DISCRETE MATHEMATICS AND ITS APPLICATIONS
Series Editor KENNETH H. ROSEN

CODES

THE GUIDE TO SECRECY FROM ANCIENT TO MODERN TIMES

RICHARD A. MOLLIN

Chapman & Hall/CRC
Taylor & Francis Group

1.5 Rise of the West

Oh, East is East, and West is West, and never the twain shall meet,
Till Earth and Sky stand presently at God's great Judgement Seat...
Rudyard (Joseph) Kipling, (1865–1936), English writer and poet
— from *The Ballad of East and West* (1892)

The word *Renaissance* literally means *rebirth.* It was coined by fifteenth-century scholars to separate the fall of ancient Greece and Rome from its rebirth and rediscovery in the middle of their own century. The fall of Constantinople in 1453 may be considered one of the dividing lines since scholars fled to Italy, bringing with them knowledge, irreplaceable books and manuscripts, as well as the classical Greek tradition of scholarship. The earliest sign of the Renaissance was the intellectual movement called *humanism*, perhaps given its biggest surge by the aforementioned influx of scholars. Humanism, born in Italy, had as its subject matter: human nature, unity of truth in philosophy, and the dignity of man. Perhaps most importantly, humanism yearned for the rebirth of lost human spirit and wisdom. While medieval thinkers preferred the idea of "one man, one job", the *Renaissance man* was a versatile thinker, thirsting for an education in all areas of knowledge, and becoming an expert in many. It is one of those men with whom we begin our discussion.

Leon Battista Alberti

If there is to be a holder of the title *Father of Western Cryptography*, it must go to Leon Battista Alberti (1404–1472). He was not only an architect, sculptor, writer, and all round-scholar, but also one of the prime movers in the development of the theory of art in the Renaissance, not to mention his contributions to cryptology, a true Renaissance man.

Alberti was born on February 14, 1404, in Genoa, Italy, the illegitimate son of a wealthy banker, Lorenzo di Benedetto Alberti. Yet, in this time of Florentine Italy, illegitimacy was less of a burden, and more of a reason to succeed. Alberti was raised as Battista in Venice where the family moved shortly after he was born. (He adopted the name Leon later in life.) At the age of 10, he had already learned Latin and his father was teaching him mathematics. His formal education was at the University of Bologna, where he ultimately earned a degree in law. However, he quickly turned his interests to artistic, and ultimately scientific thought. Alberti not only taught himself music, became an expert at playing the organ, and wrote sonnets, but also wrote on art, criminology, sculpture, architecture, and mathematics. In 1432, he went to Rome where he became a secretary in the Papal Chancery, and he remained in the arms of church for the rest of his life. In 1434, he went to Florence as part of the papal court of Eugenius IV. It was in the papal secretariat that he became a cryptographer. In fact, he was a friend of Leonardo Dato, a pontifical secretary who might have instructed Alberti in the state of the art in cryptology.

In order to understand Alberti's contributions, we need to examine some concepts first. A *homophone* is a ciphertext symbol that always represents the same plaintext symbol. For instance, with the Caesar cipher in Table 1.2 (page 11), the letter *D* is always the ciphertext for the plaintext letter *a*, so *D* is a homophone in the *monoalphabetic* cipher known as the Caesar cipher. Here "monoalphabetic" means that there is only one *cipher alphabet*, which means the set of ciphertext equivalents used to transform the plaintext. The row of ciphertext equivalents below the plaintext in Table 1.2, for instance, is the cipher alphabet for the Caesar cipher. A *polyphone* is a ciphertext symbol that always represents the same *set* of plaintext symbols, typically a set consisting of at most 3 plaintext symbols. With homophones or polyphones, there is no option for change since the relationship between plaintext and ciphertext is fixed. However, a cipher is called *polyalphabetic* if it has more than one cipher alphabet. In this type of cipher, the relationship between the ciphertext substitution for plaintext symbols is variable. Thus, since each cipher alphabet (usually) employs the same symbols, a given symbol may represent several plaintexts.

Alberti conceived of a disk with plaintext letters and numbers on the outer ring and ciphertext symbols on an inner movable circle. Alberti divided his ring and corresponding circle into 24 equal segments, called *cells*, each containing a symbol.

A representation of Alberti's disk is pictured in Figure 1.22. We have altered his original presentation since he had ciphertext in lower case and plaintext in upper case, the reverse of what we have as a convention.

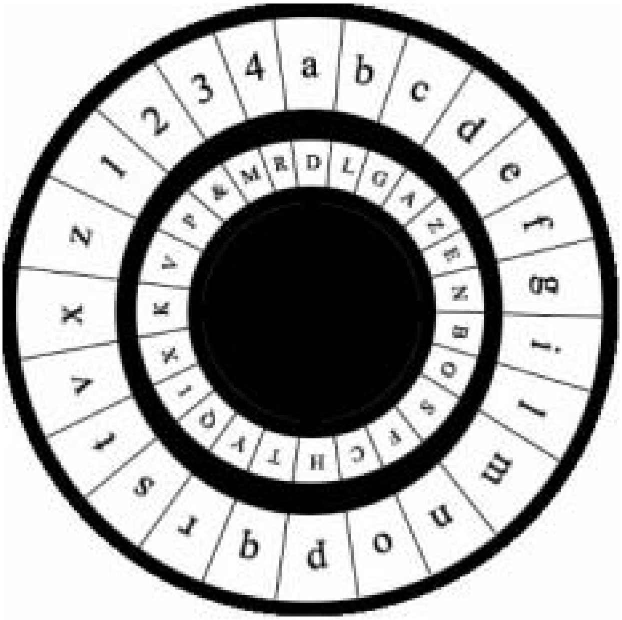

a b c d e f g i l m n o p q r s t v x z 1 2 3 4
D L G A Z E N B O S F C H T Y Q I X K V P & M R

Figure 1.22: Alberti disk.

In Figure 1.22 the plaintext letter *z* is enciphered as *V*, so in this setting (one of the 26 possible cipher alphabets), the plaintext *zebra*, for instance, would be enciphered as *VZLYD*. However, there is nothing new at this juncture that is any different from, say, the Caesar cipher with the cipher alphabet having the letter *c* below the *Z*. Alberti had an idea, however (which is why he wanted the inner circle to be able to rotate). This idea would revolutionize the forward movement of cryptological development. After a random number of plaintext words had been enciphered, usually three or four, Alberti would move the inner disk to a new setting. Hence, he would now be using a *new* cipher alphabet. Suppose that he moved the inner circle so that *z* sits over *K*. Then *zebra* would be enciphered as *KADTR*, a new ciphertext for the same plaintext as above since we have a *new* cipher alphabet. This is polyalphabeticity in action, literally! In fact, with his cipher disk, Alberti invented the first polyalphabetic cipher in history. Yet, he did not stop there.

