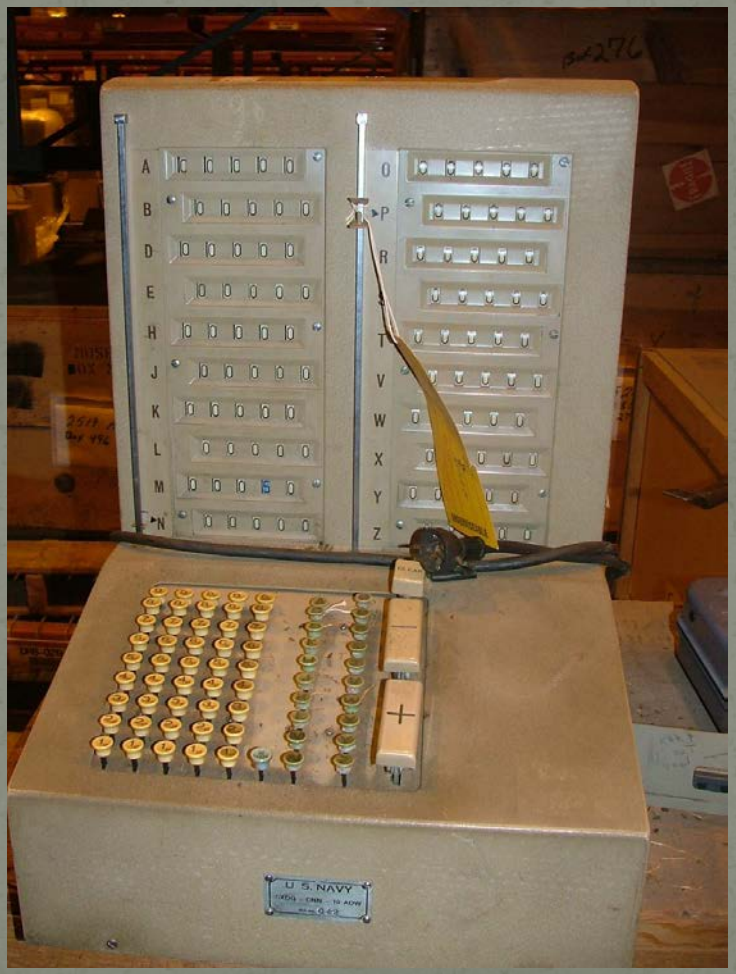
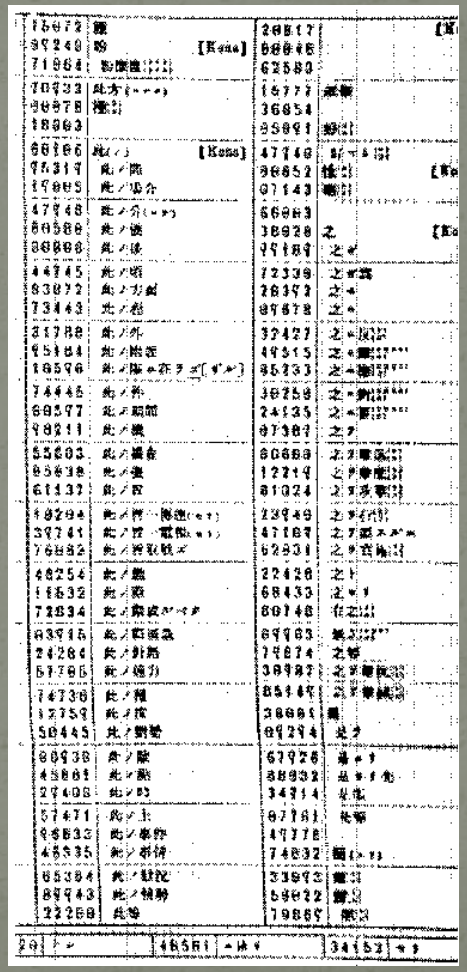
Fruit

Chris Christensen
Northern Kentucky University

CXDG-CNN-10-ADW "Fruit"



