Machine Attack on JN-25

Chris Christensen
Northern Kentucky University

Naval Communications

Laurance Safford (1890 – 1973)

CAPT LAURANCE SAFFORD, USN

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

Correspondence Course

INDEX

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
11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36

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	98	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 insolate the individual cipher equivalents of plain-text letters after they have been run together in the cryptogram.

(2) Systematically mixed numerical cipher alphabet

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

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

Problem No. 2

5 3 2 4 1	5 4 5 3 2	2 4 4 3 2	5 1 2 4 3	2 4 2 3 1
5 4 4 4 5	4 5 3 2 5	1 4 3 4 4	1 4 1 5 2	1 4 1 1 5
4 3 4 5 3	5 2 1 2 3	3 5 1 2 5	1 1 4 2 1	5 3 3 3 4
5 3 2 4 4	2 3 1 5 4	5 4 5 2 4	4 3 2 4 1	4 4 4 3 2
1 2 5 3 2	4 4 3 4 4	2 4 1 5 4	4 4 5 2 4	4 3 3 5 2
1 5 3 3 3	1 3 1 4 4	4 1 5 4 5	4 4 5 1 4	3 2 5 1 5
2 3 2 4 1	5 5 2 2 4	4 3 1 5 3	1 3 3 1 3	3 1 4 5 5
3 2 4 1 3	4 5 2 1 2	5 3 3 5 2	2 4 3 4 1	3 1 2 4 5
4 4 5 2 3	3 4 4 3 3	2 2 3 3 3	5 3 3 4 5	2 1 3 5 2
4 4 4 4 4	4 5 3 2 1	5 1 3 1 5	5 2 2 4 4	3 1 5 3 1
2 4 5 1 1	3 1 4 2 4	4 4 3 3 4	3 1 5 2 2	3 5 2 4 2
5 3 5 2 1	3 3 1 3 3	1 2 3 1 2	1 3 1 4 3	3 4 5 3 3
1 2 1 3 4	4 4 1 2 4	4 3 3 3 1	2 1 4 3 2	2 4 3 3 3
1 3 2 4 5	1 2 2 5 3	5 1 2 5 3	2 3 3 5 1	2 5 1 1 4
4 4 1 5 4	5 4 1 4 3	2 4 4 4 2	4 1 3 4 5	1 5 2 2 1
2 5 1 4 5	1 2 1 3 2	4 4 5 3 2	1 2 5 1 4	4 1 5 1 3
1 4 2 5 2	4 2 4 4 5			

OP-20-GM

Naval Communications Annex

Washington, DC

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)

NSA

- Howard Campaigne
  (Top, 10)
- Reed B. Dawson
  (Top, 11)
- William A. Blankinship
  (Top, 12)
- William Wray
  (Bottom, 6)
- J. J. Eachus
  (Middle, 6)

NCML

National Cash Register

Dayton, OH

Naval Computing Machine Laboratory

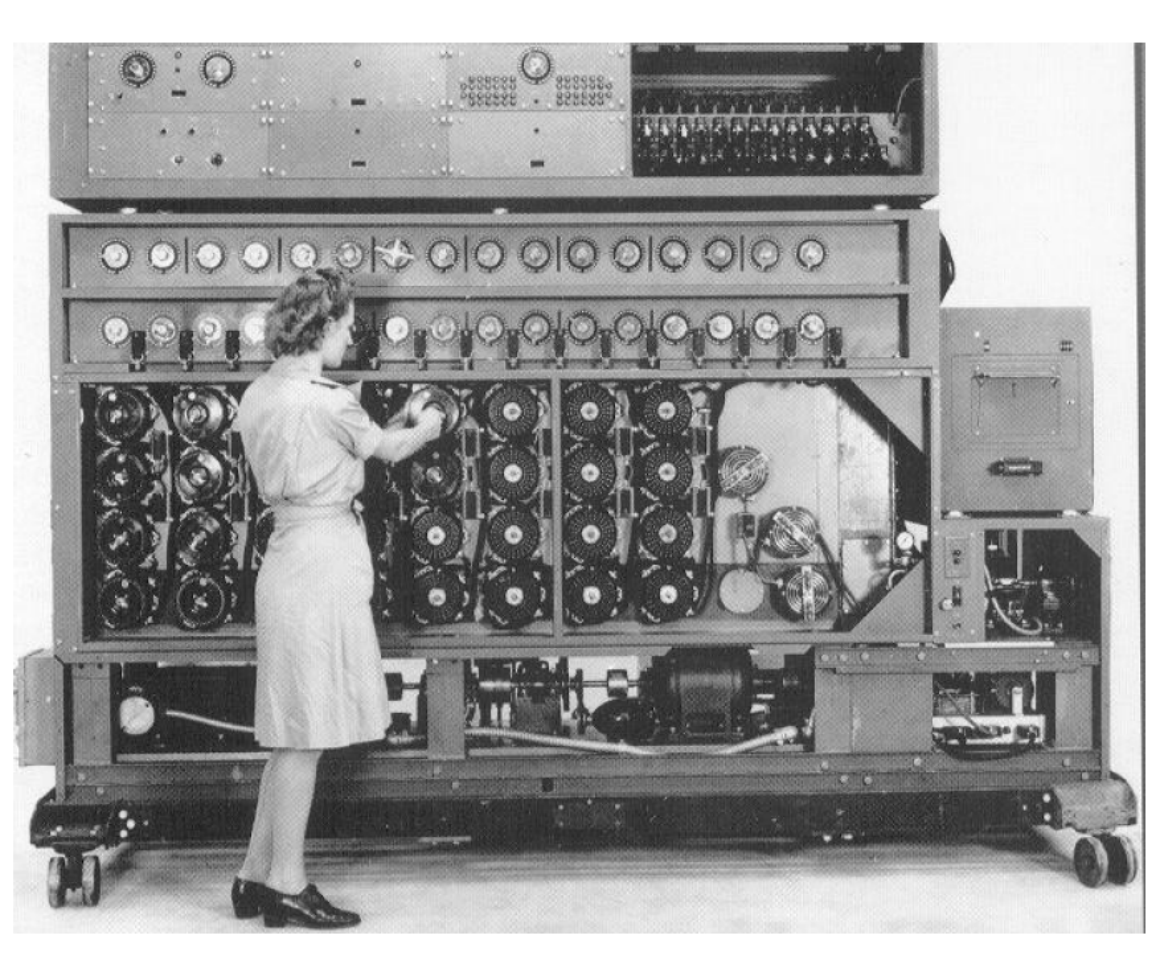
Joseph Desch (1907 – 1987)

