Machine Attack on JN-25

Chris Christensen
Northern Kentucky University
Naval Communications
Laurance Safford (1890 – 1973)

- 1924 Cryptographic Research Desk.
- July 1924 cryptanalysis problems in communications division bulletin.
INDEX

OP-20-GR RULES FOR STUDENTS (52821)

OP-20-GR MECHANICAL AIDS IN CIPHER SOLUTION (52822)

OP-20-GR ELEMENTARY COURSE IN CRYPTOANALYSIS (52823)

Assignment 1 Introduction ( )

" 2 Mechanics of the English Language (52899)

" 3 Numerical Cipher Alphabets (52899)

" 4 Polyalphabetic Substitution (52823)

" 5 Equivalent Cipher Alphabets (56457)

" 6 Sliding Strips, Cipher Discs, and Square Tables (56458)

" 7 Simple Route Transposition ( )

" 8 Anagramming (51516)

" 9 Grille Transposition Ciphers (52824)

" 10 Polygraphic Substitution ( )

" 11 Diagonal Digraphic Substitution (A36462)

" 12 Open Code ( )

Solutions for Assignments #1 to #12

Training Pamphlet #1 Reconstruction of Simple Cipher Systems (44213)

" #2 General Principles of Communication Security (A36451)

" #40 A Numerical Method for the Solution of Double Transposition Ciphers (A36463)

OP-160-4 TABLES OF STANDARD FREQUENCY DATA-ENGLISH
Assignment Three
Numerical Cipher Alphabets

Example:

Standard numerical cipher alphabet

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20

Since there are but ten digits, it is obvious that, in order to represent a complete alphabet, combinations of at least two digits are necessary.

(b) Mixed numerical cipher alphabets are those in which the cipher component is not a normal sequence of numbers, used in conjunction with a normal sequence of letters in the plain component.

Examples:

(1) Random mixed numerical cipher alphabet

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
76 88 1 67 4 80 66 99 96 2 69 90 77 5 87 60 89 79 3 78 68 93 86 70 97

This example will also illustrate a type of numerical cipher alphabet in which some of the digits may be employed singly and some in pairs to represent single plain-text letters, thus retarding the attempts of cryptanalysts to isolate the individual cipher equivalents of plain-text letters after they have been run together in the cryptogram.

(2) Systematically mixed numerical cipher alphabet

The pair of numbers which appear as row and column indicators are used as the cipher equivalent of the plain letter found at the intersection of the row and column.

That is, A plain is 11 cipher, B plain is 12 cipher, etc.

Rectangles of various shapes and sizes may be used, having various key number arrangements, and including cells for proper names and places or blank cells. Also, the plain alphabet may be any type of mixed alphabet, and may be inscribed by following any prearranged route to fill the proper cells of the rectangle.
Assignment Three: Problem 2

<table>
<thead>
<tr>
<th>Problem No. 2</th>
<th>53241</th>
<th>54532</th>
<th>24432</th>
<th>51243</th>
<th>24231</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>54445</td>
<td>45325</td>
<td>14344</td>
<td>14152</td>
<td>14115</td>
</tr>
<tr>
<td></td>
<td>43453</td>
<td>52123</td>
<td>35125</td>
<td>11421</td>
<td>53334</td>
</tr>
<tr>
<td></td>
<td>53244</td>
<td>23154</td>
<td>54524</td>
<td>43241</td>
<td>44432</td>
</tr>
<tr>
<td></td>
<td>12532</td>
<td>44344</td>
<td>24154</td>
<td>44524</td>
<td>43352</td>
</tr>
<tr>
<td></td>
<td>15333</td>
<td>13144</td>
<td>41545</td>
<td>44514</td>
<td>32515</td>
</tr>
<tr>
<td></td>
<td>23241</td>
<td>55224</td>
<td>43153</td>
<td>13313</td>
<td>31455</td>
</tr>
<tr>
<td></td>
<td>32413</td>
<td>45212</td>
<td>53352</td>
<td>24341</td>
<td>31245</td>
</tr>
<tr>
<td></td>
<td>44523</td>
<td>34433</td>
<td>22333</td>
<td>53345</td>
<td>21352</td>
</tr>
<tr>
<td></td>
<td>44444</td>
<td>45321</td>
<td>51315</td>
<td>52244</td>
<td>31531</td>
</tr>
<tr>
<td></td>
<td>24511</td>
<td>31424</td>
<td>44334</td>
<td>31522</td>
<td>35242</td>
</tr>
<tr>
<td></td>
<td>53521</td>
<td>33133</td>
<td>12312</td>
<td>13143</td>
<td>34533</td>
</tr>
<tr>
<td></td>
<td>12134</td>
<td>44124</td>
<td>43331</td>
<td>21432</td>
<td>24333</td>
</tr>
<tr>
<td></td>
<td>13245</td>
<td>12253</td>
<td>51253</td>
<td>23351</td>
<td>25114</td>
</tr>
<tr>
<td></td>
<td>44154</td>
<td>54143</td>
<td>24442</td>
<td>41345</td>
<td>15221</td>
</tr>
<tr>
<td></td>
<td>25145</td>
<td>12132</td>
<td>44532</td>
<td>12514</td>
<td>41513</td>
</tr>
<tr>
<td></td>
<td>14252</td>
<td>42445</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
US Navy Cryptologic Mathematicians
October 1945
Mathematicians

