

Chapter 3. Cryptography, a key technology for information security

During these days he had noticed a tapping code scratched into the wall of his cell, and had begun, eagerly, to send messages to whoever might be on the other side of the wall. After an hour or so of tapping, however, the door to his cell burst open, and an amused guard sauntered in to tell him, in filthy, broken English, that his neighbour wanted him to 'shot the fock op,' because, alas, 'nobody give to him the focking code.'
(Salman Rushdie, *The Moor's Last Sigh*)

In information security, cryptography – the art of secret writing – plays a vital part. It is nearly as old as the art of writing itself. “The multiple human needs and desires that demand privacy among two or more people in the midst of social life must inevitably lead to cryptography wherever men thrive and wherever they write.” [Kahn, 84]¹ As a tool for keeping communications secret, it has been widely used in intelligence, diplomacy, and wars. Revolutionary advances in cryptography have boosted its use in recent decades, opening up an amazing array of applications. It can be used to authenticate computer users, ensure the integrity and confidentiality of electronic communications, and keep sensitive information safely stored. From a secretive military technology, cryptography has emerged a key technology for all participants in the information society concerned about information security.

This chapter gives an overview of cryptography and its applications. I will sketch the history of cryptography (3.1.1) and introduce the crypto family (3.1.2), focusing on the recent developments in symmetric and public-key cryptography (3.1.3). Then, I will detail attacks on crypto systems (3.1.4) and the consequences this has for key length (3.1.5) and key management (3.1.6). Also relevant for the rest of this book are some further distinctions (3.1.7) and the technology of steganography (3.1.8). Finally, some special protocols extend the potential of cryptography (3.1.9). In the second part of this chapter, I outline the many applications of encryption, as used by providers (3.2.1), governments (3.2.2), and other users (3.2.3). I conclude with an indication of the extent cryptography is being used today (3.2.4) and a general assessment of the importance of cryptography in the information society (3.3).

¹ The historiograph of cryptography, David Kahn, opens his account nearly 4,000 years ago, with an Egyptian scribe carving an inscription with hieroglyphic substitutions about 1900 B.C.

3.1. Cryptography

3.1.1. History

Cryptography is of all times and of all cultures. In its long history, the two basic forms that have prevailed are codes and ciphers. *Codes* are lists of words, names, etc. coupled with an encrypted form, e.g., letters or numbers – comparable to a dictionary. *Ciphers* are methods to change each letter (or group of letters) into other letters, numbers, or symbols. Generally, codes work on words, whereas ciphers work on letters. For a long period, a combination of codes and ciphers in the form of nomenclators (a sort of secret dictionaries) was used. Nowadays, only ciphers avail.

Two of the cryptographic systems used in Antiquity illustrate the basic methods of ciphers that are still being used today: transposition and substitution. The Spartans used a staff of wood around which a strip of papyrus or parchment was wrapped. The message was written vertically on the staff, so that after the strip of papyrus was unwrapped, all the letters of the message were mixed up. The message could be decrypted by winding the strip around a staff of the same thickness. This process of mixing letters together is called *transposition*.

Another basic method is *substituting* letters by other letters or symbols. Julius Caesar invented a system in which each letter was substituted by the letter three places further down the alphabet (jumping from z again to a). Decrypting was done by substituting each letter by its third predecessor. The system of replacing each letter by a letter a fixed number of places down the alphabet is called a Caesar cipher. Another kind of substitution cipher is the Hebrew system of Atbash.

Whereas the operations of substitution and transposition used to be done by hand, from the First World War onwards, machines were developed to encrypt and decrypt messages automatically. These machines were widely in use during the Second World War. The British, for instance, employed tens of thousands of people to crack the German machine. A like number of US cryptanalysts managed to build a replica of the Japanese machine, so that they were able to read almost any message encrypted with it. (It was not enough to prevent Pearl Harbor, although they came close [see Kahn, Chapter 1].)

During and after the World Wars, cryptology was very much an intelligence issue. The invention and breaking of systems were reserved to military and security institutions. The world's best cryptographers were employed by the US National Security Agency, which sur-

Atbash										
Atbash is a Hebrew encryption system based on substitution. Each letter is replaced by the one below or above it in the other row.										
א	ב	ג	ד	ה	ו	ז	ח	ט	י	כ/ך
aleph	bet	gimel	dalet	heh	wav	zayin	chet	tet	jod	kaf
ת	ש	ר	ק	צ	פ	ע	ס	נ	מ	ל
tav	shin	resh	qof	tsade	pe	ayin	samekh	nun	mem	lamed
Thus, Babel (בבל) becomes Sheshach (ששח), an encryption used in Jeremiah 25:26: "and all the kings of the north, near and far, one after the other – all the kingdoms on the face of the earth. And after all of them, the king of Sheshach will drink it too." [Kahn, 77-8]										

rounded the field with an aura of utmost secrecy (the agency commonly being known as 'No Such Agency'). Although citizens and scientists were working on cryptology, results were largely classified and publications were sparse. This only changed in the 1970s, with two simultaneous developments that meant a breakthrough in cryptography.

Terminology

Encryption is the automated process of hiding data so that no unauthorized people can access them; this is done by means of a procedure (algorithm) and a key. *Decryption* is the reverse process. A *crypto system* is an implementation of an encryption scheme or algorithm. The making of crypto systems is called *cryptography*, the breaking of them is called *cryptanalysis*. *Cryptology* is the science that studies both aspects. Cryptography also includes making authentication or *digital signature* schemes that use an algorithm and a key.

A clear message is called a *plaintext* message, which is transformed by cryptography into a *ciphertext* message.

In *symmetric* crypto systems, both sender and receiver use the same key. In *asymmetric* or *public-key* cryptography, they use different keys. Symmetric keys are called *secret keys*, whereas public-key encryption uses pairs consisting of one *private* and one *public* key.

3.1.2. Intermezzo – dramatis personae

Alice and Bob have been corresponding secretly for many years, since the advent of modern cryptography. They are now the main characters in the ongoing story of cryptography literature. Their communications security is threatened by Eve, an eavesdropper who listens in on them, and Mallet, a malicious interceptor who can alter and fabricate messages. Criminal Carol is also an avid user of cryptography. Occasionally, Alice and Bob attract the attention of Leah, a law-enforcement agent, who together with policewoman Polly is monitoring Carol. Alice and Bob sometimes use the trustworthy services of Trent, a Trusted Third Party, or of Dorothy, a Key Escrow Agent who holds private keys in deposit.

3.1.3. Symmetric and public-key cryptography

In the early 1970s, in response to a request for ciphers by the US National Bureau of Standards, IBM submitted a recently developed crypto system called Lucifer. A weaker version² was developed into a new system, the Data Encryption Standard (DES), that has remained a standard to the present day. It is a conventional crypto system, using many alternating rounds of substitutions and transpositions, with a 56-bit key. It is a *symmetric* system, in that both encryption and decryption use the same key.

DES has proved a strong system. Despite doubts about the key length, its US status of Federal Information Processing Standard (FIPS) has been extended each five years; it was last recertified in 1993. Since the middle of the 1990s, DES can be cracked, but at considerable cost;³ it is still secure for most purposes. For maximum security, triple-DES is

2 The initial submission of IBM, Lucifer, contained a 112-bit key. This was reduced to 56 bits, allegedly under pressure of the NSA. When in the 1990s a new cryptanalytic method, differential cryptanalysis, was invented, DES was found to be so designed that it was optimized against this attack, a significant improvement on Lucifer. Apparently, the developers of DES already knew about differential cryptanalysis at the time they made it, fifteen years before it was reinvented. A longer key than 56 bits would not have significantly improved the strength of DES against differential cryptanalysis, and so the reduction to 56 bits turned out to be not really a weakening. [Wayner 95, 77-80].

3 Already in the 1970s, it was thought a special computer could be built at a cost of several million dollars to crack DES in a day. In 1993, it was estimated that a USD 1 million machine could crack DES in an average of 3.5 hours. [Schneier, 283-284] The Electronic Frontier Foundation built a DES cracker in 1998 at the cost

used to encrypt the message three times, using two 56-bit keys (yielding an effective key-length of 112 bits). Since DES is no longer completely reliable, the US National Institute for Standards and Technology is developing a new symmetric standard, the Advanced Encryption Standard, which can serve as a FIPS for the next decades; the AES should offer significant advantages over triple-DES.⁴

Today, many other strong symmetric systems exist, such as IDEA (developed in the 1990s and considered a strong symmetric cipher), RC4 and RC5, Blowfish, and Khufu. There is one symmetric crypto system that is provably and unconditionally secure. This is the One-Time Pad (OTP).⁵ Although it is the only provably uncrackable crypto system,⁶ it is not in wide use. Not only is it difficult to generate a truly random string of bits, but, more importantly, the key can be used only once (there is an easy method of attack if it is used twice), which makes it impracticable. Moreover, the key must be as long as the message and must be exchanged securely between sender and receiver; this pays off only for small and highly confidential messages (and for storage of information). Its main application has been (or is?) in the red line between Moscow and Washington.

