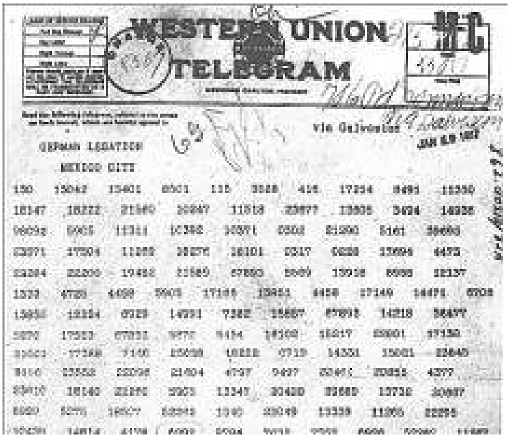
Miscellaneous Surveillance

17

Cryptologic



WESTERN UNION
TELEGRAM

via Galveston

JAN 19 1917

GERMAN LEGATION

MEXICO CITY

```
130    13042  13401  8501   115    3528   416    17214  6491   11310
18147  18222  21560  10247  11518  23677  13605  3494   14936
98092  5905   11311  10392  10371  0302   21290  5161   39695
23571  17504  11269  18276  18101  0317   0228   17694  4473
23284  22200  19452  21589  67893  5569   13918  8958   12137
1333   4725   4458   5905   17166  13851  4458   17149  14471  6706
13850  12224  6929   14991  7382   15857  67893  14218  36477
5870   17553  67893  5870   5454   16102  15217  22801  17138
21001  17388  7446   23638  18222  6719   14331  15021  23845
3156   23552  22096  21604  4797   9497   22464  20855  4377
23610  18140  22260  5905   13347  20420  39689  13732  20667
6929   5275   18507  52262  1340   22049  13339  11265  22295
```

1. Introduction

Cryptology is the study of the discovery and analysis of coded and hidden information. *Cryptologic surveillance* is the portion of this field that involves seeking the messages, discovering their existence and characteristics, and decoding their content. The decoding process is more specifically known as the field of *cryptanalysis.* Cryptologic surveillance is a subset of cryptology and is not directly involved in coding messages or devising codes.

Some portions of cryptologic surveillance overlap with chemical surveillance. When discovering 'hidden writing,' that is, writing that has been created with lemon juice or other chemicals that disappear when they dry, or that can only be seen if heated or chemically treated, chemical surveillance techniques are used.

This chapter describes messages that have been hidden to obscure the existence of the message and messages which have been encoded with a cipher or other means of obscuring the *content* of a message. Sometimes visual, chemical, and cryptologic surveillance methods are used together. For example, a message that has been encoded to defy comprehension may also have been hidden, making it necessary to engage in a two-step process to discover and decode the message.

The broader term *cryptology* is used here instead of *cryptography* because not all coded messages are graphically transcribed in words or pictures. Some may be transmitted in radio or television broadcasts, may be hidden in music, or may use senses other than those of sight or hearing. Prearranged signals are a type of coding that can be used to signal danger in adverse situations or to signal approval in private social situations. For example, an aunt cooking dinner in an occupied war zone might cook onions to signal that someone unwanted is in the house. When another family member comes home from work, she or he knows something is amiss if the smell of onions wafts out when the door is opened. Another example might be a female spy who has to signal a yes/no, safe/not-safe situation to another agent at a dinner party. If she's wearing cologne, the answer is 'yes' or 'safe,' if she's not wearing cologne (or a flower, or a dress of a certain color) the answer is 'no' or 'not-safe.' These types of one-time, simple-answer codes are probably the most difficult of any for the surveillant to detect and interpret. Most cryptologic surveillants are involved in decoding longer communications, such as written messages and radio broadcasts and, now that personal computers are linked via the Internet, email and other digital communications.

Cryptology is a technical field and those who are hired by businesses or governments to detect and decode messages are usually very smart problem-solvers who have a knack for crosswords, logic puzzles, and games like Chess and Go. They are often generalists with multidisciplinary interests and the ability to 'see outside the box,' a talent that aids in seeing solutions to unexpected problems.

Cryptography and related aspects of hidden writing frequently involve the use of chemical, mechanical, and computer technologies. A portion of chemical surveillance deals with ways of detecting and revealing hidden writing and ultraviolet light is sometimes used to reveal writing (or ancient drawings) on rocks, paper, or other materials that are difficult to see with the unaided eye.

Cryptologic surveillance is an important aspect of surveillance technology and a big topic that is only covered in its broadest aspects in this chapter. There are thousands of books on cryptographic technique, machines, and history and this chapter does not seek to repeat the information but rather to provide an overview within the general context of technological surveillance with an emphasis on cryptanalysis.

If you are interested in learning more about cryptographic surveillance or learning some ciphering or deciphering techniques, you are encouraged to seek out information in the resources described at the end of this chapter.

2. Types and Variations

Not all codes are secret, some are created for convenience, to save space, or for use with electronic devices (e.g., bar codes). In the context of this text, however, this chapter deals with the detection and discovery of codes that are intended to be private or secret.

There are two basic aspects of cryptologic surveillance which involve detecting and deciphering messages. These are hidden messages and coded messages:

hidden messages - those which are obscured from view by size, shape, color, visibility, context, or other attributes. A message may have been shrunk to microscopic size and hidden in a punctuation mark on the page of a telephone book. It might be transcribed with a material that is visible only under ultraviolet or infrared light or which is revealed only by a change in temperature or the application of chemical reagents. It may be split across a series of billboards flanking a long stretch of highway. It may be seen through a crack in the rocks only at a particular time of day. Hidden messages may or may not be coded.

coded messages - those which are obscured by transforming the information content into another system. Letters may be substituted for other letters, numbers may be substituted for letters, colors may be substituted for letters, or tonal values may be substituted for directions. One language may be substituted for another, math formulas may be substituted for musical notes, bird calls may be used to communicate outdoors. There are more sophisticated encryption systems which depend on more complicated encoding procedures than just substituting one form of information or one unit of information for another, such as key codes, and these are generally favored for sensitive documents or computer communications. Coded messages may or may not be hidden.

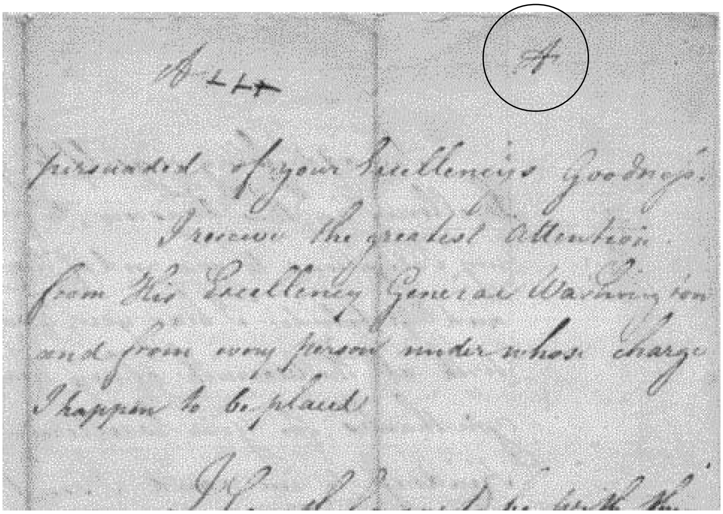
There are many different types of codes and ways to obscure messages, and not all are listed here, but a few examples include semaphore, map codes, rock codes (rocks piled to indicate direction or a message), alphabetic codes (e.g., Morse), tape codes (e.g., colored tapes on trees), machine-readable codes, and binary codes.

Invisible Ink

Invisible ink is relatively easy to make and has been used for centuries. Lemon juice is readily available for writing 'hidden' messages and during the American Revolution, writers would mix ferrous sulfate and water and write 'between the lines' of an otherwise innocent-looking correspondence to avoid interception.

There are three common ways to make invisible ink visible:

- heating, with a flame or light bulb,
- using a chemical reagent, such as sodium carbonate, or
- illuminating with a specific type of light (e.g., ultraviolet).



A 44

A

persuaded of your Excellency's Goodness.
I receive the greatest Attention
from His Excellency General Washington
and from every person under whose Charge
I happen to be placed.

I [illegible] be with the

In this letter from John André to Henry Clinton, dated September 1780, the letter "A" has been inscribed at the top of the last page, indicating that acid rather than heat should be used to reveal the message. [Clements Library Clinton Collection, copyright expired by date.]

Depending on how a message was created, using the wrong method to reveal the message may damage the chemistry and make it impossible to ascertain the contents. During the Revolution, John André, head of intelligence for the British commander-in-chief, Henry Clinton, used an initial on his letters to indicate how they should be read. The letter ‘F’ stood for ‘fire’ and the letter ‘A’ for ‘acid.’

Substitution Codes

The most common type of alphabetic cipher, and the easiest to generate, is a *substitution code* in which one unit or block of information is substituted for another unit of information. Substitution codes need not be one-to-one. A simple alphabetic substitution code in which the letters of the alphabet are substituted with another set of letters from the same alphabet is extremely easy to ‘break’ or decode. When spaces between words are eliminated, and groups of letters such as ‘ing’ or ‘sch’ are replaced with a single letter or group of letters with a different number of individual units, it becomes more difficult to decipher (though not much more difficult if you are an experienced decoder). By writing the whole message backward and adding nonsense words, it is even harder to break the code, but the general concept is still fairly simple. In spite of the ease with which substitution codes can be broken, they are still widely used in personal and business correspondence. School children often code messages to prevent classmates (and teachers) from discovering their contents.

RADIO ORPHAN
1935
ANNIE'S 35
HERE'S OUR BRAND NEW SECRET CODE AND SIGNS AND SIGNALS FOR 1935!
Radio Orphan Annie's
Secret Society
1935

A simple alphabetic ‘substitution code’ is one of the easiest and most popular means to hide a message. Spy and code stories from World War I resulted in many popular fiction and nonfiction books and commercial products for creating and reading codes. This Orphan Annie™ substitution code ring and accompanying book were released to consumers in the mid-1930s. The center ring rotates relative to the outer ring to set the ‘key’ letter relationship so that the rest of the code can be read easily off the outer dial. [Classic Concepts photos copyright 1999, used with permission.]

Key Lookup Codes

Some codes require the possession of a ‘key’ with which to decrypt and subsequently interpret a coded message. The coded message is said to be *encrypted*. A key code can be somewhat difficult to break if the format or content of the key is not known. Some of the better computer encryption schemes are based on key systems and they are now widely used to protect electronic data, including voice and computer communications.

Decoding Methods

There are thousands of decoding methods, just as there are thousands of codes, and these are discussed in a little more detail in Section 5 (Description and Functions). However, four basic foundation methods are mentioned here, as they apply to many aspects of cryptanalysis. These include

databases, tables, and precedence - A data archive of information related to a problem can sometimes be used to help solve it. For example, if a building collapses, a look at the data on similar buildings might reveal that there is a particular structural flaw common to those buildings. Another example is opening moves in chess. Over the decades, it has been noticed that certain moves lead to a higher probability of a good outcome and that Grandmaster chess players tend to favor them and to memorize them. Every once in a while someone comes up with a novel opening, but at the highly competitive international level, the openings have standardized somewhat for the first few moves to the point where they have been given names. Knowing them can give a recreational player an advantage over someone of otherwise similar playing ability. Secret service agents have vast storehouses of information about the cultures, habits, and priorities of other nations in order to interpret their actions and motives. Without this information, a move on the part of another nation that was not intended to be aggressive might be misinterpreted and lead to war. Thus, a knowledge base is an important aspect of decision-making and of carrying out cryptanalysis on foreign communications.

brute force - The process of finding a solution by trying every known possibility is called brute force. For example, one way to find out if 17 is a prime number (a number that can only be divided by one and itself) is to multiply together all the combinations of integers between 2 and 16 and see if the result of any of the calculations is 17. In other words, it's a long process that eventually yields results, but isn't necessarily the most efficient way or may only be an efficient way up to a certain point. When you want to find out if 9,342,154,673 is a prime number, brute force is going to take a long, long time, even with optimization methods. Thus, strategy and elimination are sometimes used to solve certain problems.

selected attack - With computer encryption algorithms, sometimes the nature and even the method used to encrypt a message are known. In this case, the most effective way to break the code is with mathematical techniques known to work for specific cases. Often when cryptanalysts discover a formula or technique that works for a specific code, they will publish it to make the community aware of the limitations of the code. In some cases, if the body using the encryption technique finds a way to break it, or if it is a secret service that doesn't want it known that they have broken it, they will keep the solution classified. Certain key encryption algorithms can be broken if the keys are short. In some cases, the same encryption system might be much stronger and more difficult to break, not by changing the nature of the encryption, but by making the key longer.

heuristics - Heuristics is a problem-solving process in which logic, elimination, and exploration are used to follow 'fruitful' paths of inquiry, those which are more likely to result in a solution. Artificial intelligence programs strive to incorporate effective heuristics. Many of the early computer chess programs used brute force and were slow and fairly easy to beat. Gradually, however, programmers added problem-solving heuristics (along with a database of strong opening moves) which, instead of calculating every possible move, would calculate moves based on knowledge and experience of what would more likely be strong moves. These might include strategies such as advancing pawns, crowding a Queen, using the bishop and knight in tandem, etc. Heuristics often are based on an intuitive human element and sometimes are based on algorithmic/mathematical discoveries of fruitful paths of exploration. To solve present-day computer encryption systems, a knowledge of probability, statistics, and geometry helps hone the heuristic intuition.

