To judge in this [utilitarian] way demonstrates ... how small, narrow and indolent our minds are; it shows a disposition always to calculate the reward before the work, a cold heart and a lack of feeling for everything that is great and honours mankind. Unfortunately one cannot deny that such a mode of thinking is common in our age, and I am convinced that this is closely connected with the catastrophes which have befallen many countries in recent times; do not mistake me, I do not talk of the general lack of concern for science, but of the source from which all this has come, of the tendency to look out everywhere for one's advantage and to relate everything to one's physical well being, of indifference towards great ideas, of aversion to any effort which derives from pure enthusiasm.

Gauss

We agreed then on the good things we have in common. On the advantage of being able to test yourself, not depending on others in the test, reflecting yourself in your work. On the pleasure of seeing your creature grow, beam after beam, bolt after bolt, solid, necessary, symmetrical, suited to its purpose; and when it's finished, you look at it and you think that perhaps it will live longer than you, and perhaps it will be of use to someone you don't know, who doesn't know you. Maybe, as an old man you'll be able to come back and look at it, and it will seem beautiful, and it doesn't really matter so much that it will seem beautiful only to you, and you can say to yourself 'maybe another man wouldn't have brought it off'.

Primo Levi

To be placed on the title-page of my collected works: Here it will be perceived from innumerable examples what is the use of mathematics for judgement in the natural sciences, and how impossible it is to philosophise correctly without the guidance of Geometry, as the wise maxim of Plato has it.

Galileo

Mathematicians are people who devote their lives to what seems to me a wonderful kind of play.

Constance Reid

The Pleasures of Counting

T. W. KÖRNER

Trinity Hall
Cambridge

CAMBRIDGE
UNIVERSITY PRESS

CHAPTER 13

Enigma

13.1 Simple codes

In 1929 a group of Polish mathematics students at the university of Poznán were invited, under pledge of secrecy, to attend a weekly night course in cryptology (the art of making and breaking codes). Up until then, code-breaking had been the province of the gifted amateur, usually a linguist (the Cambridge University Library still shelves books on cryptology in its palaeography section, sandwiched between Shorthand and Ancient Greek). Recently, however, the German army had switched to a mechanical enciphering method which had resisted all the efforts of the Polish code-breakers. Perhaps mathematical methods might succeed against machines when traditional means failed.

Let us consider messages written in capital letters using X to mark spaces such as, for example,

SENDXTWOXDIVISIONSXTOXPOINTXFIVEXSEVENTEEN.

It is sometimes convenient to associate letters with numbers in the following obvious way

$$\mathtt{A} \leftrightarrow 0,\ \mathtt{B} \leftrightarrow 1,\ \mathtt{C} \leftrightarrow 2, \ldots,\ \mathtt{Z} \leftrightarrow 25.$$

The first code most children learn consists in choosing an integer k and replacing the letter associated with r by the letter associated with $r+k$. This recipe is incomplete since $r+k$ may not lie between 0 and 25. To get round this, we first subtract a multiple of 26, ($26j$, say) so that $r+k-26j$ lies between 0 and 25 and replace the letter associated with r by the letter associated with $r+k-26j$. Thus if we choose $k=20$, B which corresponds to 1 goes to the letter V which corresponds to 21 and J which corresponds to 10 goes to the letter D which corresponds to $30-26=4$. This is called the Caesar code† because it is said to have been used by Julius Caesar.

†Historians and professional cryptologists draw a clear distinction between codes and ciphers. In a code, groups of letters or numbers are substituted for words or phrases according to a 'dictionary' or code book. In a cipher, letters are changed or shuffled according to a fixed set of rules. Thus the Caesar code is actually a cipher. Mathematicians are mainly interested in ciphers and use the words code and cipher interchangeably. I shall follow the lax mathematical usage. (In the British Navy a cryptographic system was a cipher when used by an officer but became a code in the hands of a non-officer.)

Exercise 13.1.1 *Show that the message above becomes*

MYHXRNQIRXCPCMCIHMRNIRJICHNRZCPYRMYPYHNYYH.

If we represent our message by π and our encoded message by $\mathrm{T}^k\pi$ then it is easy to see that

$$\mathrm{T}^k\mathrm{T}^l\pi = \mathrm{T}^{k+l}\pi,$$

and that

$$\mathrm{T}^l\pi = \pi \text{ whenever } l \text{ is a multiple of 26.}$$

In particular if we successively form $\mathrm{T}^k\pi$, $\mathrm{T}^1\mathrm{T}^k\pi$, $\mathrm{T}^2\mathrm{T}^k\pi, \dots, \mathrm{T}^{25}\mathrm{T}^k\pi$, one of these 26 expressions will be the original message. If we apply this idea to the coded message ρ of Exercise 13.1.1 we get

$\rho =$ MYHXRNQIRXCPCMCIHMRNIRJICHNRZCPYRMYPYHNYYH

$\mathrm{T}^1\rho =$ NZIYSORJSYDQDNDJINSOJSKJDIOSADQZSNZQZIOZZI

$\mathrm{T}^2\rho =$ OAJZTPSKTZEREOEKJOTPKTLKEJPTBERATOARAJPAAJ

$\mathrm{T}^3\rho =$ PBKAUQTLUAFSFPFLKPUQLUMLFKQUCFSBUPBSBKQBBK

$\mathrm{T}^4\rho =$ QCLBVRUMVBGTGQGMLQVRMVNMGLRVDGTCVQCTQCRPCL

$\mathrm{T}^5\rho =$ RDMCWSVNWCHUHRHNMRWSNWONHMSWEHUDWRDUDMSDDM

$\mathrm{T}^6\rho =$ SENDXTWOXDIVISIONSXTOXPOINTXFIVEXSEVENTEEN.

Exercise 13.1.2 *The following has been produced by applying* T^k *(for some value of* k*). Find the original message.*

GOVVHNYXO

The Caesar code is easily broken because there are only 25 such codes (or 26 if, as a mathematician would, you count the case $k = 0$).

The next code that most people learn is simple substitution in which each of the 26 letters is replaced by another in such a way that no two letters are replaced by the same one. We give an example in Table 13.1.

Table 13.1. *A simple substitution code.*

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

Exercise 13.1.3 *Show that the message about the two divisions becomes*

YNCMKDTLKMQJQYQLCYKDLKRLQCDKFQJNKYNJNCDNNC.

Since we can choose 26 letters to replace A, 25 letters to replace B (one has already been used), 24 letters to replace C (two have already been used), and so on, there are

$$26 \times 25 \times 24 \times \cdots \times 3 \times 2 \times 1 = 26! = 403\,291\,461\,126\,605\,635\,584\,000\,000$$

different simple substitution ciphers.

Exercise 13.1.4 *Use Exercise 11.4.14 to verify that the value given for 26! is not too far off.*

We cannot solve this cipher by working through all the possibilities. However, as most people know, almost any message longer than a post card which uses this kind of code can be deciphered using statistical properties of the English language.

Take, for example, the following result of using a simple substitution cipher.

VARHTAOWAOTAJBCOQCAORTHIQOIAWOMZMQAU
MOWLEEOJKJLIOVAOLIQTHNFBANOVFQOLOQCL
IDOQCJQOJIZCHWOQCATAOLMOIHOQLUAORHTO
NABLXCATLIKOBLXCATMOELDAOQCLMOLIOQCA
ORLAENOVARHTAOJIZOHROFMOCJNOQLUAOQHO
NABLXCATOJOQAEAKTJUOELDAOQCAOAOJUXEA
OKLPAIOFMOQCAOBHUXJIZOVJQQJELHIOJINO
VTLKJNAOWHFENOEHIKOJKHOCJPAOBAJMANOQ
HOAOLMQOLQOCJMOIHOXTJBQLBJEOMLKILRLB
JIBA

We tabulate the number of times each letter occurs in the coded message. as Table 13.2

The most common letter in ordinary text is X, (spaces are more frequent than any single letter), followed by E, followed by T, A, I and O (these last four having similar frequencies). Let us write the letters we guess in lower case. Since the most frequent letter in the coded message

Table 13.2. *Frequency count for a coded message.*

Letter	A	B	C	D	E	F	G	H	I	J	K	L	M
Occurrences	37	11	16	3	11	5	6	16	18	22	8	26	12
Letter	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Occurrences	10	61	2	23	7	10	13	6	6	5	6	0	4

is O and the second most frequent is A we guess that O corresponds to x and A to e. With these guesses our text becomes

```
VeRHTexWexTeJBCxQCexRTHIQxIeWxMZMQeU
MxWLEExJKJLIxVexLIQTHNFBeNxVFQxLxQCL
IDxQCJQxJIZCHWxQCeTexLMxIHxQLUexRHTx
NeBLXCeTLIKxBLXCeTMxELDexQCLMxLIxQCe
xRLeENxVeRHTexJIZxHRxFMxCJNxQLUexQHx
NeBLXCeTxJxQeEeKTJUxELDexQCexexJUXEe
xKLPeIxFMxQCexBHUXJIZxVJQQJELHIxJINx
VTLKJNexWHFENxEHIKxJKHxCJPexBeJMeNxQ
HxexLMQxLQxCJMxIHxXTJBQLBJExMLKILRLB
JIBe.
```

The three letter word QCe occurs four times in this short passage so it is a reasonable guess that it represents the (it might, of course, represent she or ate or some other word, but we must start somewhere and the occurs much more frequently in English than any of the other alternatives). With this guess Q corresponds to t and C to h. Our text now becomes

```
VeRoTexWexTeJBhxthexRTHItxIeWxMZMteU
MxWLEExJKJLIxVexLItTHNFBeNxVFtxLxthL
IDxthJtxJIZhHWxtheTexLMxIHxtLUexRHTx
NeBLXheTLIKxBLXheTMxELDexthLMxLIxthe
xRLeENxVeRHTexJIZxHRxFMxhJNxtLUextHx
NeBLXheTxJxteEeKTJUxELDexthexexJUXEe
xKLPeIxFMxthexBHUXJIZxVJttJELHIxJINx
VTLKJNexWHFENxEHIKxJKHxhJPexBeJMeNxt
HxexLMtxLtxhJMxIHxXTJBtLBJExMLKILRLB
JIBe.
```

The new text contains the word thJt suggesting that J corresponds to a and the word tH suggesting that H corresponds to o and the words L and Lt suggesting that L corresponds to i. With these suggested substitutions we get

```
VeRoTexWexTeaBhxthexRToItxIeWxMZMteU
MxWiEExaKaiIxVexiItToNFBeNxVFtxixthi
IDxthatxaIZhoWxtheTexiMxIoxtiUexRoTx
NeBiXheTiIKxBiXheTMxEiDexthiMxiIxthe
xRieENxVeRoTexaIZxoRxFMxhaNxtiUextox
NeBiXheTxaxteEeKTaUxEiDexthexexaUXEe
xKiPeIxFMxthexBoUXaIZxVattaEioIxaINx
```

```
VTiKaNexWoFENxEoIKxaKoxhaPexBeaMeNxt
oxexiMtxitxhaMxIoxXTaBtiBaExMiKIiRiB
aIBe.
```

Looking at the words iM, VattaEioI, aKo and haPe we guess that M corresponds to s, I to n, K to g and P to v. The message now reads

```
VeRoTexWexTeaBhxthexRTontxneWxsZsteU
sxWiEExagainxVexintToNFBeNxVFtxixthi
nDxthatxanZhoWxtheTexisxnoxtiUexRoTx
NeBiXheTingxBiXheTsxEiDexthisxinxthe
xRieENxVeRoTexanZxoRxFsxhaNxtiUextox
NeBiXheTxaxteEegTaUxEiDexthexexaUXEe
xgivenxFsxthexBoUXanZxVattaEionxanNx
VTiKaNexWoFENxEongxagoxhavexBeaseNxt
oxexistxitxhasxnoxXTaBtiBaExsigniRiB
anBe
```

Exercise 13.1.5 *Complete the decipherment. The passage comes from page 469 of the Penguin translation of Hašek's* The Good Soldier Švejk.

Exercise 13.1.6 *The following has been produced by a simple substitution cipher. Decipher it.*

```
LZKSTFIKSHYRNSPVSOYAZKMSPOOWMTSYRSLZ
KSTZPMLSTLPMYKTSLZKSCPQNSUWCSUDSAPKS
FRNSLZKSNFROYRCSIKRSUDSOPRFRSNPDQKSL
ZKSTFIAQKSPVSLKSLSWTKNSUDSAPKSYTSJWY
LKSQPRCSUWLSLZFLSCYXKRSUDSNPDQKSYTSM
FLZKMSTZPMLSFRNSZPQIKTSYTSYRSIDSPAYR
YPRSQWOHDSLPSTPQXKSYL.
```

If you need more text, use the rest of the message. Otherwise use it as a check.

```
DPWSOFRSTKKSVMPISLZYTSKSFIAQKSLZFLSL
ZKSQPRCKMSLZKSTFIAQKSLZKSKFTYKMSYLSY
TSLPSVYRNSLZKSOPNKSDPWSOFRSFQTPSTKKS
LZFLSYLSZKQATSLPSHRPESLZKSTWUBKOLSEZ
YOZSYTSUKYRCSNYTOWTTKNSRPLYOKSLZFLSY
RSTPQXYRCSLZYTSOPNKSDPWSZFXKSWTKNSHR
PEQKNCKSEZYOZSYLSYTSZFMNSLPSCYXKSLPS
FSIFOZYRK
```

Exercise 13.1.7 *Show that the Caesar code is a simple substitution code and use this fact to give a very quick method of deciphering any long passage encoded by using a Caesar code.*

Can we find a simple code which is difficult to crack using frequency methods? One such code is the simple rotation code R. Let us associate letters with numbers as we did in the discussion of the Caesar code so that

$$\mathtt{A} \leftrightarrow 0,\ \mathtt{B} \leftrightarrow 1,\ \mathtt{C} \leftrightarrow 2, \ldots,\ \mathtt{Z} \leftrightarrow 25.$$

If the rth letter of our code is associated with the integer i_r we replace it by the letter associated with $r-1+i_r-26j_r$ where j_r is the integer such that $0 \le r-1+i_r-26j_r \le 25$.

Exercise 13.1.8 *(i) Show that simple rotation encodes* ROTATION *as*

RPVDXNUU.

(ii) The following short coded message has been obtained using simple rotation

NPVAFFJ.

Decode it.

If we represent our message by π and our encoded message by $\mathtt{R}\pi$ we may define new codes $\mathtt{R}^2$, $\mathtt{R}^3$ and so on by taking

$$\mathtt{R}^2\pi = \mathtt{R}(\mathtt{R}\pi), \mathtt{R}^3 = \mathtt{R}(\mathtt{R}^2\pi), \ldots \mathtt{R}^{k+1} = \mathtt{R}(\mathtt{R}^k\pi),$$

for $k \ge 1$.

Exercise 13.1.9 *(i) Describe $\mathtt{R}^k$ in the same way as we described* R.

(ii) Why is it reasonable to write $\mathtt{R}^1 = \mathtt{R}$? Why is it reasonable to write $\mathtt{R}^0\pi = \pi$? Why is it reasonable to write $\mathtt{R}^{-k} = \mathtt{R}^{26-k}$ if $1 \le k \le 26$? (All these questions have at least two good answers, but the reader is only asked for one.) Define $\mathtt{R}^l$ for a general integer l in such a way that $\mathtt{R}^l(\mathtt{R}^k\pi) = \mathtt{R}^{l+k}\pi$.

(iii) Suppose we use simple rotation R *as our coding method. Explain why, in a long message, on average, any given letter* A*, say, in the original message will be coded as any given letter* C *about 1/26th of the time. Conclude that the resulting coded message will show roughly equal frequencies of each letter.*

(iv) Does the conclusion of (iii) hold if we replace R *by $\mathtt{R}^k$ and k is divisible neither by 13 nor 2? Does it hold if k is divisible by 13 but not by 2? Without making a detailed investigation, state what you think will happen if k is divisible by 2 but not by 13.*

(v) Describe a method for breaking the code $\mathtt{R}^k$ for unknown k along the lines of our first method for breaking the Caesar code. Use your method to decode BVTIIPZW.

Here are two coded passages which cannot be read quite so easily. They both come from an essay by James Thurber entitled *Exhibit X* and included in [240]. In it, he recalls his time as a code clerk at the American Embassy in Paris in 1918 using a '... new code book [which] had been put together so hastily that the word "America" was left out, and code groups so closely paralleled true meanings that "LOVVE" for example was the symbol for "love".' (Kahn writes that during the 1920s and 1930s it was rare for 'the major codes of the major powers [to be broken] — always with the exception of those of the United States whose cryptograms were as transparent as a fish tank to any competent cryptanalyst'. At the beginning of the Second World War, the British had to indicate to the American government that, whilst they had never attempted and would never, under any circumstances, dream of attempting to break American codes, nonetheless it had been suggested that those codes might, conceivably, be vulnerable.)

Passage 1

```
IBUACXPYRSRDNQEIEQGNZTMFLFGDUAUNWDPRKYBKPKTVFWVIGFLH
XALZDBGYMSENADWIXQGUACWPYFRHXZAWGKGZVWYRYCPQOIMFIFMO
ZJJJVIJDEPWYOCIKAMPCIFSGALSUQCDTJIVXHPYKMJN0ZNWCMVMO
KRUYDSGDUETVCEYQNWRTZIRIYMXLEXPGPUPYAKBBQDAPSLWBFBNO
IBUAXTMZNPUV
```

Passage 2

```
WZRFHFZOUIGBRBVGNMJBDRZNKACUUFGFNJAKTPMMQCTPUAGRBUOV
GUIDMBCEPYPESJJUWZVFHFOFLONSRYGVCQLPFJDJODIIOSSRIGQZ
ETZVCPJJXLPWKXTAJEHFHYFNYIHPOSNRNDAKJPMIOTIJKSMRIUIF
LQJOLLRZWLFHAWTAJMUQWPDNDJETAQGPIVXAZDYHKFPEPSRRDWKA
KPQJEPYQLDFESSOYJMUUWAKNNRTPZFQMHXXMCWSJTKTRJCHYMNRJ
ZYADUMRDADTPTJFOJWBCV
```

The two codes have been obtained by combining the fairly weak simple substitution method with the extremely weak rotation method to produce something stronger than either. Because the passages are so short I think that either would be quite hard to break without some hint as to the method involved. (For example, the use of frequency counts reveals nothing.)

Exercise 13.1.10 *(i) The first passage π say has been coded by first* *applying a simple substitution cipher* S *and then applying the simple rotation cipher* R *to the result. The code could thus be represented as* $C = R^kS$. *Let us write* $\sigma = C\pi$. *Explain why, if* k *is not divisible by 2 or 13, this ensures that the frequency count will normally reveal nothing.*

(ii) Does it really matter if k *is divisible by 2 (but not by 13)? Does it matter if* k *is divisible by 13? Why?*

(iii) Once we know how the code was constructed, it is not too hard to break. Explain why there exists an l *with* $0 \leq l \leq 25$ *such that* $R^lC = S$. *Explain why* $R^l\sigma$ *can be decoded by the frequency method. At first sight it still looks as though we will have to look at* $R^p\sigma$ *for* $p = 0, 1, 2, \ldots, 26$ *and try to decode each of the 26 possibilities by the frequency method, but this is not the case. Explain why, if we find the number* n_p *of the most frequently occurring letter in* $R^p\sigma$, *then we would expect* l *to be the value of* p *for which* n_p *is largest.*

(iv) In order to save the reader time, I now reveal that the code has the form $R^3\pi$ *or* $R^{-3}\pi$. *Carry out the procedure suggested in (iii) to find out which. (If you guess right the first time, you should still check the other possibility so as to see what happens if you do not guess right.)*

(v) Find the message. Since the message is short, I include two hints. The first is a note of reassurance: one of the words in the original message does, in fact, end in X. The second is to remark that solution of such puzzles is much aided by the possession of a dictionary in which words are sorted by length and kth letter so that, for example, all seven-letter words with fourth letter E are listed together. Such compilations have been made easy by, but will also in due course be made obsolete by, the computer. Such aids must be used with care, but mine [153] gives only two seven-letter words with fourth letter E *ending in* TH, *namely* SEVENTH *and* BENEATH†.

The second passage is coded in much the same way *except that we reverse the order in which we apply the two codes* by first applying a rotation cipher R^k for some k and then applying a simple substitution cipher S to the result. The code could thus be represented as $C' = SR$. In my view, $C' = SR$ presents a much severer problem than RS or even $C = R^kS$. Whether the reader accepts my opinion or not she should try to decipher the second message without using any further information. If she finds an easy solution, I should be glad to see it. If not, she may agree with me that we have a very nice example in which the order we do things radically affects the result.

†But, it has been pointed out to me, AGREETH is also a possible word.

Writing the second passage in a way that reflects the period of 26 is a sensible first step but I suspect that it will remain baffling. (Since the page is not wide enough we split the table in two.)

	0	1	2	3	4	5	6	7	8	9	10	11	12
1	W	Z	R	F	H	F	Z	O	U	I	G	B	R
2	C	U	U	F	G	F	N	J	A	K	T	P	M
3	G	U	I	D	M	B	C	E	P	Y	P	E	S
4	N	S	R	Y	G	V	C	Q	L	P	F	J	D
5	E	T	Z	V	C	P	J	J	X	L	P	W	K
6	H	P	O	S	N	R	N	D	A	K	J	P	M
7	L	Q	J	O	L	L	R	Z	W	L	F	H	A
8	E	T	A	Q	G	P	I	V	X	A	Z	D	Y
9	K	P	Q	J	E	P	Y	Q	L	D	F	E	S
10	T	P	Z	F	Q	M	H	X	X	M	C	W	S
11	Z	Y	A	D	U	M	R	D	A	D	T	P	T

	13	14	15	16	17	18	19	20	21	22	23	24	25
1	B	V	G	N	M	J	B	D	R	Z	N	K	A
2	M	Q	C	T	P	U	A	G	R	B	U	O	V
3	J	J	U	W	Z	V	F	H	F	O	F	L	O
4	J	O	D	I	I	O	S	S	R	I	G	Q	Z
5	X	T	A	J	E	H	F	H	Y	F	N	Y	I
6	I	O	T	I	J	K	S	M	R	I	U	I	F
7	W	T	A	J	M	U	Q	W	P	D	N	D	J
8	H	K	F	P	E	P	S	R	R	D	W	K	A
9	S	O	Y	J	M	U	U	W	A	K	N	N	R
10	J	T	K	T	R	J	C	H	Y	M	N	R	J
11	J	F	O	J	W	B	C	V					

Is the code effectively insoluble? Not if we know or guess correctly even a small part of the passage. Suppose that we know that the last word of the passage is 'Thurber'†. Then we know, looking at the last letter of the passage, that r in the 21st column will be encoded as V. It follows that q in the 22nd column will also be encoded as V, as will p in the 23rd column and so on. We have the following list of decodes:

	0	1	2	3	4	5	6	7	8	9	10	11	12
V decodes as	l	k	j	i	h	g	f	e	d	c	b	a	z

†Many code messages are vulnerable because the first or last words can be guessed. The German naval code-breakers of the Second World War were much aided by the admiral in command at the Canadian port of Halifax whose messages invariably began 'SNO Halifax BREAK GROUP Telegram in [some number n] parts FULL STOP Situation.' In order to prevent this sort of attack, the instructions for the German dockyard cipher called for messages to end with an irrelevant word such as *Wassereimer*, *Fernsprechen* or *Kleiderschrank* but some signalmen followed these instructions to the letter. Similar clues were given by the tendency of some code users to foul language. I have been told that, to prevent such indiscretions on the Allied side, code clerks were issued with anthologies of poetry and told to choose their 'padding' from the poem of the day.

