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
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

Page

Article 1. Enigma Machine.
Greenwood, 13 November 1943. 1
An introduction to the principal features of the machine.

Article 2. Recovery of the Grundstellung.
Greenwood, 1 February 1943. 8
This paper describes the basic "click" process which is used to find the setting of a message from a short crib, when the Stecker is known. As an example, two messages are set, and then the Grundstellung is recovered by the same process from the resulting two four-letter cribs. For a brief account of the indicator system, of which the Grundstellung is a part, see Volume 2, Article 1.

Article 3. The Number of Stories Expected From the Click Process.
Howard & Clifford, 13 October 1942. 22
The click process is described in detail, and the number of chance answers is computed for every crib length up to ten. These answers are broken down according to the click pattern in poker-hand fashion. Mr. Turing of G.C.C.S., England, pointed out that these calculations could be simplified by means of a recursion formula, although the full poker-hand breakdown is lost (see Volume 6, Article 4-C).

Article 4. Click Probabilities at Correct Position.
Howard, October 1942. 45
The probability of each click pattern is given for a crib up to ten letters in correct position. Mr. Turing's remark holds here as well as for Article 3.

Article 5. Notes on "Click" Process.
Menzel, 27 February 1943. 53
A reversal of the usual process, which enables one to drag a crib through a message without having to reload the click board.

Editor's Note: Frequently a good crib may exist for a message, but may occur anywhere in it. It must therefore be

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.

Article 6. Dragging a Certain Crib Through a Long Message Where Wheel Order and Stecker Are Known.
Ely & Cramer, Spring 1943. 58
The crib and cipher text are stripped through each of the 26 possible positions of the fast wheel, and compared for symmetry. This would be quite easy to do at the present time (1 June 1945) using either the NC-5 or Tessie (rigged for symmetric sequences); in fact the former is being used for such a job on the T-machine.

Article 7. Location of Basic Setting After Successful Bombe Solution.
Howard, 21 August 1942. 64
This article contains the original grenade idea, equivalent to the British "eel".

Article 8. Enigma Drag Machine (Medusa).
Moise, 11 October 1944. 67
This proposes a machine to try simultaneously, by means of two relay matrices, every possible position in a message for a four-letter crib with Stecker known.

TOP SECRET ~~ULTRA~~ CREAM

INDEX TO VOLUME E - 2

Page

Article 1. Recovery of Grundstellung With Bigram Tables Unknown.
Clifford, 6 March 1943 1
After a brief description of how the bigram tables are used to encipher the indicator, it is shown how one can recover the Grundstellung without the Bigram Tables by running a query menu on the grenade ("tandem-wired bombe").

Article 2. Connection Between JN-171 (JJC) and DAN.
Wray and Greenwood, 27 February 1943. 7
The connection is established by repeated trigrams in the first and last groups.

Article 3. Preliminary Report (to G.C.C.S.) of Initial Break Into JN-171.
Wray, 9 July 1943. 10
Identification of the two classes of traffic is presented. Class I is unmistakably enigma, exhibiting indicator "throw-ons". Class II exhibits vertical bigram characteristics (R.H.V. type), using 5 columns. The original of this article was sent to G.C.C.S., England, and Stimulated the British to run a throw-on menu on the bombes, which struck oil. The British christened the system "Sunfish".

Article 4. Historical Summary of JN-171.
Greenwood, 17 September 1943. 12
A complete history of the break into Sunfish.

Article 5. Kriegsmarine Indicators.
Gleason, Greenwood & Hall, 25 June 1943. . . . . .
An exposition of how the crucial hypothesis that the letters A-M were reserved for Tokyo to Berlin messages in the second indicator position, and N-Z for Berlin to Tokyo, serves to determine the Grundstellung alphabets G+1 and G+5. This induced the British to put a throw-on menu on their 4-wheel bombes (ours not having enough banks), which hit the jackpot after numerous mechanical troubles. The British christened the system "Seahorse".

