Chapter 1
Introduction: A Revolutionary Cipher

Abstract Cryptology is the science of secret writing. It is made up of two halves; cryptography consists of the techniques for creating systems of secret writing and cryptanalysis encompasses the techniques of breaking them. Over the past 2,500 years, cryptology has developed numerous types of systems to hide messages and subsequently a rich vocabulary in which to describe them. In this chapter we introduce the reader to the vocabulary of cryptology, explain the differences between codes and ciphers and begin the discussion of how to decipher an unknown message.

1.1 A Traitorous Doctor

In the summer of 1775, the American revolutionary forces were near a state of chaos. The main body of the American force was laying siege to Boston. The Continental Congress had just appointed George Washington of Virginia as commander of all continental forces. Money was scarce, enlistments were short, and most of the Continental Army was comprised of colonial militias with little training, no common equipment, and no idea of the enemy they faced. The officer corps was not in much better shape, with most of the colonial officers having had little or no command experience. Logistics were haphazard, artillery was practically non-existent, and the British held all the major urban areas in the thirteen colonies. The last thing that Lieutenant General Washington needed in September 1775 was a Tory spy in his midst sending secret messages to the British. But that is exactly what he got.

In mid-August 1775 a young patriot from Newport, Rhode Island named Godfrey Wenwood received a request from a former lover. It was to deliver a letter to a "Major Cane in Boston on his magisty's service". Wenwood was rather reluctant to deliver the letter, assuming, quite correctly, that Major Cane was a British

J. F. Dooley, *A Brief History of Cryptology and Cryptographic Algorithms*, SpringerBriefs in Computer Science, DOI: 10.1007/978-3-319-01628-3_1,

officer stationed in Boston with access to General Gage, the commander of British forces in America. Instead he took it to a friend of his, a fellow patriot and a schoolmaster, who opened it and discovered three sheets of unintelligible writing. The friend could not decipher the message and gave it back to Wenwood, who proceeded to sit on the letter for nearly two months. Figure 1.1 shows a page from the letter. Only when prompted by another letter from his former lover (whose name and fate have been lost to history) asking why the first one had yet to be delivered

