With Cryptology?

1.2.1 'I've Nothing to Hide'

I've heard this sentence over and again and think it's a big mistake. Almost everybody is careful about their physical possessions: people lock their apartment doors, don't leave their wallets lying around unattended, and lock their cars. The fact that information represents an asset doesn't seem to have crossed many people's minds. All right, you wouldn't write everything on postcards, and you don't pass on the personal identification number (PIN) of your bank card. But the problem begins when handling this PIN: people who write their PIN on the card itself are simply unaware of the things unauthorized persons can do with such information! Information often embodies a much greater value than material things. Look at this example: back in the 1990s, Philip Morris bought Kraft Foods for 12.9 billion dollars, including 1.3 billion for material assets. The buyer deemed it worth paying 90 % for know-how, experienced staff, brand name, customer base, and so on—all of this largely representing

Example of the value of a company:

- Material assets worth 1.3 billion dollars.
- Miscellaneous (know-how, customer base, brand name, staff, ...) worth 11.6 billion dollars.

Figure 1.1: Information can be more valuable than material assets.

information that could mean added value for a competitor, for example, the know-how and disclosing of the customer base [Peters, p. 27].

Or think of the huge amounts of data from seismographic measurements that could give a clue on the location of a future oil platform and would mean millions in profit for an impostor. The German Chamber of Industry and Commerce (IHK) and industrial associations estimated the damage caused by industrial espionage to be at least 4 billion euros for Germany in 1988. This has remained the only official figure. Estimates from the beginning of the millennium were between 10 and 35 billion euros. The wide range of these estimates shows better than any verbose statement how large the gray zone must be.

Yet another consideration explains the significance of information: according to Peters [Peters], virtual companies will drive other business formats out of the market, because they are much more flexible and efficient. In this context, several companies would merge temporarily and for a specific purpose. Secure exchange of information represents an immediate value-adding potential for such virtual companies.

Underestimating the value of information can have catastrophic consequences. We should have learned this much from history. In both world wars, reading encrypted messages of the adversary played a decisive role, and in both world wars, the parties concerned simply ignored the impact of it. In 1914, when the German cruiser *Magdeburg* ran aground and fell to the Russians, including the *Signalbuch der Kaiserlichen Marine* and other code books, it didn't raise suspicion on the German side; no secret code was changed on this account. A Russian prisoner then even told the Germans that they owned the code books. Obviously the Germans underestimated the significance of cryptanalysis, and they hadn't even gotten suspicious when the activities of British warships made clear that the German intelligence communication had been eavesdropped.

Breaking the German Enigma code by the Poles and British in World War II was most important for the outcome of the war. A large part of Chapter 2 is dedicated to this topic. But in England, too, it took some time until the British admiralty recognized the value of their cryptanalysts, while they had a close shave themselves: according to Kahn [KahnCode], it would have been possible for the German Wehrmacht to land in Great Britain (in fact, things had been going according to plan!)—had the British not changed their own code in time—for the Germans listened in on them. Later on things changed, not only militarily: while the British managed to listen in on the Germans increasingly faster, the German top echelon refused to consider that their Enigma ciphering machine might *not* be infallible. Many insiders think that cryptanalysis was decisive for the outcome of many wars. Kahn [KahnCode] even thinks that cryptanalysis helped gain more information than all espionage activities together. At least four events decisive for the outcome of World War II were possible only by cryptanalysis. Among others, this includes the battle off the Midway Islands, which prevented the dominance of the Japanese in the Pacific, and the shooting down of Admiral Yamamoto's plane by the US air force. However, the best example is the submarine war in the Atlantic. If the Enigma hadn't been deciphered, the USA would probably have dropped nukes over Europe. More about this in Chapter 2.

We may reasonably assume that militaries, national intelligence agencies, and other organizations learned a lot from past errors. Otherwise, there wouldn't be agencies like the NSA (National Security Agency), for example, which specializes in the 'surveillance' of global intelligence communication and cryptology, among other things. Its largest listening-post outside the USA and Great Britain is located in Bad Aibling in the south of Germany. Readers interested in the details should look at Section 8.2.1.