2011 Inductee

HALL OF HONOR
These Were the Giants

JOSEPH DESCH

US Navy Cryptologic Bombe



NCML

1 July 1942 – 1 December 1943

2 Experimental Bombes
99 Bombes
2 Double Bombes
103

1942 and 1943

JN-25

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

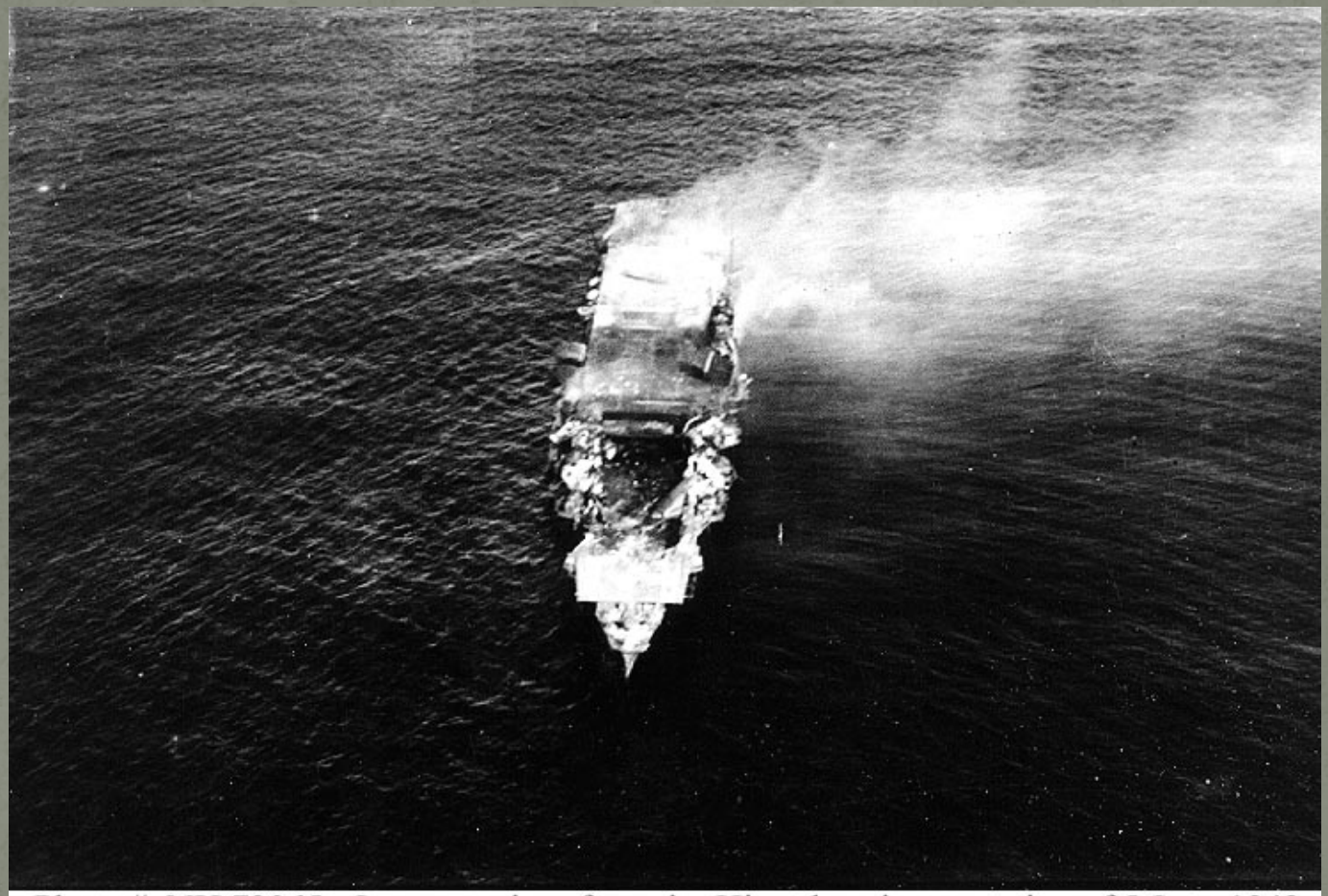
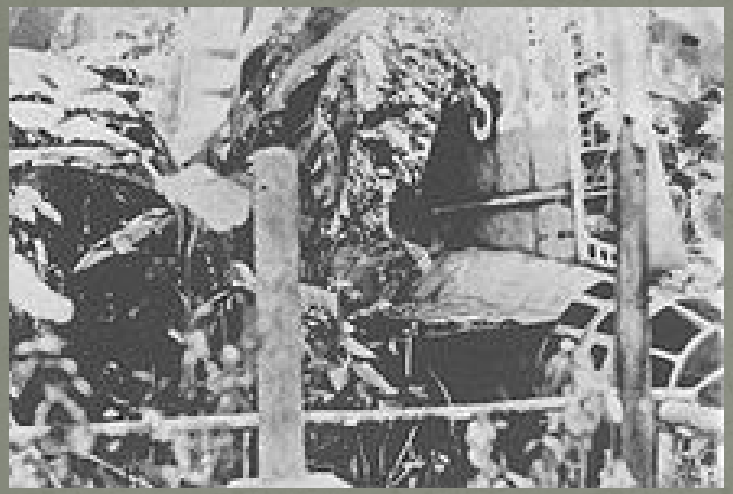