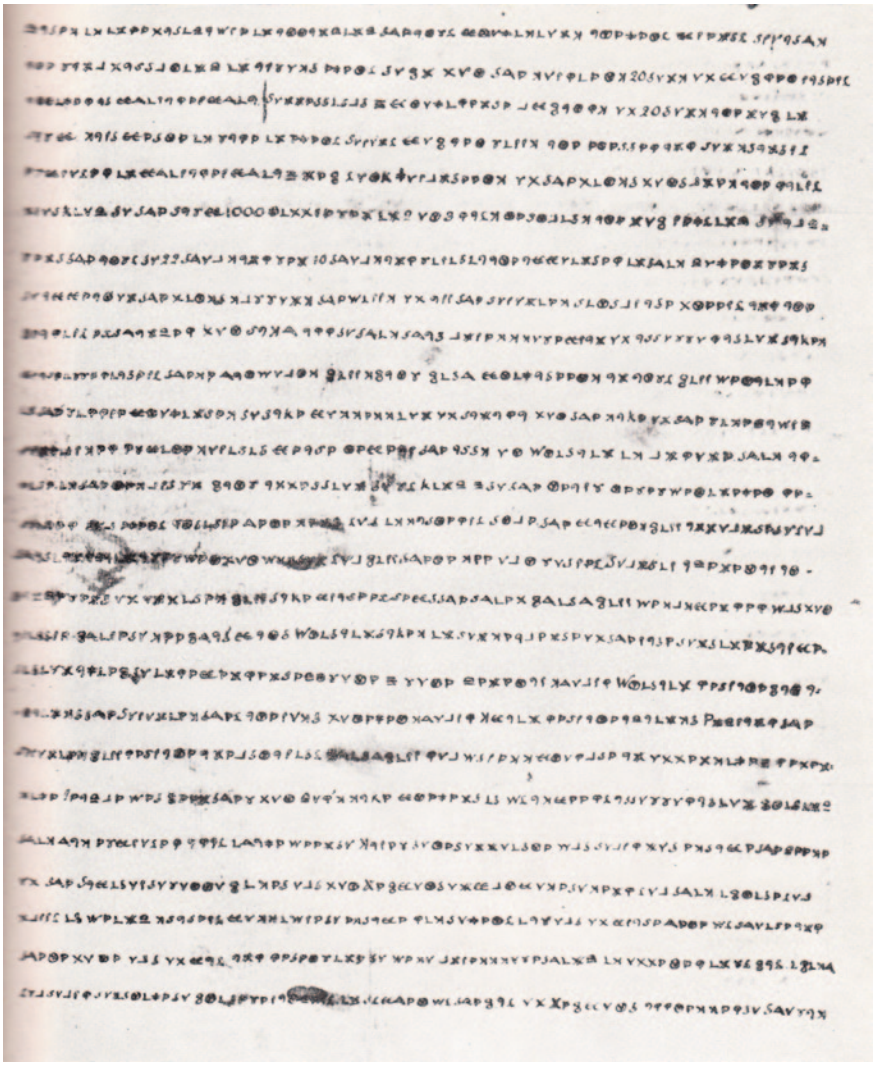

Fig. 1.1 Page from Dr. Church's cipher letter (Lib of Congress)

did Wenwood act. At the end of September 1775, he traveled the sixty-five miles from Newport to Washington's headquarters in Cambridge, Massachusetts and delivered the letter in person to General Washington.

Of course Washington, who couldn't read the letter either, ordered the woman arrested and brought to his camp for questioning. At the end of a lengthy interrogation—performed mostly by Washington himself—she gave up the name of the author of the letter—Dr. Benjamin Church, Jr., her current lover.

Dr. Church was a seemingly devoted revolutionary, a member of the Massachusetts Provincial Congress, and the head of the nascent army's medical corps as Washington's director general of hospitals. A well-to-do Boston physician, and a Harvard graduate, he was a friend of John Hancock and Samuel Adams. Dr. Church ran in all the best revolutionary circles. He was also a sham—a Loyalist to the core who had been a British spy since at least 1774, regularly reporting first to the Governor of Massachusetts and then to General Gage.

Church was brought in for questioning, and immediately acknowledged authorship of the letter. He said, despite the address on the outside, that the letter was intended for his brother in Boston and that the contents were entirely innocuous. But he refused to decipher the letter for Washington.

Washington still couldn't read the now very suspicious letter, but he thought he might know people who could. In the eighteenth century, because letters were mailed just by folding the paper on which they were written and sealing with wax, many people enciphered ordinary mail to maintain their own privacy. So there were officers in the continental army who had some familiarity with ciphers. Washington gave copies of the letter to two people, the Reverend Samuel West, a Massachusetts militia chaplain, and Elbridge Gerry, future Vice-President of the United States and originator of the gerrymander. Gerry also recruited Colonel Elisha Porter of the Massachusetts militia to help. With Gerry and Porter together, and West alone, the two teams, worked through the night, producing two identical solutions. This was the first successful cryptanalysis of the American Revolution. The letter was written in a simple monoalphabetic substitution cipher and was a blockbuster [1, pp. 541–542].

The contents of the letter were not quite damning. While Church gave much information about American army strengths and weaknesses, the letter also seemed to convey the determination of the colonists in the fight for freedom. The most damaging parts are where Church is describing how to send him correspondence—"I wish you could contrive to write me largely in cipher, by the way of Newport, addressed to Thomas Richards, Merchant." And the last line of the letter, that convinced Washington and his officers that Church was a Tory spy—"Make use of every precaution or I perish."

Washington had Church imprisoned while awaiting formal charges and a trial; a trial that never came. In 1777 the British offered to exchange Church for a captured American surgeon, but Congress declined. Finally, in 1780 Congress ordered Church exiled to the West Indies. He was put on a schooner, which sailed from Boston and was never heard of again, apparently lost at sea [2, pp. 174–176].