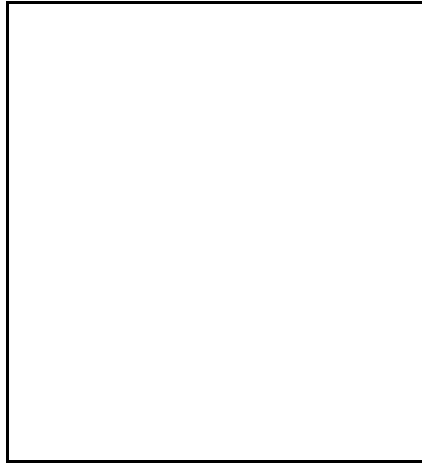
The drawback of symmetric crypto systems is that one has to first distribute the secret key securely – you cannot use conventional cryptography for this because you need a common key first. Besides, you need a lot of keys, one for each pair of persons communicating with each other. With large groups, the required number of secret keys becomes enormous (for 100 people, you need almost 5,000 keys). The thought of solving these problems triggered the development of a new kind of crypto system: one in which you can communicate securely before first having to exchange secret keys.

The idea of these crypto systems was launched in 1976 by Diffie and Hellman [Diffie].⁷ They proposed a *public-key* crypto system, in which each user has a pair of keys, one private and one public. A message encrypted with the public key can be decrypted only with the corresponding private key, and vice versa. Either key of the pair can not be derived from the other. The private keys are kept secret by the users, but the public keys are widely published. If Alice wants to send a message to Bob, she looks up his public key in a key directory,

of USD 250,000; it cracked the message in RSA's DES Challenge II in less than three days. [EFF] Compare the sidebar in 3.1.5.

- 4 The AES should specify an unclassified, publicly-disclosed, royalty-free encryption algorithm, providing strong security for twenty to thirty years. Submissions to the AES selection process include RC6, Rijndael, Serpent, and Twofish. In August 1998, the first Candidate Conference was held, initiating the Round 1 Evaluation and Analysis period. The process of adopting the FIPS will take at least two years, and likely much more. [NIST 98]
- 5 The One-Time Pad consists of a truly random string of bits that is used only once as a key. The ciphertext is the addition (XOR) of the plaintext and the key (XOR means 'exclusive or': $0+0=0$, $0+1=1$, $1+0=0$, $1+1=0$). Since the key is completely random, the ciphertext does not contain any information on the plaintext. With a different random key, it decrypts to a different plaintext, and without knowledge of the key, one has no way of knowing what the real plaintext was.
- 6 All other systems are said to be computationally secure: they have withstood public scrutiny for a long time, in that ciphertexts can not be deciphered in a reasonable time. This is the best one can say of these systems: they have good reason to be *thought* strong. The OTP is the only system that is *known* to be strong.
- 7 Actually, this was the second invention of public-key cryptography. As was revealed only in 1997, James Ellis and Malcolm Williamson of the UK Communications-Electronics Security Group had invented the same concept, 'non-secret cryptography', in 1970. CESG had kept it secret all the while. [Ellis]

encrypts the message with it, and sends it to Bob. He can decrypt it with his private key – and no-one else can, since he is the only one who knows his private key. The great advantage of this system is that you do not first have to exchange keys in a secure manner. (There is, however, another problem: you have to be sure that the public key you use is the right one; see below.)



There is another property of public-key crypto systems which makes them attractive. They can be used to authenticate messages and to prove their integrity. To do this, Bob uses his private key to ‘encrypt’ (or ‘sign’) the digest of a message to Alice, which he sends along with the message. Now Alice (or anyone else) can check the authenticity and integrity of the message (or ‘undo the signature’) by using Bob’s public key to decrypt the digest. If her own digest of the message as received matches the decrypted digest, the message cannot have been tampered with and must have been sent by Bob, since only he could have

signed the digest with his private key. This does not provide for confidentiality, since the message is sent in the clear. Secrecy can be established, however, by encrypting the message, after signing, with Alice’s public key. Then, only Alice can decrypt it with her private key, and subsequently undo the signature with Bob’s public key.

An important implementation of a public-key crypto system is RSA, named after its inventors Rivest, Shamir, and Adleman [RSA]. It was developed in the late 1970s, and counts as the best-known public-key crypto system.

The working of public-key cryptography

Public-key cryptography is based on one-way trapdoor functions. A *one-way function* is a mathematical operation that is easy to do in one way, but difficult or impossible to reverse. An everyday example is the throwing of an antique vase into thousands of pieces: easy enough to do, but almost impossible to reverse. A *trapdoor* one-way function means that there is a trick (i.e., secret information) with which it is easy to reverse the otherwise one-way operation. In public-key cryptography, you use the trapdoor one-way function to encrypt a message, and use the trapdoor to decrypt it. The pair of public and private keys consists of two numbers computed by using the trapdoor.

An analogy may clarify this. Bob has settled on translation into Kwakiutl as his crypto system. His public key is the English-Kwakiutl dictionary, which he publishes widely (say on the Internet). As private key, he uses the Kwakiutl-English dictionary, which he keeps secret. To send a message to Bob, Alice uses the English-Kwakiutl dictionary to translate her message into Kwakiutl. Now Eve, who eavesdrops on the message, has access only to the English-Kwakiutl dictionary; to translate back a single word, she has to leaf through the entire dictionary to see which English word it matches. Bob, on the other hand, can use the Kwakiutl-English dictionary to conveniently translate the message.

With this system, Bob can also sign messages. For this, he has another key pair, say Xhosa. He now publishes the Xhosa-English dictionary, while keeping secret the English-Xhosa one. To sign a message, he translates it into Xhosa. Anyone can subsequently translate it back into English, using the public Xhosa-English dictionary. Thus, they can check the signature, for Bob is the only one who 'knows' Xhosa.

Mathematically, this is done through exponentiation with numbers (typically of about two hundred digits), modulo a certain large number, the product of two prime numbers (arithmetic 'modulo k ' means reducing all numbers to a number below k , which is what you do when you say it is 7 o'clock when it is 19:00 hours: you count modulo 12). The public key is used for exponentiating the message (digitized into bits). For decryption, Eve can try to compute the inverse of the exponentiation, but this is (probably) a so-called 'hard' mathematical problem, meaning that it takes too much time to be computationally feasible.⁸ Bob, who has got the private key, uses this to make another exponentiation – the private key is chosen in such a way that the two exponentiations neutralize each other.⁹

Because the mathematical implementation of public-key cryptography uses numbers, both encrypting to keep the message secret (Kwakiutl) and encrypting for signing messages (Xhosa) can be done by the same key pair. This property makes public-key cryptography a convenient, multifunctional system.

There is one drawback. Public-key systems are slow – much slower than conventional, symmetric crypto systems. RSA is about ten times slower than symmetric systems such as DES or IDEA, making it inefficient for encrypting large messages.¹⁰ Therefore, in most applications, a combination is used to exploit the advantages of both systems. First, Alice uses RSA to send a, say, DES key to Bob; she can do this by looking up his public key. After Bob has decrypted this message with his private key, he and Alice both have got the same DES key, so now they can use the fast DES to communicate securely. The combination of a symmetric and a public key system is called a hybrid crypto system.

Authenticity, integrity, and non-repudiation

Authenticity and integrity (without confidentiality) can also be safeguarded by hash functions and message authentication codes. A *one-way hash function* is a one-way function, without a trapdoor: it can only be used to transform a message into a digest, which cannot be reversed. The digest, or hash, is usually a short, fixed-length block (typically 128 to 160 bits) (for an analogy, one can think of a mincing machine outputting a very concentrated piece of minced meat). To show that a message has not been tampered with, Alice can use a *message*

8 A 'hard' problem is a problem that can not be solved in polynomial time. This means that as the numbers involved get larger, it quickly becomes too time-assuming to solve the problem. For sufficiently large numbers, the problem is too complicated to be solved – even with supercomputers. For example, presently, 200-digit numbers are beyond factoring.

9 There is another class of public-key crypto systems (such as Diffie-Hellman and ElGamal), which are based on another mathematical problem: discrete logarithms. For convenience's sake, I restrict the description here to public-key systems based on the factoring problem, such as RSA.

10 Elliptic-curve crypto systems, which have been developed in recent years, speed up public-key cryptography significantly. However, certain elliptic curves can be cracked relatively easily, and it is not yet certain whether implementations can ensure that users avoid choosing these weak curves.

authentication code (MAC). This is a key-dependent one-way hash function (it can also be a one-way hash function that uses a symmetric crypto system to encrypt the resulting hash). With the input of the secret key, the MAC computes a hash, which is sent along with the message. Bob, who also has the secret key, can then verify the message's integrity: he also computes the hash on the received message with the secret key, and compares this with the received hash. Only if these two match can he be sure the message has not been tampered with. Mallet, if he intercepted the message, can not have altered the message and computed a new digest to send along with it, since he does not know the key Alice and Bob use. Note that a MAC does not provide for confidentiality, as the message itself is sent in the clear.