Photo # NH 73065 Japanese aircraft carrier Hiryu burning, morning of 5 June 1942

18 April 1943

Operation Vengeance



Isoruku Yamamoto (1884 - 1943)

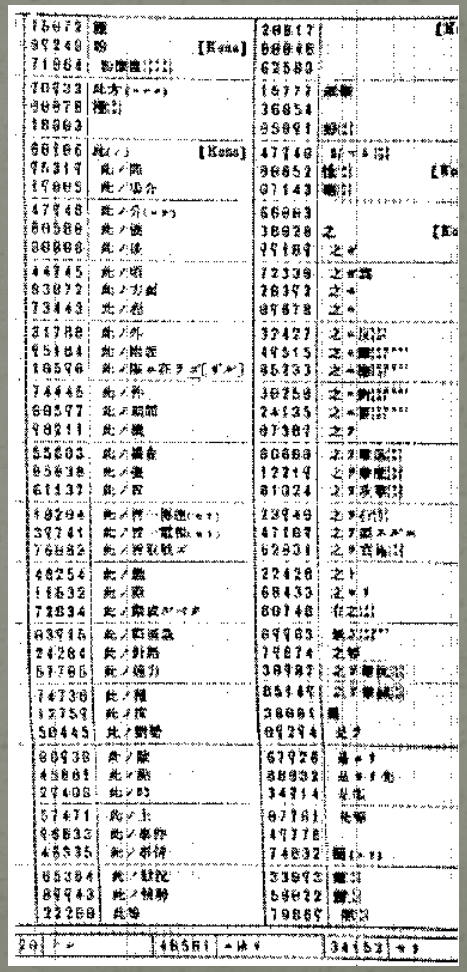
Copperheads I - V

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

Superenciphered codes

JN-25



Jn-25 Five-Digit Code

hatsu	from	58743, 78225
shuushifu	full stop	50418
maru	ship name	76833
	begin	45435
	good	34131
	commander-in-chief	41595
	radio silence	66201

Additives

Encryption		Decryption	
“Full stop”	50418	Transmitted	15766
Additive	65358	Additive	65358
False sum	15766	“Full stop”	50418

Message

67854 59199 76833 57699 10047 70863 06138 27924

Table of Additives

	35	86	79	65	49	72	52	03	62	12
87	57721	56649	01532	86060	65120	90082	40243	10421	59335	93992
92	35988	05767	23488	48677	26777	66467	09369	47063	29174	67495
26	14631	44724	98070	82480	96050	40144	86542	83622	41739	97644
55	92353	62535	00333	74293	73377	37673	94279	25952	58247	09491
59	60087	35203	94816	56708	53233	15177	66115	28621	19950	15079
53	84793	74508	57057	40029	92135	47861	46694	02960	43254	21519
66	05877	55352	67331	39925	40129	67420	51375	41395	49111	68510
96	28079	84234	87758	72050	38431	09399	73613	72553	06088	93312
28	67600	17247	95378	36759	27135	15772	26102	73492	91394	07984
17	30103	41777	17780	88154	95706	61075	01016	19166	33401	52278