You Have Information Worth Protecting

'I don't wage submarine wars, don't buy companies, and don't drill for oil', you will say, 'What should I protect?' Well, consider the following points.

- Any piece of information obtained in an unauthorized way that gives clues on your financial situation can be dangerous for you. If you have lots of money it will for sure. But even if you have no money it may: it could interest a potential employer, or your landlord. This person doesn't necessarily have to wiretap your line itself. Don't forget that information (as opposed to tape recordings) won't change even after the 15th copying between computers.

- Also your acquaintances and the possibilities for espionage or sabotage given by your work can make you an interesting subject for others—for national intelligence organizations, religious groups, or competitive companies. This is one of the fields with likely the largest percentage of undetected crimes. We don't know the proportions of the 'war behind the scenes'.

- Businesses are particularly at risk. [IHK] describes a case from the textile industry, where a company's major competitor lured away customers from that company's customer base. Address lists of any sort are cash! And people outside the business world shouldn't be indifferent about this either. Information is power, and it's usually the powerful who get to it more easily. This can lead to new types of painful competitive imbalances. The customer will feel it in the form of excessive prices, poor service, and inelastic supply.

- [IHK] points to the fact that scientists in particular see themselves as colleagues rather than competitors, and such circumstances are recklessly exploited by national intelligence organizations.

- Don't forget that some confidential information that may not be of interest to you can acutely endanger your friends or acquaintances. Possessing third-party information can also be dangerous in some situations. In February 1995, when insider information about Scientology became public on the Internet, the sender of this message had used an anonymous remailer. A remailer is a computer that strips off all information about the sender when forwarding emails (which is legitimate and sometimes necessary). On earlier occasions, such messages had been deleted by unknown people due to alleged disclosure of trade secrets. In this case, the Finnish police, called in by the FBI and Interpol, and Scientology themselves called the remailer operator and requested the sender's address be disclosed. While this led to nothing, when the Swedish daily *Dagens Nyheter* connected him with child pornography three days later, the Finnish police waved a search and seizure warrant at him two days later. The alleged child porn was found to be untenable a couple of days later. You can read more about this thriller in [Kunz.ct].

- Cryptology doesn't only deal with data secrecy. It also deals with data integrity and authorship. If your ATM card is stolen and the thief (or his organization) manages to cryptanalyze the PIN (see Section 6.6.8), you might find the money stolen to be the least painful consequence. The bank may claim that you had passed on your PIN with fraudulent

> intention and sue you. This has happened more than once. In court, your PIN is as good a judicial evidence as your signature.

Poor cryptography allows adversaries to rummage in your name, and you will be held responsible for the damage. Think of unscrupulous nuts with enough capability and a decent budget!

This book is not about national economy and data protection. But it uses examples from these fields to show you how important it is to protect information today. Together with the explosively growing popularity of the Internet, data protection gains unimagined significance. As convenient and beneficial as global communication may be, we have to learn *which* information we have to protect against unauthorized access, and *how* we can protect it. This book deals mainly with the second question.

Have you noticed something? Our real-world examples talked little about national intelligence organizations, and the popularly quoted armchair hacker wasn't mentioned at all. Information has become merchandise, and accordingly it is of interest for business. I recommend the book by Hummelt [Humm] for further reading; he worked with companies specializing in competitive analyses himself and knows what he is writing about. This explains the large number of instructive examples in his book.

Nevertheless, we should by no means underestimate the potential threat from national intelligence organizations. Thanks to rapidly evolving computer technologies, the possibilities of unnoticed surveillance grow just as rapidly. Section 8.2.1 will show you how technology can enable surveillance of our everyday lives, and how much of it has been implemented.

1.2.2 Cryptology: A Special Chain Link

Security is a Very Complex Field

Good cryptological algorithms alone offer no protection at all. Security can only be achieved by a gapless chain of measures:

- All members of staff concerned have to be trustworthy.
- All members of staff concerned have to be security-aware: none of them may write passwords on the bottom of the keyboard, have anyone looking over their shoulders as they type their passwords, let alone mumble them. Unfortunately, this happens quite often in practice.
- Data media with unencrypted information must be stored safely.