If instead of a symmetric system (with a secret key known only to Bob and Alice) Alice uses a public key system with a hash function, the result is usually called a *digital signature*. Alice signs the hash with her private key, and sends the message and the signed hash to Bob. He, upon receiving Alice's message, undoes Alice's signature of the hash, computes a digest of the message himself, and checks whether these match. If they do, only Alice could have sent the message, since she signed the hash. Moreover, the message has not been tampered with, or it would have yielded a different digest.

Besides safeguarding confidentiality, integrity, and authenticity, public-key cryptography can also be used for a fourth objective, non-repudiation. Assuming her private key has not been compromised, Alice can not repudiate messages signed with her key (in a common-sense understanding, that is – legally, she can always repudiate anything, and with a good lawyer, she might convince a court that someone else used her key). She can only repudiate signatures if she has notified a key compromise within a reasonable period after noticing the compromise. Messages will have to have been time-stamped in order to see which messages Alice can not repudiate. Non-repudiation of the receiver can in general not be effected, except by more complex protocols and procedural agreements.

Table 3.1 summarizes the objectives the various forms of cryptography can serve.

<i>crypto system</i>	<i>objective</i>	confidentiality	integrity and authenticity	non-repudiation
symmetric		yes	yes/no ¹¹	no
public key		yes	yes	(yes)
hash functions		no	no	no
message authentication codes		no	yes/no ¹¹	no

Table 3.1. Cryptography and security objectives

¹¹ Symmetric crypto systems and MACs can provide for integrity and authenticity between communicating parties. However, they cannot prove this to others: there is no way Bob can prove a message came from Alice, as he could have encrypted it with their common key himself.

3.1.4. Cryptanalysis and the strength of crypto systems

The art of breaking encoded messages and crypto systems is called cryptanalysis. It is the counterpart of cryptography, the art of making crypto systems. Cryptanalysis can attack any part of the process of encryption, for example, the algorithm used, its implementation, the key management, carelessness of the user, or the waste-paper basket.

A cryptanalyst's attack depends on the information at his disposal. The most basic is a ciphertext-only attack, where the cryptanalyst has only got a ciphertext to decipher. A known-plaintext attack is easier, as the cryptanalyst has got a ciphertext and a corresponding plaintext, for example, because he has found it somewhere or because he can guess the contents of a standard message. Still more powerful is a chosen-plaintext attack: the cryptanalyst can choose plaintexts and have them encrypted (for instance, by testing how a stolen smart card encrypts plaintexts). If the crypto system can resist a chosen-plaintext attack, it is strong indeed. In developing new systems, devisers often assume a cryptanalyst to be able to commit a chosen-plaintext attack; the system should be devised in such a way that it resists this.

Still, it is difficult to assess the strength of a crypto system. Crypto systems are always under attack, from all angles. Although one can argue that a certain algorithm is theoretically sound, and one can study an implementation to see if it contains any trapdoors, still one does not know whether the system does not yield to an attack unthought of. New attacks appear every so often. For instance, in November 1995, Paul Kocher announced a timing attack that cryptanalyzes by means of closely timing the processor's cryptographic operations [Kocher]. Against a computer, this is essentially an academic attack (someone who is powerful enough to measure to the microsecond what your computer is doing is likely also able to look over your shoulder at the screen), but it may work against smart cards. Another attack, developed in 1997 by Biham and Shamir (extending an attack developed in 1996 by Bellcore researchers), uses a micro-wave oven to trigger minor errors in the processor of a smart card; the results can be exploited for cryptanalysis through 'differential fault analysis'. [Biham]

Even the mathematical security of an algorithm can not be proven. Public key crypto systems rely on problems that are thought to be 'hard', such as taking discrete logarithms (Diffie-Hellman) or factoring large numbers (RSA). However, there is no proof that these problems are indeed hard – there could be a solution as yet unthought of to factor large numbers in reasonable time.

There is an argument in favor, though, of assessing the problem as 'hard': the problem of factoring has been studied by many specialists for decades, precisely because it has such great implications in the field of cryptography. It had already been studied for a long time before, and the fact that it has large implications in cryptography has only added to its appeal as a research object. This makes it unlikely that someone comes up with a new and easy method of factoring large numbers. The more people are attacking the problem and the longer they take, the more likely it is that the problem is indeed 'hard', even though it has not been mathematically proved.

The same argument holds for assessing the strength of a crypto system. If a crypto system has been published for a long time, has been studied by many cryptanalysts around the world, and still resists cracking, then it can be assumed to be strong. So, DES and RSA, which both were published in the 1970s, are good crypto systems which are unlikely to be broken all of

a sudden.¹² This can not be said of unpublished crypto systems: they have not been intensively scrutinized, and there might be a backdoor cracking method that its devisers overlooked.¹³

This is why most cryptologists argue that crypto systems should be published: the system will be widely studied and analyzed, so that any flaws it contains will likely be found. This way, for instance, the implementations of public key cryptography based on the ‘knapsack’ problem¹⁴ were found insecure, even though the mathematical problem was ‘hard’. Crypto systems that rely on secrecy are generally viewed with scepticism by experts (who call such systems ‘snake oil’) – they know the complexity of devising a crypto system, and only trust it when it has been studied by experts in the field. As the fundamental tenet of cryptography says: “If lots of smart people have failed to solve a problem, then it probably won’t be solved (soon).” [Kaufman, 40]

Apart from attacking the crypto system itself, the cryptanalyst will try any other possible attack. “There are numerous practical attacks that don’t involve cryptanalysis, that can expose the contents of a PGP encrypted message as easy as peeling a banana. These attacks are cheap, efficient, sometimes difficult to detect, and may be elegantly simple.” [McNamara 97] For instance, someone may have used weak keys or weak passphrases (which can be automatically cracked by, e.g., PGPCrack). Attacks often benefit from design errors. Many designers focus on theoretic attacks, resulting in products so complex that they lead to implementation blunders and consequent security failures. According to cryptanalyst Ross Anderson, almost “all security failures are in fact due to implementation and management errors.” [Anderson 94]

Even if the system and implementation are secure, someone can attack the key management by bribing someone. If the persons involved are beyond corruption, he may use a TEMPEST device to intercept the electromagnetic radiation your computer emits. If you prevent a TEMPEST attack by building a Faraday cage, he will infiltrate your favorite pizza-catering service and look over your shoulder while you type in your key. Crypto use is only as strong as its weakest link: it pays to use strong systems only if you take into account all feasible attacks. Indeed, most attacks do not seem to use cryptanalysis at all, but merely involve “crooked employees, clever sting operations, stupid implementations, integration blunders, and random idiocies.” [Schneier, 214]

12 Of course, Eve might have cracked the system and have kept silent. After cracking a few sensitive corporate messages to do profitable business on the stock market, and after selling some nuclear-technology secrets to a backwater country, she could have retired to Puka-Puka, and no-one is the wiser.

13 For instance, Bruce Schneier, John Kelsey, and David Wagner announced on 20 March 1997 that they had discovered a flaw in the privately designed Cellular Message Encryption Algorithm used in digital cellular phones, allowing an attack to succeed within minutes on a conventional personal computer. [Counterpane]

14 The knapsack problem is the task of exactly filling up a knapsack with a selection of boxes from a given collection of boxes. In mathematics, this comes down to the following exercise: given a set of integers, find a subset of these integers that add up to a given large integer.

Distributed attacks

Several efforts have shown the vulnerability of crypto systems to major, concerted attacks. Over the past two years, several cracking contests have tested the strength of symmetric crypto systems with varying key lengths. All contests except the last one were won by the combined computing power of many computers testing keys in their spare time (e.g., at night, or in the form of a screen saver), facilitated by lively discussions and software exchange over the Internet. The results show the power of networking, with more and more people participating in combined attacks.

date of crack	system and key length	time spent	number of computers involved	key space searched	cracker
28.1.97	RC-5 40 bits	3.5 hours	250	32%	Ian Goldberg
10.2.97	RC-5 48 bits	13 days	3500	58%	Germano Caronni and others
17.6.97	DES 56 bits	120 days	70,000	25%	Rocke Verser, Michael Sanders, and others
19.10.97	RC-5 56 bits	250 days	500,000	47%	David McNett and others, distributed.net
23.2.98	DES 56 bits	39 days	no information available	90%	David McNett and others, distributed.net
15.7.98	DES 56 bits	2.5 days	1	25%	EFF DES Cracker

3.1.5. Key length

A good working assumption in cryptology is that the strength of a crypto system relies entirely on the keys.¹⁵ That is, the system should be so strong that the only way to crack it is to try every possible key: a *brute-force attack*. Therefore, keys should be of sufficient length to resist a brute-force attack. Trying every possible key to see which one fits can be done in parallel, on many computers at the same time. Also, one can build special hardware for cracking algorithms; although this hardware can be used for cracking only one system, it is much quicker than general-purpose software. Brute-force attack is a trade-off between cost and time: the more money you spend on computing power, the quicker you will find the key.

