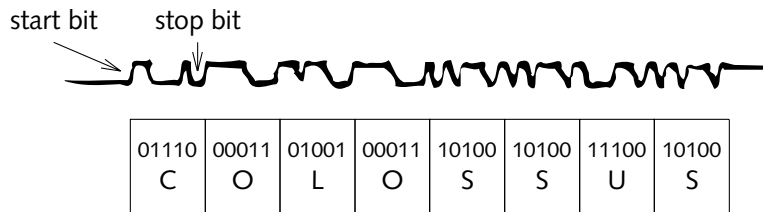


UNDULATOR DETECTION OF LORENZ CIPHER 5-HOLE TELEPRINTER CODES

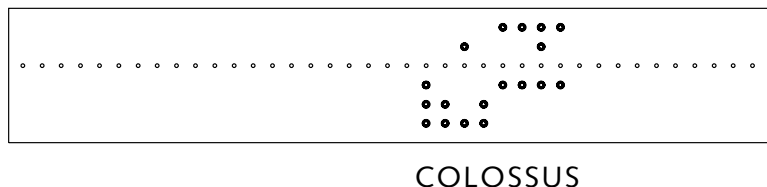
Radio reception of broadcast Lorenz-cipher traffic (at the Knockholt "Y Station" in Kent) was beset with difficulties. Transmission of the signals was directional and was pointed away from the UK. Signals were often faint and distorted. It was soon found that the best way to record the signals was via an ink trace on a sheet of paper, using technology similar to that employed for FAX.

Note that signals for one and zero were shown above and below an imaginary central line with '0' being signalled above the line and '1' below. Just as in ASCII serial line transmission, some 20 years later, the signal clock at the receiving end was turned on by a start bit immediately preceding the character and turned off by a stop bit at the end. In the case of 5-hole Lorenz traffic the start bit was a zero and the stop bit was a one. To ensure accurate detection the pulse length for the stop bit was lengthened very slightly, to be effectively "1.5 bits".

The diagram below shows a reconstructed undulator trace for the text message "COLOSSUS". In the boxes below the trace are shown the 5-bit code and the corresponding character



If reception conditions were good the above signal could be fed—directly and in parallel—with the undulator—to a teleprinter and to a tape punch. The punched output of the text 'COLOSSUS', rendered in 5-hole teleprinter code, is shown below.



If reception conditions were bad then teleprinter and tape punch were turned off. The undulator trace was then painstakingly analysed and annotated before being keyed in, by hand, to produce a 5-hole tape and a printout. After further checking the tape was relayed twice, over secure land line, to Bletchley Park (BP). If both of these transmissions resulted in identical received messages at BP then the intercept was deemed "good" and passed on to the cryptanalysts. For secure storage and archival purposes, hard copies of all materials were sent by motorcycle courier from Knockholt to BP.

Acknowledgements

The above material has been adapted from the following reference:

1. B. Jack Copeland (and others), *Colossus* (chapters 3 and 7), Oxford University Press, 2006.

Teleprinter (Baudot-Murray) Code

Binary code	Mark/space notation	Letter Shift mode	Figure Shift mode	Bletchley park notation
00000	- - - - -	NUL	NUL	/
00001	- - - - x	T	5	T
00010	- - - x -	CR	CR	3
00011	- - - x x	O	9	O
00100	- - x - -	word space	word space	9
00101	- - x - x	H	# (£)	H
00110	- - x x -	N	, (comma)	N
00111	- - x x x	M	. (full stop)	M
01000	- x - - -	LF	LF	4
01001	- x - - x	L)	L
01010	- x - x -	R	4	R
01011	- x - x x	G	@	G
01100	- x x - -	I	8	I
01101	- x x - x	P	0	P
01110	- x x x -	C	:	C
01111	- x x x x	V	=	V
10000	x - - - -	E	3	E
10001	x - - - x	Z	+	Z
10010	x - - x -	D	WRU (who are you?)	D
10011	x - - x x	B	?	B
10100	x - x - -	S	' (apostrophe)	S
10101	x - x - x	Y	6	Y
10110	x - x x -	F	%	F
10111	x - x x x	X	/	X
11000	x x - - -	A	- (dash)	A
11001	x x - - x	W	2	W
11010	x x - x -	J	BEL	J
11011	x x - x x	Figure Shift	(none)	+ or 5
11100	x x x - -	U	7	U
11101	x x x - x	Q	1	Q
11110	x x x x -	K	(K
11111	x x x x x	(none)	Letter Shift	- or 8

