Contents

Preface xiii
Editorial Notes xiv
Notes on Vocabulary xiv
List of Abbreviations xv
Cryptanalytic Significance of the Analysis of Tunny, by Whitfield Diffie xvii
Editors’ Introduction, by Whitfield Diffie and J. V. Field xxv
Statistics at Bletchley Park, by S. L. Zabell lxxv
Biographies of Authors ciii
Notes on the Editors of the Present Volume cvii
List of Figures cix

General Report on Tunny, with emphasis on statistical methods 1

Part 0: Preface

Chapter 01: Preface 3

Part 1: Introduction

Chapter 11: German Tunny 6
  11A: Fish machines 6
  11B: The Tunny cipher machine 10
  11C: Wheel patterns 16
  11D: How Tunny is used 18
  11E: The Tunny network 19

Chapter 12: Cryptographic Aspects 22
  12A: The problem 22
  12B: Modern strategy 23
  12C: Chi breaking and setting: Solution of \( Z = \chi + D \) 25
  12D: Motor and psi breaking and setting: Solution of \( D = P + \psi \) 29
  12E: Methods involving key: Solution of \( Z = K + P \), and \( K = \chi + \psi \) 30

Chapter 13: Machines 32
  13A: Explanation of the categories 32
  13B: Counting and stepping machines 33
  13C: Copying machines 34
  13D: Miscellaneous simple machines 34

Chapter 14: Organisation 35
  14A: Expansion and growth 35
  14B: The two sections in 1945 36
  14C: Circulation 37

Chapter 15: Some Historical Notes 39
Contents

Part 2: Methods of Solution

Chapter 21: Some Probability Techniques

Chapter 22: Statistical Foundations

22A: Introductory
22B: The chi-stream
22C: The motor stream
22D: The psi stream
22E: The sum of two streams
22F: The key stream
22G: The plain language stream
22H: The de-chi stream
22J: The cipher stream
22K: Sampling errors in alphabetical counts
22W: Some further streams
22X: The algebra of proportional bulges
22Y: The amount of evidence derived from a letter count

Chapter 23: Machine Setting

23A: Introduction
23B: The choice of runs
23C: Weighing the evidence
23D: Annotated exhibits
23E: $\chi$-setting with $\chi^2$ limitation
23F: Message slides
23G: Wheel slides
23H: Flogging runs
23J: Flogging the evidence
23K: Checks on setting
23L: Statistical setting of the motor
23M: $\psi$-setting
23N: Coalescence
23P: Example
23W: Calculation of the odds of the best score in a $\chi$-setting run
23X: Theory of coalescence
23Z: History of machine setting

Chapter 24: Rectangling

24A: Introductory
24B: Making and entering rectangles
24C: Crude convergence
24D: Starts for converging rectangles
24E: Rectangle significance tests
24F: Conditional rectangle
24G: Some generalized rectangles
24W: Theory of convergence
24X: Significance tests
Contents

24Y: Other theory of rectangles 136

Chapter 25: Chi-Breaking from Cipher 139
25A: The short wheel-breaking run 139
25B: Weighing the evidence 142
25C: General plan of wheel-breaking 144
25D: Particular methods 146
25E: Special methods for $\chi^2$ limitation 150
25F: Special method for $ab = 1/2$ 152
25G: Wheel-breaking exhibits 152
25W: Derivation of formulae for the weighing of evidence 180
25X: The number of legal wheels 183
25Y: Proportional bulges relating to $\chi^2$ 183

Chapter 26: Wheel-Breaking from Key 185
26A: Introduction 185
26B: Starts 185
26C: Hand counting for $\chi^2\psi_1$ limitation 191
26D: Recognising the $\psi$ repeat and numbering 194
26E: Hand counting on $\chi^2$ key 194
26F: Devil exorcism 195
26G: Key work in the Newmanry 195
26H: General considerations 198
26J: Exhibits 198
26X: Key-breaking significance tests 213
26Y: Formulae used in key-breaking 215

Chapter 27: Cribbs 219
27A: General notions 219
27B: German TP links 220
27C: German TP operating practices 221
27D: Crib prediction 222
27E: Preparation of decode and cipher 223
27F: Tape making 224
27G: Statistical technique: running on Robinson 226
27H: History of crib organisation 231
27W: Basic crib formula 231
27X: $598$ theory 232
27Y: $31$ theory 234

Chapter 28: Language Methods 237
28A: Depths 237
28B: $\psi$ setting from de-$\chi$ 239
28C: $\psi$-Breaking from de-$\chi$ 244
28D: Motor breaking and setting 246
28E: Decoding 251