The number of keys to be tried rises exponentially with their length. Every bit added to a key doubles the number of possible keys. If you are not sure how much computation capacity the attacker has got, it is wise to add a few key bits to be on the safe side – it does not cost much to use a somewhat longer key, but it makes the cryptanalyst's work of brute-forcing the key space a lot harder. A rule of thumb known as Moore's law says that the computing capacity of computers doubles about every eighteen months. To keep abreast of advances in computer technology, it therefore suffices to raise the key length by one bit every year and a half, or to add six bits every ten years.

¹⁵ Sooner or later, someone will find out how the system works (like the American cryptanalysts building a replica of the Japanese encoding machine in WWII). Cryptography experts hold that 'security through obscurity' does not work: a good crypto system relies on the secrecy of its keys, not on its own secrecy.

The required length for symmetric keys and for asymmetric keys differs due to the variety in attack. Strong symmetric systems can be attacked only through brute force (trying every possible key), whereas public key systems are attacked by trying to factor the large numbers they are based on. Symmetric keys are usually 64 to 128 bits long. DES, with its 56 bits, is crackable, although at considerable cost; to be on the safe side, triple-DES is used, with an effective key length of 112 bits. A panel of acknowledged experts in 1996 suggested a minimum symmetric key length of 75 bits for keeping messages secure for some time to come.¹⁶ Adequate asymmetric keys vary from 768 to 2048 bits in length.

Apart from using a large enough key, one can also thwart brute-force attacks by compressing a message before encryption. With a robust compression system, you can remove most information redundancy from the data. This makes it difficult, if not impossible, for a brute-force attacker to recognize the original message when he tries the right key.

Developments that may shake the field

Computer power advances rather steadily. Moore's law (computer power doubles every eighteen months) of the 1960s still holds today. This means that cryptography users can rely on current estimates of how much time and money it costs to break a crypto system. However, there are several developments that might change this outlook.

First, biotechnology can be used to solve mathematical problems. DNA has solved the 'hard' problem of the traveling salesman (find a travel path that visits a specified number of cities exactly once). With smartly chosen strings of DNA, each representing a city or a road between two cities, a (liquid) solution containing these DNA strings and an enzyme to link them together, a (problem-solving) solution was found. Although a modest project, the attempt shows that traditional computers do not have a monopoly in problem solving. Efforts are made to use biochemics for cracking crypto systems. [Leutwyler] However, it is uncertain whether such solutions scale well. According to Donald Beaver, for factoring a 1000-bit number, "far more than (...) 10^{200000} liters of solution would be needed, an amount that perhaps would have unsettled the biblical Noah." [Beaver]

Second, efforts are being made to develop quantum computers. These would rely on quantum properties of photons to represent bits of information. The uncertainty principle means that one bit could have different values at the same time, a revolution in computing. A quantum computer might factor a large number in polynomial time, possibly leading to the downfall of factoring-based public key cryptography. However, due to physical problems, it is as yet uncertain whether such computers will ever be feasible.

Apart from revolutions in computing, thermodynamics places limits on computing power. A certain amount of energy is needed to represent information: each operation involves a minimum amount of energy. According to Bruce Schneier, there is not enough energy in space to brute-force attack a 256-bit symmetric key ("until computers are built from something other than matter and occupy something other than space"). [Schneier, 158]

For the time being, one can rely on conventional computer technology and cryptography to safeguard information security. It can do no harm, though, to keep an eye on developments elsewhere in science – some application might appear to shake the present-day crypto field.

3.1.6. Key management

As the security of encryption lies mainly in its keys, not only do they have to be of sufficient length, but they also have to be kept well. Symmetric keys and private keys have to remain secret, whereas public keys require a proof of integrity. Key management is the most

¹⁶ "[K]eys used to protect data today should be at least 75 bits long. To protect information adequately for the next 20 years in the face of expected advances in computer power, keys in newly-deployed systems should be at least 90 bits long." [Blaze 96]

significant part of using encryption. Just as it is useless to have the best safe for your valuables if you stick a paper on top of it with the code, it does not help to use a strong crypto algorithm if you are careless with your keys.

Good cryptographic keys are random (or random-looking) strings of numbers of at least eight characters: they are more like *%p8@CO,hq* than like *topsecret*. Except mnemonic wizards, people have to store the keys, which usually happens immediately after generation, under protection of a password (or, ideally, a passphrase). A good option is to store the keys on magnetic or smart cards – these tokens can serve as conventional keys to be inserted in a lock in the computer or communications device. Alternatively, the keys may be encrypted by a master key, which is closely guarded by a trusted person.

Once you lose a key, you lose the information, as the system is (supposed to be) uncrackable (or you need not have used it in the first place). Also, employees can suddenly die or be bribed by the competition. It is therefore prudent to keep back-up keys somewhere, even though this might diminish security. Often, back-up keys are stored centrally with a security employee or the management. Sometimes, a key-escrow agent may be found outside the company – this is usually a Trusted Third Party (TTP).

Especially private keys, which have a lifetime of several years, should be guarded from disclosure. Once a private key has been compromised, all users should be notified, lest they rely on the corresponding public key that is no longer valid. For this, key-distribution centers or Certification Agencies maintain lists of compromised keys. To solve liability questions that may arise in case of a key compromise, a key certificate can be issued with a limited time-span, and agreements can be made on the time limit to notify the key center of a key compromise. Because the idea of using digital signatures is useless if people can sign a message and subsequently deny having signed it (“Oh, sorry, I lost my key before this message was signed.”), it is advisable to have a TTP *time-stamp* transactions. If the key center has not been notified of a key compromise before the time-stamp, the signature can be considered valid and the holder of the corresponding private key is accountable for the signature.

In public-key crypto systems, one must rely on the correctness of the public key. Mallet can issue a public key in Bob’s name. He can then read any message Alice sends to ‘Bob’. Therefore, Alice must have a way of knowing that a public key really belongs to Bob. The reliability of public keys is usually ascertained by the digital signature of a Certification Authority (CA). This CA issues key certificates containing the public key, identifying information, a time-span, and the signature of the CA.

Two systems for communications security, Pretty Good Privacy (PGP) and Privacy Enhanced Mail (PEM), illustrate potential key-certification structures. PGP has a flat, horizontal structure, with users certifying each other: if you trust someone, you sign his key. If someone’s key is signed by (someone whose key is signed by) someone you trust, you will accept his public key. So, PGP relies on a web of trust. In PEM, on the other hand, certification is hierarchic: a top certification center certifies national certification centers, which certify local or corporate certification authorities, which certify users. The trust of PEM depends on faith in the top certification center.

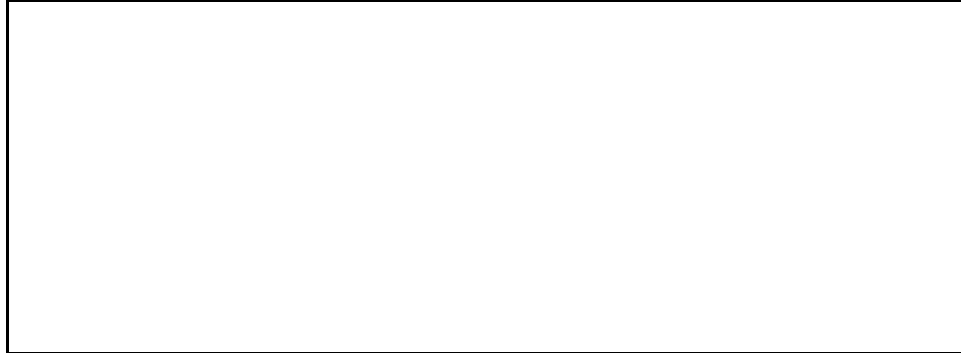


Figure 2.2. The certification structures of PEM (left) and PGP (right).

The framework for key-management services (such as key recovery, certification of public keys, and time-stamping messages) is called a Public Key Infrastructure (PKI). The establishment of a PKI is important to ensure that cryptography can be used well in the information society. People are often required to use cryptography for communicating with unknown people, and so, they must have a way of ensuring that the keys they use are valid. Trust is essential, and this can almost only be established through a certification infrastructure that has a firm basis in law (formulating requirements for CAs, for instance) as well as in practice.

