REPORT ON TUNNY

FISH MACHINES

(a) The Teleprinter Alphabet

Two teleprinters in communication consist of two enlarged electromatic typewriters connected by cable, and constructed so that whatever is typed on either keyboard is printed on both typewriters. When a key is depressed by the sender, the enlarged typewriter sends along the cable one of 32 electrical signals. These signals consist of five consecutive impulses, each of which may be positive (known as DOT) or negative (known as CROSS) and they operate the appropriate key of the receiving typewriter. The 32 signals are known as LETTERS and correspond to the keys on the teleprinter keyboard.

It is clear that the number of keys cannot be greater than 32, and it is in fact 31. However 29 out of 31 keys can have two meanings, one in figure shift and one in letter shift, the remaining two being used to operate the change to letter shift and the change to figure shift respectively.
The following table (on next page) shows the construction and meanings of the letters in the teleprinter alphabet as laid down by international convention. Figure shift meanings are liable to variation when they have a purely national significance (e.g. £). The order of the letters is specially devised for cryptographic purposes and not conventional.

CN: Bletchley Conventional Name

	IMPULSE					MEANING	
CN	1	2	3	4	5	Letter	Figure
/	.	.	.	.	.	(no meaning, not used)	
9	.	.	x	.	.	space	space
H	.	.	x	.	x	H	£ (local currency)
T	.	.	.	.	x	T	5
O	.	.	.	x	x	O	9
M	.	.	x	x	x	M	Full Stop (.)
N	.	.	x	x	.	N	Comma (,)
3	.	.	.	x	.	CR	CR = Carriage Return
R	.	x	.	x	.	R	4
C	.	x	x	x	.	C	colon (:)
V	.	x	x	x	x	V	equals (=)
G	.	x	.	x	x	G	
L	.	x	.	.	x	L	close bracket)
P	.	x	x	.	x	P	0 (zero)
I	.	x	x	.	.	I	8
4	.	x	.	.	.	Line feed	Line feed
A	x	x	.	.	.	A	dash (-)
U	x	x	x	.	.	U	7
Q	x	x	x	.	x	Q	1
W	x	x	.	.	x	W	2
5/+	x	x	.	x	x	Move To FIG.	(none)
8/-	x	x	x	x	x	(none)	Move to LET. Shift
K	x	x	x	x	.	K	Open bracket (
J	x	x	.	x	.	J	ring bell
D	x	.	.	x	.	D	Werde (Who)
F	x	.	x	x	.	F	%
X	x	.	x	x	x	X	/
B	x	.	.	x	x	B	?
Z	x	.	.	.	x	Z	+
Y	x	.	x	.	x	Y	6
S	x	.	x	.	.	S	apostrophe ( )
E	x	.	.	.	.	E	3

