Home Waters Enigma

by

Unknown Author

8 June 1943

Abstract

An account of the procedure followed in Hut 8, in dealing with the Home Waters enigma ("Dolphin"). This is a member of the Kennbuch family. The procedure is to recover the Grundstellung alphabets by putting messages in depth. This is done partly by an I.B.M, search for repeated tetragraphs, and partly by a straight I.C. count (done on "Banbury sheets") on messages known by their indicators to start within 26 of each other. See also Article 8, Volume 2.

Source: NARA, College Park, Md., Record Group 38, Crane Collection, Box 172, RIP 610, ARC Identifier: 6921399, HMS/MLR Entry Number: A1 1025
https://catalog.archives.gov/id/6921399
Enigma Series Volume 8, Article 2

Editor: Frode Weierud, Crypto Cellar Research
Web Site: www.cryptocellar.org

Version: 29 May 2022

HOME WATERS ENIGMA

This traffic, called Heimisch (or more recently Hydra) by the Germans, and Dolphin by the British, is on the 3-wheel naval enigma, and is a member of the K-book family. It is used by surface ships in the North Sea and Baltic, and by Arctic subs. The traffic has increased to over 500 messages a day. The Offizier, called Oyster by the British, has keys exactly similar to Limpet.

A diagram of the procedure followed in breaking a new day is given on page 2 below. The banburism begins as soon as the messages start coming in from the registration room, and continues well into the next day. Freeborn does not start sorting and tabulating until the day's traffic is all in, and his catalog starts coming in about 1700 of the next day. The two Grundstellung alphabets are usually complete before 2400, and the menu is sent to the bombes shortly thereafter. The correct stop is usually found by 0400, and the rest is a matter of a few minutes. A menu for the paired day has usually been prepared by that time, and is out by say 0600, leaving six current hours on the paired day. A more detailed description follows, of the determination of the Grundstellung alphabets and the middle and end wheels, the material being drawn from the day May 28.