Today, PKIs are beginning to emerge, oriented either more vertically or more horizontally, depending on their context. An intra-organization PKI, for instance of a multinational, will usually be hierarchic, but it may have a cross-certification relationship with PKIs of fellow multinationals. These could all be hierarchically incorporated in a Chamber of Commerce PKI, which could in its turn cross-certify an international NGO PKI. At the national and international levels, all sorts of PKIs are conceivable, and time will tell which PKIs will emerge where. (See further 7.1.)

3.1.7. More distinctions

Apart from the difference between ‘weak’ and ‘strong’ crypto systems,¹⁷ some more distinctions are useful in describing the field of cryptography. Cryptography can be used for protecting either *communications* or *data storage*. This influences the choice of cryptography. In general, for communications security one needs – usually short-term – confidentiality or integrity and authenticity, or all of these. For storage, only confidentiality or integrity are needed, but for a longer period. In communications, session keys can be discarded directly after the conversation; for storage, the keys obviously have to remain valid and secret for as long as the information needs to be stored. Therefore, the management of keys also varies with the application.

17 “There are two kinds of cryptography: one that keeps your little sister from reading a message, and one that keeps the government from reading a message.” [Schneier, xix]

The Spartan and Caesar ciphers show that cryptography can be implemented in *hardware* (the Spartan staff) or *software* (the Caesar algorithm). Often, modern cryptography is implemented in (tamper-proof) hardware.¹⁸ This is mainly for efficiency reasons: software implementations are slower and more vulnerable to attacks. The drawback of hardware is that it is less fit for distribution and upgrading; software implementations can be easily transmitted and upgraded. As processing speeds continue to advance, more cryptography may be implemented in software, although for specific purposes hardware solutions will probably remain preferred.

In networks, cryptography can be used link-by-link or end-to-end. *Link-by-link* encryption means that each node in the network decrypts incoming messages and encrypts outgoing messages; in the node itself, the message is in the clear. In *end-to-end* encryption, on the other hand, a message is encrypted at the start and decrypted only after arrival at its destination. The advantage of link-by-link encryption is that the sender only needs to know the key of the first node, regardless of the addressee. With end-to-end encryption, every user should know the keys of all the people he might want to communicate with. However, in link-by-link encryption, the message can be read at every node, so the overall security is only as strong as the weakest node, and all nodes have to be trusted. End-to-end encryption safeguards security over an insecure network.

3.1.8. Hiding cryptography

Just as messages can be hidden by cryptography, the use of cryptography can itself be hidden. This is called *steganography* (hidden writing). For instance, a message can be tattooed on the scalp of a courier, who – once his hair has sufficiently grown – runs to the addressee, who shaves his hair and reads the message (as Histiaeus did with a slave to urge his son-in-law to revolt against Persia, according to Herodotus [Kahn, 81]). Quicker is an ancient Chinese method of hiding a message written on very thin silk in a ball of wax which the courier hides or swallows [Kahn, 73].

More elegant forms of steganography hide messages in messages – seemingly innocent texts that contain secret messages underneath. Naive people ‘hide’ their PIN codes in their address book, writing it as a postal code¹⁹ – usually to no avail, as it is easy to detect fake postal codes. Another example is ‘Yuan Xiao’, a poem by a Chinese student in the US, which was published in the Chinese official newspaper *Renmin Ribao* (People’s Daily) in March 1991. Seemingly an innocent poem, it escaped the notice of the severe Chinese Communist Party’s censors, but most of the readers noticed the hidden message: the diagonal was a call for Prime Minister Li Peng to be replaced.²⁰ More practical than Chinese is the use of digital signatures to send subliminal messages: hiding data in the signature attached to the message. In fact, “[a]ny signature scheme can be converted into a subliminal channel” [Schneier, 536] (see also 7.3.2).

18 Note that claims of tamper-resistance should be viewed with some caution. [Anderson 96].

19 Dutch postal codes have the form *1234 AB*, which can ‘hide’ the PIN 1234.

20 Subsequently, Chinese officials have become more cautious. Public-security officers withheld a letter written by dissident Wang Dan in prison. They did not understand the poem it contained, and suspected that it contained secret signals to outsiders. Consequently, they required Wang Dan to write another letter. [*Ming Pao*, 26 August 1997]

Most methods of steganography tend to significantly enlarge the message size. A system (mockingly) proposed by a Dutch professor, in reaction to the Dutch plans to restrict crypto use, would multiply a message's size seventy times [Mulder]. Moreover, systems that hide messages in normal-language texts are hard to automate. However, efficient programs exist to hide messages in digitized images (for instance Stego, Hide and Seek). These images consist of many (usually 256) shades of white to black (or color)²¹; in the least significant bit of each byte of a pixel, a bit of the message can be hidden. This hardly alters the appearance of the image, as the subtle shade differences are unnoticeable to the human eye. Thus, you can store a 64 kilobyte message in a 1024 x 1024 grey-scale picture [Schneier, 10]. This process is also possible with digitized sounds.

Another way to 'hide' cryptography is to use a 'duress' code, which can apply two different keys to the same ciphertext: one decrypts it to its original (real) plaintext, the other decrypts it into another, innocent message.²² Some password systems use this method of duress codes: if a bank employee is forced at gunpoint to get money from the safe, he can type in a password that opens the safe but at the same time triggers a silent alarm.

Detecting cryptography

How do you distinguish, in E.M. Forster's phrase, 'mystery' from 'muddle', or cryptography from nonsense? If you have a random-looking stream of bits, how do you know whether it is an encrypted message, a picture hiding a message, or just plain nonsense? If you can transform it into something meaningful by means of a decryption algorithm, you can reasonably assume that the string was indeed the encryption of that message. Failing this, there is no real method of distinguishing between the two. Checking the pattern of the random-looking string can help, as good crypto systems transform a message into a ciphertext that satisfies the main properties of randomness. The context can give more evidence. E.g., the least significant bits of digital images have patterns not necessarily similar to those of ciphertexts, so the pattern may indicate that an image hides a message.²³

21 According to Peter Wayner, if colors are defined by 8 bits, the effects of hiding data in them can be quite significant, but with 24-bit colors the result is much better. [Wayner 96, 159-160]

22 Say you want to send the message: "twelve tons of dope" using a Vigenere system (addition of letters: A+B=B, C+D=F, et cetera). With Hamlet's monologue as a key, this yields the ciphertext:

```
plaintext:  twelvetonsofdope
key:       TOBEORNOTTOBETHA
ciphertext: MKFPJVGCGLCGHHWE
```

When forced to decrypt, you might – instead of giving the real key – use the key BWSJ YNLY NEGQ NDSR, which decrypts the message as follows:

```
ciphertext:  MKFPJVGCGLCGHHWE
key:        BWSJYNLYNEGQNDSR
plaintext:  longlivethequeen
```

This way you can decrypt the ciphertext to any plaintext you choose: from the ciphertext and the desired plaintext, you can compute the key you need to 'decrypt' to the desired plaintext.

23 One could prevent detection through this kind of analysis by building an image around the (cipher)text to be hidden, instead of hiding the text in an existing image. Computer graphics or fractals are possible candidates to compose images from (random-looking) texts.

3.1.9. Protocols

Apart from cryptographic algorithms, a large number of cryptographic protocols are being developed. These are a series of steps, involving two or more parties, designed to accomplish a task using cryptography [Schneier, 21]. They can be used for a wider variety of objectives than simple crypto systems. Indeed, it is amazing what can be accomplished through cryptographic protocols: mutually distrustful parties can do a great variety of things over a network without being able to cheat. For instance, they can fairly toss a coin or play poker over the telephone, or sign a contract simultaneously over a network.

Suppose you are a carpet dealer in Baghdad. One day, Ali Baba comes and steals a carpet. You run after him, but he flees into a tunnel in the rock. At a junction, you are at a loss; as you cannot wait all day, you choose left. Wrong: at the end there is a blank wall, but no carpet robber. Bad luck. The next day, the same happens, and this time, you go right at the junction – wrong again. The stars must be against you. By the tenth carpet you lose this way, though, you will doubt whether it is only bad luck – the chance of your choosing wrong ten consecutive times is less than one in a thousand. There must be a catch: Ali Baba knows a secret passageway connecting the two tunnel ends, so that he can escape no matter which way you go. You do not know where this secret passage is, but you are convinced it must be there. Ali Baba has used a *zero-knowledge protocol* to convince you that he knows a secret, without giving it away.

Zero-knowledge protocols have interesting applications, for instance in authentication procedures: you can authenticate yourself by showing you know a secret (for instance, a PIN code), without giving any information about the secret itself.

Other cryptographic protocols that have a great potential are secret-sharing protocols. With these, you can divide a secret among a number of people, so that they can reproduce the secret only when a certain number of them are together; still, each single holder does not have any clue to the secret. The protocol can be sophisticated into any detail desired: you can give certain (groups of) people priorities or veto rights. Secret sharing can be used for taking major decisions, such as launching a missile attack, or for sharing a vital company secret among the board.