- Alfred Clifford
  (Top, 1)
- Marshall Hall, Jr.
  (Middle, 2)
- Andrew Gleason
  (Middle, 5)
Computer Industry

- Howard Engstrom  
  (Top, 5)
- Lawrence Steinhardt  
  (Top, 8)
• Howard Campagne
  (Top, 10)
• Reed B. Dawson
  (Top, 11)
• William A. Blankinship
  (Top, 12)
• William Wray
  (Bottom, 6)
• J. J. Eachus
  (Middle, 6)
National Cash Register
Dayton, OH
Naval Computing Machine Laboratory
Joseph Desch (1907 – 1987)

2011 Inductee
US Navy Cryptologic Bombe
NCML

1 July 1942 – 1 December 1943

2 Experimental Bombes
99 Bombes
2 Double Bombes
103
1942 and 1943
Station HYPO

Joe Rochefort
(1900 – 1976)

The Codebreakers
4 – 8 May 1942

Photo # NH 51382  USS Lexington burning during the Battle of Coral Sea, May 1942
4 – 7 June 1942

Photo # NH 73065  Japanese aircraft carrier Hiryu burning, morning of 5 June 1942
18 April 1943

Operation Vengeance

Isoroku Yamamoto (1884 - 1943)
1943 The cryptologic crisis of the Battle of the Atlantic eased, and Lt. Lawrence Steinhardt was assigned the responsibility of designing machines to attack Japanese additive cipher systems.
JN-25 and JN-11
Superencrypted codes
# Jn-25 Five-Digit Code

<table>
<thead>
<tr>
<th>Term</th>
<th>Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>hatsu</td>
<td>58743, 78225</td>
</tr>
<tr>
<td>shuushifu</td>
<td>50418</td>
</tr>
<tr>
<td>maru</td>
<td>76833</td>
</tr>
<tr>
<td>begin</td>
<td>45435</td>
</tr>
<tr>
<td>good</td>
<td>34131</td>
</tr>
<tr>
<td>commander-in-chief</td>
<td>41595</td>
</tr>
<tr>
<td>radio silence</td>
<td>66201</td>
</tr>
</tbody>
</table>
## Additives

<table>
<thead>
<tr>
<th>Encryption</th>
<th>Decryption</th>
</tr>
</thead>
<tbody>
<tr>
<td>“Full stop”</td>
<td>Transmitted</td>
</tr>
<tr>
<td>Additive</td>
<td>Additive</td>
</tr>
<tr>
<td>False sum</td>
<td>“Full stop”</td>
</tr>
<tr>
<td>50418</td>
<td>15766</td>
</tr>
<tr>
<td>65358</td>
<td>65358</td>
</tr>
<tr>
<td>15766</td>
<td>50418</td>
</tr>
</tbody>
</table>
Message

