The "Tunny" Machine and Its Solution

BY BRIGADIER JOHN H. TILTMAN

~~*Top Secret Dinar*~~

This article is substantially the same as a lecture given to the Crypto-Mathematical Institute in October 1960. For that occasion an earlier lecture was completely rewritten so as to place extra emphasis on the lessons to be learnt now from the original diagnostic research which lead to the solution of the "Tunny" machine in 1941 and 1942. I tried to frame both the earlier and the later lectures in such a form that the steps of the solution could be followed by intelligent persons without cryptanalytic background, given concentrated attention. I am not of course suggesting that the solution can be completely absorbed and memorized without further study.

The aspect of exploitation, i.e., wheel-breaking and message-setting, is not treated here. I hope to persuade someone to write a sequel to this article covering the work of the Tunny sections at Bletchley Park (the war-station of GCHQ) between 1942 and 1945, stressing particularly the original statistical scoring methods devised by Dr. Turing and the early development of electronic machinery.

The cipher machine under discussion is the SZ 40, i.e., "Schluesselzusatzgeraet 1940," developed by the Germans for transmitting over the air messages converted to teleprinter form according to the international ("Baudot") teleprinter code. A photograph of the machine is shown as Fig. 15. This is not the SZ 40 but a later model, SZ 42B. It was one of the two in Marshal Kesselring's communication train, discovered at Salzburg during the course of the TICOM operations immediately after the surrender of Germany and brought back to Bletchley Park by Mr. Arthur Levenson of NSA and Major Ralph Tester of GCHQ. We gave the name "Tunny" to the machine early in 1942. Long messages were commonly perforated in advance on five-impulse paper tape instead of manual keyboard operation. During the experimental period in 1941, messages were transmitted mostly by Hellschreiber picture transmission. A photograph of the first page of an early intercept of 14 August 1941 is shown as Fig. 1. For Hellschreiber transmission the six extra symbols 3, 4, 8, 9, + and / were added to the 26 alphabetic symbols of the international code to make up the 32 possible different symbols of five-impulse code.

The international code as modified for Hellschreiber is given as Fig. 2. When the cipher mechanism was not in operation, the symbols 3, 4, and / were never used, as at the receiving station the message

was recorded on continuous sticky tape, / having no meaning anyway and 3 and 4 representing carriage-return and line-feed respectively. When the cipher mechanism was in operation, all 32 symbols were used about equally.

For purposes of this presentation, a cross or the letter X represents a perforation in the tape or an operative position, and a dot an unperforated or inoperative position.

The effect of the cipher mechanism is to apply a very long series of random impulses to the impulses of the plaintext letters in teleprinter form. After each position on the tape or each time a key is depressed, there is a movement of some of the wheels of the machine and to each successive plaintext letter a new set of five impulses is applied. The rules of application are as follows:

The result of applying cross to cross or dot to dot is a dot, cross to dot or dot to cross is a cross. For example, the letter P in the code is .xx.x; the five impulses due to the cipher mechanism at the point reached are ...**xx** (i.e., the letter O). The resultant five impulses from applying ...xx (i.e., the letter O) to .**xx**.x (i.e., the letter P) are .xxx. (i.e., the letter C). It will at once be realized that the three letters P, O and C form a "triple" within which P + O =C, P + C = O, C + O = P, in other words mod. 2 addition. Figure 3 gives a chart of "triples."

There are twelve wheels on each of which a prearranged pattern of crosses and dots can be set up. The wheels are not interchangeable and each has its own cycle of points, the twelve cycles being prime to one another. The cycles are as follows reading from the left-hand side of the machine: 43, 47, 51, 53, 59, 37, 61, 41, 31, 29, 26, 23. The first five wheels form a bank called by us Psi wheels; the sixth and seventh form the motor mechanism, called by us Mu wheels; the last five form a bank called by us Chi wheels.

The patterns of cross and dot on the Psi and Chi wheels were changed monthly in 1941, daily in the later years of the war. The patterns of the two Mu wheels were always changed daily. For each transmission a "starting setting" for each of the twelve wheels was prearranged. This setting was not indicated during the transmission except in the period prior to March 1942. Figure 4 gives as an example the patterns of the twelve wheels in use for the "Bream" link (i.e., between Rome and Berlin) on 14 April 1944. (In 1944 SZ 42B was in use. This carried a security attachment not present in SZ 40). In Fig. 5 an example is shown of the effect of encipherment using the wheel patterns of Fig. 4. An arbitrary point (shown in square brackets) is assumed to have been reached in the movement of each wheel.

I will now describe the steps of the original solution, which was accomplished without any continuity or collateral information, or any previous experience of five-unit cipher to guide us. We were fortunate in obtaining Hellschreiber intercepts (of which Fig. 1 gives an example) of early transmissions which passed between Vienna and Athens shortly after the invasion of Russia in the summer of 1941. The transmissions were frequently of very great length—I remember one of about 16,000 consecutive symbols of cipher. Each transmission began with a set of twelve personal names (Anton, Bertha, etc.), clearly a twelve-letter indicator. The symbol 9 was used as a separator in this preamble and a group of five 9's separated the clear preamble from the cipher text. At quite an early stage I had little difficulty in correlating the 26 letters of the alphabet and the six extra signs 3, 4, 8, 9, + and / with the 32 different sets of five-unit impulses. It was made easy for me by study of a series of messages of 22 July 1941 in which the crosses of the first impulse stream had not perforated, so that for example *Heinrich* was transmitted as H/INRICH and *Theodor* as TH/O3OR.