- Confidential plaintext (readable text) must never flow through a network others can eavesdrop, such as the Internet or intranets. It is believed that every data packet crossing the Internet in the USA is listened in on with a probability of 10 %. A DFN-CERT employee estimates a similar rate for Germany.
- Your computers have to be secured against illegal access over the network. *IP spoofing* (a technique used to gain unauthorized access to computers, whereby the intruder sends messages to a computer with an assumed IP address) is actually a complicated matter. But thanks to the wealth of software packages on the black market, this type of attack has become ‘respectable’, in addition to many other ingenious methods. We don’t know how many of these attacks are malicious. Firewalls are not impenetrable!

If all of this wasn’t scary enough, think of software working as an active spy. For example, the *Promis* program originally designed for criminal investigation had been universally used and might also have helped the NSA (National Security Agency) in accessing a large number of international databases, possibly including those of Swiss banks. I refer readers interested in the details to [SpiegDat] and spies you happen to know. The article referred to mentions, among other things, that every normal computer with a normal screen works like a TV transmitter. The signal can probably be filtered out from a distance of even one kilometer, and the screen contents can be reconstructed from this signal. Automatic teller machines (ATMs) are also computers, by the way. And we don’t know how many computers are out there running keyboard sniffers that simply capture keystrokes and then send passwords or other sensitive stuff they recovered over the network.

Don’t give up just yet. At the advent of the Industrial Revolution in England, most houses had no door locks, and current security technology wouldn’t have meant anything to anybody back then. The current change toward the information society is just as revolutionary, and we’ll once more have to learn things from scratch. And it will get dangerous if we fail to understand the threats.

What Cryptology Means for Data Protection

Back to our topic. You have seen that cryptology is not everything, but is something special. Why? Encryption can protect information when it is clear that unauthorized access cannot be prevented. (A classical example are the address lists on your Windows computer at your workplace.) However, I find another aspect much more significant.

Bugging a room, listening over laser mikes, extorting a company's employees, or penetrating a company's perimeters, and similar things are hard work and risky. No wonder spies are well paid. But when a popular encoding algorithm is secretly cracked, and the attack can be 'cast' in reasonably fast software, then data espionage gets much easier. Using this software is easy. Imagine somebody who can just about move a mouse suddenly getting hold of your confidential information and selling it to the brains behind the scenes to replenish his petty cash! This person won't have any hard work to do, because our networks are astonishingly easy to eavesdrop (or computers to tap), and he will normally not leave any traces. Other persons or computers can also use the program: copying the software is cheaper than buying a bug.

Yet another factor illustrates the special role of cryptology: if an eavesdropper can't decrypt encrypted messages, he can at least hoard them. One day either the encryption algorithm or the protocol will be cracked, or the eavesdropper will get access to a faster computer—and here we go, he will read all your messages in arrears. Since some information doesn't lose its value with age, even in our hectic times, you could have an unpleasant surprise after several years. For who knows what methods cryptanalysis will use in five years from now?

Fast and good decryption programs could enable large-scale surveillance the 'needlework spy' can only dream of. This is one of the new-quality risks to the information society. There are parallels to using nuclear power: the probability of an accident is much smaller than with other processes (in cryptology this means that money forging is much easier than finding an exploitable backdoor in the DES algorithm). But *when* an accident happens, the damage can outdo everything known so far.

Not even the leaky software mentioned above could have as many consequences as the fast, unauthorized decryption of a widely used algorithm—if at all possible.

All vulnerabilities mentioned so far have to be exploited individually; in contrast, cryptanalysis can be massware. You will find a small example on the CD that comes with this book: *newwpcrack* is a program that finds the password for an encrypted WordPerfect file on a PC with high probability within 10 ms.

Surprising Simplifications

I admit, I want to scare you a little. Really usable software like the one for WordPerfect doesn't normally come for free, and only the theoretical method is discussed. Almost no program will work as fast as WordPerfect. But don't rely on it, because complex mathematical problems have a peculiarity: once their solutions are found, they often become much simpler. The following examples show just how much simpler.

