COPYRIGHT NOTICE:

David G. Luenberger: Information Science

is published by Princeton University Press and copyrighted, © 2006, by Princeton University Press. All rights reserved. No part of this book may be reproduced in any form by any electronic or mechanical means (including photocopying, recording, or information storage and retrieval) without permission in writing from the publisher, except for reading and browsing via the World Wide Web. Users are not permitted to mount this file on any network servers.

Follow links for Class Use and other Permissions. For more information send email to: permissions@pupress.princeton.edu

11

CIPHERS

Secret communication is probably as old as human history. We can imagine that cave men whispered secrets, and that some symbols written on cave walls were intended only for close friends. Actual evidence of written ciphers goes back over four thousand years to a hieroglyphic substitution written by Egyptian scribes on the walls of the tomb of a nobleman. Such ciphers were intended to enhance the significance of the message or to serve as puzzles, but nevertheless they contained the elements of cryptography.

One of the most famous cipher incidences is recorded in the Old Testament in the book of Daniel. At a banquet held by King Belshazzar for a thousand of his lords, the "fingers of a human hand appeared, writing on the plaster wall of the palace." No one could interpet the riddle of the Aramaic words *Mene, Mene, Tekel, Upharsin*. Finally, Daniel was summoned and he easily read "the writing on the wall," and for this he was made one of the three leaders of the government. Although Daniel's interpretation was not strictly a decipherment, he is widely credited as perhaps being the first cryptanalyst.

Ciphers and cryptography often played a decisive role in history. Mary Queen of Scots was held in the Tower of London on suspicion of treason. Because of her stature she could not be executed unless there was definitive proof of her treachery. She communicated with her outside page by means of a complex cipher. This cipher was eventually broken, and her correspondence revealed her role in a plot to kill Queen Elizabeth and overtake the throne. This clinched the judgment, leading to Mary's beheading.

Ciphers are crucial in military campaigns. The first known use of military encryption is associated with the Spartans, who used a transposition device known as a **scytale** that scrambled the letters of a message. Julius Caesar used a simple substitution code for both military and domestic communication.

At the end of the eighteenth century, Thomas Jefferson created a **wheel cipher** that was far advanced for its time. Unfortunately, his idea was filed away and only rediscovered among his papers in 1922. Because of its strength, the system was

subsequently used by various agencies of the government and the military. Thomas Jefferson is accordingly called the father of American cryptography.

One of the most infamous ciphers is the dreaded Enigma cipher used by the Germans in World War II. It was implemented by a complex **Enigma machine** that scrambled and substituted text using a series of complex wheels and circuits. It was considered unbreakable, and for this reason the Germans relied on it. Its analysis and eventual breaking by a British agency was one of the most important military achievements of the war and is credited with shortening the war by at least two years.

Today encryption is a vital part of everyday life. Sensitive phone messages are scrambled, Internet communication is encrypted, and smart credit card and digital cash transactions are secured by encryption techniques far superior to those of early ciphers, even superior to the mysterious Enigma. The fascinating development of encryption is explored in the next few chapters.

11.1 Definitions

A generic cipher system is shown schematically in figure 11.1. The **plaintext** is the original message. It is **encrypted** to produce the corresponding **ciphertext**. This ciphertext may appear to be a jumble of letters, or it may be a series of entirely different symbols, such as ♠∇♯ ⋈ § ♠◇ ∘ ♡ □∞ ◇♮$. Once the ciphertext is received by the intended party, it is **decrypted** to reproduce the original plaintext. Of course the sender and receiver must both agree on the encryption process.

As a rule, a particular cipher method is but one of a family of similar ciphers, each separate member of the family being distinguished by a **key**. The key governs the encryption process and also the decryption. In practice, the strength of a cipher system is related to the number of possible keys.

11.2 Example Ciphers

It was as long ago as 500 BC that the Spartan government encoded messages with a scytale (pronounced SITalee), which was a cylinder of fixed radius. The sender spiraled a strip of parchment around the cylinder and wrote across it, each letter being placed on adjacent turns of the parchment. When the strip was unwound, the order of the letters was mixed up. The message was decrypted by generals in the field who possessed a duplicate scytale with the same radius. See figure 11.2.

For example, if the circumference of the scytale were equivalent to four letters of text, a strip with the ciphertext ROEOERNMICTINESNFMCG could be decrypted

FIGURE 11.1 Cipher process. Plaintext is encrypted into ciphertext, and this is sent to the receiver, who decrypts it to recover the original plaintext.

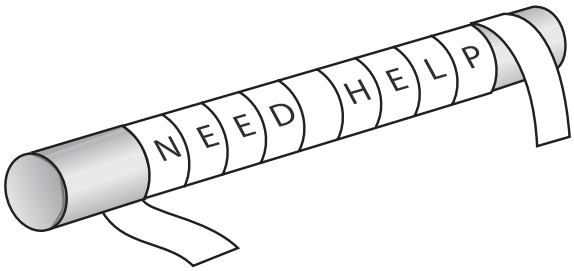


FIGURE 11.2 The scytale. A message is written across the spiraled parchment and then unwound. The scrambled message is decrypted by use of a duplicate scytale. This figure shows the start of a message that would progress across other rows as well.

by spiraling the message on a cylinder of circumference equal to four letters (to give REINFORCEMENTS . . .).

The scytale is an example of a **transposition cipher** in which the ciphertext consists of the same letters as the plaintext but physically transposed in some systematic fashion. The key of the scytale is its radius.

Transposition Ciphers

Practical transposition ciphers are similar to those produced by a scytale, but generated on the interleaving principle discussed in chapter 6 in the context of error-correcting codes. The plaintext message is written letter by letter in a matrix row by row, but converted to ciphertext by reading the letters out column by column. For good measure, the columns can be permuted.