The above methods are almost always used together to different degrees, depending on the nature of the problem to be solved.

Fields of Study

The study of coding and its related fields has been divided up in a number of ways. Some of the more common fields of study within cryptology are

- coding theory, codes, and applied coding
- general information theory and mathematics related to cryptology
- decoding, cryptanalysis, cryptologic surveillance

3. Context

Cryptology is applied to many disciplines, from computer compression schemes to secure military communications, converting plain data to other less easily recognized forms has many advantages, not all of which are related to privacy. However, cryptologic surveillance is almost always used in the context of secrecy. Whether it's a child sending a secret message to a classmate two rows away, or a war department sending a coded message to troops on an aircraft carrier, the basic premise is the same, the sender wants only the intended recipient to be able to receive and/or decipher the message. Thus, the most common contexts for cryptologic surveillance involve the deciphering or discovery of a hidden or coded message intended for someone else.

Cryptologic surveillance used to be primarily used by secret service and military agents for apprehending messages from hostile individuals, forces, or nations, but to some extent, with the advent of encoded communications devices, cryptology is now practiced somewhat by people wanting to access the communications of others. On the Internet and now on cellular phones and other electronic products, encryption is used as a security measure. There are a certain number of people who like to decode these communications just for the challenge of breaking the code. There are some who do it for material gain, as in intercepting sensitive business communications. And there are some who do it in the interests of national security.

4. Origins and Evolution

Obscured messages and their deciphering have been pivotal in decisions made during global conflicts, including World Wars I and II. But their origins stretch back much farther than that, probably farther than we can know. Coded and hidden messages have allowed friends and lovers to share secrets for centuries. They have been an integral part of political intrigue; they provided a means for Mary Queen of Scots to escape her imprisonment and for Queen Elizabeth to prevent her later escape when Mary was again imprisoned. They now form an essential aspect of computer communications and have created more consternation in government policy discussions than almost any other single aspect of computer security.

Secret writing includes many different types of hidden and open messages which may or may not be ciphered. Surveillance techniques to detect and decipher these secret messages have evolved as the secret writings themselves have evolved. Surprisingly, it is only in the last few decades that reasonably secure encryption techniques have been developed. In prior ages, the systems were simple and often effective, but they were also rather easy to decrypt by someone clever and determined to do so.

Writing itself used to be 'secret' for the simple reason that very few people were taught to read or write. For many centuries, reading was a skill known only by clergy, rulers, their elder statesmen, and a tiny portion of the population with the talent to learn to read spontaneously without formal instruction (estimated today at about 2%, but in those days people had less exposure and opportunity).

When messages were drawn in sand or carved in stone, there was no easy way to transport them, but pigments for body adornment have been used for thousands of years and early messengers may have carried messages on their backs, heads, or buttocks or other parts of their anatomy to escape detection.

We can guess that additional early examples of secret writings were probably modifications of regular writing, letters or words that were written backward or upside down or in a slightly different style or color to indicate that certain letters were more significant than others. There are examples of Egyptian hieroglyphics that differ somewhat from the norm. This could have been a means to imbue them with special meaning or perhaps it indicated some subtle way to obscure a message or call attention to particular aspects of a message.

Clay tablets used in early communications weren't very portable or flexible, but once papyrus came into use, new systems could be developed, such as rolling or folding the papyrus and writing a message that could only be read if the paper was reassembled (if torn apart) or refolded in its original configuration. (There are some biblical references that indicate that rolling may have been done.)

Hidden writing has probably been in use longer than cryptography. Certain aspects of practical chemistry were clearly well understood in antiquity, given the sophisticated embalming techniques of the Egyptians. Since writing was already in use and pigments for body adornment were common at the time, there is a possibility that someone noticed that marks made with lemon juice disappeared as they dried. It takes only a little heat to make them reappear, so heating may have been one of the first examples of surveillance of secret writing. When hidden writing and cryptography were first used is not known, but they may have roots in ancient history. Those clever enough to invent a system of hidden writing might also have sought ways to detect and decipher the hidden writing of others.

The Roman Emperor Julius Caesar was apparently supportive of the use of codes for communications. The "Caesar Cipher" is a substitution cipher Caesar is said to have used to write to Cicero. These basic Caesarian ideas continued right through the Middle Ages and were not substantially challenged with more sophisticated systems until Renaissance times.

Correspondence 'seals' have been in use for many centuries by rulers and others of high social stature to identify and protect the contents of important messages. The royal seal, stamped onto a document with heated wax, was intended to safeguard the contents both by the implication that snooping would have dire consequences and also by the physical seal that would make it hard to pry it apart to look inside. The seal was one of the first 'tamper' devices. It may seem like a rather loose security system, since one could pry it open, rewrite the message (changing it, if desired), and reheat the seal on the backside to attach it to the new document, but both opportunity and forgery skills were necessary and resources for the average person were in shorter supply in the Middle Ages than they are now.

The use of tunnels, secret drawers, and hidden compartments is documented in many texts throughout hundreds of years. The people who built and used secret implements may also have used secret writings and hidden some of those writings in the secret places.

Journals have been written in code for many years and the privacy of journals designed for teenagers is still loosely guarded with simple locking flaps and keys.

The use of a *nom de plume*, a 'pen name,' or the anonymous authoring of a message or publication are two of the simplest ways to obscure identity and were common in the Middle Ages when death or excommunication could result from expressing 'heretical' thoughts. Anonymous publications sometimes had the identity of the author encoded into the text, chapter headings, or the binding of the book and there may be many of these that have not yet been detected. Men sometimes used pen names to protect themselves from political censure and many women used male pen names right up until the 1970s, because their professional competence and place in the workforce were denied them. There have been many periods of history where censure was so strong that entire volumes were written in code.

Hidden messages within a piece of writing are common and have a long history. The first (or second, etc.) letter of each paragraph, or of each sentence, or before or after each punctuation mark, for example, can be assembled into a shorter message which then may be deciphered forward or backward or using a key. Sir John Trevanion is said to have escaped confinement in a castle by receiving a tip from a jailer in this way.

During the Renaissance, when art and culture blossomed in western Europe, a German monk named Johannes Trithemius (1462-1526) penned a document called "Steganographia," based on a system of hiding a message and providing a 'clue' or key to aid in locating and deciphering the message. To this day, the term steganography has survived to indicate messages hidden within other messages, often without any indication that they are present.

Many persons have stated that Leonardo da Vinci wrote backward, sometimes called 'mirror writing,' to hide secrets of his inventions and tools of warfare, but the author doubts this explanation. Mirrors existed in the Renaissance that easily allowed backward-writing to be read, and most artists and virtually all traditional typesetters can read backward writing fairly easily, so it's not an uncommon skill. Given that da Vinci was left-handed and writing was accomplished with slow-drying, easy-smearing, quill-pen ink in those days, it is more likely that the resourceful da Vinci simply found it cleaner and more comfortable to write in the natural direction for the left hand. Further support for this theory is that Leonardo's images, which accompanied his text, were often more explanatory than the text itself and he made no attempt to obscure those. Da Vinci was a politically astute genius who earned his reputation and his living by promoting his ideas and designs to rulers and dignitaries of the time, so it doesn't seem likely that he would have taken extensive steps to hide his efforts.

Henry VIII, on the other hand, was always trying to get away with something that might provoke the ire of his detractors or the populace. He was a highly manipulative statesman, who managed to take several wives despite religious prohibitions against doing so. King Henry is reported to have made significant use of cryptographic services during his reign.

The Elizabethan Age and Beyond

The 1500s and 1600s were times during which scholarly writings about cryptology were not unusual and their application to affairs of state undertaken on numerous occasions.

Queen Elizabeth I, in the 1500s, was a wily ruler and determined to hold onto her crown in a time when rulers were often deposed or executed within weeks or a few short years of the start of their reigns. The Queen's security system, established by Sir Francis, Earl of Walsingham (ca. 1531-1590), was probably a significant factor in her long reign and set a precedence for generations to come. Walsingham had gotten his training and experience in foreign intelligence under William Cecil, Baron Burghley, and put the knowledge to use as

Elizabeth's Joint Secretary of State.

Queen Elizabeth I retained Walsingham in this position for many years. He was a meticulous and dedicated man who made ready use of spies and various means to cipher and decipher messages that might affect the monarchy, including those of the imprisoned Mary Queen of Scots. Secret messages had enabled Mary to escape imprisonment on a prior occasion years before, but Walsingham was not so easily fooled as her previous jailers. His administrative and surveillance resources were excellent. He not only gathered evidence against her from her correspondence but claims to have retrieved dozens of different cipher systems from her premises. This eventually led to Mary's execution and the rounding up of a number of her followers, based on the written evidence provided by his surveillance efforts.

Walsingham is also known for having uncovered news of an impending attack by the Spanish Armada upon England. His secret service included dozens of agents. Thomas Phelippes was one of the most talented, able to solve codes in multiple languages.

Cryptography was a familiar tool at least by Renaissance times. In 1565, Italian Giovanni Baptista della Porta published a simple but effective cryptographic table consisting of thirteen 'key' letters, with an alphabet in which the lowest line in the table moved one position to the right for each pair of capitals.

A number of texts, systems, and counter arguments were published at this time, including

- Blaise de Vigenère (1523-1596) wrote about ciphers and secret writing and created a system that remained unbroken for centuries.
- In 1588, Timothy Bright wrote a book called "The Arte of Shorte, Swifte and Secret Writing," which detailed a system of shorthand. While only loosely a cipher system, shorthand could provide a certain measure of light security, if the system were not understood by prying eyes. While shorthand systems are easy to decipher, they still provide a deterrent to the lazy or slow.
- Francis Bacon (1561-1626) had a particular interest in cryptology and referred to it in a number of his writings.
- John Wilkins (1641-1666) published "Mercury the Secret and Swift Messenger" in 1641, cautioning against weak ciphers. He wrote of a number of systems and developed at least one of his own.

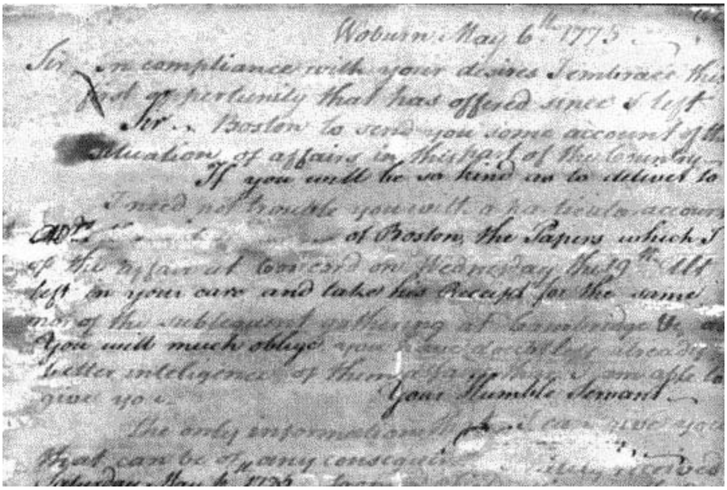
Armand Jean du Plessis, Cardinal and Duke of Richelieu (1585-1642) was the First Minister of France for almost twenty years and is said to have engaged in secret correspondence to bring about his political ends.

Technology and Cryptology

Fine craftsmanship was prevalent during and after the Renaissance. There were a lot of ingenious mechanical devices being developed in the decades that followed. Music boxes, coded looms, and concepts for calculating machines were being invented and it was only a matter of time before someone applied the idea of clockworks or cylinders to the creation of ciphering machines.