1.2 A Few (Vocabulary) Words About Cryptology

Secret writing is known to have existed for close to 2,500 years. As Kahn puts it, "It must be that as soon as a culture has reached a certain level, probably measured largely by its literacy, cryptography appears spontaneously—as its parents, language and writing, probably also did. The multiple human needs and desires that demand privacy among two or more people in the midst of social life must inevitably lead to cryptology wherever men thrive and wherever they write. Cultural diffusion seems a less likely explanation for its occurrence in so many areas, many of them distant and isolated." [2, p. 84]

Every discipline has its own vocabulary and cryptology is no different. This section does not attempt to be a comprehensive glossary of cryptology, but rather gives the basic definitions and jargon. Many of the concepts introduced here will be explored further in the chapters to come.

Cryptology is the study of secret writing. Governments, the military, and people in business have desired to keep their communications secret ever since the invention of writing. Spies, lovers, and diplomats all have secrets and are desperate to keep them as such. There are typically two ways of keeping secrets in communications. *Steganography* hides the very existence of the message. Secret ink, microdots, and using different fonts on printed pages are all ways of hiding the message from prying eyes. *Cryptology*, on the other hand, makes absolutely no effort to hide the presence of the secret message. Instead it transforms the message into something unintelligible so that if the enemy intercepts the message they will have no hope of reading it. A *cryptologic system* performs a *transformation* on a message—called the *plaintext*. The transformation renders the plaintext unintelligible and produces a new version of the message—the *ciphertext*. This process is *encoding* or *enciphering* the plaintext. A message in ciphertext is typically called a *cryptogram*. To reverse the process the system performs an inverse transformation to recover the plaintext. This is known as *decoding* or *decrypting* the ciphertext.

The science of cryptology can be broken down in a couple of different ways. One way to look at cryptology is that it is concerned with both the creation of cryptologic systems, called *cryptography* and with techniques to uncover the secret from the ciphertext, called *cryptanalysis*. A person who attempts to break cryptograms is a *cryptanalyst*. A complementary way of looking at cryptology is to divide things up by the types and sizes of grammatical elements used by the transformations that different cryptologic systems perform. The standard division is by the size of the element of the plaintext used in the transformation. A *code* uses variable sized elements that have meaning in the plaintext language, like syllables, words, or phrases. On the other hand, a *cipher* uses fixed sized elements like single letters or two- or three-letter groups that are divorced from meaning in the language. For example, a code will have a single *codeword* for the plaintext "stop", say 37761, while a cipher will transform each individual letter as in X = s, A = t, V = o, and W = p to produce XAVW. One could argue that a code is

Table 1.1 The two dimensions of Cryptology

	Cryptography		Cryptanalysis			
Codes	1-part	2-part	Theft, spying	Probable word	Context	
Ciphers	Substitution	Transposition	Classical	Statistical	Mathematical	Brute-force
	Product cipher					

also a substitution cipher, just one with a larger number of substitutions. However, while ciphers have a small fixed number of substitution elements—the letters of the alphabet—codes typically have thousands of words and phrases to substitute. Additionally, the methods of cryptanalysis of the two types of system are quite different.

Table 1.1 provides a visual representation of the different dimensions of cryptology.

1.3 Codes

A *code* always takes the form of a book where a numerical or alphabetic *codeword* is substituted for a complete word or phrase from the plaintext. *Codebooks* can have thousands of codewords in them. There are two types of codes, 1-part and 2-part. In a 1-part code there is a single pair of columns used for both encoding and decoding plaintext. The columns are usually sorted so that lower numbered codewords will correspond to plaintext words or phrases that are lower in the alphabetic ordering. For example,

1234	Centenary
1235	Centennial
1236	Centime
1237	Centimeter
1238	Central nervous system

Note that because both the codewords and the words they represent are in ascending order, the *cryptanalyst* will instantly know that a codeword of 0823 must begin with an alphabetic sequence before “ce”, thus eliminating many possible codeword-plaintext pairs.