Suppose a five by five array is used. The message THE INVASION WILL BEGIN TODAY is read in by rows as shown below.

2	**4**	**3**	**1**	**5**
T	H	E	I	N
V	A	S	I	O
N	W	I	L	L
B	E	G	I	N
T	O	D	A	Y

The message is read out by columns to obtain the ciphertext. A keyword can be used to mix the order of the columns. In this case we have selected the keyword MONEY to define the order. Remembering a word is easier than remembering a specific order. The keyword is translated into digits by following the alphabetical order of the letters in the keyword. Since E is the lowest letter in the MONEY, it becomes 1, M is the second lowest, so it is 2. Following this procedure with each letter, the keyword translates to 24315. This is the order to be used when writing out the columns. The resulting ciphertext is IILIA TVNBT ESIGT HAWEO NOLNY, which can be spaced differently so as not to reveal the column size, to say, IIL IAT VNB TES IGT HAW EON OLN YDL with two letters added to fill out the last apparent three-letter word.

A general **transposition cipher of order *p*** reorders a block of p plaintext symbols according to a given permutation. Interleaving is a simple way to construct such a permutation, but it does not include all possible permutations. For example, the symbols could be read into a triangular array row by row and read out column by column. There are in fact $p!$ possible permutations of order p and hence $p!$ transposition ciphers of order p.[1] Said another way, there are $p!$ possible keys (a key being a permutation) associated with transposition codes of order p.

Substitution Ciphers

The most common simple ciphers are **substitution ciphers** where each letter of plaintext is transformed into another letter or symbol, but the order of the letters is not changed.

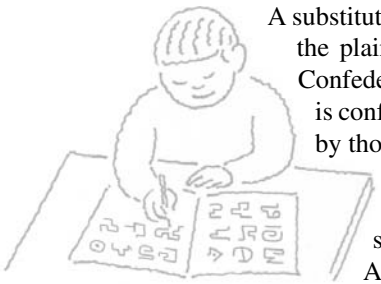
The **Caesar cipher** is one of the simplest and most well known of the substitution ciphers. In this cipher each letter of the alphabet is shifted by, say, three letters. Thus: a becomes D, b becomes E, and so forth. At the end of the alphabet, the shifting is wound around back to the beginning. The complete set of substitutions is therefore

plaintext	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
ciphertext	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Of course shift lengths other than three can be used. The length of the shift is the key, and knowing its value enables one to decrypt the plaintext message.

A modern-day version of this shift cipher is embodied by the Unix operator ROT 13, which shifts all letters by 13. Decryption is achieved by applying the same operator again, since two shifts by 13 produces a shift of 26.

Alternative Alphabets



A substitution cipher may employ a different alphabet for the ciphertext than that of the plaintext. One example is the **pigpen cipher**, said to have been used by Confederate soldiers in the Civil War and still a favorite of school-age children. It is confusing to someone who does not know the secret, but easily reconstructed by those who do. The substitution is made by drawing two simple figures: one being the same set of four lines used in a tic-tac-toe game, and the other being a large X. Letters of the alphabet are entered in pairs into the spaces created by these figures, as shown in figure 11.3.

A letter is encoded as the outline of the area in which it is contained. For example, the letter A is encrypted as ⌊. If the letter is the second of the pair

[1] There are p ways to select the new location of the first letter, $p - 1$ ways to select the new location of the second, and so forth.

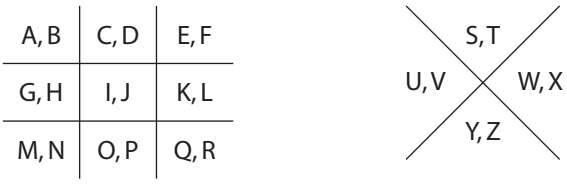


FIGURE 11.3 Pigpen cipher. The placement of letters defines symbols used in the ciphertext.

in the space, a "pig" is included in the form of a dot. Thus, B is encrypted as ⊥•. A complete message might be

which is easily decrypted.

11.3 Frequency Analysis

Simple substitution codes, such as the Caesar cipher, are vulnerable to attack based on frequency analysis using the known letter frequencies of English. For example, it is known that the most common letters, in order from most common, are E T A O I N S. When attacking the ciphertext of a substitution code, one first determines the most common letters. For the ciphertext

ZNKINKIQOYOTZNKSGOR

K, N, O, and Z each occur three times, while the others occur only once or twice. It is natural to assume that one of these most frequent symbols represents the letter e. Trying K = e and then guessing all letters are shifted by six in a Caesar code, causes everything to fall in place, producing the message, "The check is in the mail."

More complex substitution codes are designed to increase the number of possible keys and render frequency analysis less potent.

11.4 Cryptograms

Advanced substitution codes substitute letters or symbols of the ciphertext alphabet according to an arbitrary pattern. That is, a general substitution cipher may represent the letter a by K, b by X, c by F, and so forth, with the correspondence being unique in each direction. Symbols other than letters can be used for the cipher alphabet. In any case, there are 26 different symbols, each corresponding to a plaintext letter. If ordinary letters are used for the cipher alphabet, the code system can be

described by a permutation of the 26 letters of the alphabet, as shown in the example below.

Plaintext	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Ciphertext	F	J	W	S	N	O	B	K	M	U	E	I	H	Z	X	C	Q	R	D	T	A	V	L	Y	P	G

If spacing between words and punctuation is preserved, the ciphertext of such a system is termed a **cryptogram**. A cryptogram is vastly more complex than a Caesar cipher or even a pigpen cipher, for while there are 26 possible Caesar cipher keys, corresponding to the 26 possible shifts of the alphabet, there are $26! \approx 4 \times 10^{26}$ possible cryptogram keys corresponding to the 26! different permutations of the alphabet. This is an enormous number of possibilities.