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

Tables 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

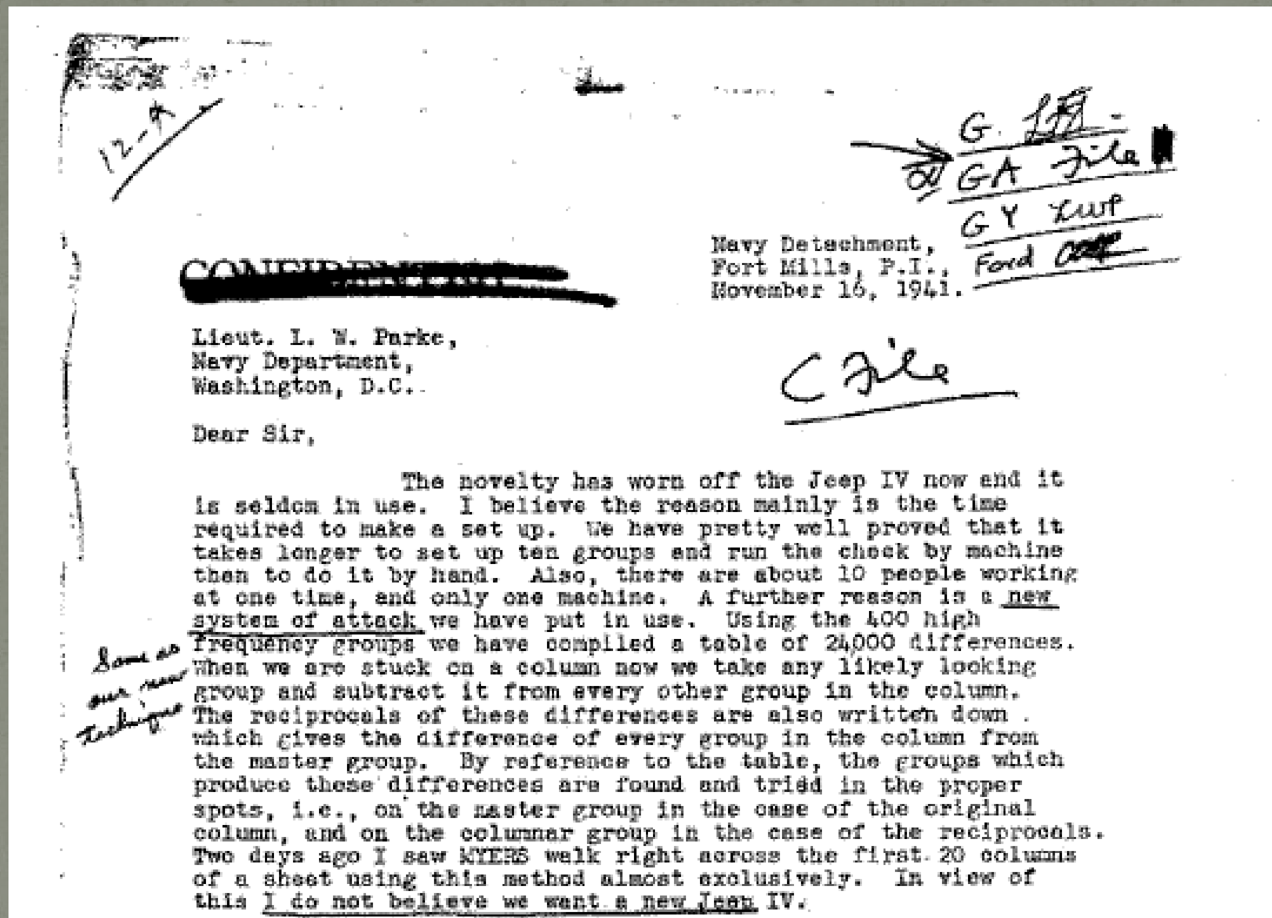
Differencing

(Codegroup 1 + Additive)

(Codegroup 2 + Additive)

Codegroup 1 – Codegroup 2

Differencing



Navy Detachment,
Fort Mills, P.I.,
November 16, 1941.