Alberti had 20 letters, as depicted in Figure 1.22[1.5] and including the numbers 1 through 4 in the outer ring of his original disk. In a book, he used these numbers in two-, three-, and four-digit sets from 11 to 4444 yielding 336 ($= 4^2 + 4^3 + 4^4$) codegroups. Beside each digit he would write a phrase such as "Launch the attack" for the number 21, say. Then, with the setting in Figure 1.22, the code group 21 is enciphered as *&P*, *enciphered code.* Alberti was the first to discover it, and it is a testimony to his being centuries ahead of his time that enciphered code, when it was rediscovered at the end of the nineteenth century, was simpler than that of Alberti!

Johannes Trithemius

Polyalphabeticity had another ally, and we have already met him in Section 1.3. In early 1508, Trithemius turned himself to the task of writing a book dedicated solely to a serious cryptographic analysis, called *Polygraphia*, with the official title, *Polygraphiae libri sex, Ioaonnis Trihemii abbatis Peopolitani, quondam Spanheimensis, ad Maximilianum Caesarem*, or *Six Books of Polygraphy, by Johannes Trithemius, Abbot at Wurzburg, formerly at Spanheim, for the Emperor Maximilian.* However, Trithemius died on December 15, 1516, in Wurzburg before the book was published. In July of 1518 it finally went to press, and was reprinted (and plagiarized) many times after that. *Polygraphia* can be said to be the first printed book on cryptography. In his book, he invented a cipher where each letter was represented as a word taken from a sequence of columns. The resulting sequence of words turned out to be a legitimate prayer. Perhaps more importantly, from the viewpoint of the advancement of cryptography, he also described a *polyalphabetic cipher.* Another way to think of such a cipher is that there is more than one enciphering key, namely, that a given symbol may be encrypted in different ways depending upon where it sits in the plaintext. An accepted modern form for displaying this type of cipher is a rectangular substitution table, about which we will learn a great deal more as we

[1.5] This excludes the letters *h*, *k*, and *y*, deemed to be unnecessary, and since *j*, *u*, and *w* were not part of his alphabet, this left 20 letters. The inner circle consists of the 24 letters of the Latin alphabet, put in the cells at random, including *&*.

Figure 1.23: Leon Battista Alberti.
(Courtesy of the Archaeological Museum of Bologna, Italy.)

continue our journey. Given below is the Trithemius tableau where all possible shifts (modulo 24) appear as rows below the plaintext, each row representing a distinct cipher alphabet (key), a total of 24 cipher alphabets (keys) in all, polyalphabeticity! Trithemius used 24 letters, excluding the letters j and v.

The Trithimius Tableau

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

To illustrate its use, we suppose that the plaintext is *maximilian*, then the ciphertext is achieved by looking at the first row for the first letter under the letter m, which is M, then for the second letter a of the plaintext look at the letter below it in the second row, which is B, for the third letter of the plaintext x, look at the letter below it in the third row, Z, and so on to get the ciphertext *MBZMQORQIX*. If we have plaintext that is longer than 24 letters, then we can start over again in the first row and repeat the process, (mod 24 arithmetic in action). Notice that unlike a simple *mono*alphabetic substitution cipher, such as the Caesar cipher, having only one cipher alphabet — the row below the plaintext — a given plaintext in a polyalphabetic letter does not always go to the same ciphertext letter. For instance, in our plaintext, the letter i goes to M in the first instance, O in the second instance, and Q in the third instance, since i sits in the fourth, sixth, and eighth places of the plaintext corresponding to the fourth, sixth, and eighth row entries of ciphertext (in other words in the corresponding cipher alphabet determined by that row) sitting below i, namely, *M,O*, and *Q*, respectively. Later, we will see how another later cryptographer, Blaise de Vigenère (see page 55), was inspired by this tableau to create one that took the idea further.

Figure 1.24: Polygraphia.

Image courtesy of the National Cryptologic Museum of The National Security Agency, Rare Books Collections. See *http://www.nsa.gov/museum/books.html.*

The attentive reader will have noticed that the Trithemius tableau (necessarily a square since there are exactly as many rows (cipher alphabets) as there are letters in the alphabet) has an advantage over Alberti's method since the cipher alphabet is changed with *each letter* enciphered, rather than after an arbitrary number of enciphered words as with Alberti's method. Moreover, the ordered table makes a quick look-up possible at a glance for each of the cipher alphabets.

Trithemius also gave examples where he switched alphabets after exhausting 24 letters of plaintext rather than starting over with the first row of the above tableau again. This is a variation of the above simple scheme. Moreover, the aforementioned method is the first cipher to use a *progressive key* where all possible cipher alphabets are exhausted before any are used again. Modern ciphers have used more variations on this theme since we now have computers to employ such key progressions. Moreover, the substitution table that he used is now a standard feature of modern-day cryptography.

Giovanni Battista Belaso

Our next ally and proponent of the advancement of polyalphabeticity is another from Italy, Giovanni Battista Belaso. Neither Alberti nor Trithemius conceived of using a key or key words in their polyalphabetic ciphers. The first in recorded history to do so was Belaso in 1553. His idea was to use a *keyphrase*, which he called a *countersign*, repeated as often as needed, to select the cipher alphabets. (We may think of this as the modern invention of the notion of a *password*.) Here is how his countersign works. First, we are going to be using Trithemius's table (page 51).

BELASO'S KEYPHRASE POLYALPHABETIC CIPHER

To employ Belaso's idea, we do three things to *encipher*.

(a) Put the plaintext letters in a row.

(b) Above each plaintext letter place the keyphrase letters, repeated as often as necessary, to cover all the plaintext.

(c) Replace each letter of the plaintext with the letter at the intersection of the row labelled by the keyphrase letter and column labelled by the plaintext letter in Trithemius's table.

We illustrate these rules with the following.