	13	14	15	16	17	18	19	20	21	22	23	24	25
V decodes as	y	x	w	v	u	t	s	r	q	p	o	n	m

Exercise 13.1.11 *Check that the guess that the last word is 'Thurber' yields the additional decodes*

	0	1	2	3	4	5	6	7	8	9	10	11	12
B	t	s	r	q	p	o	n	m	l	k	j	i	h
C	x	w	v	u	t	s	r	q	p	o	n	m	l
F	h	g	f	e	d	c	b	a	z	y	x	w	v
J	k	j	i	h	g	f	e	d	c	b	a	z	y
O	w	v	u	t	s	r	q	p	o	n	m	l	k
W	i	h	g	f	e	d	c	b	a	z	y	x	w

	13	14	15	16	17	18	19	20	21	22	23	24	25
B	g	f	e	d	c	b	a	z	y	x	w	v	u
C	k	j	i	h	g	f	e	d	c	b	a	z	y
F	u	t	s	r	q	p	o	n	m	l	k	j	i
J	x	w	v	u	t	s	r	q	p	o	n	m	l
O	j	i	h	g	f	e	d	c	b	a	z	y	x
W	v	u	t	s	r	q	p	o	n	m	l	k	j

Check that, after inserting these substitutions, the passage becomes

	0	1	2	3	4	5	6	7	8	9	10	11	12
1	i	Z	R	e	H	c	Z	p	U	I	G	i	R
2	C	U	U	e	G	c	N	d	A	K	T	P	M
3	G	U	I	D	M	o	r	E	P	Y	P	E	S
4	N	S	R	Y	G	g	r	Q	L	P	x	z	D
5	E	T	Z	i	t	P	e	d	X	L	P	x	K
6	H	P	u	S	N	R	N	D	A	K	a	P	M
7	L	Q	i	t	L	L	R	Z	a	L	x	H	A
8	E	T	A	Q	G	P	I	e	X	A	Z	D	Y
9	K	P	Q	h	E	P	Y	Q	L	D	x	E	S
10	T	P	Z	e	Q	M	H	X	X	M	C	x	S
11	Z	Y	A	D	U	M	R	D	A	D	T	P	T

	13	14	15	16	17	18	19	20	21	22	23	24	25
1	g	x	G	N	M	s	a	D	R	Z	N	K	A
2	M	Q	i	T	P	U	A	G	R	x	U	y	m
3	x	w	U	s	Z	t	o	H	m	a	k	L	x
4	x	i	D	I	I	e	S	S	R	I	G	Q	Z
5	X	T	A	u	E	H	o	H	Y	l	N	Y	I
6	I	i	T	I	t	K	S	M	R	I	U	I	i
7	v	T	A	u	M	U	Q	o	P	D	N	D	l
8	H	K	s	P	E	P	S	R	R	D	l	K	A
9	S	i	Y	u	M	U	U	o	A	K	N	N	R
10	x	T	K	T	R	s	e	H	Y	M	N	R	l
11	x	t	h	u	r	b	e	r					

The partial decode of our passage is quite promising. There are plenty of xs and it looks 'quite English'. The zs are a little hard to fit in but they might be part of place names or nonsense words. (It is usual to include a few nonsense words in messages to be encoded in order to complicate the code-breaker's task.) On the third line (columns 14–26) we have

```
xw?s?toxmak?x
```

which strongly suggests the phrase 'was to make' and gives the possible new substitutions

	0	1	2	3	4	5	6	7	8	9	10	11	12
H	r	q	p	o	n	m	l	k	j	i	h	g	f
L	c	b	a	z	y	x	w	v	u	t	s	r	q
U	p	o	n	m	l	k	j	i	h	g	f	e	d
Z	o	n	m	l	k	j	i	h	g	f	e	d	c

	13	14	15	16	17	18	19	20	21	22	23	24	25
H	e	d	c	b	a	z	y	x	w	v	u	t	s
L	p	o	n	m	l	k	j	i	h	g	f	e	d
U	c	b	a	z	y	x	w	v	u	t	s	r	q
Z	b	a	z	y	x	w	v	u	t	s	r	q	p

With these substitutions the first line of the passage becomes

```
inRenciphIGiRgxGNMsaDesNKA
```

The first two words must presumably be 'in enciphering' and there is, I think, a plausible guess for the next word.

Exercise 13.1.12 *Complete the decipherment. (If you find this hard do not worry. It is quite hard. If you find it tedious, you may begin to see that code-breaking consists of weeks of tedium and minutes of excitement.)*

Exercise 13.1.13 *If you had to encipher this code many times, what sort of mechanical aids would you ask for? If you had to decipher such codes regularly, what sort of mechanical aids would you ask for?*

Even if we cannot guess any part of the message, the code is vulnerable if we send too long a message. Observe that, if we write out the coded message in 26 columns as we did above, then *in each column* the same letter will always be encoded in the same way. If the message contains, say, more than 2600 letters, then each column will contain at least 100 letters, and it is a good, though not certain, bet that the most frequently appearing letter in a given column corresponds to the most frequently appearing letter in our messages, that is to say x.

Exercise 13.1.14 *Show that if you* **know** *which letter in each column corresponds to* x *then you can decipher the entire message.*

Even if our guess is wrong for a few columns, there will still be enough correct letters in our proposed decipherment to enable us to pass rapidly to the correct solution.

In fact, for sufficiently long messages encoded using methods of this type we do not even need to know the method used. Suppose that all we know is that there is a reasonably small integer such that if we write out the message in n columns then in each column the same letter will always be encoded in the same way. (The smallest such n is called *the period* of the code.) If we try the effect of writing out the message in m columns, then, if m and the period n have no common factor, the coding method will usually have the required effect of smoothing out letter frequencies. However, if $m = n$, the letter frequencies will usually exhibit great disparities of the same kind as we expected in the special case, discussed in the previous paragraph, when $m = n = 26$. If m and n have common factors, then we will see a greater or lesser degree of statistical regularity, but it will usually not be hard to distinguish the particular case when $m = n$. Once we have guessed n, the method of the previous paragraph may be used.

Looked at in this way, it is clear that the vulnerability of the codes discussed in this section to attacks based either on guessing certain words or on statistical methods, is due to their short periods. The natural way forward is to seek codes with longer periods. However, here we run into another problem.

Exercise 13.1.15 *(i) Encode the following message (the first part of the Zimmermann Telegram) using a code of the same type as we used on the second Thurber quotation:*

```
        WE INTEND TO BEGIN UNRESTRICTED SUBMARINE WARFARE
         ON THE FIRST OF FEBRUARY STOP WE SHALL ENDEAVOUR
        IN SPITE OF THIS TO KEEP THE UNITED STATES NEUTRAL
   STOP IN THE EVENT OF THIS NOT SUCCEEDING WE MAKE MEXICO
               A PROPOSAL ON THE FOLLOWING BASIS COLON
          MAKE WAR TOGETHER COMMA MAKE PEACE TOGETHER
```

Decode it. What will be the usual effect of mistakes in encoding the message?

(ii) (Optional but instructive) Try to construct a code which is harder to break than the ones so far discussed. Carry out the encoding and decoding of the message just given. What will be the usual effect of mistakes in encoding the message? (It is worth noting that the retransmission of a garbled message is often as valuable to the enemy code-breakers as the transmission in code of a known message.)

13.2 Simple Enigmas

If a cipher is to be used in battle, messages must be enciphered and deciphered rapidly. Long-period codes of the type discussed at the end of the previous section take a long time to encipher and decipher by hand and are vulnerable to human error. The only way forward along this route is to construct a machine to do the work for us.

Such a machine was invented by a German electrical engineer called Scherbius in 1918. Consider a simple substitution code in which A is encoded by S(A), B by S(B) and so on. It is not difficult to see that the same effect could be obtained by using a 'code wheel' or 'rotor' with 26 electrical contacts on one side of the wheel labelled A to Z and 26 electrical contacts on the other also labelled A to Z and with a wire connecting A on one side to S(A) on the other, B to S(B) and so on. If electric current enters by contact A on the first side, it leaves by contact S(A) on the other side; if it enters by contact B, it leaves by contact S(B) and so on. The code wheel has mechanised the substitution cipher S.

Now suppose the rotor rotates by one step each time we encipher a letter. The reader should convince herself that this device mechanises the code C′ = SR which was the hardest discussed in the previous section. As we saw there, the code C′ is fine for short messages but, because it has the short period 26, is vulnerable to frequency analysis for long messages. To increase the period the result of the first encoding is fed into a second code rotor *which rotates by one step once every 26 times we encipher a letter.*

Exercise 13.2.1 *Let* D *be the code which sends* A *to* B, B *to* C, ... , Z *to* A. *Let* S_1, S_2 *be two substitution codes. Show that the code defined by sending the* $(k+26l)$*th letter* α_{k+26l} *of our message to* $S_2D^{l-1}S_1D^{k-1}\alpha_{k+26l}$ *corresponds to one sent by the mechanism just proposed. Show, more generally, that the code defined by sending the* $(k + 26l + n)$*th letter* $\alpha_{k+26l+n}$ *of our message to* $S_2D^{l-1}S_1D^{k-1}\alpha_{k+26l}$ *corresponds to one sent by the mechanism just proposed started in an appropriate state.*

Barring unlikely coincidences each of the first 26 × 26 letters of our message will be encoded by a different substitution code corresponding to the 26 × 26 different arrangements of the rotors before repeating and the period of our code will be $26 \times 26 = 26^2 = 676$.

By feeding the result of the second coding into a third rotor *which rotates by one step once every* 26^2 *times we encipher a letter*, we obtain a code which will, in general, have period 26^3 and so on.

Exercise 13.2.2 *Describe the three-rotor code in the same way that we described the two-rotor code in Exercise 13.2.1.*

The three-rotor machine may be represented in diagrammatic form as shown in Figure 13.1. We refer to the machine a 'three-rotor Primitive Enigma' since modifications of this machine gave rise to the German Enigma machines which it was the task first of the Polish and then of the British code-breakers to crack.

My purpose in what follows is to explain roughly how the Enigma machines worked and why the apparently impossible task of breaking them was in fact possible. This will have several consequences.

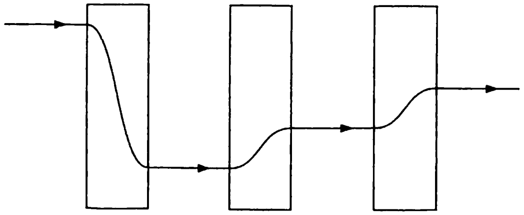


Figure 13.1: A three-rotor Primitive Enigma.

1 I shall not follow the exact path that the Poles and the British took.

2 There were several different versions of Enigma in use at various times with various branches of the German Armed Forces and they were used with various degrees of cryptographic competence. I shall concentrate on the German Naval Enigma, which was the best designed and most carefully used and, consequently, the hardest to break. British memoirs of the First World War had revealed the fact that German Naval codes had been comprehensively broken† and the German Navy was determined not to make the same mistake twice.

3 In the interests of clear exposition‡ I shall slur over or omit details both of the Enigma machine and the methods used for breaking it.

4 The omission of technical and historical detail will make things look a great deal simpler than they were. The reader who is tempted to exclaim when looking at actions of either side, 'Why, even I would have thought of that!' is almost certainly mistaken.

The reader who wishes to go further will find dozens of books and hundreds of articles on Enigma. The chief sources known to me are the accounts of Hinsley [95], Kozaczuk [132], Welchman [253] and those collected by Hinsley and Stripp in [109]. The best place to start reading is probably Kahn's *Seizing The Enigma* which also has an extensive bibliography. The journal *Cryptologia* acts in part as a newsletter for Enigma buffs.

For the rest of this section, we shall discuss the three-rotor Primitive Enigma, since many of the issues involved in dealing with the actual Enigma machines appear in this simpler context. However, the reader should keep in mind that, for reasons to be discussed later, the machine the Poles had to deal with was a much more formidable device.

At first sight, the Primitive Enigma appears totally impregnable. First, the enemy has to guess the exact nature of the coding device. (Even minor variations in design such as stepping the second rotor after 23 rather than 26 letters have been enciphered might well prove completely baffling. The pre-war British attack on Enigma was stymied by incorrect assumptions about the wiring of the typewriter keys to the first input plate.) Once he has done that, he must discover the wiring of the three rotors. When we deciphered the second Thurber passage in the previous section, we were in fact finding the wiring of the rotor in a one-rotor Primitive Enigma machine. If the reader reflects briefly, she will begin to see the magnitude of the task proposed.

†The ill effects of these revelations should be borne in mind when considering the long British silence after the Second World War. The most important British coup of the First World War was the decoding of the Zimmermann Telegram which finally brought the USA into the war.

‡And for the less easily admitted reason of sheer ignorance.

However, the German Navy expected to fight many battles and to lose some of them. Eventually, an Enigma machine and its rotors would be captured[†]. In previous wars the capture of a code book meant the cracking of the associated code, but now the loss of an Enigma machine still left the code heavily defended. When we encode using Enigma, we start off with the rotors in a certain position and the counting mechanism which turns the rotors in a certain state. There are $26^3 = 17\,576$ different starting positions for the rotors. In addition, although the enemy code-breakers know that the second rotor will move through one step after r_1, $r_1 + 26$, $r_1 + 52, \ldots$ steps of the first rotor, and that the third rotor will move through one step after r_2, $r_2 + 26$, $r_2 + 52, \ldots$ steps of the second rotor for some r_1, r_2 with $1 \leq r_1, r_2 \leq 26$, they do not know the values of r_1 and r_2 (the state of the counting mechanism). If the enemy wishes to decode an 800-letter message by working through all the possible initial positions of the rotors and all the possible values of r_1 and r_2, then they will need $26^5 = 11\,881\,376$ trial decodes, only one of which will, in general, be correct. A team of 300 cryptographers working three eight-hour shifts a day (with 100 cryptographers on each shift) and each working through each trial in half a minute would take well over a month to work through all these possibilities. It was this new level of security that made Enigma-type machines so attractive.

However, although our Primitive Enigma is indeed hard to break, it is not quite so hard to break as our vivid picture of hundreds of cryptographers working day and night would imply. Battalions of figures, like battalions of men, are not always as strong as they seem. It is not necessary to obtain a complete decode to find the position of the Enigma rotors. For reasons we shall now discuss, a very short snatch of ungarbled prose in the midst of an otherwise useless trial decode gives a sufficient clue to decoding the whole message. The Achilles heel of our Primitive Enigma which, fortunately for the Polish and British code crackers, it shared with the actual German Enigmas was the motion of the first 'fast rotor' relative to the remaining rotors. For 26 encipherments the inner rotors remained stationary while the fast rotor moved forward at a regular pace one step at a time, then the inner rotors changed to new positions and remained stationary whilst, once again, the fast rotor moved round its 26 positions. Thus, if the fragment

ERYUHUBRUNKXTANKERXNEZRTWTYFFFDMNBWUPOIJ

appeared in a trial decode, it would be well worth testing the hypothesis that our rotors were in the correct position during the decode XTANKERX,

[†] A great deal of thought has gone into the security of the electronic passwords used for automatic 'hole in the wall' banking. However, some criminals use bulldozers to steal the wall together with its automatic bank which they then break open at their leisure. Secure systems require protection against crude methods as well as subtle ones.

but that after XTANKERX, XTANKERXN or XTANKERXNE, either the second rotor of our putative encoder advanced and that of the real one did not, or vice-versa.

The discussion of the previous paragraph shows that our Primitive Enigma has a weakness, but anybody who has tried to read a book for misprints knows that human attention quickly flags and will find the thought of teams of clerks reading through thousands upon thousands of trial decodes in search of a short stretch of meaning fairly unrealistic. A more plausible approach is indicated by our solution of the second Thurber passage which we broke by guessing that it ended with the letters XTHURBER. Routine reports and routine orders tend to be very stereotyped. Welchman recalls that

> [w]e developed a very friendly feeling for a German officer who sat in the Quatra Depression in North Africa for quite a long time reporting every day with the utmost regularity that he had nothing to report. In cases like this, we would have liked to ask the British commanders to be sure to leave our helper alone.

A further aid was provided by the fact that German military men, like military men everywhere, tend to be very punctilious in giving full military titles[†]. Suppose we guess that a message enciphered on a known three-rotor Primitive Enigma has as its 10th to 16th letters GENERAL, and we know that the enciphered message has as its 10th to 16th letters SDFERTO. We now use six near copies of the Enigma machine E_1, E_2, $\ldots$, E_6, each with the same arrangement of rotors as the original but with a different stepping arrangement to be described later.

We start with the two inner rotors of the six mock Enigmas all in the same position. The outer 'fast rotor' of the first Enigma E_1 will be in some position which we call position 1. We set the outer rotor of E_2 one step further on in position 2, the outer rotor of E_3 one further step along in position 3 and so on. We now encipher G using E_1, E using E_2, N using E_3 and so on. If the positions of the rotors in E_1 coincide with those of the original Enigma when it enciphered the 10th letter G of the original message, then E_1 will produce the same encipherment S. Further, *if the inner rotors of the original Enigma did not change between the 10th and the 11th encipherment* then, since the outer rotor of the original Enigma moves forward one step, the position of the rotors in E_2 will coincide with those of the original Enigma when it enciphered the 11th letter E of the original message and so E_2 will produce the same encipherment D. Repeating the argument 4 more times, we see that if the positions of the rotors in E_1 coincide with those of the original Enigma when it enciphered the 10th letter and *if*

[†] As opposed to academics who like it to be known that they like to be known as Tom but who, in fact, like to be known as Dr Körner.

the inner rotors of the original Enigma did not change between the 10th and the 16th encipherment, the encipherment of GENERAL by our new arrangement will be SDFERTO, just as it was for the original.

The following objections may occur to the reader:

1 Our new arrangement might have enciphered GENERAL as SDFERTO by chance even if the rotor arrangement in the two machines did not coincide. It is, I suspect, quite hard to work out the exact probability of this happening, but the following argument gives a rough estimate. If we encipher a single letter (say G) at random, the chance that it will be enciphered as a particular letter (say S) is 26^{-1}. Thus if we encipher a sequence of 6 letters (say GENERAL) completely at random, the chance that they will be enciphered as a particular sequence (say SDFERTO) is 26^{-6}. If we repeat the experiment 26^3 times the chance that a particular encipherment (say SDFERTO) will come up, is about $26^3 \times 26^{-6} = 26^{-3}$ which is quite small. It is, of course, not true that our new arrangement works 'at random', but the argument makes it very plausible that the rate of 'false alarms' will not be very high. Since routine and speedy examination will reveal 'false alarms' for what they are, they will not, therefore, cause us any problems.

2 Even if we now know the positions of the rotors of the original Enigma at one point, we have little idea which of its 26^2 possible states the counting mechanism was in at this point. However, if we assume a particular state and decipher the message on that assumption, the first point where sense changes to nonsense will mark the point where either the second rotor of the actual Enigma stepped but the second rotor of the assumed Enigma did not or vice-versa. It is thus easy to synchronise the second rotors and, when needed, the third ones of the assumed Enigma with the real one.

3 Finally the reader will have noted that our method depended on the assumption that the inner rotors of the original Enigma did not change between the 10th and the 16th encipherment. One possible way of dealing with this would be to run the process another five times corresponding to the cases when the second rotor steps after the first, second, third, fourth or fifth enciphered letter, but this will take six times as long. Alternatively, we might note that the chance of an inner rotor change during the encipherment is only $5/26$ and if we are not very confident of our guess (that the 10th to 16th letters of the original message were GENERAL), we are better off using the time to test five other guesses.

Exercise 13.2.3 *Suppose we have six guesses, each of which has a chance p of being correct. There is a process A taking a time T which, if the guess chosen is correct, has a probability q of cracking the code but otherwise does nothing. There is another process B taking a time $6T$ which, if the guess chosen is correct, is certain to crack the code but otherwise does nothing. If we are given a time $6T$ to crack the code, show that we should apply process A with each of our six guesses rather than process B with one guess provided that*

$$q \geq q_0(p) \text{ where } q_0(p) = \frac{1-(1-p)^{1/6}}{p}.$$

Compute $q_0(p)$ when $p = 1/4$, when $p = 1/2$ and when $p = 3/4$.

There is another possibility when our guess is quite long. For example, suppose that our guess is 24 letters long. In that case we can split it into two guesses corresponding to the first 12 letters and the last 12 letters and be confident that the inner rotors will not move during the encipherment of at least one of them. It therefore makes sense to concentrate on methods which assume that the inner rotors do not move.

Like our proposed attack on a Primitive Enigma, the British attack on the German Naval Enigma required a mechanised 'brute-force' search through all $26^3 = 17\,576$ starting positions of the three rotors. The first such machines were built at the end of 1938 by the Poles (though they exploited a specific weakness in the German systems which was later removed) who called them *bomby* possibly because of the ice cream sundae (a *bomba*) the mathematicians ate when they discussed the project or possibly because of the regular ticking noise the *bomby* made in operation. Each British *bombe* consisted of the equivalent of 12 mock Enigmas, each of which could, apparently, be driven through the Enigma cycle of 17 576 starting positions in 15 minutes. However, for reasons which will become clear in the next chapter, even when things were going well, it was necessary to run through many Enigma cycles to find the daily German code-setting.

It was the 15-minute cycle time which made it feasible to break Enigma but it was also the 15-minute cycle time which meant that breaking Enigma was only just possible. At some times it took about 24 hours to decipher the day's transmissions for a particular Enigma system. If a change in German procedures required a ten-fold increase in Enigma cycles, then the machines could not be speeded up, since they were already running as fast as possible, nor could the number of machines assigned be increased without taking them from other decoding problems, and, unless the number of machines was increased, the best that might be hoped for was to decode every tenth day's output ten days late. Nor was this best outcome really to be hoped for, since intermittent decodes provide many fewer good initial guesses than can be obtained from a constant supply of decodes.

The great Atlantic convoy battles ran to many time-scales, from the month that it might take a slow convoy to complete its crossing, through to the minutes that a man might survive in the freezing sea. For those who tried to read the U-boat codes there were two time-scales. One was the day — information gained within 24 hours could steer convoys round the waiting submarine packs, information which took 72 hours to obtain usually came too late. The other was the cycle time of their bombes.

13.3 The plugboard

We have described how to encipher messages using our Primitive Enigma, but we have not said how the intended recipient should decipher the message so enciphered. If we describe the effect of the Primitive Enigma in a particular state s by T_s (so that A is enciphered by T_sA and so on), then we seek a deciphering method T_s^{-1} such that $T_s^{-1}(T_sA) = A$, $T_s^{-1}(T_sB) = B$ and so on. In principle this is an easy task. If X emerges from the third rotor, then, by reversing the path and finding which letter X' is enciphered by the third rotor as X, which letter X'' is enciphered by the second rotor as X', and finally which letter X''' is enciphered by the first rotor as X'', we obtain $T_s^{-1}(X) = X'''$.

If we look again at the diagrammatic version of the Primitive Enigma in Figure 13.2, we see that to decrypt a letter we 'simply reverse the arrows' (or the electric current). It is rather harder to construct a practical device to do what we have so easily described and even with such a device we must either use two machines or run the risk of errors like enciphering a message when the machine is in deciphering mode.

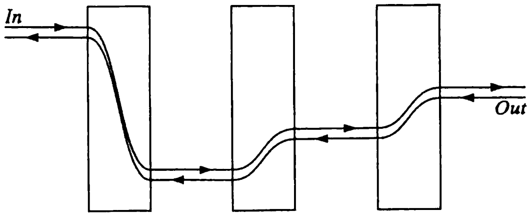


Figure 13.2: In and out of a three-rotor Primitive Enigma.

One of Scherbius's collaborators came up with an ingenious way round the problem. He added a fourth element called a reflector which took the output from the third rotor and fed it back by another path into the same third rotor, with the effect shown in Figure 13.3. If we write Ra for the encipherment of a particular letter a by the reflector acting alone and so on, we see that the effect of following the path given is to encipher a letter b, say, by $T_s^{-1}RT_sb$. Thus, if we write C_s for the effect of our new machine in state s, we obtain

$$C_s = T_s^{-1}RT_s.$$

The reflector did not move, so R did not depend on s.

Since the reflector consisted of 13 wires joining pairs of connectors, R is a simple substitution code with two special properties.

(1) If one wire connected, say, the letters e and q, then $Re = q$ and $Rq = e$. Mathematicians say that R is self-inverse and non-mathematicians that R both enciphers and deciphers. Both mean that, since

$$R(Re) = Rq = e,$$

applying R twice to any letter leaves it unchanged. Since it is natural for mathematicians to write $R(Re) = R^2e$ and to write the code which leaves everything unchanged as I (so that $Ie = e$), they would write

$$R^2e = Ie$$

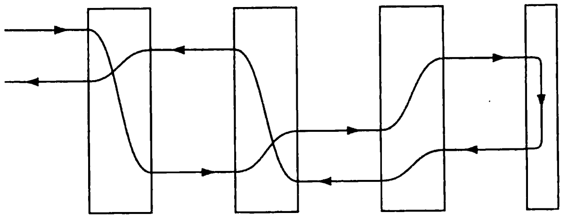
for every letter E, or still more briefly

$$R^2 = I.$$

(2) R cannot encrypt a letter as itself. (If the wire joined a connection to itself there would be a short circuit.)

It is easy to see by tracing paths through the machine in the manner of Figure 13.3 that the complete encipherment $C_s = T_s^{-1}RT_s$ must also have these properties. The reader may be interested to see this algebraically.

Figure 13.3: A Commercial three-rotor Enigma.



To prove that C_s is self-inverse, we note that

$$\begin{aligned} C_s^2 &= C_sC_s = (T_s^{-1}RT_s)(T_s^{-1}RT_s) \\ &= (T_s^{-1}R)(T_sT_s^{-1})(RT_s) = (T_s^{-1}R)I(RT_s) \\ &= (T_s^{-1}R)(RT_s) = T_s^{-1}R^2T_s \\ &= T_s^{-1}IT_s = T_s^{-1}T_s = I. \end{aligned}$$

To show that C_s cannot encrypt a letter as itself, suppose, for example, that $x = C_sx$. Applying the encryption T_s to both sides of our equation, we obtain

$$\begin{aligned} T_sx &= T_s(T_s^{-1}RT_sx) = (T_s(T_s^{-1})(RT_s)x) \\ &= I(RT_s)x = R(T_sx) \end{aligned}$$

so that R encrypts the letter T_sx as itself. Since this is impossible, it follows that our initial assumption that $x = C_sx$ is false.

The three-rotor Enigma with reflector that we have just described corresponds, apart from one further modification to be discussed later, to the Commercial Enigma which Scherbius sought, with limited success, to sell to various businesses. One of the British code-breakers recalls how, whilst the attack on Enigma was Britain's most important secret,

> [a] retired banker named Burberry, living in the [same Bletchley] hotel once ... startled me by describing the Enigma which he had used in his bank. I probably said "fascinating", and raised one eyebrow.