Among the early intercepts were a number of cases of two or more messages having the same twelve-letter indicator. Usually the two messages involved were consecutive but there were several cases in which the indicators were recognizable words, names or phrases, such as *Grafzeppelin* and *Kaeferboecks*, proving that the operator had the responsibility for selection of his message indicators. Kaeferboecks, I imagine, was some kind of a bug which was giving the sending operator trouble or a rude nickname for one of his colleagues—it appeared four times.

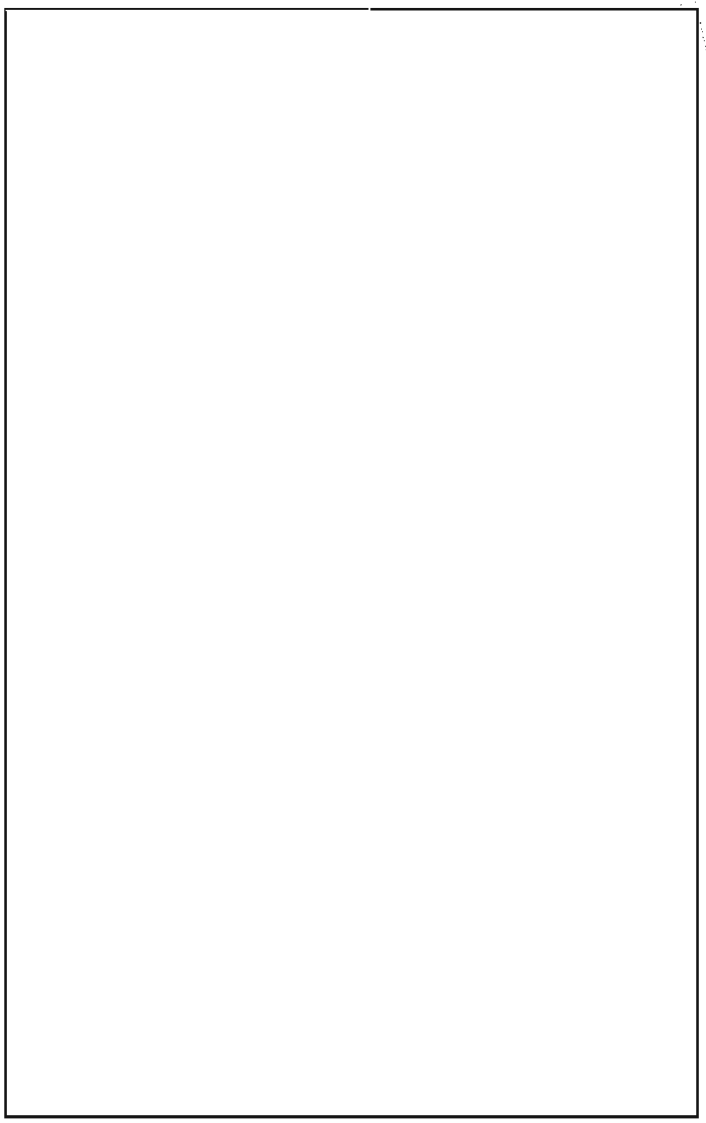
EO
1.4.(b)
EO
1.4.(c)
EO
1.4.(d)

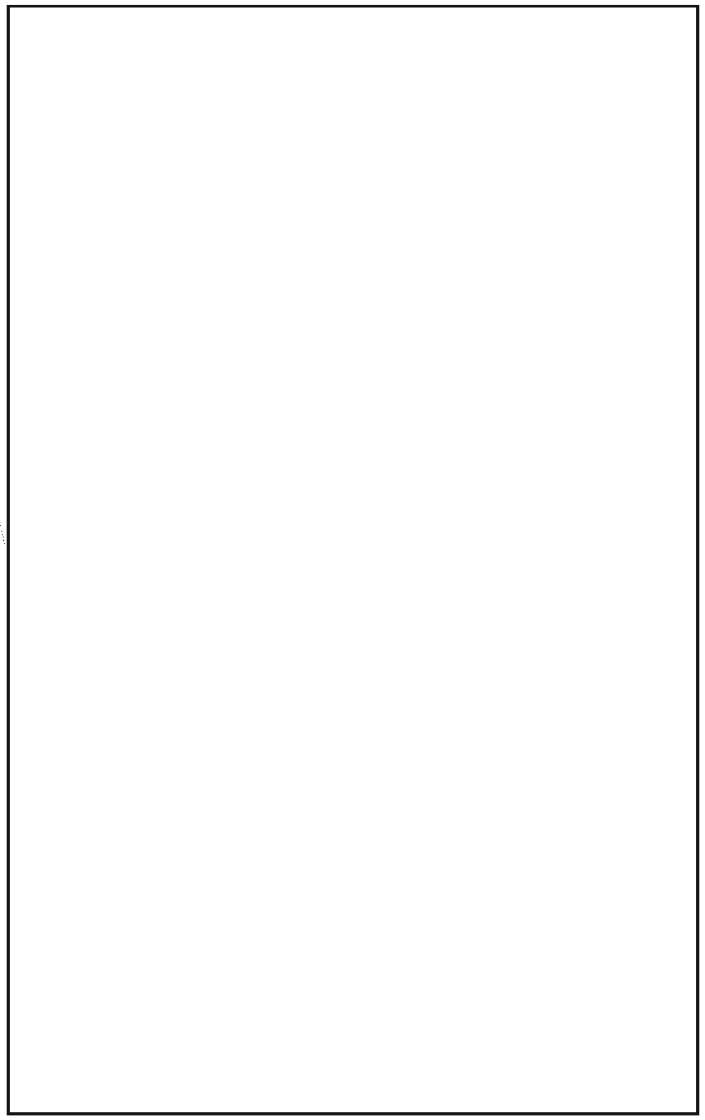
On 30 August 1941, two very long messages were intercepted from Vienna to Athens with the same indicator HQIBPEXEZMUG. One had 3976 symbols of consecutive cipher text and the other was about 500 symbols longer. research section at Bletchley Park pushed the recovery of the which we built up during the process. In this case, I was doing the work myself and I suddenly reached the point at which it became obvious that the In the course of the next ten days or so I succeeded in carrying recovery to the end of the shorter of the two messages, thereby recovering 3976 consecutive symbols of key. In this key there were, of course, a number of positions where the key was am-