BREAKING SEAN'S SECRET MESSAGE

Let us suppose that Sean has sent out a secret message (**C1**), using an XOR (Vernam/Lorenz) cipher to XOR a random 5-bit key character to each 5-bit plaintext character. The first attempt failed to be received correctly so a repeat transmission was requested using exactly the same key. The second received ciphertext (**C2**) is shorter than the first so clearly the message has probably been abbreviated.

In what follows the various streams of characters are broken up into groups of five to aid visibility (just as was done, at Bletchley Park, for Enigma cipher streams sent in Morse code). Following Bletchley Park (BP) notation, a genuine word space is signalled by a **9**, a null character by **/** and a change into figure shift by **+**

Remember **C1 = P1 ⊕ K** where **K** is the key and '⊕' means XOR from now on. Similarly **C2 = P2 ⊕ K**

Now XOR these two equations together: **C1 ⊕ C2 = P1 ⊕ P2 ⊕ K ⊕ K**

But **K ⊕ K** cancels out to nothing. So we now have: **C1 ⊕ C2 = P1 ⊕ P2 = D**

This is telling us that if we form **D** by XORing the two cipher texts, then this same **D** also represents the two plaintexts (**P1** and **P2**) XORed together. So all we need to do is to XOR plausible pieces of plaintext (**P1**, say) with **D** and note whether this guess gives equally plausible plaintext for **P2**. We find:

```
C1 = W+XAE W+-TK TEDQN VER+4 O
C2 = WMJOG DWOJ3 OEBCR VIZNU /
D = /UP++ G3U+U 3/TBI /U+QS O
```

Trying the test string of **HI DAV** XORed with **D** as the first guess at **P2** we obtain:

```
P1 = HELLO 9**** *
D = /UP++ G3U+U 3/TBI /U+QS O
P2 = HI9DA V**** *
```

Now use the tail end of **P2** to extend the guess for **P1**

```
P1 = HELLO 9DAV* *
D = /UP++ G3U+U 3/TBI /U+QS O
P2 = HI9DA VE9S* *
```

P1 seems to be using more formal language than **P2** so try **P1 = HELLO DAVID**

```
P1 = HELLO 9DAVI D***** *
D = /UP++ G3U+U 3/TBI /U+QS O
P2 = HI9DA VE9SE E***** *
```

Use the tail end of **P2** to extend **P1**:

```
P1 = HELLO 9DAVI D9SEE ***** *
D = /UP++ G3U+U 3/TBI /U+QS O
P2 = HI9DA VE9SE E9YOU ***** *
```

Once again use the tail end of **P2** to extend **P1**

```
P1 = HELLO 9DAVI D9SEE 9YOU9 L
D = /UP++ G3U+U 3/TBI /U+QS O
P2 = HI9DA VE9SE E9YOU 9LATE R
```

We have now exhausted the 21-character shorter ciphertext (**C2**) but using **P2 ⊕ C2 = K** we can get the first 21 characters of the key! Here they are:

```
K = UGKZB QLMCD BSNPF GHLMI R
```

THE TILTMAN BREAK

Here are the details of the Tiltman Break. On 30th August 1941 a German telegraphist sent out two long Tunny messages (almost 4000 characters) on the Berlin-Athens radio link, as a result of the receiving end asking for a re-transmission. The 12-letter indicator settings were the same for both messages (i.e. the messages were ‘in depth’) and this indicator (often colloquially known as ‘ZMUG’) has now passed into cryptanalysis folklore:

H Q I B P E X E Z M U G

Fortunately the second transmission was not quite identical to the first and used many abbreviations in order to shorten the tedium of re-transmission. Here are the first 30 characters of the two ciphertext messages (C1 and C2) and in the third row (D) is the result of performing bitwise XOR on the 5-bit teleprinter codes of the two ciphertexts. (Remember that / signifies the NUL character in BP notation).

```
C1 = JSH5N ZYMFS 01151 VKU1Y U4NCE JEGPB
C2 = JSH5N ZYZY5 GLFRG XO5SQ 5DA1J JHD5O
D   = ///// //FOU GF14M AQSG5 SEKZR /YWHE
```

The next stage is to guess a likely plaintext word. (In what follows consult the Teleprinter Code handout to verify the XOR operations and to remind yourself of BP notation e.g. ‘9’ for word space). It was well known that German messages of this sort often started with ‘spruchnummer’ which is the German for ‘message number’. So let’s try this out as a guess for the first plaintext (P1), XOR’d against D:

```
P1 = SPRUC HNUMM ER9** *****
D   = ///// //FOU GF14M AQSG5 SEKZR /YWHE
P2 = SPRUC HNR9+ +UP** *****
```

We see that P2 has used the abbreviation ‘nr’ for ‘nummer’ and so we now use the zig-zag procedure. We use the tail-end of P2 to extend P1 and XOR it against D to get a new P2:

```
P1 = SPRUC HNUMM ER9++ UP*** *****
D   = 00000 00FOU GF14M AQSG5 SEKZR 0YWHE
P2 = SPRUC HNR9+ +UPWU 9E*** *****
```

We now realise that this all makes sense. a word space (9) follows ‘nummer’ and then the message changes into figure shift (++)— note the German insistence on doing the shift change twice— just to be sure! The letters ‘UPWU’ are 7027 when interpreted in Figure Shift. This, of course, really *is* the message number.

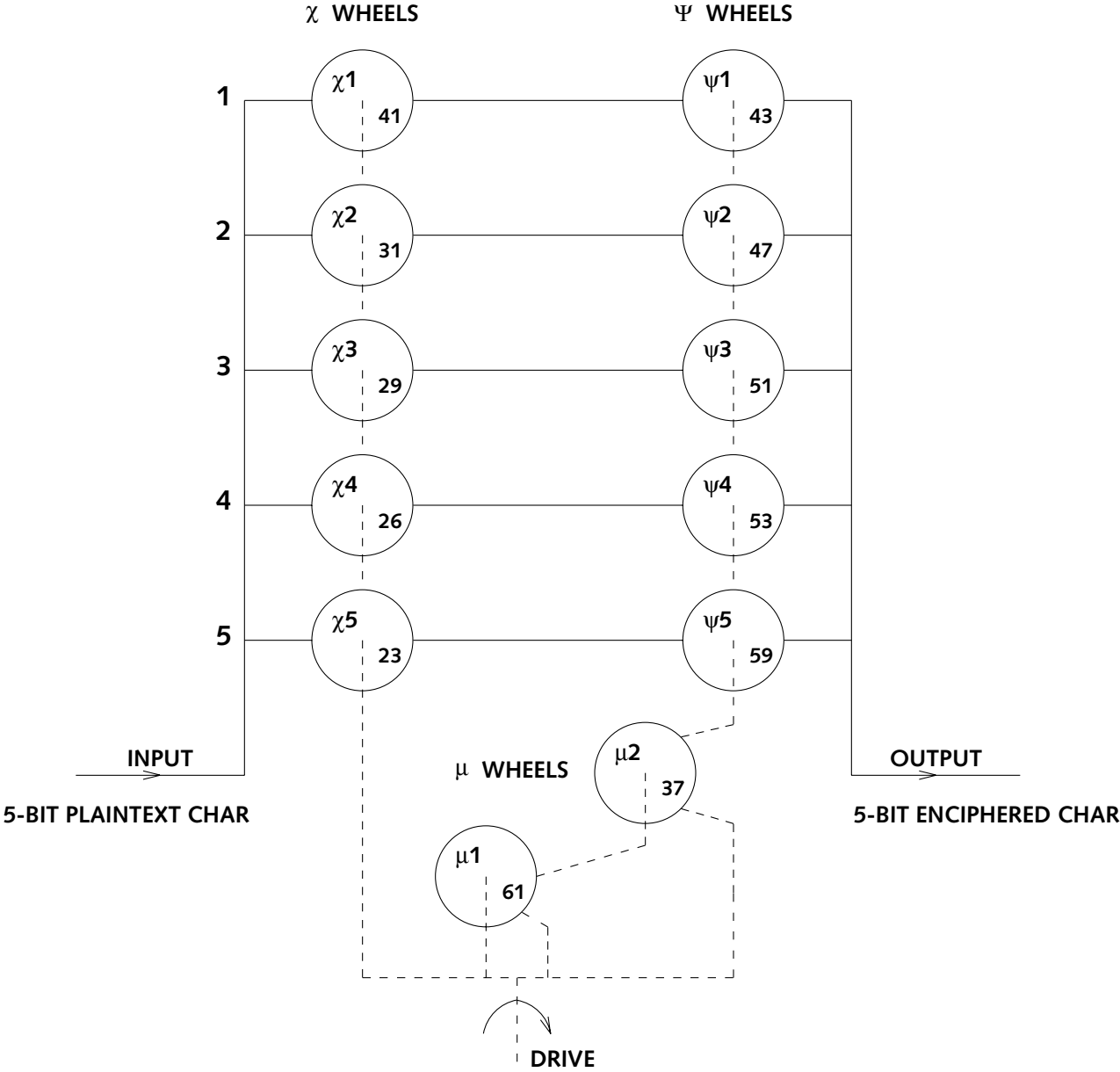
A long message like this (4000 characters) will almost certainly **not** fall into place easily, from start to finish. One has to slide guessed plaintext words against D, and do XOR operations by hand, to see if meaningful German text is delivered at certain points. These ‘decrypted islands’ then have to be linked together. It took John Tiltman (who was very proficient in German) 10 days to complete the task. But at the end of that time he had completely worked out P2 (the second shorter plaintext message). He could now apply the formula:

$$P2 \oplus C2 = K$$

to get the message key (K)— all 3800 characters of it. This was the real ‘gold dust’. Here are the first 30 characters of K for the HQIBPEXEZMUG initial settings:

```
K   = CWVS5 SBSZB EY3BH BBHOZ IVT4X K*FSC
```

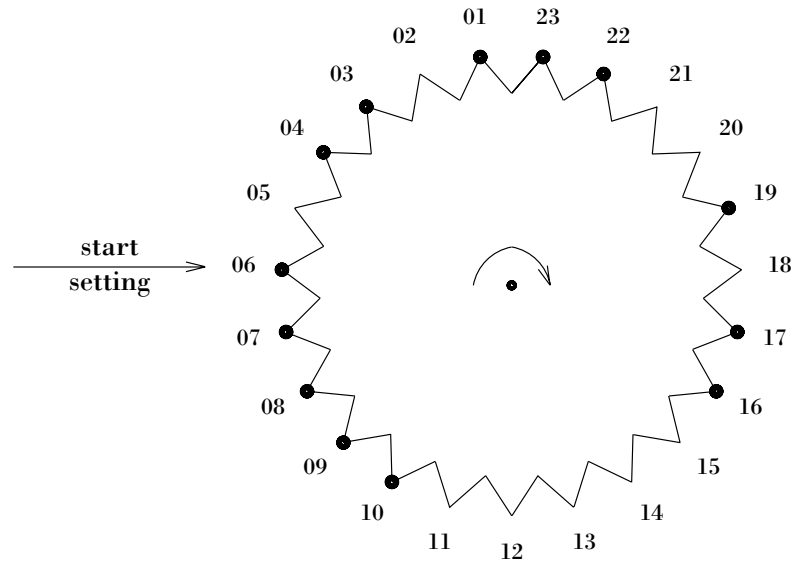
LOGICAL SETUP OF LORENZ MACHINE CIPHER WHEELS