3.2. Applications

Cryptography is used to safeguard information-security objectives: integrity, authenticity, confidentiality, and (within limits) non-repudiation. In the information society, many applications call for these objectives. Often, cryptography is virtually the only way to effectively safeguard information. This section will show to what uses cryptography can be put by the various participants in the information society.

3.2.1. Providers

Network providers can incorporate cryptography in their networks, to make sure all information transfers are secured from altering and eavesdropping. Link-by-link encryption will ensure that in between nodes all information is enciphered. The new version of the Internet Protocol (IP – the basic protocol that determines transmissions over the Internet),

IPv6, is to incorporate DES in the network layer. At the transport layer, network providers can incorporate the Secure Sockets Layer (SSL) to facilitate secure communications between communicating parties over the Internet. The ISDN protocol includes the capability of incorporating encryption. Even if built-in encryption is not always viable for large, public networks (for instance, because of lack of interoperability), network encryption can be efficient for local area networks or intranets.

The major network to incorporate cryptography is SWIFT, the international financial network. Because of the enormous value of its transactions, protection is paramount. It is estimated that daily half the world's Gross Domestic Product travels over the network. This calls for maximum transmission security safeguarding both integrity and confidentiality.²⁴

For service providers, cryptography is a good feature in new services to enlarge consumer trust. For instance, the WWW browser Netscape has a cryptography feature that allows subscribers to communicate securely: users that obtain a signed certificate are assured that all their communications are automatically encrypted (as long as, of course, the other party also has a certificate). It can also serve to authenticate clients and servers. Internet Service Providers will be required to protect the privacy of their clients (at least by providing adequate security of stored unread e-mail), and perhaps to provide their clients with means, including cryptography, to protect their online activities.

Other services that can profit from cryptography are teleconferencing, for which generally confidentiality should be safeguarded.²⁵ Still more important is the protection of mobile telecommunications, one of the fastest growing markets. As radio communications are easier to intercept than wire communications, they should be better protected. GSM has incorporated the encryption algorithm A5 to automatically encode all communications between the mobile phone and the base station.²⁶ Software developers can use Message Authentication Codes to serve as proof of correctness of software [Hueske]; especially for critical company operations, users need to be sure the software has not been tampered with.

For service providers and content providers, protecting intellectual-property rights will be a major crypto application, although the technology is yet in an early stage. Major market shares of the information society will consist of conditional-access services and payable services on demand. Pay-TV and (near) video-on-demand are quickly gaining ground. They rely on the possibility to shield transmitted information from unauthorized use. Conventional (analogue) scramblers used for encoding programs on a broadcasting net are traditionally

24 "In such business, confidentiality is paramount – consequently, security is a fundamental aspect of the entire S.W.I.F.T. system and is rigorously implemented throughout in order to address the full spectrum of risk." [SWIFT, 8]

25 The EC Council resolution on the use of videoconference and videophone techniques for intergovernmental applications of 9 June 1986 [86/C160/01] calls confidentiality one of the problems specific to the use of videoconference facilities by governments. Likewise, most company meetings contain sensitive information, and private video-conferencing may be privacy-sensitive.

26 Encryption can also be used to prevent the cloning of mobile phones: the reprogramming of a stolen analogue phone to resemble a legitimate phone, causing the calls to be billed to the legitimate owner. Fraudulent use of stolen mobile phones by cloning rose by 500 per cent in 1995. Newer systems, such as GSM, use encryption to prevent cloning. [CLSR, January-February 1996]

easily breakable.²⁷ For video-on-demand to really take off, better encoding schemes are called for, relying on good crypto systems to prevent unauthorized decoding. Likewise, Digital Versatile Disks (DVDs, the next-generation compact disk) will incorporate encryption to prevent piracy of the movies stored on them.

Also, for the online distribution of copyrighted works, such as books, compact discs, or digitized art works,²⁸ encrypted distribution and electronic copyright-management systems are necessary.²⁹ Such protection may include 'locking' products (publishing a product of which the main part is cryptographically locked; users can download it and pay a fee to receive the decoding key), fingerprinting (adding buyer-specific data to each sold copy),³⁰ and watermarking (marking the source and copyright information with steganographic methods, so that the watermark will be preserved when the product is copied or altered),³¹ all of which measures require some form of cryptography. Since it is impossible to prevent authorized users from redistributing the product (they, after all, have legitimate access to the product as it is), mechanisms to track unauthorized re-use, such as watermarks, may be even more important than secure distribution to authorized users. Cryptography can help tracing the source of leaks, when 'traitors' (authorized recipients) allow non-authorized parties to obtain the data [Chor].

The technical protection for conditional-access services and for copyright-management schemes is being supplemented by legal protection. First, the European Commission has presented a draft *Directive on legal protection of conditional access services* in July 1997 [COM (97) 356], which covers all broadcasting and online services offered on a conditional-access basis. The draft requires member states to prohibit commercial activities that facilitate unauthorized access to pay services.³² Second, the WIPO Copyright Treaty requires legislation to prohibit the circumvention of technological copyright-management information.³³ The European Union and the US are taking steps to implement these requirements.

27 For instance, illegal decoders were publicly marketed for decoding European Broadcasting Union transmissions of the European Championships soccer in 1996. [*Volkskrant*, 29 February 1996]

28 Marketing digitized art constitutes an emerging market, but museums worry about losing control of their collections. "Some computer-literate museum employees are starting to think about ways to encrypt such images so that only authorized users can look at them." [Powell]

29 "Technologies developed for securing information hold promise for monitoring the use of protected information, and provide a means for collecting and compensating the owners of intellectual property." [OTA]

30 Such fingerprinting can also be done anonymously. [Pfitzmann]

31 For instance, Playboy is watermarking its online photos to track use of its images on the Web. [Lazarus]

32 The scope of the draft directive is broader than the original *Green Paper on the legal protection of encrypted services in the internal market* of July 1996, which covered only illegal decoding of broadcast services. Amendments to the draft directive raised concerns within the cryptographers community in early 1998, as they appeared to also prohibit cryptanalytic research. However, the final proposal for the Directive [COM(98) 332] implemented these amendments.

33 Article 11, 'Obligations concerning Technological Measures', of the WIPO Copyright Treaty, adopted 20 December 1996, reads: "Contracting Parties shall provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used by authors in connection with the exercise of their rights under this Treaty or the Berne Convention and that restrict acts, in respect of their works, which are not authorized by the authors concerned or permitted by law." The WIPO

The Dutch government likewise recognizes that criminal law should protect against infringements of technical measures, such as encryption, that protect information [25880, nrs 1-2, 6].

Cryptography also facilitates new business processes for content providers. For instance, record companies welcome the option of recording music at different places at the same time – vocals in New York, the band in London. They can efficiently exchange the recordings over the Internet in a secured, confidential way, and mix the recordings.

3.2.2. Government

Traditionally, governments have been the main users (and breakers) of cryptography. They employ it in diplomatic services, intelligence gathering, military affairs, internal memoranda, et cetera. The ‘black chambers’ of the eighteenth century, which deciphered virtually all diplomatic correspondence [Kahn, 157-188], have a modern counterpart in intelligence agencies that employ a large number of mathematically trained cryptanalysts.

Yet cryptography is not only used for intelligence purposes. It shields personal registries maintained by the government, such as municipal, social-security, and police registries. Equally important, it protects intra-government communications. Some examples of government networks requiring high levels of information security are a trans-European public administration network called for by the Bangemann report, OB2000 (a Dutch network for electronic messages within (local) governments and for communication between government and citizens), and C2000 (a Dutch single, high-grade network for mobile voice and data communications between police, fire brigades, ambulances, and military constabulary). More specific applications also call for encryption, such as the information interchange between the Central Criminal Intelligence Agency and Interpol [Hendriks], and the online checking of license-number information by traffic wardens [*Telecommagazine*, September 1996].

As government information is increasingly published electronically to facilitate access to public-sector information, the concern for integrity is growing. In many cases, for instance, in applying for a subsidy or in setting up a business, people must be able to rely on the correctness of the electronic administrative information.

Also, cryptography opens up new ways for improving the relationship between citizen and administration.³⁴ For instance, online tax declaration is a client-friendly and expedient medium. Electronic elections and referendums may be held, with large efficiency gains. The reliability and unforgeability of votes can only be safeguarded by cryptography, such as digital signatures with private keys issued by an election Certification Authority. Electronic toll collection or road-pricing schemes can be implemented. The data used in these projects must not only be correct, but also confidential, as information on traveling behavior can be privacy-threatening.

Performances and Phonograms Treaty of the same date contains a similar requirement.