One approach to breaking a substitution code is by trial and error, trying each possible key until a result makes sense. We can imagine a fast computer applied to the problem of solving a cryptogram by this trial-and-error procedure. The computer would cycle through the possible permutations of 26 letters, checking if the result were reasonable. Assuming that the computer could check 100 million permutations per second (which is optimistic since there would be considerable effort to determine if the result were reasonable), it would take about $2 \times 10^{26}/10^8 = 2 \times 10^{18}$ seconds to check one-half of the permutations (which on average is all that would need to be checked). There are $60 \times 60 \times 24 \times 365 = 31,536,000$ seconds in a year. So it would take $2 \times 10^{18}/(.31536 \times 10^8) \approx 6 \times 10^9 = 6$ billion years to complete the computation.

Despite the complexity of a general substitution code, it preserves much of the character of plaintext language. Letter frequencies are preserved, being merely translated to the substitute letters or symbols. If e is coded as K, then K will likely appear more frequently than any other letter in the cipher, and this will suggest that K is the substitute for e. Word structure is also preserved. For example, double letters in plaintext appear as double letters in the ciphertext.

Edgar Allan Poe heightened public curiosity about cryptograms with publication of his engaging and now classic short story *The Gold Bug*, in which Captain Kidd's treasure is discovered with the help of a special species of golden bug and the breaking of a cryptogram left by Kidd. Poe was fascinated by cryptograms and in his regular column in the Philadelphia newspaper *Alexander's Weekly Messenger* he challenged readers to submit cryptograms and boasted that he would solve them all. He was inundated with submissions, but he readily solved all that were legitimate.

Poe's method was the same that amateur fans of cryptograms use today, a combination of frequency analysis and word structure analysis, although there is evidence that Poe emphasized the latter over the former.

Example 11.1 (An important message). To attack the ciphertext

GFX XCXRU WK QJKWGWJCXD JC GFX FWVV GJ GFX XBKG

we first perform a frequency analysis, realizing that it may not be accurate for such a short message. The following counts are obtained:

X	7	G	6
J	4	F	4
W	4	C	3
K	2	V	2

All the rest have counts of 1.

Frequency analysis suggests X = e and G = t. Then the fact that the word GFX appears three times suggests that it is *the*, the most common three-letter word. This gives F = h. We note that the two-letter word GJ starts with t under our assumption, and it is logical therefore to assume the word is *to*, which gives J = o. This means that the two-letter word JC starts with an o and hence it likely that C = n.

The two-letter word WK contains no t, o, h, or n. Hence, a likely choice is is, which gives W = i and K = s. At this point we have the message

t h e	e n e	i s	o s i t i o n e
G F X	X C X R U	W K	Q J K W G W J C X D

o	n	t h e	h i	t o	t h e	e s t
J	C	G F X	F W V V	G J	G F X	X B K G

From here it is easy to fill in the missing letters to obtain the message: the enemy is positioned on the hill to the east.

This approach has been duplicated in a computer program for solving cryptograms, which includes a dictionary of the 1,000 most common words in English, partitioned into words of different lengths and different structure. For example THAT, HIGH, and AREA are in the same group because the first and fourth letters agree in each of these words. The method systematically tries letter assignments in an attempt to maximize the number of words that match those in the dictionary.

Cryptograms of about 30 letters in length appear in puzzle books as challenges, and most can be easily solved by hand in half an hour or so.

11.5 The Vigenère Cipher

The substitution ciphers discussed so far are termed **monoalphabetic** since there is a single alphabet (and single substitution order) used to construct the cipher. By the sixteenth century, the weakness of this type of cipher was recognized, and more complex ciphers that varied the substitution process from letter to letter were proposed. Such ciphers are termed **polyalphabetic** since more than one alphabet substitution is used. The most practical and popular of these was invented by Blaise de Vigenère in about 1562.

The **Vigenère cipher** uses a keyword to vary the substitution formula with each new letter. Each substitution is determined by a simple shift of the alphabet as in a Caesar cipher, but the length of the shift is determined by the key. To assist in the process of shifting, one may use the Vigenère table of table 11.1.

As an example, suppose the keyword is chosen to be CODE. To encrypt a message, it is written letter by letter with the keyword lined up above it and repeated over and over so that it spans the entire message. The keyword letter that is written above the plaintext letter is the shift as determined by table 11.1. An example is shown below.

Keyword	C O D E C O D E C O D E C O D E C O D E C O D E C O D E C O D E C O D E
Message	T H E P R E S I D E N T I S I L L W I T H A H I G H F E V E R T O D A Y
Ciphertext	V V H T T S V M F S Q X K G L P N K L X J O K M I V I I X S U X Q R D C

TABLE 11.1
Vigenère Table. Each row is a shift of the one above it.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
B	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a
C	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b
D	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c
E	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d
F	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e
G	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f
H	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g
I	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h
J	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i
K	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j
L	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k
M	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l
N	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m
O	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n
P	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
Q	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p
R	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q
S	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r
T	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s
U	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t
V	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u
W	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v
X	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w
Y	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x
Z	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y

The Vigenère cipher destroys ordinary frequency and word structure. A given plaintext letter is likely to be encrypted differently in its several occurrences in the message. Likewise a double letter will not appear as a double letter. The Vigenère cipher is therefore much more difficult to attack than a standard monoalphabetic substitution code. The strength of the cipher, however, depends on the length of the key. If the key is short, the cipher may be broken by using an enhancement of frequency analysis.

Cryptanalysis of the Vigenère Cipher

Vigenère ciphers with relatively short keywords can be attacked by using the numerical values of relative letter frequencies. A table of such frequencies is shown in table 11.2.

Suppose a received message is

CMFUSBIEXKLMDETGNU.