Example 1.1 *We will suppose the keyphrase, used by Belaso, is* OPTARE MELIORA*, and the plaintext is* countersign is key*. Then one places the keyphrase over the plaintext, repeated until the plaintext runs out as illustrated below.*

o	p	t	a	r	e	m	e	l	i	o	r	a	o	p	t
c	o	u	n	t	e	r	s	i	g	n	i	s	k	e	y
Q	D	O	N	L	I	D	X	T	P	B	A	S	Y	T	R

For example, the letter o *labels the row that intersects the column headed by the letter* c *at the ciphertext letter* Q*, and so on.*

To *decipher* using the Trithemius square, we do three things.

(a) Put the ciphertext letters in a row.

(b) Put the keyword letters above the ciphertext letters, repeating them as required, to cover all ciphertext.

(c) Locate the column labelled by each keyword letter, and find the row in which the ciphertext letter sits below it. Then the label of that row is the plaintext.

Applying these rules to Example 1.1, we get the following.

Example 1.2

o	p	t	a	r	e	m	e	l	i	o	r	a	o	p	t
Q	D	O	N	L	I	D	X	T	P	B	A	S	Y	T	R
c	o	u	n	t	e	r	s	i	g	n	i	s	k	e	y

For instance, since the letter o *sits over the ciphertext letter* Q*, the row of which is labelled by* c*, then this is the first letter of plaintext, and so on.*

Employing standard alphabets in his use of a keyphrase, Belaso created a polyalphabetic cipher with much greater flexibility than that of Alberti or Trithemius. With this use of a keyphrase, Belaso ensured that, instead of repeating the enciphering of each letter with 24 standard cipher alphabets, as Trithemius proposed, the key could be changed at will. For example, if the key were compromised in some fashion, it could be discarded and a new one issued to, say, diplomats of the day for their correspondence. Even with keys of length 13, as in the above keyphrase from Belaso, there are 24^{13} possible encipherments of a given plaintext letter, more than a hundred quadrillion choices. Quite an advancement! Nevertheless, however prodigious this contribution seems to be, it would be for another individual to put together all the pieces in order to create the first forerunner of a modern polyalphabetic cipher.

Porta and Cardano

Giovanni Battista Porta (1535–1615) was born in Naples, Italy, in 1535. At the age of 22, he published his first book, *Magia Naturalis*, or *Natural Magic*, a text on "experimental magic". However, in 1563, he published *De Furtivis Literarum Notis*, which contained the cryptographic advances in which we are interested. In this book is the first appearance of a *digraphic cipher*, meaning a cipher in which two signs represent a single symbol. (Later, we will see how this notion was reinvented in the twentieth century by Lester Hill using only elementary matrices (page 111), and how the first *literal* digraphic cipher was invented much later. Here Porta is using signs rather than letters.) Moreover, he introduced some of the modern fundamentals of cryptography, namely a separation of *transposition ciphers* and *substitution ciphers*, as well as *symbol substitution* (substituting an unusual symbol for a letter). Porta also looked at methods, albeit elementary by modern standards, of cryptanalyzing polyalphabetic ciphers. In fact, in a second edition of his book, published in 1602, Porta added a chapter with these cryptanalytic observations. Although Porta also ultimately did glue together the ideas of Alberti, Belaso, and Trithemius, by adding mixed alphabets and shifts, to produce what we consider to be a basic polyalphabetic substitution cipher, there was work to be done to make polyalphabetic ciphers more secure, the essence of which was in how the key was used.

Figure 1.25: Natural Magic.

Image courtesy of Scott Davis: *http://homepages.tscnet.com /omard1/jportat5.html*.

The first to see how this could be accomplished was Girolamo Cardano (1501–1576). Cardano was born on September 24, 1501, in Pavia, Duchy of

Milan, Italy. In his younger years, he assisted his father who was a lawyer and a mathematics lecturer primarily at the Platti foundation in Milan. Cardano himself came to be known as one of the greatest mathematicians of his time. He wrote more than 130 books in his lifetime. The two that are best known for his mathematical contributions are *Liber de ludo aleae*, or *Book on Games of Chance*, considered to be the first book on probability theory, and *Ars Magna* (1545), considered to be one of the great books in the history of algebra. The ones of interest to us from a cryptographic perspective were his books, *De Subtilitate* (1550), and a follow-up called, *De Rerum Varietate* (1556). In these two books, he introduced the idea of an *autokey,* meaning that the plaintext, itself, is used as its own key. However, Cardano implemented the idea in a flawed manner, which allowed for multiple possible decryptions as well as the fact that, in his implementation, the receiver of the message was in no better position than a cryptanalyst at trying to determine the first plaintext word, from which there would be total decryption. Thus, the idea of an autokey has not been attributed to Cardano. He is remembered for an invention of a steganographic device, which we call the *Cardano grille.* Cardano's idea involved the use of a metal (or other rigid substance) sheet consisting of holes about the height of a written letter and of varying lengths. The sender of a message places the grill on a piece of paper and writes the message through the holes. Then the grille is removed and the message is filled in with some innocuous verbiage. Use of the Cardano grille continued well into the seventeenth century, and has even popped up in various places in modern times. Thus, it is the case that due to his flawed idea for an autokey, he is remembered largely for his steganographic device. He died on September 21, 1576, in Rome with his fame not attached to the greater cryptographic record that he sought. That fame would go to another.

Blaise de Vigenère

Blaise de Vigenère (1523–1596) had his first contact with cryptography at age 26 when he went to Rome on a two-year diplomatic mission. He familiarized himself with the works of his predecessors, Alberti, Belaso, Cardano, and Trithemius. His own work, published in 1585, containing his contributions to cryptography, is called *Traicté des Chiffres.* Vigenère discussed steganographic techniques, and a variety of cryptographic ideas. Among them was the idea for an autokey polyalphabetic substitution cipher.

He employed the idea that Cardano had invented of using the plaintext as its own key. However, he added something new, a *priming key*, which is a single letter (known only to the sender and the legitimate receiver), that is used to decipher the first plaintext letter, which would, in turn, be used to decipher the second plaintext letter, and so on. To understand the details of how this works, we use a Vigenère square, given on page 56, with the full 26-letter alphabet, as opposed to Trithemius' use of 24. It rightfully deserves to be called a *Trithemius* square, as the reader will note, but history has deemed it to have Vigenère's name attached to it.

THE VIGENÈRE TABLEAU

	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 AUTOKEY POLYALPHABETIC CIPHER

(a) Put the plaintext letters in a row.

(b) Place the priming key letter below the first plaintext letter. Then put the first plaintext letter below the second, the second below the third, and so on to the penultimate below the last.