It now had the advantage that, because C_s was self-inverse, the same machine and the same settings could be used for encryption and decryption. The Commercial Enigma was clearly good enough to ensure complete security for normal business transactions, but it is worth asking whether the changes between the Primitive and the Commercial versions made Enigma more or less secure.

Once again we must distinguish between the problems faced by an enemy cryptographer trying to reconstruct the wiring of an unknown machine including the rotors from various clues (capturing the machine by cryptographic means) and those faced by the same enemy who knows the wiring of the machine and its rotors but is trying to find out how it has been set up on a particular day (recovering the daily key). It seems plausible that the extra complication of having to find the wiring of the reflector would make the job of anyone seeking to reconstruct the machine by cryptographic means that much harder, but that argument does not apply to someone who already knows the machine's structure (including the reflector wiring) and is now trying to find the daily key.

At first sight, it might be argued that the extra complexity of the new path through the three rotors, through the reflector and back out through the three rotors in reverse order, must make the task harder, but complexity of method need not produce complexity of outcome. Exactly the same brute-force method that we described at the end of the previous section will (provided, as before, we start with a correct guess of some part of the message) produce the day's setting with the same amount of work. Viewed in this way, the new Enigma is no harder to crack than the old. Viewed in another way, might it not be easier?

A good secret code should have the aspect of a glass wall — vertical, smooth and featureless, presenting no hand-holds for the code-breaker. (As we have seen, one of the attractions of Enigma-type codes is that they automatically flatten letter frequency.) The Commercial Enigma presents two hand-holds (in addition to the Achilles heel of the 'fast rotor' which it inherits from the earlier Primitive version), the first being the, otherwise desirable, property of being self-inverse and the second that it cannot encipher letters as themselves.

One of the Italian Navy systems used an ordinary Commercial Enigma. One day, Mavis Lever, one of the youngest cryptanalysts

> ... sensed something strange in an Italian intercept, realised after a moment that the message had not a single L in it, and knowing that the Enigma never replaced a plaintext letter, concluded that the message was a dummy whose plaintext consisted entirely of *l*'s.

Such windfalls (which might well enable one to capture the whole machine by cryptanalysis) are rare, but the non-self-encipherment property is helpful in any attack on the code by guessing part of an enciphered message (in the jargon of cryptanalysis a 'probable word' method). The problem facing cryptanalysts using this method is that they not only have to guess a part of a message, say warningxminesxatxsquare xsevenxsix† but they also have to guess *exactly* where the guessed part came in a longer message. If the longer message was encoded as, say,

WSDTCNNXCLKEUFWNPVYQJGIBFE...

then our guessed phrase could not start in the first place because w cannot encipher as W, nor in the third since the fourth letter of the guessed phrase is n which cannot encipher as N the seventh letter of the coded message.

Exercise 13.3.1 *Suppose that you have a guessed passage $\omega = w_1w_2\ldots w_n$ of length n. Show that the probability that a sequence $\Omega = W_1W_2\ldots W_n$ of n letters chosen at random does not coincide with α in any place (in other*

†There was 'a procedure known as "gardening", whereby the RAF laid mines in specified positions solely to generate warning messages. The positions were carefully chosen to avoid numbers, especially 0 and 5, for which the Germans used more than one spelling in their signals.'

words $\mathtt{w}_j \neq \mathtt{w}_j$ for each $1 \leq j \leq n$) is

$$f(n) = \left(\frac{25}{26}\right)^n = \left(1 - \frac{1}{26}\right)^n.$$

Compute $f(n)$ for $n = 6, 12, 18$. For what value of n do we have $f(n) \approx 0.1$, $f(n) \approx 0.01$, $f(n) \approx 0.001$? Explain why you would expect to locate the exact position of a phrase of 200 letters 'buried' in a coded message of 400 letters by inspection of matchings, but you would not expect to be able to perform the same trick with a phrase of 6 letters buried somewhere in a coded message of 12 letters.

There was, however, one further difference between the Primitive and the Commercial Enigmas which greatly strengthened its defences. The rotors were now made removable and interchangeable. Even if only three rotors were available, they could be arranged in any of $3 \times 2 \times 1 = 6$ ways so that even when opponents knew the wiring of each rotor and the reflector, they were, in effect, faced with 6 possible machines. If they then used brute-force search methods, these would take them 6 times as long (or require 6 times as many mock Enigmas) to cope with the machines. During the war, the German Army selected its daily set-up from 5 rotors giving $5 \times 4 \times 3 = 60$ possible machines and the German Navy from 8 rotors giving $8 \times 7 \times 6 = 336$ possible machines.

Exercise 13.3.2 *(i) If it takes a mock Enigma 15 minutes to work through all possible starting positions with a certain combination of rotors, how long will it take to run through 336 combinations? How many mock Enigmas will you require to run through all the combinations in a day?*

(ii) Let u_n be the number of possible three-rotor machines which can be made with n rotors. Find u_{n+1}/u_n and tabulate its value for $n = 3, 4, 5, 6, 7$. What happens to u_{n+1}/u_n as n increases? Explain why increasing the number of rotors from which the choice is made beyond a certain point not only makes the system unwieldy but fails to increase its security a great deal.

The armed forces of several countries adopted Enigma-type machines but most sought to make them more secure than the basic Commercial Enigma. The British Air Force adopted a machine whose name shifted from 'RAF Enigma' to 'Type X' and finally to 'Typex'. Internal memoranda stated frankly that 'The machine ... was copied from the German "ENIGMA" with additions and alterations suggested by the Government Code and Cipher School.' However, 'Difficulty arises in remunerating the patentees, in the near future at any rate,' and the matter of such payment was deferred 'until it is permissible for us to negotiate with them.' The British Army adopted the same system, but the Navy stuck with older and more established methods (see Figure 13.4). It appears that the designers of the Typex machine sought extra security by using many rotors in series (so we might talk of a ten-rotor Enigma) and a more complex stepping system.

How much does the addition of extra rotors add to the security of an Enigma machine? Clearly the answer may depend on the type of machine, so let us ask the question first about our original Primitive Enigma. If we use the method of attack described at the end of the last section, then finding the setting of an n-rotor Primitive Enigma will require a brute-force search through 26^n positions. This suggests that each extra rotor makes the task of our opponent 26 times more difficult.

On the other hand, if we look at our ten-rotor Primitive Enigma as it encodes a 200-letter message, we see the fast outer rotor taking a step with every letter, the more stately second rotor taking a step every 26th letter, and, if we are lucky, we may see the third rotor taking the step it takes every $26^2 = 676$th letter. The remaining rotors will, in all likelihood, imitate the House of Peers which

..., throughout the war
Did nothing in particular
And did it very well.

Unless we can explain exactly how the remote possibility that the higher

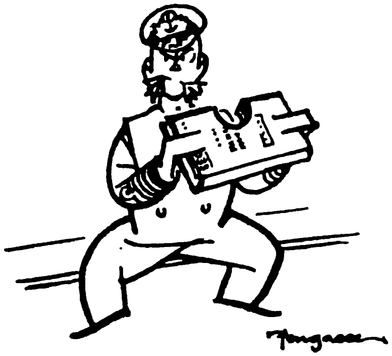


Figure 13.4: Preventing a code book from falling into enemy hands.

order rotors might rotate adds greatly to our security, it seems unwise to take the argument of the previous paragraph at its face value.

There is another problem connected with increasing the number of rotors. Increasing mechanical complexity means decreasing reliability and increasing size, and the new theories of *Blitzkrieg* called for a machine small enough and reliable enough to accompany a general's command car into battle. Some unknown but extremely clever German Army engineer came up with another solution: the 'plugboard' or 'steckel'. On entering and leaving the machine, the current passed through a plugboard which could be set up to interchange any chosen set of non-overlapping pairs of letters and leave the remaining letters unchanged (or 'self-steckered'). The set-up is shown in Figure 13.5.

If the three-rotor Commercial machine has the effect C_s in state s, then adding the plugboard is to produce a machine which has effect

$$\mathrm{E}_s = \mathrm{P}\mathrm{C}_s\mathrm{P}$$

where P is the effect of the plugboard alone. Since P interchanges certain pairs of letters and leaves the remaining letters unchanged, the effect of applying P twice is to leave everything unchanged. In other words, P is self-inverse.

$$\mathrm{P}^2 = \mathrm{I}.$$

It is now easy to check that E_s retains both the desirable property of being self-inverse and the undesirable property of not enciphering letters as themselves.

Exercise 13.3.3 *Prove this by arguments along the same lines as those at the beginning of this section in which we showed that* C_s *is self-inverse and does not encipher letters as themselves.*

The exciting thing about the plugboard is that it appears to rule out any brute-force attack on Enigma even if the enemy holds copies of our machine and its rotors and knows some of our messages, both in encrypted and unencrypted form. In the previous section we talked somewhat glibly about machines stepping through the $26^3 = 17\,576$ different rotor positions. The initial plugboard specification only called for six pairs of letters to be interchanged (leaving 14 self-steckered) but, even with this restriction, there are over 10^{11} different plugboard arrangements — and the plugboard can be changed whenever we wish.

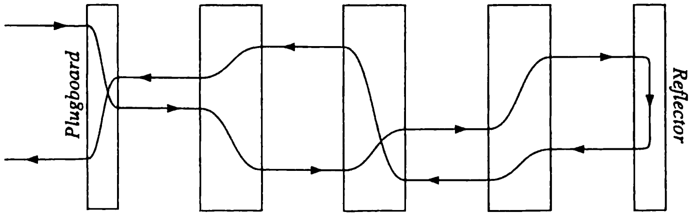


Figure 13.5: A three-rotor Enigma with plugboard.

Exercise 13.3.4 *Let* v_r *be the number of possible arrangements of the plugboard in which* $2r$ *letters are self-steckered* $[0 \leq r \leq 13]$. *Explain carefully why*

$$v_r = \frac{26!}{2^{13-r}(2r)!(13-r)!}.$$

Compute v_{r+1}/v_r. *For which values of* r *do we have* $v_{r+1}/v_r \geq 1$? *Show that* v_r *is largest when* $r = 2$. *Find* v_2 *and* v_3. *Verify the statement about* 10^{11} *plugboard arrangements made just before this exercise.*

Later, the number of self-steckered letters was reduced to 6. The exercise just done shows that this is close to optimal, giving about 1.5×10^{14} different plugboard arrangements from which to choose. There is no way we could conduct a brute-force search through this number of possibilities.

Numbers, by themselves, are no guarantee of cryptographic safety, and the German code experts identified one chink in Enigma's armour. Remember that a three-rotor Enigma, once set, runs through a cycle of $26^3 = 17\,576$ steps and then starts again. At each step it acts like a simple substitution cipher acting first, say, as E_1, then, after one step as E_2, after two steps as E_3 and so on. If, every time we use our Enigma, we start at the same point, then the first letter of each message will be enciphered using E_1, the second using E_2 and so on. If we treat the sequence of first letters as a message encoded using the substitution cipher E_1, the simple statistical techniques along the lines used in Section 13.1 (made easier by the fact that E_1 is self-inverse) will usually tell us what E_1 is. If we do the same for E_2 and so on then, just by knowing the E_j, we can now decipher the messages. The situation is, in fact, rather worse since it is quite plausible that possession of sufficiently many E_j will enable the wiring of the rotors to be discovered.

One of the British code-breakers recalls how, when dealing with one small German communication network,

> [we] were amazed to be presented with twenty or more messages sent on the same day *with the same [setting].* Presumably the operator had

> not read his manual. This extraordinary lapse enabled us to recover the complete details of an unknown Enigma, using no other data than that the messages were in German.

The Swiss, Spanish, and Italian governments not only used Commercial Enigmas, but enciphered all messages for a given day with the same setting. During the 1930s, the chief British code-breaker 'Dilly' Knox broke both the Spanish and the Italian systems 'by hand'. (The Poles had some trouble with the Swiss system until they realised that the Swiss used German, French and Italian for their messages. The Swiss were warned indirectly that their system was vulnerable.) Although the main Italian Naval codes, which were of the old-fashioned 'book' type, were seldom read, the Italian Navy also used Enigma-type machines for other purposes. Information from this 'secondary' source enabled the British to maintain control of much of the Mediterranean in the face of what could have been a formidable Italian challenge. It also enabled them to locate and sink many of the tankers carrying fuel for Rommel's forces in North Africa, severely limiting his mobility. A secondary but welcome effect of these actions was to help destroy the (already limited) German trust in the reliability of their Italian ally.

In order to avoid this problem we must make sure that different messages start at different stages of the Enigma cycle. Since the Enigma cycle has 26 × 26 × 26 steps, each step can be identified in a unique way by a sequence of three letters like ERT or FKA. We shall call this sequence the 'text setting'. By choosing text settings corresponding to widely spaced stages in the Enigma and using a different text setting each time, we can destroy any prospect of using the methods described in the previous two paragraphs. However, for the receivers (whether friends or foes) to decipher our transmitted message, they will need to know the text setting. How can we ensure that our friends know the text setting but our foes do not?

Consider the organisation of a wolf-pack attack on a convoy. We note the following points:

1 The U-boats need to communicate with each other as well as with High Command.

2 The order in which and the times at which the U-boats communicate cannot be fixed in advance.

3 An individual U-boat may not hear all the messages transmitted. (For example, it might be submerged at the time of a given transmission.) For these reasons the message *itself* must identify the text setting.

Similar considerations apply to the use of Enigma in *Blitzkrieg* operations. To get round the problem, the German Army decided on the following procedure:

1 The operator chose two three-letter sequences at random. The first (say, NDX) we shall call the 'indicator setting' and the second (say, CVE) would act as the text setting.

2 The operator transmitted the indicator setting (in our case NDX) as it stood.

3 Using the indicator setting as a temporary text setting, he encoded the six-letter sequence consisting of the actual text setting repeated twice (in our case, CVECVE) obtaining a new six-letter sequence (say, ERTFYU). He then transmitted the encoded sequence (in our case, ERTFYU).

4 He then used the text setting (in our case, CVE) to encode the rest of the message and transmitted it.

The recipient then looked at the first nine transmitted letters (in our case, NDXERTFYU). Using the first three letters (in our case, NDX) as a text setting, he decoded the next six letters (in our case, ERTFYU) obtaining a repeated three-letter sequence (in our case, CVECVE). He then used the three-letter sequence (in our case, CVE) as a new text setting and decoded the rest of the message using it.

The repetition of the text sequence guarded against errors in the initial encipherment and transmission. The German Navy used a different procedure.

Exercise 13.3.5 *What weaknesses, if any, can you find in the Army system? If you can find any, how would you exploit them? (An unexploitable weakness is not a weakness.)*

CHAPTER 14

The Poles

14.1 The plugboard does not hide all finger-prints

As an inveterate browser, even in airport and railway bookstalls, I frequently come across books with titles like *Ten Spies Who Changed The World*, but closer inspection reveals that the only common characteristic of the spies described is that their actions failed to change anything. It is, however, just possible that the disaffected employee of the German Cryptographic Agency who sold documents concerning Enigma to the French from the early 1930s onwards did indeed change the course of history. The documents gave the general structure of the Military Enigma, including the existence of the plugboard. They also gave the keys including the plugboard settings for certain periods (in effect, allowing a code-breaker to reduce the Military Enigma to a Commercial Enigma for those periods). What they did not give was the internal wiring of the Enigma and its rotors.

Unable to make much of this material, the French offered it to their British and Polish allies. The British, who did not yet see Germany as a major threat, seem to have given it a fairly cursory inspection before deciding that they too could make nothing of it. The Poles gave the material to one of their new 'mathematical' code-breakers named Rejewski who did what the French and British experts had considered impossible and recovered the complete wiring of the Enigma and its rotors: 'a stunning achievement [and] one that elevates him to the pantheon of the greatest cryptanalysts of all time.' However, this removed only the outer defences of the plugboard Enigma, leaving the inner citadel of the daily settings untouched. In this section we discuss the elementary mathematical idea which gave Rejewski his first handhold on the plugboard Enigma, and in the next section I shall show how Rejewski and his colleagues captured the daily settings. Since we shall be discussing points that escaped the experts of the German Army,

the reader must expect to use paper, pencil and hard thought to follow the arguments of the next few sections.

Rejewski's first insight was that the plugboard, complicated though it is, does not hide the inner Commercial Enigma entirely from view. To see why this might be so, let us consider a much simpler situation. Let S and T be substitution codes and T^{-1} the substitution code which recovers the message π from the encoded message $T\pi$. Thus, in the notation introduced in the previous section, $T^{-1}T = I$. We consider the new substitution code $D = TST^{-1}$.

Exercise 14.1.1 *(i) Explain why* $TT^{-1} = I$.
(ii) Explain why D *defined above is a substitution code.*
(iii) If T *is self-inverse show that* $D = TST$.

Can we tell anything about S by examining D? To mathematicians a substitution code is a special case of what they call a 'permutation'. The study of permutations goes back to the investigations into the solubility of quintic and other polynomial equations by radicals (now called Galois theory) and is the subject of group theory. The most obvious way of writing a substitution code S is in the form of a table.

ABCDEFGHIJKLMNOPQRSTUVWXYZ
UGCJWNKSLQFTOZPVDBYREXHMAI

Group theorists have another way of writing permutations. Observe that S takes A to U, U to E, E to W, W to H, H to S, S to Y and Y back to A. We thus have a cycle (AUEWHSY). In the same way, starting at B we obtain the cycle (BGKFNZILRTR). Starting at C we return immediately to C giving the cycle (C) and starting at D we obtain the cycle (DJQ). The letters E, F, G, H, I, J, K, L, M and N occur in cycles we have already found, but O does not. Starting at O we obtain the cycle (OPVXM) and this exhausts the letters of the alphabet. We write S in *cycle form* as

(AUEWHSY)(BGKFNZILTR)(C)(DJQ)(OPVXM).

Notice that we can interchange the order of the cycles without changing the code, so that, for example

(AUEWHSY)(BGKFNZILTR)(C)(DJQ)(OPVXM)
= (DJQ)(OPVXM)(BGKFNZILTR)(AUEWHSY)(C)

and that we can rotate each individual cycle round, so that, for example

(OPVXM) = (PVXMO) = (VXMOP) = (XMOPV) = (MOPVX).

We say that a cycle containing n letters is a cycle of length n so that, for example, (AUEWHSY) is a cycle of length 7.

Exercise 14.1.2 *(i) Express in cycle form the substitution code which has the table*

ABCDEFGHIJKLMNOPQRSTUVWXYZ
XCDEBHGFPQVTYSZRWJKLMUOANI

(ii) Find the table for the substitution code which has the cycle form

(AFYZ)(BLCQHI)(D)(ER)(G)(JK)(MOVXW)(NTS).

Now suppose that S is given the table

Original letter	A B C D E F G H I J K L M ...
Substituted letter	A′B′C′D′E′F′G′H′I′J′K′L′M′...

and we wish to find a table for $D = TST^{-1}$. The easiest way to go about this is not to ask for the effect of D on A, B, ... but to ask for the effect of D on TA, TB, ... (which is just a rearrangement of the alphabet A, B, ... We observe that

$$\begin{aligned} D(TA) &= TST^{-1}(TA) \\ &= TS(T^{-1}TA) \\ &= TSA = TA', \end{aligned}$$

and, similarly $D(TB) = TB'$ and so on, giving a table for $D = TST^{-1}$ in the following form.

Original letter	TA TB TC TD TE TF TG TH TI TJ TK TL TM ...
Substituted letter	TA′TB′TC′TD′TE′TF′TG′TH′TI′TJ′TK′TL′TM′...

Looking at the tables for S and $D = TST^{-1}$ in the form we have given them it certainly looks as though some of the pattern of S has survived into TST^{-1} but, at first sight, it is not clear quite what it is.

To find out what is happening let us consider the particular example we started with of the substitution code S given by the table (which we have had to split in two)

ABCDEFGHIJKLMNOPQRSTUVWXYZ
UGCJWNKSLQFTOZPVDBYREXHMAI

so that $D = TST^{-1}$ has the table

T(A)	T(B)	T(C)	T(D)	T(E)	T(F)	T(G)	T(H)	T(I)	T(J)	T(K)	T(L)	T(M)
T(U)	T(G)	T(C)	T(J)	T(W)	T(N)	T(K)	T(S)	T(L)	T(Q)	T(F)	T(T)	T(O)

T(N)	T(O)	T(P)	T(Q)	T(R)	T(S)	T(T)	T(U)	T(V)	T(W)	T(X)	T(Y)	T(Z)
T(Z)	T(P)	T(V)	T(D)	T(B)	T(Y)	T(R)	T(E)	T(X)	T(H)	T(M)	T(A)	T(I)

Let us try to work out a cycle form for D. We start by considering the effect of D on T(A). We see that D takes T(A) to T(U), T(U) to T(E), T(E) to T(W), T(W) to T(H), T(H) to T(S), T(S) to T(Y) and T(Y) back to T(A). We thus have a cycle (T(A)T(U)T(E)T(W)T(H)T(S)T(Y)). In the same way, starting at B, we obtain the cycle (T(B)T(G)T(K)T(F)T(N)T(Z)T(I)T(L)T(T)T(R)), and so on. Thus the cycle form for $D = TST^{-1}$ is

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

Recalling that S has the cycle form

(AUEWHSY)(BGKFNZILTR)(C)(DJQ)(OPVXM),

we see that the cycle forms of S and of TST^{-1} look the same.

Exercise 14.1.3 *If a substitution code* S′ *has cycle form*

(AFYZ)(BLCQHI)(D)(ER)(G)(JK)(MOVXW)(NTS)

write down, without calculation, the cycle form of $TS'T^{-1}$ *and then check your answer.*

What precisely do we mean by saying that the cycle forms of S and of TST^{-1} look the same? After a little thought, we see that it means that the two codes have the same number of cycles of each length. In the case given, S has one cycle of length 1, one cycle of length 3, one cycle of length 5, one cycle of length 7 and one cycle of length 10, and so does TST^{-1}. In Exercise 14.1.3, S′ has two cycles of length 1, two cycles of length 2, one cycle of length 3, one cycle of length 4, one cycle of length 5 and one cycle of length 6, and so does $TS'T^{-1}$. Group theorists call the list giving the number of cycles of each length the 'cycle type'. We thus have a theorem:

Theorem 14.1.4 *If* S *and* T *are two substitution codes then* S *and* TST^{-1} *have the same cycle type.*

In first year university algebra, the theorem is stated as 'cycle type is invariant under conjugation'. Few undergraduates would name this as the dullest theorem of the year, but most would consider it a contender. For the mathematicians who struggled with Enigma, it represented the first hint that the plugboard might not be as strong as it seemed.

Exercise 14.1.5 *(i) Describe how you can recognise a self-inverse substitution code by its cycle type. (If you are stuck, write down the table of some self-inverse substitution code and find its cycle form.) Show that a self-inverse substitution code must have one of 14 different cycle types.*

(ii) Using the fact that cycle type is preserved, show that if S *is a self-inverse substitution code, then so is* $\mathtt{TST}^{-1}$.

(iii) Describe how you can recognise a substitution code which does not encipher letters as themselves by its cycle type.

(iv) Using the fact that cycle type is preserved, show that if S *is a substitution code which does not encipher letters as themselves, then so is* $\mathtt{TST}^{-1}$.

(v) Show that every self-inverse substitution code which does not encipher letters as themselves has the same cycle type and that every code with that cycle type is self-inverse and does not encipher letters as themselves. Show that there are

$$\frac{26!}{2^{13}13!} \approx 7.9 \times 10^{12}$$

such codes.

Let us see how Theorem 14.1.4 might be used. Suppose that we know that S and T are substitution codes and that we know that $\mathtt{D} = \mathtt{TST}^{-1}$ enciphers GENERAL as LBXBYGA. Then we know that D takes G to L, L to A and A back to G. Thus $\mathtt{D} = \mathtt{TST}^{-1}$ has a cycle of length 3 and so S must have a cycle of length 3.

Exercise 14.1.6 *Find the possible cycle types of the 26 Caesar codes and show that the code* S *just discussed cannot be a Caesar code.*

Of course, we have dealt only with a single unchanging substitution code and the Commercial Enigma changes with each step. (Another depressing thought is that even if we could halt the Enigma mechanism so that it remained the same for each step we would learn nothing by studying its cycles since, by Exercise 14.1.5(v), every self-inverse substitution code which does not encipher letters as themselves has the same cycle type.) However, a theorem like Theorem 14.1.4 should not be treated as an isolated fact but as a signpost indicating a possible direction in which to proceed. I shall not discuss how Rejewski used this signpost in reconstructing the Enigma wiring but in the next section I shall show how using the nine-letter initial signal for the German Army's Enigma messages (the NDXERTFYU discussed at the end of the previous section), the Poles were able to reconstruct the daily setting of Enigma.

The reader who wishes to find out how the Enigma wiring was reconstructed will find Rejewski's own account in Appendix E of [132].. (An interesting point is that the interchanging of rotors which makes the solution of the daily keys harder, makes finding the wiring of the rotors easier since each rotor will, eventually, turn up as the outermost 'fast' rotor.) There is an instructive discussion of how to find rotor wirings for Primitive Enigmas in Kronheim's 1981 book [127]. It is a sign of the times that this last reference is, in effect, a textbook for those interested in using cryptography to maintain the security of computer systems.

