Cryptologia, 38:152–177, 2014

ISSN: 0161-1194 print
DOI: 10.1080/01611194.2013.797050

Taylor & Francis
Taylor & Francis Group

The National Cash Register Company Additive Recovery Machine

CHRIS CHRISTENSEN

Abstract During World War II, The National Cash Register Company built an additive recovery machine for the U.S. Navy. The machine was designed to attack the Imperial Japanese Navy cipher JN-25, which was a superenciphered code. This article describes how that machine, called "Fruit" by the British, implemented three methods of additive recovery: the known-word method, the difference method, and Knepperizing.

Keywords additive recovery, differencing machine, JN-25, National Cash Register Company, Naval Computing Machine Laboratory, OP-20-G, subtractor machine

1. Alan Turing's Visit to National Cash Register

During the winter of 1942–1943, Alan Turing visited the United States as a liaison to American codebreakers [10]. Turing visited the Naval Computing Machine Laboratory (NCML) at the National Cash Register Company (NCR) in Dayton, Ohio to examine progress on the U.S. Navy cryptologic bombe. While at the NCML (December 1942), Turing saw a subtractor machine. In his report to Bletchley Park, Turing noted the following:

> **Subtractor machine** At Dayton we also saw a machine for aiding one in the recovery of subtractor groups when messages have been set in depth. It enables one to set up all the cipher groups in a column of material, and to add subtractor groups to them all simultaneously. By having the digits coloured white red or blue according to the remainders they leave on division by 3 it is possible to check quickly whether the resulting book groups have digits adding up to a multiple of 3 as they should with the cipher to which they apply it most.[1] A rather similar machine was made by Letchworth for us in early 1940, and although not so convenient as this model, has been used quite a lot I believe. [20, pp. 6–7]

Address correspondence to Chris Christensen, Department of Mathematics and Statistics, Northern Kentucky University, Highland Heights, KY 41099, USA. E-mail: christensen@nku.edu

Color versions of one or more of the figures in the article can be found online at www.tandfonline.com/ucry.

[1]"The cipher to which they apply it most" is clearly the Imperial Japanese Navy's General Operational Code, which was known to the Allies as JN-25. JN-25 was a superenciphered 5-digit code. The clear code groups were 5-digit numbers divisible by 3.

The subtractor machine was produced for the U.S. Navy by NCR. The Navy called the machine CXDG–CNN-10 ADW, but the British, who received copies of the machine, called it "Fruit." "Fruit" is an informal British term for a "slot machine."[2] (See Figures 1–3).

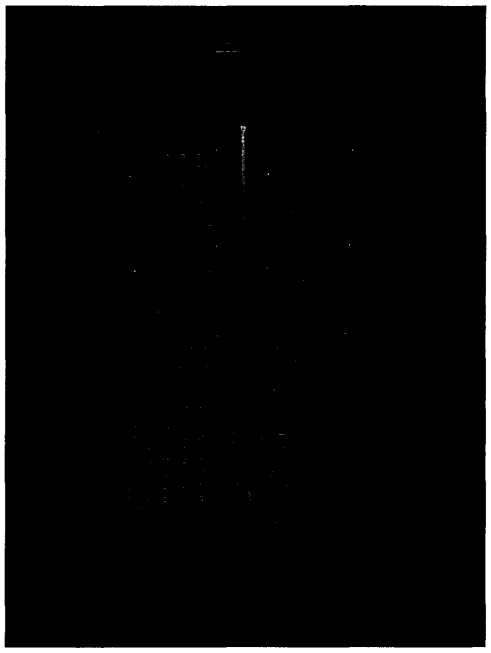


Figure 1. Fruit machine on display at the Wenger Command Display.[3] Photograph by CTRCM John Gustafson, USN (Ret).

The machine is large: 14.5 inches wide, 20.5 inches high, and 17.25 inches deep. It is also heavy; the label on the crate of one of the machines in the NSA warehouse shows a weight of 156 pounds (which probably includes the weight of the crate).

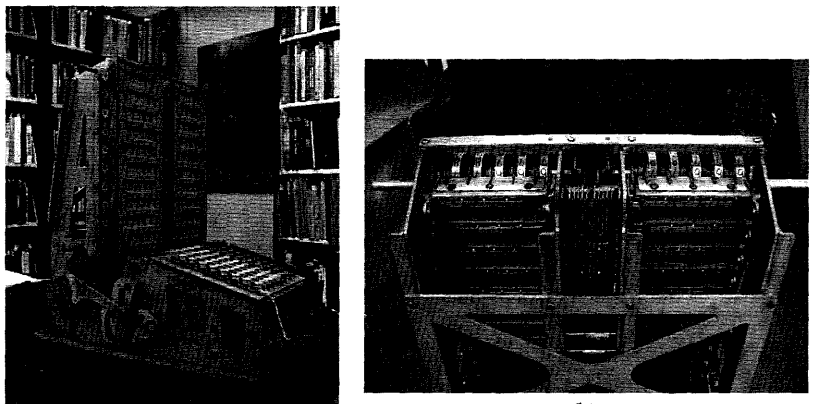
In *Information and Secrecy*, Colin Burke referred to Fruit as a "backward technological step":

> OP-20-G took another very effective but even greater backward technological step to deal with additive problems. It was probably recommended by [Navy] Yard engineers. A very complex special superencipherment "additive" desk calculator was manufactured for the Navy by NCR. The Fruit machines seemed to have been planned very early, perhaps in late

[2]The classic fruit machine had three windows. Behind each window was a wheel, and on the circumference of each wheel, images of fruit were displayed. The wheels rotated independently, and the payout was determined by the three images that appeared in the windows.

[3]This machine has serial number 012. It is described as " 'Fruit Machine,' a donation from the British during World War II" (http://www.navycthistory.com/Command_Display_room3_1.html; accessed 11 November 2012).

1941. They were quite innovative but they were based on 1920s electric machine technology and could only add and subtract.[4] [2, p. 253]



(a) (b)

Figure 2. An NCR additive recovery machine from the NSA inventory.[5] The cover has been removed, and some of the internal mechanical parts are visible. Photographs were taken by the author.

"The History of GYP-1"[6] describes an evolution of three machines for differencing.

> Three types of machines have been introduced which reduce the mechanical labor of differencing. ... The earliest of these machines, the Park[7] [sic] machine, was introduced in 1941; the second, the Shinn[8] machine,

[4]That the machines could only (falsely) add and subtract should not be a criticism. Although more technologically advanced machines were being planned for other purposes (e.g., to place ciphertext in depth or to align ciphertext and additives), JN-25 additive recovery only required (falsely) adding and subtracting.

[5]The NSA has two of these differencing machines in their warehouse. The description of one of them reads, "Special purpose calculator/differencing machine developed by the U.S. Navy and manufactured by NCR. Model CXDG-CNN-10 ADW, Serial No. 008. ID no: 001036. Account no: 70092. Designed simply to invert (undo) the non-carrying addition of numerical code groups to plain text, a practice used in Japanese Army systems. Non-carrying addition is a basic operation in modular arithmetic, and the inverse operation, which amounts to adding the additive inverse, is called differencing, so this device is otherwise called a differencing machine, or cryptanalytic differencing machine." The description of the other machine is identical with the exception that its serial number is 042.

[6]OP-20-GYP-1 designates a section of U.S. Naval Communications OP-20-G: cryptanalysis (Y), Pacific (P), and JN-25 (1).

