FOREWARD TO ENIGMA SERIES

CRYPTANALYTIC RESEARCH PAPERS

This series consists of original memoranda written by members of the cryptanalytic 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 of 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 cryptanalytic or mathematical theories which underly the techniques. On the other hand, machine research (from an engineering point of view) is not covered in this Series.

Some of the papers of 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 undersirable. In this line of endeavor, a chance remark may be worth a week's work.

The E-Series consists of the following volumes, this one being marked by a star.

	Volume			Title
RIP 603	E-1		have index	Click Process
" 604	E-2		" "	Indicator Attacks
" 605	E-3		have index	Statistical Studies
606 " 606	E-4		" "	Wiring Recovery
" 607	E-5	*	have index	Bombe Computations
608 " 608	E-6		"	Duenna
" 609	E-7		have index	Miscellaneous
" 610	E-8		have index	Reports From England
Box 63 " 601	E-9		have index	

The E-Series consists of the following volumes, this one being marked by a star.

	Volume	Title
	E-1	Click Process
	E-2	Indicator Attacks
	E-3	Statistical Studies
	E-4	Wiring Recovery
*	E-5	Bombe Computations
	E-6	Duenna
	E-7	Miscellaneous
	E-8	Reports From England

Index to Volume E-1

tried at every possible position, which is very tedious using the ordinary click process. The British solution is embodied in their "Click Machine". The American solution is embodied in HYPO, which is based on a statistical solution, and is preferable for fairly long messages since no crib is needed (see Volume 3, Articles 2-5). Articles 5, 6, and 8 are concerned with methods for crib-dragging. Regarding Article 8, Medusa itself was not built, but it stimulated the construction of the Drag Grenade.

TOP SECRET ~~ULTRA~~ CREAM

INDEX TO VOLUME E - 2