Assume first that the length of the keyword is known. Suppose it is three. Then the collection of every third letter can be analyzed as if these were produced by a simple shift cipher. That is, one looks only at the letters 1, 4, 7, 10, ... For the sample message above these letters are CUIKDG.

A variation of frequency analysis can be applied to this collection of letters using a simple optimization procedure. A certain keyword letter is proposed and the letters in the collection are transformed by this shift. Then each letter in this transformed collection is assigned a value equal to its standard occurrence frequency as given in table 11.2.

The first three key letter possibilities are shown in table 11.3. If the key letter were A, the letters in the collection would be identical to the corresponding cipher letters. The first section of the table lists these letters together with their standard frequencies (as a percent). These values are summed to obtain a total score of 19.582. Next, assuming the key letter were B, the message letters would have been shifted forward by one letter to construct the cipher letters, so now they are shifted backward by one

TABLE 11.2
Letter Frequency Occurrences in English. The frequencies are given as percentages.

A	8.167	J	0.153	S	6.327
B	1.492	K	0.772	T	9.056
C	2.782	L	4.025	U	2.758
D	4.253	M	2.406	V	.978
E	12.702	N	6.749	W	2.36
F	2.228	O	7.507	X	0.15
G	2.051	P	1.929	Y	1.974
H	6.094	Q	0.095	Z	0.074
I	6.966	R	5.987		

TABLE 11.3
Analysis of a Vigenère Cipher. Actual frequency values are assigned to each possible shift and the maximum is indicative of the possible key letter.

	Key Letter					
	A		B		C	
	C	2.782	B	1.492	A	8.167
	U	2.758	T	9.056	S	6.327
	I	6.966	H	6.094	G	2.051
	K	.772	J	.153	I	6.966
	D	4.253	C	2.782	B	1.492
	G	2.051	F	2.228	E	12.702
Score		19.582		21.805		37.705

letter to obtain the hypothetical message letters. These are shown in the second section together with their corresponding scores. The total score under the assumption that B is the key letter is 21.0805. Similarly, the score under the assumption that C is the key letter is found to be 37.705. This procedure can be carried out for each possible key letter, producing a score for each one. In this example, it turns out that the key of C gives the highest score, so it is a prime candidate for the actual key letter.

The same process can be carried out for the collection consisting of the letters in positions 2, 5, 8, 11, 14, 17 and for the collection of letters in positions 3, 6, 9, 12, 15, 18. The maximum scores for these sets are obtained by the key letters A and B respectively, implying that the entire keyword is CAB. Indeed, using this as the keyword converts the message to AMESSAGEWILLBESENT, or A MESSAGE WILL BE SENT.

This simple technique may not always be successful on messages as short as this example, but it is highly successful on messages that have a length at least 10 times the key length.

If the length of the keyword is not known, this procedure can be repeated for various lengths until a high total score is achieved, indicating the true key or at least the true length.

The entire procedure can be easily carried out in a spreadsheet program.

The Autokey Cipher

An ingenious variation of the Vigenère cipher that does not require a long key but has some of its advantages, is the **autokey cipher** also devised by Vigenère. In this cipher, the message itself is used as the key. The process is started with a **seed key**, which could be as short as a single letter, but it is better to use a longer one. When as many letters as in the seed key have been encrypted, new key letters are taken from the message itself starting at the beginning. For example, if the key is the single letter C and the message is "We have captured a spy," The actual key would be CWEHAVECAPTUREDASP, producing the ciphertext YALHVZGCPINLVHDSHN.

11.6 The Playfair Cipher

Another way to confound frequency analysis is to encode letters in pairs rather than singly. For example, the pair *th* might be encrypted as 356, and the pair *te* by 12. In its most general form, specification of a symbol for each pair requires a table of size 26^2 by 26^2, which is quite unwieldy. However, such a table can be constructed so that the resulting cipher is completely immune from first-order frequency analysis, and second-order analysis would be effective only on lengthy messages.

The **Playfair cipher** is a simple procedure for encrypting pairs. It was popularized by Lyon Playfair, first Baron Playfair of St. Andrews, but it was actually invented by his good friend Sir Charles Wheatstone, a scientist of unusual breath and creativity. Wheatstone's contributions to telegraphy and his influence on the invention of the telephone are mentioned briefly in chapters 19 and 20.

8	J	E	Q	D	N	5	O
P	U	3	A	R	F	L	W
4	V	C	2	T	M	B	I
K	7	Z	S	G	X	H	Y

FIGURE 11.4 A Playfair matrix. The matrix defines a pair-wise substitution cipher that is difficult to break.

The cipher is defined by an array such as shown in figure 11.4. Any size array is suitable as long as it has at least two columns and two rows and contains at least 26 elements (or 25 if *i* and *j* are considered identical). The figure shows a four by eight array constructed by scattering the alphabet among the cells and filling the remainder with integers.

A message to be encrypted is first partitioned into pairs of adjacent letters. If this would lead to a double letter, an X is inserted between the two. For example, the message LET US MEET AT NOON is rewritten as

LE TU SM EX ET AT NO ON.

An X is inserted between the two Es, but not between the two Os, which are in different pairs. If there is a final single letter, an X is appended.

A pair of letters is encoded according to the following rules:

1. If the letters are in the same row, encode the letters by using those to the immediate right in the same row. If at the right end, use the first letter in the row (that is, consider that the rows wrap from the right end to the left). For example, the pair TI is encrypted as M4.
2. If the letters are in the same column, encode the letters by using those immediately below in the same row. If at the bottom, use the top letter of the column. For example, the pair RG is encrypted as TD.
3. If the letters appear in different rows and columns, encode each as the letter in the same row but in the column of the other letter. For example, the pair LE is encrypted as 35.

The message LET US MEET AT NOON becomes, when grouped in fours, 35VR X2NZ DCR2 5885.