INDEX TO VOLUME E-2

Page

Article 5. (Contin.) While waiting for the British to make the trial run, an attempt was made to recover the wiring from the indicator alphabets (see Article 4 in Volume 4). 24

Article 6. History of Kriegsmarine Attack.
Greenwood. 27 September 1943. 28
A complete history of the break into Seahorse.

Article 7. Formula for a Seahorse Probability.
Gleason, January 1945. 32
This concerns the number of stops in a grenade run (wheel order and Stecker known), when the information plugged up is the set of 13 letters going into letters of the set A-M.

o Article 8. Enigma Machine - Indicator Analysis.
Greenwood, 15 November 1943. 36
A thorough job was done on the sample of a day's Home Waters traffic (678 messages) sent us early in 1942 by the British as an educational problem. The British procedure is described in Article 2, Volume 8, from an operational standpoint. The present article goes more into the underlying theory.

Article 9. Continuing British Attack.
Ely, 4 March 1942. 50
Remarks that the cycles (or "boxes" in British terminology) formed from the two recovered successive Grundstellung alphabets should cut down the number of possible settings considerably.

o Article 10. Presentation of Double Grund Problem.
Ely, 19 June 1944. 53
This article presents the problem, together with a few ideas thereon.

o Article 11. Indicator Analysis in Double Grund System.
Campaigne, 24 June 1944. 55
This article shows how one can recover the component Grundstellung alphabets uniquely from two double Grund alphabets having one Grund in common.

INDEX TO VOLUME E-2

Page

Article 12. Expected Number of Stops in a Double Grund Grenade Run.
Greenwood, 9 August 1944, ... 58
A brief account is given of how the British bombe out the daily (net) Grund and Ringstellung, knowing two of the station Grunds, and the expected number of stops is calculated and tabulated. This bombing technique led to the Pluggable Grenade.

INDEX TO VOLUME E-3

		Page
Article 1.	Dottery. Eachus & Clifford, 8 January 1943	1
	This is the standard British method of recovering the Stecker without a crib when the wheel order and setting of a message is known. (For a method with crib, see Article 4, Volume 7).	
Article 2.	HYPO - General Nature and Projected Use. Ely, 17 March 1943	12
	The Hypo machine is the American solution to the problem of finding the setting of a message, without using a crib, when the Stecker (and usually the wheel order) is known.	
Article 3.	Notes on the Use of EEE----Sequence. Greenwood, Krall & Wray, 12 April 1943	25
	A study on how effectively a message could be set by counting coincidences between it and an encipherment of the letter E at every position of the machine cycle (a simplification of the Hypo principle). The method was later successfully applied on a 3-wheel problem, using the I.C. machines, before Hypo came aboard.	
Article 4.	Use of an All "E" Sequence. Greenwood, 16 September 1943	32
	Application of the method of Article 3 to recover the Ringstellung of the initial Seahorse break. It would have been successful, had not the British found the rings first by other means.	
Article 5.	Use of HYPO for Wired Wheels With Unknown Ring Settings. Greenwood, 7 July 1944	38
	It is shown that Hypo has sufficient power to set a message of 430 letters making only 6 (out of 676 possible) runs, namely with two assumed ring settings for the cipher (called the	

INDEX TO VOLUME E-3

		Page
Article 6.	Statistical Determination of Fast Wheel Position. Ely, 29 April 1943 . . . . . By stripping the cipher text and the high-frequency letters through the (known) Stecker and through the fast wheel in each of its 26 possible positions, as in the Hypo procedure, and counting all click possibilities, a two-sigma bulge over random expected was found on a 390-letter message.	52
Article 7.	A Statistical Method for Determining the Fast Wheel Position for an Enigma Message. Eachus, 16 January 1945 . . . . . As in the preceding article, the Stecker must be known, and the identity of the fast wheel known or assumed. The method depends on counting click possibilities arising from plain text diagraphs which occur in the rod square of the wheel. As pointed out by the author, "a large number of notches at unknown positions would invalidate the method, which is exactly what happened when it was applied to the Cougar depth (Volume 7, Article 10).	66
Article 8.	A Recognition Test for "Strip" Cipher. Greenwood, 11 January 1945 . . . . . A scoring test is presented for telling whether a (sufficiently large) sample of cipher text is of "strip" (or "non-crashing" type) enciphered in such a way that no letter can go into itself, but is evenly spread over the remaining 25 letters (as in enigma text). This test is then applied to various classes of traffic.	77
Article 9.	Distinction Test for Romaji and German. Greenwood, 20 March 1944 . . . . . A test for telling whether the plain text underlying a batch of enigma traffic (or any non-crashing system) is Romaji or German.	86