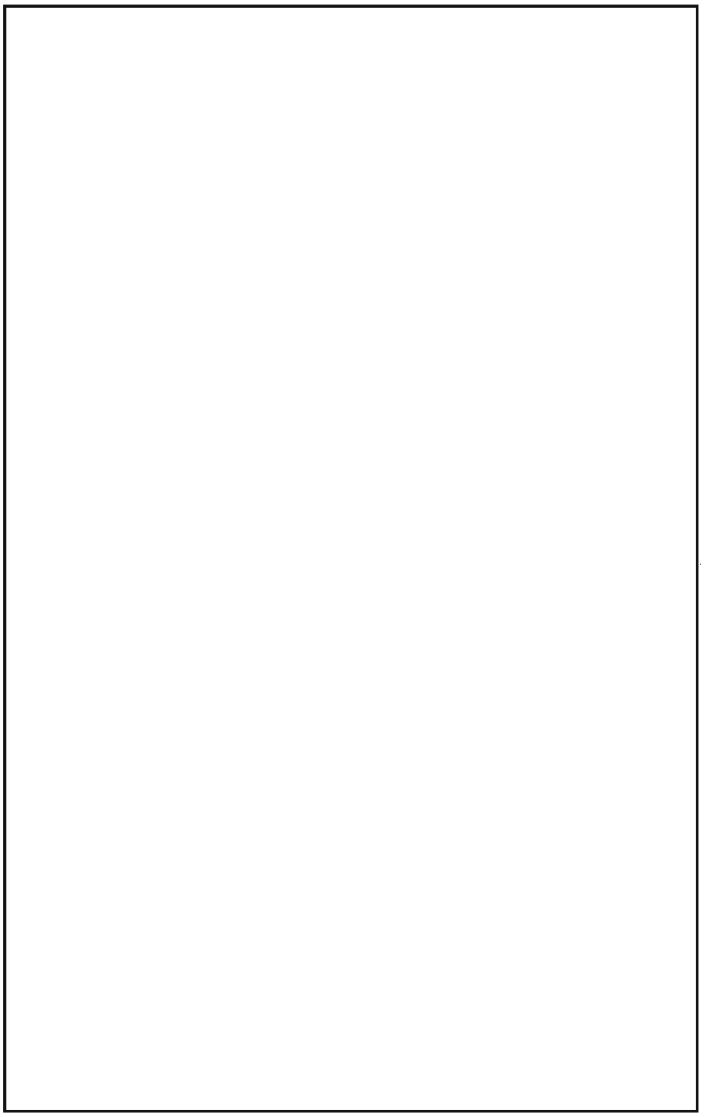
biguous, though not generally for more than three consecutive symbols. You will, I am sure, understand that when working in mod. 2 there is usually no way of telling which plain text belongs to which cipher transmission and thus [redacted] are produced. In this case, however, the ambiguity disappeared when I reached the end of the shorter message. The plain text proved to be a report for the personal information of the German military attache in Athens on the situation on the [redacted] In both plaintext versions, there were many places where the sending operator had struck a wrong key or made some other mistake necessitating long stretches of corrections and repetitions. [redacted]