In the 1700s, the fathers of democracy, Thomas Jefferson, Benjamin Franklin, and George Washington all were interested in hidden writing and cryptography. During the American Revolution, written communications were routinely surveilled by both the British and Americans. Runners and riders were intercepted and the contents of their mailbags searched, often turning up war-related letters. Many of the British documents captured by George Washington are now archived in the U.S. Library of Congress.

To reduce the possibility of messages being intercepted, secret communications were used by George Washington's networks of spies when he commanded the Continental Army. Troop movements and other news were forwarded to General Washington through a system of secret correspondence. Invisible ink allowed hidden messages to be written between the lines of other innocent-looking correspondence. His secretary, Alexander Hamilton, used secret inks, codes, and symbols to conceal information from British eyes. James Lovell, a Boston school teacher who is considered the 'father of American cryptanalysis' provided George Washington with news about British troop activities.



Woburn May 6th 1775

Sir In compliance with your desires I embrace the
first opportunity that has offered since I left
Sir Boston to send you some account of the
situation of affairs in this part of the Country
If you will be so kind as to deliver to
I need not trouble you with a particular account
Mr. [illegible] of Boston, the Papers which I
of the affair at Concord on Wednesday the 19th Ult
left in your care and take his Receipt for the same
nor of the subsequent gathering at Cambridge &c as
You will much oblige you have doubtless already
better intelligence of them [illegible] I am able to
give you
Your Humble Servant
The only information [illegible] I can give you
that can be of any consequence [illegible] received
Saturday May 6th 1775 [illegible]

This detail of a three-page letter, written by Benjamin Thompson in 1775, actually carries two messages, a longer visible message and a short invisible message. The visible letter begins "Sir, In compliance with your desires ...." However, interspersed within it is a message written in invisible ink (now made visible) that states "Sir | If you will be so kind as to deliver to | Mr.   of Boston, the Papers which I | left in your care, and take his Receipt for the same, | You will much oblige | Your Humble Servant | [erased] | Saturday May 6th 1775." [Clements Library Gold Star Collection historical document, copyright expired by date.]

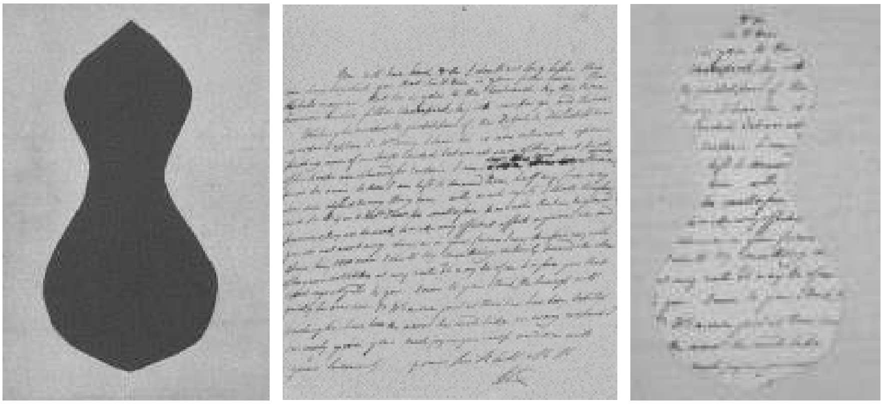
Navajo band members were also reported to have been used as messengers. Since the Navajos had no written language, and their spoken language wasn't known to many and didn't resemble English, there was pretty effective 'encryption' inherent in transmitting a message through spoken Navajo.

American and British spies in the Revolutionary War used both simple and elaborate schemes for hiding messages and the paper on which they were written. They were often rolled or folded and hidden inside bullet casings, small silver balls (which could be swallowed), quill pens, and buttons. The methods of detecting these messages ranged from simple searches, to the use of emetics to cause the suspected messenger to vomit up anything which might have been swallowed. It may be that some of these messages were never delivered or discovered and are still hidden in garments of the era (or buried with their bearers). With new X-ray and other scanning technologies, it may now be possible to examine preserved relics in museums without taking them apart or otherwise damaging them.

Some of the methods of conveying secret messages during the Revolution are revealed by John André in a four-page letter to Joseph Stansbury in May 1779 in which he writes about codes, hidden writing, key words in conversation, and keeping the messengers ignorant of the contents of their messages.

> “You will leave me a long book similar to yours. Three Numbers make a Word the 1st is the Page and the 2d the Line the third the Word a comma is placed between each Word when only the first letter of the line is wanted in order to compose a Word not in the book, the number representing the Word will be + Unit with a stroke across. In writings to be discover’d by a process F is fire and A acid.
>
> In general information, as to the Complesion of Affairs an Old Woman’s health may be the Subject. The Lady might write to me at the Same time with one of her intimates She will grasp who I mean, the latter remaining ignorant of interlining & sending the letter. I will write myself to the friend to give occasion for a reply. This will come by ~~any~~ a flag of truce, exchang’d Officer & @ every messenger remaining ignorant of what they are charg’d with, the letters may talk of the Meschianza & other nonsense.
>
> You will take your mysterious notes from this letter and burn it or rather leave it Sealed for me with -------”
>
> [Excerpt transcribed from the original John André letter in the Clements Library Clinton Collection.]

The Journals of the Continental Congress notes from Friday, 7 April 1786, mention the use of cipher for correspondence in a letter of December 1785 from John Adams to John Jay that was referred back to the Secretary for Foreign Affairs to report. The report was regarding the attitude of Great Britain toward the United States, recorded as being transcribed in cipher No. 84, VI, folio 43, with a translation in folio 51.

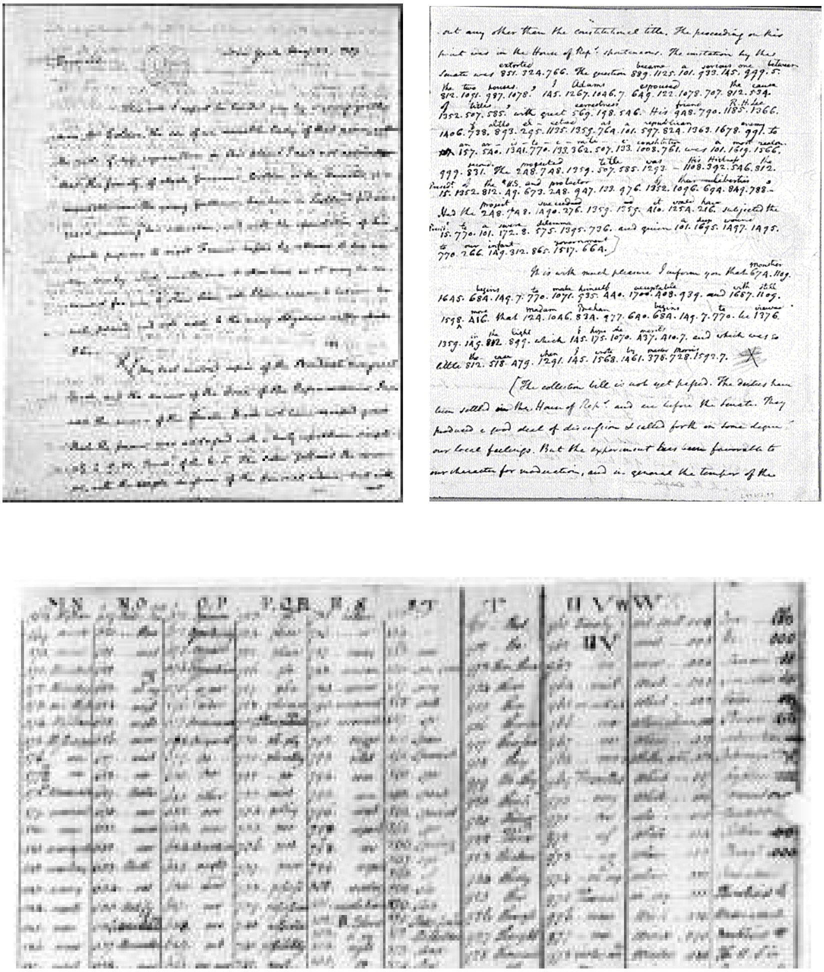


Sometimes a mask was used to create a seemingly innocent message with a hidden message incorporated into the main part of the text. Henry Clinton wrote a letter to John Burgoyne dated 10 August 1777 that used this technique. The mask is shown on the left, the innocent-seeming message in the middle and the intended message through the mask on the right. Careful composition of the words in the letter had to be considered when writing the text. If it was awkward, rather than natural, it might create suspicion. [Clements Library Gold Star Collection, copyright expired by date.]

The Jefferson cylinder was developed in the 1790s, consisting of three dozen discs, each with a random alphabet, which could be organized in different ways to change the code. This cylinder somewhat resembled the metal cylinders that were coded with pegs or bars to make music boxes.

In 1830, a passionate French teenager named Evariste Galois (1811-1832) wrote a paper in mathematics that was published after he died in a duel. This remarkable paper led to further research in finite fields called Galois fields, which were to become important years later in disciplines such as cryptology, coding theory, and specialized areas of geometry.

In 1833, Kerckhoff wrote "The Handbook of Applied Cryptography" which discussed some generally preferred characteristics of an effective cryptosystem. Kerckhoff shed light on a way to decipher an 'unbreakable' system devised by de Vigenère in the 1500s. Kerckhoff principles are still mentioned today.



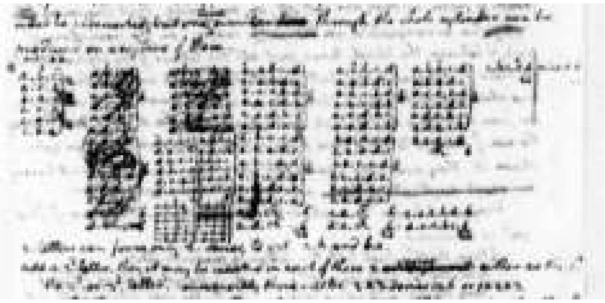
-out any other than the constitutional title. The proceeding on this
point was in the House of Rep.s spontaneous. The imitation by the
extorted became a serious one between
Senate was 851. 324. 766. The question 889. 1125. 101. 933. 145. 999. 5.
the two houses. J. Adams espoused the cause
812. 1051. 987. 1078. 145. 1267. 1046. 7. 649. 122. 1078. 707. 812. 534.
of titles, earnestness friend R. H. Lee
1352. 507. 585. with great 569. 198. 546. His 948. 790. 1185. 1366.
republican enemy
1406. 738. 893. 295. 1135. 1359. 764. 101. 597. 824. 1363. 1678. 991. to
constitution a most
157. 540. 1341. 770. 133. 362. 507. 133. 1008. 761. was 101. 1619. 1566.
second projected title was His Highness the
999. 831. The 248. 748. 1359. 507. 585. 1293. – 1108. 392. 546. 812.
Presid.t of the U.S. and protector of their liberties
15. 1352. 812. 49. 673. 248. 947. 133. 976. 1352. 1096. 694. 849. 788. –
project succeeded it would have
And the 248. 748. 1490. 276. 1359. 1359. 410. 1254. 216. subjected the
Presid.t to a severe dilemma a deep wound
15. 770. 101. 172. 8. 575. 1395. 736. and given 101. 1695. 1497. 1495.
to our infant government
770. 266. 149. 312. 865. 1517. 664.]

monsieur
It is with much pleasure I inform you that 674. 1109.
begins to make himself acceptable with still
1645. 684. 149. 7. 770. 1071. 935. 440. 1700. 408. 939. and 1657. 1109.
more madam Brehan begins to viewed
1598. 416. that 124. 1046. 834. 977. 640. 684. 149. 7. 770. be 1376.
in the light I hope she merits
1359. 149. 812. 899. which 145. 175. 1070. 437. 410. 7. and which was so
the case when I wrote by master Morris
little 812. 518. 479. 1291. 145. 1568. 1461. 378. 728. 1592. 7.

[The collection bill is not yet passed. The duties have been settled in the House of Rep.s and are before the Senate. They produced a good deal of discussion & called forth in some degree our local feelings. But the experiment has been favorable to our character for moderation, and in general the temper of the

A letter from James Madison to Thomas Jefferson in 1789 clearly shows a portion written in cipher. Note the cipher digits on the second page, with the translation penned in above the numbers. The bottom image shows the lookup table used to determine which words correspond with the numbers in a letter. A closer look indicates that it is a very orderly cipher, with numbers assigned to the words alphabetically, which actually weakens the security of the cipher. If some of the numbers are decoded and the orderly pattern of the numbers is discovered, it is much easier to decode the rest of the message than if the numbers had been assigned to words on a random basis. Jefferson made use of a number of different ciphers. [Library of Congress James Madison and Thomas Jefferson Papers, public domain by date.]