67854  59199  76833  57699  10047  70863  06138  27924
### Table of Additives

<table>
<thead>
<tr>
<th>35</th>
<th>86</th>
<th>79</th>
<th>65</th>
<th>49</th>
<th>72</th>
<th>52</th>
<th>03</th>
<th>62</th>
<th>12</th>
</tr>
</thead>
<tbody>
<tr>
<td>87</td>
<td>57721</td>
<td>56649</td>
<td>01532</td>
<td>86060</td>
<td>65120</td>
<td>90082</td>
<td>40243</td>
<td>10421</td>
<td>59335</td>
</tr>
<tr>
<td>92</td>
<td>35988</td>
<td>05767</td>
<td>23488</td>
<td>48677</td>
<td>26777</td>
<td>66467</td>
<td>09369</td>
<td>47063</td>
<td>29174</td>
</tr>
<tr>
<td>26</td>
<td>14631</td>
<td>44724</td>
<td>98070</td>
<td>82480</td>
<td>96050</td>
<td>40144</td>
<td>86542</td>
<td>83622</td>
<td>41739</td>
</tr>
<tr>
<td>55</td>
<td>92353</td>
<td>62535</td>
<td>00333</td>
<td>74293</td>
<td>73377</td>
<td>37673</td>
<td>94279</td>
<td>25952</td>
<td>58247</td>
</tr>
<tr>
<td>59</td>
<td>60087</td>
<td>35203</td>
<td>94816</td>
<td>56708</td>
<td>53233</td>
<td>15177</td>
<td>66115</td>
<td>28621</td>
<td>19950</td>
</tr>
<tr>
<td>53</td>
<td>84793</td>
<td>74508</td>
<td>57057</td>
<td>40029</td>
<td>92135</td>
<td>47861</td>
<td>46694</td>
<td>02960</td>
<td>43254</td>
</tr>
<tr>
<td>66</td>
<td>05877</td>
<td>55352</td>
<td>67331</td>
<td>39925</td>
<td>40129</td>
<td>67420</td>
<td>51375</td>
<td>41395</td>
<td>49111</td>
</tr>
<tr>
<td>96</td>
<td>28079</td>
<td>84234</td>
<td>87758</td>
<td>72050</td>
<td>38431</td>
<td>09399</td>
<td>73613</td>
<td>72553</td>
<td>06088</td>
</tr>
<tr>
<td>28</td>
<td>67600</td>
<td>17247</td>
<td>95378</td>
<td>36759</td>
<td>27135</td>
<td>15772</td>
<td>26102</td>
<td>73492</td>
<td>91394</td>
</tr>
<tr>
<td>17</td>
<td>30103</td>
<td>41777</td>
<td>17780</td>
<td>88154</td>
<td>95706</td>
<td>61075</td>
<td>01016</td>
<td>19166</td>
<td>33401</td>
</tr>
</tbody>
</table>
Encipher

67854  59199  76833  57699  10047  70863  06138  27924
51375  41395  49111  68510  28079  84234  87758  72050
18129  90484  15944  15109  38016  54097  83886  99974
<table>
<thead>
<tr>
<th></th>
<th>35</th>
<th>86</th>
<th>79</th>
<th>65</th>
<th>49</th>
<th>72</th>
<th>52</th>
<th>03</th>
<th>62</th>
<th>12</th>
</tr>
</thead>
<tbody>
<tr>
<td>87</td>
<td>57721</td>
<td>56649</td>
<td>01532</td>
<td>86060</td>
<td>65120</td>
<td>90082</td>
<td>40243</td>
<td>10421</td>
<td>59335</td>
<td>93992</td>
</tr>
<tr>
<td>92</td>
<td>35988</td>
<td>05767</td>
<td>23488</td>
<td>48677</td>
<td>26777</td>
<td>66467</td>
<td>09369</td>
<td>47063</td>
<td>29174</td>
<td>67495</td>
</tr>
<tr>
<td>26</td>
<td>14631</td>
<td>44724</td>
<td>98070</td>
<td>82480</td>
<td>96050</td>
<td>40144</td>
<td>86542</td>
<td>41739</td>
<td>97644</td>
<td>97644</td>
</tr>
<tr>
<td>55</td>
<td>92353</td>
<td>62535</td>
<td>00333</td>
<td>74293</td>
<td>73377</td>
<td>37673</td>
<td>94279</td>
<td>25952</td>
<td>58247</td>
<td>09491</td>
</tr>
<tr>
<td>59</td>
<td>60087</td>
<td>35203</td>
<td>94816</td>
<td>56708</td>
<td>53233</td>
<td>15177</td>
<td>66115</td>
<td>28621</td>
<td>19950</td>
<td>15079</td>
</tr>
<tr>
<td>53</td>
<td>84793</td>
<td>74508</td>
<td>57057</td>
<td>40029</td>
<td>92135</td>
<td>47861</td>
<td>46694</td>
<td>02960</td>
<td>43254</td>
<td>21519</td>
</tr>
<tr>
<td>66</td>
<td>05877</td>
<td>55352</td>
<td>67331</td>
<td>39925</td>
<td>40129</td>
<td>67420</td>
<td>51375</td>
<td>41395</td>
<td>49111</td>
<td>68510</td>
</tr>
<tr>
<td>96</td>
<td>28079</td>
<td>84234</td>
<td>87758</td>
<td>72050</td>
<td>38431</td>
<td>09399</td>
<td>73613</td>
<td>72553</td>
<td>06088</td>
<td>93312</td>
</tr>
<tr>
<td>28</td>
<td>67600</td>
<td>17247</td>
<td>95378</td>
<td>36759</td>
<td>27135</td>
<td>15772</td>
<td>26102</td>
<td>73492</td>
<td>91394</td>
<td>07984</td>
</tr>
<tr>
<td>17</td>
<td>30103</td>
<td>41777</td>
<td>17780</td>
<td>88154</td>
<td>95706</td>
<td>61075</td>
<td>01016</td>
<td>19166</td>
<td>33401</td>
<td>52278</td>
</tr>
</tbody>
</table>
## Indicators