A 2-part code eliminates this problem by having two separate lists, one arranged numerically by codewords and one arranged alphabetically by the words and phrases the codewords represent. Thus one list (the one that is alphabetically sorted) is used for encoding a message and the other list (the one that is numerically sorted by codeword) is used for decoding messages. For example, the list used for encoding might contain

Artillery support	18312
Attack	43110
Company	13927
Headquarters	71349
Platoon strength	63415

while the decoding list would have

13927	Company
18312	Artillery support
43110	Attack
63415	Platoon strength
71349	Headquarters

Note that not only are the lists not compiled either numerically or alphabetically, but also there are gaps in the list of codewords to further confuse the cryptanalyst.

Cryptanalyzing codes is very difficult because there is no logical connection between a codeword and the plaintext code or phrase it represents. With a 2-part code there is normally no sequence of codewords that represent a similar alphabetical sequence of plaintext words. Because a code will likely have thousands of codeword-plaintext pairs, the cryptanalyst must slowly uncover each pair and over time create a dictionary that represents the code. The correspondents may make this job easier by using standard salutations or formulaic passages like "Nothing to report" or "Weather report from ship AD2342". If the cryptanalyst has access to enough ciphertext messages then sequences like this can allow her to uncover plaintext. Still, this is a time-consuming endeavor. Of course the best way to break a code is to steal the codebook! As we will see, this has happened a number of times in history, much to the dismay of the owner.

Codes have issues for users as well. Foremost among them is distributing all the codebooks to everyone who will be using the code. Everyone who uses a code must have exactly the same codebook and must use it in exactly the same way. This limits the usefulness of codes because the codebook must be available whenever a message needs to be encoded or decoded. The codebook must also be kept physically secure, ideally locked up when not in use. If one copy of a codebook is lost or stolen, then the code can no longer be used and every copy of the codebook must be replaced. This makes it hard to give codebooks to spies who are traveling in enemy territory, and it also makes it very difficult to use codes in battlefield situations where they could be easily lost.

1.4 Ciphers

This brings us to *ciphers*. Ciphers also transform plaintext into ciphertext, but unlike codes, ciphers use small, fixed-length language elements that are divorced from the meaning of the word or phrase in the message. Ciphers come in two

general categories. *Substitution ciphers* will replace each letter in a message with a different letter or symbol using a mapping called a *cipher alphabet*. The second type will rearrange the letters of a message, but will not substitute new letters for the existing letters in the message. These are *transposition ciphers*.

1.5 Substitution Ciphers

Substitution ciphers can use just a single cipher alphabet for the entire message; these are known as *monoalphabetic substitution ciphers*. Cipher systems that use more than one cipher alphabet to do the encryption are *polyalphabetic substitution ciphers*. In a polyalphabetic substitution cipher each plaintext letter may be replaced with more than one *cipher letter*, making the job significantly harder for the cryptanalyst. The cipher alphabets may be *standard alphabets* that are shifted using a simple key. For example a shift of 7 results in,

```
Plain:  abcdefghijklmnopqrstuvwxyz
Cipher: HIJKLMNOPQRSTUVWXYZABCDEFG
```

And the word *attack* becomes HAAHJR. Or they may be *mixed alphabets* that are created by a random rearrangement of the standard alphabet as in

```
Plain:  abcdefghijklmnopqrstuvwxyz
Cipher: BDOENUZIWLYVJKHMFPTCRXAQSG
```

And the word *enemy* is transformed into NKNJS.

All substitution ciphers depend on the use of a *key* to tell the user how to rearrange the standard alphabet into a cipher alphabet. If the same key is used to both encrypt and decrypt messages then the system is called a *symmetric key system*.

Just like the security of a codebook, the security of the key is of paramount importance for cipher systems. And just like a codebook, everyone who uses a particular cipher system must also use the same key. For added security, keys are changed periodically, so while the basic substitution cipher system remains the same, the key is different. Distributing new keys to all the users of a cryptologic system leads to the *key management problem.* Management of the keys is a problem because a secure method must be used to transmit the keys to all users. Typically, a courier distributes a book listing all the keys for a specific time period, say a month, and each user has instructions on when and how to change keys. And just like codebooks, any loss or compromise of the key book will jeopardize the system. But unlike codebooks, if a key is lost the underlying cipher system is not compromised and merely changing the key will restore the integrity of the cipher system.