The Playfair cipher is easy to implement but extremely difficult to break. For this reason Wheatstone and Playfair described the system to the under secretary of the Foreign Office, suggesting that it was ideal for field work. The under secretary complained that the system was too complex. Wheatstone said that he could readily teach it to three out of four elementary school boys in 15 minutes, but the under secretary responded, "That is very possible, but you could never teach it to attachés."

11.7 Homophonic Codes

Standard frequency analysis is powerless against a **homophonic code** that assigns more than one symbol to each letter in such a way that the frequency of the code alphabet is uniform. If 100 symbols are used (such as the two-digit numbers from 00 to 99), the number of symbols assigned to a letter can be chosen to closely match the relative frequency of that letter. For example, since the letter A occurs approximately 8 percent of the time, 8 symbols are assigned to it. Likewise, E which occurs approximately 12 percent of the time is assigned 12 symbols. Table 11.4 shows such a code. During encryption the particular symbol to be used to represent a letter is chosen

TABLE 11.4
A Homophonic Code. If the symbols assigned to a letter are selected randomly when encrypting that letter, each symbol will occur with approximately equal probability, rendering ordinary frequency analysis virtually useless.

A	04, 25, 30, 43, 45, 47, 68, 86
B	51
C	67, 72, 93
D	22, 41, 55, 84
E	02, 12, 36, 48, 50, 53, 59, 66, 70, 77, 82, 89
F	06, 71
G	23, 29
H	11, 17, 52, 74, 78, 96
I	16, 20, 27, 46, 49, 62, 99
J	87
K	69
L	09, 32, 54, 73
M	44, 85
N	00, 14, 21, 33, 56, 90
O	01, 34, 37, 57, 61, 80, 91
P	07, 94
Q	63
R	05, 19, 28, 38, 58, 60
S	08, 24, 39, 65, 95, 81
T	10, 18, 26, 35, 42, 75, 76, 79, 83, 88
U	15, 40, 64
V	13
W	31, 97
X	98
Y	03
Z	92

randomly from those assigned to the letter, randomness being applied on each occurrence. The great mathematician Gauss is reported to have discovered the homophonic code and believed it to be unbreakable. (It is not.)

11.8 Jefferson's Wheel Cipher

Thomas Jefferson probably invented his **wheel cipher** during the 1790s. He described his invention in his personal papers, but apparently never put it to practical use. According to his description, the wheel is made from a wooden cylinder about 2 inches in diameter and 6 inches long, with a 1/4 inch hole bored through the center. This cylinder is sliced up into 36 disks, each about 1/6 of an inch thick. Around the circumference of each disk are inked the 26 letters of the alphabet in random order, each disk with a different order. The disks are then threaded through their center holes onto a shaft. The series of disks then define 26 rows, each of 36 random letters. A message of up to 36 characters is encoded by rotating the disks one at a

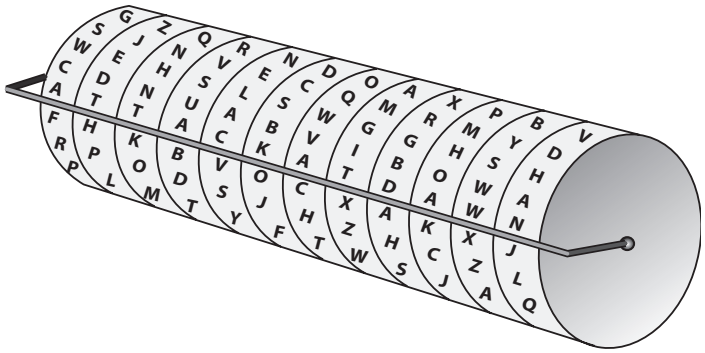


FIGURE 11.5 Simplified Jefferson's wheel cipher. The disks can be threaded on in any order. They are then rotated so as to spell out a message, and the ciphertext is taken as the text of any other row.

time so that one of the rows (and it does not matter which row) matches the text of the message. Once in position, Jefferson suggests locking the arrangement with a screw. The ciphertext is then taken to be the letters read across any other row. See figure 11.5 for a simplified version with only 12 disks.

This ciphertext is decrypted by the intended recipient, who has an identical wheel, by rotating the disks so as to match the ciphertext across one of the rows. The recipient then locks the disks in that position and turns the whole apparatus until a message that makes sense is observed across a row.

The disks of the wheel are numbered, and they can be threaded onto the shaft in numerous orders. The threading order is the key of the cipher system. Jefferson realized that there are 36! orders and computed (correctly) that this is about 3.72×10^{41} possible keys.[2]

Jefferson's wheel cipher is extraordinarily difficult to break. However, he apparently felt that it was too complex, and mysteriously, he selected instead a Vigenère cipher as the official cipher for the Lewis and Clark expedition. Had his wheel cipher been adopted by the U.S. government, it would certainly have been the most advanced encryption device available well into the 20th century.

11.9 The Enigma Machine

In 1918 the German inventor Arthur Scherbius filed a patent for a mechanical encryption machine that became known as the **Enigma machine**. It was not the first encryption machine, for seeds of the Enigma concept were contained in the early scytale, in Thomas Jefferson's cipher wheel, and in several other cipher machines. However, the Enigma remains the most advanced machine of that type actually manufactured, and was to play a vital (even pivotal) role in World War II.

The machine looks like an overgrown typewriter, for in fact the message is typed in on typewriter keys. (See figure 11.6.) The machine contains several other features, but the most important is the series of three disks (termed **rotors**) that implement complex

[2]The exact answer is 371,993,326,789,901,217,476,999,448,150,835,200,000,000.