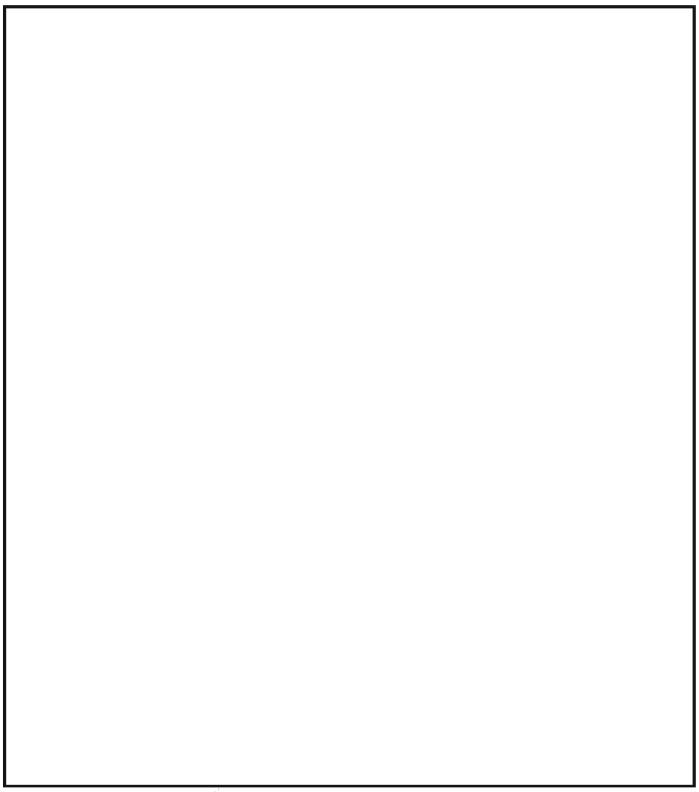
I took no part in the reconstruction of the machine from the long stretch of key which I had recovered. It was studied in its five individual impulse streams by the members of my Research Section and most of the work of reconstruction was done by Dr. Morgan and Mr. Tutte. However, no obvious periodicity was at first observed and no progress was made for about four months. [redacted]

[redacted]









(Illustrations begin on following page.)

S.1319. Est. May, 1923. Mod. Nov. 1931.

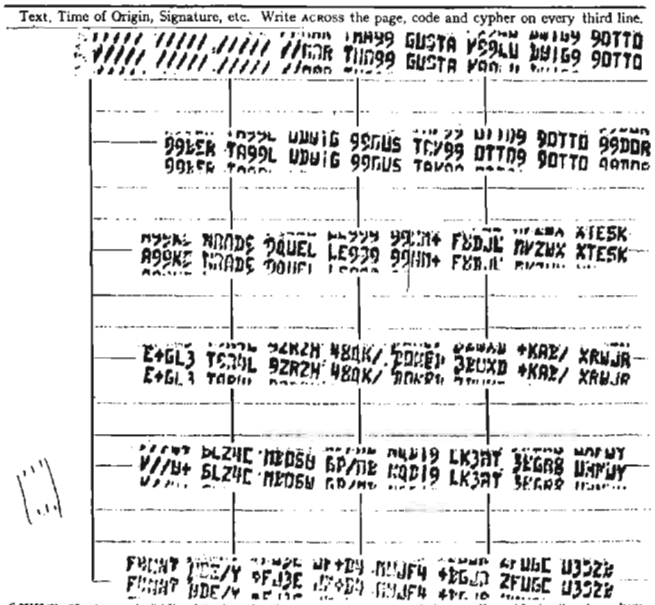
W/T RED FORM.

Ref. No. /
Page

Ship or Station.	Set		Date.	4/8	Operator's Remarks.*
927	Opr.	L	Time Ended G.M.T.	1843.	Q. S. A. Also on undulator
	Tot†	A	Frequency & System.	6530	
	From†	C			

All before the Text. 6408 MGLOBLC OODKQ

Text, Time of Origin, Signature, etc. Write across the page, code and cypher on every third line.



G 85556/28 *Constancy and reliability of signals, quality of operating, interference, atmospherics, etc. †Name of Station; if not known leave blank.
Sta. 1/30.
Sta. 163/31.

S.1319.

Fig. 1.

LOWER CASE	UPPER CASE	
A	–	x x . . .
B	?	x . . x x
C	:	. x x x .
D		x . . x .
E	3	x . . . .
F		x . x x .
G		. x . x x
H		. . x . x
I	8	. x x . .
J		x x . x .
K	(	x x x x .
L	)	. x . . x
M	.	. . x x x
N	,	. . x x .
O	9	. . . x x
P	ø	. x x . x
Q	1	x x x . x
R	4	. x . x .
S		x . x . .
T	5	 x
U	7	x x x . .
V		. x x x x
W	2	x x . . x
X	/	x . x x x
Y	6	x . x . x
Z	REPEAT	x . . . x
LINE FEED		. . . x .
CAR. RETURN		. x . . .
	LOWER CASE	x x x x x
SPACE		. . x . .
UPPER CASE		x x . x x
NO MEANING		. . . . .

Fig. 2.—International T/P Code

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

Fig. 3.—Chart of "Triples"