•XXXX••X• <u>XX••X••••X•••XXXXX•X•XXXXX•••X</u>	A
X••••XX•X•••X•XXX•XX•XXX•••XXX•XX•XXX••X	
•XX•X•X•X•••••XXXXXXXXX•X••••XX•XX••XXX•	B
•X•XX•XXXXXXXX•XX•X•••XXXXX•X•X•••••XXX•••	
•••XXXXXXXXXXXXXXXXXX•XX•X•••XXX•X•XXXXX••X•X•	
•••XX••X•XX••X••••••XX•X•XX•••XX•X•X•XX	
XXX•••••X••••••X•XX•XXXXX•X•XXX•••••XX•	
•••XX•XX•XXX•XXXX•X•X•••X••••X••X•X•X•X•	
•••XX•XX•XXX•XX••••••XX•XXXXX••XX•XXX•••	
X•••• <u>XXX•XXXXXXXXXX•XX•</u> XXX•X•XX•X•XX•XXX•••	C
•••XX•XX•••X••X••X••X••X••XX•••XX•X•X•••	
•X•XX••X••X•XX•X••X•XXX•X•XXX••XX•XX••XX	
X•X•••••XX••X••XXXXX•XXX•X•XXX•X••••X•••	
•••XX••••••X••XXXXX•••XXX•XX•••XXXXXX••X	
XXXXXX••••••XX•XXXXX••••X•X•X•X••XX••••	
•X•X••••••X•••X•XXXXXXXXXX•X•X••XXXXX•X•X	
•XX••••X•••X••X•XXX•••X•••X•••XX•XX•••X	
XXX•X•••X•••••XXXXXXXXXXXXX•••X•X••X••X•X•	B
•XXXXXXXXX••X••X••XX•XXXXX••••X•X•XX••XXX•	
•X•XX•XX••XXXXX•X••X••••X•X•••XX•XX•X•X•X	
•XX•X••X••XX•XX•X•••XXX•X•X•X•XXXXXX•X•••X	
X•X••X••XXXXXX•••X••••••XXXXX•••XXX•••X•X	
X••••X••X•••XX•XX•XX•••X•XXXXX•XXXXX•XX••XX	
X•X••XX•XXX•X••XX•XXXXXXXXX•••XX•X•XXXXXX•XX•	
X•X•••••••••X••XXXXX•XXXXXXXXXXXXX•X•XXX•X•••X	
X••X•X••XXXXX•X••••••X•••XXXXX•X•XXX•X•XXX	A
X•••••X•XX••XX•XX••X••XX••X•X•••XXX•X•XX•	
X•X••XXXXXX•X••XXXXXXXXXXXXX•X•X•X•XXXXX•X•X	
X•X•X•••••XX•••X•XXX••XX•••X•X•X•XX•••XX•	
X••X•X•••XXX••X•••••X••X•XXXXXX••XXX•X•XXX	
XXX••X•X••XX••••••X••XX•X•XXXXX•XXXXX•••X	
XXXXXX•••••XX•••X•XXXXX•X•X••X••••X••X•X•	
•XX•XXXXXX•XX••X•••••XXX•XXX•••X•XXX•••XX•	
X••XXXXX•XXXXXXXXXX•XX•••X••••X•••XX•XX•••X	C

Bill Tutte's analysis of Impulse 1 of the keystream from the Tiltman Break
The rows are of width 41 characters (Note: • represents 0 and x represents 1)

WHEEL SETTINGS AND WHEEL PATTERNS ON THE LORENZ MACHINE



Example of a wheel setting and wheel patterns on the 23-tooth Lorenz wheel

- A black blob indicates where a cam has been raised behind a given tooth so that when the tooth rotates past the setting point then a '1' is emitted rather than a '0'.
- Note that the phrase *wheel settings* refers to the (different) start positions for all 12 of the Lorenz wheels, whereas the phrase *wheel patterns* refers to the pattern of raised and lowered cams on each of the wheels. It is these raised and lowered cams on all 12 wheels that provide the changing pattern of 1s and 0s that gets exclusive-ORed, in two stages, with the incoming 5-bit plaintext character stream.