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

Indicator 6386652

	35	86	79	65	49	72	52	03	62	12
87	57721	56649	01532	86060	65120	90082	40243	10421	59335	93992
92	35988	05767	23488	48677	26777	66467	09369	47063	29174	67495
26	14631	44724	98070	82480	96050	40144	86542	83622	41739	97644
55	92353	62535	00333	74293	73377	37673	94279	25952	58247	09491
59	60087	35203	94816	56708	53233	15177	66115	28621	19950	15079
53	84793	74508	57057	40029	92135	47861	46694	02960	43254	21519
66	05877	55352	67331	39925	40129	67420	51375	41395	49111	68510
96	28079	84234	87758	72050	38431	09399	73613	72553	06088	93312
28	67600	17247	95378	36759	27135	15772	26102	73492	91394	07984
17	30103	41777	17780	88154	95706	61075	01016	19166	33401	52278

Indicators

00300	78389	89535	87019	49073	38472	91259	86989	38094
00303	30962	49517	75834	29851	43682	42742	43467	40719
00301	27755	98185	29481	03559	60851	33868	56611	92166
00306	87033	67676	18443	16011	86097	12379	57368	00502
00304	57508	66911	89708	63482	24236	98011	96177	72072

Vertical Alignment of Messages

00300	78389	89535	87019	49073	38472	91259	86989	38094
00303				30962	49517	75834	29851	43682
00301		27755	98185	29481	03559	60851	33868	56611
00306							87033	67676
00304					57508	66911	89708	63482

Differencing

(Codegroup 1 + Additive)

(Codegroup 2 + Additive)

Codegroup 1 – 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

S E C R E T

Op-20-G/mb

SECRET

27 October 1944.

MEMORANDUM

From: OP-20-GM.
To: OP-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.

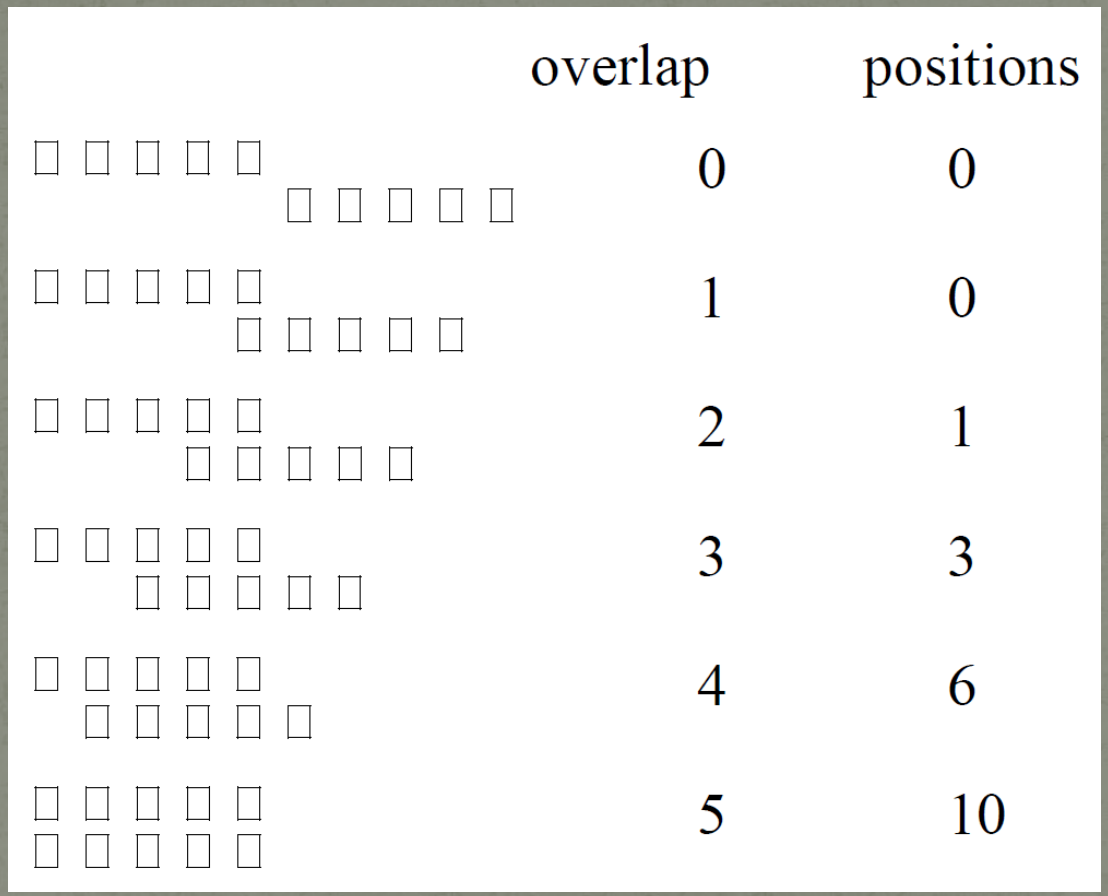
2. For an overlap of "t" between two messages, the number of chances at a double repeat is:

$$\frac{(t)(t-1)}{2}$$

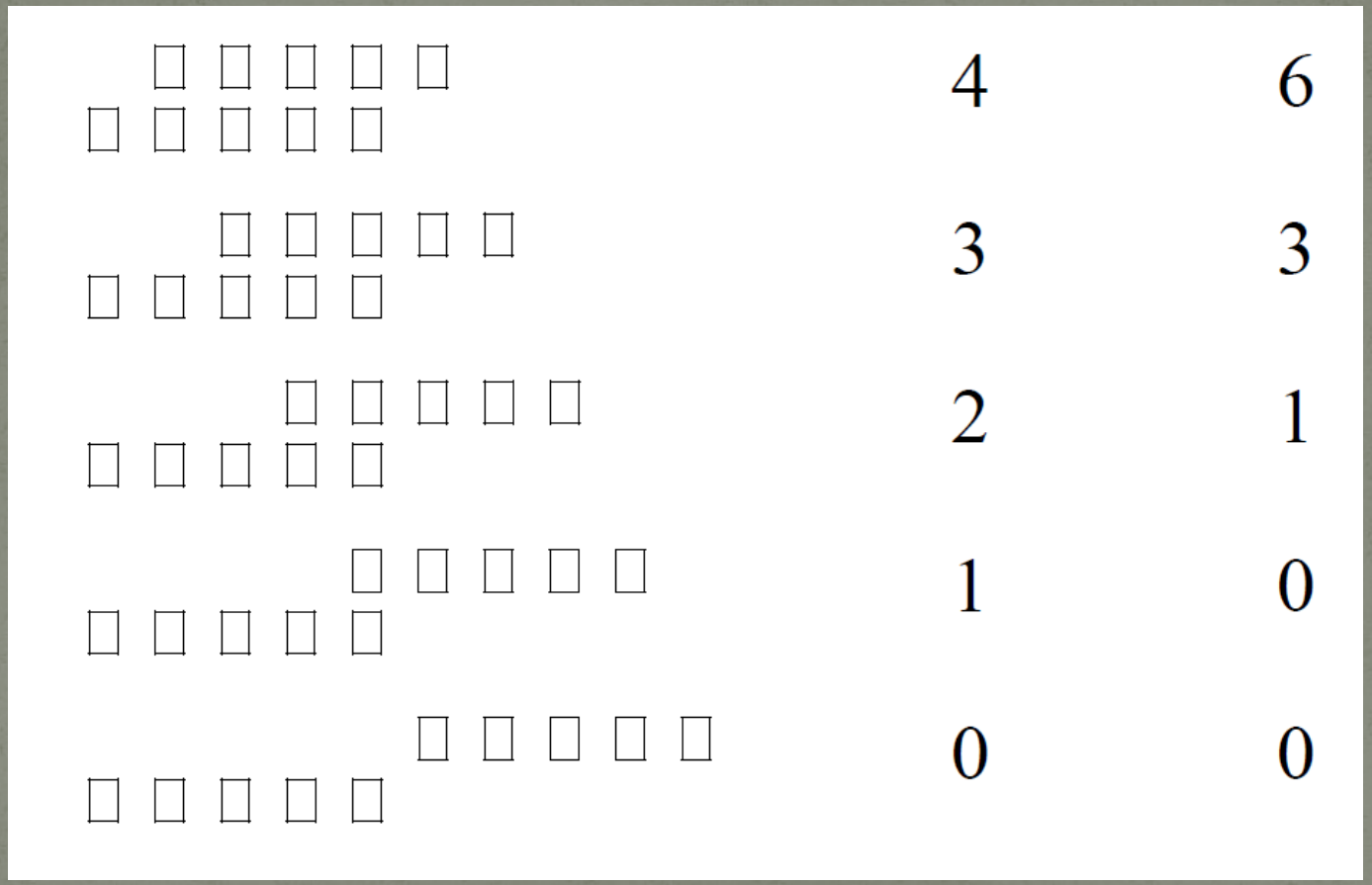
If two messages of equal length "L" are slid into and out of alignment, the sum of the total tries for a double repeat is:

$$2\sum_{t=1}^{t=L} \frac{(t)(t-1)}{2} - \frac{(L)(L-1)}{2}$$

Number of Positions for Double Repeats



Number of Positions for Double Repeats



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 = 100 328, 350

Positions for Double Repeats

$$328350 \times \frac{1000 \times 999}{2} = 16.4 \times 10^{10}$$

Repeats

One repeat

$$\underbrace{\frac{1}{10^5}\times\frac{1}{10^5}+\frac{1}{10^5}\times\frac{1}{10^5}+\cdots\frac{1}{10^5}\times\frac{1}{10^5}}_{\frac{1}{10^5}}=\frac{1}{10^5}$$