(c) Replace each letter of the plaintext with the letter at the intersection of the row labelled by the plaintext letter and column labelled by the key letter.

Example 1.3 *Let us first choose a priming key, say* x, *and assume that the plaintext is* form secret diction*.*

f	o	r	m	s	e	c	r	e	t	d	i	c	t	i	o	n
x	f	o	r	m	s	e	c	r	e	t	d	i	c	t	i	o
C	T	F	D	E	W	G	T	V	X	W	L	K	V	B	W	B

For instance, the row labelled f *intersects with the column labelled* x *at the ciphertext letter* C*, and so on. To decipher, the receiver knows the priming key* x*, so this letter is placed above the ciphertext letter* C *and looks in the row labelled* x *to find the letter* C*, then the label of the column in which* C *sits is the plaintext, namely* f*, and so on, as follows.*

x	f	o	r	m	s	e	c	r	e	t	d	i	c	t	i	o
C	T	F	D	E	W	G	T	V	X	W	L	K	V	B	W	B
f	o	r	m	s	e	c	r	e	t	d	i	c	t	i	o	n

Unfortunately, as is the case too often, Vigenère's idea was forgotten and reinvented at the end of the nineteenth century. However, what was rediscovered was a weakened version of his idea. Essentially it amounted to exactly what Belaso has discovered, which we discussed on page 53, applied to the Vigenère square rather than that of Trithemius, so we need not replay it here.

One obvious improvement to the above is to have not a single priming key letter, but rather a priming *keyphrase*. Moreover, in the interests of security, the keyphrase should be as long as possible and feasible. Later we will see a very secure cipher where the key is as long as the plaintext itself, called the *one-time pad* (page 83). For instance, consider the following depiction of the more general idea of extending Vigenère's idea to a keyphrase.

Example 1.4 *Suppose that we want to encipher, again:* form secret diction*, but this time using the priming* keyphrase*:* "xanadu"*. Then we proceed as in steps* (a)–(c) *on page 56, this time with our more general keyphrase sitting below plaintext letters before introducing the plaintext into the key, as follows.*

f	o	r	m	s	e	c	r	e	t	d	i	c	t	i	o	n

x	a	n	a	d	u	f	o	r	m	s	e	c	r	e	t	d
C	O	E	M	V	Y	H	F	V	F	V	M	E	K	M	H	Q

Then to decipher, we proceed as in Example 1.3, but with the full keyphrase this time, rather than the key letter, as follows.

x	a	n	a	d	u	f	o	r	m	s	e	c	r	e	t	d
C	O	E	M	V	Y	H	F	V	F	V	M	E	K	M	H	Q
f	o	r	m	s	e	c	r	e	t	d	i	c	t	i	o	n

The Vatican and Cipher Secretariats

Before we meet our next character, who will help us close the door on the Renaissance and this section, we must backtrack a bit in time to set the stage in another scene populated by the Italian City States, the Vatican, and Cipher Secretariats.

In Pavia, Italy on July 4, 1474, Cicco Simonetta, secretary to the Dukes of Sfoza, oligarchs of Milan, wrote the first known manuscript devoted *solely* to cryptanalysis. He wrote thirteen rules for symbol substitution ciphers. Later, another Italian, Giovani Soro, was appointed *Cipher Secretary* for Venice in 1506. Soro's cryptanalytic prowess gained him two assistants and an office in the Doge's Palace above the Sala di Segret, in 1542. (The *Doge's Palace* was the official residence of the doges in Venice. The *Doge* (from the Latin *dux* or *leader*, or *duke*, in English) was the highest official of the republic of Venice for more than a millennium (roughly 800–1800 AD). They represented the virtual emblem of the sovereignty of the Venetian State.) Soro, and his highly placed assistants, worked on the most elevated level of security, deciphering all messages from foreign powers, intercepted by the Venetians.

Cryptographic assistants were also available at the Vatican. The practice became of such high consequence to the popes that the office of *Cipher Secretary to the Pontiff* was established in 1555. The first of these was Triphon Benicio de Assisi. Assisi assisted Pope Paul IV during warring times with King Philip II of Spain. In 1557, Assisi was adept at deciphering the King's cryptograms. By September 12, 1557, peace was made, due in no small measure to the cryptanalytic skills of Assisi.

In the late 1580s, the Argentis, a family of cryptologists, took over the cipher secretariat. They were the first to institute certain cryptanalytic methods, use of which later became widespread. This included a *mnemonic* or *memory aid* key to mix a cipher alphabet. Of great interest to us is Matteo Argenti, who wrote a 135-page book on cryptology, which many consider to be the height of Renaissance cryptography. The Argentis distributed polyalphabetic ciphers to cardinals for their personal use, but failed to trust them for the bulk of their cryptographic traffic. When they used these ciphers, they employed relatively long keys, for reasons cited below.

It was Matteo Argenti who laid claims to being able to cryptanalyze certain autokey polyalphabetic ciphers. Yet part of this success was due to the use of "weak keys", some of which could be easily guessed. However, by the time Vigenère had developed his ideas and they were refined, the methods of mixing alphabets and using large keys was sufficient to thwart the cryptanalysts of the day. Nevertheless, the nomenclators (discussed earlier, see page 40), held sway for three more centuries over its more powerful cousin, the polyalphabetic autokey cipher. The reasons for this stem from the user more than the cipher. Cryptographers of the day were not enamored with the slowness of polyalphabetic ciphers, of having to always keep track of cipher alphabets, and what they perceived as a lack of precision, too much room for errors, and so on. Although not popular in the main, polyalphabetic ciphers did play a role, often a vital one at the time. We will learn more about this in the next section.

We close this section with Sir Francis Bacon, (1566–1626) whom we already discussed on page 36. He developed a steganographic device where one simply changes the typeface of random text to hide the existence of a message. He also invented a cipher, called *the bilateral cipher* (which today would be known as 5-bit encryption), in which he used a combination of substitution and steganography.

In the Chapter 2, we have another 500 years to put under the microscope.