INDEX TO VOLUME E-3

Page

Article 10. Analysis of Known Plain-Cipher Line-Ups.
Moise, 12 November 1943. 90
An experimental test of the British method of counting a reencodement (plain-cipher line-up) for (1) probable location of fast wheel turn-over, (2) whether fast wheel has one or two turnover notches (type "Sigma" or "Delta" respectively). This method is reported in Volume 8, Article 4. The results of Article 10 point to the conclusion that (1) is effective, but (2) is not.

INDEX TO VOLUME E - 4

Page

o Article 1. Beta Wheel or Umkehrwalz or Both Unknown.
Clifford, 12 January 1943. 1
A method is described of how to recover the wiring of the Beta wheel and Umkehrwalz, when both of these are unknown, from three successive "combined Umkehrwalz" alphabets. This is equivalent to the recovery of a "one-wheel" enigma with known Stecker, i.e. an enigma consisting of simply a single moving wheel and reflector.

Article 2. Reproduction of Wheel Wiring by Means of a Crib.
Krall, 11 March 1943. 9
The method of Article 1 is extended to apply to a crib of 140 letters. It was later found that the method was a standard one with the British - not surprising. The essential step of advancing the cipher letters in the rth text column r-1 steps along the normal alphabet (or along the end-plate sequence, such as QWERTZU . . ., if it is other than normal), is called "buttoning the text onto the fast wheel".

Article 3. On the Possibility of Determining Wheel Wirings by Digraphic Counts.
Greenwood, Spring 1943. 15
The cipher text is buttoned onto the fast wheel (called "stripping" here), and a digraphic count is made of the buttoned text. The 26 digraphs on the left side of the fast wheel form a sort of closed set in that any one enciphers into another of the set, if not broken by a turnover. From this closed set one could recover the wiring of the fast wheel. However, 19,000 digraphs was not nearly enough to identify this set.

Article 4. Kriegsmarine Indicators.
Gleason & Greenwood 25 August 1943. 26
It is shown how the wiring of the fast wheel can be recovered, with known Stecker, from the pairs of

INDEX TO VOLUME E - 4

Page

Article 4. (contin.) successive alphabets G+1, G+2, G+5, G+6. In fact, G+2 and G+6 need not be unique. An attempt was made to apply this to the Kriegsmarine Grundstellung alphabets which had been recovered (see Volume 2, Article 5), assuming the end-plate sequence QWERTZU. . . . Since this traffic uses a steckered machine (4-wheel naval), the attempt was doomed to failure.

Article 5. Report on GM-8 Project M-211.
Moise, 10 November 1943. 34
A first attempt to recover the wiring of the fast wheel from a long crib with unknown Stecker. When the Stecker is unknown, we cannot button the text onto the fast wheel, and so an entirely new attack must be made. The problem was later successfully solved (Article 8 below).

Article 6. On the Elimination of "Twists" in Wired Wheels.
Greenwood, 2 January 1945. 36
In a wiring recovery problem, there is an inescapable ambiguity in the recovered wheel known as a "twist". This can be visulaized as taking hold of both faces of the wheel, and rotating one face relative to the other. Such a twist is then compensated for by a rigid rotation (not a twist) of the combined reflector. This malady can be cured only by a correct recovery of the Rings, or by a change in wheel order

Article 7. Enigma Wiring Recovery from the Reading of a Depth.
Greenwood, Gleason, Clifford & Hanson.
19 April 1945. 47
This is with Stecker unknown. Reading the depth of 20 gives us a block of partial (but reasonably fat) alphabets. The ones actually used are 1-4, 27-30, 53-56, and 79-82. Menu #1 is formed from alphabets 1, 27, 53, 79; Menu #2 from 2, 28, 54, 80; etc. These menus are isomorphic, and the first step is the recovery of the substitutions T_1, T_2, T_3 transforming Menu #1 into #2, #2 into #3, and #3 into #4. T_3 is a transform of T_2, and T_2 of T_1, both by the same