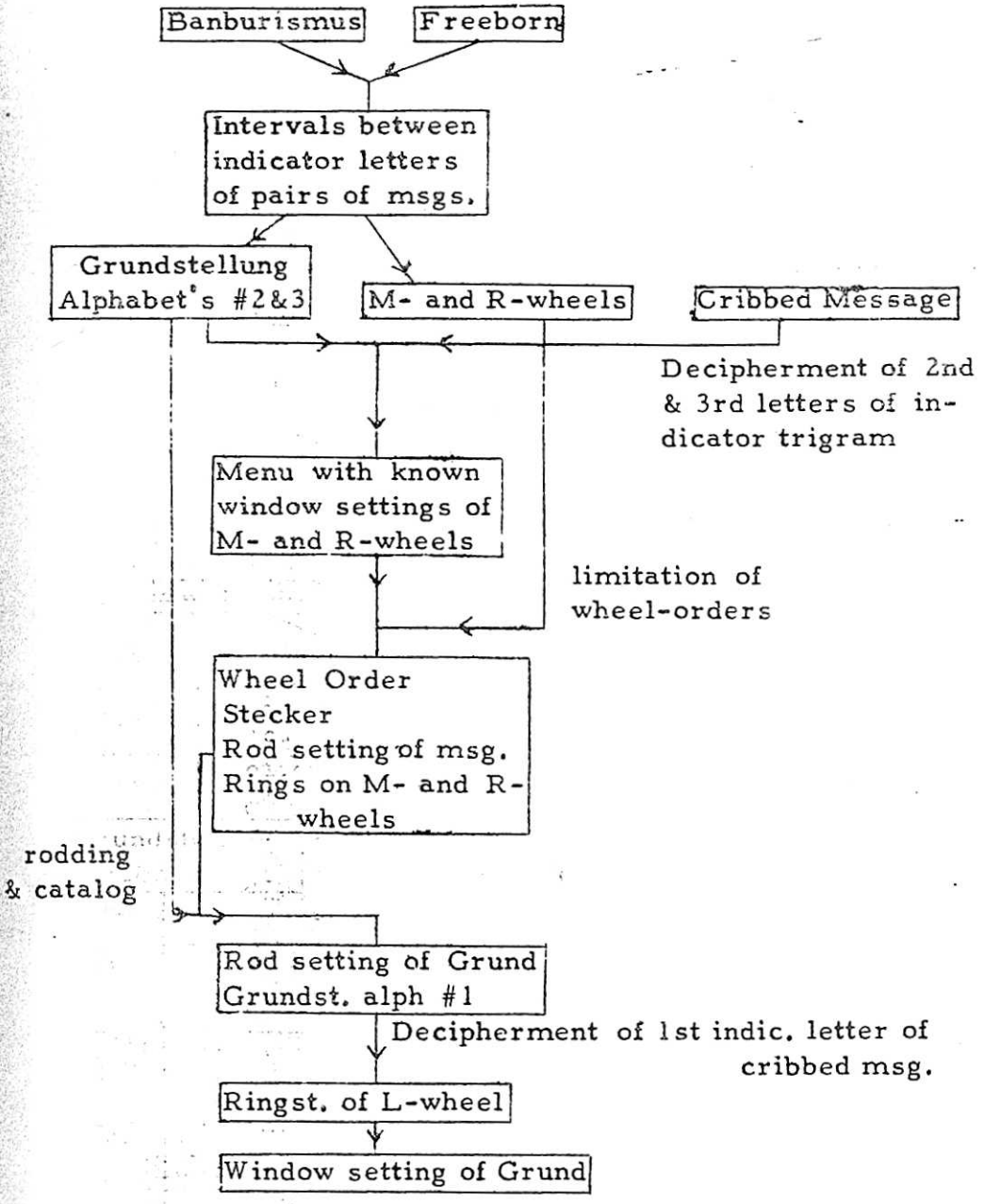
The Dolphin messages are first separated out by K-booking, and registration numbers assigned. The dummyismus percentage for each message is recorded on it, and the Roms Category (see below page 4) in which it falls. Each message is entered on the Foss sheet, and a Banbury sheet is punched up, with the dummy percentage and Roms Category recorded thereon, as well as the enciphered indicator trigram (after bigramming, of course). A blue line is drawn on the Banbury sheet to indicate virtually certain plain text to the left thereof, as dummy messages always begin with plain (even if non-sensical) text for 30 to 60 letters before launching into a string of consonants.

All pairs of messages having their first two indicator letters the same are compared at all positions from -25 to +25. The counts are entered on one of 26 score sheets, namely the one lettered by the earlier of the third trigram letter. Thus the match WEE/WEP is entered on the E-sheet (Exhibit 1). WEE is 132 letters long, with the blue line drawn at 60, and a dummy percentage 65%. WEP has dummy percentage 5%, and (this being so low) has no blue line; its length is 104.

WEE ← - - 60 - → / ← - - - - - - 132 - - - - - - →

WEP ← - - - - 104 - - - - - →

DIAGRAM OF DOLPHIN PROCEDURE



The upper line (opposite the letters WEE) gives the score at each position as WEP is moved to the right, the overlap decreasing from 59 to 35. The lower line (opposite WEP) gives the score at each position as WEE is moved to the right, the overlap remaining 60. The score is simply the number of coincidences, with a little x indicating a bigram. Thus in the position WEE = WEP + 8 there are 7 coincidences including a bigram, while at WEP = WEE + 24 there are no coincidences. If the dummy percentages are not too bad, scores are made beyond the blue line as well. For example, for RPO = RPE + 16, there are 2 coincidences in an overlap of 45 up to the blue line (on RPO), and 3 in the remaining 51 overlap.

The banbury counts are evaluated from one of three double-entry tables. In the row given by the number of coincidences and the column given by the overlap is found the value (expressed in half decibans) which is entered on the deciban sheet (Exhibit 2). In Table 1 this value is 20 times the log of the ratio of the a posteriori to the apriori odds that the line-up is correct. The values in Table 2 are reduced to allow of a small probability that one or both of the messages be dummy. Those in Table 3 are still further reduced to allow of a large such probability. Before entering the table, to the number of coincidences is added 1 for a bigram, 2 for a trigram, and 4 for a tetragram.