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

Copperhead I

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

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

0	1
3	35
6	210
9	715
12	1745
15	3246
18	4840
21	5875
24	5875
27	4840
30	3246
33	1745
36	715
39	210
42	35
45	1

0	9.76%
1	17.60%
2	5.36%
3	5.36%
4	17.60%
5	9.765%
6	2.77%
7	14.51%
8	14.51%
9	2.77%

Weights

Hall's weights

Shinn weights

Hall's Weights

78132

06936

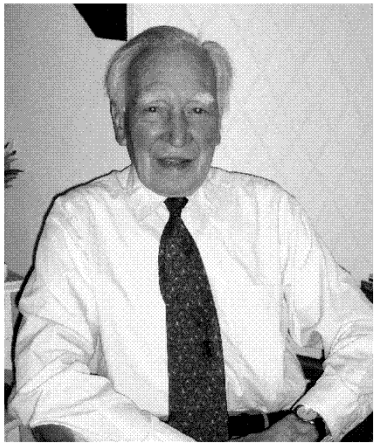
72206 02267* 421

38804 03488

Edward Simpson

Edward Simpson: Bayes at Bletchley Park

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, though 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 cryptanalytic attack on the German teleprinter cipher that the codebreakers called Tunny, and enabled it to be read.

Tunny was even more complex than the better-known Enigma. The machine that enciphered it was made by the Lorenz company. Its size meant that it was not a portable device like Enigma. It was used exclusively 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 break it. To name only three of them: Tunny's enciphering system was worked out, without anyone ever having seen the machine, by Bill Tutte; the concept and specification of high-speed electronic processing of the cryptanalysis and the leadership of its

Shinn Weights

Differences of Scanning Groups

	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	5	6	7	8	9
1	1	0	9	8	7	6	5	4	3	2
2	2	1	0	9	8	7	6	5	4	3
3	3	2	1	0	9	8	7	6	5	4
4	4	3	2	1	0	9	8	7	6	5
5	5	4	3	2	1	0	9	8	7	6
6	6	5	4	3	2	1	0	9	8	7
7	7	6	5	4	3	2	1	0	9	8
8	8	7	6	5	4	3	2	1	0	9
9	9	8	7	6	5	4	3	2	1	0

Distribution of Differences

0	.1304
1	.0906
2	.0754
3	.1246
4	.1094
5	.0696
6	.1094
7	.1246
8	.0754
9	.0906

Shinn Weights

Difference	Shinn Weights
0	438
1 or 9	300
2 or 8	249
3 or 7	418
4 or 6	365
5	230

Shinn Weights

78132	1	
06936	4	
	7	
	3*	418

Copperhead V

Align JN-25 messages in depth

Copperhead V

2	4	2	8	8	8	2	0
02082	02688	04107	04455	06525	09207	09274	22871
	5	8	5	4	7	6	6
	00492	01962	05235	07377	07406	09520	12490
	9	4	3	4	1	6	4
	300	365	418	365	300	365	365

Copperhead V

Never Produced.

Mamba

Align JN-25 messages and recovered additives

Mamba

0	9.76%
1	17.60%
2	5.36%
3	5.36%
4	17.60%
5	9.765%
6	2.77%
7	14.51%
8	14.51%
9	2.77%

Additive False Sum	MAX Cards	MIN Cards
0	1, 4, 7, 8	2, 3, 6, 9
1	0, 3, 6, 7	1, 2, 5, 8
2	9, 2, 5, 6	0, 1, 4, 7
3	8, 1, 4, 5	9, 0, 3, 6
4	7, 0, 3, 4	8, 9, 2, 5
5	6, 9, 2, 3	7, 8, 1, 4
6	5, 8, 1, 2	6, 7, 0, 3
7	4, 7, 0, 1	5, 9, 6, 2
8	3, 6, 9, 0	4, 5, 8, 1
9	2, 5, 8, 9	3, 4, 7, 0

Mamba

Message

5	6	8	4	6	9	3	5
49073	38472	91259	86989	38094	38898	66585	89960

Additive

5	4	0	6	4	4	4	9
82229	89383	25426	39390	28057	68035	60457	62046

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

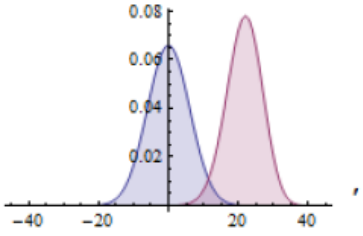
Mamba

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:

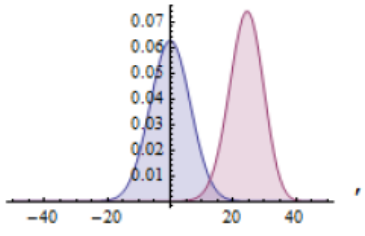
$$\text{Maximal} - \text{Minimal} \geq AZ + C$$

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 .3 and C at 5, then a hit should be registered if the difference is 8 at an overlap of 10 and