FIGURE 11.6 The Enigma machine. The machine has typewriter keys for entry, three rotors to define a letter substitution, a plugboard to implement a further substitution, and finally, lightbulbs to indicate the result.

substitutions. The rotors, similar to Jefferson's disks, have circumferences divided into 26 segments. The Enigma rotors are made of nonconducting material such as hard rubber or ceramic. On the face of each rotor are 26 electrical contacts evenly spaced near the outer rim to match the 26 divisions. These contacts are electrically connected in pairs, one on the front face of the rotor, the other on the back face, but these pairs are in a random pattern. The first contact on the front might be connected to the sixteenth on the back. A rotor therefore defines a substitution cipher. If the machine were made with only a single rotor of this type, it would be arranged so that striking a keyboard key would apply voltage to the corresponding contact on the front face of the disk, and that current would pass to the corresponding contact on the back face, which would activate a lightbulb connected to that contact. Twenty-six lightbulbs are arranged in the same configuration as keys, so that each bulb represents letters by their position.

The three rotors are connected in series. Each rotor has a different arrangement of inner connections and thus represents a different set of permutations. When a key is struck, an electrical circuit passes through the first rotor, into and through the second, then into and through the third.

Now the true enigmatic nature comes to play. After a key is struck and a bulb lit, the first rotor rotates one space, thereby changing the permutation of the first rotor for the next letter. The second rotor rotates a single space after the first rotor makes a complete cycle of 26 spaces, like an automobile odometer; the third rotor steps one space only after the second makes a complete cycle.

The rotors are numbered 1, 2, and 3 and are themselves interchangeable. Thus the rotors might be placed in the machine in order 3, 1, 2. In later models a total of five rotors were available, from which three were chosen for a given setting.

There is a fourth disk termed a **reflector** that does not rotate and has 26 contacts only on one face. These contacts are connected in pairs so that current entering one contact emerges from another, sending the current back through the other three rotors along a path different from that taken in the forward direction. When it completes its circuit, the current lights one of 26 lamps, which indicates the encrypted version of the typed letter. The reflector adds no new complexity but greatly simplifies decryption because now an electrical path from a typewriter key (say Z) to a bulb (say K) is the same as the path from key K to bulb Z. Hence a message can be decoded by keying in the ciphertext, with the bulbs now giving the plaintext. The basic Enigma structure is illustrated in figure 11.7.

There is yet another complication. A **plugboard** allows for the interchange of two letters before they enter the rotors. This is accomplished by plugging the ends of a cable into holes corresponding to two letters. In later models, a total of up to 13 pairs of letters could be swapped in this way. In practice only 10 were used.

Finally, another complication is that associated with each rotor is a **ring** with a notch that determines when in a rotor's cycle it advances the next rotor. This would be like an odometer that advances the next digit on, say mile 4, instead of mile 0. The rings can be set at any of the 26 possibilities.

In practice, the German military provided a list of basic settings for each day, consisting of three ordered rotor numbers, ring settings, initial rotor positions, and plugboard arrangement. Then each message during the day varied only the initial rotor positions, which were sent as the first part of the message.

The number of possible Enigma keys is enormous. The number can be computed in steps, the largest contribution being from the plugboard.[3]

$$\begin{aligned}
\text{Rotor choice} &= 5!/(2!\,3!) = 10 \text{ (selecting 3 from 5)} \\
\text{Rotor order} &= 3! = 6 \\
\text{Rotor positions:} &= 26^3 = 17{,}576 \\
\text{Ring positions:} &= 26^2 = 676 \text{ (since only the first two matter)} \\
\text{Plugboard combinations} &= 26!/[6!\,10!\,2^{10}] = 150,738,274,937,250
\end{aligned}$$

[3]The total number of combinations when n cables are used is $26!/[(26-2n)!(2n!)]$ (the number of ways to select $2n$ holes from 26), times $(2n)!$ the number of ways of inserting $2n$ cable ends), divided by 2^n (because connecting A to B is the same as connecting B to A), divided by $n!$ (the number of ways the cables can be ordered).

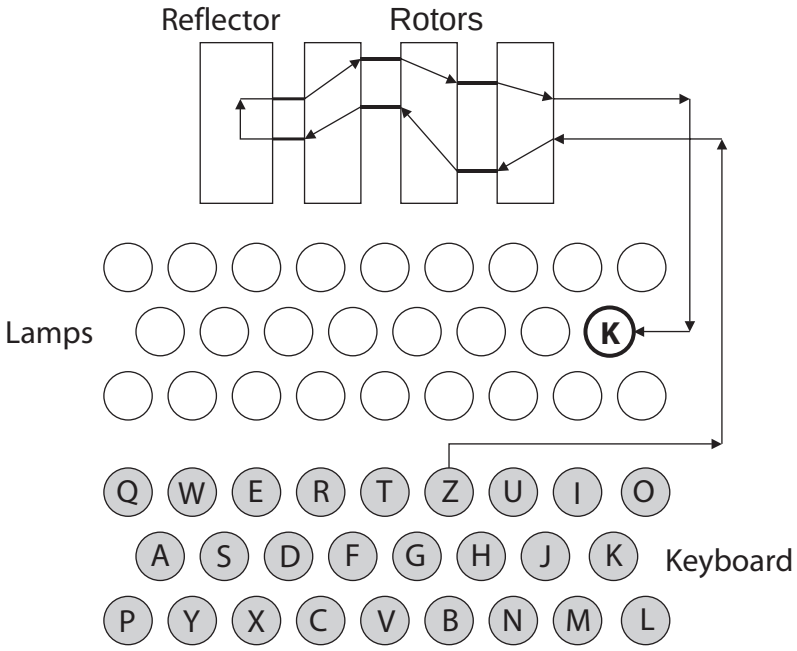


FIGURE 11.7 Basic Enigma structure. Pressing key Z completes an electrical circuit that passes through the three rotors, the reflector, and back through the rotors to light lamp K that indicates the encrypted version of Z. The path is reversible so that pressing K will light lamp Z. The actual Enigma includes additional complications of a plugboard and rings.