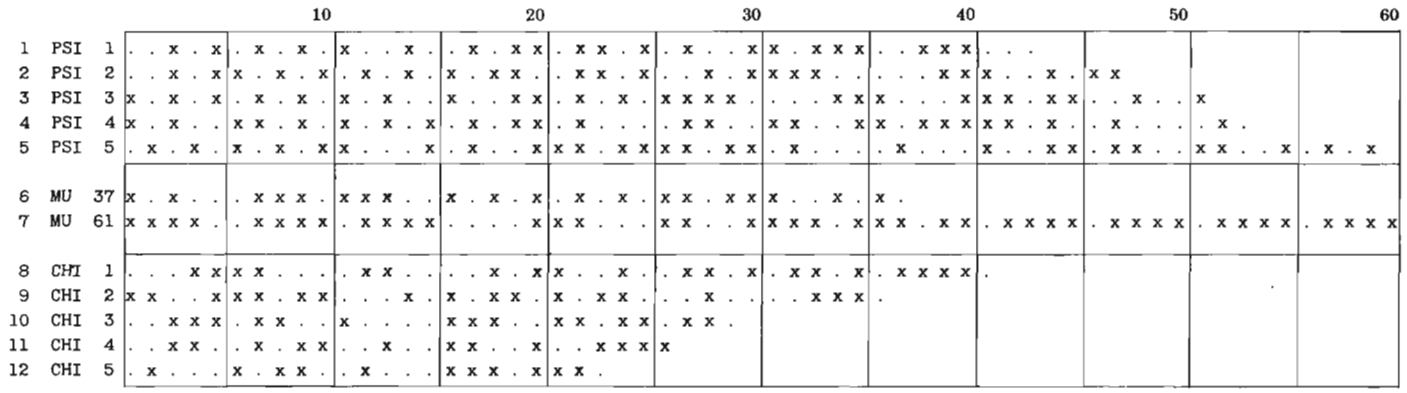


Fig. 4.—Wheel-Patterns for "Bream" Link (Berlin and Rome) 14th April 1944

Example of effect of cipher mechanism.
20 letters of plain text (not the beginning) of a message of 4/14/44.

P 9 8 9 U N D 9 8 9 E I N G E S E T Z T E (A)

Wheel-patterns of 4/14/44 are given in Figure 4. An arbitrary point (shown in square brackets below) is supposed to have been reached on each of the 12 wheels.

I. *Motor mechanism.* Mu 61 moves one step for every letter enciphered
Mu 37 moves one step after x in Mu 61
Mu 37 remains still after . in Mu 61

```
Mu 61  [26] x x . . x x x x . x x x . x x . x x x x
            1 2 3 3 3 4 5 6 7 7 8 9 10 10 11 12 12 13 14 15   (B)
Mu 37  [ 7] x x x . x x x . . x . x . x .
            1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
BM          x x x x x . x x x x . . x x . x x . x . BM = Basic (C)
            1 2 3 3 3 4 5 6 7 7 8 9 10 10 11 12 12 13 14 15  Motor (B)
```

II. Psi patterns

```
Psi  1 [ 5] x . x . x . x . . x . . x . x
Psi  2 [31] x x x . . . . . x x x . . x .
Psi  3 [12] . x . . x . . x x . x . x . x
Psi  4 [50] . . x . x . x . . x x . x . x
Psi  5 [37] x . . . x . . x x . x x . . x
  Psi       W I J / X / D H P J V T F 4 X
```

All five Psi wheels move one step after x in BM
All five Psi wheels remain still after . in BM
The Psi patterns owing to retardation by dots of BM become extended

```
   BM          x x x x x . x x x x . . x x . x x . x .   (C)
Extended Psi W I J / X / / D H P J J J V T T F 4 4 X    (D)
```

III. Chi patterns

```
Chi  1 [15] . . . x . x x . . x . . x x . x . x x .
Chi  2 [ 2] x . . x x x . x x . . . x . x x . .
Chi  3 [ 6] . x x . . x . . . . x x x . . x x . x x
Chi  4 [18] . . x . . x x x x . . x x . . x . x x .
Chi  5 [10] . . x . . . x x x . x x x . . x . . . x
  Chi       4 9 M A 4 K B G G E H M 8 E 4 X I J F H   (E)
```

All five Chi wheels step regularly—their movement *is* not interrupted by BM

IV. The total Key (K) is obtained by applying Chi to extended Psi

```
Extended Psi  W I J / X / / D H P J J J V T T F 4 4 X   (D)
  Chi         4 9 M A 4 K B G G E H M 8 E 4 X I J F H   (E)
  K           Z 4 Q A 8 K B W C Q 8 Q H 8 L F J D K D   (F)
```

V. K is now applied to P to give Z, final cipher version

```
K  Z 4 Q A 8 K B W C Q 8 Q H 8 L F J D K D   (F)
P  9 8 9 U N D 9 8 9 E I N G E S E T Z T E   (A)
Z  Y X W 9 W I X N R P B + C V Q N + 0 8 3
```

VI. Special rules for the beginning of a transmission.
All 12 wheels move one step between first and second letters. Between the second and third letters the bank of Psi wheels moves if the sign of Mu 37 is x and remains still if the sign of Mu 37 is . , i. e., the sign of Mu 61 has no influence at this point.

Fig. 5.

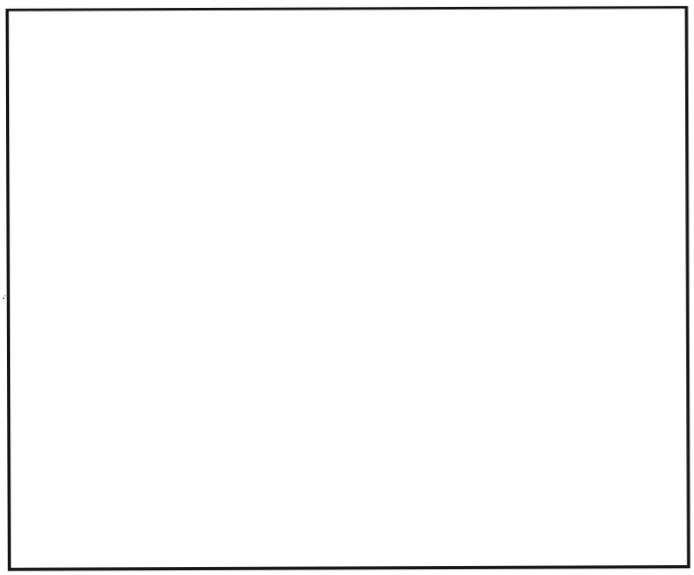


Fig. 6.