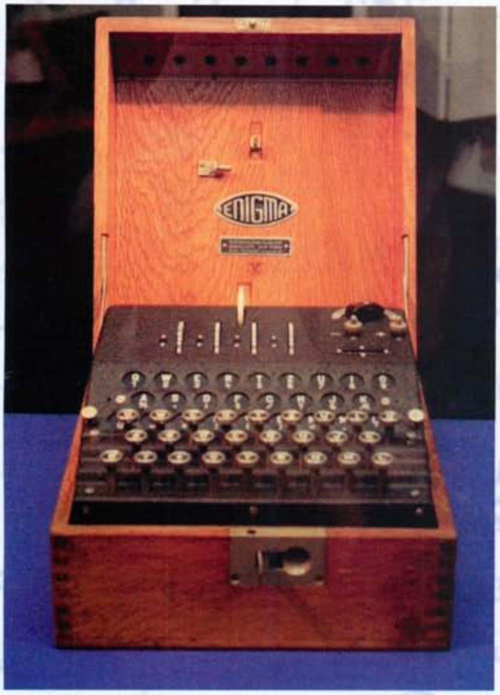
Codebreaker

THE HISTORY OF CODES AND CIPHERS, FROM THE ANCIENT PHARAOHS TO QUANTUM CRYPTOGRAPHY

STEPHEN PINCOCK

BUY THE BOOK
BREAK THE CODES

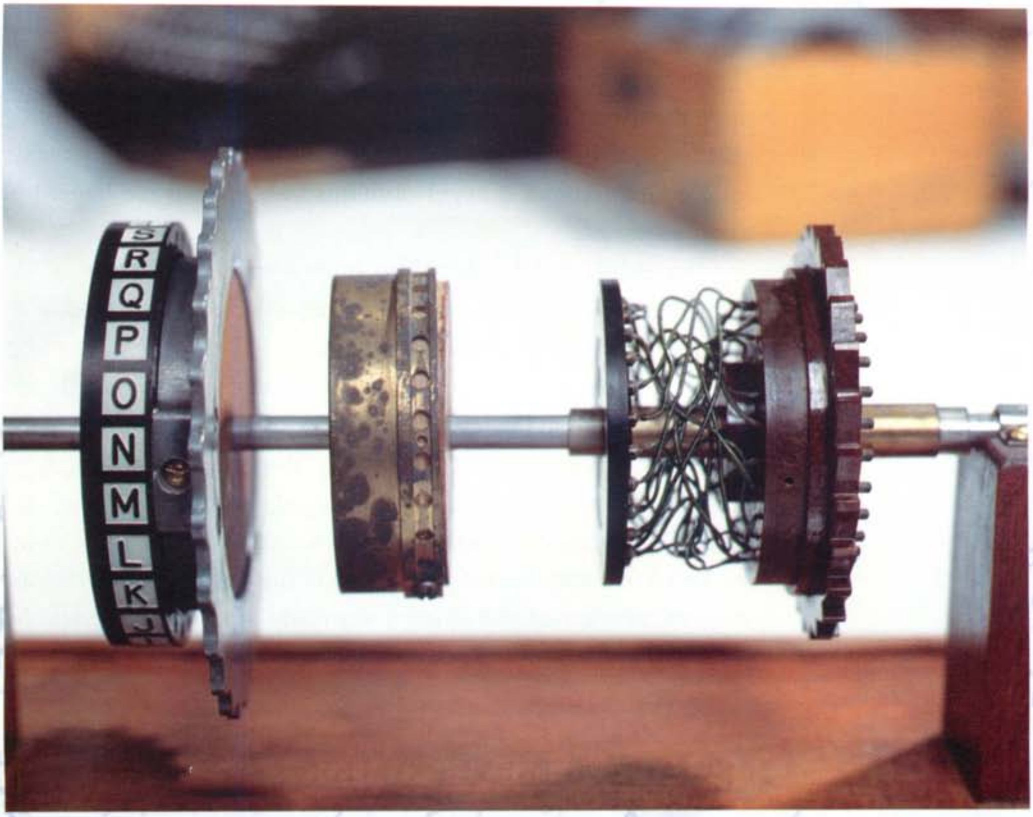
THE ENIGMA MACHINE



Dr Arthur Scherbius, an engineer living in Berlin, developed the first Enigma machine in the 1920s as a means of encrypting commercial messages. The German government adopted the machine three years later, making substantial modifications to improve the security that the device offered.

The Enigma machine was a portable encryption machine about the same size as the processor unit of a desktop computer. A keyboard at the front of the machine was used to type in the message. Above the keyboard was a series of 26 lamps, each showing a letter of the alphabet. When a key was pressed, one of the lamps lit up, showing what that letter needed to be replaced with in the encrypted text. The letters were then noted down by a second operator, who then sent the encrypted message using Morse code. These messages were then picked up by the intended recipients, who typed them into their own Enigma machine, set up in the same way as the sender's, and obtained the original message. However, eavesdroppers could also pick up these encrypted radio messages, and that is exactly what the Allies did through a series of radio listening posts. Even if eavesdroppers had their own Enigma machine, it would need to be set up in the same way as the sender's to decode the message. The internal complexity of the Enigma machine made this incredibly difficult.

Inside the original version of the machine were three rotating cylinders, or rotors. Each rotor had a series of internal wirings and electrical contacts on their faces so that every different position of the rotor resulted in a different electrical connection between the keyboard keys and the lamps. When a key was pressed, the right-most rotor rotated by one character in a similar way to a milometer in a car. After 26 rotations, the middle rotor would then rotate by one character. After 26 rotations of this rotor, the left-most rotor would rotate. These turn-overs, as they were called, were effected by a notch in the rotor ring. However, to increase the complexity of the encryption, it was possible for the operator to set the notch on each ring to 26 different positions.



Above: Rotor from an Enigma machine. The green wires on the right made an electrical connection between the keyboard, where the message was typed in, and the display, where the encrypted version of each letter would light up.

This might mean that the middle rotor might rotate after the first 10 characters had been typed and only then after every 26th rotation.

A reflector at the end of the rotors meant that the signal went back through the three rotors by a different route than on the way through.

Although these elements gave an almost unimaginable number of possible settings, the complexity of the encryption was further increased by a plugboard at the front of the machine. With this, specific pairs of letters could be interchanged by inserting cables between the plugs (or steckers as they subsequently became known to codebreakers, using the original German word) marked with those letters.

According to Frank Carter and John Gallehawk, there were 158 million million million possible different ways of setting up the machine at the beginning of the cipher process. It is little wonder that the Germans had high confidence in its ability to keep messages secret.

Although it is often imagined that British and American codebreakers did not have access to an Enigma machine until just before the start of the war, in fact they had one of Scherbius' commercial machines as early as 1926, purchased in Vienna by Dilly Knox, a member of C.C.&C.S. Indeed, it has subsequently been revealed that the patents for the commercial Enigma machine had been lodged with the British patent office in the 1920s.