The total number of keys is therefore the astronomical number 107, 458, 687, 327, 250, 619, 360, 00 $\approx 1.0 \times 10^{23}$.

Actually the number of keys, though huge, is less than the 26! $\approx 4 \cdot 10^{26}$ keys of a single substitution code of 26 letters and much less than that of Jefferson's wheel cipher. Most of the Enigma keys are due to the plugboard substitutions. If these substitutions constituted the entire encryption, the Enigma would be susceptible to elementary frequency analysis and hence could be easily broken. The strength of the Enigma is that it scrambles the message in so complex a manner that basic letter frequency and word structure are effectively obliterated.

The Enigma served as the primary encryption system for the entire German military beginning in about 1928. During the war years, the Germans purchased over 30,000 Enigmas. The first successful attack on the Enigma was accomplished by the Polish cryptologist Marian Rejewski in about 1932. He had obtained design specifications for the early version of the machine used at that time. This used only three rotors and six plugboard possibilities. His method exploited a protocol of German messages that required each message to begin by repeating a three-letter rotor key to be used for that message. This minor redundancy was enough to decode the message by the use of a complex machine termed a **bombe** that Rejewski had built for the purpose.

When the Enigma was enhanced in 1938 by the addition of two more Enigma rotors, from which to select three, and the number of plugboard cables was increased

from six to 10, this additional complexity was enough to render Rejewski's method impotent.

During the Second World War the later models of the Enigma provided essentially complete security for the German military. It was used to issue orders to submarines, coordinate land and air battles, respond rapidly to special situations, and in general direct the war in a way that was potentially devastating. Hundreds or thousands of messages were sent each day, all with perfect secrecy.

During the war, the British established a cryptography center at Bletchley Park to attempt to decipher German messages. The brilliant Alan Turing was recruited for the effort. Turing was a young mathematician who had already answered one of the greatest mathematical–philosophical questions of the time by showing, with the invention of an imaginary computer termed a **Turing machine**, that there are mathematical propositions that mathematics itself cannot resolve. At Bletchley Park, in a feat of tremendous genius and hard work, Turing devised a method for decoding the German transmissions. His method relied on an insightful analysis of the structure of the coded messages produced by the Enigma, the use of guesses or knowledge of the plaintext fragments (such as the German word WETTER, which appeared regularly in daily weather reports), and the development of a huge machine, again termed a bombe, that tried the large number of combinations that remained after incorporation of the first two method of attack. Turing's method was operational during 1940 – 42, and the British were able to read a high percentage of German communications. Of course, it was critical that the Germans not know that their "unbreakable system" had been broken. A challenge faced by the British then was to decide whether and how to intervene in military operations without raising the suspicion that the Enigma had been breached.

It is generally agreed that the war was shortened by about two years because of the breaking of the Enigma system using Alan Turing's method.

When the war ended, Turing worked at the National Physical Laboratory in London, and in 1948 he became the deputy director of the Computing Laboratory at Manchester, where the first electronically programmable computer was built. But later, Turing was not celebrated as a hero. Instead, this man who solved one of the most outstanding mathematical–philosophical problems of the age, played a decisive role in the war effort, and helped launch modern computing was arrested and had his secret clearance suspended because he admitted to having a homosexual relationship (which was illegal at the time). In 1954 at the age of 42 Alan Turing died from potassium cyanide poisoning widely believed to have been purposely self-administered.

11.10 The One-Time Pad

The strength of the Vigenère cipher increases with the length of the key: frequency characteristics and word structure are essentially eliminated. In fact, if the key is as long as the message, and itself completely random, the associated ciphertext will be random as well, with absolutely no structure that can form the basis for cryptanalysis. This special version of the Vigenère cipher is termed a **one-time pad**, the name coming from the practice of writing the random key letters on a pad of paper and using this pad to encrypt messages. Each page of a pad contains a different random

sequence, and each key letter is used once only. When an entire pad has been used, it is discarded. A one-time pad provides perfect secrecy according to the precise definition given in the next chapter. It is mathematically impossible to decrypt it without the key.

Because of the ultimate security provided by the one-time pad, it has often been used in sensitive situations. In the military, the pads of random key letters took the form of a codebook, with a separate page to be used for each date. Capture of an enemy codebook was a great military prize.

The security of the one-time pad is sometimes approximated by using an actual published book such as a novel, with the letters of the novel used sequentially to define the Vigenère shift of successive message letters. The key letters are not strictly random in this case, and this may compromise the code's security.

Although the one-time pad is ideal in theory, there are number of practical difficulties that discourage it from being used widely. How can the random letters be generated? How can the long sequences be distributed to the various communicating parties who are a great distance apart? What if the pad falls into enemy hands? If the same pad is used by all communicating parties on any one day, doesn't that introduce redundancy that the enemy might use to advantage? These questions highlight the fundamental issue associated with classical encryption methods. Security rests with the key, and the question of distributing keys is itself an issue of secret communication. It is this question that motivated the development of the entirely new approach to encryption described in chapter 13.

11.11 EXERCISES

1. (An easy cipher) Decode the following:

   ZNOY OY GT KGYE IOVNKX ZU YURBK

2. (Autokey cipher) The following message was coded with the autokey system using a seed only one letter long. What is the message?

   PCN LMI ZNVQ WAL WWIH?

3. (Transposition cipher) Consider a transposition cipher that uses a five by five matrix and permutes the columns before reading them out.
   (a) How many keys are possible in such a cipher?
   (b) Decrypt the following.

   HTASL LEEOT ASWME TSSAP EMGCE.