14.2 Beautiful Polish females

As might be expected, the Third Reich devoted massive resources to intelligence and code-breaking. The Germans started with a core of able cryptanalysts, some with mathematical training. But, as Kahn remarks: 'though the cryptological agencies ... grew in size they did not necessarily grow in effectiveness.' There were some substantial successes, such as the joint Italian–German effort which enabled them to read the reports on the British forces in North Africa sent by the American Military Attaché, and major coups against the convoy codes used by the British. However, these successes were achieved against traditional codes and not against Enigma-type machines. Whereas the Poles and, later, the British recruited from young graduates, particularly in mathematics, the Germans used older, called-up reserve officers with a knowledge of foreign languages. The General Staff also tried recruiting archaeologists specialising in unknown ancient writing systems but the results were disappointing. The same went for mathematicians. Kozaczuk quotes the head of German Naval Intelligence to the effect that

> [a]s far as mathematical training goes, pure mathematicians were not well suited to the [job], since they tended to get lost in theoretical abstractions. Their speculative investigations would strike against an inpenetrable barrier when it was necessary to go beyond formulas to solve a problem that was insoluble from the standpoint of pure mathematics.

The Poles and the British were lucky to find pure mathematicians with the ability to 'go beyond formulas'.

As we have seen, a Military Enigma consists of a Commercial Enigma which acts as a substitution code $\mathtt{E}_1$ for the first encipherment, a substitution code $\mathtt{E}_2$ for the second encipherment and so on, together with a plugboard associated with a self-inverse substitution code P. The full machine acts as a substitution code

$$\mathtt{C}_r = \mathtt{PE}_r\mathtt{P}$$

for the rth encipherment. In addition, we know that C_r is self-inverse and cannot encipher a letter as itself (we shall call such codes non-self-enciphering).

We saw in Section 13.3 that once the plugboard, the arrangement of rotors and counting mechanism had been set up according to the daily setting, the operator chose two three-letter combinations at random: the first the 'indicator setting' and the second the 'text setting'. He transmitted the indicator setting as it stood and then, using the indicator setting as a temporary text setting, he encoded the six-letter sequence consisting of the actual text setting repeated twice, obtaining a new six-letter sequence, and then transmitted the encoded sequence.

During the transmission of these six letters, the Commercial Enigma goes through six steps E_1, E_2, ... , E_6. In the argument that follows, we shall suppose that these are randomly and independently chosen self-inverse, non-self-enciphering substitution codes. As pure mathematicians, we know that this is not strictly true — the Enigma does not toss coins to establish how to move from E_1 to E_2 but moves in a mechanical and predictable manner from one state to the next. (Indeed, our ultimate purpose is to uncover the exact law governing the movement of Enigma.) On the other hand, a great deal of care has been lavished on Enigma to make it look random and there is no reason why we should not make use of this work, particularly when it is 'necessary to go beyond formulas to solve a problem that' appears 'insoluble from the standpoint of pure mathematics.'

The Poles noticed that among the initial nine-letter messages like FDW KRM GSA, RCX LAY JRC there were a certain number in which the 4th and 7th letters were the same, as in FMW THS TVU. When the 4th and 7th, 5th and 8th or 6th and 9th letters were repeated, they called them 'females'. How common are females? Let us start by looking at the 4th and 7th letters. In each case the same (unknown) letter is being enciphered first by $C_1 = PE_1P$ and then by $C_4 = PE_4P$. For the reasons given in the previous paragraph we may suppose C_1 and C_4 to be random and independent (self-inverse, non-self-enciphering) substitution ciphers. To fix ideas, suppose the unknown letter is A and $C_1A = B$. Then the 4th and 7th letters are females only if $C_4A = B$ also. But a random self-inverse, non-self-enciphering substitution code is equally likely to take A to any of the 25 remaining letters, so $\Pr(C_4A = B) = 1/25$. Since our choice of particular letters A and B is irrelevant to the computation,

$$\Pr(\text{the 4th and 7th letters are females}) = \frac{1}{25}.$$

Similarly

$$\Pr(\text{the } (3+i)\text{th and } (6+i)\text{th letters are females}) = \frac{1}{25}$$

for $i = 1, 2, 3$, and so

$$\begin{aligned}
&\Pr(\text{the message contains females})\\
&\quad = 1 - \Pr(\text{the message contains no females})\\
&\quad = 1 - \prod_{i=1}^{3} \Pr(\text{the } (3+i)\text{th and } (6+i)\text{th letters are not females})\\
&\quad = 1 - \left(1 - \frac{1}{25}\right)^3 \approx 0.115.
\end{aligned}$$

Thus, if 100 messages are sent each day, we may expect on average between 11 and 12 females (with, of course, more on some days and fewer on others).

The Poles realised that, although the plugboard P affects whether a female appears when one is possible for the Commercial Enigma, *the plugboard cannot make a female exist when no female is possible for the Commercial Enigma.* The plugboard does not hide all finger prints. Let us say that two substitution codes S_1 and S_2 'permit females' if there exists a letter x, say, such that $S_1x = S_2x$.

Theorem 14.2.1 *Let S_1, S_2 and T be substitution codes. Then TS_1T^{-1} and TS_2T^{-1} permit females if, and only if, S_1 and S_2 do.*

Proof If $S_1x = S_2x$, then

$$TS_1T^{-1}(Tx) = TS_1x = TS_2x = TS_2T^{-1}(Tx).$$

Thus, if S_1 and S_2 permit females, so do TS_1T^{-1} and TS_2T^{-1}.

On the other hand, if $TS_1T^{-1}x = TS_2T^{-1}x$, then

$$S_1(T^{-1}x) = T^{-1}(TS_1T^{-1}x) = T^{-1}(TS_2T^{-1}x) = S_2(T^{-1}x).$$

Thus, if TS_1T^{-1} and TS_2T^{-1} permit females, so do S_1 and S_2. ■

It follows, in particular, that $C_{i+3} = PE_{i+3}P$ and $C_{i+6} = PE_{i+6}P$ permit females if, and only if, E_{i+3} and E_{i+6} do. Thus if we observe females in the $(i+3)$th and $(i+6)$th place, we know (by direct observation) that C_{i+3} and C_{i+6} permit females and (by deduction) so must E_{i+3} and E_{i+6}. What proportion of possible daily settings are excluded by the existence of one pair of females? A good estimate would be $1 - \alpha$, where α is the probability that two randomly chosen self-inverse, non-self-enciphering, substitution codes E and E' permit females. It is not obvious how to compute α, but it is not hard to show that $\alpha \leq 13/25$, and this will be our next task.

Lemma 14.2.2 *Two self-inverse, non-self-enciphering, substitution codes* $\mathtt{E}$ *and* $\mathtt{E}'$ *permit females if, and only if, when written in cycle form they contain (at least) one cycle of length 2 in common.*

Proof Suppose that $\mathtt{E}$ and $\mathtt{E}'$ permit females. Then there is a letter $\mathtt{X}$ say, such that $\mathtt{EX} = \mathtt{E}'\mathtt{X} = \mathtt{X}'$ say. The cycle $(\mathtt{XX}')$ thus occurs in the cycle expansion of both $\mathtt{E}$ and $\mathtt{E}'$.

Conversely suppose that the cycle $(\mathtt{XX}')$ thus occurs in the cycle expansion of both $\mathtt{E}$ and $\mathtt{E}'$. Then, trivially, $\mathtt{EX} = \mathtt{X}' = \mathtt{E}'\mathtt{X}$ and $\mathtt{E}$ and $\mathtt{E}'$ permit females. ■

Lemma 14.2.3 *The probability* α *that two randomly chosen self-inverse, non-self-enciphering, substitution codes* $\mathtt{E}$ *and* $\mathtt{E}'$ *permit females satisfies the inequality* $\alpha \leq 13/25$.

Proof Write $\mathtt{E}$ in cycle form as

$$(\mathtt{X}_1\mathtt{X}_2)(\mathtt{X}_3\mathtt{X}_4)\dots(\mathtt{X}_{25}\mathtt{X}_{26}).$$

By the previous lemma $\mathtt{E}$ and $\mathtt{E}'$ permit females if, and only if, $\mathtt{E}'\mathtt{X}_{2i-1} = \mathtt{X}_{2i}$ for some $1 \leq i \leq 13$. Thus

$$\begin{aligned}\Pr(\mathtt{E}\text{ and }\mathtt{E}'\text{ permit females}) &= \Pr(\mathtt{E}'\mathtt{X}_{2i-1} = \mathtt{X}_{2i}\text{ for some }1 \leq i \leq 13)\\ &= \Pr\left(\bigcup_{1=1}^{13}\{\mathtt{E}'\mathtt{X}_{2i-1} = \mathtt{X}_{2i}\}\right)\\ &\leq \sum_{1=1}^{13}\Pr(\mathtt{E}'\mathtt{X}_{2i-1} = \mathtt{X}_{2i})\\ &= 13\Pr(\mathtt{E}'\mathtt{X}_1 = \mathtt{X}_2) = 13/25,\end{aligned}$$

as claimed. ■

Thus α is less than about 1/2. We shall use this estimate in what follows but Exercise 14.2.4 at the end of the section shows that α can be computed exactly. If the reader uses the formula there, she will find that α is, in fact, quite close to 0.4 and so the method works rather better than our cruder estimates would suggest.

Remark The reader who has not been bludgeoned into acquiescence by the references to Group Theory, Probability and other Mysterious Capitalised Mathematical Theories may object that the probabilistic estimates of this section are unnecessary. If we want to know the

average number of females among the initial nine-letter messages, all we have to do is take a month's worth of such messages and count them. In the same way we could obtain a good estimate of α by setting up a mock Enigma at random 1000 times and examining the substitution codes at the first and fourth encipherings. To this objection I would reply that the Polish mathematicians could make the probabilistic estimates much more quickly than they could gather the suggested statistics and then, having seen that these estimates were favourable, could then check them in the practical manner suggested. Before embarking on a project which will absorb most of our available resources (and, in particular, exclude other desirable projects) it is desirable to have both theoretical and experimental backing for it.

Do the females give us enough information to find the daily setting? Let us consider the simplest case in which the rotors of the Commercial Enigma and their order are known. There are then $26^3 = 17\,576$ possible daily settings. Each observed female allows about half of the possible daily settings. If we assume sufficient randomness, then the probability that a certain setting is permitted by n observed females should be about $(\frac{1}{2})^n$. Thus 10 females should reduce the number of possible settings by a factor of about $(\frac{1}{2})^{10} \approx 1/1000$ leaving about 17 possible settings. Of course, this probabilistic argument cannot be pushed too far since it appears to show that 15 females would reduce the possible settings to below 1. What it means, in practice, is that with more than 18 females we might expect only one possible consistent daily setting. Using this knowledge and our stock of initial messages (all of which consist of an unknown three-letter word enciphered *twice*), it should be easy to recover the plugboard $\mathtt{P}$. If we have fewer females or are otherwise unlucky, we will obtain several possible daily settings and we will have to go through the procedure of trying to find $\mathtt{P}$ for each of them. In all but one case we will uncover an inconsistency or, if we do not, any attempt to read the main messages will produce rubbish. This procedure, which would take too long applied to all 26^3 daily settings, becomes perfectly feasible when we have reduced the problem to 20 or even 60 possibilities.

How might we proceed in practice? Suppose that we have the initial signal KNRTYSFYD or, in a clearer form, KNR TYS FYD. We note that there is a female in the second place of TYS and FYD, so we go to a room marked 2. In Room 2 (just as in Rooms 1 and 3) there are 26 bookshelves marked with the 26 letters of the alphabet. We go to the bookshelf marked K, corresponding to the first letter of the message. On this bookshelf (as on all the other bookshelves) there are 26 boxes marked with the 26 letters of the alphabet. We take down the box marked N, corresponding to the second letter of the message. In this box (as in all the other boxes) there are 26 perforated cards. We extract the card marked R corresponding to the third letter of the message. The card has a pattern of 26×26^2 squares on it, each square corresponding to one of 26^3 possible daily settings. The pattern is the same on all the cards, but our card (corresponding to the 'indicator setting' KNR with females in the 3+2=5th and 6+2=8th place) has holes punched in all those squares for which the daily setting permits females in the 3+2=5th and 6+2=8th place when the indicator setting KNR is used. When we have collected several such cards corresponding to different initial signals containing females, we place them in a pile so that the squares corresponding to the same daily settings are aligned and shine a light beneath the pile. Only those squares which let the light through will correspond to possible daily settings. (Welchman suggests that this accounts for the word 'female' by analogy between a punched hole, through which a light can shine, and a female socket into which a plug can be inserted to make an electrical connection.) By using a little extra ingenuity (see [253]) and slightly more complicated cards it is possible to reduce the number of cards needed from 26^3 to 26. The resulting cards were known as Zygalski sheets after their inventor.

Exercise 14.2.4 *This exercise is devoted to showing how α could be found. Since the journey is more interesting than the goal, we take the long way round. You will need enough knowledge of probability theory to interpret* $\Pr(A \cap B)$ *(the probability of events A and B both occurring) and similar expressions. We approach the matter via another problem.*

The wrong envelope problem considers a mathematician who has written letters to n different people and prepared n correctly addressed envelopes to them. Overcome by the effort involved, the mathematician now places the letters in the envelopes at random (but exactly one letter in each envelope). What is the probability that all the letters are now in the wrong envelopes? The reader should first attack this problem for herself and then start the problem sequence below.

(i) Let A and B be finite sets. We write $|A|$ for the number of elements of A and so on. Explain why

$$|A \cup B| = |A| + |B| - |A \cap B|$$

(In a particular instance, the number of people who speak at least one of the languages French and German equals the number of French speakers plus the number of German speakers minus the number of people who speak both languages.)

(ii) Show that if A, B and C are finite sets

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |B \cap C| - |C \cap A| + |A \cap B \cap C|.$$

(iii) State and prove the corresponding result for four sets.

(iv) Satisfy yourself that you understand the following formula for n finite sets $A_1, A_2, \dots, A_n$,

$$\left|\bigcup_{1\le i\le n} A_i\right| = \sum_{i=1}^{n} |A_i| - \sum_{1\le i<j\le n} |A_i \cap A_j| + \sum_{1\le i<j<k\le n} |A_i \cap A_j \cap A_k| - \cdots.$$

(The notation is ghastly, but can you think of anything better?)

(v) Show that if A, B and C are events

$$\begin{aligned}\Pr(A \cup B \cup C) &= \Pr(A) + \Pr(B) + \Pr(C)\\ &\quad - \Pr(A \cap B) - \Pr(B \cap C) - \Pr(C \cap A) + \Pr(A \cap B \cap C).\end{aligned}$$

(vi) Satisfy yourself that you understand the following formula for n events $A_1, A_2, \dots, A_n$,

$$\begin{aligned}\Pr\left(\bigcup_{1\le i\le n} A_i\right) &= \sum_{1\le i\le n} \Pr(A_i) - \sum_{1\le i<j\le n} \Pr(A_i \cap A_j)\\ &\quad + \sum_{1\le i<j<k\le n} \Pr(A_i \cap A_j \cap A_k) - \cdots.\end{aligned}$$

(The results of parts (iv) and (vi) are known as 'inclusion–exclusion formulae'.)

(vii) Now let us look at the wrong envelope problem. If we take A_i to be the event that the ith letter finds itself in the right envelope, explain why

$$\Pr(\textit{some letter in right envelope}) = \Pr\left(\bigcup_{1\le i\le n} A_i\right)$$

and so

$$\Pr(\textit{no letter in right envelope}) = 1 - \Pr\left(\bigcup_{1\le i\le n} A_i\right).$$

Substitute in this last equation using the formula of part (vi).

(viii) Explain why if i, j, k, … are distinct

$$\begin{aligned}\Pr(A_i) &= \Pr(A_1) = \frac{1}{n}\\ \Pr(A_i \cap A_j) &= \Pr(A_1 \cap A_2) = \frac{1}{n(n-1)}\\ \Pr(A_i \cap A_j \cap A_k) &= \Pr(A_1 \cap A_2 \cap A_3) = \frac{1}{n(n-1)(n-2)}\end{aligned}$$

and state the general formula.

If $N(1)$ *is the number of integers* i *with* $1 \le i \le n$,
$N(2)$ *is the number of pairs* (i,j) *with* $1 \le i < j \le n$,
$N(3)$ *is the number of triples* (i,j,k) *with* $1 \le i < j < k \le n$,

and so on, show that

$$N(1) = \frac{n}{1!}$$
$$N(2) = \frac{n(n-1)}{2!}$$
$$N(3) = \frac{n(n-1)(n-2)}{3!}$$

and state the general result.

Hence show that

$$\begin{aligned}\Pr(\textit{no letter in right envelope}) &= 1 - N(1)\Pr(A_1) + N(2)\Pr(A_1 \cap A_2)\\ &\quad - N(3)\Pr(A_1 \cap A_2 \cap A_3) + \cdots\\ &= 1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \cdots + (-1)^n\frac{1}{n!}.\end{aligned}$$

(ix) Let p_n *be the probability that every letter is in the wrong envelope when there are n envelopes. Use the formula at the end of part (viii) to compute* $p_1, p_2, p_3, \ldots, p_{10}$. *Can you see a quick way of explaining why* p_1 *and* p_2 *have the values you have calculated?*

(x) Many readers will know that, in fact,

$$1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \cdots + (-1)^n\frac{1}{n!} \approx e^{-1} \approx 0.36788$$

for large n. This part of the question is devoted to the problem of finding rapid estimates for sums of the form

$$s_n = u_0 - u_1 + u_2 - \cdots + (-1)^n u_n$$

where the u_j *form a sequence of decreasing positive real numbers (in other words* $u_j \ge u_{j+1} \ge 0$ *for all j).*

Show that

$$s_{2m} \ge s_{2m+2},\ s_{2m+3} \ge s_{2m+1} \text{ and } s_{2m} \ge s_{2m+1},$$

for any $m \ge 0$. *Deduce that*

$$s_0 \ge s_2 \ge s_4 \ge \ldots s_{2M} \ge s_{2M+1} \ge s_{2M-1} \ge s_{2M-3} \cdots \ge s_3 \ge s_1$$

and so, if $n \ge 2p$, *then*

$$s_{2p} \ge s_n \ge s_{2p+1}.$$

Conclude that

$$0 \le s_{2p} - s_n \le s_{2p} - s_{2p+1} = u_{2p+1}.$$

Show similarly that, if $n \ge 2p+1$, *then*

$$0 \le s_n - s_{2p+1} \le s_{2p+2} - s_{2p+1} = u_{2p+2}.$$

Combining these two results, show that, if $0 \le m \le n-1$, *then*

$$|s_n - s_m| \le u_{m+1}.$$

This is sometimes stated as 'the error is less than the first term neglected'. Look at the values of p_j *that you calculated at the end of part (ix) in the light of this result.*

(xi) Now suppose that we have n pairs of cards each pair having the same label but the labels of each pair being different. (Thus we might have two aces, two kings, and so on.) We shuffle the pack and lay out the 2n cards in n pairs. What is the probability q_n *that no pair consists of cards with the same label? Explain why the problem differs from the wrong envelope problem.*

Use the same ideas as we used to solve the wrong envelope problem to show that

$$\begin{aligned}q_n =& 1 - \binom{n}{1}\frac{1}{2n-1} + \binom{n}{2}\frac{1}{(2n-1)(2n-3)} - \cdots\\ &+ (-1)^r\binom{n}{r}\frac{1}{(2n-1)(2n-3)\ldots(2n-r)} + \ldots\\ &+ (-1)^n\frac{1}{(2n-1)(2n-3)\ldots 1}.\end{aligned}$$

Explain why $\alpha = q_{13}$. *Use the ideas of part (x) to show that* $\alpha < 1/2$ *and obtain better estimates.*

Exercise 14.2.5 *If you enjoyed the solution of the wrong envelope problem and if you know the formula*

$$e^x \approx 1 + \frac{x}{1!} + \frac{x^2}{2!} + \cdots + \frac{x^N}{N!}$$

for large N, you may enjoy the following variation.

A large and cheerful crowd of N junior wizards leave their staffs in the porter's lodge on the way to a long night at the Mended Drum. On returning, each collects a staff at random from the pile, returns to his room and attempts to cast a spell against hangovers. If a junior wizard attempts this spell with his own staff, there is a probability p that he will turn into a bullfrog. If he uses someone else's staff he is certain to turn into a bullfrog. Show that the probability that in the morning the bedders will find N very surprised bullfrogs is approximately e^{p-1}.

14.3 Passing the torch

On 15 December, 1938 the German Army increased the number of rotors in use from three (giving six possible different configurations) to five (giving 60). Although the Poles reconstructed the two new rotors, the cost of finding the daily keys (measured in man-hours required to prepare suitable 'Zygalski sheets', the number of non-excluded daily settings to be examined, or in any other realistic terms) had now risen beyond any resources the Polish code-breakers could hope to command. On 30 March, 1939 the British and French Governments guaranteed Poland 'all support' in the event of an unprovoked German attack. On 27 April, Germany renounced her non-aggression pact with Poland. As tension rose, the Polish General Staff decided to share its cryptographic secrets with its allies.

The revelation of Polish success was performed in a suitably theatrical manner. The British and French delegations were ushered into a room containing tables on which stood several objects under covers. The covers were removed to show the Polish copies of the German Enigmas. When the British proposed bringing in their own draftsmen to copy the plans of the machines, the Poles announced that they had prepared two machines as gifts for their allies. The Poles also showed their *bomby* and Zygalski sheets and explained how they worked. One of the British representatives was 'Dilly' Knox, the doyen of British code-breakers. His attack on the Enigma had been foiled by his inability to work out the way the keyboard was connected to the input for the first disc. He knew that it was not the same as in the Commercial Enigma (where QWERTZU was connected up in the order 123456, following the layout of the German typewriter) and had given up hope of dealing with an unknown secret wiring. In answer to his question the Poles replied that the secret was simple — the military machine had ABCDEF connected up in the order 123456! (Had the Germans used a more complex system even Rejewski might have been foiled.) One of Knox's junior colleagues recalls the story that:

> after the meeting, Dilly returned to his hotel in a taxi with his French colleague, chanting, 'Nous avons le QWERTZU, nous marchons ensemble'†.

On 1 September, Germany and the USSR attacked Poland which was overwhelmed within three weeks. The nature of her conquerors is sufficiently illustrated by the chilling statistic that, during the Second World War, Poland was to lose 5 400 000 killed, all but 120 000 after her surrender. No hint of the pre-war success against Enigma reached German ears.

†'We have the QWERTZU, we march together.'

There is a story about a Cambridge don during the First World War who was asked why he was not at the front fighting for civilisation and replied 'Madam, I am the civilisation they are fighting to protect.' However, it is only a story, and a generation of Britain's most promising scientists had been included in the great slaughter. This time, the British were determined to make better use of their intellectual resources. By the time of the Polish meeting, the cryptological establishment had overcome its earlier prejudice against mathematicians (apparently based on the view that mathematicians were dreamy creatures liable to blurt out state secrets in a fit of absent-mindedness) and had started to recruit in earnest. (Those who still objected to the employment of mathematicians were told that everybody knew that mathematicians were good chess players and everybody knew that chess players made good code-breakers. It must also be said that the stresses of the time resulted in the recruitment of several experts on cryptogams†.) Since messages once deciphered have to be read and interpreted, linguists (including classicists, as the most likely to be able to learn Japanese), historians and others, thought to have special talents or just to be very bright, joined them. To these had to be added engineers, wireless experts and support staff. This ever-growing group worked in an ever-expanding collection of temporary huts and buildings in the grounds of Bletchley Park.

The superior British resources enabled them to cope with the tenfold increase in rotor arrangements. Production of the Zygalski sheets required examination of $60 \times 26^3 = 1\,054\,560$ rotor settings, and at the beginning of 1940 the British broke their first Enigma key. The best accounts of these events like [96] and [110] emphasise that the British code-breakers were involved in a race against the constant improvements that the German cryptographers made, both in the Enigma machines and in the way they were used. In a long-distance race any runner who falls behind the leaders will find it almost impossible to catch up. By giving their allies the wiring of the Enigma and the Zygalski sheets, the Poles had given the British the start they needed but the race was to be a close-run thing.

On 10 May, the Germans invaded France and, on the same day, in accordance with the best cryptographic principles, they changed their Enigma procedures in such a way that the 1560 Zygalski sheets, each with their carefully drilled 1000 or so holes, became just so much waste cardboard. The Zygalski method depended on the fact that the three-letter text setting was repeated twice giving rise to two different encipherments of the same three letters. The repetition guarded against the possibility of the text setting being garbled in transmission but, as the Germans now realised, went against the basic principle of

†Plants with no stamens or pistils, such as ferns and mosses. I have heard this story from two independent sources.

cryptography that the same message should never be transmitted twice. From now on the text setting was enciphered only once.