Part 3: Organisation

Chapter 31: Mr Newman’s Section 262
31A: Growth 262
31B: Staff requirements 262
31C: Administration 263
Contents

31D: Cryptographic staff 263
31E: W.R.N.S. 264
31F: Engineers 265
31G: Education 265
31H: Statistics bureau 266
Chapter 32: Organisation of the Testery 267
Chapter 33: Knockholt 268
  33A: Ordering tapes 268
  33B: Treatment of tapes 268
Chapter 34: Registration and Circulation 269
Chapter 35: Tapemaking and Checking 271
  35A: Introduction 271
  35B: General rules 271
  35C: Checking and alteration of tapes 271
  35D: Preparation of message tapes 272
  35E: Making of de-chis 273
  35F: Wheel tapes and test tapes 273
  35G: Rectangles 274
  35H: Other Tunny jobs 274
Chapter 36: Chi-Breaking from Cipher 275
  36A: History and resources 275
  36B: Rectangles and chi2 cap runs 275
  36C: Times 276
Chapter 37: Machine Setting Organisation 277
Chapter 38: Wheel-Breaking from Key, Organisation 280
Chapter 39: Language Methods 282
  39A: Circulation 282
  39B: Cryptography 282
  39C: Decoding 283
  39D: Issuing 283

Part 4: Early Methods and History

Chapter 41: The First Break 284
  41A: Early traffic 284
  41B: Tunny shown to be a letter subtractor 285
  41C: A depth read 285
  41D: Key analysed 286
  41E: Two more depths 289
Chapter 42: Early Hand Methods 290
  42A: First efforts at message setting 290
  42B: Machine breaking for March 1942 291
  42C: Message setting for March 1942 292
  42D: April 1942 293
  42E: The indicator method 294
Chapter 43: Testery Methods 1942–44 298
  43A: Breaking Tunny August–October 1942 298
## Contents

43B: Turingery 298
43C: The pre-Newmanry QEP era 300
43D: The foundation of the Newmanry and after 302

Chapter 44: Hand Statistical Methods 305
44A: Introduction of the QEP (QSN) system 305
44B: Setting — statistical methods 306
44C: Introduction of $P_\chi$ limitation 308

### Part 5: Machines

Chapter 51: Introductory 309

Chapter 52: Development of Robinson and Colossus 312

Chapter 53: Colossus 316
53A: Introduction 317
53B: The $Z$ stream 317
53C: The $\chi$, $\mu$, $\psi$ streams 318
53D: Stepping and setting 319
53E: Differencing 319
53F: Counting 320
53G: Recording of scores 320
53H: Spanning 322
53J: $Q$ panel 323
53K: Plug panel 326
53L: Multiple test 328
53M: Colossus rectangling gadgets 332
53N: Control panel 334
53P: Colossus testing 334

Chapter 54: Robinson 336
54A: Introduction 336
54B: How scores are exhibited 336
54C: Bedsteads and position counting 337
54D: The plug panel 338
54E: The switch panel 340
54F: Miscellaneous counter facilities 342
54G: The printer 343
54H: Control tapes 343
54J: Some Robinson plugging used operationally 344

Chapter 55: Specialized Counting Machines 346
55A: Dragon 346
55B: Proteus 347
55C: Aquarius 348