In the 1840s, Edgar Allen Poe, poet and writer of dark and mysterious literature, showed himself to be an aficionado of cryptology. In his story, "The Gold Bug," he developed a mystery around a secret message that may have spurred interest in this fascinating subject on the part of the public.

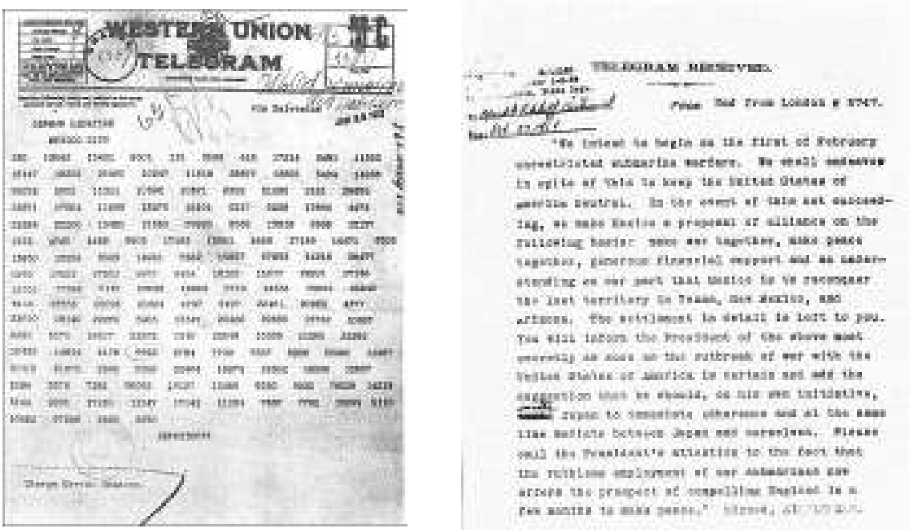


A portion of Thomas Jefferson's correspondence describing a cipher wheel system. [Library of Congress Thomas Jefferson Papers, public domain by date.]

When Allan Pinkerton, the famous detective, and Samuel Morse Felton apparently uncovered a secessionist plot to assassinate President Lincoln, Pinkerton sent Felton a coded message "Plums delivered nuts safely," to indicate that he had arranged the successful transport of President Lincoln through Baltimore. Pinkerton and his colleagues were actively engaged in intercepting and interpreting enemy communications during the Civil War.

World War I

Sometimes a single encrypted message can be a pivotal document during a War.



WESTERN UNION TELEGRAM

TELEGRAM RECEIVED.

From 2d from London # 5747.

"We intend to begin on the first of February unrestricted submarine warfare. We shall endeavor in spite of this to keep the United States of America neutral. In the event of this not succeeding, we make Mexico a proposal of alliance on the following basis: make war together, make peace together, generous financial support and an understanding on our part that Mexico is to reconquer the lost territory in Texas, New Mexico, and Arizona. The settlement in detail is left to you. You will inform the President of the above most secretly as soon as the outbreak of war with the United States of America is certain and add the suggestion that he should, on his own initiative, invite Japan to immediate adherence and at the same time mediate between Japan and ourselves. Please call the President's attention to the fact that the ruthless employment of our submarines now offers the prospect of compelling England in a few months to make peace." Signed, ZIMMERMANN.

The Zimmermann telegram described the German intent to break the Sussex Pledge and engage in unrestricted submarine warfare. It further entreated Mexico to join the Germans against the U.S. in exchange for U.S. territory. The breaking of this code by British agents was a pivotal piece of intelligence drawing the then-neutral U.S. into World War I. The coded telegram on the left is signed Bernstorff, the German ambassador in Washington. [Clements Library Gold Star Collection, copyright expired by date.]

The European nations were engaged in a significant armed conflict between 1914 and 1917. Under Woodrow Wilson, the United States remained neutral until early 1917. When Germany broke a pledge (the Sussex Pledge) to limit submarine warfare, the United States severed its diplomatic ties with Germany. The conflict came to be known as the Great War and now is more commonly known as World War I.

In January 1917, British cryptographers deciphered a telegram from Arthur Zimmermann (1864-1940), the German Foreign Minister, to von Eckhardt, the German Minister to Mexico. The content of the message entreated Mexico to join in the German cause in exchange for U.S. territory. In February, the British revealed the telegram to President Woodrow Wilson and it was published in the press in March. On 6 April 1917, the U.S. formally declared war on Germany and its allies.

Following the War, a German engineer named Arthur Scherbius (1878-1929) developed a cryptographic machine and tried to interest the German Navy in the invention. The Navy declined, so Scherbius marketed it instead to businesses such as banks that wanted to secure their communications. It was named “Enigma.” The German forces evidently changed their minds about the Enigma machine, adapting modified versions for the Navy, Army, and Air Force during the 1920s and 1930s.

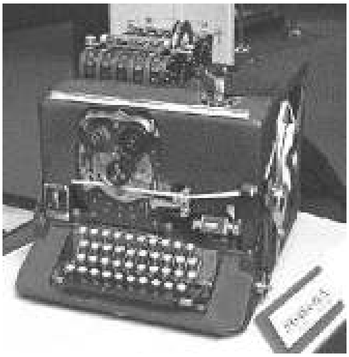
The cracking of the German code in World War I inspired a wave of enthusiasm for spies and ciphers in the post-War years. Three examples of simple alphabetic substitution coders/ decoders sold or given away to consumers are shown here. They consist of rings that could be turned in relation to each other to create different codes based on the same principle; they are just packaged in different ways Left: A simple cardboard dial. Right: A collectible metal “Captain Midnight” decoder. Bottom: A “Spy King” decoder box with the code ring built in on the left side. [Classic Concepts photos copyright 1999, used with permission.]

Thus, the Enigma was known before the outbreak of World War II, and Polish and French cryptanalysts had already broken a portion of the Enigma code by the late 1920s. This would later aid British cryptologists, although it would still be a challenge, with the Germans making changes to the system during the War.

America After World War I

Herbert O. Yardley (1889-1958) was a telegrapher for the U.S. State Department during World War I. After the war, Yardley established a cryptanalytic bureau whose job it became to decipher codes in foreign diplomatic correspondence. This organization came to be known as the "Black Chamber" or MI-8 and made history by decrypting encyphered Japanese correspondence. In 1929, Yardley was directed to shut down operations and turn the unit resources over to William F. Friedman (1891-1969) and the Signal Intelligence Service. Friedman, a Russian immigrant who had set up a cryptology school with his wife, became director in 1930. In response, the disenchanted Yardley wrote "The American Black Chamber" describing the detailed activities of his former unit. The second edition was suppressed by the U.S. government, but not before the first edition reached other nations, who promptly changed their codes.

Friedman had his work cut out for him. Not only had the foreign codes been changed, but foreign nations were now especially wary. Nevertheless, Friedman's unit succeeded, a few years later, in decoding the new Japanese code, called the Purple Code. This allowed the U.S. to decipher many of the Japanese communications during the war.

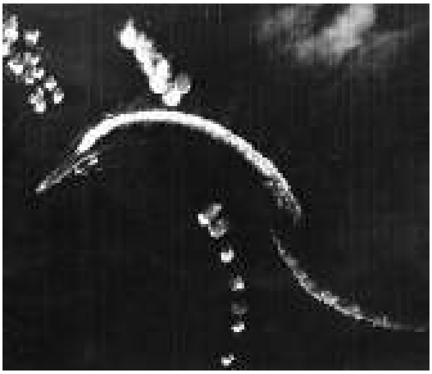


The National Security Agency sponsors the National Cryptologic Museum, which includes, among other exhibits, historical information and artifacts related to Yardley and the Black Chamber (left) and a variety of cipher machines, including some from other countries. Shown here is a Jade machine, in the same family of encryption machines as the famous Japanese Purple machine cracked by U.S. Cryptologists. A portion of a Purple machine is also on exhibit. [National Security Agency Cryptologic Museum news photos, released.]

In August 1940, U.S. Army Intelligence engaged in a decryption effort named MAGIC to break the Japanese diplomatic code, making it possible to access the content of a radio message on 7 Dec. 1941 from Tokyo to the Japanese Embassy in Washington, D.C. Thus, eight hours before the Japanese bombed Pearl Harbor, news of the break in diplomatic relations between Japan and the U.S. was intercepted, but the political policies necessary to quickly process and respond to this information and avert the bombing were not in place or, apparently, were ineffective.

> "Prior to the attack, the Americans had broken several Japanese naval and diplomatic codes and ciphers and also had intelligence indicating that an action was imminent. Lacking was the accurate and timely processing and evaluation of the available information, which in a well-organized and smoothly running organization would have been a matter of routine. Pearl Harbor stimulated the development of an efficient secret service and led to the establishment of the CIA in its present form." [Dr. Georg Walter, "Secret Intelligence Services," August 1964.]

The U.S. Navy Radio Intelligence Section had responsibility for providing communications intelligence on the activities of the Japanese Navy. It had to intercept the radio communication, decipher them, translate the text, and forward the results to the appropriate authorities. The various intercept stations, dotted around the Pacific, exchanged information, data, codes, and keys. The Navy had two categories, Traffic Intelligence (TI), more general information about the communication, and Decryption Intelligence (DI), more specific information derived from the content of the message itself. In spite of the gradual losses of some of its intelligence stations, the Navy learned about Japanese plans to attack Port Moresby and Tulagi, prior to the Battle of the Coral Sea. While U.S. losses were high in the Battle of the Coral Sea, it was a turning point and a setback for the Japanese and weakened their position in the Battle of Midway that followed. After the Battle, even those skeptical about the value of cryptologic data had to accede that it had provided essential information strongly affecting the outcome.



Left: An aerial surveillance photo shows the Japanese aircraft carrier Hiryu maneuvering to avoid bombs dropped by the U.S. Air Force B-17 bombers. Naval intelligence cryptanalysts had advance notice of the 'surprise' attack and were able to rally forces to counter the Japanese offensive. Right: Burning oil tanks are seen in the background after the Japanese air attack on Sand Island, Midway, in June 1942. [U.S. Navy historical photos, released.]

The War on the British Front

Alan Turing (1912-1954), the shy and eccentric father of much of modern computing became part of the elite group of code-breakers working on the German Enigma code, and its successors such as the Fish codes, at Bletchley Park. The cryptanalysts at Bletchley Park were there under the umbrella of the British Foreign Office's Government Code and Cypher School and their activities were kept secret as much as was possible.

During the War, Turing and Johann (John) von Neumann (1903-1957), the brilliant founder of game theory, were involved in developing concepts of programmable computers which were used in the efforts to crack the German codes. The highly classified Colossus, an advanced Boolean logic calculator that preceded the ENIAC, was based in part on their ideas.

The British had a code machine of their own, called the British Typex, which was similar to the Enigma, but apparently more complex and presumably more secure. The Typex was apparently never fully put into service.

Cryptology had a significant impact on the outcome of World War II. Allied knowledge of the content of intercepted communications about German movements and plans gave them a decisive advantage.

Postwar Developments

The defeat at Pearl Harbor and the failure of U.S. officials to process the information obtained by cracking the Japanese code and intercepting radio communications illustrated the need for better lines of communication with the cryptologic unit. In 1945, the U.S. State Department, Army and Navy forces, acknowledged that a better system was needed. As a result, the Coordinator for Joint Operation (CJO) was established in 1946 to coordinate cryptologic services. The Joint Intelligence Bureau, which replaced the Joint Intelligence Committee in 1946, became a primary agency for Central Intelligence Analysis.

In 1947, General Hoyt Vandenberg of the U.S. Air Force endorsed a separate Air Force cryptologic intelligence organization to provide independent support to the evolving Strategic Air Command. A 1948 agreement between the Air Force and the Army Security Agency set out a mobile and tactical role for the U.S. AFSS. In June 1948, the Air Force Security Group was established to oversee the transfer of resources to the as-yet unestablished Air Force cryptologic agency. In spring 1949, Secretary of Defense Louis Johnson announced the Armed Forces Security Agency (AFSA) to oversee the separate cryptologic efforts.

One of the groups that is currently most active in gathering and interpreting historical information on intelligence which includes cryptologic information is the International Intelligence History Study Group. Members of IIHSG are engaged in compiling the manuals and cover sheets related to the ciphering methods used by the Wehrmacht (the German armed forces), as a complete set had not been reconstructed as of 1996. Gilbert Bloch, who suggested the project, has also obtained a monthly list of Enigma settings, "Sonder-Maschinenschlüssel BGT." These efforts are gradually beginning to build a clearer picture of one of the most historically significant uses of cryptology in warfare.