THE TUNNY CIPHER MACHINE

(a) Addition

	/	9	H	T	O	M	N	3	R	C	V	G	L	P	I	4	A	U	Q	W	5	8	K	J	D	F	X	B	Z	Y	S	E	
/	/	9	H	T	O	M	N	3	R	C	V	G	L	P	I	4	A	U	Q	W	5	8	K	J	D	F	X	B	Z	Y	S	E	/
9	9	/	T	H	M	O	3	N	C	R	G	V	P	L	4	I	U	A	W	Q	8	5	J	K	F	D	B	X	Y	Z	E	S	9
H	H	T	/	9	N	3	O	M	V	G	R	C	I	4	L	P	Q	W	A	U	K	J	5	8	X	B	D	F	S	E	Z	Y	H
T	T	H	9	/	3	N	M	O	G	V	C	R	4	I	P	L	W	Q	U	A	J	K	8	5	B	X	F	D	E	S	Y	Z	T
O	O	M	N	3	/	9	H	T	L	P	I	4	R	C	V	G	5	8	K	J	A	U	Q	W	Z	Y	S	E	D	F	X	B	O
M	M	O	3	N	9	/	T	H	P	L	4	I	C	R	G	V	8	5	J	K	U	A	W	Q	Y	Z	E	S	F	D	B	X	M
N	N	3	O	M	H	T	/	9	I	4	L	P	V	G	R	C	K	J	5	8	Q	W	A	U	S	E	Z	Y	X	B	D	F	N
3	3	N	M	O	T	H	9	/	4	I	P	L	G	V	C	R	J	K	8	5	W	Q	U	A	E	S	Y	Z	B	X	F	D	3
R	R	C	V	G	L	P	I	4	/	9	H	T	O	M	N	3	D	F	X	B	Z	Y	S	E	A	U	Q	W	5	8	K	J	R
C	C	R	G	V	P	L	4	I	9	/	T	H	M	O	3	N	F	D	B	X	Y	Z	E	S	U	A	W	Q	8	5	J	K	C
V	V	G	R	C	I	4	L	P	H	T	/	9	N	3	O	M	X	B	D	F	S	E	Z	Y	Q	W	A	U	K	J	5	8	V
G	G	V	C	R	4	I	P	L	T	H	9	/	3	N	M	O	B	X	F	D	E	S	Y	Z	W	Q	U	A	J	K	8	5	G
L	L	P	I	4	R	C	V	G	O	M	N	3	/	9	H	T	Z	Y	S	E	D	F	X	B	5	8	K	J	A	U	Q	W	L
P	P	L	4	I	C	R	G	V	M	O	3	N	9	/	T	H	Y	Z	E	S	F	D	B	X	8	5	J	K	U	A	W	Q	P
I	I	4	L	P	V	G	R	C	N	3	O	M	H	T	/	9	S	E	Z	Y	X	B	D	F	K	J	5	8	Q	W	A	U	I
4	4	I	P	L	G	V	C	R	3	N	M	O	T	H	9	/	E	S	Y	Z	B	X	F	D	J	K	8	5	W	Q	U	A	4
A	A	U	Q	W	5	8	K	J	D	F	X	B	Z	Y	S	E	/	9	H	T	O	M	N	3	R	C	V	G	L	P	I	4	A
U	U	A	W	Q	8	5	J	K	F	D	B	X	Y	Z	E	S	9	/	T	H	M	O	3	N	C	R	G	V	P	L	4	I	U
Q	Q	W	A	U	K	J	5	8	X	B	D	F	S	E	Z	Y	H	T	/	9	N	3	O	M	V	G	R	C	I	4	L	P	Q
W	W	Q	U	A	J	K	8	5	B	X	F	D	E	S	Y	Z	T	H	9	/	3	N	M	O	G	V	C	R	4	I	P	L	W
5	5	8	K	J	A	U	Q	W	Z	Y	S	E	D	F	X	B	O	M	N	3	/	9	H	T	L	P	I	4	R	C	V	G	5
8	8	5	J	K	U	A	W	Q	Y	Z	E	S	F	D	B	X	M	O	3	N	9	/	T	H	P	L	4	I	C	R	G	V	8
K	K	J	5	8	Q	W	A	U	S	E	Z	Y	X	B	D	F	N	3	O	M	H	T	/	9	I	4	L	P	V	G	R	C	K
J	J	K	8	5	W	Q	U	A	E	S	Y	Z	B	X	F	D	3	N	M	O	T	H	9	/	4	I	P	L	G	V	C	R	J
D	D	F	X	B	Z	Y	S	E	A	U	Q	W	5	8	K	J	R	C	V	G	L	P	I	4	/	9	H	T	O	M	N	3	D
F	F	D	B	X	Y	Z	E	S	U	A	W	Q	8	5	J	K	C	R	G	V	P	L	4	I	9	/	T	H	M	O	3	N	F
X	X	B	D	F	S	E	Z	Y	Q	W	A	U	K	J	5	8	V	G	R	C	I	4	L	P	H	T	/	9	N	3	O	M	X
B	B	X	F	D	E	S	Y	Z	W	Q	U	A	J	K	8	5	G	V	C	R	4	I	P	L	T	H	9	/	3	N	M	O	B
Z	Z	Y	S	E	D	F	X	B	5	8	K	J	A	U	Q	W	L	P	I	4	R	C	V	G	O	M	N	3	/	9	H	T	Z
Y	Y	Z	E	S	F	D	B	X	8	5	J	K	U	A	W	Q	P	L	4	I	C	R	G	V	M	O	3	N	9	/	T	H	Y
S	S	E	Z	Y	X	B	D	F	K	J	5	8	Q	W	A	U	I	4	L	P	V	G	R	C	N	3	O	M	H	T	/	9	S
E	E	S	Y	Z	B	X	F	D	J	K	8	5	W	Q	U	A	4	I	P	L	G	V	C	R	3	N	M	O	T	H	9	/	E
	/	9	H	T	O	M	N	3	R	C	V	G	L	P	I	4	A	U	Q	W	5	8	K	J	D	F	X	B	Z	Y	S	E	