<table>
<thead>
<tr>
<th>00300</th>
<th>78389</th>
<th>89535</th>
<th>87019</th>
<th>49073</th>
<th>38472</th>
<th>91259</th>
<th>86989</th>
<th>38094</th>
</tr>
</thead>
<tbody>
<tr>
<td>00303</td>
<td>30962</td>
<td>49517</td>
<td>75834</td>
<td>29851</td>
<td>43682</td>
<td>42742</td>
<td>43467</td>
<td>40719</td>
</tr>
<tr>
<td>00301</td>
<td>27755</td>
<td>98185</td>
<td>29481</td>
<td>03559</td>
<td>60851</td>
<td>33868</td>
<td>56611</td>
<td>92166</td>
</tr>
<tr>
<td>00306</td>
<td>87033</td>
<td>67676</td>
<td>18443</td>
<td>16011</td>
<td>86097</td>
<td>12379</td>
<td>57368</td>
<td>00502</td>
</tr>
<tr>
<td>00304</td>
<td>57508</td>
<td>66911</td>
<td>89708</td>
<td>63482</td>
<td>24236</td>
<td>98011</td>
<td>96177</td>
<td>72072</td>
</tr>
</tbody>
</table>
Vertical Alignment of Messages

<p>| | | | | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>00300</td>
<td>78389</td>
<td>89535</td>
<td>87019</td>
<td>49073</td>
<td>38472</td>
<td>91259</td>
<td>86989</td>
<td>38094</td>
</tr>
<tr>
<td>00303</td>
<td>30962</td>
<td>49517</td>
<td>75834</td>
<td>29851</td>
<td>43682</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>00301</td>
<td>27755</td>
<td>98185</td>
<td>29481</td>
<td>03559</td>
<td>60851</td>
<td>33868</td>
<td>56611</td>
<td></td>
</tr>
<tr>
<td>00306</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>87033</td>
<td>67676</td>
</tr>
<tr>
<td>00304</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>57508</td>
<td>66911</td>
<td>89708</td>
</tr>
</tbody>
</table>
Differencing

(Codegroup \text{1} + \text{Additive})
(Codegroup \text{2} + \text{Additive})

\text{Codegroup 1} - \text{Codegroup 2}
Two Problems

Align message groups vertically – in depth
Align message groups and recovered additives
Align Message Groups Vertically – in Depth

Copperhead I
Double Repeats

05661 06511 07465 07495 12143 14240 14963 18673

78009 57047 79519 06511 90318 72216 12143 94860 70240
Double Repeats

05661 06511 07465 07495 12143 14240 14963 18673 40876

06511 90318 72216 12134 94860 70240 54911 32814
Double Repeats

MEMORANDUM

27 October 1944

From: CP-20-CM
To: CP-20-G-50

Subj: Double Repeats Expected by Chance on COPPERHEAD I.

1. This is a memorandum for the files regarding the approximate number of chance answers expected on COPPERHEAD I. Derivations of the formulae and calculations were done with the aid of Lt. Comdr. Cramer, Lt. Hall, and Lt. Gleason.

2. For an overlap of "t" between two messages, the number of chances at a double repeat is:

\[
\frac{(t)(t-1)}{2}
\]

If two messages of equal length "L" are slid into and out of alignment, the sum of the total tries for a double repeat is:

\[
\sum_{t=1}^{t=L} \left( \frac{(t)(t-1)}{2} \right) - \left( \frac{(L)(L-1)}{2} \right)
\]
## Number of Positions for Double Repeats

<table>
<thead>
<tr>
<th>overlap</th>
<th>positions</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>4</td>
<td>6</td>
</tr>
<tr>
<td>5</td>
<td>10</td>
</tr>
</tbody>
</table>
### Number of Positions for Double Repeats