GA File

C File

[redacted]

Lieut. L. W. Parke,
Navy Department,
Washington, D.C.

Dear Sir,

The novelty has worn off the Jeep IV now and it is seldom in use. I believe the reason mainly is the time required to make a set up. We have pretty well proved that it takes longer to set up ten groups and run the check by machine than to do it by hand. Also, there are about 10 people working at one time, and only one machine. A further reason is a new system of attack we have put in use. Using the 400 high frequency groups we have compiled a table of 24000 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, i.e., on the master group in the case of the original column, and on the columnar group in the case of the reciprocals. Two days ago I saw MYERS walk right across the first 20 columns of a sheet using this method almost exclusively. In view of this I do not believe we want a new Jeep IV.

Same as our new technique

Scanning

67854 59199 76833 57699 10047 70863 06138 27924

Differencing and Scanning

38898	00000			
42742	14954	00000		
92166	64378	50424	00000	
18443	80655	76701	**26387**	00000
24236	96448	82594	32170	16893

18443 – 92166 = 26387

50418 – 34131 = 26387

18443	92166
50418	34131
68035	68035 additive

38898 – 68035 = 70863

42742 – 68035 = 84717

92166 – 68035 = 34131

18443 – 68035 = 50418

24236 – 68035 = 66201

Distribution

None Scan	.132
One Scans	.329
Two Scan	.329
Three Scan	.165
Four Scan	.041
Five Scan	.004