However, complex mathematics on its own was not enough. To use these theories, they needed to construct a card-based catalog listing all the possible permutations for the more than 100,000 possible rotor configurations, a hugely arduous task without the benefit of a computer.

The Polish codebreakers also built a machine known as the cyclometer, constructed from two Enigma rotors, and used it to generate these permutations more quickly.

The cyclometer was used to prepare a catalog of the length and number of cycles in the "characteristics" for all 17,576 positions of the rotors for a given sequence of rotors. Since there were six such possible sequences, the resulting "catalog of characteristics," or "card catalog," comprised a total of 6 x 17,576 = 105,456 entries.

Rejewski wrote that the preparation of the catalog, "was laborious and took over a year, but when it was ready ... daily keys [could be obtained] within about fifteen minutes."

ENCRYPTING THE ENCRYPTION

In 1938, the Germans changed the way Enigma machines were operated. Instead of using the common rotor starting positions in the manual, every operator chose his own settings. The start settings were transmitted unencrypted. So, for example, the message might start with AXN as before. However, the operator would then think of a different rotor start setting that would be used to encrypt the message itself, HVO, say. He would then type this into the Enigma machine twice—HVOHVO. However, because the machine had already been set up with the initial AXN setting, it would encrypt HVOHVO as something entirely different—EYMEHY, for example. It is important to notice that there is no repetition in this encrypted version, since with each character typed the rotors move on by one position. Thus, the message sent by the operator would begin AXNEYMEHY and be followed by the message encrypted using HVO rotor settings.

On receiving this message, the recipient would see instantly that he should set his rotors to AXN initially. Typing in EYMEHY would then give him HVOHVO, and he would reset the rotors to the HVO position. The rest of the message would then be unencrypted as he typed.

This new complication invalidated the catalog method developed by the Poles and must have been a soul-destroying experience after so much time and resources were invested in it. However, they soon discovered another method, again using mathematical group theory.

You will notice in our example of the rotor settings above that the message settings were encrypted as EYMEHY and that the first and fourth characters are the same—the letter E. Rejewski and his colleagues noticed that this repetition of individual characters in the first and fourth positions (and also the second and fith and the third and sixth) happened relatively frequently. The instances where this occurred came to be known as "females."

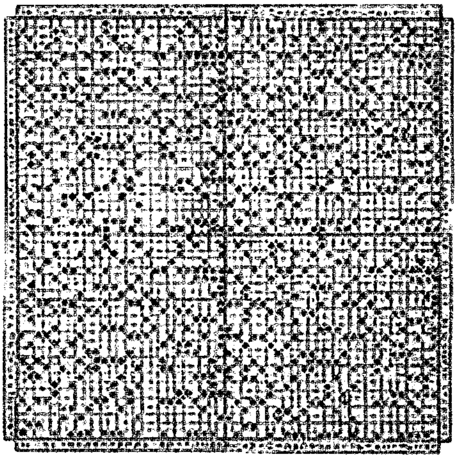
The Poles built six machines called "bombas," each of which comprised three Enigma rotors mechanically coupled together, which mechanically searched for rotor settings that would produce such females. Six were produced so that all possible orders of rotor could be checked at the same time – i.e. AXN, ANX, NAX, NXA, XAN, and XNA.

However, using the bombas in this way relied on none of the letters involved being steckered. Initially, just three letter pairs were steckered, but later the Germans increased this to ten pairs, so Zygalski devised an alternative method using perforated sheets of cardboard.

The process of creating these "Zygalski sheets" was very time consuming, as large numbers of sheets were required and the perforations—often up to a thousand per sheet—were made by hand using razor blades.

26 sheets were created, each one representing one possible starting position of the left-hand rotor in the Enigma machine. On each sheet, a 26 x 26 grid was marked with the letters A to Z down the left hand side and A to Z across the top. The letters on the left represented the starting position of the middle rotor while those across the top represented the initial starting position of the right-hand rotor.

Below: Example of a Zygalski sheet.



We know that our message starting AXN EYMEHY contains a female where the first and fourth characters of the message settings are the same. This means that on the Zygalski sheet representing the letter A in the left-hand rotor position, there would be a hole perforated on the grid at the point where X on the left-hand column meets N from the top row.

If other messages are transmitted on the same day by the same operator, and also include females in their message settings, we can start to stack sheets together so that their grids overlap exactly. When this stack of sheets is held up to the light, only those settings where there the holes overlap—and the light shines through—are possible settings that day. Each sheet added to the pile reduced the number of potential start settings still further. Given enough messages of the right format, the initial message settings might ultimately be deduced.

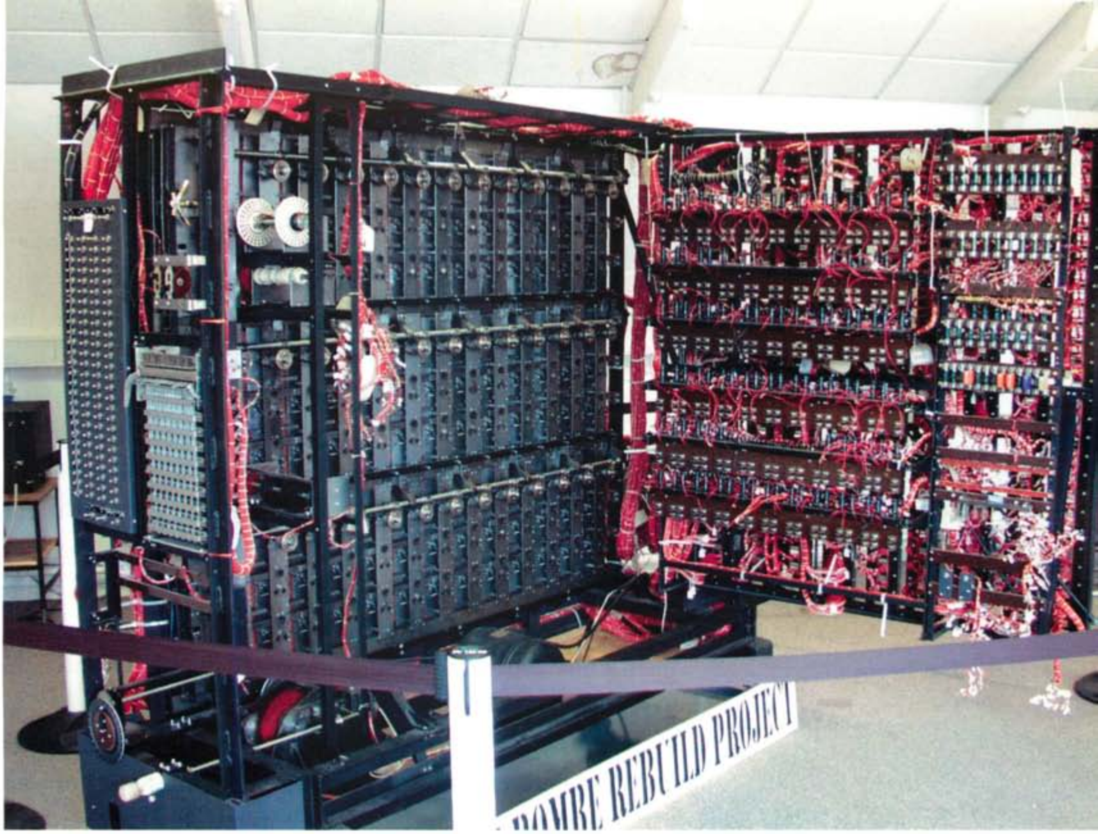
In December 1938, even this method became impractical, when the Germans introduced a new sophistication to the system. Instead of using three rotors in any permutation, operators could now choose any three rotors from a set of five. This increased the number of rotor settings tenfold and the task of creating the necessary sheets was beyond the codebreakers' resources.