INDEX TO VOLUME E - 4

Page

Article 7. (contin.) substitution. Recovery of the latter immediately yields the Stecker. The idea behind this method was discovered (by Gleason) from group-theoretical considerations. A brief account of the latter is given in paragraph 3, page 15, of this article. This method can also be applied to a long crib, as indicated in Paragraphs 5 and 6.

Article 8. Recovery of Enigma Wheel Wiring from a Long Crib. Hall & Hampton, 26 May 1945. 76
With Stecker unknown, as in Article 7, the Stecker and wheel wiring are recovered from a crib of 5000 letters. The approach (which is rather different from that employed in the last part of Article 7) is to attack the wheel square directly. The latter is visualized as containing the unknown Stecker in its diagonal.

INDEX TO VOLUME E-5

RIP 607

		Page
Article 1.	American Hot-Point Method. Clifford, August 1942. . . . . An account of the operation of the bombe, as we conceived it at that time, and of the computation of the expected number of chance answers (here called "successes", and called "stories" by the British). These were later recomputed more exactly, and are tabulated in Article 3. For an algebraic formula, see Paragraph 2 of Article 4.	1
Article 2.	Number of Ways of Intersteckering N Letters. Howard & Pearsall, 12 December 1942. . . . . This article tabulates the number of ways of intersteckering N letters, from N=1 to N=26, broken down according to the number of self-steckers.	18
Article 3.	Table of Number of Stories to be expected From Chance. Church & Howard, 5 April 1943. . . . . This is Church's modification of Howard's basic table, with an explanatory note by the Editor. It gives the number of stories for a single short run (3-wheel cycle). For a long run (4-wheel cycle), multiply each entry by 26.	27
Article 4.	Clark Test. Clifford, 22 May 1945. . . . . This test (invented by and named after a Britisher) evaluates the merit of a story from its "confirmations" - the number of self-steckers and pairs of intersteckered menu letters. We computed the table in late 1942, but not (as it now appears) the best possible way.	29
Article 5.	Expected Number of Stories When Subsidiary Chain is Present. Clifford, October 1942. . . . . If the menu is in two disconnected pieces (called main chain and subsidiary chain), and both are energized on the bombe ("double	33

INDEX TO VOLUME E-5

RIP 607
Page

Article 5. (Contin.) input" or "D.I.") the number of stories to be expected by chance is simply 25 times what the number would be if the two chains were connected by a single link. But if only the main chain is energized ("single input" or "S.I") a great deal of further computation is called for. This article explains the method, and verifies the British S.I. table for a single case. . The reason why we failed to verify the British D.I. table is that their meaning of a D.I. story is a case which is a story on the main chain and a stop on the subsidiary. A case which is a story on both they call a "Warspite" story.

Article 6. Single Input Stories - Short Run.
Howard & Pearsall, Fall 1942. 47
These tables give the end result of the program of calculation outlined in Article 5, together with the British figures for comparison. The good agreement is no indication that our labor was wasted - we needed greater accuracy in the scarce regions because each entry must be multiplied by 26 for a 4-wheel run. Thus the case 13-3-0, which is not given at all on the British table, yields one tenth of a story on a short run, or 2.6 stories on a long one.

Article 7. Double Input Bombes.
Campaigne, 29 March 1944. 52
An experimental investigation to see if it would pay to rig our bombes with double input.

Article 8. Distribution of Number of Stops
Howard, Summer 1943. 54
Results of counting the number of stops in each of 336 runs on a test menu are exhibited graphically.

Article 9. Note on Expected Number of Stops.
By the Editor, 29 May 1945. 55
We never succeeded in computing the expected number of stops. This note explains the difficulty, and describes briefly an averaging method we might have used. As a substitute, L. Cdr. Church extrapolated from the British tables, with satisfactory operational results.