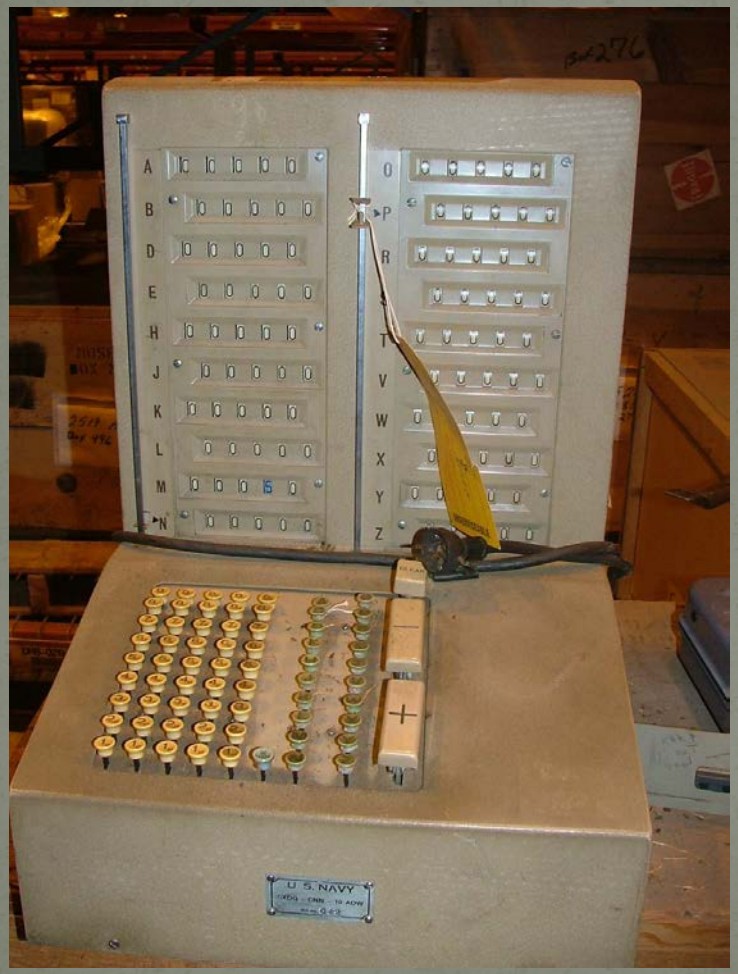
Dayton, OH 21 December 1942

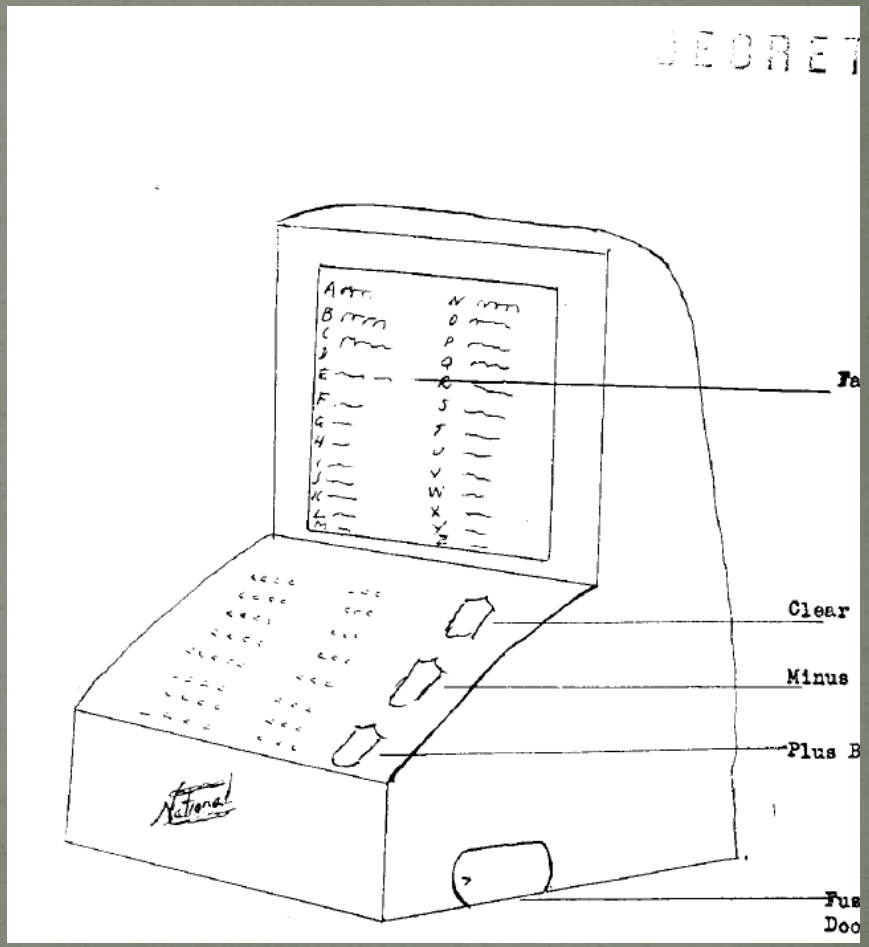
… we also saw a machine for aiding one in the recovery of subtractor groups when messages have been set in depth.

A rather similar machine was made by Letchworth for us in early 1940, and although not nearly so convenient as this model, has been used quite a bit I believe.

Alan Turing

CXDG-CNN-10-ADW "Fruit"





Keyboard

Fruit

Display

Colors

0	White	5	Blue
1	Red	6	White
2	Blue	7	Red
3	White	8	Blue
4	Red	9	White

Scanning Combinations

All White

1 Red and 1 Blue

2 Red and 2 Blue

3 Blue

3 Red

1 Red and 4 Blue

1 Blue and 4 Red

Fruit Attack

1	2	3	4
22435		37354	69235
06009	43713	53115	28362
28434		80469	87597
KANA NI		M/S	Begin A/T
92851	74751	15300	45433
14286		42654	04668
ROMAN N		ROMAN R	ROMAN K
45085	89854	17704	88702
67410		44058	47937
HATSU		xUnit Commander	XSHINSHOO
70518	78330	70723	18934
92943		07077	77169
REPEAT A		NUM. SEP.	#30
82206	98366	18114	83221
04631		45468	42456
		BEI KOME	KANA NO
28808	56055	24364	78863
40233		51618	37198
GAI SOTO			SHIN NOBU