<table>
<thead>
<tr>
<th>Positions</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>□ □ □ □ □ □</td>
<td>4</td>
</tr>
<tr>
<td>□ □ □ □ □</td>
<td>4</td>
</tr>
<tr>
<td>□ □ □ □ □</td>
<td>3</td>
</tr>
<tr>
<td>□ □ □ □</td>
<td>3</td>
</tr>
<tr>
<td>□ □ □ □</td>
<td>2</td>
</tr>
<tr>
<td>□ □ □ □</td>
<td>2</td>
</tr>
<tr>
<td>□ □ □ □</td>
<td>1</td>
</tr>
<tr>
<td>□ □ □ □</td>
<td>1</td>
</tr>
<tr>
<td>□ □ □ □</td>
<td>0</td>
</tr>
<tr>
<td>□ □ □ □</td>
<td>0</td>
</tr>
<tr>
<td>□ □ □ □</td>
<td>0</td>
</tr>
</tbody>
</table>
Positions for Double Repeats

\[ \frac{t(t-1)}{2} \]

\[ 2 \sum_{t=1}^{L} \frac{t(t-1)}{2} - \frac{L(L-1)}{2} \]
Positions for Double Repeats

$L = 100 \quad 328, 350$
Positions for Double Repeats

\[ 328350 \times \frac{1000 \times 999}{2} = 16.4 \times 10^{10} \]
Repeats

One repeat

\[
\frac{1}{10^5} \times \frac{1}{10^5} + \frac{1}{10^5} \times \frac{1}{10^5} + \cdots \frac{1}{10^5} \times \frac{1}{10^5} = \frac{1}{10^5}
\]
Double Repeat

\[ \frac{1}{10^5} \times \frac{1}{10^5} = \frac{1}{10^{10}} \]
Random Double Repeats

\[ 16.4 \times 10^{10} \times \frac{1}{10^{10}} = 16.4 \]
Copperhead I

Align messages in depth
19 November 1943 Proposal for Copperhead I submitted.

6 December 1943 Copperhead I program was approved.

3 November 1944 Copperhead I shipped to NCA.
Copperhead I

- 25 August 1944 Engstrom to NCML
  Copperhead I will need to handle 4-digit systems.
- 26 August 1944 Reply
  Will provide switch to change from 4 to 5 digits.
- 25 September 1944 From Engstrom
  Copperhead I needed as soon as possible.
- 14 October 1944 From Engstrom
  Request status report on 4-digit problem.
October-November 1944

- 23 – 26 October 1944 The Battles of Leyte Gulf.

- 24 – 27 October 1944 Desch’s name no longer appears on existing communications records.

- 15 – 18 November 1944 Attack on Hi-81.
Copperhead II
Align messages and recovered additives
Copperhead II

Slide recovered additives along messages, subtract, and check for high frequency code groups.
Stripping

68377  35159  31043  47671  50280  80284  55463  10816
86060   90082              59335  93992
59199   57699              06138  27924
Copperhead II

20 December 1943 Copperhead II is low priority.

8 November 1944 Copperhead II project is terminated.
Copperheads III and IV
JN-25

Error detection property
JN-25

67854 59199 76833 57699 10047 70863 06138 27924
## JN-25 Bias

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>35</td>
</tr>
<tr>
<td>6</td>
<td>210</td>
</tr>
<tr>
<td>9</td>
<td>715</td>
</tr>
<tr>
<td>12</td>
<td>1745</td>
</tr>
<tr>
<td>15</td>
<td>3246</td>
</tr>
<tr>
<td>18</td>
<td>4840</td>
</tr>
<tr>
<td>21</td>
<td>5875</td>
</tr>
<tr>
<td>24</td>
<td>5875</td>
</tr>
<tr>
<td>27</td>
<td>4840</td>
</tr>
<tr>
<td>30</td>
<td>3246</td>
</tr>
<tr>
<td>33</td>
<td>1745</td>
</tr>
<tr>
<td>36</td>
<td>715</td>
</tr>
<tr>
<td>39</td>
<td>210</td>
</tr>
<tr>
<td>42</td>
<td>35</td>
</tr>
<tr>
<td>45</td>
<td>1</td>
</tr>
</tbody>
</table>

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>9.76%</td>
</tr>
<tr>
<td>1</td>
<td>17.60%</td>
</tr>
<tr>
<td>2</td>
<td>5.36%</td>
</tr>
<tr>
<td>3</td>
<td>5.36%</td>
</tr>
<tr>
<td>4</td>
<td>17.60%</td>
</tr>
<tr>
<td>5</td>
<td>9.765%</td>
</tr>
<tr>
<td>6</td>
<td>2.77%</td>
</tr>
<tr>
<td>7</td>
<td>14.51%</td>
</tr>
<tr>
<td>8</td>
<td>14.51%</td>
</tr>
<tr>
<td>9</td>
<td>2.77%</td>
</tr>
</tbody>
</table>
Weights