[7]The name refers to Captain Lee W. Parke, USN. Parke became the first chief of the Division of Cryptography in the Department of State. (See, for example, [14, p. 501].) The machine is likely the machine called "Jeep IV." The name might come from "GYP-4." Jeep IV was famously mentioned in the 1941 letter from Parke to Lietwiler [18].

[8]The named refers to Dr. Lawrance E. Shinn, who served with the Navy in OP-20-G during World War II. Shinn held a doctorate in bacteriology from the University of Pittsburgh. He served with the AFSA and the NSA after World War II.

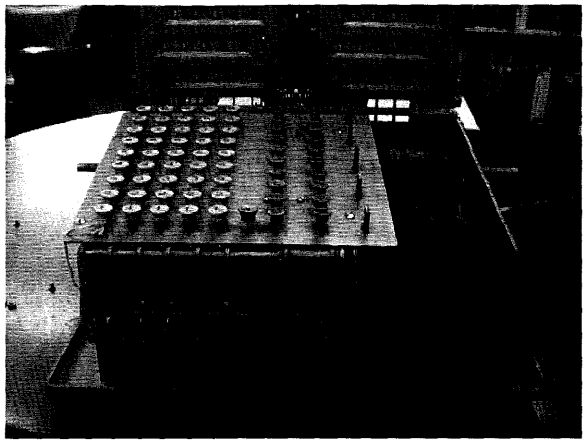


Figure 3. A small electric motor on the right side of the machine drives the gears. Photograph taken by the author.

> in 1942; and in 1943 an electrically-operated machine specially built for the section by the National Cash Register Company.[9]

2. JN-25

The Imperial Japanese Navy General Operational Code, which was known to the Allies as JN-25, was a five-digit superenciphered code. For each word or phrase of the message, the sending operator would select from a codebook the clear code group—the five-digit number that corresponded to the word or phrase that was being sent (e.g., M/S ["Begin Message Here"[10]] 80469).[11] Then, a string of additives—five-digit random numbers selected from a book of additives—was

[9]I thank Ralph Erskine for pointing out this paragraph. The quote comes from a single page of a document. The date and the document are otherwise unknown.

[10]The group "M/S" occurs in over 99% of the messages. A transmitted message in JN-25 is to be regarded as a cyclic system; that is, the sequence of text values (or their code groups) is such that reading from left to right the last group of the transmitted message is the immediate antecedent of the first group of the transmitted message. In messages as short as ten or 15 groups, this is unlikely to create any confusion "reading." The transmitted texts:

1. Arrived	2. SASEBO	3. 12	4. 00	Etc.
SASEBO	12	00	Jan	
12	00	Jan	25	
00	Jan	25	Arrived	
Jan	25	Arrived	SASEBO	
25	Arrived	SASEBO	12	

are all easily legible. The structure of the Japanese language (which carries verbs to the end, puts modifying clauses before the thing modified, etc.) and the compressed character of the text necessitate, however, that for longer messages some indicator be inserted to signify the true beginning of the message. This indicator is usually "Begin message here" or simply, "M/S." The exact Japanese phrase used is BUN KATSU KIGOO [5, pp. 241–242].

[11]M/S was commonly used and therefore had multiple clear code groups to reduce the high frequency that would occur if there were only one clear code group. For M/S, there were "twenty-odd clear code groups" [19, p. V-A-6].

added, group by group, to the clear code groups of the message. The addition was "false addition" which means to "add without carries" (i.e., to add vertically in columns modulo 10). For example, say that the additive 32470 would be added to 80469 by false addition to obtain the enciphered code group.[12]

Clear code group for "M/S"	80469
Additive	32470
Enciphered code group	12839

"Enciphered code group" is the terminology of [5]. In other documents, the more descriptive "group as transmitted" or "GAT" is used.

Knowing the string of additives, the receiving operator could then remove them by false subtraction ("no borrowing," i.e., subtract vertically modulo 10).

12839	Enciphered code group
32470	Additive
80469	Clear code group for "M/S"

The term "additive" as used above refers to "additive from the encipherer's point of view."

Instead of subtracting from the enciphered code group to recover the clear code group, 00000 minus the additive

00000
32470
78630

could be added to the enciphered code group.

12839
78630
80469 M/S

Because Navy cryptanalysts were working with enciphered code groups, and addition was less likely to result in error than subtraction, their use of "additive" refers to "additive from the decipherer's point of view": 00000 minus the additive from the additive book.

Because of the possibility of garbled groups ("A garbled group is one in which one or more incorrect digits appear, caused by error in enciphering, transmission, reception, transcription, or deciphering" [5, p. 215]), the Japanese built a garble-check into JN-25 clear code groups.[13] Instead of using all five-digit numbers as clear code groups, JN-25 included only five-digit numbers that are

[12]There are many descriptions of JN-25 encipherment. A good description is by Edward Simpson, "Enciphering by JN-25," which is Appendix V of [8], pp. 400 and 401.

[13]The valid code groups for the "Nan" cipher JN-25, which was introduced on 25 July 1944, and JN-25P, which followed it, did not scan. All other versions of JN-25 had the scanning property [13, p. 119].

divisible by 3 as clear code groups: the 33334 numbers 00000, 00003, 00006, . . . , 99996, 99999.[14]

Navy codebreakers referred to five-digit numbers that were divisible[15] by 3 as groups that "scanned." The property was called "scanning." Saying that a code group scanned only meant that it was divisible by 3 and therefore *potentially* the correct clear code group; it was still necessary to determine whether or not the meaning of the code group fit the context of the message.

When a large number of messages were intercepted (as was typically the case with JN-25), strings or portions of strings of additives would likely be reused, and it might be possible to align a collection of intercepted messages "in depth": in columns that have been enciphered with the same additive.

An indicator system was used to enable the sending operator to tell the receiving operator where the additive string began in the additive book; therefore, if the indicator system had been broken, intercepted messages could be placed in depth. Machines[16] were also designed to align messages in depth.

3. NCR Additive Recovery Machine

The NCR machine was used for additive recovery: determining the correct additive for a column of enciphered code groups that were aligned in depth. So, the use of Fruit assumed that messages could be placed in depth. The term "depth" refers to the number of messages in the column when the messages were aligned vertically in depth.

The machine's vertical display consists of 20 rows arranged in two parallel columns of length 10 (Figure 1). The ten rows in the column on the left are labeled A, B, D, E, H, J, K, L, M, and N; and the ten rows in the column on the right are labeled O, P, R, S, T, V, W, X, Y, and Z.[17] Each row has five windows. Behind each window was a wheel, and on the circumference of each wheel the digits 0, 1, 2, 3, 4, 5, 6, 7, 8, and 9 were displayed. One digit at a time can be displayed in each window. As Turing noted, the digits are colored red, white, or blue (for a reason that will be explained later). Just to the right of center on the keyboard (Figure 4) are two columns of round buttons that are labeled to correspond to the rows. The left half of the keyboard contains five columns of round buttons—nine buttons to a column—that are labeled (from top to bottom) with two numbers per button

[14]The requirement that all clear code groups should be divisible by 3 probably was of little value to the Japanese. The receiving operator could detect a garble by not being able to locate the deciphered group in the code book if the deciphered group was not divisible by 3 (which would occur two times out of three for a garble). The receiving operator would not detect a garble—except by context—if the garble resulted in a deciphered group which was divisible by 3 and therefore did appear in the codebook (which would occur one time out of three). However, the garble-check was of great value to Allied codebreakers. If, for example, a trial additive were stripped from a column of groups in depth and all the deciphered groups were divisible by 3, this would be strong evidence that the additive were correct. See also [6].