Depth

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

Zeroize 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

Differencing

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

B – A = 31048

D – A = 46141

E – A = 35637

H – A = 55653 = 55457

J – A = 13342

Differencing

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

B – A = 31048

From the difference table

A = 26349

If A = 26349

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

A	26349	O	83636
B	57387	P	83636
D	62480	R	83636
E	51966	S	83636
H	71992	T	83636
J	39681	V	83636
K	83636	W	83636
L	83636	X	83636
M	83636	Y	83636
N	83636	Z	83636

Distribution

None scan	0.088
One scans	0.263
Two scan	0.329
Three scan	0.219
Four scan	0.082
Five scan	0.016
Six scan	0.001

Horizontal Alignment

1	2	3	4
22435		37354	69235
06009	43713	53115	28362
28434		80469	87597
KANA NI		M/S	Begin A/T
92851	74751	15300	45433
14286		42654	04668
ROMAN N		ROMAN R	ROMAN K
45085	89854	17704	88702
67410		44058	47937
HATSU		xUnit Commander	XSHINSHOO
70518	78330	70723	18934
92943		07077	77169
REPEAT A		NUM. SEP.	#30
82206	98366	18114	83221
04631		45468	42456
		BEI KOME	KANA NO
28808	56055	24364	78863
40233		51618	37198
GAI SOTO			SHIN NOBU

Differencing

B – A = 26349

D – A = 46141

E – A = 35627

H – A = 55653 = 55457

J – A = 13342

A = 26349

A = 57147

A = 70104

A = 39336, 64827

Zeroize B

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

Differencing

D – B = 15103 B = 89172

Differencing

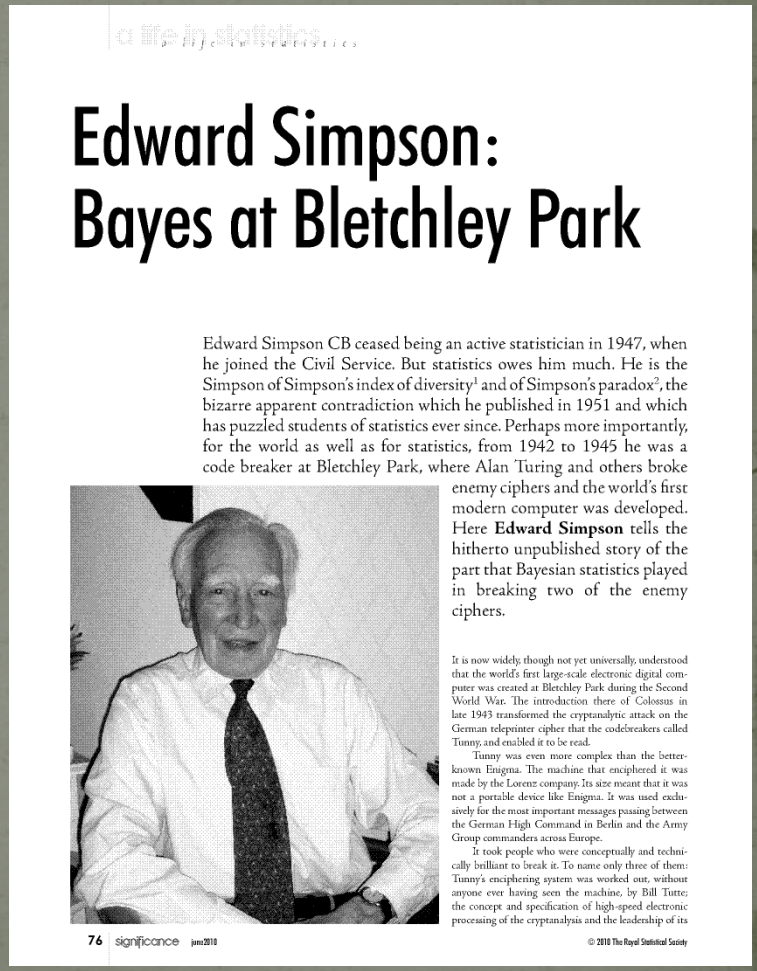
A	58134	O	15421
B	89172	P	15421
D	94275	R	15421
E	83751	S	15421
H	03787	T	15421
J	61476	V	15421
K	15421	W	15421
L	15421	X	15421
M	15421	Y	15421
N	15421	Z	15421