This change should have blinded the British pursuers as effectively as a handful of pepper in the eyes but, even in its new form, the German Army's Enigma procedures had a basic flaw, though one which is more obvious to a generation brought up on computer passwords. It is very difficult for people to behave randomly. If asked to choose an integer between 1 and 10, more people will choose 7 than any other number. When asked to choose a computer password, people often used the names of boyfriends, girlfriends or well known dates. In [59], Feynman describes how he made his reputation as a safe-cracker by exploiting these weaknesses. Not all German code clerks were paragons of patriotic efficiency, and few, even of the paragons, fully understood the limitations of the magic 'uncrackable' Enigma machines they were told to operate. In 1932, when the Poles started their operations, clerks would use triples like AAA. Orders were given forbidding the use of such triples so the clerks switched to ABC or running their fingers down the diagonals of the keyboards. Using their knowledge of the bad habits of individual code clerks and of code clerks in general, the British managed to overcome the crisis. Chapter 6 of Welchman's book gives a clear account of some of the methods used. Of course, if the Zygalski sheets had not been available in time, the detailed knowledge required to exploit the code clerks' weaknesses would not have existed; this was a race in which the code-breakers could not afford to fall behind.

The fruit of all this effort was distinctly bitter as Bletchley observed one of the greatest military disasters in British history.

> When any one of [the German] armoured units was held up by an Allied defensive position, we would probably decode an Enigma message from the unit's commander requesting air support. A little later we would hear that an attack by dive-bombing Stukas had been effective, and the armoured unit had resumed its advance. At intervals, all the major Panzer commanders would report their progress and their assessment of Allied capabilities.

The code-breakers consoled themselves that:

> Our decodes must have given early warning that the military situation was utterly hopeless. The mass of combat intelligence can hardly have failed to speed the extraordinary fleet of miscellaneous boats that brought so many back from the beaches of Dunkirk.

This was cold comfort indeed.

As the fall of France showed, even when Enigma decodes flowed freely, British commanders were only in the position of a poker player who catches an occasional glimpse of a card in his opponent's hand. Weak hands remained weak hands — the knowledge from breaking the German Railway's Enigma that a German invasion of Greece was imminent did not prevent the defeat of the Greek and British armies — and often, as with intercepts during the Battle of Britain, it is difficult to see how battles could have been fought differently, with or without the extra intelligence. What Enigma decodes did, time after time, was to shade the odds and, as it were, convert an unlucky card player into a lucky one.

A typical example, from a slightly later stage, occurred in 1941 when the German battleship *Bismarck*, having confirmed that she out-classed any single ship of the British or American navies by her destruction of the *Hood*, pride of the British fleet, vanished into the Atlantic. There followed many hours of 'desperate and sometimes irrational searching' by British ships and aircraft. After a day of wavering and contradictory advice and orders from the Admiralty, the Admiral in charge of the main British force decided to act on the assumption that the *Bismarck* was making for Brest. Although some Naval Enigma messages were being decoded, the time taken (three days or more) meant that no use could be made of this. On the other hand, the Air Force codes were being read quickly. The Luftwaffe chief of staff, General Hans Jeschonnek, was in Athens, directing his Air Force's part in the successful airborne invasion of Crete. His son was a junior officer aboard and the General abused the privilege of rank on 25 May to ask about the *Bismarck's* progress and destination. Within less than an hour of the British Admiral's original decision, he was given confirmation of its correctness and for the next 15 hours the British battleships pounded towards Brest.

On the morning of 26 May, the *Bismarck* was finally sighted by the radar of a Coastal Command aircraft. An attack by torpedo bombers found one of the few weak points (or, for all anybody knows, the only weak point) of the *Bismarck* by hitting her rudder and putting her steering out of action. With only a few more hours of fuel left, the British battleships at last caught up with and destroyed their formidable opponent.

The sequel illustrated another problem with the use of Enigma intelligence. The German Navy had planned a three-month cruise for the *Bismarck* and its companion warship to disrupt the convoy system totally. Tankers and other ships had already been dispatched and, armed with Enigma decodes, the British set out to hunt them down.

Two ships which were to be spared in order to make the other losses appear accidental had the misfortune to encounter Royal Navy ships by chance and were also sunk. This massacre aroused German suspicions and a full-scale enquiry ensued. Although it concluded that Enigma remained unbroken, extra precautions were introduced which substantially increased the difficulty of reading the Submarine Enigma.

The code-breaking at Bletchley did something else as well. In a period when disaster followed disaster and the avoidance of defeat was hailed as victory, it gave Britain's leaders a glimmer of hope, however illusory that hope may have been†. It can be argued that, if the only result of the whole complex and expensive effort had been to keep Churchill's spirits up while Britain stood alone, it would still have been worth it.

Churchill's romantic soul loved the excitement and secrecy surrounding Bletchley. He relished the way that

> [t]he old procedures, like the setting up of agents, the suborning of informants, the sending of messages written in invisible ink, the masquerading, the dressing-up, the secret transmitters, and the examining of the contents of waste-paper baskets, all turned out to be largely cover for this other source, as one might keep some old-established business in rare books going in order to be able, under cover of it, to do a thriving trade in pornography and erotica.

Each morning, a summary of the previous day's decrypts together with the most important individual messages were brought to Churchill in a special buff-coloured dispatch box. He visited Bletchley to thank 'the geese who laid the golden eggs and never cackled'. Looking at the disparate, unkempt and definitely unmilitary crew formed by his top code-breakers, he is said to have added to his head of Intelligence 'I know I told you to leave no stone unturned to find the necessary staff, but I did not mean you to take me so literally!'

The early successes gained by the use of the Polish gift gave Bletchley the prestige and goodwill needed in the constant battles for scarce resources and personnel. Building on this base, it had been able to ride the blow dealt by new German procedures, but this success was based on the bad habits of a few operators (and the number of such mistakes was to decrease very rapidly after 1941). The German Navy used a different method to identify message settings which avoided the dangers inherent in the Army and Air Force systems, and no progress had been made against the Navy codes. As late as the summer of 1940, the administrative head of Bletchley told the head of the Naval Section, 'You know, the Germans don't mean you to read their stuff, and I don't suppose you ever will.' The main hope of any further success against Enigma rested with the new 'Turing bombes'.

†An optimism shared at a lower level by the intercept operators whose tedious job it was to listen to faint morse code and take down gibberish with perfect accuracy. Welchman worried that the extra attention given to some messages might reveal they were being broken. 'I discovered, however, that the intercept operators believed that all their intercepts were decoded.'

The new bombes used the 'probable word method' discussed at the end of Section 13.2. The reader should reread that section and then ask herself how the simple method proposed there against the Commercial Enigma could possibly be adapted to work in the presence of a plugboard†.

†The Polish *bomby* depended on the fact that, initially, the Germans only 'steckered' 6 pairs of letters and so, from time to time, the short initial message would only involve 'self-steckered' letters (that is letters unaffected by the plugboard).

CHAPTER 15

Bletchley

15.1 The Turing bombes

Kahn writes that 'In Britain, Cambridge students and graduates were the cream of the nation and [Bletchley] took the cream of the cream.' Even among so many clever people, Turing was 'viewed with considerable awe because of his evident intellect and the great originality of his contributions. ... Many people found him incomprehensible, perhaps being intimidated by his reputation but more likely put off by his character and mannerisms. But all the Post Office engineers who worked with him ... found him very easy to understand. ... Their respect for him was immense,' though they also voiced the caveat at the end of Mitchie's recollection:

> He was intrigued by devices of every kind whether abstract or concrete — his friends thought it would be better if he kept to the abstract devices but that didn't deter him.

Before the war, Turing had himself designed an electrically operated enciphering machine and built part of it with his own hands. (He also made a start at building an ingenious analogue device for calculating the zeros of the Riemann zeta function. Just as importantly, some of his pre-war work was on what were then some of the deeper parts of probability theory.) It is interesting to note that Shannon, whose reputation also rests on rather deep and abstract results, is another great gadgeteer whose collected papers include one on the building of a calculator to work in Roman numerals (rather than binary).

Peter Hilton, an admiring younger colleague, recalled that

> [t]here was always a sense of immense power and ability to tackle every problem, and always from first principles. I mean, he not only, in our work during the war, did a lot of the theoretical work but he actually designed machines to help in the solution of problems — and with all the electrical circuitry that would be involved, as well. In all these ways he

> always tackled the whole problem and never ran away from a calculation. If it was a question of wanting to know how something would in fact behave in practice, he would then do the calculations as well.

Hilton goes on to describe one of Turing's odder gadgets (a metal detector) adding 'But it worked — it worked. As with all things with Turing, it really did work.'

He also tells a typical Turing story.

> Turing was a civilian, working in Intelligence, and he believed — again typical of Turing thinking in first principles — that the Germans might very well invade England and that he should be able to fire a rifle efficiently, and so he enrolled in what was called the Home Guard. The Home Guard was a civilian force, but which submitted to military training and in particular its members learnt how to fire a rifle. ... In order to enroll you had to complete a form, and one of the questions on this form was: 'Do you understand that by enrolling in the Home Guard you place yourself liable to military law?' Well, Turing, absolutely characteristically, said 'There can be no conceivable advantage in answering this question: "Yes"', and therefore he answered it "No". And of course he was duly enrolled, because people only look to see that things are signed at the bottom. And so he was enrolled, and he went through the training, and became a first class shot. Having become a first-class shot, he had no further use for the Home Guard, so he ceased to attend parades. And then in particular we were approaching a time when the danger of a German Invasion was receding and so Turing wanted to get on to other and better things. But, of course, the reports that he was missing on parade were constantly being relayed back to Headquarters and the officer commanding the Home Guard eventually summoned Turing to explain his repeated absence. It was a Colonel Fillingham, I remember him very well, because he became absolutely apoplectic in situations of this kind. This was perhaps the worst he had to deal with, because Turing went along and when asked why he had not been attending parades he explained it was because he was now an excellent shot and that was why he had joined. And Fillingham said: 'But it is not up to you whether you attend parades or not. When you are called on parade, it is your duty as a soldier to attend.' And Turing said: 'But I am not a soldier'. Fillingham: 'What do you mean, you are not a soldier! You are under military law!' And Turing: 'You know, I rather thought this situation could arise,' and to Fillingham he said: 'I don't know I am under military law.' And anyway, to cut a long story short, Turing said: 'If you look at my form you will see that I protected myself against this situation.' And so, of course, they got the form; they could not touch him; he had been improperly enrolled. So all they could do was to declare that he was not a member of the Home Guard. Of course that suited him perfectly.

> It was quite characteristic of him. And it was not being clever. It was just taking this form, taking it at face value and deciding what was the optimal strategy if you had to complete a form of this kind. So much like the man all the way through.

He remembers that

> [w]e were all very much inspired by him, [not only] his interest in the work but the simultaneous interest in almost everything else. As I say, it might be chess, it might be Go, it might be tennis and other things. And he was a delightful person to work with. He had great patience with those who were not as gifted as himself. I remember he always gave me enormous encouragement when I did anything at all noteworthy. And we were all very fond of him.

Turing was thus the natural person to develop machines to break codes produced by machines. It was an idea whose time had come. The code-breakers of all the major powers used the latest punch-card machinery. The code-breaking section of the German Foreign Office had many machines 'assembled out of standard parts for special purposes by Hans-Georg Krug, a former high school mathematics teacher who possessed a positive genius for this sort of thing'. We have already mentioned the Polish *bomby* which stepped through the 26^3 different positions of a given Enigma. But, in all these applications, the machines supplied the brute-force and human beings the subtlety. The Turing bombe supplied both.

The new bombes were the work of many people — one key idea came from Welchman and, no doubt, the fact that the Polish *bomby* had actually worked must have been a substantial encouragement — but it seems clear that the driving force and the source of many of the ideas was Turing. I shall content myself with trying to show why the Military Enigma was breakable in principle. The kind of electrical circuitry required is shown in the Appendix to Welchman's book. Let us suppose we guess a 12-letter stretch in some enciphered message. The method described at the end of Section 13.2 calls for us to set up 12 linked mock Enigmas (so that the outer rotor letter of each Enigma is one step further advanced than that of the previous one) and then drive the machine through its 26^3 possible states. As before, we shall assume that the inner rotors of the actual Enigma used to produce the message did not move during the encipherment of our 12 letters. The reasons for making this assumption are the same as those set out in Section 13.2.

We shall concentrate on the specific example given in Table 15.1. The second column shows the message, and the final column the enciphered message. The middle block shows the substitution alphabets supposed to be produced by the Commercial Enigma without plugboards. Thus looking at line 5 we see that, in the absence of a plugboard, the Enigma would encipher the 5th letter of the message according to the rule A goes to O, B goes to F and so on.

Let us write D ↔ J if D is steckered to J. Instead of considering all possible plugboard arrangements, let us ask simply which steckerings are possible for A. We begin by considering the possibility

(1) A ↔ A.

Looking at row 1, we see that the plugboard takes A to A, the Commercial Enigma takes A to J so, in order to arrive at the encipherment, the plugboard must take J to M. Thus J ↔ M. In the same way, looking at row 6, we see that V ↔ K. Thus

(2) A ↔ A, J ↔ M, V ↔ K.

Notice that at stage (2) we actually have five pieces of information since the symmetric plugboard arrangement also gives M ↔ J and K ↔ V. Notice also that any one of the three statements in (2) implies the two others.

Since M ↔ J, we can now use row 3 to show that O ↔ S. But we can do more. The reader may remember that in Section 13.3, using the advantages of 20/20 hindsight, I hinted that the self-inverse property of the Enigma was a cryptographic weakness. Since MLSYJKYHMLSH is encrypted as ADMIRALOFTHE, we may work from right to left as well as from left to right. Looking at row 5, we see that the plugboard takes J to M, the Commercial Enigma takes M to N so, in order to arrive at the encipherment, the plugboard must take N to R. Thus N ↔ R. In the same way, looking at line 9, we see that F ↔ Y. Thus

Table 15.1. *Successive Enigma encipherments.*

	In	ABCDEFGHIJKLMNOPQRSTUVWXYZ	Out
1	A	JFQXHBSEKAIYZTVUCWGNPORDLM	M
2	D	PNSKUZOWVLDJRBGATMCQEIHYXF	L
3	M	KDPBIQTMEOANHLJCFTGRXZYUWV	S
4	I	XODCHZLEPYUGQWBIMVTSKRNAJF	Y
5	R	OFYEDBZXLWQINMASKVPUTRJHCG	J
6	A	VWPTMXKUOLGJEZICRQYDKABFSN	K
7	L	DRTAGUEMZKJXIVYWSBQCFNPLOI	X
8	O	VZEJCQUNLDYIRHWXFNTSGAOPKB	H
9	F	HXIZGPEACYOVSTKFWUMNRLQBJD	M
10	T	HVXMZIKAFSGWDQURNPJYOBLCTE	L
11	H	OWMPYLTZKXIGCUADRQVFNSBJEH	S
12	E	SUZLJYITGEMDKXQROAPHBWVNFC	H

(3) A ↔ A, J ↔ M, V ↔ K, O ↔ S, N ↔ R, F ↔ Y,

and, as before, any one of the statements in (3) implies all the others.

Line 8 from left to right now gives T ↔ H, line 4 from right to left Z ↔ I and line 11 from right to left A ↔ H so

(4) A ↔ A, J ↔ M, V ↔ K, O ↔ S, N ↔ R, F ↔ Y, T ↔ H, Z ↔ I A ↔ H

and, as before, any one of the statements in (4) implies all the others.

We have now obtained a contradiction since (4) contains both the statement A ↔ A and the statement A ↔ H. The most obvious thing to do is to stop at this point and examine the remaining 25 possibilities one by one. Once we have shown that each of the 26 steckerings A ↔ A, A ↔ B, A ↔ C, ... A ↔ Z are impossible, we know that the particular Enigma position cannot produce the correct encipherment *whatever the plugboard* and we can move on to the next one.

However, the most obvious thing to do is not necessarily the best one. Observe that we do not actually have to test for the possibility A ↔ H, since any one of the statements in (4) implies all the others so, in particular, A ↔ H implies A ↔ A. This insight suggests that it might be worth while to press on to stage (5). Using line 10, together with the statement from (4) that T ↔ H, we obtain A ↔ L so we will not have to test for this possibility. We observe also that we can reuse line 1 together with the statement A ↔ H from (3) to get E ↔ M and that line 6 can be reused in a similar manner.

With luck, as we move from stage (4) to (5), from (5) to (6) and onwards we will gather an avalanche of statements which will eventually include all of A ↔ A, A ↔ B, A ↔ C, ... A ↔ Z. All of these statements will be deducible from each other and all will thus give contradictions. (This would parallel the principle of formal logic which states *ex falso quodlibet* that is 'given any false statement we may deduce anything we want from it'†.) Thus working out all the consequences of the single statement A ↔ A will (with luck) suffice *by itself* to exclude the possibility that the particular Enigma position could produce the correct encipherment with any plugboard whatsoever.

Moving a little closer (but not much) to the practical implementation of this scheme, I ask the reader to consider the 'skeletons' shown in Figure 15.1. Here we connect two letters if one is the encipherment of the other so that, for example, looking at row 1, A is joined to M, looking at row 2, D is joined to L. The letters then fall into a collection of connected components. In this case I have labelled them (a), (b), (c) and (d). It turns out that it is possible to set up electrical circuits in such a way as to perform all possible deductions (involving a specified letter, say A, and starting from a single specified steckering, say A ↔ A) essentially simultaneously. The only limitation is that we cannot use

†It is said that the philosopher McTaggart once challenged Bertrand Russell to use the statement '1=2' to prove that he was the Pope. This presented no problem. 'I and the Pope are two. But 1=2 so I and the Pope are one.'

more lines than there are mock Enigmas in a bombe. A standard bombe had 12 mock Enigmas, so we could use all of (a), (b), (c) and (d), but the first two prototypes only had 10 so we could only use (a) and (b) for them. We refer to the collection of components used (together with the list of the lines involved) as the menu.

This brings us to the second point. I have spoken of a possible 'avalanche of statements' but I have not given much evidence that it will occur. Actually, there are two separate points involved:

1 Will the avalanche start?
2 Once started, will it continue?

Both of these questions should more correctly be posed probabilistically as follows. Given a random choice of 12 (or whichever number of alphabets† is involved) is there a very high probability that:

1′ the avalanche will start, and
2′ once started will continue?

In Section 17.1 I will discuss the much easier problem of the propagation of surnames. To see a connection, consider a 'mother statement' say A ↔ A from which we deduce 'daughter statements' say J ↔ M, V ↔ K. Some statements will have no offspring, some will have one daughter, some two and so on. It is clear that in order to produce an avalanche, each mother must produce an average of more than one daughter (and, of course, the larger the family size the better). However, the problem is complicated by the fact that no 'generation' of daughters, granddaughters, great-granddaughters, or whatever, can exceed the number of lines involved by the menu.

It is clear on common sense grounds that (if avalanches occur at all) some menus must be more likely to provoke avalanches than others. The menu shown in Figure 15.1 is not a very good menu (for the

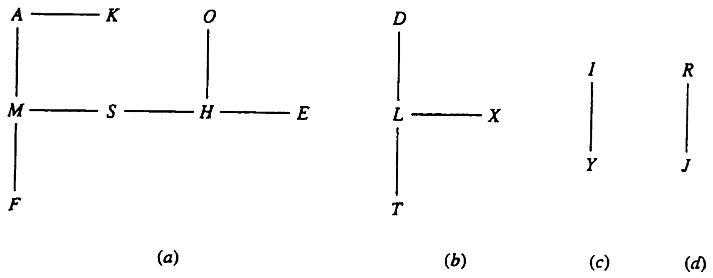


Figure 15.1: A possible menu.

†That is mock Enigmas, or lines involved by the menu.

purposes of exposition, it helps if the number of deductions at each step is not too large) since it lacks closed circuits of the type shown in Figure 15.2. The reader should not find it hard to convince herself that the existence of closed circuits increases the probability that 'deductions get fed back into the system' and so increases the average family size.

Exercise 15.1.1 *Suppose that the encipherment of* THEGENERALHE *is*

ALAPHQNSNTTL

but the trial alphabets are as in Table 15.1. (For convenience we give the appropriate alphabets in Table 15.2.) Draw a menu and carry out a few stages of the appropriate deductions.

In Chapter 13 of [94], Derek Taunt discusses the work involved in setting up a menu. We can well believe that 'Much skill, ingenuity, and judgement could be expended on the composition of good menus from otherwise intractable material.' The construction of the prototype bombes must have been accompanied by many hand trials, much discussion of more or less plausible mathematical models and a great deal of nail-biting.

Table 15.2. *A possible Enigma encipherment?*

	In	ABCDEFGHIJKLMNOPQRSTUVWXYZ	Out
1	T	JFQXHBSEKAIYZTVUCWGNPORDLM	A
2	H	PNSKUZOWVLDJRBGATMCQEIHYXF	L
3	E	KDPBIQTMEOANHLJCFTGRXZYUWV	A
4	G	XODCHZLEPYUGQWBIMVTSKRNAJF	P
5	E	OFYEDBZXLWQINMASKVPUTRJHCG	H
6	N	VWPTMXKUOLGJEZICRQYDKABFSN	Q
7	E	DRTAGUEMZKJXIVYWSBQCFNPLOI	N
8	R	VZEJCQUNLDYIRHWXFNTSGAOPKB	S
9	A	HXIZGPEACYOVSTKFWUMNRLQBJD	N
10	L	HVXMZIKAFSGWDQURNPJYOBLCTE	T
11	H	OWMPYLTZKXIGCUADRQVFNSBJEH	T
12	E	RUZLJYITFEMDKXQROAPHBWVNFC	L

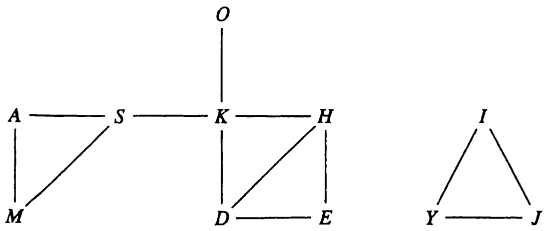


Figure 15.2: A good menu.

So far we have dealt with what will happen if our rotors and their positions do not correspond to those in the original Enigma. What will happen if they do? Table 15.3 shows an encipherment (for some unrevealed plugboard setting) corresponding to the 12 substitution codes shown.

Exercise 15.1.2 *Suppose we are in the situation given by Table 15.3. Draw the menu and carry out completely all the appropriate deductions which can be made starting from* E ↔ L.

I believe that the reader who carries out Exercise 15.1.2 will obtain the statements E ↔ L, N ↔ N, I ↔ I, Z ↔ B, D ↔ A, H ↔ Y, G ↔ C, X ↔ F, T ↔ Q and no more. This suggests that (as, in fact, is the case) we have the correct alphabets (and so the correct rotors in the correct positions) and the correct steckering E ↔ L. What will happen if we test another steckering, say E ↔ E?

Exercise 15.1.3 *Suppose we are in the situation given by Table 15.3 (and for which you drew the menu in Exercise 15.1.2). Carry out the first few stages of deductions starting from* E ↔ E.

Once again we expect an avalanche of statements to follow from the false assumption E ↔ E. However, *there is one statement about the steckering of* E *that cannot form part of the avalanche.* We have already seen that every statement in the avalanche is deducible from every other.

Table 15.3. *A correct Enigma encipherment.*

	In	ABCDEFGHIJKLMNOPQRSTUVWXYZ	Out
1	T	JFQXHBSEKAIYZTVUCWGNPORDLM	G
2	H	PNSKUZOWVLDJRBGATMCQEIHYXF	F
3	E	KDPBIQTMEOANHLJCFTGRXZYUWV	N
4	G	XODCHZLEPYUGQWBIMVTSKRNAJF	A
5	E	OFYEDBZXLWQINMASKVPUTRJHCG	I
6	N	VWPTMXKUOLGJEZICRQYDKABFSN	B
7	E	DRTAGUEMZKJXIVYWSBQCFNPLOI	F
8	R	VZEJCQUNLDYIRHWXFNTSGAOPKB	J
9	A	HXIZGPEACYOVSTKFWUMNRLQBJD	B
10	L	HVXMZIKAFSGWDQURNPJYOBLCTE	B
11	H	OWMPYLTZKXIGCUADRQVFNSBJEH	L
12	E	RUZLJYITFEMDKXQROAPHBWVNFC	A

But in Exercise 15.1.2 we saw that the statement E ↔ E was not among those deducible from E ↔ L so it follows that the statement E ↔ L will not be among those deducible from E ↔ E. On the other hand, there seems to be no reason to exclude any other statement concerning the steckering of E from the avalanche. Thus, with luck, statements deducible from E ↔ E will include 25 of the 26 statements E ↔ A, E ↔ B, E ↔ C, ..., E ↔ Z but cannot include the statement E ↔ L.

If we test a particular steckering, say X ↔ X by running our mock Enigmas through their 26^3 positions, then at each step one of three desirable things may happen:

1 All 26 steckering possibilities for X are deducible. We then *know* that we have the wrong Enigma set up and the machine moves on.

2 Nó new steckering possibilities for X are deducible. There should be a good chance that we have the right Enigma rotors in the right positions (and, though this is far less important, that our test stecker for X is correct). We should investigate further 'by hand'.

3 All but one of the 26 steckering possibilities for X are deducible. There should be a good chance that we have the right Enigma rotors in the right positions (and, though this is far less important, that the excluded steckering possibility for X is correct). We should investigate further 'by hand'.