Hall’s weights
Shinn weights
Hall’s Weights

78132  06936
72206  02267*
38804  03488
421
Edward Simpson CB ceased being an active statistician in 1947, when he joined the Civil Service. But statistics owes him much. He is the Simpson of Simpson's index of diversity\(^1\) and of Simpson's paradox,\(^2\) the bizarre apparent contradiction which he published in 1951 and which has puzzled students of statistics ever since. Perhaps more importantly, for the world as well as for statistics, from 1942 to 1945 he was a code breaker at Bletchley Park, where Alan Turing and others broke enemy ciphers and the world's first modern computer was developed. Here Edward Simpson tells the hitherto unpublished story of the part that Bayesian statistics played in breaking two of the enemy ciphers.

It is now widely thought not yet universally understood that the world's first large-scale electronic digital computer was created at Bletchley Park during the Second World War. The introduction there of Colossus in late 1943 transformed the enigma-breaking effort on the German enigma cipher that the contributors called Turing and switched it to its end. Turing was even more complex than the later ‘Nazi’ Enigma. The machine that weighed it was made by the Lorenz company. Its size ensured that it was not a portable device like Enigma. It was used radioliterally for the most important messages passing between the German High Command in Berlin and the Army Group commanders across Europe.

It took people who were conceptually and technically brilliant to build it. To name only three of those Turing’s engineering system was worked out, without anyone ever having seen the machine, by Bill Tutte, the concept of the machine and the specification of its mechanical processing of the cryptanalysis, and the leadership of its

---


## Shinn Weights

### Differences of Scanning Groups

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>9</td>
<td>8</td>
<td>7</td>
<td>6</td>
<td>5</td>
<td>4</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>1</td>
<td>0</td>
<td>9</td>
<td>8</td>
<td>7</td>
<td>6</td>
<td>5</td>
<td>4</td>
<td>3</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>2</td>
<td>1</td>
<td>0</td>
<td>9</td>
<td>8</td>
<td>7</td>
<td>6</td>
<td>5</td>
<td>4</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>3</td>
<td>2</td>
<td>1</td>
<td>0</td>
<td>9</td>
<td>8</td>
<td>7</td>
<td>6</td>
<td>5</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>4</td>
<td>3</td>
<td>2</td>
<td>1</td>
<td>0</td>
<td>9</td>
<td>8</td>
<td>7</td>
<td>6</td>
</tr>
<tr>
<td>6</td>
<td>6</td>
<td>5</td>
<td>4</td>
<td>3</td>
<td>2</td>
<td>1</td>
<td>0</td>
<td>9</td>
<td>8</td>
<td>7</td>
</tr>
<tr>
<td>7</td>
<td>7</td>
<td>6</td>
<td>5</td>
<td>4</td>
<td>3</td>
<td>2</td>
<td>1</td>
<td>0</td>
<td>9</td>
<td>8</td>
</tr>
<tr>
<td>8</td>
<td>8</td>
<td>7</td>
<td>6</td>
<td>5</td>
<td>4</td>
<td>3</td>
<td>2</td>
<td>1</td>
<td>0</td>
<td>9</td>
</tr>
<tr>
<td>9</td>
<td>9</td>
<td>8</td>
<td>7</td>
<td>6</td>
<td>5</td>
<td>4</td>
<td>3</td>
<td>2</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

### Distribution of Differences

<p>| | | | | | | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1304</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>0.0906</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>0.0754</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>0.1246</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>0.1094</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>0.0696</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>0.1094</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>0.1246</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>0.0754</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>0.0906</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Difference</td>
<td>Shinn Weights</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>------------</td>
<td>---------------</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>438</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1 or 9</td>
<td>300</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2 or 8</td>
<td>249</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3 or 7</td>
<td>418</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4 or 6</td>
<td>365</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>230</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Shinn Weights

78132  1
06936  4
7  418
3*
Copperhead V

Align JN-25 messages in depth
<table>
<thead>
<tr>
<th>2</th>
<th>4</th>
<th>2</th>
<th>8</th>
<th>8</th>
<th>8</th>
<th>2</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td>02082</td>
<td>02688</td>
<td>04107</td>
<td>04455</td>
<td>06525</td>
<td>09207</td>
<td>09274</td>
<td>22871</td>
</tr>
<tr>
<td>5</td>
<td>8</td>
<td>5</td>
<td>4</td>
<td>7</td>
<td>6</td>
<td>6</td>
<td></td>
</tr>
<tr>
<td>00492</td>
<td>01962</td>
<td>05235</td>
<td>07377</td>
<td>07406</td>
<td>09520</td>
<td>12490</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>4</td>
<td>3</td>
<td>4</td>
<td>1</td>
<td>6</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>300</td>
<td>365</td>
<td>418</td>
<td>365</td>
<td>300</td>
<td>365</td>
<td>365</td>
<td>365</td>
</tr>
</tbody>
</table>
Copperhead V