[15]Saying that a number is divisible by 3 is mathematically equivalent to saying that the sum of its digits is divisible by 3.

[16]Two such machine designs were the Navy's Copperhead I and (the never produced) Copperhead V.

[17]The unused letters are C, F, G, I, Q, and U. None of the documents upon which this article is based explain the choice of unused letters.

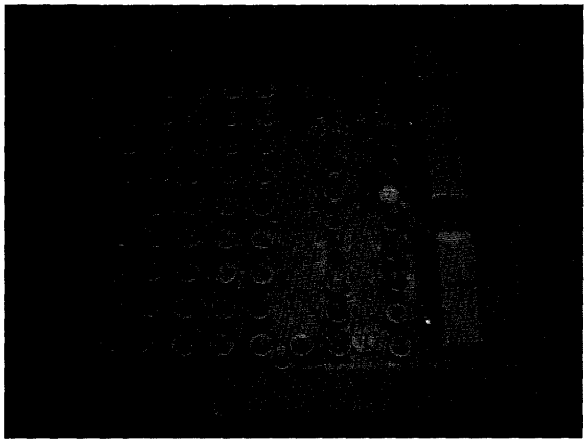


Figure 4. NCR additive recovery machine keyboard. Photograph by CTRCM John Gustafson, USN (Ret.).

(brown/red): 9/1, 8/2, 7/3, 6/4, 5/5, 4/6, 3/7, 2/8, and 1/9. On the right side of the keyboard are three larger rectangular "bars": from top to bottom, "Clear-bar," "Minus-bar," and "Plus-bar."

The description of the machine's operation and the examples that will be explained in the following are based upon "Cryptanalysis of JN-25" by OP-20-GY-1, Chapter VIII "Additive Recovery," pages 214–297.[18] This document is often referred to as the "GYP-1 Bible" and is dated July 1943.

Operation begins by clearing the machine of previous entries. This is done by striking the "Clear-bar" if no "1, 2, 3, ... Keys" and no "A, B, D, ... Keys" are depressed or by striking the "Minus-bar" and then the "Clear-bar" if some keys are depressed. All rows on the display should then register 00000. The "Plus-Bar" and the "Minus-Bar" do not function as their symbols might suggest. The "Plus-Bar" directs that keyboard action is to be applied to a single row, and the "Minus-Bar" directs that keyboard action is to be applied to all rows simultaneously. To enter a five-digit enciphered code group, say 47039, into a row, say H, the following procedure is followed.

Depress the "brown 4 key" in the column on the left.
In the next column, depress the "brown 7 key."
In the next column, do not depress any keys.
In the next column, depress the "brown 3 key."
In the column on the right, depress the "brown 9 key."
Depress the "H Key."
Strike the "Plus-Bar."

47039 should then appear in row H, and all keys should return to their normal position.

---

[18] I thank John Mack and Peter Donovan for sharing their digital version of this document with me.

Up to 20 "in depth" enciphered code groups can be entered. Assume that six enciphered code groups have been entered:

A	43713	O	00000
B	74751	P	00000
D	89854	R	00000
E	78330	S	00000
H	98366	T	00000
J	56055	V	00000
K	00000	W	00000
L	00000	X	00000
M	00000	Y	00000
N	00000	Z	00000

The machine can perform arithmetic operations simultaneously on all 20 rows of the display. There are two such operations.

One of the operations is to "zeroize" by a row: to falsely subtract one of the 20 rows from each of the others. Say, in the display above, that row B is to be "zeroized": Row B is to be falsely subtracted from all the rows. The operator depresses the "B Key" and then strikes the "Minus-Bar." The wheels in the display rotate so that 7 is falsely subtracted from all entries in the column on the left, 4 is falsely subtracted from all entries in the next column, etc. The display changes to the following:

A	79062	O	36359
B	00000	P	36359
D	15103	R	36359
E	04689	S	36359
H	24615	T	36359
J	82304	V	36359
K	36359	W	36359
L	36359	X	36359
M	36359	Y	36359
N	36359	Z	36359

Striking the "Minus-Bar" again restores the original code groups.

The other arithmetic operation that the machine performs is to falsely add a five-digit number to each row. Say, in the original display, that 15421 is to be added to each row. The operator depresses keys according to the red numbers[19]—"red 1," "red 5," "red 4," "red 2," and "red 1"—and then strikes the "Minus-Bar." The display becomes

A	58134	O	15421
B	89172	P	15421
D	94275	R	15421

[19]Presumably the wheels always rotate in the same direction. Subtracting 4 from 9, for example, would use the "brown 4 key" and rotate the wheel that displays the digit from position 9 to position 5. Adding 4 to 9 would use the "red 4 key" (the "brown 6 key") and rotate the wheel that displays the digit from position 9 to 3. On each key, the red digit and the brown digit are additive inverses. Depressing red keys 15421 and then the "Minus-bar" subtracts 95689 (the brown digits corresponding to 15421) from each row. Subtracting 95689 is equivalent to adding 15421.

E	83751	S	15421
H	03787	T	15421
J	61476	V	15421
K	15421	W	15421
L	15421	X	15421
M	15421	Y	15421
N	15421	Z	15421

4. Additive Recovery

"Cryptanalysis of JN-25" [5] describes three techniques for additive recovery. All the techniques are described using the following worksheet. The worksheet contains portions of six enciphered messages, which are shown in rows. Four consecutive enciphered code groups are shown for each message (e.g., 06009, 43713, 53115, and 28362 from Message 1). It is assumed that the six messages have been aligned "in depth" (i.e., the enciphered code groups in each column have been enciphered with the same additive). Each column has depth 6; the "depth of traffic" is 6.

	1	2	3	4
	22435		37354	69235
Message 1	06009	43713	53115	28362
	28434		08469	87597
	KANA NI		M/S	Begin A/T
Message 2	92851	74751	15300	45433
	14286		42654	04668
	ROMAN N		ROMAN R	ROMAN K
Message 3	45085	89854	17704	88702
	67410		44058	47937
	HATSU		xUnit Commander	XSHINSHOO
Message 4	70518	78330	70723	18934
	92943		07077	77169
	REPEAT A		NUM. SEP.	#30
Message 5	82206	98366	18114	83221
	04631		45468	42456
			BEI KOME	KANA NO
Message 6	28808	56055	24364	78863
	40233		51618	37198
	GAI SOTO			SHIN NOBU

The columns are numbered at the top of the worksheet. Additives have already been recovered for columns 1, 3, and 4; the recovered additives (22435, 37354, and 69235) are noted just below the column numbers—just above Message 1. For each of the six messages, what is shown on the worksheet in each column is

Enciphered code group
Clear code group
Plaintext word or phrase

Blanks appear where information has not yet been recovered. The additive has not been recovered for column 2, and Message 5 apparently has a garble in column 1 because 04631 is not a valid clear code group: It does not scan.
The second column of the worksheet would be entered on Fruit as

A	43713	O	00000
B	74751	P	00000
D	89854	R	00000
E	78330	S	00000
H	98366	T	00000
J	56055	V	00000
K	00000	W	00000
L	00000	X	00000
M	00000	Y	00000
N	00000	Z	00000

4.1. Known-Word Method

One of the three methods of additive recovery is the "known-word" method. From the context of Message 1, it is "strongly suspected" that the word in column 2 of Message 1 is SHINSHUTSU. The clear code group for this text is 58134; therefore, the trial additive for column 2 is 15421 (43713 falsely added to 15421 results in 58134).