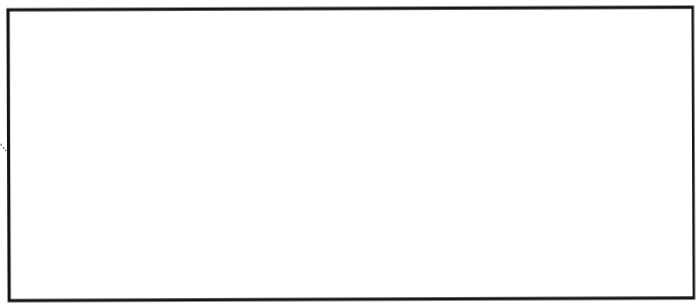
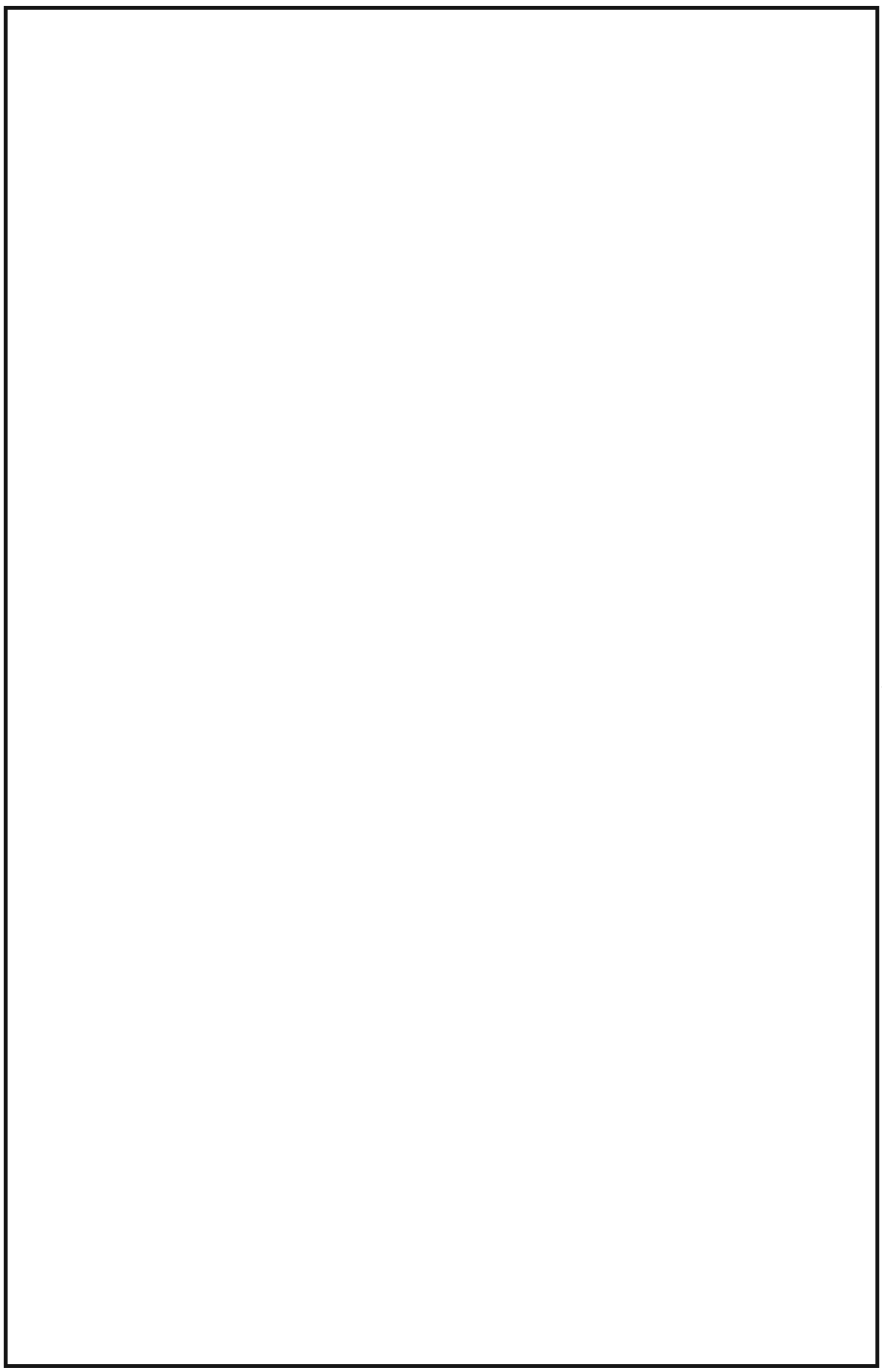


Fig. 7.



EO 1.4.(b)
EO 1.4.(c)
EO 1.4.(d)

Fig. 8.

Fig. 9.

Fig. 10.