34 Indeed, in less democratic countries, cryptography may even enhance the democratic value of parliamentary decisions itself. In early 1998, China’s National People’s Congress put into use a new electronic voting system that “is designed to make it impossible to track down any individual deputy’s voting options” [*Xinhua*, 4 March 1998]. This might help in transforming the traditional applause machine into a more critical legislative body.

One of the most important uses of cryptography in this context is that it helps to prevent crime. Cryptography protects against computer crime, fraud, and industrial espionage. In the words of James Fotis, Executive Director of the Law Enforcement Alliance of America, “the threat to public safety comes from the lack of encryption; files that are not secure are ripe for theft and misuse. (...) [B]y using encryption we can reduce computer theft crimes and lower economic espionage.” [Fotis]

Last, a quaint application has been proposed in the draft Dutch Computer Crime Act II. Cryptography can be used for ‘seizing’ or ‘attaching’ information that the judiciary wants to bring out of someone’s power (for instance, because it is child pornography), comparable to the traditional seizure of property. If the seizure of the information carrier is disproportionate, the ‘cybersheriff’ could encrypt the information on the owner’s disk, so that the information would get out of reach of the person involved (provided he does not have a copy somewhere). Only when the judge grants replevin, the information would be decrypted and thus ‘returned to the owner’.³⁵

3.2.3. Other users

Besides the government, the other users of the information society – both individual and corporate – can gain much from new ICT applications. In many cases, integrity, authenticity, or confidentiality are called for.

Financial applications

First, financial transactions have to be secure. Home banking is an increasingly popular activity, which relies on the integrity, authenticity, and confidentiality of transmitted requests and orders. For online payment, transmitting credit-card numbers over networks is, to say the least, risky. Losses through the interception of credit-card numbers have occurred repeatedly. Information that is directly valuable should be encrypted before being sent online, if not before being typed at all – packet sniffers can intrude in terminals and record information to be downloaded later by the initiator of the sniffer (which can even bypass firewalls). It is wiser to use a zero-knowledge protocol to give the credit-card number,³⁶ for instance, by challenged signed response: the server gives the client a random number, which he types into a personal calculator containing a chip with the credit-card number. Inside, the chip computes a hash from the random number and the credit-card number, which the client send to the server. The server can then verify the correctness of the credit-card number by computing the same hash.

35 First suggested by Ministry of Justice official Alexander Patijn [Patijn, 805], it was incorporated in the draft Computer Crime Act II, proposed article 125o. Another way to ‘seize’ data would be to copy them and delete the ‘original’ data.

36 “An Internet user should not be required to type in a password or reveal any personal characteristics that someone else could copy. Instead users should be asked to provide answers that depend on their knowledge of some secret without revealing it.” [Beth]

Other methods are being developed for online payment. Electronic cash (e-cash) systems have been proposed and are being tested in practice.³⁷ An electronic coin or note is a (large) number digitally signed by the issuing bank. An (electronic) shop-owner can verify the bank's signature and send it to the bank to add to his account. All e-cash systems incorporate a feature to prevent or to detect and trace double spending. Anonymity is a disputed feature: it is desirable from a privacy point of view (normal cash, after all, is anonymous), but it creates opportunities for illegal purposes, like money laundering, tax evasion, and cashing a ransom anonymously with no risk of being traced [Solms].

A particular use for electronic cash is micropayment: paying very small fees for very small services, like viewing a WWW page. Such a feature might stimulate the development of good web pages: page makers would be rewarded for their efforts, and competition would ensure that the web does not perish in a chaos of infinitely many web pages where no-one can find his way. Micropayment could be a feature implemented in browsers: each user has a stack of electronic coins (each, say, of tens of a cent), of which the browser would automatically transfer one to the holder of the requested web page, while transferring the page to the user.

Digital money will increasingly be stored on smart cards. Altogether, smart cards hold great promise, not only for storing digital money (in Dutch the 'chipknip' or 'chipper'), but also for membership cards, medical-insurance cards, museum cards, and public-traffic permits. To protect the information on smart cards, which can have direct financial value or be privacy-sensitive, cryptography should be used to guarantee authorized use only of the information stored.³⁸

Privacy and sensitive data

Cryptography will also ensure that on multi-functional smart cards, people can only read the sections they are allowed to access – an important feature to prevent the making of privacy-threatening personal profiles. More in general, cryptography serves to protect personal data files, as required by data-protection laws.³⁹ Moreover, for many purposes, Privacy Enhancing Technologies (PET) can be used to protect personal information from unnecessary disclosure: pseudonymous data often suffice for the purposes of collecting personal data. A Norwegian report thus recommends 'pseudonimizing' health registries, so that data can be gathered for research purposes without threatening personal privacy [NOU]. A joint report of the Dutch and Ontarian data protection registrars strongly recommends the use of PET in a variety of applications. Often, it is not necessary to know the identity of the people involved: a *pseudo-*

37 DigiCash has developed *ecash*TM, a digital equivalent of cash which was accepted as currency by Mark Twain Bank (until September 1998) and by some other banks on an experimental basis. Contrary to the 'cash' of DigiCash, other online-payment systems rely on encrypted transmission of credit-card numbers or account information (CyberCash, First Virtual, Netscape's built-in encryption software developed with MasterCard and Visa) or on smart cards (Mondex).

38 "Smart cards have been technologically demonstrated. Whether the business and personal privacy issues they raise can be settled is another matter. Companies in a wide variety of businesses see uses for smart cards, but each has an interest in controlling the personal information that will be stored on them." [Zysman]

39 According to the Dutch Data Protection Authority, encryption is one of the most powerful tools to protect data bases and data supply as required by the Data Registries Act. [Registratiekamer 94]

identity suffices. Only for authorizing and billing is it necessary to know the name and address of the users of the service. [Registraatkamer 95] Cryptography will help implement the ‘identity protector’ used in privacy-enhancing technologies. Similarly, cryptography can protect data bases, so that it is easy to find the data of a single person but hard to extract an entire mailing list from the data base [Schneier, 73-4].

In general, storage will require encryption to shield sensitive information in a variety of situations, from keeping a secret diary⁴⁰ or shielding adult material from your kids to outlining plans you do not want others to know of – both in private and business surroundings.

Aside from the protection of stored personal data, data security often also requires communications safety. Business communications need to be protected, both from eavesdropping and from altering. Many intra-enterprise communications are confidential, such as annual figures, research and development information, personnel mutations, and travel information of high corporate officials who run a risk of being taken hostage. Many (larger) companies use private networks or intranets, where the security risk is lower. Still, even private networks are vulnerable to hacking and eavesdropping, so that sensitive information should be protected additionally by cryptography. Also, cryptography is a good means of shielding information from unauthorized users within a company (especially important since the larger part of security threats comes from employees) .

Also for private use, cryptography will be required for communications security. As the use of e-mail is soaring, increasingly people are sending confidential information across public networks. One of the principles of the US NII Task Force reads: “Individuals should be able to safeguard their own privacy by having (...) the opportunity to use appropriate technical controls, such as encryption, to protect the confidentiality and integrity of communications and transactions”. [NIITF] The use of e-mail encryption will likely be a major application of cryptography in the near future. Examples are electronic private letters, electronic confessions,⁴¹ online psychological help,⁴² or escaping from government scrutiny. Lawyers and their clients will often want to communicate confidentially through encryption.⁴³

Human rights

Cryptography can be life-saving for political and human-rights activists who fear persecution from human rights violating governments. The US State Department report on human-rights practices lists quite a number of countries whose governments illegally monitor the

40 In 1996, an employee of Emmen municipality was suspended when his diary, which he kept at work on his hard disk, was found to contain rather unkind statements about his colleagues. Although the diary had been erased from the hard disk, two colleagues managed to unearth it with undelete utilities while he was on holiday. Cryptography would have helped the employee to keep his diary secret – and his job.

41 In 1996, an Austrian priest went online to offer a confession service. He encouraged people who wanted to confess to use PGP. [Cf. Landwehr]

42 Psychologist Robert Wilson expects 40 per cent of psychological help to take place online within a few years, especially since it is decidedly cheaper. [*Intermediair*, 25 September 1997]

43 The Iowa Supreme Court Board of Professional Ethics and Conduct has stated that e-mail containing sensitive material must be encrypted, or else the lawyer must obtain written acknowledgment from the client that he consents to the risk. [*EPLR* 1996, 515]

communications and illegally search the houses of its citizens, notably of dissidents.⁴⁴ Phil Zimmerman, maker of PGP, received several messages from a Central European human-rights activist who thanked him for writing PGP. “Without PGP we would not be able to function and protect our client group. Thanks to PGP I can sleep at night knowing that no amount of prying will compromise our clients. (...) There is no Constitution, enforced by capable courts in this part of the world able to protect us from such abuses, so we must have the right to protect ourselves from abuse” [Zimmerman 96]. Human Rights Watch has called on governments to allow “users of the GII to encrypt their communications and information without restriction.” [HRW] When Hong Kong had been handed over to China in 1997, Amnesty International called on its China coordinators to encrypt all communications with Amnesty’s Hong Kong Regional Office. After the 1996 publication of Nicky Hager’s book on the global surveillance system Echelon (see sidebar in 4.3.2), a project was started in the Pacific to promote and supply publicly-available encryption software to democracy movements in countries with repressive governments. [Hager]

Public and private networks

Encryption is important in connections with the outside world. More and more individuals and companies connect to public electronic networks. Security is a major concern, especially when connecting to the Internet. Firewalls generally protect internal systems from outside threats, but some sophisticated attacks can bypass even firewall protection. Sensitive information has to be additionally protected with cryptography from spoofing attacks.⁴⁵ In connections with the outside world, virus protection is paramount. Cryptographic integrity checks (for instance, a signed hash) can serve to assure that a software program has not been altered by a virus. Each time the program is invoked, the computer first checks the hash to see if the program is still the same.