Results

58143	Scans
89172	Scans
94275	Scans
83751	Scans
03787	Garble
61476	Scans

Edward Simpson

… Washington sent us a dozen or so calculating machines made by the National Cash Register Company. We called them the "fruit machines" … .
They proved prone to mechanical failure … eventually we gave up on them altogether.



a life in statistics

Edward Simpson: Bayes at Bletchley Park

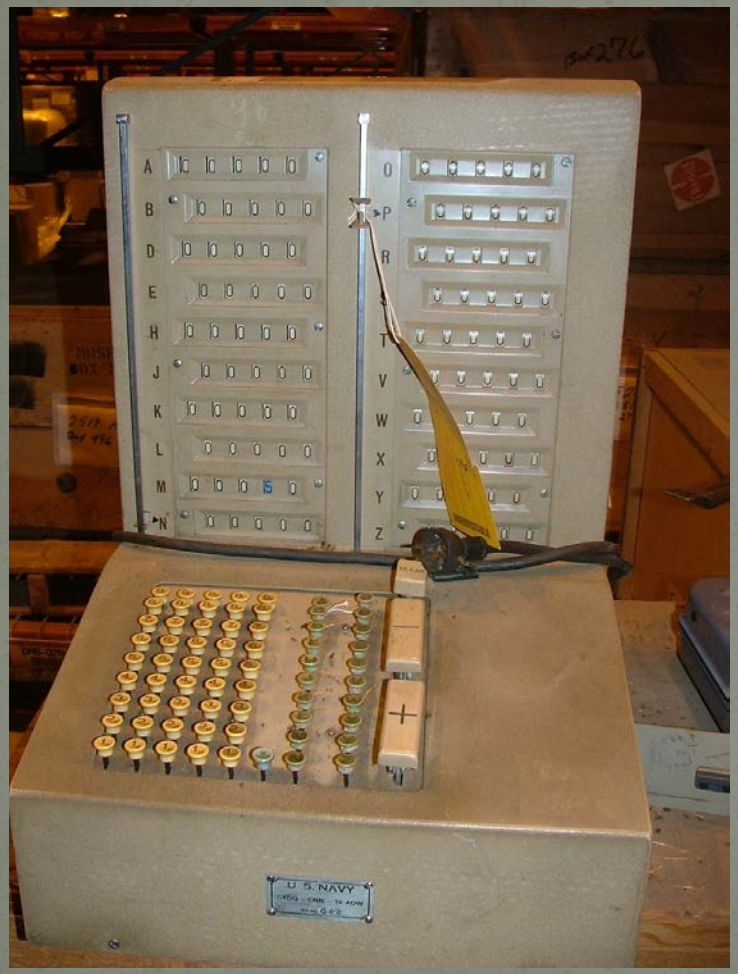
Edward Simpson CB ceased being an active statistician in 1947, when he joined the Civil Service. But statistics owes him much. He is the Simpson of Simpson's index of diversity[1] and of Simpson's paradox[2], the bizarre apparent contradiction which he published in 1951 and which has puzzled students 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