Events soon overtook the Poles. With the impending invasion of the country, they realized they needed to share their work with others. As Germany prepared to invade, the Poles gave locally-built replicas of military Enigma machines to both G.C.&C.S. and French intelligence.

Below: Alan Turing (1912–1954), who devised a number of techniques for breaking German ciphers, including the "bombe," which could find settings for the Enigma machine.

BREAKING ENIGMA

In order to decrypt a message, the recipient—and any eavesdropper—needed to know which three rotors had been chosen and their positions in the machine, where the turn-over



notches had been set, which starting positions had been used for each rotor (as indicated by the letters shown in the small windows at the top right), and which letters had been interchanged using the steckers.

Above: The "bombe," which was used to decode Enigma settings.

It was the increased number of stecker pairs that gave Bletchley Park's codebreakers their biggest challenge. For each rotor setting, there were more than 2.5 million million million possible plugboard settings. This seemingly impossible task was made easier with the invention of an electrical device known as a "bombe," conceived by the Cambridge mathematicians Alan Turing and Gordon Welchman. The name reflected the Polish "bomba," but was in fact a totally different device.

Essential to this approach was being able to find what is known as a crib. If you consider the nature of written correspondence, it is highly structured. For example, when you write a letter to someone, you often begin with "Dear Sir/Madam," and end with "Yours faithfully."

This was also the case with many of Germany's wartime messages, although the structured elements were often different. Messages might

Above: The "bombe."

frequently begin with the word "secret," while messages from naval vessels often included the weather and their position. One operator was particularly fond of using IST—the German word for is—as his message setting. Another operator in Bari frequently used the initials of his girlfriend as the starting positions of the rotors. Breaking Enigma, then, was as much about highlighting human frailties as technical ones.

Finding the correct position of this crib in the ciphertext was not child's play—some Enigma operators prefixed often-repeated phrases or words with dummy characters to confound potential codebreakers.

The design of the bombe allowed its operators to check the 26 possible stecker partners of a given input letter simultaneously for each of the nearly 18,000 possible rotor settings. As it ran through these settings, if it came across a series of settings that corresponded with the crib, it stopped. Manual techniques, such as frequency analysis, were then used to test these rotor settings. If the frequency of letters corresponded generally with what would be expected from a typical German text, then other stecker pairs would be suggested. Eventually, from all this hard work and a huge amount of good fortune, they would arrive at the original message settings used for that day's messages, though this did not happen every day.

One interesting technique used by B.P. was known as "gardening." This involved provoking the German forces to include known words in their messages. For example, if an area had been cleared of mines, B.P.'s codebreakers would request of the Army that the area be mined again in the hope that the Germans would include the word *minen* in messages emanating from the area.

The first Enigma message was broken at Bletchley Park on January 20, 1940, but it was of vital importance not to let Germany know that the Allies were now able to read many of its messages. In order to hide the existence and success of Bletchley Park, the British

Above: Reinforcements disembarking at a Normandy beach during the Allied invasion of France on D-Day (June 6, 1944).

Government invented a spy with the codename Boniface, and an imaginary network of agents in the Fatherland. Thus, messages would be sent to various parts of the British military that implied that Boniface, or one of his spies in Germany, had overheard a conversation between high-ranking German officers, or had found a classified document in a wastebin. This way, if the information was leaked back to the Germans, they would not realize that their wireless signals were being eavesdropped.

By the end of the war, the Bletchley Park team had broken more than two and a half million Enigma messages, and had made highly significant contributions to the Allied victory. Certainly, the D-Day landings would have been considerably more difficult without the ability to decode German messages. The ability of Bletchley Park's codebreakers to read Enigma code in all probability shortened the war.

INVISIBLE INK AND OTHER TOOLS OF THE SPYING TRADE

About 10 minutes past midnight on June 13, 1942, four men from a German U-boat came ashore on Long Island, New York with the aim of sabotaging the production of American equipment and supplies and striking fear into the U.S. population.

The men had come laden with $175,200 in U.S. currency and enough explosives to fuel a two-year campaign, but within 48 hours, their mission faltered. On the evening of June 14, the leader of the group, George John Dasch, lost his nerve, and turned himself in with a call to the F.B.I. in New York.

Within days, he had been taken into custody and thoroughly interrogated. F.B.I. agents going through Dasch's things came across a handkerchief that they subjected to a test using ammonia fumes. The test revealed invisible writing in a copper sulfate compound, listing incriminating names, addresses, and contacts for Dasch's group and another party of saboteurs who had come ashore in Florida. The plot was revealed, and Dasch and another spy by the name of Ernest Burger were the only two of the eight men not put to death the following month.

Like the Nazi saboteurs, spies throughout history have used invisible ink and other forms of steganography to hide information from their enemies. Working incognito, it isn't enough for a spy to disguise the meaning of a message with cryptography—he or she needs to hide the fact that there is a message there at all.