- You certainly know about Rubik's cube, which challenges you to turn the layered pieces such that each of its six sides has a different color. It took me two weeks of occasional trial and error to get my first two layers in place. The next attempt succeeded after three days, then it took only one—I had grasped the trick. I then felt I had to proceed more systematically. Within a week, I found a sequence of 'pieces' and composed a puzzle out of them. Later I handled the cube without training (but using a crib) within five to ten minutes. I'm convinced that everybody can do this.
- A much more drastic example is the base problem in functional analysis. The problem itself originates from mathematical basic research; I won't explain it here. Anyway, it concerns an assumption expressed in the 1930s which is relatively easy to formulate, as many hard problems are. For decades, leading mathematicians had cut their teeth over it. Nobody was able to prove it, until a Dutchman found a counterexample in the mid-1970s: it was all wrong! The proof that this was a counterexample in the first place was said to have been about 600 pages long—an inconceivable mental achievement. I heard a lecture about this proof, cut down to 'only' 80 pages, in Warsaw. Coryphées in functional analysis I so much admired shook their heads over the complexity of a single theorem. So I wasn't really sad that I failed to understand most of it. Six months later, a Polish mathematician told me that the proof had been cut down to less than five pages and had become readable.

Such stories seem to repeat themselves more often than not in mathematics. The so-called Hilbert problems were very popular at the end of the 19th century. I remember that at least one of them had been solved by an 'outsider', a student from former Leningrad.

So let's summarize:

- Even if great minds cannot solve a problem, an unknown person with unconventional ideas may sometimes be successful.
- Even if a solution initially appears outrageously complicated, it can sometimes be drastically simplified.

Chess programs appear to be subject to such changes, too. The playing strength of current computers is certainly due not only to their computation power, but also to chess theory. These programs have become so efficient because their development is rewarding: they sell well. Conversely, the only vendor of cryptanalytic software I know of is AccessData.[1] Their software makes encrypted files from numerous programs readable again (older versions handled WordPerfect, Lotus 1-2-3, Excel, Symphony, Quattro Pro, Paradox, and Word; their Web site also mentions Microsoft's encrypted EFSD file system). Confirming what I said above, one of the software's designers said they built wait loops into the software to make sure people wouldn't be shocked by its real speed [Hoff]. You will see for yourself in this book how much the encoding algorithm of WordPerfect is worth.

Normally, cryptanalysts are satisfied with showing the principle and occasionally demonstrating a program. Easily usable and efficient cryptanalytic software for more sophisticated algorithms is developed by somebody who deems it worthwhile—and then the average punter won't get the product. Large corporations and national intelligence organizations pay more and want to keep the goodies for themselves.

However, there is at least one sensational exception: [Hoff] mentions that governmental agencies in the USA use a program to crack the cipher contained in *pkzip*; more details in Section 5.7.1. You can find such a program on the Web site at `www.wileyeurope.com/go/cryptology`.

Don't get me wrong: value addition can be achieved when information is exchanged, and not when it is held back. But carelessly handling the protection of information can destroy these values—faster today than in the near future. On the other hand, thanks to cryptology, not only will our world become more secure, our lives will become more comfortable. Think of electronic payment systems, electronic elections, or digital signatures. Cryptology will perhaps also finally help us to download a brief chapter from a textbook (or a soundtrack) for a few bucks over a computer network rather than having to buy the entire book (or CD).

1.3 What This Book Doesn't Cover—Another Story

Security is an endless topic, and the existing literature is accordingly large: How do I protect my computer/the local area network against unauthorized

[1] http://www.accessdata.com. The software is not cheap.

access? What do I have to be particularly careful about when backing up data? What risks can arise from third-party software (particularly operating systems)?

This book doesn't deal with these topics. Readers interested in the security landscape can find plenty of material on the Internet, for example by visiting the DFN-CERT servers, because the information offered there is current.[2] This book deals mainly with encryption algorithms and their analysis in view of the previously explained special role cryptology plays.

