Non-Reciprocal Stecker

by

Lt. Howard H. Campaigne and Lt. Andrew M. Gleason

24 July 1944

Abstract

The 40 Steckers produced from the daily one by the Enigma Uhr device (see preceding article) fall into 4 classes of 10 each; the cyclic structure of each of these classes is given. The bulk of the article is concerned with how to find the daily Stecker from the one recovered on the bombe.

Source: NARA, College Park, Md., Record Group 38, Crane Collection, Box 172, RIP 609, ARC Identifier: 6921398, HMS/MLR Entry Number: A1 1025, hhttps://catalog.archives.gov/id/6921398
Enigma Series Volume 7, Article 9

Editor: Frode Weierud, Crypto Cellar Research
Web Site: www.cryptocellar.org

Version: 22 April 2025

TOP SECRET ULTRA

FOREWORD TO ENIGMA SERIES

CRYPTANALYTICAL RESEARCH PAPERS

This series consists of original memoranda written by members of the cryptanalytical research section of the U.S. Naval Communications Intelligence Staff, and by others working with the research group. A brief description of the contents of each paper is given in the Index to each volume. While an effort toward completeness has been made, the reader is referred for greater detail to the various R.I.P's put out by the Atlantic Operations Department, especially R.I.P. 450. There he will also find polished techniques, which appear in this Series of their original form.

The name of the author and the date of the paper are also given in the Index, which lends an historical flavor to the Series. The Editor feels that there is considerable merit in an anthology for this sort, full of original ideas both good and bad, which supplements the finished publication. It should be further emphasized that R.I.P. 450 is concerned mainly with the techniques themselves, while this Series considers the cryptanalytical or mathematical theories which underlie the techniques. On the other hand, machine research (from an engineering point of view) is not covered in this Series.

Some of the papers in this Series are expository, but most represent original work. It must always be borne in mind that we owe to the British the basic solution of the Enigma, and many of the basic subsidiary techniques, together with the underlying mechanical and mathematical theories. Much of what we call "original" is only a retracing of steps previously taken by the British, and the Editor has striven to point this out in the Index. But there is also a great deal that extends or improves British methods, and some that strikes out in new directions.

It must be pointed out that the author of a paper may be entitled to credit only for his literary toil. Our group of eight or ten men worked as a team, and an assignment of "credit" would be as difficult as it is undesirable. In this line of endeavor, a chance remark may be worth a week's work.

NON-RECIPROCAL STECKER

The following considerations are advanced as having possible value on Jaguar runs.

1. The positions of the "commutator" divide themselves naturally into four classes, designated by the residues modulus 4 of the indicator. These classes have the following properties.

1,1 The O class has a reciprocal stecker with 6 self steckers as usual. Its cyclic structure is 10 transpositions and 6 identities, or 2,2,2,2,2,2,2,2,2,2, 1,1,1,1,1,1.

1,2 The I class has the cyclic structure 14,4,2,1,1,1,1,1,1.

1,3 The Z class has structure 12, 8, 1,1,1,1,1,1.

1,4 The 3 class has a structure similar to that of 1: 14, 4, 2, 1,1,1,1,1,1.

1,5 It seems impractical to build an attachment to the bombs to test for these structures in the same way that the diagonal board tests for reciprocity. This is because such an attachment gets its power from the inferred completion of a cycle, and the long cycles are too frequently completed.

But this property may be used to test stories which have come from the bomb.

2. After the bombs have gotten one of the forty steckers, we still have the problem of determining the original. We consider an example

X G S X P K Y B S V D K S P L X G K Z P X X K I W F F
A N A N G U S T A V Y S O P A N T O N

We know the plain text of the message, the non-reciprocal stecker used, and the self-steckered letters used: A D F O W Y. The cycle structure of the stecker tells us that the heading, which cannot be read, is a number congruent to 2 modulus 4. We know it consists of eight letters. Therefore it is one of the following:

E I N S N U L L
E I N S V I E R
E I N S A C H T
Z W Ø S E C H S
Ø R E I N U L L
Ø R E I V I E R
Ø R E I A C H T

Letters known to be self-steckered are shaded.

None of these crash out. We must then try each of them. To do this we relay on self steckered letters.

2,1 We try

w x y z a b c d
X G S X P K Y B
- - - - N U L L

We get in succession L/B and B/R. Contradiction.

2,2 w x y z a b c d
X G S X P K Y B
E I N S V I E R

We get in order E/B, R/O, X/I, G/M, K/K. The last we know to be impossible.

2,3 w x y z a b c d
X G S X P K Y B
E I N S A C H T

We get H/B, T/U, P/Q, quite possible. To test further we turn to the table at the end of this paper, or try all possible steckers on S.

2,4 w x y z a b c d
X G S X P K Y B
Z W Ø S E C H S

We get H/B, S/U, S/U. This confirmation practically establishes that this is the correct case. Consulting the table we see that H is 0, 5, 10 or 14. Each assumption gives us the entire stecker, since S/U ties the cycles together.

3. To test a candidate for original stecker, we can use the known cycle structure as follows. Write out the recovered stecker in cycles: (BRSXQHPT) (CGENMZJVLUIK) (A) (D) (W) (F) (O) (Y). Then we note the interval in these sequences spanned by the stecker pairs recovered. In our case we have H/B, T/U, B/Q with intervals 3 in the 8-cycle, undefined, and 2 in the 8-cycle. If the components of the stecker pair are in different clcyes, the interval is not defined, and is ignored. Our table shows no interval 2 in the 8-cycle under hypothesis 18. In fact, no even interval is possible! Therefore this hypothesis is impossible.

