Notes on Jaguar Problems

by

Lt. W. Randolph Church

15 July 1944

Abstract

The Enigma Uhr attachment converts the daily Stecker into any one of 40 possible modified Steckers, only 10 of which are reciprocal. (It was first introduced on the G.A.F. key Jaguar). The expected number of stops and stories is given for bombe runs with diagonal board unplugged.

Source: NARA, College Park, Md., Record Group 38, Crane Collection, Box 172, RIP 609, ARC Identifier: 6921398, HMS/MLR Entry Number: A1 1025, https://catalog.archives.gov/id/6921398
Enigma Series Volume 7, Article 8

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.

NOTES ON JAGUAR PROBLEMS

1. It is possible that the British will send one or more Jaguar problems to be run for non-reciprocal stecker.

2. The example furnished by the British is shown below (Engs 909, 912).

Position	BCDEFGHIJKLMNOPQRSTUVWXYZ
Cipher	CFDLZEJHLYMOGHRKAZNJTEYXK
Plain	EINSNULTHISSHOULDBEPLAINY
	←—A—→←————B————→

Part A is enciphered with ordinary reciprocal stecker,

Stecker A: B/H C/G E/X G/C H/B I/K J/N K/I L/R M/V
N/J P/Z Q/T R/L S/U T/QU/S V/M X/E Z/P

starting at AAB and wheels (B-9) 123. After that is complete the stecker is changed to the non-reciprocal stecker (this is determined by scale 10) in which the letter on the outside of the machine is given first

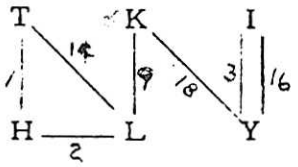
Stecker B: B/K C/T E/U G/Q H/C I/G J/R K/M L/Z M/X
N/B P/V Q/N R/E S/H T/J U/S V/I X/L Z/P

and the encipherment of part B is continued. (Actually this second stecker consists of the reciprocal stecker A preceded by a non-reciprocal substitution--or stecker--

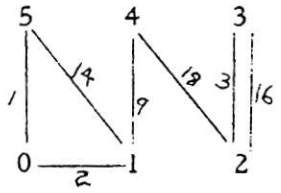
Stecker BA^{-1}: B/I C/Q E/S, etc.

probably applied mecahnically, but equivalent to performing the substitution on the plain and cipher text before and after encipherment with the machine and reciprocal stecker A.)

3. Such a problem gives rise to the menu



For convenience in running at the machines, the letters are replaced arbitrarily by O, 1, - - - - to give



Examination of the attached sheets will show that this is drawn up as usual (for either C hoppity, H hoppity, long, or other runs) except

a) all numbers on the menu except O should be unplugged from the diagonal board;
b) the original letters should be put on the test sheet above the column headings.

The bombes will print at every stop position; the number of stops is

$$\text{Stops} = \frac{26^{n+1}}{26^{c}}$$

where c is the number of closures and n the order of the machine cycle (3 or 4 wheel). An added factor for number of banks is needed for C-hoppity, as usual.

4. Since two letters cannot be steckered to the same one, the first step in testing prints is to reject those prints with a duplicate letter (this is done by the diagonal connections in normal runs). The remaining prints may be called stories. We have the relation

$$\text{Stories} = \text{Stops} \cdot \frac{25}{26} \cdot \frac{24}{26} \cdot \frac{23}{26} \cdot \text{- - - - -}$$

The number of factors multiplying the stops is one less than the number of letters in the menu (if there is no minor). Accordingly, as many letters as possible should be tied on to to menu to reduce the number of stories. (Note that this was not done with the sample problem.) A short table of the factor multiplying stops to give stories follows.

Letters in Menu	Factor
2	.961
3	.887
4	.785
5	.664
6	.536
7	.412
8	.301
9	.208
10	.136
11	.084
12	.048

5. Further test will, as usual, be for further plain text. There are two points to observe carefully.

a. The only principle for rejecting a possible stecker is to have two different letters steckered to the same letter, as in paragraph 4.

b. In using the partial stecker furnished by the print, and in adding to it, the order of each stecker pair must be carefully preserved. Error from failure of this kind will be avoided if the headings of the columns are replaced by letters as on the sample test sheet and if the testing is done only with letters. Then a given cipher or plain letter will be converted into a number by the print. Entering the M-9 with this number will produce a number which will be converted into a letter (plain or cipher) by the stecker.

6. In sending such problems to the machine, the serial number should be preceded by the letter N in addition to other letters, such as C or H.

/s/ W. R. CHURCH

W. R. CHURCH
Lieut., U.S.N.R.