Steganography

There is another method for protecting information against unauthorized tapping, in addition to 'open' encryption. This method is called **steganography**, and it hides messages in messages. Its purpose is to hide the existence of information rather than making it unreadable. There is no limit to the wealth of ideas. One example: my father was never allowed to tell anybody of his whereabouts during World War II. So in his army mail, he sort of accidentally underlined a digit in a date, say 5. All my mother needed to do was find the first letter of every fifth word in the message to recover his location. When I heard this as a child, I was sure nobody would ever be able to see through such a smart trick. How wrong I was! Steganography is an art that is thousands of years old, and it had reached totally different heights, as well as the routine of its recovery. Minimal changes to some letters, slightly varying spaces between words, previously agreed templates—everything conceivable had certainly been exploited. You can admire a so-called *semagram* in the seminal book by Kahn [KahnCode, p.523]: the naive pen-and-ink drawing of a brook with bridge, flowers, and houses. The receiver knew that she had to look at the blades of grass along the river bank: a Morse code had been hidden in their different lengths. Invisible ink is also something that belongs here, and microdots—entire A4 pages are accommodated in a single typewriter dot using microphotographic methods. (Kahn explains in detail how to produce microdots. Just this much here: they won't help you against surveillance anymore!) Other methods are discussed in [BauerDS] and [BauerMM].

The usual steganography has a serious drawback: the message is not protected by a secret and changeable key, but by a fixed method. Once the method is

[2] http://www.cert.dfn.de, ftp.cert.dfn.de

revealed, all messages are compromised. This is the reason why a message is normally encrypted before you hide it steganographically.

Steganography is still popular today. Encrypted emails must not be sent to some countries (including Russia and Saudi Arabia), which means that one is enormously tempted to hide the very existence of secret messages.

There are free software products for at least two methods intended to help keep emails secret:

The *first method* creates ‘artificial words’, which behave statistically similar to readable text. The message is hidden in the sequence of these artificial words. Of course, everybody who looks inside the mail itself will see that it doesn’t contain normal text (see Figure 1.2). But it helps fool a listening computer.

Nevertheless, I have my doubts. Analyzing written language is by far easier than analyzing the spoken word, and even for the latter research has come a long way. The statistical study alone gives many clues. Surely every software designer will think of letter frequencies (and perhaps frequencies of pairs). As an adversary interested in picking encrypted texts from a data stream, I would definitely select more intelligent functions, at least ones that the popular free programs don’t consider.

> Only an UFO buff like you would want to have fun with Buster Keaton. You know that Sigmund Freud was Eva Peron’s granola supplier in a previous life. Glucose Chips! So ripe that it’s the eighth wonder of the world! Gonzo Q! So expensive that it’s the eighth wonder of the world! Yo! Burt Reynolds would be Best Actor of the Year if he hadn’t evenly got hair all over Dwight Eisenhower. How can you rob Cortez so disappointedly? Having a part-time lover makes you more cannibal prosimian. Wheaty! So nasty that it’s the eighth wonder of the world! Have a Lipash-brand hat for your pteranodon! Bless my virtue! Eat tripe—the moth intestines of the earth! Bless my stomach! You’re Scotch, my little father. Bozhe moi, your power ties are really amusingly freaky. Frobo brand grape soda is flamboyant and crisp! Roger Bacon is into Scientology. Sugar Pimples, for the people who can’t get enough sugar! Possibly L Ron Hubbard and Paul Cezanne get paid a whole lot, but all they ever do is artfully write protest letters to Congress. C’mon, gimme the spiritual renewal.

Figure 1.2: This ‘artificial’ text hides encrypted information—it is a so-called mimic function by Wayner (more details in the mimic.txt file on our Web site, see A.1).

Compression won’t do the trick either, by the way. Compressed text can be decompressed, and those who try to be particularly clever by making encrypted text pass for compressed text forget that compressed data obey certain rules, too. More about this topic in Chapters 2 and 3.

I’m convinced that sufficient testing options can be found, except they aren’t generally known.