Never Produced.
Mamba

Align JN-25 messages and recovered additives
# Mamba

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>9.76%</td>
</tr>
<tr>
<td>1</td>
<td>17.60%</td>
</tr>
<tr>
<td>2</td>
<td>5.36%</td>
</tr>
<tr>
<td>3</td>
<td>5.36%</td>
</tr>
<tr>
<td>4</td>
<td>17.60%</td>
</tr>
<tr>
<td>5</td>
<td>9.765%</td>
</tr>
<tr>
<td>6</td>
<td>2.77%</td>
</tr>
<tr>
<td>7</td>
<td>14.51%</td>
</tr>
<tr>
<td>8</td>
<td>14.51%</td>
</tr>
<tr>
<td>9</td>
<td>2.77%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Additive False Sum</th>
<th>MAX Cards</th>
<th>MIN Cards</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1, 4, 7, 8</td>
<td>2, 3, 6, 9</td>
</tr>
<tr>
<td>1</td>
<td>0, 3, 6, 7</td>
<td>1, 2, 5, 8</td>
</tr>
<tr>
<td>2</td>
<td>9, 2, 5, 6</td>
<td>0, 1, 4, 7</td>
</tr>
<tr>
<td>3</td>
<td>8, 1, 4, 5</td>
<td>9, 0, 3, 6</td>
</tr>
<tr>
<td>4</td>
<td>7, 0, 3, 4</td>
<td>8, 9, 2, 5</td>
</tr>
<tr>
<td>5</td>
<td>6, 9, 2, 3</td>
<td>7, 8, 1, 4</td>
</tr>
<tr>
<td>6</td>
<td>5, 8, 1, 2</td>
<td>6, 7, 0, 3</td>
</tr>
<tr>
<td>7</td>
<td>4, 7, 0, 1</td>
<td>5, 9, 6, 2</td>
</tr>
<tr>
<td>8</td>
<td>3, 6, 9, 0</td>
<td>4, 5, 8, 1</td>
</tr>
<tr>
<td>9</td>
<td>2, 5, 8, 9</td>
<td>3, 4, 7, 0</td>
</tr>
</tbody>
</table>
### Mamba

<table>
<thead>
<tr>
<th>Message</th>
<th>Additive</th>
</tr>
</thead>
<tbody>
<tr>
<td>5 6 8 4 6 9 3 5</td>
<td>5 4 0 6 4 4 4 9</td>
</tr>
<tr>
<td>49073 38472 91259</td>
<td>82229 89383 25426</td>
</tr>
<tr>
<td>86989 38094 38898</td>
<td>39390 28057 68035</td>
</tr>
<tr>
<td>66585 89960</td>
<td>60457 62046</td>
</tr>
</tbody>
</table>
Mamba

5 6 8 4 6 9 3 5
6 7 1 5 7 7 7 2
9 0 4 8 0 0 0 5
2 3 7 1 3 3 3 8
3 4 8 2 4 4 4 9
5 4 0 6 4 4 4 9
7 8 2 6 8 8 8 3
8 9 3 7 9 9 9 4
1 2 6 0 2 2 2 7
4 5 9 3 5 5 5 0
2. The detector should register a hit if the difference between the maximal and minimal contributions is equal to or greater than the following formula:

\[ \text{Maximal} - \text{Minimal} \geq AZ + C \]

where \( A \) equals a constant controllable by a calibrated dial over the range from 0.1 to 0.5, \( Z \) is the overlap, and \( C \) is a constant controllable by a calibrated dial over the range from 0 to 10. For example, if \( A \) is set at 0.3 and \( C \) at 5, then a hit should be registered if the difference is 8 at an overlap of 10 and 20.
Distributions