When 15421 is added to all the entries on the display, the entries become

A	58134	O	15421
B	89172	P	15421
D	94275	R	15421
E	83751	S	15421
H	03787	T	15421
J	61476	V	15421
K	15421	W	15421
L	15421	X	15421
M	15421	Y	15421
N	15421	Z	15421

With the exception of H (Message 5), the first six entries correspond to valid clear code groups that "make sense" in the messages.

58134	SHINSHUTSU
89172	ROMAN E
94275	A/T foll. 2 groups[20]
83751	#142
03787	(garble)
61476	NANYOO

[20]"A/T" refers to "Auxiliary" table or "Alternate" table. For example, consider the two clear code groups 13347 and 24882. 13347 means "A/T follows 1 group," i.e., the meaning of the next clear code group should be located on the auxiliary table. In the auxiliary table, 24882 means "xOriginator." "24882 may have a meaning in the 'Normal' table, but is here, in virtue of the indicator, 13347, given its alternative text value." [5, p. 242].

Because Message 5 has a garble in column 1, it is reasonable to assume that Message 5 also has a garble in column 2 and that the additive for column 2 is 15421.

A machine operator can recognize garbles because of the color code to which Turing referred in his report. Note that in the known-word method example, column 2 of Message 5 displayed 03787; $0+3+7+8+7=25$, which is not divisible by 3 and therefore does not scan. It was not necessary for the operator to do the arithmetic; recognizing color patterns was sufficient. The digits 0, 3, 6, and 9 (the digits that are divisible by 3) were colored white; the digits 1, 4, and 7 (the digits that have a remainder of 1 when divided by 3) are colored red; and the digits 2, 5, and 8 (the digits that have a remainder of 2 when divided by 3) are colored blue. The scanning combinations of colors are as follows:[21]

- All white,
- One red and one blue and three white,
- Two red and two blue and one white,
- Three blue and two white,
- Three red and two white,
- One red and four blue,
- One blue and four red.

Row H 03787, for example, would display the colors

White-White-Red-Blue-Red,

two white and two red and one blue, which is not a scanning combination. Row B 89172 would display

Blue-White-Red-Red-Blue,

two red, two blue, and one white, which is a scanning combination.

4.2. Difference Method

A second method of additive recovery is called the "difference" method. The foundation of differencing is the mathematical fact that the difference between two enciphered code groups that have been enciphered with the same additive is equal to the difference between the corresponding clear code groups. For example, if message A and message B are both enciphered with the additive X, the enciphered code groups would be A – X and B – X.[22] Their difference $(A - X) - (B - X) = A - B$, the difference of the clear code groups.

The codebreakers constructed "difference tables" by computing the difference of each pair of "the highest frequency code groups, each of which is subtracted falsely from every other" [5, p. 221].

> For specialized uses, difference tables may be constructed on some basis other than overall frequency indicators, Romans, numbers, etc. have all been suggested and tried. [5, p. 221, footnote]

[21]These color combinations are the "winning combinations" on Fruit.

[22]Recall that "additive" as used in our discussion is "additive from the decipherer's point of view": subtract to encipher and add to decipher.

In his book *Elementary Course in Probability for the Cryptanalyst* [11], Andrew Gleason[23] indirectly sheds light on differencing in a counting example. Gleason uses four-digit code groups.[24]

> Minor differences are important in the analysis of enciphered codes. The minor differences of two numerical code groups is the lesser of the two digitwise mod 10 differences. Examples:
>
> | | | | | | |
> |---|---|---|---|---|---|
> | First code group | 7321 | 2207 | 7396 | 7859 | 6989 |
> | Second code group | 6184 | 3264 | 2891 | 2391 | 6975 |
> | First difference[25] | 1247 | 9043 | 5505 | 5558 | 0911 |
> | Second difference | 9863 | 1067 | 5505 | 5552 | 0199 |
>
> The minor differences are underlined. The advantage of minor differences is that they are independent of the order in which the two code groups are considered. [11, pp. 5–8]

Apparently, pairs of high frequency clear code groups were differenced, and their minor difference was recorded in a table along with the smaller of the two clear code groups. Recording only the minor difference cuts the size of the difference table (nearly) in half.

> If the difference between these groups is discoverable in the difference table, it may be assumed, for the moment, that the clear code group indexed in the table corresponds to the group which was the minor group in the subtraction effected on the work sheet. According to the system now in use, only the minor group – "B" [this notation corresponds to the example given above] is indexed in the difference table. The trial additive is then simply the false difference between the clear code group and the corresponding enciphered code group. [5, pp. 221–222]

Bletchley Park codebreaker Edward Simpson (in "Recovering by Differencing," which is Appendix VI of [8], pp. 402–405, and in [17, p. 78]) described a difference table that contained along with each minor difference the two clear code groups that produced it.

Returning to the worksheet, assuming that the known-word method has not been applied, differencing is applied to column 2.

A	43713	O	00000
B	74751	P	00000

---

[23]Gleason was a mathematician at OP-20-GM, the research section of OP-20-G, during World War II. (See [4].) This book "represents in its basic form an expansion of classroom notes that accompanied a series of lectures on probability given to U.S. cryptanalysts during World War II by [then] LCDR Andrew M. Gleason. In the late 1950s, however, the contents of this book were substantially rewritten and revised by Walter F. Penny and Ronald E. Wyllys [of the NSA]" [11, p. III].

[24]JN-11, for example, uses a four-digit code.

[25] The second code group is falsely subtracted from the first. The second difference results from falsely subtracting the first code group from the second.

D	89854	R	00000
E	78330	S	00000
H	98366	T	00000
J	56055	V	00000
K	00000	W	00000
L	00000	X	00000
M	00000	Y	00000
N	00000	Z	00000

[5, p. 227] notes that based upon context,

> High frequency groups are evidently to be expected in lines 2 [B] and 3 [D], an A/T indicator in the second case, and a Roman letter in the first; the difference between these two groups can be expected to correspond to a value in the difference table.

Therefore, to get the minor difference for the pair B and D, B would be subtracted from D—"zeroize by B"—and from all the entries, and the display on Fruit would read[26]

A	79062	O	36359
B	00000	P	36359
D	15103	R	36359
E	04689	S	36359
H	24615	T	36359
J	82304	V	36359
K	36359	W	36359
L	36359	X	36359
M	36359	Y	36359
N	36359	Z	36359

Under 15103 in the table appear two possible clear code groups: 89172 and 01488.[27] An experienced additive worker would immediately recognize 89172 as "Roman E" and apply it to the column [5, p. 227].

A	58134	O	15421
B	89172	P	15421
D	94275	R	15421
E	83751	S	15421

[26] Although when a single pair of enciphered code groups is differenced, it is possible—by subtracting the smaller from the larger—to guarantee that the minor difference will be obtained, when zeroizing a column some of the differences (e.g., J 82304 in this example) might be major rather than minor differences. In that case, if the difference table contains only minor differences, the codebreaker must falsely subtract the difference from 00000 (in this case, $00000 - 82304 = 28706$) to obtain the minor difference.

[27] [5, p. 227] also mentions the difference 95907, which would result from subtracting D from B, as appearing in the difference table with two possible clear code groups: 94275 (which would then be the correct entry for D) and 15681. This comment implies that the difference table that was used included both minor and major differences because 95907 is the major for the pair B and D.