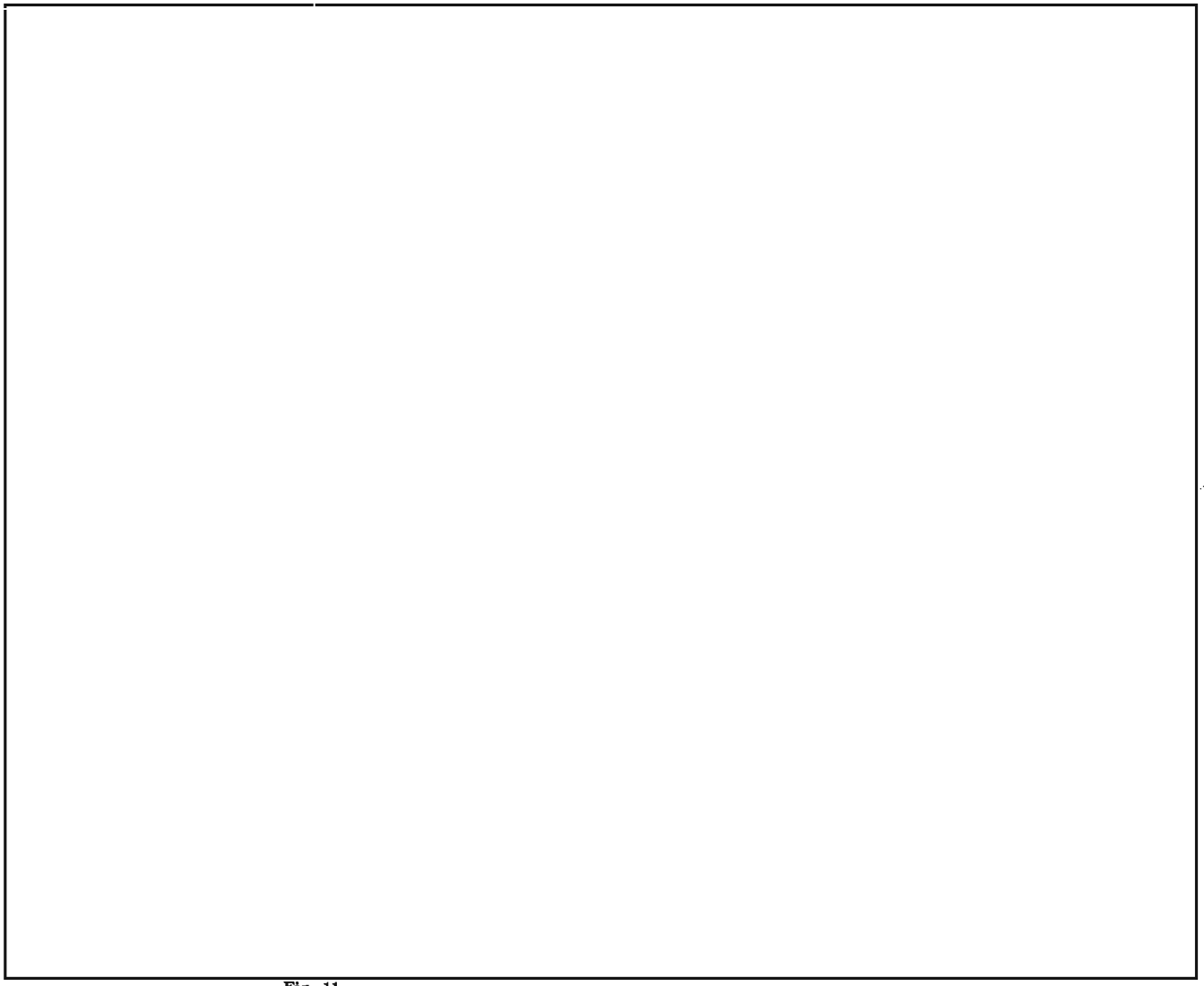
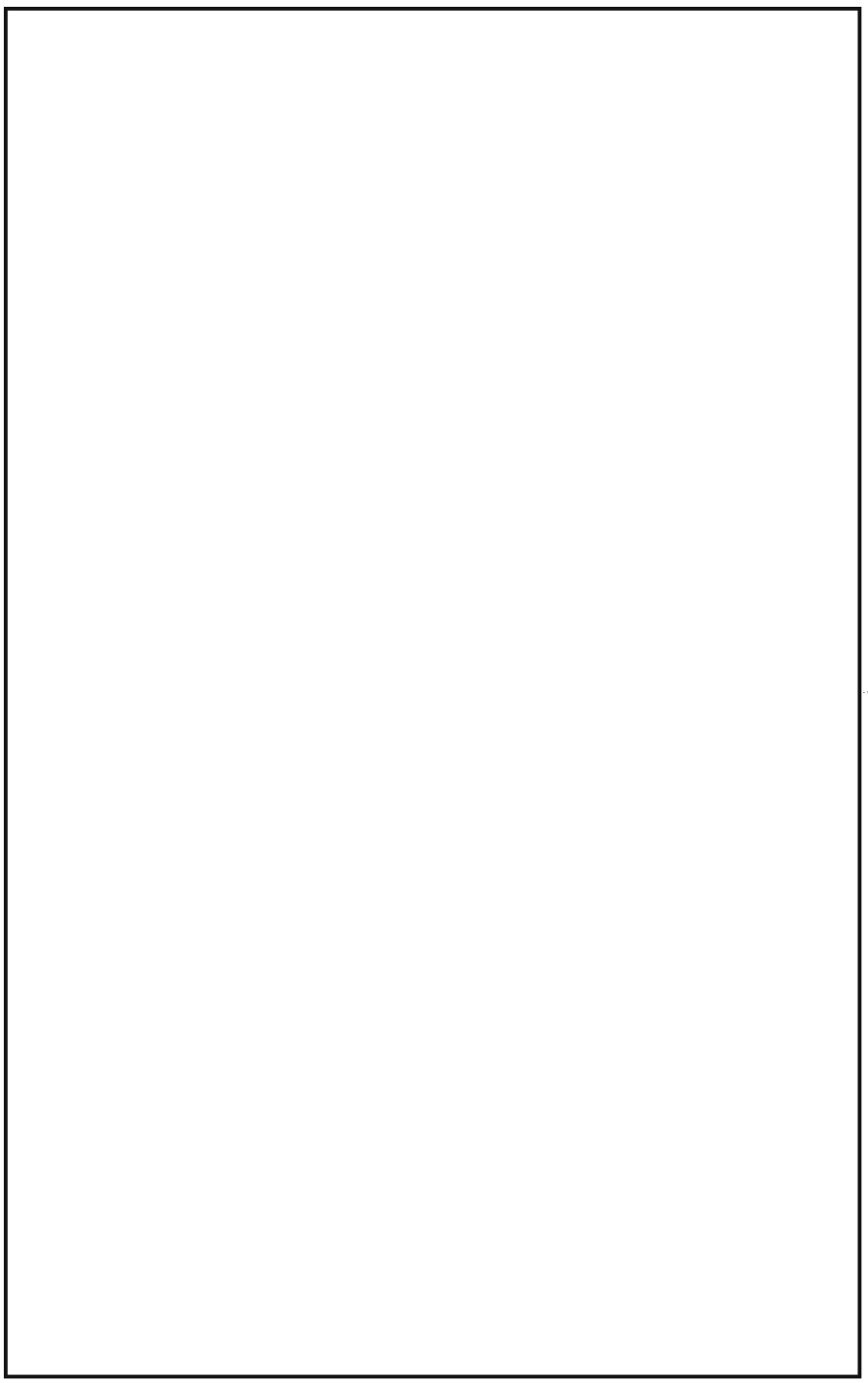