Of course, there remains a fourth, unpleasant, possibility:

4 The number of steckering possibilities for X which are deducible is k with $2 \leq k \leq 24$.

Provided this only occurs rarely, we can also investigate the associated Enigma setting by hand. If not, then (since the technology of 1940 will not permit a more complicated scheme) we will have to revert to our original naïve approach and examine each of the 26 steckerings X ↔ A, X ↔ B, X ↔ C, ... X ↔ Z in turn. Such an approach will take 26 times as long.

Fortunately, as we now know, it was possible to find menus which provoked avalanches and the approach outlined above did actually work. The plugboard had been vanquished though the effectiveness of the approach remained crucially dependent on the number of bombes involved and the time available to use them. Examination of a 12-letter menu required 12 linked mock Enigmas (forming one bombe) which took perhaps 15 minutes to work through all the possibilities. Recall that the Army and Air Force Enigmas had 60 rotor orders and the Navy Enigma 336.

15.2 The bombes at work

There is a further problem. If the reader looks at the description at the end of Section 13.3 of how the German Army transmitted its 'text setting' (the stage of the Enigma cycle at which the message began), she will see that, once the daily setting has been discovered, it is as easy for the code-breakers to read the day's messages as it is for the intended recipient. The Navy provided no such obvious help. It thus appears that the deciphering of one message (the contents of which we may well already know, since our method depends on knowing or guessing several letters of the text) provides no help in deciphering another. A moment's reflection convinces us that this ought not to be so since our first successful decipherment revealed both the plugboard arrangement and the particular Enigma cycle (specified by the arrangement of the rotors and the state of the counting mechanism at one point in the cycle). We have thus reduced the problem of deciphering any given message from one involving astronomical numbers of possibilities to one of finding which particular stage, out of a possible 26^3 of the Enigma cycle, the machine was in at the start of the message.

In English, the most frequently occurring single letter is E, the most frequent sequence of two letters is TH and the most frequent sequence of three letters is THE. (Having made such a statement we must immediately qualify it. Presumably, different kinds of communication — military, scientific, and so on — have different frequencies for given sequences. Again different strategies for dealing with the spaces between words — replacing them by X, ignoring them, and so on — will also alter frequencies, possibly quite substantially.) Our attack will concentrate on what we expect to be a frequently occurring sequence of four letters, say THEX. By running an Enigma-like machine through the entire cycle we obtain the $26^3 = 17\,576$ different encipherings of THEX, corresponding to each starting point on the Enigma cycle, and record them on punch-cards. The kind of punch-card machinery available in 1940 was perfectly capable of scanning a text (once that, too, had been entered on punch-cards) and detecting coincidences. If a possible enciphering of THEX is detected we can set up an Enigma so that it is at the appropriate stage in its cycle and run it over the whole enciphered message and see if the trial decipherment makes sense.

Exercise 15.2.1 *(i) Show that the probability of a random sequence of four letters corresponding to one of our punch-cards is 1/26 and conclude that scanning a 200-letter message will produce, on average, about eight false alarms.*

(ii) What would happen if, instead of using a four-letter sequence, we used a three-letter sequence? What would happen if, instead of using a four-letter sequence, we used a five-letter sequence? Why do we use a four- rather than a three- or five-letter sequence?

Exercise 15.2.1 shows that the number of false alarms is not too great but, of course, the method is only useful if there is a reasonable probability of a positive outcome. Fortunately, the German language is rich in frequently occurring four-letter sequences ('tetragrams' in code-breakers jargon). According to [94] page 114 the tetragram EINS was used but it appears to me that the method would still have been feasible if the test had been run several times with different tetragrams.

Exercise 15.2.2 *Suppose that each of n tetragrams has probability p of occurring in a 200-letter message and that their occurrence is independent (this cannot be strictly true but will be close to the truth in practice). Roughly how many false alarms will occur if we test for each one and what is the probability that at least one of the tetragrams will appear? Look at the results you have obtained for various values of p (say* $p = 0.25, 0.1, 0.01$*) and n.*

The bombes were tended by Wrens, that is members of the Women's Reserve Naval Service. One of them, Diana Payne, recalls an interview at which she was asked if she could keep a secret, to which 'I answered that I really did not know as I had never tried.' A few weeks later she was ordered to Bletchley where in the morning

> [t]he conditions of the work were disclosed. It would involve shift work, very little hope of promotion, and complete secrecy. On this limited information we were given until lunchtime to decide whether we could face the ordeal.

She and the Wrens with her

> decided to face the challenge, and all signed the Official Secrets Act which committed us to the job for the duration of the war, and to keep the secret forever.

After suitable training the work began.

> The bombes were bronze-coloured cabinets about eight feet tall and seven feet wide. The front housed rows of coloured circular drums, each about five inches in diameter and three inches deep. Inside each was a mass of wire brushes, every one of which had to be meticulously adjusted with tweezers to ensure that the electrical circuits did not short. The letters of the alphabet were painted round the outside of each drum. The back of the machine almost defies description — a mass of dangling plugs on rows of letters and numbers.
>
> We were given a menu, which was a complicated drawing of numbers and letters from which we plugged up the back of the machine and set the drums on the front. ...
>
> We only knew the subject of the key and never the contents of the messages. It was quite heavy work getting it all set up, and [we needed] good height and eyesight. All this work had to be done at top speed, and at the same time 100 per cent accuracy was essential. The bombes made a considerable noise as the drums revolved, each row at a different speed, so there was not much talking during the eight-hour spell. [From time to time] the bombe would suddenly stop, and we took a reading from the drums.

Since such a stop only indicated a possible setting and could have been due to what was called a 'legal contradiction', the bombe was restarted and the reading hurriedly phoned through to another room where operators using British Typex machines modified to model the German Enigmas would carry out the final decipherment. If they were successful

> the good news would be a call back to say, 'Job up; strip machine'. It was a thrill when the winning stop came from one's own machine.

The Wrens worked on watches of four weeks duration: 8 a.m. to 4 p.m. the first seven days, 4 p.m. to midnight the second week, midnight to 8 a.m. the third and then a hectic three days of eight hours on and eight hours off, ending with a much needed four days leave. The bombes broke down frequently and could deliver unpleasant electric shocks. It was a monotonous 'life of secrecy and semi-imprisonment' overshadowed by the knowledge that 'any mistake or time wasted could mean lives lost.' The strain showed itself in nightmares and digestive troubles. Occasionally girls would simply collapse or go berserk on duty[†].

More and more bombes were built and more and more Wrens were recruited to run them. Since they were in the Navy they worked under Naval discipline and the places they worked were treated as ships (some of them even had a quarter deck which all Wrens had to salute[‡]). And then after three and a half years

> Helen Rance, one of the hundreds of ... Wrens of HMS *Pembroke* remembers the 'eerie silence' in the rooms of that stone frigate when the bombes were finally switched off. Several of the girls could not resist rolling the heavy drums across the floor — something they had never been allowed to do before; then '... we sat down and took all the drums to pieces with screwdrivers; everything was dismantled.'

[†] But, although at least one British dramatist has portrayed Bletchley as run along the lines of the society of H. G. Wells's *The Time Machine* with the Eloi and Morlocks of different sexes, the correct reference is surely to the same author's *The Land Ironclads*.

[‡] Naturally, the minibus in which they went on leave was known as 'The Liberty Boat'.

Exercise 15.2.3 *Welchman says that 'It was possible to choose a sequence of [rotor] orders that would not call for more than one drum [corresponding to one rotor] to be changed between successive runs.' Set up such a schedule for the 60 runs required by the five German Army rotors.*

With the coming of the bombes, the breaking of German codes could take place on an industrial scale. But, although many messages could be read routinely, the vital Naval Enigma had a further layer of protection. For the bombes to work they needed an initial crib, that is part of a message known or guessed both in unenciphered and in ciphered form. The knowledge, gained earlier, of the kinds of messages transmitted by particular Army or Air Force sources gave such cribs, but the Naval Enigma had not been read before, so no such cribs existed. Moreover, the standard of cryptographic discipline of the German Navy was high. Messages were kept short and often encoded by another method before being enciphered by Enigma. The Navy maintained groups to monitor its own communications and report on any lapses detected. Under these conditions, where could the needed cribs be found?

For reasons ultimately, but subtly, connected with the earth's rotation, weather conditions tend to move from West to East. The U-boats in the Atlantic and the German armies in Europe needed weather forecasts and the forecasters needed information from over the Atlantic. The information was gathered in three ways: by reports from German warships and merchant ships (and, after the first year, the surface dominance of the British Navy meant that only U-boats were left in the Atlantic), by aircraft flights and by weather ships. The British managed to break the codes used in the retransmission of these reports and the weather forecasts based on them. This had the immediate advantage of giving the British meteorologists extra information on which to base their own forecasts and raised the possibility of using the decoded weather reports and forecasts as cribs for the U-boat Enigma. It was not surprising that the British Navy reacted strongly and unfavourably to an RAF proposal to shoot down German aircraft engaged in meteorological flights.

However, the submarines did not transmit Enigma encipherings of weather reports directly, but first encoded the reports in the form of short signals of just a few letters long (we give an example in Section 16.2). This was done mainly to keep radio transmissions as short as possible, but the extra level of security was an added bonus for German cryptographers. The method for encoding the weather reports was given in a booklet which we shall call the Short Weather

Cipher. A plan was conceived† to capture a German Weather ship and seize the month's Naval Enigma settings together with the precious Short Weather Cipher. How this was done, not once but twice, without arousing German suspicions forms the central episode of Kahn's exciting *Seizing The Enigma.*

Armed with these documents, Bletchley was at last able to read the U-boat Enigma and to read it fast enough to influence events. At a rough estimate, the evasive routing of convoys using the information thus yielded saved about 2 000 000 tons of shipping (or between 300 and 350 ships) during the last six months of 1941. The decrypts also enabled Naval Intelligence to build up a detailed picture of the U-boat organisation and tactics.

A naval officer posted to Bletchley vividly remembers

> the sense of shock produced on my first arrival at the Park by the grimness of its barbed-wire defences, by the cold and dinginess of its hutted accommodation, and by the clerk-work we were first set to do. But this was soon swept aside by the much greater shock of discovering the miracles that were being wrought at the Park. In Iceland I had been interrogating the survivors of the many merchant ships sunk in the, at first, highly successful offensives against the Atlantic convoys launched by the U-boats ... I had spent many hours trying to analyse their strength and tactics. I could have spared my pains. For I now discovered that all this, and everything else about U-boats, was known with precision by those privy to the Enigma decrypts‡. Leafing through the files of past messages ... I shivered at seeing the actual words of the signals passing between Admiral Dönitz and the boats under his command whose terrible work I had seen at first hand. ... No less shocking was the revelation of the bestiality that underlay this sophisticated form of warfare. This emerged vividly from Dönitz's exhortations to his captains — 'Kill, kill, kill!' and from the names given to the wolf-packs, such as *Gruppe Blutrausch* ('Blood Frenzy').

It was well that Bletchley was so successful for those six months because the British advantage did not last much beyond them.

15.3 SHARK

From the first day of February 1942 darkness once more obscured Dönitz's communications from his opponents. The German Navy had introduced the four-rotor Enigma. A total redesign would have created many difficulties both in the manufacture and use of the new machine, so the new four-rotor Enigma was a clever modification of the old three-rotor one. By using a new thinner reflector it became possible to

†By a history student named Hinsley recruited straight from Cambridge. When I was an undergraduate, Hinsley and his colleagues were still around, some running the University, some trying to teach me algebra. They seemed to me pleasant, unadventurous but, above all, conventional people.

The oldest hath borne most; we that are young
Shall never see so much, nor live so long.

‡The information which Blackett attributes to 'the accounts of prisoners of war from sunken U-boats' presumably came, in great part, from Enigma decrypts still secret at the time he wrote.

introduce a fourth 'thin rotor' which did not revolve but which could be set in any of 26 positions. In order to retain compatibility with the three-rotor Enigma used in the other armed services, the combination of the new reflector and a particular 'neutral' position of the new thin rotor replicated the effect of the old reflector.

Clues as to the nature of the new machine had accumulated at Bletchley during the previous six months, and an incident in which a message had been transmitted by mistake in the new code and then (by a much greater mistake) retransmitted in the old, enabled the British cryptologists to reconstruct the wiring of the fourth rotor and the new reflector before they entered service. Even with this knowledge, the introduction of the new machine remained a catastrophe for Bletchley. The fourth rotor multiplied the number of starting positions and thus the labour of the brute-force searching on which the decoding depended by a factor of 26. The new system was called SHARK by those who now sought to break it.

If bombes could have been brought forth in unlimited amounts, the situation would have been less serious, but at the end of 1941 there were only 12 bombes in action and by the end of 1942, only 49. On the 14 March 1942, a long message containing news of Dönitz's promotion to full Admiral was sent out in another code which Bletchley could read. On the assumption that a particularly long SHARK transmission was an encoding of the same message, the bombes were set to work and succeeded in recovering that day's keys. However, this required 6 bombes working for 17 days. It would have required 100 bombes working full time to reduce the decoding time to one day. (Nor was Dönitz promoted every day. The Germans had also changed their weather signals, so where were the cribs to come from to start the process?)

Plans were immediately made to build new four-rotor bombes working 26 times as fast, but the old three-rotor bombes had been built as close to the limits of existing technology as could be managed. It is not surprising that the task proved more difficult than expected and the first fast four-rotor bombes only entered service (and, according to Hinsley, experienced severe teething problems) on the British side in June 1943 and (slightly later but with fewer problems) on the American side in August 1943. By the end of 1943, a substantial number of four-rotor bombes would be in service but until then the old slow, three-rotor bombes would have to suffice.

In 1941, about 4 300 000 tons of shipping (representing about 1300 ships) had been lost world-wide, of which 2 400 000 tons (about 500 ships) were lost in the North Atlantic. German losses amounted to 35 U-boats. In 1942, the figures rose to 7 800 000 tons of shipping (representing about 1700 ships) lost world-wide, of which 5 500 000 tons (about 1000 ships) were lost in the North Atlantic. German losses amounted to 86 U-boats. It took the United States six months from its entry into the war, in December 1941, to organise proper coastal convoys and the resulting 'happy time' for the U-boats, whilst increasing the total tonnage sunk, took pressure off the Atlantic convoys for a time, but by the end of 1942 the main battle had returned to the Atlantic.

In retrospect, we may see some gleams of hope. Such was American industrial might that, by the end of 1942, new Allied ship building could more or less keep pace even with these dreadful losses. (It was not, however, clear that replacement crews could forever be found to man replacement ships.) This meant that, in the coldest strategic terms, the Battle of the Atlantic was not being lost, though neither was it being won. It was also true that, although the exchange rate of U-boats destroyed against ships sunk remained extremely unfavourable, the number of U-boats required to sink a given tonnage was steadily increasing. What had been courageous weighing of odds in the presence of newly-trained escorts became foolhardy risk-taking against more experienced and better trained opponents. One by one, the U-boat aces were killed or captured whilst the more cautious captains survived.

This, also, was little comfort to the convoys. As the American official historian wrote:

> By April 1943, the average kill per U-boat had sunk to 2000 tons [per month]. This might be interesting as a sort of sporting score, but the number of U-boats operating had so greatly increased that it was of little significance in solving the problem. When Daniel Boone, who shot fifty bears a year, was replaced by fifty hunters who averaged one each, the bears saw no occasion to celebrate the decline in human marksmanship.

Dönitz now had 200 submarines available. Storms in December 1942 and January 1943 greatly hampered the U-boats, though they sank seven out of nine tankers in one convoy heading for North Africa. In February, the great North Atlantic convoy battles resumed. A six-day battle in early February involved 21 submarines against 63 merchant ships with 12 escorts. Twelve merchant ships were sunk by torpedoes and another sank after collision, for the cost of three U-boats. The total of 380 000 tons for Allied losses in February was dwarfed by March's 590 000 tons. Two convoys, the one overtaking the other, were attacked day and night over a six-day period by 45 submarines. Twenty-one of the 92 merchant ships were sunk whilst the 18 escorts managed to sink only one submarine. Some 161 000 tons of cargo were lost including everything from steel and explosives to sugar, wheat and powdered milk.

The British official historian's summary runs as follows:

> The Admiralty ... recorded that 'the Germans never came so near to disrupting communications between the New World and the Old as in the first twenty days of March 1943'. Even at the present distance in time ... one [cannot] yet look back on that month without feeling something like horror over the losses we suffered. In the first ten days, in all waters, we lost forty-one ships; in the second ten days, fifty-six. More than half a million tons of shipping was lost in those twenty days: and what made the losses so much more serious than the bare figures can indicate, was that nearly two-thirds of the ships sunk during the month were sunk in convoy. 'It appeared possible,' wrote the Naval Staff after the crisis had passed, 'that we would not be able to continue [to regard] convoy as an effective system of defence.' It had, during three-and-a-half years of war, slowly become the lynchpin of our maritime strategy. Where could the Admiralty turn if the convoy system had lost its effectiveness? They did not know; but they must have felt, though no one admitted it, that defeat stared them in the face.

Just under half of the crews of merchant ships lost by enemy action could expect to survive. The official historian states that:

> It seems not unlikely that a quarter of the men who were in the Merchant Navy at the outbreak of war, and perhaps an even higher proportion, did not survive until the end, or if they survived, lived permanently damaged lives, still in the shadow of death.

Although certain élite corps (such as the bomber crews) suffered even higher casualty rates, proportionate losses among merchant seamen thus greatly exceeded those in the 'Fighting Services'. Traditionally, the occupation was poorly paid and insecure and though, mainly through the addition of 'war risk' (or 'danger') money, wages more than doubled during the first three years of war, the wage of an ordinary seaman in the middle of 1942 was less than £23 a month†.

These, in the day when heaven was falling,
The hour when earth's foundation fled,
Followed their mercenary calling
And took their wages and are dead.

Their shoulders held the sky suspended;
They stood, and earth's foundation stay;
What God abandoned, these defended,
And saved the sum of things for pay.

†Agricultural labourers who were near the bottom of the wages ladder received about £10 a month. The poverty line for a family of five was considered to be about £18 a month. It must be remembered that wages were only paid for the voyage. The immemorial customs of the industry meant that survivors knew that their wages had ceased to be paid from the moment their ship sank.

The effectiveness of the submarine campaign can be seen from the map in Figure 15.3 (copied from [111]). It shows how submarine activity had been pushed outward into the air-gap, but it also shows how Dönitz exploited every Allied weakness to sink yet more ships. This world-wide battle was directed by one man with a tiny staff, a Führer for submarine warfare moving his chess pieces in the service of a greater Führer.

But to control his chess pieces, the player needs to know where they are.

> Not only did returning U-boats always signal their expected time of arrival; every outward-bound U-boat reported on clearing Biscay or, if leaving from Norway or the Baltic, after crossing 60°N. Except when a U-boat sailed for a special task or a distant area, it received its destination point and its operational orders by [radio] after it had put to sea; these were matters which had to be settled in the light of the latest situation and of which all U-boats at sea had to be informed. No U-boat could deviate from its orders without requesting and receiving permission, and, without requesting and receiving permission, none could begin its return passage. In every signal it transmitted the U-boat was required to quote its present position; if it did not do so, or if it did not transmit for several days, it was ordered to report its position. To each of its signals, again, the U-boat was expected to append a statement of the amount of fuel on hand† ...
>
> The U-boat command ... ordered the formation and reformation of the patrol lines between specified geographical positions at regular intervals, addressing by name each U-boat commander who was to take place in a line and giving him his exact position in it. It informed each line of U-boats what to expect in the way of approaching convoys and, in addition, supplied for the attention of all U-boats at sea a steady stream of situation reports and general orders. When a convoy was sighted, the Command decided the time, the direction and the order of attack. The exercise of this degree of remote control ... required U-boats in contact with the target to transmit on high frequencies detailed descriptions of the situation.

The British had developed high frequency radio direction-finding equipment, 'Huff-duff', based on pre-war research on tracking thunderstorms. Under the impulsion of Blackett, eight land-based stations were set up from Land's End to the Shetlands. Exercise 3.3.2 explains why the line of stations was made as long as possible and also gives one of the many reasons why (as the Germans expected) they could not give accurate bearings from more than 500 kilometres away and were ineffective (at least for tactical purposes) in mid-Atlantic. However

†Hinsley gives the following signal as typical.

From: Schultze (U 432)
To: Admiral Commanding U-boats
In square 8852 have sunk one steamship (for certain) and one tanker probably. Set one tanker on fire on October 15th. My present position is square 8967. Have 69 cubic metres of fuel oil left. Have two (air) and one (electric) torpedoes left. Wind south-west, force 3 to 4. Pressure 996 millibars. Temperature 21 degrees centigrade.

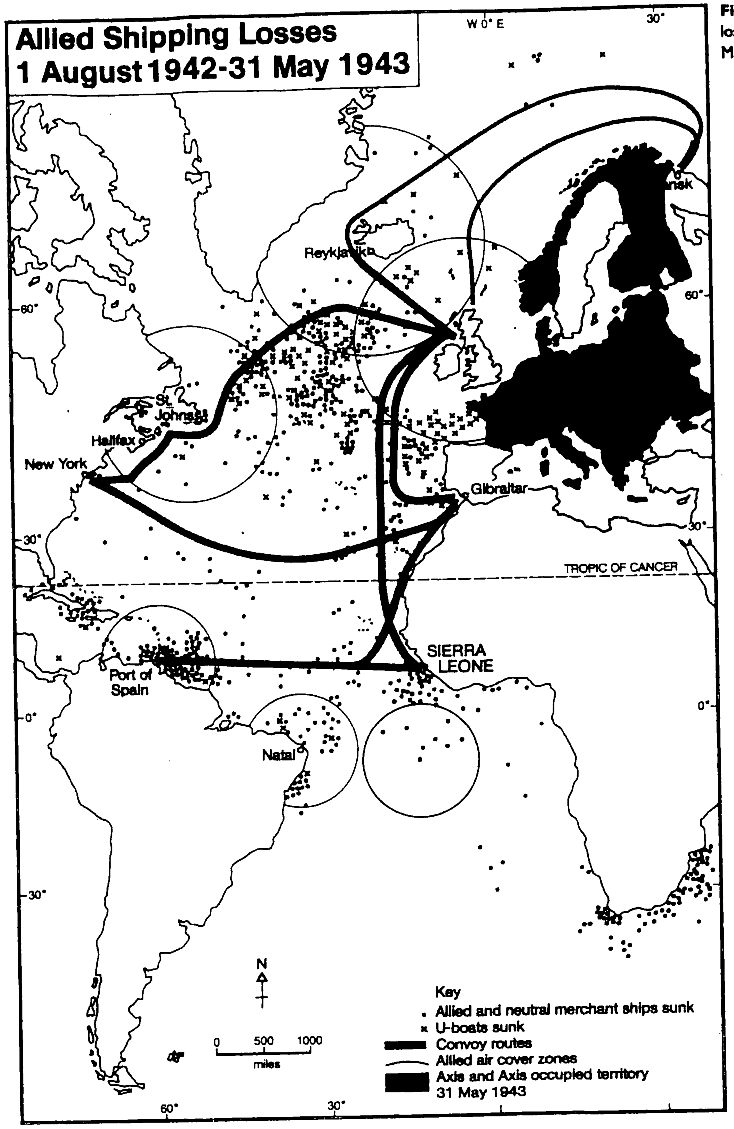


Figure 15.3: Allied shipping losses 1 August 1942 to 31 May 1943

(as the Germans had not anticipated), Huff-duff sets were made small enough to go to sea with the escorts. This was a major tactical advance, but, to route convoys, only Enigma would do. It is no wonder that the Operational Intelligence Centre which sought to track the submarines urged the code-breakers to focus 'a little more attention' on SHARK and told them that the U-boat campaign was 'the one campaign which Bletchley Park are not at present influencing to any marked extent — and it is the only one in which the war can be lost unless BP *do* help. I do not think this is any exaggeration.'

In late October 1942, three British naval seamen boarded a sinking German submarine and rescued papers from it. First Lieutenant Fasson and Able Seaman Grazier went down with the submarine whilst seeking further papers. The third seaman, a cook's assistant called Brown, turned out to have lied about his age in order to join up. He was decorated for his bravery and sent home, only to die two years later trying to save his sister from a fire caused by a bombing raid.

Among the seized papers was the second edition of the Short Weather Cipher. Bletchley now had a supply of cribs to work on, but the fourth rotor still meant working through 26 times as many possibilities. On 13 December, they found a solution† and discovered, to their delight, that weather messages were transmitted with the fourth rotor in neutral, making the four-rotor machine in effect into a three-rotor machine. (This had been done so that the three-rotor machines of the weather service could continue to be used.) By itself, this should not have compromised SHARK, but it turned out that the same setting for the first three rotors was used in non-weather messages. Once the weather setting was known, the cryptanalysts had only to try the 26 possible settings of the thin rotor to solve the code completely. It is possible that the normally extremely competent German naval cryptologists made this mistake because of their obsessive fear of the enemy within. The fourth rotor was thus intended not to prevent the British breaking a system which was believed unbreakable, but to prevent unauthorised reading of submarine communications by other branches of the German military.