Computers, Electronics, and Cryptology

Gigantic, expensive, vacuum-tube computer systems with limited calculating abilities began to emerge in the 1940s and 1950s. For the first two decades of their existence, they were used almost exclusively in government, scientific research, and big business settings. The ENIAC computer, used by the U.S. Army to calculate ballistics tables and trajectories beginning in 1946, weighed in at 30 tons.

Computers changed cryptology and cryptanalysis in some fundamental ways. Not only could more complex or extensive encryption and decryption techniques be applied, but codes of an entirely different character could be developed, compared to those devised by hand or with mechanical tools.

Another important aspect of early computing was that it was expensive. Since only a privilege few had access to computing resources, it put encryption and decryption sciences in the hands of those with power or money. It was not until the transistor was invented in 1947, and electronics gradually came into the hands of the general public, that controversies over who could encrypt their messages and who couldn't became hotly contested.

The development of computers and computer networks also provided a means by which private citizens could more closely follow the actions and decisions of government policy makers and secret service agencies. Computer networks further facilitated global communications on an unprecedented scale. Individuals bent on crime could now collaborate with others in distant states in a way that had never before been possible. Dealers in illegal shipments and money launderers could carry on their business on a grander scale, using encrypted telecommunications technologies. Concerns on the part of law enforcement agents over these changes in society led to attempts to update wiretapping authorizations to include electronic communications. The National Security Agency sought empowerment to decrypt foreign telecommunications and private citizens grew concerned about how generalized policies might affect their basic freedoms. As computing moved into the late 1980s and early 1990s, controversy followed every new evolution in encryption technology and every step on the part of the government to gain access to private communications.

The 1990s - Secure Communications and Controversy

By the 1990s, businesses were computerized, business software was sold with various security features, and the electronic encryption of radio and data communications was becoming commonplace. National security experts were alarmed at the potential for criminals to carry out clandestine planning without intervention by law enforcement agencies and the general public was alarmed because the NSA and the FBI wanted broader access and wiretapping authorization in order to be able to intercept secure electronic communications. This important struggle is discussed at some length in the historical sections of Chapter 1 (Introduction and Scope) and Chapter 2 (Audio Surveillance).

By 1990, the U.S. National Security Agency (NSA) had established a lab for developing special-needs computer resources, such as electronic chips and circuit boards. This served two purposes. It allowed the NSA to design and construct circuits that weren't obtainable through commercial channels and it ensured the secrecy of the specialized circuits and the state-of-the-art of NSA resources. The NSA was developing one of the most extensive computer facilities in the country which was used, in part, for encryption and decryption development and applications.

In 1993, the Clinton Administration announced the *Escrowed Encryption Initiative* (EEI) commonly known as the *Clipper Initiative* after it was developed as a hardware device called the *Clipper Chip*. The Clipper Chip was a hotly contested system incorporating a classified, secret-key encryption algorithm called SKIPJACK that was implemented in an Escrowed Encryption Standard (EES). The controversy over the EEI arose partly because of a Law Enforcement Access Field (LEAF) incorporated into the system intended to allow access by law enforcement agents to otherwise secure communications. The keys were intended to be deposited with the National Institute of Standards and Technology and the U.S. Treasury's Automated Systems Division. Thus, a court-authorized 'wiretapping' could be deciphered through obtaining the key information. The computing population didn't like the system and debated it over the Internet and through elected representatives.

Transfers of Regulatory Authority

Two key events occurred in 1996 with regard to encryption. The Government relented to public pressure and presented a modified Clipper Chip plan. It also reclassified encryption technology. Up to this point, encryption was treated pretty much the same as a physical weapon. The export of the technology was regulated under Arms Export acts and regulations. However, regulatory control for non-military encryption technology was transferred to the U.S. Department of Commerce and new regulations were issued at the close of the year, to be administered by the Bureau of Export Administration. Categorical distinctions for different types of encryption were now being formally recognized.

Thus, the government came back with a modified plan (Clipper II) with a change in the escrow agencies with input from users. The debate still didn't die down. A government draft in 1996 (called Clipper III by some) proposed a key management infrastructure based on a voluntary key escrow plan. At this point, users would be permitted to choose their encryption algorithms. Public-key certificates would be issued by a Certification Authority. In some cases, if certain requirements were met, self-escrow might be an acceptable option. These were significant adjustments to the original plan, but there was still opposition. A Technical Advisory Committee was formed, but after many meetings, a comfortable agreement between government and business was not reached.

In 1997, the Department of Defense made an announcement that the National Security Agency (NSA) would not be implementing EES in favor of a *key recovery* system. It was published as the "Electronic Data Security Act of 1997." It was amended only two months later, as a response to further criticisms. A number of bills and options were presented over the next two years with no general consensus. Monetary incentives in the form of tax credits for developing and producing recoverable cryptography were even proposed to try to come to a resolution or compromise.

By summer 1998, the U.S. Department of Commerce restrictions on software exports were being challenged at several court levels, with courts initially ruling that the government export regulations on encryption were constitutional.

By this time, programmers and hardware designers had developed ways to integrate the Internet with public telephone systems and started promoting Internet phone systems. The traditional phone carriers were alarmed and opposed the systems, which essentially threatened to make long distance calls over the Internet free of charge. Internet phone systems also blurred the line between regular phone regulations and regulations for electronic communications. Law enforcement agents were more concerned than ever about their ability to intercept communications and sought to adjust the scope of 'wiretapping' to encompass electronic technologies while still facing continued opposition.

Encryption's Soft Underbelly

At the 1998 EPIC Cryptography Conference, Robert Litt spoke on behalf of the Attorney General's office regarding the strength of DES and reiterated the need for a law enforcement 'back door' to access encrypted communications. Shortly thereafter, government assertions regarding security faced an even stronger challenge from cryptanalysts.

In July 1998, the Electronic Frontier Foundation announced that its EFF Data Encryption Standard Cracker (ESC) machine had cracked the Digital Encryption Standard (DES) in less than three days, substantially faster than a network of computers that had previously established a record of 39 days.

Undersecretary William Reinsch responded to this announcement a month later on behalf of the Department of Commerce stating law enforcement's point of view, which included the following statement regarding the practicality of the code-breaking success:

> "... Spending 56 hours breaking a single message in a situation where those making the attempt knew where the message was and, presumably, knew it was in English, is not analogous to the real-time problems facing law enforcement. At the same time, this is a fast-moving sector, and recent developments in it, including EFF's own efforts, demonstrate a need to continually review our policy in light of such changes. In fact, such a review is underway right now, but like previous reviews, it will continue to be based on the same fundamental principles that underlie our current policy...."
>
> [William A. Reinsch, United States Department of Commerce letter to Barry Steinhardt, President, the Electronic Frontier Foundation, 26 August 1998.]

Half a year later, the Encryption Standard Cracker, designed by John Gilmore at a cost of under $250,000, had cracked a message encoded by RSA Data Security in less than a day. This strengthened the skepticism surrounding the security of DES and U.S. Government advocacy of its use. The ESC machine had cracked the code in conjunction with the nonprofit Distributed.net for the DES Challenge, which was an annual event hosted by RSA Data Security offering cash prizes for successful attacks and larger prizes for fast attacks.

Data Security and International Software Export Regulations

The Technical Advisory process on electronic encryption continued and the group released a report for which feedback could be submitted until winter 1999. Before the deadline for comments on the report, in September 1999, a proposed draft of the “Cyberspace Electronic Security Act of 1999” was released. Once again, it contained provisions for access to encryption keys by law enforcement agents. The FBI was to be provided with funding to aid law enforcement agencies to deal with what they considered to be increasing encryption use by criminals.

While the public and the government were trying to work out issues of information access and privacy, U.S. computer vendors were trying to maintain their leadership in the global marketplace. For several years there had been pressure on the government from the U.S. software-marketing community for looser restrictions on encrypted products. Vendors had persistently argued that U.S. export restrictions had a negative effect on their international competitive edge. On the other hand, law enforcement officials who feared that covert communications of an illegal nature would be facilitated by stronger encryption argued against the change. The law enforcement community was further concerned that the detection and collection of evidence to convict in cases of criminal activities, both domestic and foreign, would be greatly impeded by increased encryption.

U.S. businesses wanted to be able to export stronger encryption schemes. The U.S. public didn’t want the government to have special privileged access to any kinds of messages and the various security agencies felt their power to carry out their responsibilities were being eroded. Trade-offs were proposed. Certain government parties suggested that encryption export laws could perhaps be relaxed if law enforcement was provided with keys or other methods of access. A bargaining tone had been set.

Meanwhile, the European Union was continuing its task of uniting Europe into a common market that would exceed the population size of the U.S. once it was fully integrated. In conjunction with this, a number of European nations were beginning to export stronger encryption technologies than were being provided by American vendors. The competitive pressure was cited in further U.S. encryption debates.

In July 1999, a House Armed Services Committee hearing listened to concerns by the Attorney General and the Director of the FBI regarding the proposed relaxation of encryption restrictions on electronic communications-related products. Law enforcement officials warned that the ability to carry out investigations of illegal activities would be severely hampered if the U.S. sanctioned high-level encryption on products ranging from cell phones to computer software. Officials were particularly concerned that their ability to detect and investigate criminal activities such as international terrorism, economic fraud, narcotics and weapons trafficking, and related violent crimes would be greatly curtailed.

Export Regulations Adjustments

In September 1999, President Clinton relaxed restrictions on the export of privacy-protecting encryption products, a move intended to ‘level the playing field’ in terms of international protection of data security.

The White House countered the opposition of the FBI and others by promising to enable law enforcement agents to obtain encryption ‘keys’ stored with third parties, following a court order similar to that obtained for requesting a wiretap. The situation could still be complicated however, by two-key systems, if the person holding the second key refused to divulge the information.

It's possible that the export-relaxation announcement may also have been a political 'face-saving' gesture to the international community. Widespread criticism broke out in Europe in the mid-1990s when it was discovered the U.S. software for export was only weakly protected, with most of the encryption key information provided to the National Security Agency (NSA). Several European nations discovered that their documents were far less secure than they had assumed at the time of purchase.

Whatever the motivations for the Clinton announcement, encryption was officially sanctioned by the White House, pending submission of the encrypted products to the U.S. Department of Commerce for one-time review prior to export. Thus, regulations for products with up to 64-bit key lengths were loosened and those with over 64 bits could be allowed a license exemption provided they were not shipped to a short list of countries suspected of terrorist intentions (along with a few other stipulations).

These regulatory changes were clearly intended to address the needs of vendors shipping products packaged in physical boxes. The guidelines still left a lot of questions regarding the distribution of virtual packages on the Web and multinational collaborative projects. Presumably software vendors couldn't permit the download of software by foreign buyers without a Department of Commerce review, a bureaucratic hurdle that could hurt individual software developers and small entrepreneurial companies establishing Web-based businesses.

The resolution of encryption policies will take time. Meanwhile, new encryption technologies continue to be explored and developed.

An Unfortunate Enigma

On 1 April 2000, an Enigma three-rotor cipher machine, a valued historic relic of World War II was stolen from the mansion at Bletchley Park where the gifted scientists and codebreakers applied their skills to breaking the German codes in the 1940s.

5. Description and Functions

Some people write coded messages to give a little privacy to their correspondence, or simply because it is personally convenient. Beatrix Potter, the author of the Peter Rabbit books, used a sort of 'coded' writing in her journal, but it may have been a way that was comfortable for her rather than a deliberate attempt to obscure. As mentioned earlier, Leonardo da Vinci probably wrote backward for reasons of convenience.

Businesses encrypt their messages and electronic financial transactions to ensure privacy and protection against theft and fraud. This is especially true for Internet transactions and other computer network electronic transfers, particularly those in the banking business.

Governments encrypt their communications to prevent against aggression, economic disadvantage, and terrorist acts. They also rely heavily on encryption software for creating, sending, and decrypting messages. These are usually based on 'key' encryption systems, which are difficult to break if the keys are sufficiently long.

Since this chapter is about cryptologic surveillance, it is not about coding messages, but rather about discovering them and, to some extent, decoding them. Thus, it focuses on two aspects, discovering messages and discerning their contents.

Discovering Messages

Hidden messages may be found deliberately or accidentally. Checking the pockets of a slain or captured messenger might reveal a written or other type of message. Rifling the drawers of someone suspected of stealing might bring out a coded diary. More often, though, hidden messages are deliberately sought during wartime or during times of highly competitive business transactions.