INDEX TO VOLUME E-6

Page

Article 1. Introduction to Duenna.
The Editor, 28 May 1945. 1
The basic cryptanalytic procedure, for which Duenna was designed, is described and illustrated by an example. This procedure is really very simple. No knowledge is required of the British method of hand-breaking (Article 3, Volume 8), nor of the "equidistances" on which it bases its attack. We consider the possibility of rigging Duenna to take advantage of them, but decided it was not worth while. Historically, however, Duenna traces her ancestry to hand-breaking, through Campaigne's masks (Article 6, Volume 7), and Mona, a one-wheeled machine which was never built.

Article 2. Conference, 27 May 1944. 4
This report may serve to give some idea of the accessories that were put on Duenna, and also of the problems that confronted us in its design and projected operation.

Article 3. Alexander's Tables. 7
These tables, giving in a sense the expected number of stops ("no-come-outs") for menus of a certain simple type, are described in Paragraph 5 of Article 2. They were computed by Mr. C. H. O'D. Alexander, of G.C.C.S., England, while he was visiting the Naval Communication Annes. He did all the preliminary cryptanalytic spade-work for Duenna.

Article 4. Performance of Duenna
Clifford, 7 September 1944. 11
This work represents the result of our efforts to answer the questions put in Article 2. After a brief introduction, the component memoranda are as follows: (The results of Article 4C were known to the British; see Editor's Note at end of article).

INDEX TO VOLUME E-6

		Page
Article 4. (Contin.)	A. Analysis of Long Cribs.	14
	B. Estimation by Trials of Risk of Missing Jackpot.	24
	C. Click Probabilities by Recursion Formula.	46
	D. Expected Number of Random Stops.	57
	E. Choice of Threshold Function.	81
	F. Bobtail Menus.	90
	G. Analysis of Short Cribs.	100
Article 5.	Report on Duenna Covering First Six Weeks of Operation. Clifford, Hanson & Landers, 13 January 1945. . . . While this report is chiefly of operational interest, it also considers quite a few of the theoretical questions. Of theoretical interest, for example, is the no-threshold run; the computed distribution of no-come-outs is not too far off the actual in the region for which it can be computed (Table 4A).	105
Article 6.	Duenna Menuing. Landers, Cambridge & Gilman, 1 June 1945. . . . This article contains a description of some of the more important menuing techniques. Illustrative problems are included.	127
Article 7.	Summary of Duenna Operations to 1 June 1945. Landers, 1 June 1945.	147

INDEX TO VOLUME E - 7

Page

Article 1. Dummy Recovery by Catalog.
Ely, 11 March 1943. 1
With Bigram Tables only partially recovered, we may get a presumed dummy message with known position of Beta and fast wheel. This article tells how to recover the positions of the middle and slow wheels from the catalog by negative cribbing of the impossible letters, A, E, I, O, U, J, Y.

Article 2. Recovery of Text Where Fast (and Next) Wheels, their Position, Stecker and Ring are Known.
Ely, 18 March 1943. 3
When the Stecker and fast wheel position are known, a plain text assumption leads to a middle-wheel-alphabet link, which in turn may yield one or more new plain values. This procedure was known to the British as "decoding on the rods".

Article 3. 11-15-17 Cycle Length.
Ely, 29 April 1943. 14
A quick proof that the cycle length of the 11-15-17 machine (see Article 10 below) is 26^4.

Article 4. Stecker-Recovery from Single 5-Group B'B'.
Willis, Spring 1943. 15
Knowing the wheel order, rings, and the indicator (and hence the setting) of a B'B' message (short signal), a paired day could be gotten out if certain of the letters of the B'B' could be successfully cribbed.

Article 5 Construction of Menu to Give Stories at Given Positions.
Ely, 30 April 1943. 21
The purpose of this was to provide a test for the bombes, a topic which lies outside the scope of this Series, but the method of construction is of crypto interest.