<table>
<thead>
<tr>
<th>( L )</th>
<th>( \mu )</th>
<th>( \sigma )</th>
<th>( \mu )</th>
<th>( \sigma )</th>
<th>( \mu )</th>
<th>( \sigma )</th>
<th>( \mu )</th>
<th>( \sigma )</th>
</tr>
</thead>
<tbody>
<tr>
<td>45</td>
<td>0.</td>
<td>6.</td>
<td>21.6266</td>
<td>5.08328</td>
<td>0.</td>
<td>6.32456</td>
<td>24.0255</td>
<td>5.35825</td>
</tr>
<tr>
<td>50</td>
<td>0.</td>
<td>6.</td>
<td>26.4325</td>
<td>5.61978</td>
<td>0.</td>
<td>6.9282</td>
<td>28.8354</td>
<td>5.86967</td>
</tr>
<tr>
<td>55</td>
<td>0.</td>
<td>6.</td>
<td>33.6413</td>
<td>6.10934</td>
<td>0.</td>
<td>7.48331</td>
<td>36.0443</td>
<td>6.56249</td>
</tr>
<tr>
<td>60</td>
<td>0.</td>
<td>6.</td>
<td>38.4472</td>
<td>6.77771</td>
<td>0.</td>
<td>8.30296</td>
<td>40.9827</td>
<td>6.89892</td>
</tr>
<tr>
<td>65</td>
<td>0.</td>
<td>7.2111</td>
<td>44.2027</td>
<td>8.21597</td>
<td>0.</td>
<td>8.</td>
<td>46.9289</td>
<td>8.43417</td>
</tr>
<tr>
<td>70</td>
<td>0.</td>
<td>7.</td>
<td>50.9601</td>
<td>8.51372</td>
<td>0.</td>
<td>8.55423</td>
<td>51.9441</td>
<td>8.64724</td>
</tr>
<tr>
<td>75</td>
<td>0.</td>
<td>7.74597</td>
<td>57.9037</td>
<td>9.87048</td>
<td>0.</td>
<td>8.5263</td>
<td>58.8277</td>
<td>10.0859</td>
</tr>
<tr>
<td>80</td>
<td>0.</td>
<td>8.</td>
<td>64.7632</td>
<td>10.3767</td>
<td>0.</td>
<td>9.15693</td>
<td>64.9111</td>
<td>10.6022</td>
</tr>
</tbody>
</table>
Mamba

12 April 1944 “Mamba Theory.”

2 May 1944 “Communications on design.” JN-11 is no longer a priority.


1 August 1944 JN-11 is no longer priority.

18 November 1944 Status of Mamba? Acme Pattern and Tool Company.
NCML

1 December 1943 – 1 July 1945 production
<table>
<thead>
<tr>
<th>NCML</th>
<th>1 December 1943 – 1 July 1945</th>
</tr>
</thead>
<tbody>
<tr>
<td>Copperhead One</td>
<td>1 Parallel Grenade</td>
</tr>
<tr>
<td>Vipers</td>
<td>Mamba</td>
</tr>
<tr>
<td>Mike</td>
<td>Wave Filters</td>
</tr>
<tr>
<td>Rattlers</td>
<td>Boa</td>
</tr>
<tr>
<td>Gypsy-Topas</td>
<td>Special Boa</td>
</tr>
<tr>
<td>Double Bombes</td>
<td>Satyr</td>
</tr>
<tr>
<td>Asp</td>
<td>495 Pluggable Reflectors</td>
</tr>
<tr>
<td>Sliding Grenades</td>
<td>4 Standard Grenades</td>
</tr>
<tr>
<td>M-9</td>
<td>Drag Grenade</td>
</tr>
<tr>
<td>M-8</td>
<td>Coast Guard Grenade</td>
</tr>
<tr>
<td>5</td>
<td>10</td>
</tr>
<tr>
<td>10</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>30</td>
</tr>
<tr>
<td>3</td>
<td>60</td>
</tr>
<tr>
<td>2</td>
<td>10</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>60</td>
<td>1</td>
</tr>
<tr>
<td>8</td>
<td>1</td>
</tr>
<tr>
<td>5</td>
<td>10</td>
</tr>
<tr>
<td>8</td>
<td>8</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>8</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>8</td>
</tr>
<tr>
<td>1</td>
<td>5</td>
</tr>
<tr>
<td>1</td>
<td>3</td>
</tr>
</tbody>
</table>
It is believed that considerable thought should be given to the desirability of building equipment of general usefulness which might do this and other jobs rather than a number of machines each designed to meet a specific need.
Universal Machine

This thought is advanced because it is felt that we should be building for the future where in machines built for specific purposes may become obsolete but the value of a more generally universal machine might become enhanced.

J. Howard
Engineering Research Associates
CSAW

Joseph Wenger

ERA

- Howard Engstrom
- William Norris
- John Parker
“Task 13” ERA 1101
A Similar Point of View: Colossus
An Alternative Point of View: ENIAC
Thanks