H	03787	T	15421
J	61476	V	15421
K	15421	W	15421
L	15421	X	15421
M	15421	Y	15421
N	15421	Z	15421

which is the same solution that was obtained by the known-word method. (Notice that the additive 15421 appears in each of the rows that were originally 00000.)

The choice of 89172 was made based upon context. If the additive worker had not used context and chosen 01488, adding this to all the entries would result in a display on Fruit of

A	70440	O	37737
B	01488	P	37737
D	16581	R	37737
E	05067	S	37737
H	25093	T	37737
J	83782	V	37737
K	37737	W	37737
L	37737	X	37737
M	37737	Y	37737
N	37737	Z	37737

Then, column 2 would result in

70440	The group scans but has no known meaning.
01488	SHINKYUU
16581	#7
05067	The group scans but has no known meaning.
25093	The group does not scan.
83782	The group does not scan.

This is an unlikely correct result.

The choice above to "zeroize by B" was made by context, but differencing does not depend on context. Ignoring context, the first try might have been to zeroize by A:

A	00000	O	67397
B	31048	P	67397
D	46141	R	67397
E	35627	S	67397
H	55653	T	67397
J	13342	V	67397
K	67397	W	67397
L	67397	X	67397
M	67397	Y	67397
N	67397	Z	67397

From the difference table, corresponding trial clear code groups would have been obtained.

Difference	Corresponding clear code group
31048	26349
46141	
35627	57147
55653	79194
13342	39336 and 64827

Adding 26349, for example, to all entries in the display would result in A 26349 (which scans, but must because it is a clear code group from the difference table), B 57387 (which does not scan), D 62480 (which does not scan), E 51866 (which does not scan), H 71992 (which does not scan), J 39681 (which scans), and an additive of 83636. This is an unlikely correct result.

Differencing by all entries beginning from the top would yield the following differences:[28]

Zeroize by	A	B	D	E	H
A	00000				
B	31048	00000			
D	46141	15103	00000		
E	35627	04689	99586	00000	
H	55653	24615	19512	20036	00000
J	13342	82304	77201	88725	68799

Recall that 15103 is correct.

Notice that a combination of vertical alignment (depth) and horizontal alignment (context) has been used to determine the correct additive. Speculative additives were often determined by depth alone using "the proportion of well-recognized groups which a certain additive produces. Necessarily, the number of groups in a column (depth of traffic) is a limiting factor in [the use of this method]. If the traffic is very shallow, the proportion of high-frequency groups may be high throughout without the additives being correct. Also, accidental garbles [groups that do not scan] may exist in the column produced by the application of the correct additive, whereas an incorrect additive may bring out a column entirely free of garbles [groups that do not scan]. Generally speaking, a depth of about eight lines[29] may be considered a reasonable minimum for judging correctness by internal characteristics alone though occasionally four very high frequencies in four lines of traffic will occur—in which case, the additive is quite probably correct." [5, pp. 218–219]

One case pointed out in [5, pp. 229–230] that provides strong evidence for a correct additive occurs when a column contains three or more enciphered code

[28] It is only necessary, for example, to difference C – B and search for the minor difference rather than difference both C – B and B – C. Therefore, the table of differences can stair-step down toward the right. Such a table seems to have been called a "flag."

[29] "Generally speaking, the term 'deep' traffic is applied to any region where the columns average eight code groups per column or better. Traffic is called 'shallow' where the columns average four code groups or less" [5, p. 217].

groups that correspond to high frequency clear code groups. Assume that A, B, C, and D are high frequency clear code groups that have been used in constructing the difference table. Assume that each has been enciphered with the additive X and that they appear in depth on the work sheet.

A – X
B – X
C – X
D – X

After zeroizing by A, the column would be

A – A
B – A
C – A
D – A

If these are the minor differences, then each difference would be associated in the difference table with the clear code group A. "The group A, appears three times. In practice, then, if a set of differences generated by one zeroizing of the column produces duplication, triplication, etc., of a clear code group when reference is made to the difference table, considerable weight is given to the assumption that the repeated clear code group does, in fact, underlie the zeroized enciphered code group." [5, p. 230]

4.3. Knepperizing

A third method of additive recovery was called "Knepperizing"[30] which is described as a combination of the known-word method and the difference method.

> Where a given text value for which multiple clear code groups exist is expected in a given position, or where one among several possible clear code groups with analogous meanings is expected, this technique is extremely valuable.
>
> Subtract the enciphered code group (in the given position) from three or four other groups in the same column, choosing the groups whose messages have been "running well"—i.e., have shown little tendency to garble. Add these differences successively to the possible clear code groups and where scanning groups result for these additions, proceed as in the "known-word" method. [5, p. 223]

---

[30]The name refers to E. W. Knepper, who was an officer in the USN and served with OP-20-GY during World War II. Donald McDonald, who served in OP-20-GY-1, -2 during World War II and later with the Armed Forces Security Agency and the National Security Agency, recalls: "I did know Ed Knepper slightly while in GY. He was clearly regarded by the old-timers around as an expert cryptanalyst on the JN-25 system. At the time I think he was a Navy Cdr.... I saw him in Japan around 1955" [16]. [12] includes a reference to a 7 March 1958 memorandum for "Captain E. W. Knepper, USN, Chief of Staff, Production, NSA."

Returning to the worksheet assuming that neither the known-word method nor the difference method has been applied, Knepperizing is applied to column 2.

A	43713	O	00000
B	74751	P	00000
D	89854	R	00000
E	78330	S	00000
H	98366	T	00000
J	56055	V	00000
K	00000	W	00000
L	00000	X	00000
M	00000	Y	00000
N	00000	Z	00000

In Message 3 (which corresponds to row D), one of the "A/T" indicators should be applied just prior to 44058. "This indicator is definitely not 'A/T foll. 1 group,'[31] but it may be 'A/T foll. 2 groups,' 'A/T foll. 3 groups,' or 'A/T begin using.'" [5, p. 234]

The corresponding clear code groups are [5, p. 235]

A/T foll. 2 groups	30804
A/T foll. 2 groups	39351
A/T foll. 2 groups	75684
A/T foll. 2 groups	94275
A/T foll. 3 groups	04965
A/T foll. 3 groups	22884
Etc.	

First, zeroize by D:

A	64969	O	21256
B	95907	P	21256
D	00000	R	21256
E	99586	S	21256
H	19512	T	21256
J	77201	V	21256
K	21256	W	21256
L	21256	X	21256
M	21256	Y	21256
N	21256	Z	21256

[31] From the context, it was determined that the next two or more clear code groups were taken from the auxiliary or alternate table. The indicator tells how many of the following groups are taken from that table. "A/T foll. 2 groups," for example, apparently indicates that the following two groups were taken from the auxiliary table.

Then, to try one version of "A/T foll. 2 groups," 30804 is added to each entry:

A	94763	O	51050
B	25701	P	51050
D	30804	R	51050
E	29380	S	51050
H	49316	T	51050
J	07005	V	51050
K	51050	W	51050
L	51050	X	51050
M	51050	Y	51050
N	51050	Z	51050

Focusing on Message 1 (row A), Message 2 (row B), and Message 4 (row E)[32]: 94763 does not scan, 25701 scans, and 29380 does not scan. Two of three groups do not scan. This is an unlikely correct result.