Page

0 Article 6. American Modification of British "Hand-Breaking" Procedure.
Cramer, August 1943. 28
An account of Campaigne's idea of using masks, punched up from the crib, on a standard click board. The British method is given in Volume 8, Article 3. This mask idea was the precursor of MONA, and this in turn of DUENNA (Volume 6).

Article 7. Hand-Attack on Enigma Using Two Wheels.
Campaigne, 22 April 1944. 37
This article indicates that it would not be practicable to use 2-wheel development tables (and hence a single reflector, as in Duenna) in the hand attack.

0 Article 8. Notes on Jaguar Problems.
Church, 15 July 1944. 39
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.

0 Article 9. Non-Reciprocal Stecker.
Campaigne & Gleason. 24 July 1944. 42
The 40 Steckers produced from the daily one by the Enigma Uhr device (see preceding article) fall into 4 classes of 10 each; the cyclic structure of each of these classes is given. The bulk of the article is concerned with how to find the daily Stecker from the one recovered on the bombe.

0 Article 10. Report on Breaking of Cougar Depth of 14.
Cramer, 5 May 1945. 48
"Cougar" is the U.S. Coast Guard cover name for a certain German Secret Service circuit between Madrid and Prague. The author describes his break into a depth of 14 (really 12, as 2 were misplaced) by means of a "lobster", a place where all three wheels and reflector turn at once. The machine was suspected of being of the 11-15-17 type, which has three interchangeable wheels having

Page

Article 10. (Contin.) 11, 15 and 17 turnover notches, respectively, and metric (rather than true "enigma") motion. Other (unsuccessful) attacks are also described; the most interesting failure being that of counting for fast wheel position (see Volume 3, Article 7).

Article 11. Stepping Patterns of T-Wheels in Enigma-Motion. Dawson, 18 May 1945. 59
The T-machine has eight 5-notch wheels. This paper describes and tabulates all possible turnover patterns for an 8-letter stretch. It gives the general principles underlying any many-notched enigma motion.

RIP 610

TOP SECRET ~~CREAM~~

INDEX TO VOLUME E-8*

		Page
Article 1.	Mediterranean Enigma. 26 May 1943. . . . . An account of the procedure followed in Hut 8 in dealing with the Mediterranean enigma ("Porpoise"). This has the "throw-on" type of indicator, and one recovers the Grundstellung alphabets by "boxing". (Sunfish and Seahorse also have this type of indicator; see Volume 2, Articles 3 and 5.	1
Article 2.	Home Waters Enigma. 8 June 1943. . . . . An account of the procedure followed in Hut 8, in dealing with the Home Waters enigma ("Dolphin"). This is a member of the Kennbuch family. The procedure is to recover the Grundstellung alphabets by putting messages in depth. This is done partly by an I.B.M. search for repeated tetragraphs, and partly by a straight I.C. count (done on "Banbury sheets") on messages known by their indicators to start within 26 of each other. See also Article 8, Volume 2.	19
Article 3.	Handbreaking by Equidistances. 3 July 1943. . . . . This is an account of the British method of breaking into a new key by means of a certain combination of letters, known as an "equidistance", which sometimes occurs in a long crib ("reencodement"). The amazing thing about this method is that nothing need be known (Stecker, wheel order, Ringstellung, or window setting). The identity of the fast wheel must be assumed (or the eight possibilities tried one after the other). Its position may be assumed fixed by using the "generalized Stecker" trick. One then proceeds to make Stecker	36

* This volume consists of four reports sent to OP-20-G by Lt. Clifford while serving as liaison officer with the British Government Code & Cipher School.

INDEX TO VOLUME E - 8

		Page
Article 3. (Contin.)	assumptions on one of the letters involved in the equi-distance, from which to build up middle-wheel-alphabet links, and from these to get new Steckers. The mechanics of doing this is greatly facilitated by Campaigne's method of using a click board and masks (Volume 7, Article 6).	36
Article 4.	Counting a Re-encodement for Sigma vs. Delta and Turnover Probabilities. 8 August 1943. . . . . This is an account of the British method of counting a long crib (re-encodement) for the two purposes: (1) to tell which type of fast wheel (Sigma=single-notch or Delta = double-notch) is the more likely, and (2) to find a stretch for menuing which is least likely to be broken by turnover. For an experimental assessment of the efficacy of this procedure, see Volume 3, Article 10.	53

INDEX TO VOLUME
E-9

Page

0 Article 1. Hypo-Bombe.
Eachus, December 1943. 1
Original suggestion for hypo-bombe (statistical grenade). Each deciphered letter is weighted according to the logarithm of its plain-text frequency. The U.S. Army machine referred to is the "Dudbuster", which simply counts high frequency letters (effectively assigning wieght 0 or 1).