Fig. 11.

Fig. 12.

EO 1.4.(b)
EO 1.4.(c)
EO 1.4.(d)

Fig. 13.



EO 1.4.(b)
EO 1.4.(c)
EO 1.4.(d)

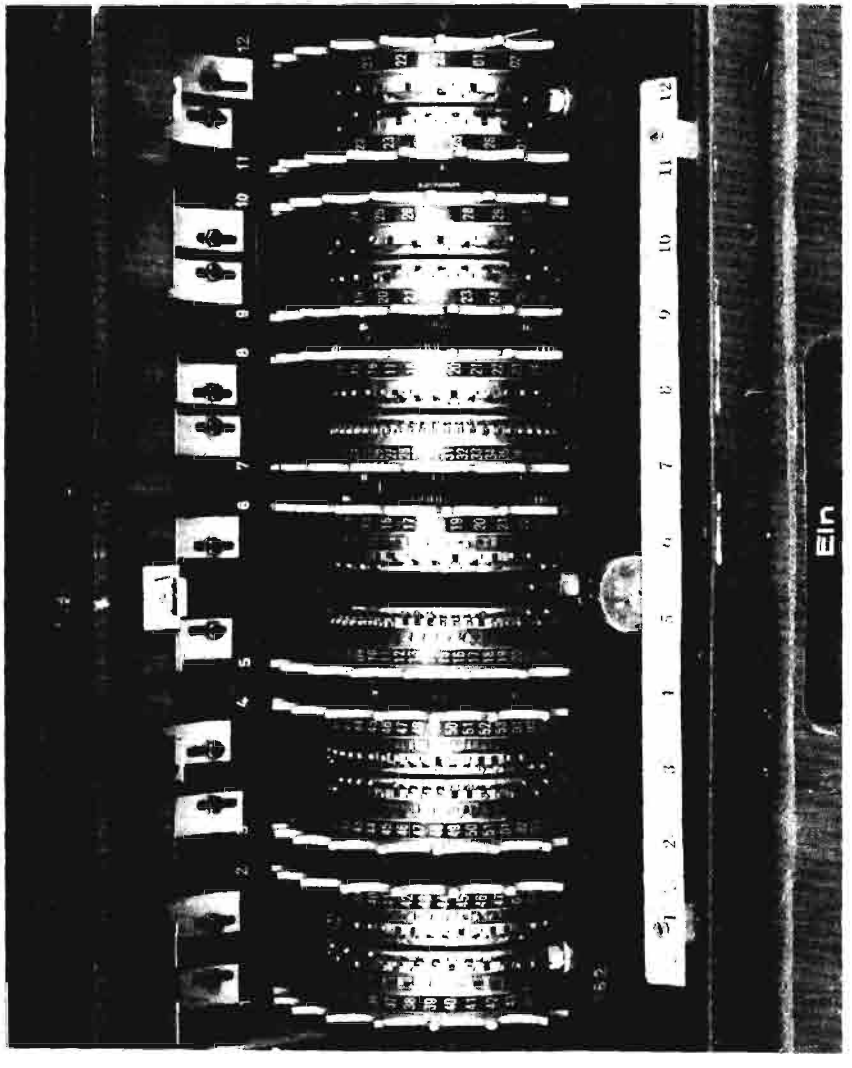


Fig. 15.—The "Tunny" Machine Rotor Maze.