Similarly, trying the other possible clear code groups results in [5, p. 235]

30804	2 of 3 groups do not scan.
39351	1 of 3 groups does not scan.
75684	2 of 3 groups do not scan.
94275	All 3 groups scan.
04965	2 of 3 groups do not scan.
22884	2 of 3 groups do not scan.
Etc.	

94275 "A/T foll. 2 groups" appears to be correct, which is the same solution that was obtained by the known-word method and by the difference method.

[5, pp. 235–237] discusses in detail an example of Knepperizing using Fruit to place "Begin Parenthesis" in the appropriate position of consecutive recovered columns.

5. Machine vs. Manual Differencing

From the "GYP-1 Bible":

> Differencing is usually effected by manual means, but can also be carried out by machine. From time to time, various types of machines,[33] some power-operated and some hand-operated, have been used in the additive recovery rooms. . . . The machines in use at present[34] are electrically driven (manufactured by the National Cash Register Company) and embody virtually all of the essential principles of previous machines devised. [5, p. 230]

[32]Message 3 (row D) will, of course, scan because it is a clear code group.

[33]This suggests that there might have been more than the three types of machines mentioned in "The History of GYP-1."

[34]This document is dated July 1943.

Robert Cahill, who was a cryptanalyst with the Navy during World War II and later with the NSA, comments on the use of what appears to be Fruit.

> After a while, when I was still in Washington but at Nebraska Avenue [the Naval Communications Annex and home to OP-20-G], we got adding machines that looked like cash registers to help us do our work. These machines were good if there was no depth because they helped us try different possibilities. I found these machines too slow if there was depth because I could add faster by hand. (From Oral History 11-80, Robert D. Cahill; interviewer: Robert Farley. Quoted in [15, p. 65]).

Howard Campaigne[35] (see [3]), referring to attacks on Japanese ciphers, commented

> We went to the National Cash Register Company, and they even built a special device for this, which wasn't terribly popular with [cryptanalysts]. I don't know why. Some of these became very adept at doing a lot of these in their heads. They could do—I remember when I first worked on this, the best I could do in one day would be twelve groups. But there was a Warrant Officer there who would always get a hundred every day and sometimes 120 or 130. Way ahead of anybody else. And he didn't want one. He didn't like these calculating machines. The adding machine had to be special because the addition is done without carry, that's to avoid multiplying the errors again. Well, there were a number of those things built by the National Cash Register Company, but they weren't too successful.

The "GYP-1 Bible" notes that "over a period of time, the scores of individual men working with the machines is not noticeably higher or lower than the man-average over the same period," and "the machines seem ... to be satisfactory as accessories in additive production though they have not startlingly increased production over the period of their operation." [5, p. 263]

The mechanical reliability of the machine also seems to have been a problem. Simpson[36] in "Solving JN-25 at Bletchley Park" noted that

> At one stage when we were struggling to keep up with the increasing quantity of incoming traffic Washington sent us a dozen or so calculating machines made by the National Cash Register Company. We called them the 'fruit machines.' They were big, perhaps four feet tall, and floor-standing; mechanical, not electrical. They were set up to do non-carrying addition and subtraction of five-digit numbers. For example, all the enciphered groups of a column of depth could be entered and then a speculative additive placed at their head: one pull of the handle stripped the additive from all the subgroups simultaneously to reveal all the

[35]Howard Campaigne was a mathematician who was recruited to serve with Naval Communications during World War II. After the war, he continued to serve in successor agencies and later became director of research for the NSA. (See [4].)

[36]Notice that Simpson's recollection of Fruit does not match the machines that are in the NSA warehouse of the Wenger Command Display.

> speculative codegroups, which could be tested immediately for scanning. The enciphered groups stayed on the machine until all the speculative additives for that column had been tried. At first and at their best the machines were a great help, faster than manual stripping and easier on the eyes. The trouble was that they proved prone to mechanical breakdown and, as there seemed to be few technicians around capable of mending them, they were out of action for long periods. Confidence in them waned and eventually we gave them up altogether. [8, p. 136]

6. Differencing

David Kahn noted that "Axis, Allied, and neutral cryptanalysts employed the identical technique ["the difference method"], which each major power apparently developed independently, probably between the wars." [14, p. 440]

The 16 November 1941 letter from Lietwiler to Parke [18] sheds light on the beginning of the Navy's use of differencing.

> A new system of attack that we have put in use [in the Philippines]. Using the 400 high frequency groups we have compiled a table of 24,000[37] differences. When we are stuck on a column now we take any likely looking group and subtract it from every other group in the column. The reciprocals of these differences are also written down which gives the difference of every group in the column from the master group. By reference to the table, the groups which produce these differences are found and tried in the proper spots.

A handwritten manuscript comment on page 1 of the letter said, "Same as our new technique." Ralph Erskine commented, "The manuscript comment has clearly been added by 20-G (probably by Parke himself—note 'what I meant' in the penultimate comment on p. 1)." [7]

7. Differencing Machines

As noted at the beginning of this article, [13] describes an evolution of three machines for differencing: the Parke machine (1941), the Shinn machine (1942), and an electrically-operated machine built by NCR [13, p. 10]. The "GYP-1 Bible" suggests that there might have been more than three. (See note 32.) The NSA inventory includes at least three machines other than the NCR machine that were used for differencing or to determine whether groups scanned.

One of the machines in the NSA inventory is identified as "CRYPTANALYSIS Depth Reader Device. Five multiple-disk sets of numerical bands made of wood. Reads 'To 20Q–Park's Jeep Model, 3-16-42.' Handmade. Presumably to assist in counting depth of traffic keys, actual use unknown." (See Figure 5).

Also included in the NSA inventory is a hand-operated differencing machine used by the U.S. Army. This machine permits a depth of 10 with five-digit code groups (Figure 6).

---

[37]The number of pairs would be 79800. Different pairs could, of course, produce the same difference.

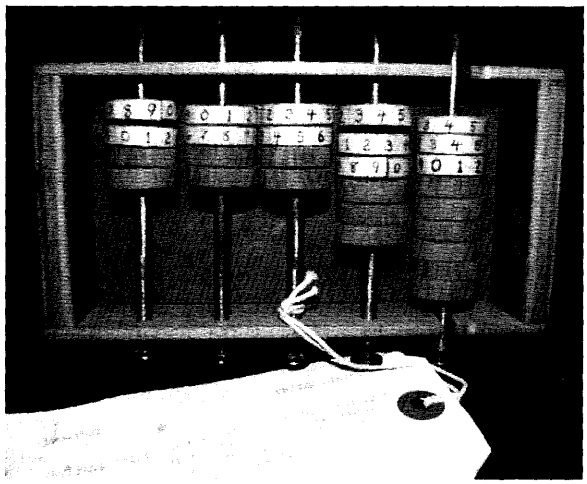
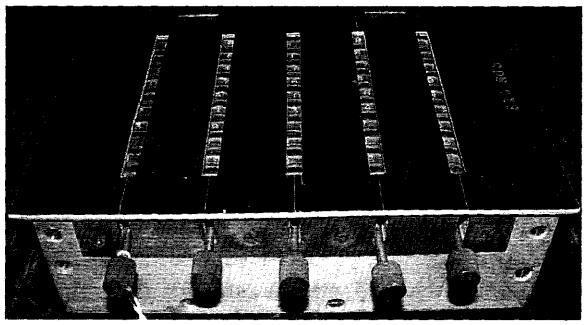
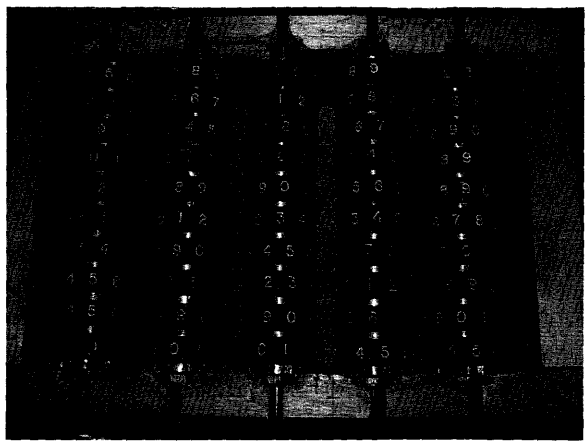


Figure 5. Handmade depth reader device. Photograph courtesy of the NSA.