Article 2. Suggestion for Hypo-Bombe presented by Lt. Eachus.
Campaigne, 14 January 1944. 3
Comments favorably on Article 1. Gives the expected number of stops for certain levels of probability of getting the jackpot, without details of computation (see also Article 7 below).

Article 3. Statistical Bombe.
Howard, 4 September 1944. 4
Original proposal for a statistical bombe. This article can serve as an introduction to the subject. It is pointed out that the Double Unit ("Grandad") could be modified to give 64 banks, or that several bombes could be run synchronously (somewhat like the British "Giant"). The former idea was eventually adopted. Figures are given for sensing by number of blanks. This proved too weak (see Article 6 below). Sensing by Chi-square (equivalent to I.C.) is suggested, and this was eventually adopted.

0 Article 4. Gleason Weights for Monicity.
As told to Clifford by Gleason.
11 October 1944. 11
As applied to a frequency count, the word "monic" is short for "mono-alphabetic substitution on plain text". The standard I.C. test is a good measure of roughness (non-randomness), but these weights also take plain text distribution into account. This article gives their derivation. The British have long used these weights to score dotteries (Volume 3, Article 1).

ORIGINAL

INDEX TO VOLUME E - 9 (con.) Page

0 Article 5. Gleason Weights for Shark Text with Samples of 32, 48, 64.
Cramer, October 1944. 13
The computation of Gleason weights for the three sample sizes is described, and the results tabulated. In the application to the statistical bombe, a pure sample would arise as the decipherment of a single cipher letter in all its occurrences in the message. Hence this letter must be omitted in the language count from which the weights (for a 25-letter alphabet) are computed. It was found that this made only a trivial difference in the weights except when the cipher letter is E.

Article 6. Monicity Tests for a Statistical Bombe.
Cramer, 28 October 1944. 20
This article describes an experimental job to determine which of the following monicity tests were best for the proposed statistical bombe, and how effective each would be: (a) Number of blanks, (b) I.C. (c) Gleason weights. About two thousand 16-letter samples of random text, and a similar number of plain, were frequency-counted, and these merged to form 32, 48, and 64-letter samples. These were then scored, and the results tabulated. (a) proved too weak by itself. (c) was not appreciably better than (b), and the latter was adopted in the construction of Bulldozer, being mechanically simpler.

Article 7. Systems of Weights for a Hypo-Bombe.
Wray, 2 December 1944. 29
An experimental job to determine the effectiveness for the hypo-bombe of (a) log frequency weights, and (b) straight frequency weights. They are both effective, with not much preference between the two.

Article 8. Proposal for Statistical Grenade and Bombe.
Howard, 8 November 1944. 42
This is the final proposal. It gives a comprehensive treatment of statistical machinery, with emphasis on the cryptographic aspect, and the reader who is not mechanically minded can easily skip the few pages

INDEX TO VOLUME E-9 (cont.)

Page

Article 8. where specific mechanical suggestions are made.
(Contin.) The chapters are as follows:

General Theory of Statistical Machinery. 42
The Converted Double Unit as a Statistical Machine. 45
o Detection of Mono-Alphabetic Substitution. 47
An example is treated, using sums of squares of the frequencies. Two tables are given, based on the work described in Article 6.
Proposed Final Form of Statistical Bombe. 67
Hypo-Bombe Discussion (Statistical Grenade) 68
Table II is taken from Article 7.

Article 9. Appendix to Cougar Report.
Cramer, 7 May 1945. 73
Describes the unsuccessful attempt to solve the Cougar depth on Bulldozer.