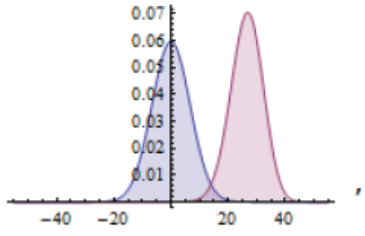
Distributions



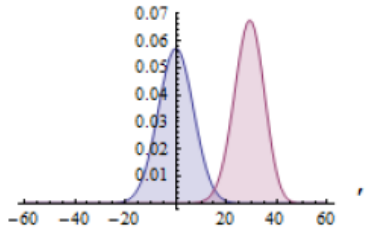
L = 45	Random	CodeGroups
μ	0.	21.6266
σ	6.	5.08328



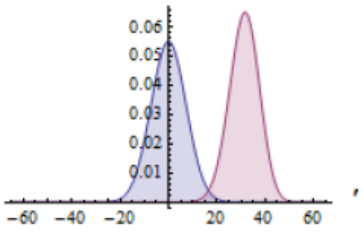
L = 50	Random	CodeGroups
μ	0.	24.0295
σ	6.32456	5.35825



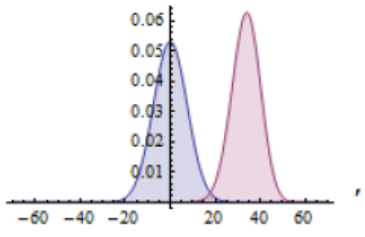
L = 55	Random	CodeGroups
μ	0.	26.4325
σ	6.63325	5.61978



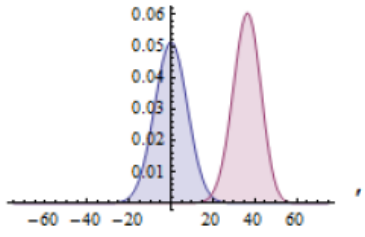
L = 60	Random	CodeGroups
μ	0.	28.8354
σ	6.9282	5.86967



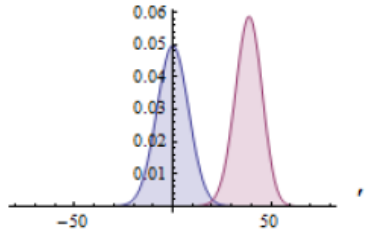
L = 65	Random	CodeGroups
μ	0.	31.2384
σ	7.2111	6.10934



L = 70	Random	CodeGroups
μ	0.	33.6413
σ	7.48331	6.33997



L = 75	Random	CodeGroups
μ	0.	36.0443
σ	7.74597	6.56249



L = 80	Random	CodeGroups
μ	0.	38.4472
σ	8.	6.77771

Mamba

12 April 1944 “Mamba Theory.”

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

3 May 1944 Recommend 2 Mambas. Not required for JN-11.

1 August 1944 JN-11 is no longer priority.

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

Mamba

NCML

1 December 1943 – 1 July 1945 production

NCML

1 December 1943 – 1 July 1945

5 Copperhead One
10 Vipers
1 Mike
3 Rattlers
2 Gypsy-Topas
1 Double Bombes
1 Asp
2 Sliding Grenades
60 M-9
8 M-8

1 Parallel Grenade
1 Mamba
30 Wave Filters
60 Boa
10 Special Boa
1 Satyr
495 Pluggable Reflectors
4 Standard Grenades
1 Drag Grenade
1 Coast Guard Grenade