Before considering in detail the operations of the Tunny machine it is necessary to define the addition of two teleprinter letters. Teleprinter letters are added by summing corresponding impulses according to the rules

. plus x equals x
. plus . equals .
x plus . equals x
x plus x equals .

Exemple: 9 (. . x . .) + Y (x . x . x) = Z (x . . . x)

From this example it is clear that not only 9 + Y = Z but also that 9 + Z = Y and Y + Z = 9. This is an important result which may be stated in the form of the theorem: Addition and Subtraction of teleprinter letters (or characters) is the same thing. Any proof required is left to the reader.

(b) Tunny Key

For each letter in turn of the unciphered stream of impulse signals, the Tunny machine makes up a key-letter (K) and adds it to the plain text (P) to get a ciphered letter (Z). The P-stream can contain any letter of the teleprinter alphabet except Carriage-Return and Line-Feed. Of the letters that do occur 9 (space), 5 or +(Move to Figure) , 8 (Move to Letter), and E are particularly common. The K-stream and therefore Z-stream, contains each letter of the teleprinter alphabet approximately an equal number of times.

(c) The Wheels

12 wheels are used to generate the key. Each wheel consists of a pattern of dots and crosses of a given length. Each character moves into the active position in turn, and when the wheel has gone round completely the pattern is repeated. The wheels are divided into three groups with the following names and lengths.

CHI Wheels
- Chi wheel 1 length 41 characters
- Chi wheel 2 length 31 characters
- Chi wheel 3 length 29 characters
- Chi wheel 4 length 26 characters
- Chi wheel 5 length 23 characters

PSI Wheels
- Psi wheel 1 length 43 characters
- Psi wheel 2 length 47 characters
- Psi wheel 3 length 51 characters
- Psi wheell 4 length 53 characters
- Psi wheel 5 length 59 characters

MOTOR or MU Wheels
- Mu wheel 61 length 61 characters
- Mu wheel 37 length 37 characters

The key-letter is the sum of the letter of chi-key formed by the five characters in the active positions of 1; 2; 3; 4; 5, and the letter of psi-key formed by the five characters in the active positions of 1; 2; 3; 4; 5.

(d) Chi-key

After each letter of the P-stream has been enciphered each chi moves on once. The pattern of characters added to each impulse of the P-stream has a period equal to the length of the corresponding chi-wheel, and since the lengths of these wheels are prime to each other, the stream of letters generated by the chis has a period of 41 31 29 26 23.

(e) Psi-key

The motion of the psis is irregular and determined by the motor. After a letter has been enciphered either each psi wheel moves on once and a new letter of the psi-key is used for ciphering the next letter or all five psis remain still and the same letter of psi-key is used again. When happens there is said to be an extension of the psi-stream. The term EXTENDED PSI (Psi') stream is used for the actual sequence of letters added by the Psis to the P-stream, and the i term -stream for the sequence of letters that the psis would generate if there were no extensions.