Through external connections, communicating with other parties, for instance, in distance selling, negotiating mergers, exchanging marketing information, and tendering, is increasingly done online. Electronic Data Interchange (EDI) uses standardized communication formats, for instance for insurance contracts, court pleadings, bills of sale, and shipping documents. Production and sale chains can be set up for just-in-time order and delivery; in consequence, the stock can be much smaller and efficiency is enhanced. The factories and companies in the chain have to rely on the integrity and authenticity of the orders; these objectives can be effected through digital signatures and message authentication codes.

Cryptography is essential for electronic commerce. Digital signatures and Certification Authorities can address the need for non-repudiation, integrity, and authenticity of requests

44 For instance, on China, the report states: “In practice, however, authorities frequently monitor telephone conversations, fax transmissions, electronic mail, and Internet communications of foreign visitors, businessmen, diplomats, residents, and journalists as well as Chinese dissidents, activists, and others. Authorities also open and censor domestic and international mail. (...) Government security organs monitor and sometimes restrict contact between foreigners and citizens, particularly dissidents.” [DoS]

45 In a spoofing attack, TCP/IP packets are faked so that a server is fooled into believing they come from an authorized user; this way, one can even bypass firewalls. The only real method of protecting information against these sophisticated attacks is to use cryptographic authentication.

and delivery (provided international legal recognition and liability issues are solved). Often, confidentiality may be called for. "The use of strong encryption which ensures the confidentiality of both sensitive commercial and of personal data is one of the foundation stones of electronic commerce." [COM(97)157, at 50] The Bonn conference likewise recognizes "the importance of the availability of strong encryption technology for electronic commerce." [Bonn, at 35]

Another option created by electronic networks is teleworking. If employees work at home, they may save commuting time and child-care costs. Access to the company's network and automation facilities can be established through telephone-modem connections, but the openness of the public telephone network warrants encrypting all communications between the company and home.

Other applications

Besides confidentiality, integrity of communications is often necessary. R&D information, annual returns, and the like must be relied on. Integrity is also paramount in safety-critical processes. For instance, in automated medical procedures, such as the administering of medicine or computer-supported operations, the integrity of the data used is a matter of life and death.⁴⁶ As a result of a nurse altering data in the data base of a British hospital, a child with meningitis received medication for a heart disease [Breed, 17]. Several cases are known of factory robots having killed people [Neumann, 65]. In safety-critical applications, both the integrity of information input and of the software used must be ensured; cryptographic checks play a significant part in this.

A secret-sharing protocol (3.1.9) can help to protect key company secrets, such as the recipe of the company's product or the combination to the safe. It is dangerous to have a single person keep secrets (what happens if he debauches, defects, or dies?), so the secret should be shared among, say, five company officials and employees, in such a way that each three of them can decrypt the secret. A secret-sharing protocol ensures that the secret is divided among them, without any single person having knowledge of the secret: it is only with a minimum number of them that they can reconstruct it. So, if any one holder defects to a competing company, he can give away no information, and the secret can still be reconstructed. The chances of the competition bribing a number of employees is significantly smaller than the chance of a single employee being corrupt.

Last, the advent of public-key cryptography creates a curious possibility: you can prove you have made an invention without making known how it works. You simply make a hash of the document describing your invention, sign it with your private key, and publish it in the *New York Times*. Later, by the time you want to market your invention, you can patent it; the published and signed hash serves as proof that you made the invention at the time of publishing, which invalidates claims of others that made the same invention after you. Delaying marketing of a new invention gives you more time to sophisticate it or to do market research; with traditional patent claims, time runs against the inventor.

⁴⁶ A woman who had been told she and her children had incurable syphilis killed her daughter and tried to kill her son and herself. The medical information turned out to be based on a computer error. [Neumann, 71]

3.2.4. Cryptography in practice

Cryptography is widely available. A worldwide survey of cryptographic products by Trusted Information Systems found 1619 products as of December 1997 (rising from 1393 in December 1996). Of these, 656 non-US products were identified from 29 countries (43 per cent using DES), mostly in Europe, but also in Argentina, India, Iran, Mexico, and Russia. These products were produced and distributed by 949 companies (475 US, 474 non-US) in at least 68 countries. [TIS]

Although the potential applications for cryptography are abundant, its present use is confined to a few major areas. It protects the integrity of valuable information, it authenticates people who engage in transactions, and it shields confidential information from unauthorized access. It is mainly used in financial areas (bank transactions, home banking, smart cards, e-cash), in privacy protection (personal registries, smart cards, government registries, sensitive information storage), and communications security (e-mail, facsimile, the air interface of GSM).

A survey of business cryptography use, ordered by the Dutch government in 1994 when it prepared its hapless law to restrict crypto use, concluded that cryptography is mainly used by large organizations. Of the 97 respondents, 18 organizations indicated they used cryptography, and ten expected to start using it within the next ten years – a total of 29 per cent. Cryptography was mainly used in business provision of services (notably banks) and in telecommunications. The researchers expected that future cryptography spread would be larger than the results indicated, given the fast growth of the number of computers and modern applications like home banking and EDI. [KPMG 94, 6-7] In the US, the Chamber of Commerce estimated that 17 per cent of companies used encryption for confidentiality in 1995. They expected the figure to rise to 60 per cent by 2000 [mentioned in Denning 97b].

So, in practice, cryptography is still mainly used by large entities: banks, great enterprises, administrations. Individuals and small and medium-sized enterprises are starting to use it, but in general they lag behind, possibly through a failure to recognize the importance of information security, and through a lack of standardized, user-friendly cryptography products. It is commonly expected, however, that crypto use will rise significantly in the near future, as more and more areas of life are digitized and as encryption technologies become more widespread and user-friendly.⁴⁷

3.3. Conclusion – the importance of cryptography

“Cryptographic technologies are nowadays widely recognised as the essential tool for security and trust in electronic communication. (...) Encryption of data is very often the only effective and cost-efficient way of meeting these requirements.” [COM(97) 503]

47 “The market for encryption in distributed computation, databases, and electronic mail is beginning to expand exponentially as the U.S. and other countries develop and popularize electronic commerce, public networks, and distributed processing. (...) Less technologically advanced countries, where demand for encryption software is reportedly negligible, will soon undergo widespread development and computerization leading to increased demand for encryption software within the next 10 years.” [DoC]

Through the advent of public-key encryption, a whole range of crypto applications has opened up to secure information. Some of these are exotic, but many applications are basic and will be essential in the information society – for providers, for users, and, not least, for governments. The confidentiality and integrity of communications and stored information will often have to be safeguarded through encryption.

The importance of cryptography is widely recognized by governments. For instance, the Dutch Ministry of Economic Affairs stated: “It is undisputed that for businesses and government alike cryptography forms an indispensable and useful instrument for the reliability and security of message traffic and of the infrastructure and telecommunications services used for this.” [24565, nr 1, 5] Likewise, the German Ministry of Economic Affairs found that “effective information protection requires secure encryption methods (...) A reliable protection of [confidential] information from unauthorized access is often only to be effected through the deployment of secure encryption methods.” [BfW] The Australian Walsh Report found that the “ready availability of strong encryption (...) is the most effective safeguard of individual privacy.” [Walsh, finding 1.2.39]

Most importantly, even proponents of restricting cryptography in view of cryptocriminals recognize the need for strong cryptography. “Practically everyone agrees that cryptography is an essential information security tool, and that it should be readily available to users. I take this as a starting assumption and, in this respect, have no disagreement with the crypto anarchists” [Denning 96] (written when professor Denning still advocated systems with built-in law-enforcement access to keys). Even the director of the FBI, Louis Freeh, agrees: “We see encryption as a public safety issue, and we are (...) absolutely committed to the development of encryption technology. In order to do all of the things we want to do in public safety – as well as in commerce and for national security – we must be strong proponents of encryption.” [Freeh 95b]