Chapter 56: Copying Machines 350
56A: Hand perforator 350
56B: Angel 350
56C: Insert machine 350
56D: Junior 351
56E: Garbo 351
56F: Miles 352
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data</td>
<td>352</td>
</tr>
<tr>
<td>56H: Miles A</td>
<td>355</td>
</tr>
<tr>
<td>56J: Tunny and decoding machines</td>
<td>358</td>
</tr>
<tr>
<td>56K: The (Newmanry) Tunny machine</td>
<td>358</td>
</tr>
<tr>
<td>56L: Decoding machine</td>
<td>360</td>
</tr>
<tr>
<td>Chapter 57: Simple machines</td>
<td>361</td>
</tr>
<tr>
<td>Chapter 58: Photographs</td>
<td>362</td>
</tr>
<tr>
<td><strong>Part 6: Raw Materials</strong></td>
<td></td>
</tr>
<tr>
<td>Chapter 61: Raw Materials — Production, with Plans of Tunny Links</td>
<td>381</td>
</tr>
<tr>
<td><strong>Part 7: References</strong></td>
<td></td>
</tr>
<tr>
<td>Chapter 71: Glossary and Index</td>
<td>387</td>
</tr>
<tr>
<td>Chapter 72: Notation</td>
<td>435</td>
</tr>
<tr>
<td>Chapter 73: Bibliography</td>
<td></td>
</tr>
<tr>
<td>Chapter 74: Chronology</td>
<td>444</td>
</tr>
<tr>
<td><strong>Part 8: Conclusions</strong></td>
<td></td>
</tr>
<tr>
<td>Chapter 81: Conclusions</td>
<td>452</td>
</tr>
<tr>
<td>81A: Organisation</td>
<td>452</td>
</tr>
<tr>
<td>81B: Theory</td>
<td>454</td>
</tr>
<tr>
<td>81C: Machines</td>
<td>455</td>
</tr>
<tr>
<td><strong>Part 9: Appendices</strong></td>
<td></td>
</tr>
<tr>
<td>Chapter 91: The 5202 Machine</td>
<td>456</td>
</tr>
<tr>
<td>91A: Principle of the 5202</td>
<td>456</td>
</tr>
<tr>
<td>91B: Technical aspects</td>
<td>458</td>
</tr>
<tr>
<td>91C: Times and routines</td>
<td>464</td>
</tr>
<tr>
<td>91D: Crib run</td>
<td>467</td>
</tr>
<tr>
<td>91E: Conclusions</td>
<td>467</td>
</tr>
<tr>
<td>Chapter 92: Recovery of Motor Patterns from De-chi</td>
<td>471</td>
</tr>
<tr>
<td>92A: Introduction and outline</td>
<td>471</td>
</tr>
<tr>
<td>92B: Decibanage of $D$ letters</td>
<td>472</td>
</tr>
<tr>
<td>92C: Construction of Motor Rectangle</td>
<td>473</td>
</tr>
<tr>
<td>92D: The Scoring of Columns against each other</td>
<td>473</td>
</tr>
<tr>
<td>92E: The Recovery of Patterns (A). Finding the dottage of $\mu_{61}$</td>
<td>474</td>
</tr>
<tr>
<td>92F: The Recovery of Patterns (B). The approximate $\mu_{57}$ and $\mu_{61}$</td>
<td>476</td>
</tr>
<tr>
<td>92G: Finishing off the $\mu$’s</td>
<td>478</td>
</tr>
<tr>
<td>92H: Recovery of the $\psi$ patterns</td>
<td>479</td>
</tr>
<tr>
<td>92I: Example of method (b)</td>
<td>479</td>
</tr>
<tr>
<td>92K: Experiment in recovery by method of the smooth $\mu_{61}$</td>
<td>479</td>
</tr>
</tbody>
</table>
## Contents

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>93</td>
<td>Thrasher</td>
<td>482</td>
</tr>
<tr>
<td>94</td>
<td>Research into the QEP System</td>
<td>484</td>
</tr>
<tr>
<td>95</td>
<td>Mechanical Flags</td>
<td></td>
</tr>
<tr>
<td></td>
<td>95A: General description</td>
<td>488</td>
</tr>
<tr>
<td></td>
<td>95B: Mechanical ordinary flag</td>
<td>489</td>
</tr>
<tr>
<td></td>
<td>95C: Mechanical combined key flag</td>
<td>491</td>
</tr>
<tr>
<td>A</td>
<td>Appendix A: Transmission of Teleprinter Signals, by J. A. Reeds</td>
<td>495</td>
</tr>
<tr>
<td>B</td>
<td>Appendix B: Activities at Knockholt, by J. A. Reeds</td>
<td>503</td>
</tr>
<tr>
<td>C</td>
<td>Appendix C: The 5202 Machine, by J. A. Reeds</td>
<td>530</td>
</tr>
<tr>
<td>D</td>
<td>Appendix D: Initial Conception of Colossus, by J. A. Reeds</td>
<td>535</td>
</tr>
<tr>
<td>E</td>
<td>Appendix E: List of Scanned Exhibits</td>
<td>540</td>
</tr>
<tr>
<td></td>
<td>Supplementary Glossary</td>
<td>542</td>
</tr>
<tr>
<td></td>
<td>Biographical Notes</td>
<td>547</td>
</tr>
<tr>
<td>Notes</td>
<td></td>
<td>561</td>
</tr>
<tr>
<td>Bibliography</td>
<td></td>
<td>624</td>
</tr>
<tr>
<td>Index</td>
<td></td>
<td>645</td>
</tr>
</tbody>
</table>