During the next few months, the British had increasing success in breaking keys, though there were crises when a new Short Weather Cipher went into effect and when a second thin rotor was introduced. SHARK keys were found for 90 of the 112 days between 10 March and the end of June. As we have seen, March witnessed the greatest German convoy victories of the war. Those victories were also the last. The figures of Table 15.4 tell their own story. At the end of May, Dönitz withdrew his forces from the North Atlantic to seek easier

†I cannot resist a little name-dropping here. The man in charge at the time that the break was made was Shaun Wylie, one of my predecessors at Trinity Hall.

targets elsewhere. In July, he tried the North Atlantic again when his submarines sunk 123 327 tons (18 ships) for a loss of 37 of their number but again withdrew, essentially for good. May marked the point when it became clear to Dönitz that 'We had lost the Battle of the Atlantic.'

Echoing Dönitz, Hitler attributed 'the temporary set-back to our U-boats ... to one single technical invention of our enemy,' that is the new 10 centimetre radar mounted in anti-submarine aircraft. To this, as Dönitz well realised, must be added the closing of the air-gap by very-long-range aircraft and improvised aircraft carriers. In theory, the submarine command was awake to the possibility that codes might be broken. In his memoirs, written before Allied code-breaking successes became known, Dönitz wrote:

> Our ciphers were checked and rechecked, to make sure they were unbreakable; and on each occasion the head of the Naval Intelligence Service at Naval High Command adhered to his opinion that it would be impossible for the enemy to break them.

In practice, to admit that the codes might be broken would destroy the entire Dönitz system and it was easier to blame radar, careless talk, spies† and bad luck. In the same way, although Huff-duff was more useful to escorts than 10 centimetre radar, all losses were blamed on radar.

> Some U-boat commanders returning from patrol commented on the curious coincidence that a [wireless] transmission was so often followed by an attack, and suggested that there might be some connection. But [Naval Intelligence] could conceive of no such thing. Any U-boat commander who insisted was regarded as something of a crank.

Table 15.4. *Monthly losses in the North Atlantic, 1943.*

Month	Tonnage lost	Ships lost	U-boat losses
March	476 349	82	15
April	235 478	39	15
May	163 507	34	41

One consequence of the lifting of the Enigma black-out was to administer a bitter though effective medicine to the British code-breakers who were also responsible for the security of British codes. The response of U-Boat Command to the re-routeing of convoys showed that the main British Naval cipher used for communication between the US and Royal Navies and convoy control had been comprehensively broken by German Naval Intelligence. The Royal Navy had the humiliating experience of being lectured to on security by its US counterpart. On 10 June, German Naval Intelligence noted that FRANKFURT had fallen silent. The new codes now introduced remained unbroken and Dönitz lost a source of information which, as he said, gave him half his intelligence.

The information provided by Enigma also enabled the Allies to hunt down nine out of the ten 'Milch Cows', large submarine tankers, on which Dönitz relied for the efficient conduct of operations in more distant waters. Although at one point the British dispatched a warning that some of the American successes were 'Too true to be good', the Germans seem to have taken the losses as just another disaster among many.

To this catalogue of German problems must be added new Allied weapons† and, thanks to operational research, more effective use of old ones. It is probable that the closing of the air-gap was the most important single factor in the victory but it was the combination of factors which made the victory overwhelming.

Dönitz continued his U-boat war until the bitter end. On the whole, naval historians hold this decision to be 'correct' in the sense that the U-boat threat continued to tie down large numbers of Allied naval ships and aircraft, although others point out that the U-boat campaign itself drew heavily on limited German resources. But, whether it was correct or not in a narrow military sense, in a broad strategic sense the decision was irrelevant. In the two remaining years of the war, only 337 Allied merchant ships were sunk at the cost of 534 U-boats. (Of the 45 U-boats which took part in the March convoy battles, only 2 survived the war and the rest were sunk, most without survivors.) Meanwhile a continuous stream of convoys crossed the Atlantic bearing the men, weapons and fuel required, first for the invasion of Italy and then for the Normandy landings and the subsequent battles.

We need not speculate about what would have happened if the Battle of the Atlantic had been lost. But if victory in that battle had required even a few more months, the Normandy landings would have been delayed for a year and we enter the province of 'alternative histories'. A more demonstrative age might have celebrated such a victory with a massive piece of statuary, perhaps showing a handsome but well-draped female representing Science with the armoured God of War prostrate under her foot, or perhaps the giant figures of Blackett and Turing gazing forever over the Western Approaches. In the absence of such a monument, Figure 15.4, taken from page 379 of Volume 2 of Roskill's splendid history, is a sufficient memorial.

†In 1945 an American Intelligence Officer noted that the bookcases of the German security services 'seemed to be lined with spy novels about the diabolically clever British.'

†Including an air-dropped homing torpedo, 'Wandering Annie', developed by the Americans. Since it homed onto the cavitation produced by the submarine's propeller, the weapon could easily be countered by slowing the submarine. It was thus vital to keep the torpedo's existence secret. The first example was brought into Britain under tight security but the officer in charge relates that shortly afterwards 'I received a buff-coloured envelope with "OHMS" across the top, by ordinary post. Inside was a letter from His Majesty's Customs; they wanted to know why I had imported into the United Kingdom "packing cases containing what is believed to be some form of aerial homing torpedo for use against submarines." Why had I failed to declare them?'

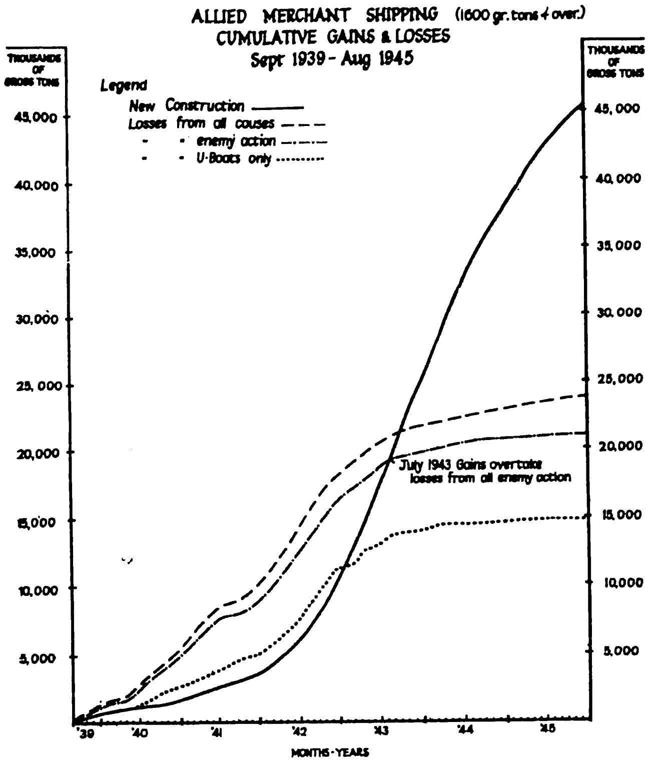


Figure 15.4: Cumulative gains and losses of shipping 1939–45.

he nations of Western
urope still maintain
ensive anti-submarine
ces. In order to train
e forces, they need
bstantial submarine
ets. In order to pay for
e submarine fleets,
y sell submarines and
marine technology
other nations. The
session of submarines
other nations increases
submarine threat
inst which it is
essary to maintain
ensive forces.
mpressive and extensive
ing procedures now
ard the security of
tchley's successor
ablishment but, as
Good who also worked
Naval Enigma observed,
was lucky that the
rity people didn't know
out Turing's
mosexuality early on,
ause if they had known,
might not have obtained
clearance and we might
e lost the war.'

CHAPTER 16

Echoes

16.1 Hard problems

At the end of the war, the British Government wished to hide two interlocked secrets — the fact that it and its American allies could read codes used by many other nations (there was a flourishing market in second-hand German Enigma machines) and the darker, greater secret, of how nearly the submarine war had ended in defeat†. Although thousands of people had worked in or with Bletchley, the secret was kept for 30 years. By the time the truth leaked out, the British had, finally, started to lose interest in their finest hour, and, in any case, there was hardly room for a homosexual pure mathematician in the pantheon of saviours of the nation‡.

However, fame, for mathematicians, consists in having their theorems remembered and their names mis-spelt. That Turing achieved this distinction in his own lifetime is revealed by the glossary of a 1953 book on computers.

> *Türing Machine.* In 1936 Dr Turing wrote a paper on the design and limitations of computing machines. For this reason they are sometimes known by his name. The umlaut is an un-earned and undesirable addition, due presumably to an impression that anything so incomprehensible must be Teutonic.

Turing also has the much rarer distinction, for a mathematician, of a first-class biography. Hodges' book [96] is a labour of love which had the unexpected, but fortunately temporary, side-effect of turning its hero into a cultural icon.

After the war, Turing worked on the development of the electronic computer foreshadowed in his Universal Machine and the later Bletchley machines. As might be expected, there was great debate at the time as to whether such machines might think, and, as might be expected from

It gives the number of ways of selecting r things from n (no attention being paid to order) and appears in the binomial expansion

$$(x+y)^n = \sum_{r=0}^{n} \binom{n}{r} x^r y^{n-r}.$$

- If x is a function of t the following are common expressions for the derivative of x at t:

$$\frac{dx}{dt} = \frac{d}{dt}(x(t)) = \dot{x}(t) = x'(t).$$

APPENDIX 3

Sources

The following tale is told of the Mullah Nasrudin.

> Jalal, an old friend of Nasrudin called one day. The Mullah said, 'I am delighted to see you after such a long time. I am just about to start on a round of visits, however. Come, walk with me, and we can talk.'
>
> 'Lend me a decent robe', said Jalal, 'because, as you see, I am not dressed for visiting.' Nasrudin lent him a very fine robe.
>
> At the first house Nasrudin presented his friend. 'This is my old companion, Jalal: but the robe he is wearing, that is mine!'
>
> On the way to the next village, Jalal said: 'What a stupid thing to say! "The robe is mine" indeed! Don't do it again.' Nasrudin promised.
>
> When they were comfortably seated at the next house, Nasrudin said: 'This is Jalal, an old friend come to visit me. But the robe: the robe is *his*!'
>
> As they left Jalal was as annoyed as before. 'Why did you say that? Are you crazy?'
>
> 'I only wanted to make amends. Now we are quits.'
>
> 'If you do not mind,' said Jalal, slowly and carefully, 'we shall say no more about the robe.' Nasrudin promised.
>
> At the third and final place of call, Nasrudin said: 'May I present Jalal, my friend. And the robe, the robe he is wearing ... but we mustn't say anything about the robe, must we?'

This book is not a work of scholarship. However, a few of my readers may wish to check some of my statements or simply to read further. This list of sources is intended to help them.

- Page ii *To judge in this [utilitarian] way ...* Quoted in [22].
- Page ii *We agreed ...* From *The Wrench* (Tiresias, page 53 of [143]) .
- Page ii *To be placed on the title-page ...* Quoted in [194].
- Page ii *Mathematicians are ...* In [3].
- Page ix *some may assert ...* In *The Essays*, Book III, Essay 12.

ever likened Lord Salisbury to a ‘lath of wood painted to look like iron.’)

- Page 258 *first with the most*, Reported saying of Nathan Bedford Forrest, a Southern cavalry commander.
- Page 258 *‘Build no more fortresses, build railways,’* ... [242], Chapter 6.
- Page 268 *Braess produced the following example* ... For references see [112].
- Page 292 *He who fights with monsters* ... Nietzsche, *Beyond Good and Evil*, Chapter IV, 146.
- Page 292 *Both direct and indirect approaches were tried* ... [37].
- Page 293 *Mathematicians are like Frenchmen* ... Maxim 1279, quoted in [163].
- Page 298 *accidents were not as frequent as might be expected.* [119].
- Page 300 *named after the accident* ... [171].
- Page 301 *estimated that it would take five years* ... [6].
- Page 301 *Studies have shown that for every six* ... [68].
- Page 304 *The author feels that* ... [122], Preface.
- Page 305 *Here a difficulty presents itself* ... [61], First Day.
- Page 311 *Hodge's splendid biography of Turing* [96],
- Page 325 *the major codes of the major powers* ... [110], page 49.
- Page 327 *followed these instructions to the letter* ... See [110], page 119.
- Page 331 *We intend to begin unrestricted submarine warfare* ... Text given in [241].
- Page 335 *We developed a very friendly feeling* ... [253], page 132.
- Page 340 *A retired banker named Burberry* ... [160], page 35.
- Page 341 *sensed something strange in an Italian intercept* ... [110], page 139.
- Page 341 *a procedure known as "gardening"* ... [94], page 122.
- Page 342 *Difficulty arises in remunerating the patentees* ... Quotations taken from [236], pages 40–1.
- Page 343 *Preventing A Code Book From Falling Into Enemy Hands.* The cartoon comes, via page 485 of [109], from the British Admiralty, *Merchant Ships Signal Book*, III.
- Page 343 *Did nothing in particular* ... Gilbert and Sullivan, *Iolanthe.*
- Page 345 *We were amazed to be presented with twenty* ... [94], page 130.
- Page 346 *the Swiss, Spanish, and Italian governments* ... According to [132].
- Page 348 *a stunning achievement* ... [110], page 66.

- Page 353 *though the cryptological agencies ... grew in size* ... [109], page 455.
- Page 353 *As far as mathematical training goes* ... [132].
- Page 362 *after the meeting, Dilly returned* ... [94], page 127.
- Page 364 *Our decodes must have given early warning* ... [253], page 96.
- Page 366 *I discovered, however, that the intercept operators* ... [253], page 93.
- Page 366 *The old procedures* ... [165], page 139.
- Page 366 *You know, the Germans don't mean you to read their stuff* ... [94], page 236.
- Page 368 *In Britain , Cambridge students* ... [110], page 280.
- Page 368 *viewed with considerable awe* ... [160], pages 77–8.
- Page 368 *There was always a sense of immense power* ... and succeeding quotations [93], page 48–52.
- Page 370 *assembled out of standard parts for special purposes* ... [109], page 440.
- Page 378 *The conditions of the work were disclosed* ... and succeeding quotations [94] Chapter 17.
- Page 379 *Helen Rance, one of the hundreds* ... [102], pages 395–6.
- Page 380 *It was possible to choose a sequence* ... [253], page 144.
- Page 380 *the British Navy reacted strongly and unfavourably* ... See [11], page 208.
- Page 381 *The oldest hath borne most* ... Shakespeare, *King Lear.*
- Page 381 At a rough estimate ... Based, for example, on the figures given on pages 216 and 217 of [110].
- Page 381 *the sense of shock* ... [94], Chapter 3.
- Page 383 *By April 1943 the average kill* ... Quoted in [248], page 444.
- Page 384 *The Admiralty ... recorded that* ... [204], Volume 2, pages 367–8.
- Page 384 *It seems not unlikely that a quarter* ... [12].
- Page 384 *poverty line for a family of five* ... Based on the discussion in [21].
- Page 384 *These, in the day when heaven was falling,* ... Housman, *Epitaph on an Army of Mercenaries.*
- Page 385 *Not only did returning U-boats always signal* ... [95], Volume 2, pages 549–50.
- Page 388 *seemed to be lined with spy novels* ... Quoted in [86], page 639.
- Page 388 *Some U-boat commanders returning from patrol* ... [258], page 250.

- Page 388 *I received a buff-coloured envelope* … Quoted in [189], pages 123–4.
- Page 391 *The nations of Western Europe* … See [198].
- Page 391 *It was lucky that the security people didn't know* … [160], page 34.
- Page 392 *supposing there were a machine* … Section 17 of the Monadology quoted in [129].
- Page 393 *It is clear, I think, that we may account* … [238], page 271.
- Page 393 *Laplace once went in form* … [47], Volume 2, pages 1–2.
- Page 398 *Shannon thought they should play music to it* … [96], page 251.
- Page 399 *into single letters using tables* … [110], Appendix.
- Page 399 *The redundancy of language* … [216].
- Page 400 *Normal infants begin to acquire real speech* … [139], Chapter 23.
- Page 407 *they swept the contents of his desk into sacks* … An exageration, but not too far from the truth, see [239].
- Page 410 *[a]t quarter past midnight* … [239], page 123.
- Page 413 *Generations pass while some trees stand* … Sir Thomas Browne, *Urn Burial (Hydriotaphia)*, Chapter V.
- Page 413 *The decay of the families of men* … [64] reprinted in [219].
- Page 417 *The Microbe is so very small* … Belloc, *The Microbe* in *Cautionary Verses.*
- Page 430 *Table 17.1* … taken from a paper of Radovich ([69], pages 110–11),
- Page 433 *Between 1964 and 1968 Norwegians invested* … [69], page 53.
- Page 435 *rapidly changed to dark wings.* Details are given in [116].
- Page 435 *[t]he identity of many plants* … Darwin [44], Chapter XI.
- Page 445 *The Indians die so easily* … [157], page 211.
- Page 445 *Two Union soldiers* … See, for example [158], Chapter 15.
- Page 445 *The worst case was presented* … [36], page 104.
- Page 446 *Our business was done at the river's brink* … Browning, *The Pied Piper of Hamelin.*
- Page 449 *In scarcely any house did only one die* … Quoted in [218], page 48.
- Page 450 *Perhaps one third of the population* … See [89] for a discussion of the English figures.

- Page 450 *not a disease of human beings at all* … [25], page 225.
- Page 450 *It is possible that we have acquired measles* … See [36].
- Page 450 *The most likely forecast* … [25], page 263.
- Page 450 *During the last two decades* … [48], Introduction.
- Page 451 *He knew the tale he had to tell* … Translated by Stuart Gilbert in the Penguin Modern Classics series.
- Page 460 *I have a cat called Socrates.* Ionesco, *Rhinoceros*, Act 1.
- Page 465 *Ah! Why, ye Gods* … Pope, *The Dunciad*, Book 2.
- Page 468 *The method of "postulating"* … [207], Chapter VII.
- Page 472 *civilisation advances by extending* … [255].
- Page 482 *checked by machine* … [247].
- Page 488 *I am very honoured to be the first recipient* … [156].
- Page 494 *At a literary dinner* … From *The Life and Letters of Lord Macaulay* by G. O. Trevelyan, Volume II, Chap.XII.
- Page 495 *of no writing — except perhaps Henry James's* … [75].
- Page 501 *Insiders pronounce the χ of TEX* … Chapter 1 of [122].
- Page 501 *man's reach* … Browning, *Andrea del Sarto.*
- Page 506 *When I was a rather disrespectful student* … [140], Volume 5, pages 310–11.
- Page 508 *I am Alpha and Omega,* Revelation 1:7
- Page 511 *Jalal, an old friend* … Told as *The Robe* in [214].
- Page 517 *lath of wood* … See the second edition of the *Oxford Dictionary of Quotations.*
- Page 521 *A man will turn over half a library to make one book.* Boswell, *Life of Johnson* April, 1775.

BIBLIOGRAPHY

[1] M. Abramowitz and I. A. Stegun. *Handbook of Mathematical Functions.* Dover, New York, 1965. The various Dover printings of this are reprints of various Government printings.

[2] F. S. Acton. *Numerical Methods That Work.* Harper and Row, New York, 1970.

[3] D. J. Albers and G. L. Anderson, editors. *Mathematical People.* Birkhäuser, Boston, 1985.

[4] R. M. Anderson and R. M. May. *Infectious Diseases of Humans.* OUP, Oxford, 1991.

[5] V. I. Arnol'd. *Catastrophe Theory.* Springer, Berlin, 1983. Translated from the Russian: Later editions contain interesting extra material.

[6] C. Arthur. Pressurised managers blamed for ambulance failure. *New Scientist,* page 5, 6 March 1993.

[7] O. M. Ashford. *Prophet or Professor? (The Life and Work of Lewis Fry Richardson).* Adam Hilger, Bristol, 1985.

[8] N. T. J. Bailey. *The Mathematical Theory of Epidemics.* Charles Griffin, London, 1957.

[9] W. W. Rouse Ball and H. S. M. Coxeter. *Mathematical Recreations and Essays.* University of Toronto, Toronto, 12th edition, 1974.

[10] G. K. Batchelor. G. I. Taylor. *Obituary Notices of Fellows of the Royal Society,* 30:565–633, 1985.

[11] P. Beesly, editor. *Very Special Intelligence.* Sphere, London, revised edition, 1978.

[12] C. B. A. Behrens. *Merchant Shipping and the Demands of War.* HMSO, London, 1955.

[13] E. T. Bell. *Men of Mathematics.* Simon and Schuster, New York, 1937. 2 vols.

[14] E. R. Berlekamp, J. H. Conway, and R. K. Guy. *Winning Ways.* Academic Press, London, 1982. 2 vols.

[15] G. Birkhoff. *Hydrodynamics.* Princeton University Press, Princeton, N. J., 1950.

[16] G. Birkhoff and S. MacLane. *A Survey of Modern Algebra.* Macmillan, New York, revised edition, 1953.

[17] P. M. S. Blackett. *Studies of War.* Oliver and Boyd, Edinburgh, 1962.

[18] M. Born. *Einstein's Theory of Relativity.* Dover, New York, revised edition, 1962.

[19] A. Bourke. *The Visitation of God? The Potato and the Irish Famine.* Lilliput Press, Dublin, 1993.

[20] E. G. Bowen. *Radar Days.* Adam Hilger, Bristol, 1987.

[21] A. Briggs. *A Social History of England.* Weidenfeld and Nicholson, London, 1983.

[22] W. K. Bühler. *Gauss, A Biographical Study.* Springer, Berlin, 1981.

[23] J. P. Bunker, B. A. Barnes and F. Mosteller, editors. *Costs, Risks and Benefits of Surgery.* OUP, Oxford, 1977.

[24] J. C. Burkill. *A First Course in Mathematical Analysis.* CUP, Cambridge, 1962.

[25] M. Burnett and D. O. White. *Natural History of Infectious Disease.* CUP, Cambridge, 4th edition, 1971.

[26] R. Burns, editor. *Radar Development to 1945.* Peter Peregrinus (on behalf of IEE), London, 1988.

[27] D. M. Campbell and J. C. Higgins. *Mathematics: People, Problems, Results.* Wadsworth, Belmont, Calif, 1984. 3 vols.

[28] CAST. Preliminary Report: Effect of encaide and flecainide on mortality in a randomised trial of arrythmia suppression after myocardial infarction. *New England Journal of Medicine,* 312:406–12, 1989.

[29] Somerset De Chair, editor. *Napoleon's Memoirs.* Faber and Faber, London, 1958.

[30] A. Charlesworth. Infinite loops in computer programs. *Mathematics Magazine,* 52:284–91, 1979.

[31] G. Cherbit, editor. *Fractals.* Wiley, New York, 1991.

[32] L. Childs. *A Concrete Introduction To Higher Algebra.* Springer, Berlin, 1989.

[33] W. S. Churchill. *The Second World War.* Cassel, London, 1948-53. 6 vols.

[34] K. Clark. *Leonardo da Vinci.* Penguin, Harmondsworth, England, 1989. Revised Pelican edition of a work first published by CUP in 1939.

[35] R. W. Clark. *Tizard.* Methuen, London, 1965.

[36] A. Cliff, P. Hagett, and M. Smallman-Raynor. *Measles, An Historical Geography.* OUP, Oxford, 1988.

[37] W. H. Cockroft *et al. Mathematics Counts.* Her Majesty's Stationery Office, London, 1982. Report of a Committee of Enquiry into the Teaching of Mathematics in Schools.

[38] E. Colerus. *From Simple Numbers to the Calculus.* Heinemann, London, 1955. English translation from the German.

[39] F. M. Cornford. *Microcosmographia Academica.* Bowes and Bowes, Cambridge, 2nd edition, 1922.

[40] R. Courant and H. Robbins. *What is Mathematics?* OUP, Oxford, 1941.

[41] H. S. M. Coxeter. *Introduction to Geometry.* Wiley, New York, 1961.

[42] H. M. Cundy and A. P. Rollett. *Mathematical Models.* OUP, Oxford, 1951.

[43] J. Darracott. *A Cartoon War.* Leo Cooper, London, 1989.

[44] C. Darwin. *On the Origin of Species by Means of Natural Selection.* Murray, London, 1859.

[45] H. Davenport. *The Higher Arithmetic.* Hutchinson, London, 1952.

[46] P. J. Davies and R. Hersh. *The Mathematical Experience.* Birkhäuser, Boston, 1981.

[47] A. De Morgan. *A Budget of Paradoxes.* Books for Libraries Press, Freeport, New York, second, reprinted edition, 1969.

[48] R. S. Desowitz. *The Malaria Capers.* Norton, New York, 1991.

[49] K. Dönitz. *Memoirs.* Weidenfeld and Nicholson, London, 1954. English translation.

[50] S. Drake. *Galileo at Work.* University of Chicago Press, Chicago, 1978.

[51] C. V. Durell. *General Arithmetic for Schools.* G.Bell, London, 1936.

[52] A. Einstein and L. Infeld. *The Evolution of Physics.* CUP, Cambridge, 1938.

[53] A. Einstein, H. A. Lorentz, H. Weyl and H. Minkowski. *The Principle of Relativity.* Dover, 1952. A collection of papers first published in English by Methuen in 1923.

[54] R. J. Evans. *Death in Hamburg.* OUP, Oxford, 1987.