4. (Beaufort cipher) Let $k = (k_1, k_2, \ldots, k_n)$ be a keyword of length n, and let $p = (p_1, p_2, \ldots, p_n)$ be a plaintext message of length n. The Beaufort encryption of the message is the ciphertext $c = (c_1, c_2, \ldots, c_n) = (k_1 - p_1, k_2 - p_2, \ldots, k_n - p_n)$, where $k_i - p_i$ denotes a backward shift of k_i by the shift corresponding to the letter p_i. For example, if $k = (H, I)$ and $p = (B, Y)$, then $c = (G, K)$.
   (a) Encode the message HELLO with the keyword JUMPS.
   (b) Show that encryption and decryption of a Beaufort cipher are identical processes. That is, to decipher it is only necessary to encrypt the ciphertext with the same keyword.

5. (Vigenère and transposition) Suppose a Vigenère cipher is constructed with a key that is three letters long. The result of this first encryption is further encrypted with a Vigenère cipher, with another three-letter key.
   (a) How many possible keys are embodied in the final ciphertext?
   (b) Suppose that after the first Vigenère encipherment, the resulting text is transformed by a transposition code that reads the text into a three by three matrix row by row and reads it out column by column after the columns are permuted. Effectively how many possible keys are embodied in the resulting double-encrypted ciphertext?
   (c) Suppose that after the Vigenère encryption and the transposition encryption, the text is subjected to another Vigenère cipher with a key of length 3. How many possible keys are embodied in this final result?
   (d) Suppose that after the first Vigenère cipher, the transposition cipher, and the second Vigenère cipher, the transposition is reversed (perhaps because the transposition key is discovered). The result is then equivalent to a compound Vigenère cipher. What is the length of the keyword in this compound Vigenère cipher?
   (e) How many possible keys are embodied in this compound Vigenère cipher?

6. (Affine ciphers) Let a be an integer between 1 and 26, and let x be the integer corresponding to one of the 26 letters of the alphabet. The corresponding linear cipher transforms the message x into the ciphertext y by

   $$y = ax \mod 26.$$

   For example, if $a = 3$ and the message is "d," the ciphertext is $y = 3 \times 4 = 12$. If the message is "k," the ciphertext is $y = 3 \times 11 \bmod 26 = 33 \bmod 26 = 7$.

To be acceptable, the value of a must be **invertible** mod 26, such that the correspondence from x to y can be uniquely inverted. A case that does not have this property is $a = 4$, for then both $x = 3$ (for "c") and $x = 16$ (for "p") lead to $y = 12$. An a is invertible if it has no common factor, other than 1, with 26. Hence, 4 is not invertible since both 4 and 26 share the factor 2. (See section 13.5.)

(a) List the acceptable values of a.

(b) Decipher the following linear ciphertext:

13 9 9 10 7 10 20 11 20 9.

(c) An **affine cipher** is of the form $y = ax + b$ mod 26, where both a and b are integers between 1 and 26, with a being one of the values in part (a). How many keys are there in affine ciphers?

(d) An affine cipher can be combined with a Vigenère cipher by fixing a but using k different values of b and cycling through these b values, letter by letter. How many keys are there in this compound cipher?

7. (Hill cipher) Hill devised a cipher that extends both transposition and linear ciphers. It has the form

$$y = xA \bmod 26$$

where A is an $n \times n$ matrix of integers. The n-dimensional message (row) vector x is transformed into the ciphertext vector y. For example, with

$$A = \begin{bmatrix} 11 & 8 \\ 3 & 7 \end{bmatrix}$$

the message $x = (8, 9)$ can be transformed by the Hill transformation as

$$y = (8,9)\begin{bmatrix} 11 & 8 \\ 3 & 7 \end{bmatrix} = (88 + 27, 64 + 63) \bmod 26 = (11, 23).$$

To decipher the result, the inverse of the matrix A (mod 26) is applied. This inverse will exist if the determinant of A has no common factor, except 1 and 26, with 26. Often it is arranged that the determinant of A mod 26 is in fact 1. For example, the determinant of the matrix A given above is $11 \times 7 - 8 \times 3 = 53 = 2 \times 26 + 1 \rightarrow 1$ in mod 26 terms.

(a) Find the inverse of the A matrix given above. (Recall that the inverse of a two by two matrix is

$$\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}^{-1} = \frac{1}{D}\begin{bmatrix} a_{22} & -a_{12} \\ -a_{21} & a_{11} \end{bmatrix}$$

where D is the determinant of A.)

(b) Decipher the ciphertext (1, 2).

11.12 Bibliography

There are a number of excellent presentations of classical cryptography, including the elementary and entertaining [1], [2], and [3] and the more advanced [7]; as well as the texts referenced for chapter 12. Comprehensive histories of cryptography and its role in significant life circumstances are the large and wonderful books [4] and [5]. A computer program to solve cryptograms was outlined in [6]. See [7] for a good discussion of the affine, Hill, and Beaufort ciphers.

References

[1] Gardner, Martin. *Codes, Ciphers, and Secret Writing*. Mineola, N.Y.: Dover, 1984.

[2] Pickover, Clifford A. *Cryptorunes: Codes and Secretc writing.* Rohnert Park, Calif.: Pomegranate Communications, 2000.

[3] Beutelspacher, Albrecht. *Cryptology*. Trans. J Chris Fisher. Washington, D.C.: Mathematical Association of America, 1996.

[4] Kahn, David. *The Code Breakers*. New York: Scribner, 1996.

[5] Singh, Simon. *The Code Book*. New York: Doubleday, 1999.

[6] Hart, George W. "To Decode Short Cryptograms." *Communications of the ACM* 27, no. 9 (1994): 102–8.

[7] Mollin, Richard A. *An Introduction to Cryptography*. Boca Raton: Chapman & Hall/CRC, 2001.