Fruit


U.S. NAVY

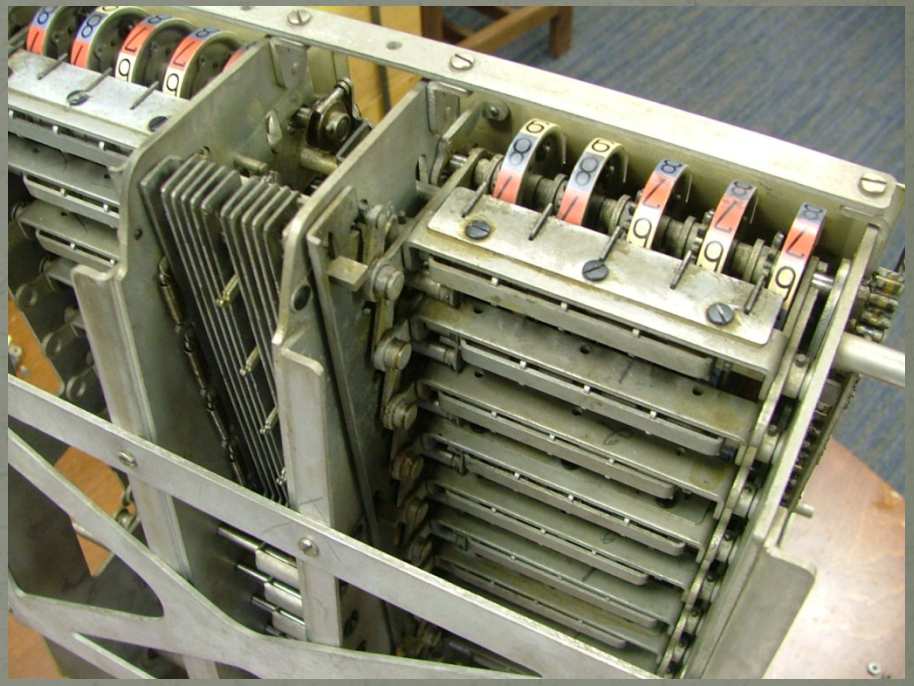

super
SLOTS
CREDITS
BET
WINNER PAID
25¢
RESET
PAY TABLE
SPIN

Fruit

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 1941. [T]hey were based on 1920s electric machine technology and they could only add and subtract.

Colin Burke

Fruit



Howard Campaigne

… it immediately occurred to a lot of people "here's a way to mechanize," and we went to National Cash Register Company, and they even built a special device for this … .

[These machines] were not too successful.