(a)



(b)

Figure 6. Differencing machine constructed by the U.S. Army in 1943 for locating overlaps in Japanese code enciphered by additives. Photographs courtesy of the NSA.

Volume 2 "Notes on German High Level Cryptography and Cryptanalysis" of the 1946 Target Intelligence Committee[38] "TICOM" report illustrates a German differencing machine that is similar to the U.S. Army device and is described as fulfilling the same purpose as Fruit [9, pp. 57–60] (Figure 7).

> Differencing calculator (non-recording) and additive tester.—This machine (German name not known) was a manually-operated device to assist additive recovery in superenciphered code problems, by speeding the differencing of depths of super-enciphered code groups and the trial of likely additives thereon. It cost approximately $40.00. It was identical in its function to the U.S. Navy "CXDG-CNN-10ADW." [O]ften called the N.C.R. differencing calculator. The German version had a capacity of thirty 5-figure groups, as against the N.C.R. capacity of twenty. The German device was much slower to operate, though far simpler in construction. [9, pp. 57–58]

In a footnote, the report noted that "Army Security Agency constructed a differencing calculator in 1943 identical in principle to the German device. It was a rough model and was not perfected because the N.C.R. devices were made available. It is now in the Army Security Agency Museum." [9, p. 58]

The TICOM report gave one example of the use of the German differencing calculator.

> Differencing a column of 5-figure enciphered codegroups was a simple process with this machine. The five rods were locked into position with the top (fixed) row of rollers reading "00000." Then the first enciphered code group in the depth was set up on the next row of rollers (marked row "1" in the sketch) then the second enciphered code group was set up on row "2," the third enciphered code group on row "3," etc., until all the enciphered code groups were set up. Then the five rods were unlocked.
>
> To subtract the first enciphered code group (appearing in row "1") from all the others, all one had to do was to rotate the five rods until the rollers in row "1" read "00000." The numbers appearing in all the lower rows now represented "differences." These differences could now be looked up in "difference tables," and the most probable unenciphered pairs of code groups they represented be noted down for trial—an analytic process familiar to all cryptanalysts. To "try" one of these likely unenciphered groups with the aid of the machine, all one had to do was to rotate the five rods until it appeared in the window instead of the enciphered code group supposed to be representing it; immediately all other rows represented the consequences of the assumption, and the very top row (above the row marked "1") represented the enciphering additive. [9, pp. 58, 60]

[38]The Target Intelligence Committee was formed near the end of World War II in Europe. As part of the project, U.S. and British codebreakers followed military forces into Germany to examine captured cryptologic equipment and to interview German codebreakers. The reference is to one of nine volumes of "European Axis Signals Intelligence in World War II as Revealed by 'TICOM' Investigations and other Prisoner of War Interrogations and Captured Material, Principally German," which is a report on the TICOM prepared for the Army Security Agency in 1946 and which is available online.

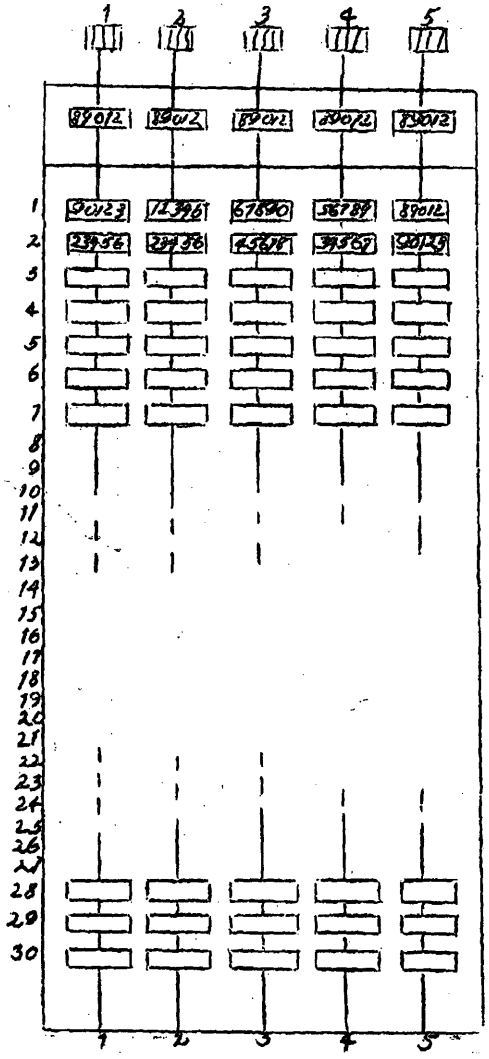


Figure 7. German differencing device.[39]

A third machine in the NSA inventory resembles the machines shown above but was used to determine whether groups scanned (Figure 8). The machine is identified as "M-4 for testing divisibility of 5 digit numbers by 3. Second developmental model, designed/built by NCSL [Navy Code and Signal Laboratory; i.e., the Navy Yard] in 1941/1942. First was built in Washington in 1940, succeeded

[39]The sketch was made by Dr. Erich Hüttenhain (1905–1990). The sketch shows the German machine with its cover removed. Presumably, it would be similar in appearance to the U.S. Army device. Hüttenhain studied mathematics and astronomy in Münster. In 1936, he entered the Cipher Board (*Chi*) of the *Oberkommando der Wehrmacht* (OKW) and became head of group IV (analytic cryptanalysis). After the war, from 1956 until 1973, he directed the "German Cipher Board" [1, p. 423].

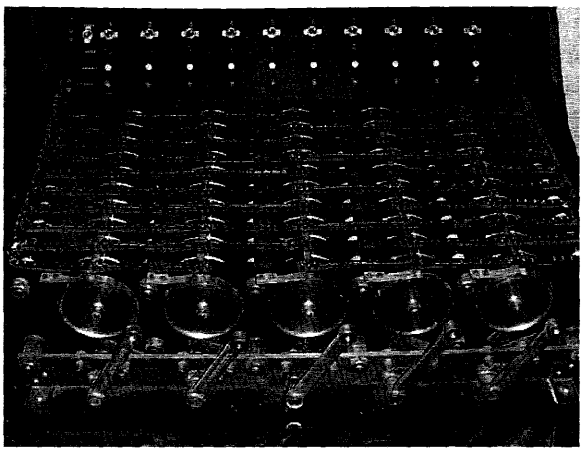


Figure 8. M-4. Photograph courtesy of the NSA.

by the NCR machine; previous inventory numbers IN-24, item 16. Device later referred to as a calculator."

The M-4 has 10 rows for five-digit code groups. On the base are ten switches labeled to correspond to the rows. With each switch is a set of three lights (from top to bottom in the photograph): red ("under"), white ("divisible"), and green ("over").