TOP SECRET
ORLEM

WHEEL POSITION

SPAN CYCLE	1/14	1/4	2	3/14	5/14	7/14	CLASSES 1 & 3 STECKERS 14	4	2
1	0/10	----	----	8/16	5/14	2/15	(0 17 4 16 5 15 8 19 1 14 9 13 2 10)	(6 11 7 18)	(3 12)
3	8/16	----	----	0/10 4/11	----	1/12 3/18	(0 11 7 12 4 18 8 16 5 17 1 10 3 13)	(6 19 9 15)	(2 14)
5	6/17 2/15	7/19	----	0/10 3/18	5/14	----	(1 18 5 17 6 16 9 10 2 15 0 14 3 11)	(7 12 8 19)	(4 13)
7	6/17 1/12 4/11	0/10	----	9/13	5/14	----	(1 12 8 13 5 19 9 17 6 18 2 11 4 14)	(7 10 0 16)	(3 15)
9	----	----	5/14	6/17 7/19 1/12 2/15	4/11 3/18	----	(2 19 6 18 7 17 0 11 3 16 1 15 4 12)	(8 13 9 10)	(5 14)
11	0/10 9/13 7/19 2/15	----	----	3/18	5/14	----	(2 13 9 14 6 10 0 18 7 19 3 12 5 15)	(8 11 1 17)	(4 16)
13	1/12 7/19	----	----	3/18	----	8/16	(3 10 7 19 8 18 1 12 4 17 2 16 5 13)	(9 14 0 11)	(6 15)
15	----	----	----	7/19	4/11 8/16	0/10	(3 14 0 15 7 11 1 19 8 10 4 13 6 16)	(9 12 2 18)	(5 17)
17	6/17 4/11 3/18	1/12	----	----	5/14	----	(4 11 8 10 9 19 2 13 5 18 3 17 6 14)	(0 15 1 12)	(7 16)
19	5/14 8/16	----	----	1/12	4/11 2/15	----	(4 15 1 16 8 12 2 10 9 11 5 14 7 17)	(0 13 3 19)	(6 18)
21	0/10	----	----	7/19	3/18	4/11 5/14	(5 12 9 11 0 10 3 14 6 19 4 18 7 15)	(1 16 2 13)	(8 17)
23	9/13	----	7/19	8/16	2/15	6/17 3/18	(5 16 2 17 9 13 3 11 0 12 6 15 8 18)	(1 14 4 10)	(7 19)

E 7 - 45

RIP 609

CLASS 2

SPAN CYCLE	1 8	1 12	3 8	3 12	5 12	STECKERS 12	STECKERS 8
2	----	----	----	0/10 7/19	----	(0 11 5 15 3 19 8 17 7 10 1 13)	(6 18 4 12 2 16 9 14)
6	1/12	7/19	----	----	4/11 8/16	(1 12 6 16 4 10 9 18 8 11 2 14)	(7 19 5 13 3 17 0 15)
10	8/16	2/15	----	----	7/19 9/13	(2 13 7 17 5 11 0 19 9 12 3 15)	(8 10 6 14 4 18 1 16)
14	----	0/10 1/12	7/19 2/15	3/18 8/16	----	(3 14 8 18 6 12 1 10 0 13 4 16)	(9 11 7 15 5 19 2 17)
18	3/18 8/16	7/19 5/14	0/10	9/13	4/11 2/15	(4 15 9 19 7 13 2 11 1 14 5 17)	(0 12 8 16 6 10 3 18)
22	4/11 9/13	0/10 2/15	7/19	8/16	3/18 5/14	(5 16 0 10 8 14 3 12 2 15 6 18)	(1 13 9 17 7 11 4 19)
26	----	6/17 7/19	0/10 5/14	4/11 9/13	----	(6 17 1 11 9 15 4 13 3 16 7 19)	(2 14 0 18 8 12 5 10)
30	9/13	5/14	----	----	0/10 8/16	(7 18 2 12 0 16 5 14 4 17 8 10)	(3 15 1 19 9 13 6 11)
34	0/10	6/17	----	----	3/18 9/13	(8 19 3 13 1 17 6 15 5 18 9 11)	(4 16 2 10 0 14 7 12)
38	----	----	----	0/10 7/19	----	(9 10 4 14 2 18 7 16 6 19 0 12)	(5 17 3 11 1 15 8 13)

25	1/12 4/11 8/16	----	----	7/19	----	0/10	(6 13 0 12 1 11 4 15 7 10 5 19 8 16) (2 17 3 14) (9 18)
27	6/17 1/12 3/18	2/15	----	7/19 9/13	----	----	(6 17 3 18 0 14 4 12 1 13 7 16 9 19) (2 15 5 11) (8 10)
29	8/16	3/18	----	6/17 1/12	9/13 5/14	----	(7 14 1 13 2 12 5 16 8 11 6 10 9 17) (3 18 4 15) (0 19)
31	0/10	----	----	7/19 2/15 5/14	----	----	(7 18 4 19 1 15 5 13 2 14 8 17 0 10) (3 16 6 12) (9 11)
33	6/17 2/15	----	----	9/13	3/18	----	(8 15 2 14 3 13 6 17 9 12 7 11 0 18) (4 19 5 16) (1 10)
35	6/17	----	----	3/18	2/15 5/14 8/16	----	(8 19 5 10 2 16 6 14 3 15 9 18 1 11) (4 17 7 13) (0 12)
37	1/12	6/17	----	----	3/18 9/13 8/16	7/19	(9 16 3 15 4 14 7 18 0 13 8 12 1 19) (5 10 6 17) (2 11)
39	----	5/14	----	6/17	---- ←	0/10 4/11 7/19 2/15	(9 10 6 11 3 17 7 15 4 16 0 19 2 12) (5 18 8 14) (1 13)