(f) Motors

The dots and crosses arranged round the motor wheels do not mean the same as the symbols usually called dots and crosses.

A dot means STOP
A cross means GO.

Mu61 moves on once after each letter is enciphered. When mu61 has a cross in the active position (before moving) mu37 moves on once: when it has a dot in the active position (before moving) mu37 stays still. The character of mu37 in the earlier active position is the active character of the BASIC MOTOR (BM). In other words BM = Mu37 “extended by Mu61”.

Example

```
P          9 8 9 U N D 9 B 9 E I N G E S E T Z T E
Chi (H)    4 9 M A 4 K B G G E H M 8 E 4 X I J F H
Psi'(S)    W I J / X / / D H P J J J V T T F 4 4 X
K=H+S      Z 4 Q A 8 K B W C Y 8 Q H 8 L F J D K D
Z=P+K      Y X W 9 W I X N R P B + C V Q N + O 8 3

Mu      61   x x . . x x x x . x x x . x
Mu      37   x x x . x x x . . x . x . x
BM           x x x x x . x x x x . . x x

Chi 1 . . . x . x x . . x . . x x . x . x x .
Chi 2 x . . x x x . x x . . . x . x . x x . .
Chi 3 . x x . . x . . . . x x x . . x x . x x
Chi 4 . . x . . x x x x . . x x . . x . x x .
Chi 5 . . x . . . x x x . x x x . . x . . . x
H     4 9 M A 4 K B G G E H M 8 E 4 X I J F H

Psi 1 x . x . x . x . . x . . x . x
Psi 2 x x x . . . . . x x x . . x .
Psi 3 . x . . x . . x x . x . x . x
Psi 4 . . x . x . x . . x x . x . x
Psi 5 x . . . x . . x x . x x . . x
      W I J / X / D H P J V T F 4 X
BM    x x x x x . x x x x . . x x

Psi' 1 x . x . x . . x . . x x x . . . x . . x
Psi' 2 x x x . . . . . . x x x x x . . . x x .
Psi' 3 . x . . x . . . x x . . . x . . x . . x
Psi' 4 . . x . x . . x . . x x x x . . x . . x
Psi' 5 x . . . x . . . x x . . . x x x . . . x
S      W I J / X / / D H P J J J V T T F 4 4 X
```

MESSAGE SETTING FOR MARCH 1942

The success obtained with the near depth of March 3rd. Confirmed the theory of indicators. It was now taken for granted that the setting of each wheel was controlled by a single letter of the indicator, that the first five letters of the indicator correspond to the five Psi wheels, in order. Then we have the Mu37, the Mu61 and finally the Chi wheels, in order. Example: HQIBPEVEZMUG. The obvious assumption that the same indicator letter in the same place for two messages meant that the corresponding wheel had the same setting in both messages was also made.

Here is the preamble in detail: Each message began with a clear preamble in which there appeared first the serial number, repeated several times, and then a list of 12 proper names, not necessarily all different. The symbol 9 (space) was used as a separator in this preamble, and a group of five 9's separated the clear preamble from the cipher text. Immediately after the cipher text there appeared a sequence of 8's. The serial number was given in letter form by means of a simple keyboard substitution, the digits 1,2,3,4,5,6,7,8,9,0 being represented by the letters Q,W,E,R,T,Y,U,I,O,P respectively.

The purpose of the 12 proper names was evidently to give the twelve letters indicator by their initial letters, and to give them in such a way that a few corrupt letters would not cause a misunderstanding. The proper names were always taken from the following list (in which no name begins with J)

Anton
Bertha
Caesar
Dora
Emil
Frierdrich
Gustav
Heindrich
Ida
Konrad
Ludwig
Martha
Nordpol
Otto
Paula
Quelle
Richard
Siegfried
Theodor (or Toni)
Ulrich (or Ullrich)
Victor
Wilheim (or Willi)
Xanthippe
Ypern (or Ypsillon)
Zeppelin