[55] J. Fauvel and J. Gray, editors. *History of Mathematics: A Reader.* Macmillan, Basingstoke, England, 1987.

[56] W. Feller. *An Introduction to Probability Theory and its Applications,* volume I. Wiley, New York, 3rd edition, 1968.

[57] R. P. Feynman. *The Character of Physical Law.* BBC Books, London, 1965.

[58] R. P. Feynman. *QED, The Strange Theory of Light and Matter.* Princeton University Press, Princeton, N. J., 1985.

[59] R. P. Feynman. *Surely You're Joking, Mr Feynman!* W. W. Norton, New York, 1985.

[60] R. P. Feynman *et al. The Feynman Lectures on Physics.* Addison-Wesley, Reading, Mass., 1963. 3 vols.

[61] Galileo. *Dialogues Concerning Two New Sciences.* Macmillan, London, 1914. Translated by H. Crew and A. De Salvio.

[62] Galileo. *Dialogues Concerning the Two Chief World Systems.* University of California Press, Berkeley, Calif, 1953. Translated by S. Drake.

[63] Galileo. *Discoveries and Opinions of Galileo.* Anchor Books (Doubleday), New York, 1957. Translated by S. Drake.

[64] F. Galton and H. W. Watson. On the probability of the extinction of families. *Journal of The Anthropological Institute,* 4:138–44, 1874.

[65] M. Gardner. *Fads and Fallacies in the Name of Science.* Dover, New York, 1957.

[66] M. Gardner. *The Flight of Peter Fromm.* William Kaufman, Los Altos, California, 1973.

[67] M. Gardner. *Penrose Tiles to Trapdoor Ciphers.* W. H. Freeman, New York, 1989.

[68] W. W. Gibbs. Software's chronic crisis. *Scientific American,* pages 72–81, September 1994.

[69] M. H. Glantz and J. D. Thompson, editors. *Resource Management and Environmental Uncertainty.* Wiley, New York, 1989.

[70] E. Gold. L. F. Richardson. *Obituary Notices of Fellows of the Royal Society,* 9:217–35, 1954.

[71] M. Goosens, F. Mittelbach, and A. Samarin. *The LaTeX Companion.* Addison-Wesley, Reading, Mass., 1994.

[72] S. J. Gould. *Ever Since Darwin.* Penguin, Harmondsworth, England, 1980.

[73] M. Gowing. *Independence and Deterrence,* volume I. Macmillan, London, 1974.

[74] R. L. Graham, D. E. Knuth, and O. Patashnik. *Concrete Mathematics.* Addison-Wesley, Reading, Mass., 1979. The second edition contains interesting new material.

[75] G. Greene. The austere art. *The Spectator,* 165:682, 1940.

[76] J. Gross. *The Rise and Fall of the Man of Letters.* Weidenfeld and Nicholson, London, 1969.

[77] J. Grossman, editor. *The Chicago Manual of Style.* Chicago University Press, Chicago, 14th edition, 1993.

[78] J. Hadamard. *The Psychology of Invention in the Mathematical Field.* Princeton University Press, Princeton, N. J., 1945.

[79] J. B. S. Haldane. *On Being the Right Size.* OUP, Oxford, 1985.

[80] P. R. Halmos. *Naive Set Theory.* Van Nostrand, Princeton, N. J., 1960.

[81] P. R. Halmos. *I Want to be a Mathematician.* Springer, Berlin, 1985.

[82] J. M. Hammersley. On the enfeeblement of mathematical skills by 'modern mathematics' and by similar soft intellectual trash in schools and universities. *Bulletin of the Institute of Mathematics and its Applications*, 4:68–85, 1968.

[83] G. H.' Hardy. *A Course of Pure Mathematics.* CUP, Cambridge, 1914.

[84] G. H. Hardy. *A Mathematician's Apology.* CUP, Cambridge, 1940.

[85] G. H. Hardy and E. M. Wright. *An Introduction to the Theory of Numbers.* OUP, Oxford, 1938.

[86] A. D. Harvey. *Collision of Empires.* Phoenix, London, paperback edition, 1994.

[87] J. Hašek. *The Good Soldier Švejk.* Penguin, Harmondsworth, England, 1973. English translation by C. Parrott.

[88] M. Hastings. *Bomber Command.* Michael Joseph; London, 1979.

[89] J. Hatcher. *Plague, Population and the British Economy 1348–1530.* MacMillan, London, 1977.

[90] T. L. Heath. *The Works of Archimedes.* Dover, New York, reprint edition, 1953.

[91] T. L. Heath. *The Thirteen Books of Euclid's 'Elements'.* Dover, New York, reprint edition, 1956. 3 vols.

[92] H. Hertz. *Electric Waves.* Dover, New York, reprint edition, 1963. English translation by D. E. Jones first published in 1893.

[93] P. J. Hilton. Algebra and logic, Lecture notes in mathematics 450. In J. N. Crossley, editor, *Algebra and Logic*, Berlin, 1975. Springer.

[94] F. H. Hinsley and A. Stripp, editors. *Codebreakers.* OUP, Oxford, paperback edition, 1994.

[95] F. H. Hinsley, E. E. Thomas, C. F. G. Ransome and R. C. Knight. *British Intelligence in the Second World War.* HMSO, London, 1979-88. 5 volumes.

[96] A. Hodges. *Alan Turing, The Enigma of Intelligence.* Hutchinson, London, 1983.

[97] M. Howell and P. Ford. *The Ghost Disease.* Penguin, Harmondsworth, England, 1986.

[98] D. Howse. *Radar At Sea.* Macmillan, London, 1993.

[99] D. Huff. *How to Lie with Statistics.* W. W. Norton, New York, 1954.

[100] ISIS-2 Collaborative Group. Randomised trial of intravenous streptokinase, oral aspirin, both, or neither among 17 187 cases of suspected acute myocardial infarction. *The Lancet*, pages 349–60, August 1988.

[101] ISIS-3 Collaborative Group. A randomised comparison of streptokinase versus tissue plasminogen activator versus anistreptase and of aspirin plus heparin versus aspirin alone among 41 299 cases of suspected acute myocardial infarction. *The Lancet*, 339:753–70, March 1992.

[102] B. Johnson. *The Secret War.* BBC Publications, London, 1978.

[103] R. V. Jones. Winston Churchill. *Obituary Notices of Fellows of the Royal Society*, 12:35–106, 1966.

[104] R. V. Jones. *Most Secret War.* Hamish Hamilton, London, 1978.

[105] R. V. Jones. *Reflections On Intelligence.* Mandarin, London, paperback edition, 1990.

[106] C. M. Jordan. *Cours d'Analyse de l'Ecole Polytechnique.* Gauthier-Villars, Paris, 2nd edition, 1893–6. 3 vols.

[107] M. Kac. *Selected Papers.* MIT, Cambridge, Mass, 1979.

[108] J.-P. Kahane and R. Salem. *Ensembles parfaits et séries trigonométriques.* Herman, Paris, 1963.

[109] D. Kahn. *The Codebreakers.* Macmillan, 1967.

[110] D. Kahn. *Seizing the Enigma.* McGraw Hill, 1982.

[111] J. Keegan. *The Price of Admiralty.* Hutchinson, London, 1988.

[112] F. P. Kelly. Network routing. *Philosophical Transactions of the Royal Society A*, 337:343–67, 1991.

[113] D. Kendall *et al.* Obituary of A. N. Kolmogorov. *Bulletin of the London Mathematical Society*, 22:31–100, 1990.

[114] D. G. Kendall. Branching processes since 1873. *Journal of The London Mathematical Society*, 41:385–406, 1966.

[115] D. G. Kendall. The genealogy of genealogy .... *Bulletin of The London Mathematical Society*, X:225–53, 1975.

[116] B. Kettlewell. *The Evolution of Melanism.* OUP, Oxford, 1973.

[117] C. Kinealy. *This Great Calamity.* Gill and Macmillan, Dublin, 1994.

[118] J. F. C. Kingman. The thrown string. *Journal of the Royal Statistical Society, Series B*, 44(2):109–38, 1982. With discussion.

[119] G. M. Kitchenside and A. Williams. *British Railway Signalling.* Ian Allan, Shepperton, Surrey, UK, 3rd edition, 1979.

[120] M. Kline. *Mathematical Thought from Ancient to Modern Times.* OUP, Oxford, 1972.

[121] D. E. Knuth. *The Art of Computer Programming.* Addison-Wesley, Reading, Mass., 1968–73. 3 volumes. This was intended to be 7 volumes. As I go to press there are persistent rumours that Knuth will take up the task again.

[122] D. E. Knuth. *The TeXbook.* Addison-Wesley, Reading, Mass., 1984.

[123] D. E. Knuth. *Computers and Typesetting.* Addison-Wesley, Reading, Mass., 1986. 5 volumes. Volume A of the set is *The TeXbook.*

[124] A. H. Koblitz. *A Convergence of Lives.* Birkhäuser, Boston, 1983.

[125] N. Koblitz. *A Course in Number Theory and Cryptography.* Springer, Berlin, 1987.

[126] A. N. Kolmogorov. *Selected Works.* Kluwer Academic Publishers, Dordrecht, The Netherlands, 1991. 3 vols. Annotated translation of the Russian.

[127] A. G. Konheim. *Cryptography.* Wiley, New York, 1981.

[128] S. Körner. *The Philosophy of Mathematics.* Hutchinson, London, 1960.

[129] S. Körner. *Fundamental Questions of Philosophy.* Penguin, Harmondsworth, England, 1969.

[130] T. W. Körner. Uniqueness for trigonometric series. *Annals of Mathematics*, 126:1–34, 1987.

[131] S. Kovalevskaya. *A Russian Childhood.* Springer, Berlin, 1978. Translated from the Russian by B. Stillman.

[132] W. Kozaczuk. *Enigma, How the German Cypher Machine was Broken.* Arms and Armour, London, 1984. Translated from the Polish by C. Kasparek.

[133] S. G. Krantz. *How to Teach Mathematics: A Personal Perspective.* AMS, Providence, Rhode Island, 1993.

[134] E. Laithwaite. *Invitation to Engineering.* Blackwell, Oxford, 1984.

[135] L. Lamport. *LaTeX, A Documement Preparation System.* Addison-Wesley, Reading, Mass., 2nd edition, 1994.

[136] F. W. Lanchester. *Aircraft in Warfare.* Constable, London, 1916.

[137] E. Landau. *Foundations of Analysis.* Chelsea, New York, 1951. Translated from the German by F. Steinhardt.

[138] H. Lauwrier. *Fractals.* Princeton University Press, Princeton, N. J., 1991. Translated from the Dutch.

[139] P. Leach. *Babyhood.* Penguin, Harmondsworth, England, 2nd edition, 1983.

[140] H. Lebesgue. *Oeuvres Scientifiques.* L'Enseignement Mathématique, Geneva, 1972–3. 5 vols.

[141] I. Lengyel, S. Kádár and I. R. Epstein. Transient Turing structures in a gradient-free closed system. *Science*, 259:493–5, 1993.

[142] M.-C. Van Leunen. *A Handbook for Scholars.* Alfred A. Knopf, Inc., New York, 1978.

[143] P. Levi. *The Wrench.* Abacus (part of the Penguin group), London, 1988. English translation by W. Weaver.

[144] C. E. Linderholm. *Mathematics made Difficult.* Wolfe Publishing Ltd, London, 1971.

[145] J. E. Littlewood. *A Mathematician's Miscellany.* CUP, Cambridge, 2nd edition, 1985. Editor B.Bollobás.

[146] J. L. Locher *et al.* *Escher.* Thames and Hudson, London, 1982. Translated from the Dutch. Contains a complete illustrated catalogue of his graphic works.

[147] J. D. Logan. *Applied Mathematics.* Wiley, New York, 1987.

[148] E. N. Lorenz. *The Essence of Chaos.* University of Washington Press, 1994.

[149] B. Lovell. P. M. S. Blackett. *Obituary Notices of Fellows of the Royal Society*, 21:1–115, 1975.

[150] J. Luvaas. *The Military Legacy of the Civil War.* Kansas University Press, Kansas, 1988.

[151] C. H. Macgillavry. *Symmetry Aspects of M. C. Escher's Periodic Drawings.* A. Oosthoek's Uitgeversmaatschappij NV for the International Union of Crystallography, Utrecht, 1965.

[152] A. J. Marder. *From the Dreadnought to Scapa Flow.* OUP, Oxford, 1961–70. 5 vols.

[153] E. Marshall, editor. *Longman Crossword Key.* Longman, Harlow, 1982.

[154] E. A. Maxwell. *Fallacies in Mathematics.* CUP, Cambridge, 1959.

[155] J. C. Maxwell. *Matter and Motion.* Dover, New York, 1991. Reprint of the 1920 edition, the first edition was published in 1877.

[156] D. McDuff. Satter prize acceptance speech. *Notices of the AMS*, 38(3):185–7, March 1991.

[157] W. H. McNeill. *Plagues and Peoples.* Blackwell, Oxford, 1976.

[158] J. M. McPherson. *Battle Cry of Freedom.* Blackwell, Oxford, 1993.

[159] K. Menninger. *Number Words and Number Symbols.* MIT Press, Cambridge, Mass, 1969.

[160] N. Metropolis, J. Howlett, and Gian-Carlo Rota, editors. *A History of Computing in the Twentieth*

Century. Academic Press, London, 1980.

[161] A. A. Michelson. *Light Waves and Their Uses.* Chicago University Press, Chicago, 1903.

[162] Y. Mikami. *The Development of Mathematics in China and Japan.* Open Court, Chicago, 1914. There is a Chelsea reprint.

[163] R. E. Moritz. *On Mathematics and Mathematicians.* Dover, New York, 1958. Reprint of the original 1914 edition.

[164] R. J. Morris. *Cholera 1832.* Croom Helm, London, 1976.

[165] M. Muggeridge. *Chronicles of Wasted Time*, volume 2. Collins, London, 1973.

[166] C. D. Murray. The physiological principle of minimum work (Part I). *Proceedings of the National Acadamy of Sciences of the USA*, 12:207–14, 1926.

[167] J. D. Murray. *Mathematical Biology.* Springer, Berlin, 1989.

[168] J. R. Newman, editor. *The World of Mathematics.* Simon and Schuster, New York, 1956. 4 vols. Reprinted by Tempus Books, Washington in 1988.

[169] I. Newton. *Principia.* University of California Press, Berkeley, Calif, 1936. Motte's translation revised by Cajori.

[170] Nobel Foundation. *Nobel Lectures in Physics 1942–62*, Amsterdam, 1964. Elsevier.

[171] O. S. Nock. *Historic Railway Disasters.* Ian Allan, Shepperton, Surrey, UK, 1966.

[172] P. Padfield. *Dönitz.* Gollancz, London, paperback edition, 1993.

[173] A. Pais. *Subtle Is the Lord ... .* OUP, Oxford, 1982.

[174] A. Pais. *Inward Bound.* OUP, Oxford, 1986.

[175] D. Pedoe. *The Gentle Art of Mathematics.* English Universities Press, London, 1958.

[176] H.-O. Peitgen and P. H. Richter. *The Beauty of Fractals.* Springer, Berlin, 1986.

[177] R. Penrose. *The Emperor's New Mind.* OUP, Oxford, 1989.

[178] Petrarch. On his own ignorance and that of many others. In *The Renaissance Philosophy of Man.* Chicago University Press, Chicago, 1948.

[179] S. Pinker. *The Language Instinct.* Penguin, Harmondsworth, England, 1994.

[180] Plato. *Meno.* Penguin, Harmondsworth, England, 1956. Translated by W. K. Guthrie.

[181] G. W. Platzman. A retrospective view of Richardson's book on weather prediction. *Bulletin of the American Meteorological Society*, 48:514–50, 1967.

[182] G. W. Platzman. Richardson's weather prediction. *Bulletin of the American Meteorological Society*, 49:496–500, 1968.

[183] H. Poincaré. *Science and Method.* Dover, New York, reprint edition, 1952. Translated by F.Maitland.

[184] G. Pólya. *Mathematics and Plausible Reasoning.* Princeton University Press, Princeton, N. J., 1954. 2 vols.

[185] G. Pólya. *How to Solve It.* Princeton University Press, Princeton, N. J., 2nd edition, 1957.

[186] G. Pólya. *Mathematical Discovery.* Wiley, New York, 1962. 2 vols.

[187] A. E. Popham. *The Drawings of Leonardo da Vinci.* Cape, London, 1946.

[188] W. Poundstone. *Prisoner's Dilemma.* Doubleday, New York, 1992.

[189] A. Price. *Aircraft versus Submarine.* William Kimber, London, 1973.

[190] A. Price. *Instruments of Darkness.* Granada, London, 1979.

[191] S. Pritchard. *The Radar War.* Patrick Stephens, Wellingborough, Northamtonshire, England, 1989.

[192] H. Rademacher and O. Toeplitz. *The Enjoyment of Mathematics.* Princeton University Press, Princeton, N. J., 1957.

[193] A. S. Ramsey. *Dynamics (Part 1).* CUP, Cambridge, 1929.

[194] J. H. Randall. *The Making of the Modern Mind.* The Riverside Press, Cambridge, Massachusetts, 1940.

[195] E. Raymond. *The New Hacker's Dictionary.* MIT Press, Cambridge, Mass, 1991.

[196] J. Reader. *Missing Links.* Penguin, Harmondsworth, England, 2nd edition, 1988.

[197] C. Reid. *Hilbert.* Springer, Berlin, 1970.

[198] D. J. Revelle and L. Lumpe. Third World submarines. *Scientific American*, pages 16–21, August 1994.

[199] L. F. Richardson. *Weather Prediction by Numerical Process.* CUP, Cambridge, 1922.

[200] L. F. Richardson. *Arms and Insecurity.* Boxwood, Pittsburg, 1960.

[201] L. F. Richardson. *Statistics of Deadly Quarrels.* Boxwood, Pittsburg, 1960.

[202] L. F. Richardson. *Collected Works.* CUP, Cambridge, 1993. 2 vols.

[203] C. E. Rosenberg. *The Cholera Years.* University of Chicago Press, Chicago, 1962.

[204] S. W. Roskill. *The War At Sea, 1939–1945.* HMSO, London, 1954–61. 3 volumes in 4 parts.

[205] A. P. Rowe. *One Story of Radar.* CUP, Cambridge, 1948.

[206] M. J. S. Rudwick. *The Great Devonian Controversy.* University of Chicago Press, Chicago, 1985.

[207] B. Russell. *Introduction to Mathematical Philosophy.* George Allen and Unwin, London, 1919.

[208] T. Sandler and K. Hartley. *The Economics of Defence.* CUP, Cambridge, 1995.

[209] Admiral R. Scheer. *Germany's High Sea Fleet in the World War.* Cassell, London, 1920.

[210] P. A. Schillp, editor. *Albert Einstein: Philosopher-Scientist.* Library of Living Philosophers, La Salle, Ill, 1949.

[211] K. Schmidt-Nielsen. *Scaling.* CUP, Cambridge, 1984.

[212] W. A. Schocken. *The Calculated Confusion of Calendars.* Vantage Press, New York, 1976.

[213] M. R. Schroeder. *Number Theory in Science and Communication.* Springer, Berlin, 1984.

[214] I. Shah. *The Exploits of the Incomparable Mulla Nasrudin.* Jonathan Cape, London, 1966.

[215] C. E. Shannon. *Collected Papers.* IEE Press, 445 Hoes Lane, PO Box 1331, Piscataway, NJ, 1993.

[216] C. E. Shannon and W. Weaver. *The Mathematical Theory of Communication.* University of Illinois Press, Urbana, Ill, 1949.

[217] R. Sheckley. *Dimension of miracles.* Dell, New York, 1968.

[218] J. F. D. Shrewsbury. *A History of the Bubonic Plague in the British Isles.* CUP, Cambridge, 1971.

[219] D. Smith and N. Keyfitz. *Mathematical Demography.* Springer, Berlin, 1977.

[220] J. Maynard Smith. *Mathematical Ideas in Biology.* CUP, Cambridge, 1968.

[221] C. P. Smyth. *Our Inheritance in the Great Pyramid.* Alexander Strahan and Co., London, 1864.

[222] J. Snow. *Snow on Cholera.* The Commonwealth Fund, New York, 1936. Facsimile Reprint.

[223] South West Thames Regional Health Authority, 40 Eastbourne Terrace, London W2 3QR. *Report of the Inquiry into the London Ambulance Service*, 1993.

[224] M. Spivak. *Calculus.* Bejamin, New York, 1967.

[225] M. D. Spivak. *The Joy of TEX.* AMS, Providence, Rhode Island, 2nd edition, 1990.

[226] I. N. Steenrod, P. R. Halmos, *et al. How to Write Mathematics.* AMS, Providence, Rhode Island, 1973.

[227] H. Steinhaus. *Mathematical Snapshots.* OUP, New York, 3rd edition, 1969.

[228] I. N. Stewart. *Galois Theory.* Chapman and Hall, London, 1973.

[229] I. N. Stewart. *Game, Set and Math.* OUP, Oxford, 1989.

[230] W. Stukeley. *Memoirs of Sir Isaac Newton's Life.* Taylor and Francis, Red Lion Court, Fleet Street, London, 1936.

[231] J. L. Synge. Letter to the editor. *The Mathematical Gazette*, LII:165, February 1968.

[232] G. I. Taylor. *Scientific Papers of Sir Geoffrey Ingram Taylor.* CUP, Cambridge, 1958.

[233] G. I. Taylor. The present position in the theory of turbulent diffusion. *Advances In Geophysics*, 6:101–11, 1959.

[234] G. I. Taylor. Aeronautics before 1919. *Nature*, 233:527–9, 1971.

[235] G. I. Taylor. The history of an invention. *Eureka*, 34:3–6, 1971. c/o Business Manager, Eureka, The Arts School, Bene't Street, Cambridge, England.

[236] J. Terraine. *The Right of the Line.* Hodder and Stoughton, London, 1985.

[237] J. Terraine. *Business in Great Waters.* Leo Cooper Ltd, London, 1989.

[238] D. W. Thompson. *On Growth and Form.* CUP, Cambridge, 1966. This is an abridged edition edited by J. T. Bonner.

[239] T. M. Thompson. *From Error-Correcting Codes through Sphere Packings to Simple Groups.* Mathematical Association of America, Washington, 1983.

[240] J. Thurber. *The Beast in Me.* Hamish Hamilton, London, 1949.

[241] B. W. Tuchman. *The Zimmermann Telegram.* Constable, London, 1959.

[242] B. W. Tuchman. *August 1914.* Constable, London, 1962.

[243] E. R. Tufte. *The Visual Display of Quantitative Information.* Graphics Press, PO Box 430, Cheshire, Connecticut 06410, 1982.

[244] E. R. Tufte. *Envisioning Information.* Graphics Press, PO Box 430, Cheshire, Connecticut 06410, 1990.

[245] A. M. Turing. On computable numbers with an application to the Entscheidungsproblem. *Proceedings of the London Mathematical Society (2)*, 42:230–65, 1937. There are some minor corrections noted in the next volume of the *Proceedings*.

[246] A. M. Turing. *Collected Works.* North Holland, Amsterdam, 1992. 3 vols.

[247] L. S. van B. Jutting. *Checking Landau's "Grundlagen" in the AUTOMATH System.* Mathematisch Centrum, PO Box 4079, 1009 AB Amsterdam, The Netherlands, 1979.

[248] D. Van der Vat. *The Atlantic Campaign.* Hodder and Stoughton, London, 1988.

[249] D. Van der Vat. *The Pacific Campaign.* Hodder and Stoughton, London, 1991.

[250] S. Vogel. *Vital Circuits.* OUP, Oxford, 1992.

[251] C. H. Waddington. *OR in World War 2.* Elek Science, London, 1973.

[252] D. W. Waters. The science of admiralty. *The Naval Review*, LI:395–410, 1963. Continued in Volume LII, 1964, on pages 15–26, 179–94, 291–309 and 423–37.

[253] G. Welchman. *The Hut Six Story*. Allen Lane, London, 1982.

[254] R. S. Westfall. *Never At Rest*. CUP, Cambridge, 1980.

[255] A. N. Whitehead. *An Introduction to Mathematics*. Williams and Norgate, London, 1911.

[256] C. M. Will. *Was Einstein Right?* OUP, Oxford, 1988.

[257] D. Wilson. *Rutherford*. Hodder and Stoughton, London, 1983.

[258] J. Winton. *Convoy*. Michael Joseph, London, 1983.

[259] A. Wood. *The Physics of Music*. Methuen, London, 1944.

P. 31. Victory has many fathers
while defeat is an orphan.

Additional bibliography
(added at reprinting)

[260] J. D. Altringham. *Bats, Biology and Behaviour*. OUP, Oxford, 1996.

[261] G. I. Barenblatt. *Scaling, Self-similarity and Intermediate Asymptotics*. CUP, Cambridge, 1996.

[262] G. K. Batchelor. Kolmogoroff's theory of locally isotropic turbulence. *Proceedings of the Cambridge Philosophical Society*, 43:533–59, 1947.

[263] G. A. Grätzer. *Math into LaTeX*. Birkhäuser, Boston, 1996.

[264] S. H. Lui. An interview with Vladimir Arnol'd. *Notices of the AMS*, 44(3):432–8. April 1997.

INDEX