The *second method* hides information in digitized images. Nope, this time not in the length of a blade of grass: the color of each image dot (pixel) is described by several bits, e.g., 4, 8, or even 24 (accordingly 16 million possible colors). In this method, the first few bits determine the pixel color, while the last few bits serve merely for ‘fine tuning’. Changes in these last bits are hardly visible in the presentation; they are often even truncated when output on a screen. These bits are used to hide secret information. Here too, I have my doubts about the method’s security. Images are subject to certain well-known rules—otherwise, there wouldn’t be effective image compression methods. These rules also apply to the least significant bits. Now, if these bits contain an encrypted message, they are purely random, leaping to the eye exactly because of this, though our naked eye can’t recognize anything. Adapting to the statistics of the image would certainly be possible, but costly and never perfect. Rumors have it that every photo (at least the digitized ones) that leaves NASA is previously checked for hidden information. Why shouldn’t such programs work in large mail nodes? Basically, all objections made against the first methods apply to this method, too.

‘Real’ steganography hides information such that its existence cannot be proved lest you know the secret key. This is extremely difficult. You would have to

- filter out ‘noise’ independent of the actual information from a data stream;
- replace this noise by a secret text with equal statistical properties (not hard with so-called ‘white noise’, because secret texts created by good methods are equally distributed statistically);
- and finally mix this noise back into the reduced signal.

However, I have to warn you that statistical independence doesn’t mean deterministic independence! It means that there might be a very simple test that shows whether or not encrypted messages had been hidden. This is the critical point when using steganography.

Approaches that hide information in *video conferences* or *digitized speech* (audio files) are of particular interest (see [Westf], [Pfitzstego]). Such data are physically created and superimposed by an independent semi-conductor noise. This nourishes hopes for secure steganography, in contrast to cryptography, where we are still searching for a practically *and* provably secure algorithm. Studies conducted by Westfeld [Westf] look promising and show that a GSM phone call can be transmitted behind an ISDN video conference.

I should mention a (former) product of Steganos (*www.steganos.com*), a company based in Frankfurt, Germany, at this point: the product was used to camouflage information about the choice of synonymous formulations. As a side effect, the software was able to improve the style (e.g., avoiding repeated words). This provided an excellent pretense for using the program, and proving that steganography was involved became really difficult. Currently, the company offers only a program for embedding messages in images.

We will discuss another approach that's also secure, but not universally usable, in connection with subliminal channels in digital signatures in Section 6.3.3. This topic will also turn up again in Section 6.7.

Cryptanalyzing steganographic methods doesn't appear to be in advanced development stages in public research (see the next section about digital watermarks). The two methods mentioned above are uncritically praised over and again as a panacea. Prohibiting the free use of cryptography would encourage research and perhaps encourage the discovery of practically usable subliminal channels in methods other than digital signatures.

Steganography has *one* function in any event: It makes surveillance of data communications harder. Though thorough statistical studies are possible, they require sufficient material and considerable computation power. Together with the innumerable data formats commonly used, this can be a problem for eavesdroppers, though we should by no means underestimate the power of current supercomputers. More about this in Section 8.2.1.

Digital Watermarks

Another very young field of research is closely related to steganography. Intellectual property is becoming increasingly available in electronic versions—think of MP3 players, CDs, and DVDs, just to name the most obvious. As the use of these formats rises, so does the amount of piracy. If illegal copying cannot be entirely stopped, then we will at least want to be able to prove fraud.

With this in mind, manufacturers try to accommodate hidden, mostly irremovable information about the author in digital documents; we also speak of **digital watermarks** (copyright marking systems). A digital signature wouldn't help since it can be easily removed. A good example is the protocol by Birgit Pfitzmann described in [Pfitzfinger], which safeguards the anonymity of the honest customer.

However, in this hide-and-seek game, too, there are ways to make hidden information unusable, if it cannot be protected. Perhaps the first attack of this type against steganographic methods is described in [PetAndMark]. The authors are convinced that this type of analysis has helped steganography in making progress just as cryptanalysis has furthered cryptography. I understood from their work that the development of automatic tests for revealing hidden information is still in its infancy—at least in the civilian sector. [Ditt] is a book that thoroughly discusses the possibilities and risks.