One technique makes use of a pack of cards. The pack is arranged into an agreed order, and a message written on the side of the deck. Once the pack is shuffled, the marks on the side of the pack become almost invisible until the desired recipient rearranges them.

In ancient Greece, Aeneas the Tactician also described a technique that involved poking tiny holes in a book or message above or below existing letters as a way of conveying secret words—very similar methods were still in use during twentieth-century wars.

Another means of hiding large amounts of secret information in a tiny space was reportedly developed by the Germans during World War II.

Opposite: German spy Ernest Burger, arrested after one of the men turned himself in to the F.B.I.
Above: 1942: German submarines off the U.S. coast.

This trick, called a microdot, consists of an image —for example of a secret document—that has been photographed and reduced to the size of a type-written period. The miniscule size of the dots allowed them to be concealed in letters or telegrams sent through the normal channels. The intended recipient could then read the dot's contents with a microscope.

In modern times, steganography has entered the digital realm. Digital pictures or audio files, which contain large amounts of data, have been used to hide messages. By making subtle changes to the binary code for the file, it is possible to embed data that could go un-noticed.

HOW TO MAKE INVISIBLE INK

Invisible ink can be made from a wide variety of substances, some of which you probably have around the house. The simplest are citrus juices, onion juice, or milk. By dipping a brush, pen nib, or even your finger into the juice and writing on a piece of paper, you can inscribe an invisible message. These inks will be made visible with the heat of a light bulb or iron. In the case of lemon juice, this is because the paper that has absorbed some of the acidic juice browns at a lower temperature than the rest of the paper.

Another easily obtained invisible ink is vinegar, which is revealed by red cabbage water. A host of other chemicals can be used, including copper and iron sulfates, and ammonia.

When writing in invisible ink, it's a good idea to write a decoy message on the paper using a normal ball-point pen, since blank paper might look suspicious.

HITLER'S CIPHER

Variations on Enigma were used for most of the secret messages the German military were exchanging. However, some messages—principally those sent by Hitler to his various generals—were considered too secret for even that supposedly secure means of encryption.

Messages that had been encrypted using a cipher system other than Enigma were first intercepted in 1940. The codebreakers at B.P. gave messages encrypted in this way the generic nickname "Fish."

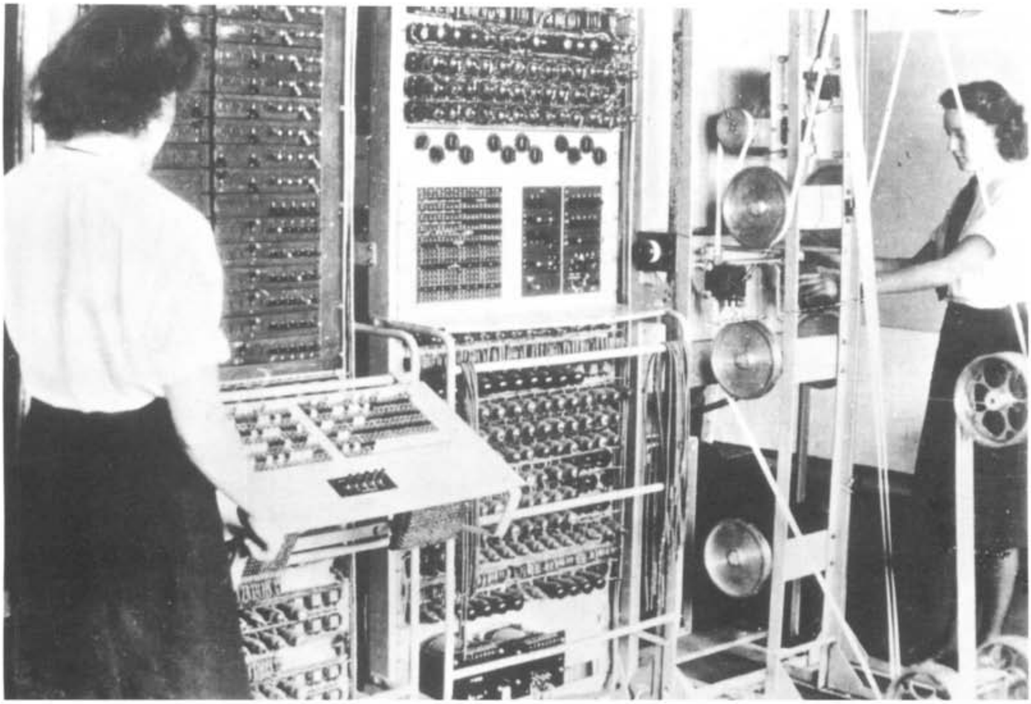
It later emerged that a machine much larger than the portable Enigma machines was used to encrypt these messages. The Lorenz SZ40 used 12 rotors, and as a result was almost unimaginably more complex than Enigma. Of course, the only way that the codebreakers at B.P. were aware of the machine was through the encrypted messages it produced. They gave this unseen machine the nickname "Tunny," after the fish of the same name. Later in the war, other encryption machines used by the Germans were also given fishy nicknames: "Sturgeon," for example.

ANALYSIS

The SZ in the Lorenz machine name stood for *Schlüsselzusatz*, or additive key, and this gives the basis on which the machine encrypted its text. The machine represented letters using a five-character-long string of binary zeros and ones. For example, the letter A was 11000, while L was 01001.

Each letter was encrypted by combining its binary representation with the representation of another letter using an operation known as exclusive-or (XOR). This operation has the following properties on individual binary digits:

0 XOR 0 = 0
0 XOR 1 = 1
1 XOR 0 = 1
1 XOR 1 = 0



Above and opposite:
The *Colossus* machine, the world's first programmable computer.

Part of the problem was keeping two punched paper tapes traveling at high speed in synchronization. B.P.'s Alan Turing had previously worked with a young telephone engineer called Tommy Flowers when constructing the bombes used for decoding Enigma, and asked for his help again. Flowers suggested building a machine that replaced one of the paper tapes with a series of valves that acted like digital switches, eliminating the synchronization problems.

It took ten months and 1,500 valves to build the machine, and the first was installed and began work at B.P. in December 1943. The machine, *Colossus*, was the world's first programmable computer. It was the size of a room and weighed a ton, but the valve technology meant that *Colossus* could crack a Lorenz-encrypted message in hours rather than days. It worked by comparing the two data streams, counting each match based on a programmable function. An improved *Coloussus Mark II* was installed in June 1944, and by the end of the war, 10 *Colossi* with an even higher number of valves were in use at B.P.