The US Navy Bombe:
OP-20-G's First Thoughts

April 25, 1942

Unknown Author

Editors' Preface

This one-page document, written by an unknown author, was recently found by Ralph Erskine in the US Navy Security Group's Crane collection in the US National Archives. The document, in its present form, is published on the personal Web Page of Frode Weierud and has been faithfully retyped by the two editors, Ralph Erskine and Frode Weierud. The original document was typed and had the style and layout of a typewritten document of that period. To make the re-edited presentation more pleasing the document has been both left and right justified and a more modern type font has been used. Apart from these modifications to the layout the document has the appearance of the original.

Where there are obvious typing errors these have been corrected. The original text has been retained but with a stroke through while the corrections appear within square brackets. Where we are not sure about the corrections this has been indicated with a question mark.

The Editors,

Ralph Erskine,
Frode Weierud, © November 2000

Source:

National Archives and Records Administration (NARA), Record Group 38, Inactive Stations, Box 54, File: CNSG 3200/1.

Updated: 15 November 2000

SECRET [1]

April 25, 1942

It is desired to construct a machine of the general type and characteristics described below:

The machine is what may be described as a High-Speed Cipher machine. Here we seek to search all possible settings of a cipher machine of the following general set-up:

(a) There is a 26-place plug board into which can be sent current representing the letters of the alphabet scrambled in a random fashion but fixed throughout a single cycle of the machine.

(b) A maze through which is sent the current fed into the plug board. The maze is made of a set of cross-wired wheels, selected out of a larger set. The wheels rotate coaxially and move eccentrically each wheel picking up its motion when another wheel to which it is mated reaches a given position. For purposes of initial experiment it might be assumed that the full set of wheels is 10, that they are used 3 at a time, and that their motion is in ordinary meter fashion.

(c) A 26-place output-board from which the current passes after leaving the maze. NOTE: In actuality it would be desirable to consider the case in which the current leaving the maze the first time met a fixed reflecting board which sent the current back through the maze along a different path, and thus caused the input plugs to also serve as outposts.

Given such a machine it is desired to construct an ultra high speed representation of it, such that this representation would generate in proper sequence the successive effective cross-wirings between input and output plugs for any given wheel combinations; and when this full cycle has been completed, to repeat this process for all of the remaining wheel combinations.

The ultimate desire is to be able to run synchronously a series of machines initially set and thereafter run in such fashion that their settings are always at fixed intervals, each from the other. Further, the outposts of each machine would be wired to the inputs of its neighbors in a fashion to be determined by the cryptanalysts. It would then be required to discover and record those settings and wheel combinations for which the circuits established by these cross wirings were active.

Since it would be desired to test as many as possible of the inter-wirings of the machine determined by the cryptanalysts, there is no limit to the speed desired. to the number of hits expected, and consequent size of record, this would vary with the complexity of inter-wiring which the cryptanalysts might devise. On an average however, it might be said that no more than [?0?] hits for each trial of all wheel combinations and settings ~~is~~ [are] to be expected.

[1] The word SECRET is stamped on the original.