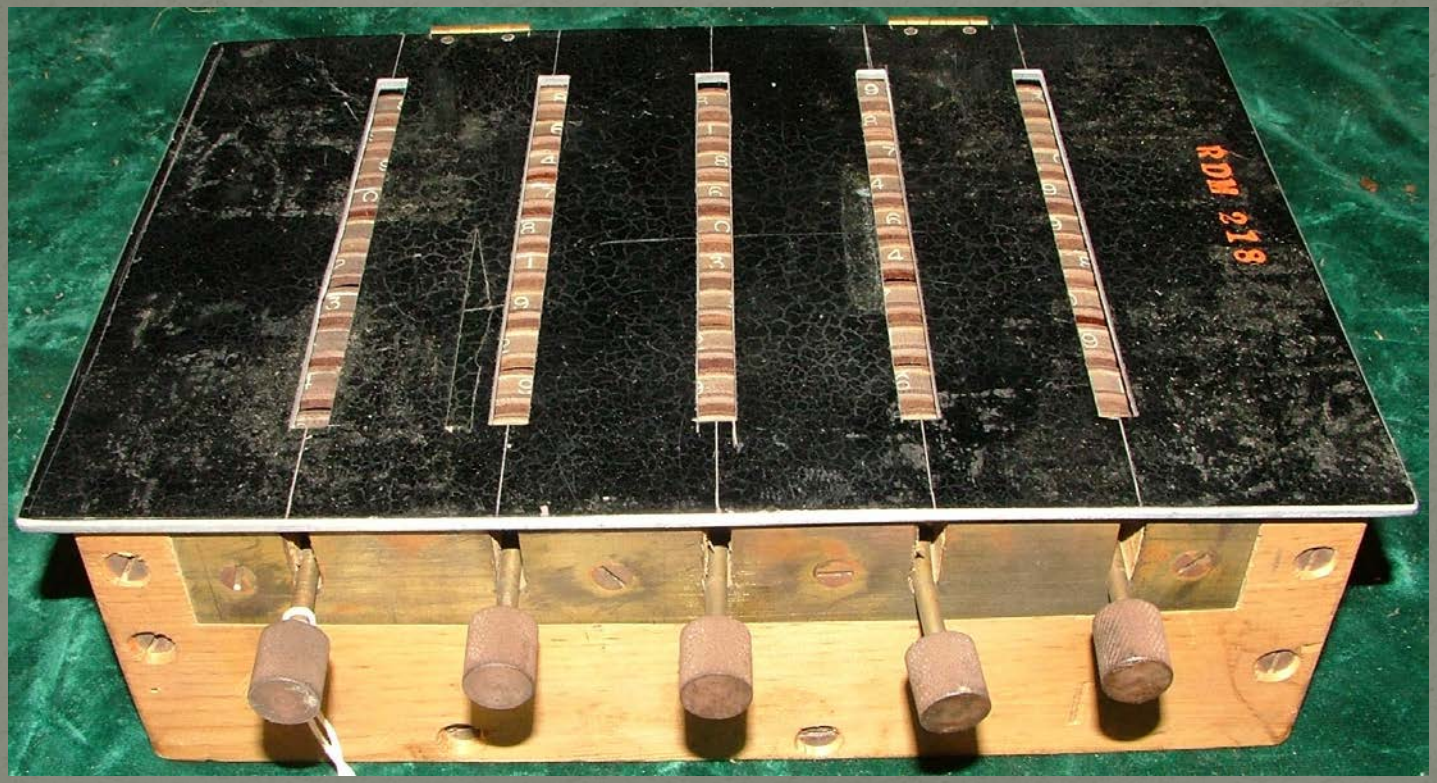
Differencing Machine Evolution

- Parke Machine 1941.
- Shinn Machine (Mathew?) 1942.
- NCR Machine 1943.

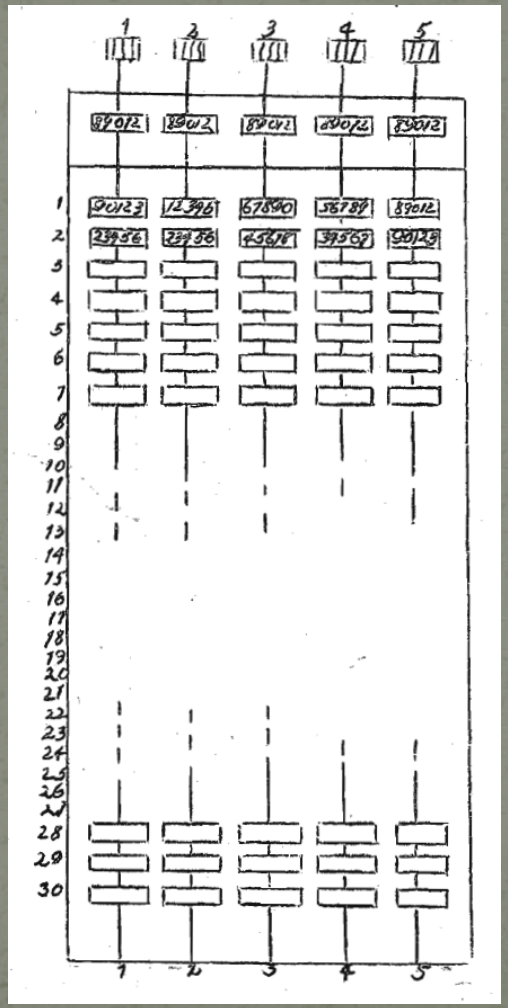
"To 20Q Park's Jeep Model 3-16-42"

Differencing Machine 1943

Differencing Machine



German Differencing Calculator



Joseph Desch (1907 – 1987)

2011 Inductee

HALL OF HONOR
These Were the Giants

JOSEPH DESCH

Thanks.