The fact that a message is obscured is not necessarily a secret. We all know that sensitive government communications are classified, obscured, secured, and often encrypted. Many employees sign voluntary nondisclosure agreements when they are hired by a new employer. Users who buy spread-spectrum wireless phones usually know they are getting a certain amount of security built in to their private or business communications.

Discerning Message Contents

Sometimes people decipher messages because they are nosy, usually wanting to know about personal relationships. Some people do it to get a 'news scoop' or for other monetary reasons related to business. Some people do it because they are temperamentally drawn to solving puzzles and 'mysteries.' Others do it in the course of their work duties, particularly those employed by the secret services.

The motive for deciphering a message is often related to how hard a person will try to decipher it. For most personal motives and many business motives, people will give up fairly easily. It isn't worth the weeks or months that it takes to unravel the messages and not everyone has the skill and patience to succeed. Those who like to solve mysteries usually devote only as much time as they feel they have to spare. Those who do it in the course of their work may spend months or years unraveling the more sophisticated problems.

There is no one method for breaking a code, because there are thousands of ways to make a code. It takes persistence, patience, logic, insight, and a little bit of intuition to find and decipher hidden and encrypted messages. It also helps to have a good background in the various schemes that have been used over the years. These days, with sophisticated computer programs and advanced mathematical techniques, it is almost essential to have a good math background, as well, in order to deal with the types of software that are now used to handle a great majority of encrypted communications. Codes are becoming harder to break, but 'unbreakable' codes are often shown to be fallible by some brilliant sleuths who put their minds and computer resources into cracking them.

Some codes can be broken in more than one way. Obviously, in breaking a simple substitution code, the easiest way is to get a hold of the original coding ring or table or one like it. Since this is often not possible, analyzing the patterns of letters until familiar landmarks appear will eventually lead to the same result. It just takes a little longer. Finding a written translation by the recipient of the coded letter is a third option and, while some people might laugh at this solution, it is often the best, as the person is usually the weakest link in any code. In other words, looking on a person's computer monitor for a Post-it™ note with a password written on it is often much easier and faster than trying to 'break in' to their secure account by trying thousands of passwords. A knowledge of human nature is important in all aspects of cryptology. Birthdays, names, and information about loved ones are frequently used as passwords. Knowing this makes it easier to gain unauthorized access to accounts.

Cryptanalysis Strategy

One of the key aspects of breaking a code is finding a weak element. The human element was mentioned in the previous paragraph as it is often the weakest link, but sometimes the human element is not available for analysis, or the code is intercepted far from its origin or destination. In these cases, other weak elements can be sought. Here are just a few examples:

- The weak element might be the language in which it is written. For example, the English language has many consistent patterns. Sentences are constructed in certain ways, each letter of the alphabet has a particular frequency of use in normal correspondence, and certain words like 'the' or 'a' or 'I' are common giveaways. Sometimes parts of an intercepted message aren't even encoded. If a time or date or important name is spelled out, it can provide a key as to the content of the entire message. Thomas Jefferson and his correspondents would sometimes encode only part of a message, betraying information about sentence style, possible content, etc. through the unencoded portions of the text.
- The weak element might be tidiness. Lookup tables that are neatly numbered or alphabetized or organized according to categories are security weaknesses. If small parts of a message with random lookups are decoded, the decoded parts don't give away much about the rest of the message. If ordered lookups are used, however, decoding small parts can provide significant clues as to the structure of the rest of the message.
- Sometimes the weak element is sloppiness. Many codes derive their security from the fact that the key or code changes every time it is used. Thus, decoding one message may not provide any information about subsequent messages. However, if the coder (or the computer algorithm) fails to change the code each time, the next message may give away the structure of the previous message and its own from a cross-comparison.
- The overt nature of the message itself might be the weak element. Even before a message is decoded, its situation or basic characteristics will often give away its contents. For example, if a teacher sees a piece of paper being passed between two giggling teenagers of the opposite sex a few days before the school dance, she can make a pretty good guess as to what it says. Similarly, if the Germans in World War II sent a short coded telegraphic message to an Axis country after just sinking an Allied submarine, cryptanalysts could make a pretty good guess as to what its contents might be before it is even decoded. This, in turn, can provide 'Rosetta Stone' clues to future correspondence. Further, the length of the message, the material on which it is transcribed, whether it is typed or written, may all give away clues as to its origin or intent. The archetypal kidnap ransom note is often depicted with newspaper letters cut out and pasted on a sheet of paper, intended to prevent the kidnapper's handwriting from being analyzed. However, the source of the letters, the type of paper, the skill of the job, and even the brand of glue and who sells it can betray the kidnapper's location and characteristics.
- One of the weaknesses in computer encryption systems is that many rely on 'random' number generators. Pseudorandom numbers are the rule on computers and thus represent a security weakness that can sometimes be replicated by using a similar system. Many computer encryption technologies use pseudorandom numbers at some point in their processing.

Data Encryption Approaches

It's impossible in this limited space to include all the encryption techniques now used in electronic communications, but it is worthwhile to mention a few. Various methods of breaking these systems have been attempted and have sometimes succeeded. Both differential and linear cryptanalysis have been used, and other attacks such as interpolation. Two general categories include *stream encryption* (small substitutions which change as they go) and *block encryption* (larger blocks of substitutions which include some of the key encryption techniques).

Key encryption is accomplished with a string of data that determines the mapping of the unencrypted data to the encrypted data to make it possible to encrypt or decrypt that data. Some schemes have two keys, often a *public key* and a *private key* known only to the user. Keys have different lengths which are usually related to the 'strength' of the encryption. Key encryption is one of the most prevalent means of encrypting electronic data for security purposes. (Compression algorithms also encrypt data, but their primary purpose is not usually to obscure the meaning of the data but rather to create a means to store or transmit the data more efficiently.)

In general, stronger encryption means longer encryption and/or decryption times, though this is not true in every instance, as more efficient algorithms are sometimes devised. The choice of encryption techniques depends very much on the need for convenience and the level of security that is required. Personal letters are less sensitive than classified government documents, for example, and function well with lower levels of encryption and single keys (or no keys).

Encryption techniques can be symmetric, in which the encryption and decryption use the same key or in which the encryption and decryption processes require about the same amount of time. They can also be asymmetric, with different keys, or substantially different encryption/decryption times. For purposes of security, a method that is quickly encrypted and slowly decrypted is favored for some purposes. For general correspondence, however, slow decryption is an inconvenience, as are multiple keys.

Encryption systems can be deterministic or nondeterministic. One which generates the same result each time, given the same key, is deterministic and is generally not as strong as one which generates a different result, given the same key. However, true randomness in computer operations is not usually the rule and many systems are deterministic.

Encryption algorithms can be reversible or irreversible. A reversible scheme is one in which data can be recovered back to its unencrypted state. Irreversible schemes cannot be recovered, but since they tend to be used as authentication or tamper mechanisms rather than as message recovery mechanisms, they are valuable for certain tasks.

Some specific encryption schemes of interest to give an idea of the breadth and variety of the field include

AES - IA-8314: Advanced Encryption Standard. A new, stronger encryption algorithm intended by the National Institute of Standards and Technology (NIST) Computer Security Division to replace DES. The project was initiated in January 1997 as a standard laboratory network protocol.

Blowfish - Designed by Bruce Schneier and first presented in 1994. Widespread. Standard in OpenBSD. A symmetric block cipher that accepts a variable-length key from 32 bits up to a maximum of 448 bits. It can be used as a replacement for DES or IDEA. Small block size, good speed, uncomplicated interface. Introduced in Dr. Dobb's Journal in Apr. 1994, with source published in Dr. Dobbs Journal in Sept. 1995. Variations on Blowfish have been developed, including Blowfish Updated Re-entrant Project (BURP) by Geodyssey Limited. Blowfish is unpatented and license-free.

Discussions on weaknesses and attempted breaks of Blowfish include papers by Serge Vaudenay and Vincent Rijmen.

DEAL - Data Encryption Algorithm with Larger blocks. A 128-bit block cipher based on DES (DEA), but which is intended to overcome some of its weaknesses. DEAL allows for key sizes of 128, 192, and 256 bits. It is intended to deter 'matching ciphertext attacks' that can be used against DES.

DES (DEA) - IA-8307: Standard Unclassified Data Encryption Protocol, approved for use in 1977. A 64-bit block cipher that accepts a 64-bit key, of which 56 bits are active. Established as a standard in Dec. 1993. With current computing systems, it is possible to break 64-bit systems and thus DES is no longer considered sufficiently secure for high-security applications. To overcome this weakness, DES may be encrypted multiple times with multiple independent keys to improve security somewhat (e.g., Triple-DES). Is expected to be superseded by AES.

Kerberos - A client-server sign-on model in which cryptographic keys are exchanged. Similar to SESAME, but focused on UNIX systems. See SESAME.

PGP - Pretty Good Privacy. Developed by Philip Zimmermann, based on Blowfish technology, PGP provides a measure of privacy and authentication for data communications. It is widely used for email communications. Freely distributable for noncommercial use. Acquired by Network Associates in 1998.

RSA - Designed by RSA Data Security, Inc. A well-recognized, patented asymmetric public-key/private-key cryptography standard named for its developers, Rivest, Shamir, and Adelman.

SESAME - Secure European System for Applications in a Multi-vendor Environment. A scalable, client-server, sign-on, distributed access control system using digitally signed Privilege Attribute Certificates supporting cryptographic protection of remote applications and communications between users. Uses authentication tokens. It is an Open Systems protocol which provides components for computer product developers. SESAME is partly funded by the European Commission. It originated in the late 1980s as part of the Open Systems Standards work of the European Computer Manufacturers Association and was beta released in 1994. It is similar to Kerberos.

Solitaire - Designed by Bruce Schneier. An output-feedback mode stream cipher (key generator). A physical system, though it can work on computers. Not fast, but intended to be highly secure when used for small messages, even against those who understand the algorithm. Security is dependent on keeping the key secret. To maintain security, the same key should never be used for more than one message and the deck must be reshuffled after encryption. The system requires diligence, for if an error is made in the process of encryption, everything beyond that point will be incorrect.

Twofish - Designed by B. Schneier, J. Kelsey, D. Whiting, D. Wagner, C. Hall, N. Ferguson at Counterpane Labs. A 128-bit block cipher that accepts a variable-length key up to a maximum of 256 bits. It can be implemented in hardware in 14000 gates. Counterpane has extensively tried to break Twofish, reporting that the best attack "breaks 5 rounds with $2^{22.5}$ chosen plaintexts and 2^{51} effort." Selected as a finalist for the Advanced Encryption Standard (AES). The source code is license-free, uncopyrighted, and free.

Yarrow - Designed by Bruce Schneier and John Kelsey. A pseudorandom number generator intended to be secure compared to the native 'random' number generators incorporated into compilers or computer hardware. The system is unpatented and license-free.

There are many others, including FEAL, variations on LOKI, MacGuffin, MAGENTA, SAFER, SSL, TEA, etc. Information on these schemes and attacks against them can be found on the Net and in Print and Online Resources listed at the end of the chapter.

6. Applications

The actual application of cryptanalysis is much like the playing of chess. It takes time, energy, talent, and practice. It is also very specific, very technical, and thus beyond the scope of this book beyond its basic introduction.

Cryptanalysis is intensely interesting, challenging, and rewarding to those who enjoy it and inscrutable and mystical to those who don't have the mindset for this particular type of problem-solving. For this reason, code-breaking, beyond the basic alphabetic substitution code, is only practiced by a very small portion of the population. However, that small portion can have enormous power and influence over the affairs of state if they happen to find weaknesses in classified domestic or foreign codes or if they are unscrupulous enough to surveil private business or financial dealings.

Code-breaking was a pivotal surveillance technology affecting the outcome of World War II and it may be a pivotal technology in the competitive economic race that is playing itself out on the global stage.

Code-breaking is mainly used in the government secret services and, to some extent, by the computing and mathematical communities in the pursuit of knowledge and better encryption/decryption algorithms and systems.

7. Problems and Limitations

Inconvenience

One of the biggest problems with encryption systems is that they add time to any task. Some aspects of encryption can be automated. Email can be automatically encrypted when sent and decrypted when received, which certainly adds a good measure of security to messages en route, but then the computer on which the email is stored may be wide open. If the computer is password-protected, it's safer, but then you have to remember the password and a hundred other passwords for all the different services and features offered by banks, retailers, and various Web sites. Anyone who uses the Net regularly has at least a dozen passwords and some have hundreds. Putting them in a database isn't secure. Writing them down isn't secure. Memorizing them is beyond the capabilities of most people. The only reasonable solution is an algorithmic password and even that can have its disadvantages, depending on how it is designed.