8. The Next Steps

The differencing machine called Fruit by the British was in use in 1943. It was an electromechanical machine that evolved from "by hand" techniques and hand-operated machines. Fruit assisted with additive recovery, but it seems that adept codebreakers could work nearly as quickly, and the machines tended to break down. In the second half of 1943, as the cryptanalytic Battle of the Atlantic was beginning to be won by British and American codebreakers, U.S. Navy mathematicians/codebreakers turned more of their attention toward attacking Japanese ciphers. They designed several codebreaking machines—more advanced than Fruit—to align ciphertext JN-25 messages in depth and to align recovered additives against intercepted messages. These machines were engineered by Joseph Desch and other engineers at NCR in Dayton, Ohio, in the NCML where Alan Turing saw Fruit.

Appendix

Comment 1

The following comments and quote are based upon: "Report by Dr. A.M. Turing, Ph. D." dated 28 November 1942 at Washington, DC, which is in the British National Archives HW 57/10 CS41948.

On the first page of this article, there is a quote from Alan Turing commenting on the subtractor machine that he saw during his December 1942 visit to the Naval Computing Machine Laboratory in Dayton, Ohio. That quote suggests that Turing was aware of an attack on a superenciphered code having valid code groups divisible

by 3. However, a report by Turing "Report on Cryptographic Machinery Available at Navy Department Washington" (which reports on his visit to the Washington codebreakers and occurred at the beginning of the trip that included the visit to Dayton) casts doubt on Turing's knowing about JN-25 and its having valid code groups that were divisible by 3. Turing began his Washington visit on 17 November 1942. Referring to the Navy's use of IBM machinery, Turing says:

> The I.B.M. machinery which I saw was mostly the same as that at G.C. & C.S. Two machines were shown to me as being new. One of them did not really seem of any particular importance: it was intended for use with book codes where there is a 'value' of a particular kind; viz. the digits have to add up to a multiple of 3. They say they get quite a lot of it, but I never heard of it before. [p. 17]

This quote suggests that Turing was not at that time aware of JN-25. The quote in the report from Dayton suggests that at the time of the visit to the NCML he was aware of a code having valid code groups that scanned. It would be interesting to know more about the subtractor machine built at Letchworth – in particular whether it checked for scanning.

Comment 2

Four documents (or partial documents) that are in the Colin Burke Collection at the National Cryptologic Museum shed additional light on the NCR additive recovery machine. Some writing on the documents is hard to read, and some documents are poor copies. The documents refer to the NCR additive recovery machine as M-40. One page that appears to be a Bletchley Park document has a section titled "The 'Fruit Machine'" that briefly describes the NCR additive recovery machine and its use. There is a parenthetical statement that says "lease-lent to us." A 11 January 1944 message from Commander Howard Engstrom (who headed OP-20-GM, the research section of OP-20-G) to Captain Ralph Meader (who commanded the Navy personnel at the NCML) states that "The figure of six M-40 adding machines for the British has been raised to eighteen." A 15 March message from Meader to Engstrom states that "Nine of [M-40s] on order for the British are for tropical use." A 20 March 1944 message that appears to be from Meader to Engstrom states that "have taken tropical conditions into consideration on [M-40s] they will be satisfactory." It is noted in the message that "[NCR] has not yet received a contract to make these."

About the Author

Chris Christensen teaches mathematics and cryptology at Northern Kentucky University. Recently, he has been exploring the codebreaking machines designed by OP-20-GM mathematicians to attack Japanese ciphers.

Acknowledgments

Thanks to Ralph Erskine for being so willing to share his documents and knowledge on this and other cryptologic topics; to Edward Simpson for communications about

Fruit and about attacking JN-25 at Bletchley Park; René Stein for searching for documents and images and for arranging for me to examine one of the Fruit machines in the NSA inventory; to Scott Massey for bringing a Fruit machine from the NSA warehouse to the National Cryptologic Museum and for literally "doing the heavy lifting"; to Debbie Anderson whose exploration of the work of her father Joe Desch and the work at the NCML led to this exploration of the Fruit machine; to CTRCM John Gustafson, USN (Ret). for providing information about and photographs of the Fruit machine at the Wenger Command Display; to NKU student Jared Antrobus who is exploring Mamba and who insisted that all of the explanations in this article should be understandable; and to the Kentucky Section of the Mathematical Association of America and the Mathematics Department of the United State Naval Academy for opportunities to present this material.

References

1. Bauer, F. L. 2000. *Decrypted Secrets: Methods and Maxims of Cryptology*. Berlin: Springer.
2. Burke, C. 1994. *Information and Secrecy: Vannevar Bush, Ultra, and the Other Memex*. Lanham, MD: The Scarecrow Press, Inc.
3. Campaigne, H. 1970. Smithsonian Computer Oral History of Howard Campaigne, interviewed by Richard R. Mertz. http://invention.smithsonian.org/downloads/fa_cohc_tr_camp700709.pdf (accessed 11 November 2012).
4. Christensen, C. 2011. "US Navy Cryptologic Mathematicians during World War II," *Cryptologia*, 35(3): 267–276.
5. "Cryptanalysis of JN-25 (GYP-1 'Bible')," National Archives at College Park, MD (NARAII), RG 38, Records of the Naval Security Group Central Depository, Crane, IN, CNSG Library, Box 16, 3222/65.
6. Donovan, P. 2004. "The Flaw in the JN25 Series of Ciphers," *Cryptologia*, 18(4): 325–340.
7. Correspondence between the author and Ralph Erskine, 1 October 2012.
8. Erskine, R. and M. Smith. 2011. *The Bletchley Park Codebreakers*. London: Biteback.
9. "European Axis Signals Intelligence in World War II, Volume 2." 1946. http://www.nsa.gov/public_info/declass/european_axis_sigint.shtml (accessed 11 November 2012).
10. Gladwin, L. A. 2001. "Alan Turing's Visit to Dayton," *Cryptologia*, 25(1): 11–17.
11. Gleason, A. M. 1985. *Elementary Course in Probability for the Cryptanalyst* (revised edition), revised by W. F. Penny and R. E. Wyllys. Walnut Creek, CA: Aegean Park Press.
12. Hatch, D. A. 2004. "DDE & NSA: An Introductory Survey," *Cryptologic Quarterly*, 23:1–2.
13. "The History of GYP-1," NARAII, RG 38, CNSG Library, Box 116.
14. Kahn, D. 1996. *The Codebreakers: The Story of Secret Writing*. New York: Scribner.
15. Maneki, S. A. 2011. *The Quiet Heroes of the Southwest Pacific Theater: An Oral History of the Men and Women of CBB and FRUMEL*. Fort George G. Meade, MD: Center for Cryptologic History.
16. Correspondence between the author and Donald McDonald, 12 September 2012.
17. Simpson, E. 2010. "Edward Simpson: Bayes at Bletchley Park," *Significance*, 7(2): 76–80.
18. Stinnett, R. B. 2002. Pearl Harbor Document: Letter from Leitweiler [sic] to Parke. http://www.independent.org/issues/article.asp?id=1432 (accessed 16 October 2012).
19. "Techniques and Procedures used in the Cryptoanalysis of JN-25 by Station Negat Reg. No. 1," NARAII, RG 38, RIPs, Box 138, RIP 171.
20. Turing, A. 2001. "Visit to National Cash Register Corporation of Dayton, Ohio," *Cryptologia*, 25(1): 1–10.