While most cipher systems substitute one letter at a time, it is also possible to substitute two letters at a time, called a *digraphic* system, or more than two, called a *polygraphic* system. A substitution cipher that provides multiple substitutions for some letters but not others is a *homophonic* system. It is also possible to avoid the

use of a specific cipher alphabet and use a book to identify either individual letters or words. This is known as a *book* or *dictionary cipher*. The sender specifies a particular page, column, and word in the book for each word or letter in the plaintext and the recipient looks up the corresponding numbers to decrypt the message. For example, a codeword of 0450233 could specify page 045, column 02, and word 33 in that column. Naturally, the sender and recipient must each have a copy of exactly the same edition of the book in order for this system to work. But carrying a published book or dictionary is significantly less suspicious than a codebook.

1.6 Transposition Ciphers

Transposition ciphers transform the plaintext into ciphertext by rearranging the letters of the plaintext according to a specific rule and key. The transposition is a *permutation* of all the letters of the plaintext message done according to a set of rules and guided by the key. Since the transposition is a permutation, there are n! different cipher texts for an n-letter plaintext message. The simplest transposition cipher is the *columnar transposition*. This comes in two forms, the *complete columnar transposition* and the *incomplete columnar*. In both of these systems, the plaintext is written horizontally in a rectangle that is as wide as the length of the key. As many rows as are needed to complete the message are used. In the complete columnar transposition once the plaintext is written out the columns are then filled with nulls until they are all the same length. For example,

```
s e c o n d
d i v i s o
n a d v a n
c i n g t o
n i g h t x
```

The ciphertext is then pulled off by columns according to the key and divided into groups of five for transmission. If the key for this cipher were 321654 then the ciphertext would be

```
cvdng eiaii sdncn donox nsatt oivgh
```

An *incomplete columnar transposition cipher* doesn't require complete columns and so leaves off the null characters resulting in columns of differing lengths and making the system harder to cryptanalyze. Another type of columnar transposition cipher is the *route transposition*. In a route transposition, one creates the standard rectangle of the plaintext, but then one takes off the letters using a rule that describes a route through the rectangle. For example, one could start at the upper left-hand corner and describe a spiral through the plaintext, going down one column, across a row, up a column and then back across another row. Another method is to take the message off by columns, but alternate going down and up each column.

Cryptanalysis of ciphers falls into four different, but related areas. The *classical* methods of cryptanalysis rely primarily on language analysis. The first thing the cryptanalyst must know about a cryptogram is the language in which it is written. Knowing the language is crucial because different languages have different language characteristics, notably letter and word frequencies and sentence structure. It turns out that if you look at several pieces of text that are several hundred words long and written in the same language that the frequencies of all the letters used turn out to be about the same in all of the texts. In English, the letter 'e' is used about 13 % of the time, 't' is used about 10 % of the time, etc. down to 'z', which is used less than 1 % of the time. So the cryptanalyst can count each of the letters in a cryptogram and get a hint of what the substitutions may have been.

Beginning in the early 20th century, cryptanalysts began applying *statistical* tests to messages in an effort to discern patterns in more complicated cipher systems, particularly in polyalphabetic systems. Later in the 20th century, with the introduction of machine cipher systems, cryptanalysts began applying more *mathematical analysis* to the systems, particularly bringing to bear techniques from combinatorics, algebra, and number theory. And finally, with the advent of computers and computer cipher systems in the late 20th century, cryptanalysts have had to fall back on *brute-force* guessing to extract the key from a cryptogram or, more likely, a large set of cryptograms.

References

1. Freeman, Douglas Southall. 1951. *George Washington*: *Planter and patriot*. New York: Charles Scribner's Sons.
2. Kahn, David. 1967. *The codebreakers*: *The story of secret writing*. New York: Macmillan.