The Human Element

While advanced mathematics and more powerful computers have made it possible to develop encryption systems that are difficult and, in some case, perhaps even impossible to break, it will never be 100% possible to ensure the security of information before it gets encoded or after it has been decoded. Encryption is not a panacea. At best it is like locking a door; it will deter people who are opportunists or who are lazy. It won't deter the persistent and determined. No encryption system is secure because people make mistakes, they lose keys, they forget passwords, they insert 'back doors,' they get vengeful, they get sloppy, they may have to tell the truth in court, or they may accept bribes. An increase in the level of encryption in communications systems will probably result in spies shifting their focus from the technology back to the people who create the messages in the first place.

Arrogance

One of the problems with 'secure' systems is that the designers of new encryption systems are almost always certain they are unbreakable until someone breaks them. The events of the past ten years have revealed some remarkable feats of cryptanalysis that many encryption experts didn't anticipate. This has certainly advanced the science, but it has also taught us the lesson that no matter how sure you are, you can't be absolutely sure there isn't some way to solve what at first appears to be an intractable problem.

Politics

One of the problems with encryption systems is well-known to law enforcement and secret service agents. They feel that they are cut out of the communications loop if they do not have access to encryption keys or other means to access seized or surveilled information. Unfortunately, normal law-abiding citizens rarely are comfortable with giving access to these agents, feeling that past abuses with wiretapping and other surveillance activities on the part of government officials make them vulnerable to corrupt or unethical activities. These issues are discussed to some extent in Chapters 1 and 2 and they are as yet unresolved.

Another aspect of political balance is between the needs of national security and the needs of businesses. U.S. security professionals don't want the U.S., the leader in world software, supplying other nations with strongly encrypted business and communications tools. Other countries, on the other hand, will supply them if the U.S. does not, thus leading to a loss of momentum on the part of American software vendors. This issue has recently been hotly debated with the result that export requirements were relaxed to allow U.S. companies to retain a competitive advantage. Some agencies strongly opposed this move. At one point, the National Security Agency was given access to a portion of encryption keys in order to reduce the amount of time it might take to decode a communication. This issue, too, met with a lot of comment and resistance.

8. Restrictions and Regulations

There are important export laws on encrypted products and encryption schemes intended to safeguard national security. This is a very difficult situation to legislate. It is relatively easy to say you can't ship an encrypted physical product overseas, but what if users download the product off the Internet? What if you have a note on the site saying foreigners can't download it but U.S. residents can? What if you post the source code to the encryption system for anyone to download, or perhaps you want to post just the theory. Is that considered an export of the technology? What about emailing the same code? If you collaborate with a mathematician in a foreign country on developing encryption technology, what types of export restrictions apply? If you have questions about the legality of encryption matters, it is recommended that you consult sites specifically devoted to cryptology legal issues

Some Acts of particular interest, in order of date, include

Computer Fraud and Abuse Act of 1986. Public Law 99-474. USC Title 18, Part 1 - Crimes, Chapter 47 - Fraud and False Statements. Defines fraudulent computer-related activities such as access without authorization or in excess of authorization and describes penalties. Cites the Atomic Energy Act of 1954.

Electronic Communications Privacy Act of 1986 (ECPA). USC Title 18, Part I - Crimes, Chapter 121 - Stored Wire and Electronic Communications and Transactional Records Access. Defines unlawful access to stored communications and associated penalties.

Computer Security Act of 1987. Intended to improve the security and privacy of sensitive information in Federal computer systems by establishing minimum acceptable security practices. Amends the Act of 3 March 1901 to assign standards and guidelines development to the National Bureau of Standards. Stipulates mandatory periodic training requirements for persons managing or using Federal systems with sensitive information.

Encrypted Communications Privacy Act (ECPA). Introduced in March 1996 to provide a higher legal level of security for computer network transmissions and protection of civil liberties by preventing unlimited access to computer records by the government. Affirms Americans' rights to use any encryption strength in order to maintain a competitive advantage in the world marketplace. Proposed barring of government-mandated key recovery or key escrow encryption allowing user to choose their method of encryption and protect the privacy of online communications and data files. Affects export restrictions on the export of strongly encrypted products to allow U.S. firms to compete in the global marketplace, meeting the demands of customers.

The lawmaking process is often slow, requiring three or more years for definitions and priorities to be sorted out before they pass through all the bureaucratic hurdles. In addition to the Acts and restrictions mentioned above, there have been many proposed and amended acts since 1997, and some which have passed into law. They are not discussed in detail here, but here are some for study and review. They are in various stages of completion, review, or rejection, and provide a feeling for the complexity of the process of integrating technological change and law.

Cyberspace Electronic Security Act of 1999. September proposal. Intended to protect the growing use of encryption for the protection of privacy and confidentiality by businesses and individuals, while still providing a means for law enforcement to obtain evidence to investigate and prosecute criminals using encryption to hide criminal activity. This would further provide funding to the FBI's Technical Support Center to establish a new cryptologic unit. The bill does not seek to regulate domestic use or sale of encryption.

Secure Public Networks Act (SPNA). Introduced to extend regulations.

Security and Freedom Through Encryption (SAFE) Act. Introduced to facilitate the removal of computer export restrictions, it was almost immediately amended to make substantial changes.

9. Implications of Use

The struggle for balance between the need for public freedom and privacy and the need for access to evidence of criminal activity in order to safeguard public safety is one of the more potent and intractable debates facing the U.S. government and its citizens. In another age and time, the government might have implemented encryption restrictions with impunity, but times have changed and personal input into government decisions is at an all-time high, as is the rate of technological change. It has never been easier to use secure communications and it has never been harder to gain outside access to those communications. Whether there is a solution within the current social structure is debatable. Perhaps new technology which has nothing to do with electronic communications needs to be developed to combat crime. Or perhaps the solution is closer to home. Perhaps another approach is to devote more resources to family support and efforts to remove some of the motivations for crime in the first place as *we will reach a point, perhaps soon, when the difficulty of breaking strong encryption and returning the genie to the bottle may exceed the difficulty of implementing a whole different class of preventive measures throughout the world.*

Technological Enhancements

One of the more interesting implications of cryptanalysis is that a system designed to be more secure than previous systems sometimes opens the door to security weaknesses in previous systems. For example, it has been proposed by scientists exploring quantum computing that quantum computers may be capable of better security than previous systems but that the quantum computers might make it much easier to break existing codes. In other words, in advancing the technology, it may obsolete all existing systems and all the documents created with older schemes.

Thus, there may be a time in the future when nations who have stockpiled formerly undecipherable documents might gain access to a new computing scheme that makes the old encryption methods weaker and the once-secure documents vulnerable to access by unauthorized users. This is not unlike what has happened with DNA technology. Rapists who went free ten years ago for lack of evidence can now be prosecuted, on the basis of sperm samples stored in evidence lockers, using new DNA techniques. Emailers who send messages now without fear of capture or reprisal might find themselves in a situation of being unable to deny their guilt at some time in the future.

10. Resources

Inclusion of the following companies does not constitute nor imply an endorsement of their products and services and, conversely, does not imply their endorsement of the contents of this text.

10.a. Organizations

American Cryptogram Association (ACA) - Established in 1929, to further the professional and recreational strategy/gaming aspects of cryptography for the enjoyment and elucidation of its members. The ACA publishes The Cryptogram, a bimonthly journal. http://www.und.nodak.edu/org/crypto/

Americans for Computer Privacy (ACP) - A coalition of businesses and association in a wide variety of computer-related industries. The group provides information on legislations, facts relating to encryption, FAQs, and terms. http://www.computerprivacy.org/

Consolidated Cryptologic Program (CCP) - Provides personnel to staff the Community Open Source Program within the CIA. Personnel are also drawn from the General Defense Intelligence Program, the Central Intelligence Agency Program, and others.

International Association for Cryptologic Research (IACR) - A nonprofit scientific organization to promote research in cryptology and related fields. http://www.iacr.org/

Security Technology Research Group (STRG) - STRG promotes interdisciplinary, interdepartmental research on all aspects of cryptology theory and applications. Sponsored by the Department of Computer Science and Electrical Engineering at the University of Maryland. STRG sponsors regular seminars. http://www.cs.umbc.edu/www/crypto/

10.b. Print

Babson, Walt, "All Kinds of Codes," New York: Four Winds Press, 1976.

Bauer, Friedrich, "Decrypted Secrets: Methods and Maxims of Cryptology," Berlin: Springer-Verlag, 1997, 448 pages. A technical reference on mathematical aspects of cryptology.

Biham, Eli; Shamir, Adi, “Differential Cryptanalysis of the Data Encryption Standard,” Springer-Verlag, 1993. Out of print.

Brazier, John R. T., “Possible NSA Decryption Capabilities,” discussion draft, U.K., June 1999. This study estimate the costs and capabilities which could make it possible for the NSA to break certain difficult encryption codes, based partly on work on a DES cracker by the Electronic Frontier Foundation. It describes the hardware, controllers, and other aspects of building a machine to accomplish this task.

Electronic Frontier Foundation, “Cracking DES: Secrets of Encryption Research, Wiretap Politics & Chip Design,” O’Reilly & Associates, 1998, 272 pages. How, after 20 years, the DES was attacked, with implications for political encryption efforts.

Flaconer, J., “Rules for Explaining and Deciphering All Manner of Secret Writing, Plain and Demonstrative,” London, 1692.

Foster, Caxton, “Cryptanalysis for Microcomputers,” Hayden, 1982.

Friedman, William F., “Elements of Cryptanalysis: Military Cryptanalysis,” Laguna Hills, Ca.: Aegean Park Press, 1984. This has been published in a series of at least four parts, each on different types of systems.

Gaines, Helen Fouche, “Cryptanalysis: A Study of Ciphers and their Solutions,” New York: Dover Publications, 1939 and 1956. This book can still be found, despite its original publication date. Descriptions of ciphers and methods of attack.

Hinsley, Francis; Knight, R. C.; Thomas, Edward E., “British Intelligence in the Second World War,” multiple volumes, London: Cambridge University Press, 1982.

Hinsley, F. H.; Stripp, Alan, Editors, “Codebreakers: The Inside Story of Bletchley Park,” Oxford: Oxford University Press, 1994, 321 pages.

Junken, Jeremiah S.; Kline, Gary, Editor; Simons, Peter, Editor, “PGP: A Nutshell Overview,” 1994.

Kahn, David, “The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet,” New York: Scribner, 1996, revised edition, 1181 pages. The author is a member of the U.S. Intelligence Community Editorial Board. It is a history of cryptography which doesn’t require a technical background to enjoy.

Kerckhoff, “The Handbook of Applied Cryptography,” 1883.

Kullback, Solomon, “Statistical Methods in Cryptanalysis,” Laguna Hills, Ca.: Aegean Park Press, 1976, a reprint from a 1938 publication.

Marks, Leo, “Between Silk and Cyanide: A Codemaker’s War, 1941-1945,” New York: Free Press, 1999. A personal account from the Bletchley Park days of a young man who became part of the Special Operations Executive (SOE) as head of communications. It includes new details reflecting Marks’ contribution and those of others, with a history of the SOE woven through the narrative.

Menezes, A. J.; van Oorschot, P. C.; Vanstone, S. A., “Handbook of Applied Cryptography,” Boca Raton, Fl.: CRC Press, 1997. A good technical reference to the subject.

Meyer, Carl; Matyas, S. M., “Cryptography: A New Dimension in Computer Data Security,” New York: Wiley, 1982.

Nelson, N., “Codes,” New York: Thomson Learning, 1993.

Sarnoff, J.; Ruffins, R., “The Code and Cipher Book,” New York: Charles Scribner’s Sons, 1975.

Schneier, Bruce, “Applied Cryptography,” John Wiley & Sons, 1996. The author is a practitioner and author of well-known encryption schemes.

Schomburg, Bernd prepared a study on behalf of the Bundesamt on the achievements of German cryptology up to 1945. Most of these documents have been lost.

Simmons, Gustavus, “Contemporary Cryptology,” IEEE Press, 1992, 640 pages. A survey of cryptology and its mathematical relationships.

Sinkow, Abraham, "Elementary Cryptanalysis: A Mathematical Approach," The Mathematical Association of America, 1980.

Smedley, William T., "The Mystery of Francis Bacon," London, Robert Banks, 1912, 196 pages.

