

TOP SECRET - ULTRA

TABLE OF CONTENTS AND LIST OF EFFECTIVE PAGES

<u>CONTENTS</u>	<u>CHANGE NO.</u>	<u>PAGE NO</u>
Letter of Promulgation	0	I
Distribution List	0	II
Correction Page	0	III
Table of Contents and List of Effective Pages	0	IV-V
Foreword	0	VI
Table of Figures	0	VII-IX
<u>PART I - INTRODUCTION</u>	0	1-2
Purpose of Book - to illustrate how abuse broke an unbreakable machine.		
<u>PART II - THE MACHINE</u>	0	2-29
a) General Characteristics	0	2-10
b) Its Security - Basic Test - The Maze and its elements - Stecker - Wheels - Reflector Combination.	0	10-18
c) Weaknesses of the Device - regularity of motion and brevity of cycle - Stecker, Wheels, Reflector & Reflector Wheel	0	18-20
d) Possible Remedies - Multiple Notches - Varying number of Non-Reciprocal Steckers - Pluggable Reflectors	0	21-22
e) Summary - Still a highly secure machine if properly used.	0	22-29
<u>PART III - USAGE OF THE MACHINE - GENERAL</u>	0	29-41
a) General Regulations for the Enigma Capture and Betrayal versus Cryptanalysis	0	29-32
b) Cipher Aids - Key Sheets - Allotment Lists - Indicator Book - Bigram Tables - Areas	0	32-38
c) Emergency Procedures - Machine out of Order, Hand Procedure - Compromise, New Keys	0	38-41
<u>PART IV - FLAWS OF PARTICULAR CRYPTOGRAPHIC AIDS</u>	0	41-95
a) Introduction - general flaws - gradual and systematic changes.	0	41

CHANGECHANGE NO.PAGE NO.

b) General Key Sheets - System in Wheel Orders - Non-random and 3-Wheel Rings. Six Self-Reciprocal Steckers - Systematic Grunds.	0	41-47
c) Allotment Lists - Blocks of adjacent numbers - overlapping Bigram Tables	0	47-51
d) Kennbuch - Well constructed but too long used.	0	51-55
e) Bigram Tables - Needlessly reciprocal - Infrequent change - Betrayed by Dummies	0	55-59
f) Offizier, Stab & Sonder Keys - Steckers last too long Non-random Settings - "good for all months"	0	59-68
g) Key changes when Compromised - Reserve on Board - Slides - Not Slippery enough - Standard Phraseology.	0	68-72
h) Reserve Hand Systems - Discriminating this type of Cipher - Substitution and Transposition - Analogous Non-Atlantic Practice	0	73-85
i) Cipher Areas - Cover Names Increasing Complexity - New Keys not really so.	0	85-95
 PART V - <u>UNDERLYING TEXT - U-BOATS</u>	0	95-107
a) Principal Codes	0	95-107
i) Fleet Short Signal	0	97-102
ii) Weather Short Signals	0	102-105
iii) E-Bar Signals	0	105-107
iv) Disguised Squares	0	107a
b) Plain Text Usage - The Worst German Crime - What Allied Cryptanalysts needed was given - Standard Phraseology - Re-Encodements - the easy way out not taken.		108-112
 PART VI - <u>NON-ATLANTIC AND NON-U-BOAT SYSTEMS</u>	0	113-132
a) Naval Saboteur	0	113-115
b) Merchant Marine	0	115-120
c) Naval Attache	0	120-129
d) Jap-German Liaison	0	129-131
e) Minor Codes and Ciphers	0	132-134
 PART VII - <u>THE INDICTMENT OF GERMAN CRYPTOGRAPHERS</u>	0	134-136
a) A review of the counts.	0	134-135
b) The moral of the story		135-136

TOP SECRET-ULTRA

<u>LIST OF FIGURES</u>	<u>PAGE</u>
1a. Schlüssel M - The German Cipher Machine	3
1b. Schlüssel M - Wheel cover Open	4
2a. Captured Enigma Wheel No. III (left side)	5
2b. Captured Enigma Wheel No. III (right side)	6
2c. Captured Enigma Wheel No. III (front view)	7
3. Schlüssel M - Power Supply and Printer	8
4. Diagram of Electric Circuit through Schlüssel M - Machine	9
5. Stecker Plugs	12
6. Captured Enigma Wheel (smashed)	13
7. Enigma Reflector (front and back view)	15
8a-f. General Regulations and Translations	23-28
9. German List of Cipher Aids	30
10. Folder for Cipher Aids	31
11. Sample of Intercepted Enigma Message	36
12a. Inner Settings for Triton Keys, June 1945	39
12b. Outer Settings for Triton Keys, June 1945	40
13. Cipher Allotment List - Coverword "Forelle"	45
14. Effective dates of Allotment Lists	46
15a. The general Indicator Book (K-Buch) Cover	48
15b. Sample Page Part I - K-Buch (Numerical)	49
15c. Sample Page Part II - K-Buch (Alphabetical)	50
16a. Coversheet for Bigram Table "Teich"	52
16b. Indicator Table Plan - "Teich"	53
16c. Bigram Table A - "Teich"	54
17a. Offizier Key Sheet, June 1945	57
17b. Envelope for Offizier Keys, June 1945	58
17c. German Cipher Form	60