1 Cilli Grenade
8 Inverted Bombes
Modified 25 Bombes
25 Squelcher Circuits

3 April 1944

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

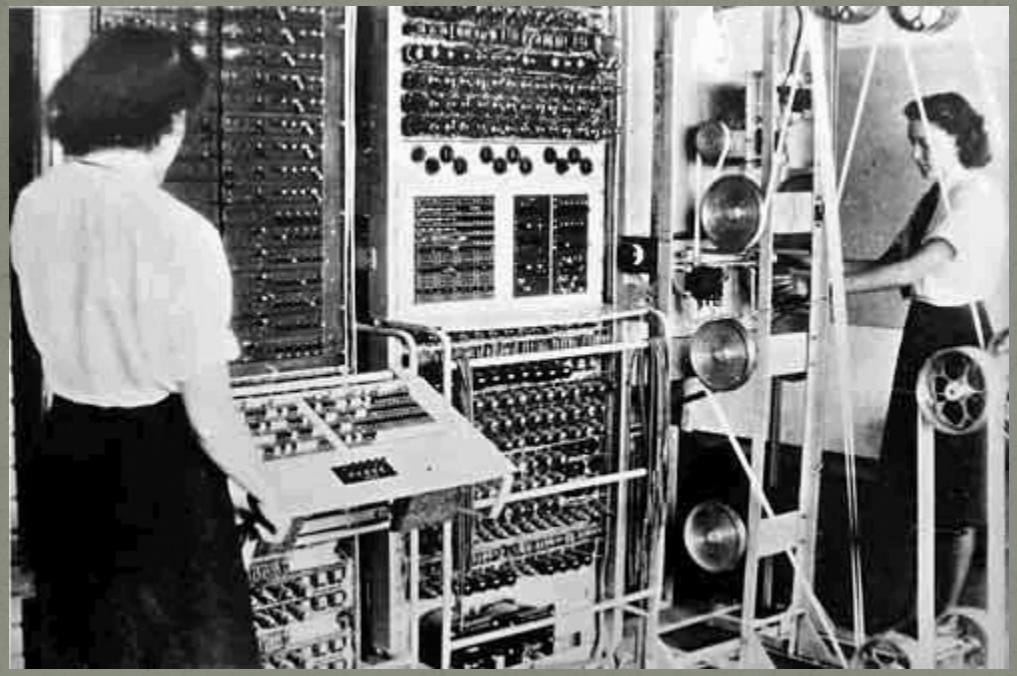
Joseph Wenger

ERA

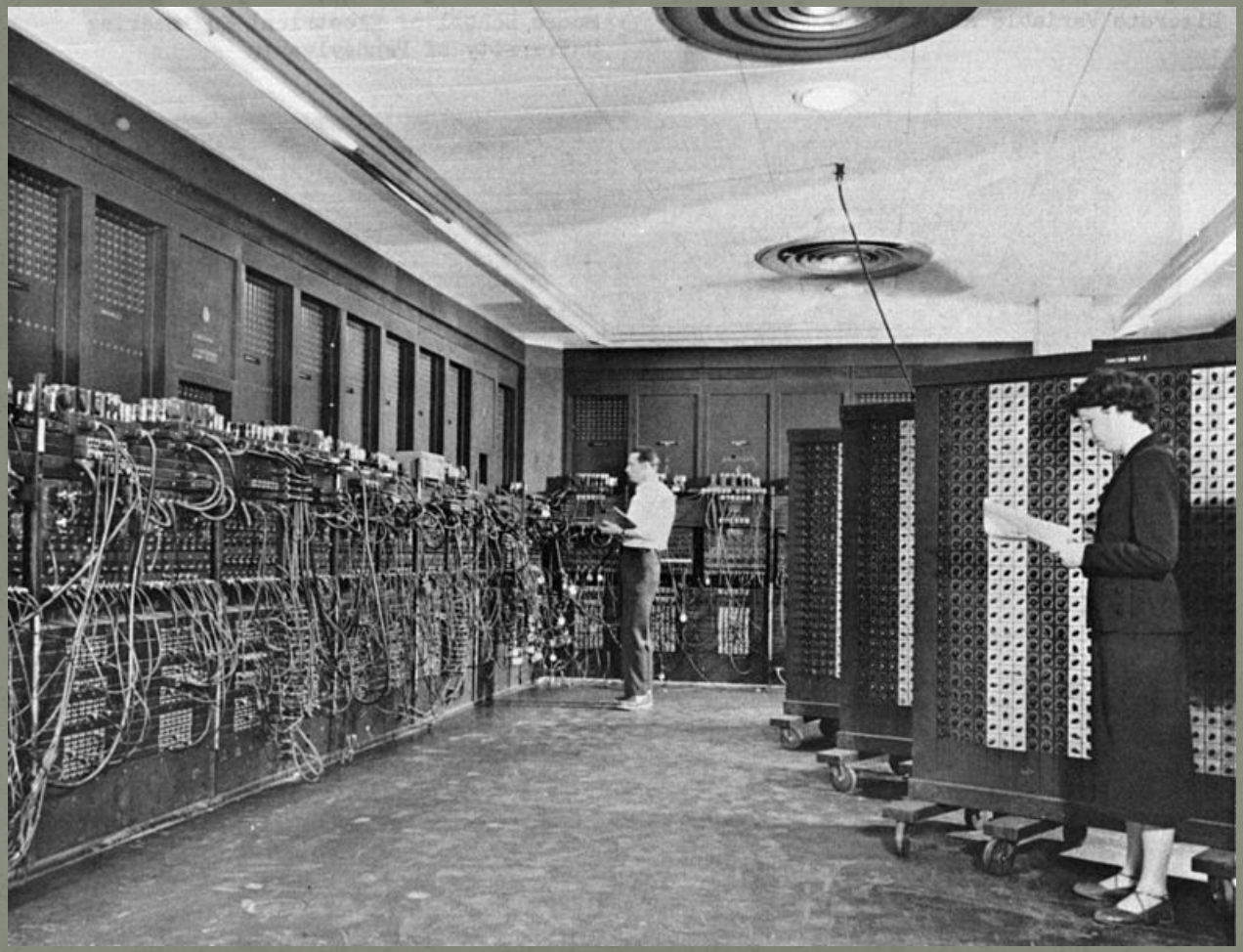
- Howard Engstrom
- William Norris
- John Parker

“Task 13” ERA 1101

A Similar Point of View: Colossus



An Alternative Point of View: ENIAC



Thanks