Smith, Michael; "Station X: Decoding Nazi Secrets," London: TV Books Inc., 2000, 240 pages. Mostly anecdotes which have appeared in other texts. The breezy style does not include a strong analytical history.

Stallings, William, "Cryptography and Network Security: Principles and Practice," Prentice Hall, 1998. Introductory text and implementation reference for public-key cryptography, ciphers, and others.

Stinson, D. R., "Cryptography: Theory and Practice," Boca Raton, Fl.: CRC Press, 1995.

Tuchman, Barbara, "The Zimmermann Telegram," New York: MacMillan, 1978, 244 pages. A historical account of British intelligence efforts to decipher German codes during World War I that is suitable for secondary educational programs.

Wayner, Peter, "Disappearing Cryptography," Boston: Academic Press Professional, 1996, 295 pages.

Yardley, Herbert O., "The American Black Chamber," Indianapolis: Bobbs-Merrill, 1931, 375 pages.

"Zimmermann Telegram," the coded and decoded Zimmermann telegrams from World War II are archived in the General Records of the U.S. Department of State, Record Group 59 as Decimal File 862.2021/82A and 862.20212/69.

Articles

Den Boer, B, "Cryptanalysis of F.E.A.L.," *Advances in Cryptology - EUROCRYPT '88 Proceedings,* Springer-Verlag, 1988, pp. 275-280. Lists some means of attacking the FEAL algorithm.

Diffie, W.; Hellman, M., "Exhaustive cryptanalysis of the NBS data encryption standard," *Computer*, pp. 74-84, 1977.

Diffie, W.; Hellman, M. E., "Privacy and Authentication: An introduction to cryptography," *Proceedings of IEEE*, March 1979, V.67(3), pp. 397-427.

Kelsey, J.; Schneier, B.; Wagner, D., "Key-schedule cryptanalysis of IDEA, G-DES, GOST, SAFER, and triple-DES," *Advances in Cryptology: CRYPTO'96, LNCS 1109*, Springer-Verlag, 1996, pp. 237-251.

Krebs, Gerhard, "Radio decoding in the Pacific during World War II," IIHSG 1996 annual conference presentation. (See next listing.)

Leiberich, Otto, provided a personal description of the development of information technology security in the Federal Republic of Germany at the IIHSG 1996 annual conference presentation. This included information on the development of cryptography.

Pearson, P. "Cryptanalysis of the Ciarcia Circuit Cellar Encryptor," *Cryptologia*, 1988, V.12(1), pp. 1-9. For those who remember Byte Magazine when it was a "Small Systems Journal," Steve Ciarcia wrote the popular Circuit Cellar electronics column.

Retter, C., "A key search attack on MacLaren-Marsaglia systems," *Cryptologia*, 1985, V.9, pp. 114-130.

Schneier, Bruce, "A self-study course in block-cipher cryptanalysis," Counterpane Internet Security, Inc. A paper that presents the literature related to block-cipher cryptanalysis as an introduction to breaking new algorithms. For those interested in the practice and technical aspects of cryptanalysis, it lists many references for the cryptanalysis of specific encryption schemes.

Siegenthaler, T., "Decrypting a class of stream ciphers using ciphertext only," *IEEE Transactions on Computers*, 1985, C-34, pp. 81-85.

Ulbricht, Heinz, "The Enigma coding machine - Enigma 95," IIHSG 1996 annual conference presentation. The science and math of radio decoding in World War II. Enigma is used as a backdrop for how coding can be enhanced with personal computers.

van der Meulen, Michael, "Werftschlüssel: A German Navy hand cipher system," A multipart article in *Cryptologia* beginning in 1995, V.XIX(4), pp. 349-364.

Journals

"ACM Transactions on Information and System Security," published by the Association for Computing Machinery. http://www.acm.org/pubs/tissec/

"Advances in Cryptology," regularly published proceedings of the annual international Cryptology Conference (e.g., Crypto 2000).

"Antenna," Newsletter of the Mercurians, in Society for the History of Technology. Includes a range of articles about systems for encryption.

"Cipher," an electronic newsletter of the Technical Committee on Security & Privacy of the IEEE. Back issue archive is available online. http://www.issl.org/cipher.html

"Crypto-gram Newsletter," an email newsletter from Bruce Schneier, developer of Blowfish and Twofish encryption schemes.

"The Cryptogram," a bimonthly journal of the American Cryptogram Association, which takes a strategic/gaming approach to cryptography, published for 70 years.

"Cryptolog," published by Naval Cryptologic Veterans Association (NCVA).
http://www.usncva.org/clog/

"Cryptologia," a quarterly scholarly journal established in 1977 and published at but not by the U.S. Government.

"Designs, Codes and Cryptography," An international journal available electronically through Kluwer Online.

"IACR Newsletter," published electronically by the International Association for Cryptologic Research. http://www.iacr.org/

"Journal of Cryptology," published by Springer-Verlag. The official journal of the International Association for Cryptologic Research.

10.c. Conferences and Workshops

Many of these conferences are annual events that are held at approximately the same time each year, so even if the conference listings are outdated, they can still help you determine the frequency and sometimes the time of year of upcoming events. It is very common for international conferences to be held in a different city each year, so contact the organizers for current locations.

Many of these organizations describe the upcoming conferences on the Web and may also archive conference proceedings for purchase or free download.

The following conferences are organized according to the calendar month in which they are usually held.

"International Workshop on Coding and Cryptography," Paris, France, 8-12 Jan. 2001. Organized by INRIA and sponsored by the Écoles de Coëtquidan.

"Network and Distributed System Security Symposium," San Diego, California, 1-9 Feb. 2001. The 8th annual symposium.

"RSA Conference 2001," San Francisco, California, 8-12 April 2001. A large crypto and data security conference sponsored by RSA Security Inc. which developed the RSA system.

"Information Hiding Workshop," Pittsburgh, Pennsylvania., 25-27 April 2001. The 4th international conference.

"Eurocrypt 2001," Innsbrück, Austria, 6-10 May 2001. Proceedings from previous years are available online.

"History of Cryptography Symposium," Bletchley Park, U.K., 20 June 1998.

"Crypto 2000," 20th annual conference organized by the IACR and IEEE and Computer Science at the University of California, Santa Barbara, California, 20-24 Aug. 2000.

"AFITC - Air Force Information Technology Conference," Montgomery, Alabama, 29-31 August 2000.

"Asiacrypt 2000," Kyoto, Japan, 3-7 Dec. 2000.

10.d. Online Sites

The following are interesting Web sites relevant to this chapter. The author has tried to limit the listings to links that are stable and likely to remain so for a while. However, since Web sites do sometimes change, keywords in the descriptions below can help you relocate them with a search engine. Sites are moved more often than they are deleted.

Another suggestion, if the site has disappeared, is to go to the upper level of the domain name. Sometimes the site manager has simply changed the name of the file of interest. For example, if you cannot locate http://www.goodsite.com/science/uv.html *try going to* http://www.goodsite.com/science/ *or* http://www.goodsite.com/ *to see if there is a new link to the page. It could be that the filename* uv.html *was changed to* ultraviolet.html*, for example.*

Crypto Law Survey. This site, compiled by Bert-Jaap Koops, provides an extensive set of links to cryptography that are not used for digital signatures (see next listing). It includes import/export and domestic control links and links to laws of a large list of countries. The U.K. and U.S. links include further details on bills and regulations and bills presented before the U.S. Congress.
http://cwis.kub.nl/~frw/people/koops/lawsurvy.htm

Cryptography.org Archive. This site has both ftp and http access to many directories of source code and notes for major encryption technologies in PC, Amiga, and other formats. Includes Blowfish, BeOS crypto support, DES, Enigma, HASH, IDEA, etc. You must be eligible in terms of location and residence to download files. http://www.cryptography.org/

Digital Signature Law Survey. This site is like the one above, except that it covers cryptography related to digital signatures, providing information and links to legislation in a list of countries. There are also U.N. information, descriptions of research projects and policy statements. The site is compiled by Simone van der Hof. http://cwis.kub.nl/~frw/people/hof/DS-lawsu.htm

Glossary of Cryptographic Terms. A good list of cryptographic concepts and terms including some specifically related to cryptanalysis. It also includes some links of interest to other cryptology sites.
http://www.identification.de/crypto/cryterms.html

Introduction to Cryptography. An basic, illustrated introduction to the main concepts and historical events associated with cryptography.
http://www.cs.adfa.oz.au/teaching/studinfo/csc/lectures/classical.html

Spy Letters of the American Revolution. This is a wonderful educational exhibit from the Clements Library at the University of Michigan. It contains scanned letters from the Revolution that illustrate not only military strategies and secrets of the time, but also the methods that were used to convey them, including codes and hidden writing. The images have been scanned at high resolution so that the text of the messages can be read in conjunction with the transcriptions supplied on the site. The methods to hide the messages and sometimes the paper on which they were written are explained. A site worth visiting. http://www.si.umich.edu/spies/

Standard Specification for Public-Key Cryptography. This describes the IEEE P1363 project for issuing standards for public-key cryptography, the method commonly used for electronic data communications. It includes links to completed documents and those in progress.
http://grouper.ieee.org/groups/1363/index.html

Steganography. An introduction to the practice of hiding data or information inside another message, communication, or entity in order to obscure its presence. Includes links and information on the Steganography Mailing List. http://www.iks-jena.de/mitarb/lutz/security/stegano.html

Wiretapped.net. An Australian Web site devoted to archiving downloadable information and source code on cryptographic development resources, computer security, privacy, and network-related operations. The archive categories are divided into security-related files, cryptography-related files, and audio files. http://www.wiretapped.net/

10.e. Media Resources

"The National Cryptologic Museum," has been open to the public since December 1993 and is sponsored by the National Security Agency. Exhibits dedicated to people and devices that played important roles in the history of cryptology. It includes a rare book collection, cipher machines and wheels, and other information of interest. http://www.nsa.gov/museum/

Note: If you don't enjoy typing in long Web addresses (URLs), you can access the links on the support site set up by the author for your convenience. http://www.abiogenesis.com/surveil

11. Glossary

Titles, product names, organizations, and specific military designations are capitalized; common generic and colloquial terms and phrases are not.

ADARS	Airborne Digital Audio Recording System. An RC-135V/W recording system used by cryptologic intelligence crew.
AFCO	Air Force Cryptologic Office
AFELTP	Air Force Exportable Language Training Program. Training program for cryptologic linguists.
ANNULET	a cryptologic maintenance system
ASTW	312TRS exportable computer-based training cryptologic program
attack	an attempt to discern, break, or penetrate a communication or encrypted data by an entity (usually human or machine) not intended or authorized to have access to the information
CCP	Consolidated Cryptologic Program
CHAINWORK	A cryptologic maintenance course
cryptanalysis	the principles and practice of decoding an encrypted message without knowledge of the encryption technique or key
cryptography	the analysis of encoded written communications
cryptology	the study and analysis of encoded information
CTAC	Cryptologic Training Advisory Committee
CTAP	Cryptologic Training Appraisal Program
CTC	Cryptologic Training Council
CTEP	Cryptolinguistic Training and Evaluation Program
CTS	Cryptologic Training System
DES	Data Encryption Standard, an encryption standard developed by the U.S. government in the 1970s to establish an official method for government use
ECAC	Encyphered Communications Analysis Course

ECB	electronic code book
encryption	the process of coding a communication in order to obscure its contents or to facilitate its storage or administration
key	a data packet, number, word, or other reasonably compact information entity which is intended to provide a quick means to encrypt and/or decrypt a communication by mapping to data in a unique way. It is often used to protect the security of electronic communications, just as a physical key will allow a locked door to be quickly locked or unlocked.
key escrow	a key 'bank' or data storage vehicle, that is, a databank to hold keys so that authorized personnel can access the information for communications or security requirements
MECCAP	Middle Enlisted Cryptologic Career Advancement Program
NCS	National Cryptologic School
PGP	Pretty Good Privacy, an encryption and authentication system developed by Philip Zimmermann in the early 1990s, based on Blowfish technology
plaintext	an uncoded text message
RSA	an encryption algorithm published by Ron Rivest, Adi Shamir, and Len Adleman
S-box	substitution box or table
SCE	Service Cryptologic Element
Stealth	a stenographic software program that strips out RSA headers and other identifying crypto marks so that PGP-encrypted communications may masquerade as or be imbedded in other types of files (e.g., graphics)
steganography	the practice of hiding data inside other data in order to obscure its existence
symmetric key	an encryption system in which the encryption key and the decryption key are the same
TRANSEC	transmission security (see steganography)
USCS	U.S. Cryptologic Service (formerly USSS)