If scores are made only up to the blue line, Table 1 is used. If two scores are made, Table 1 is used for the overlap before the blue line and Table 3 for the overlap after it. If the dummy percentages are small on both messages, the blue line (if any) is ignored and the scores evaluated from Table 2. The table or tables to be used, namely 1, 2, or 1/3, are found entered on Exhibit 1. The values are also found entered there in comparisons of type 1/3, and these are added for entry on deciban sheet.

One sheet is made for each third indicator letter, and each pair is entered twice. Thus WEE/WEP is entered on both the E-sheet (Exhibit 2) and the P-sheet. On the E-sheet, the letter E is written down the center (0-column). In the x-column is entered the value of the score at which WEP = WEE + x (positive to the right, negative to the left). Thus the value contributed by this match to a spatial assumption E. . . . P (x = 5) or P. . . . . E (x = 7) is found by putting E under E and reading off the value above P. The values of the same match on the P-sheet are just the reversal of these, since + and - distance is reversed. Red scores are positive, black negative. Underlining means a trigram. A note is made of especially good line-ups, e,g. those with a repeated tetragram.

As the traffic comes in, a copy of each message is sent to Freeborn, who punches up a card for each trigram, with registration number, indicator trigram, the two preceding and six following letters of the text, and the location in the message of the first letter of the trigram (101 means initial letter, 201 means 27th letter, 318 means letter in position 2 x 26 + 18 = 70). 500 messages of average length 150 means about 75,000 such cards! These are sorted (perhaps manually, as punched up) into 26 "folders" according to the first letter of the indicator trigram.

When all the traffic is in, Freeborn sorts his cards and tabulates the repeated trigrams. His tabulation is called the "catalog" (Exhibit 3 is a page from the E-folder). It comes in folder by folder, and as they come in they are scanned visually for tetragrams. These are entered on the "tetra squares"(Exhibits 4A and 4B), one for the end-wheel and one for the middle. Thus in Exhibit 3, the repeated tetra LUIZ occurs in position 6.05 of EUC and in position 2.14 of EZV. Hence EUC is the earlier of the two by the amount 6.05 - 2.14 = 3.17, or

$$EZV = EUC + 3.17$$

This means (if correct!) that V = C + 17 in the end-wheel alphabet, and Z = U + 3 or 4 in the middle-wheel alphabet. In the E.W. (end wheel) tetra square, V is entered in line C column 17, and C in line V column 26 - 17 = 9. The subscript E is attached for reference purposes. Similarly on the M.W. Square, Z is entered in the U-row and 4-column (the larger of the two alternatives); only one entry is made on the M.W. Square.

The matches with repeated tetras are also entered on a large tetra sheet (Exhibit 5) for convenience in recording their values computed by a method called ROMS ("Resources of Modern Science".) Each message is classified into one of 18 categories, designated by a Roman numeral, to be used in step (1) in the following description of the Roms table and its use. The values throughout, added or subtracted successively, are all in half decibans.

(1) The tetra in each of the two messages is evaluated according to its position in the message, and the category of the message. For categories V, VI, and XVI the values for the various positions are:

POSITION		V	VI	XVI
	1	24	34	30
(always -00)	2	-00	-00	-00
	3	14	8	4
	4	17	20	17
	5	12	28	4
	6	9	31	11
	7	16	27	17
	8	17	20	16
	9	13	33	11
	10-30	20	23	14
(middle)	β	22	23	19
(end)	γ	19	20	12

The two values are added, and a correction is applied:

-00 to 1	31
0 to 18	32
19 to 22	33
23 to 26	34
27 to 30	35
31	36
32 to 34	37
Very slight beyond here	

(2) A triangular table is entered according to dummy percentages, and the result subtracted.

%			
5	1		
15	2	3	
25	3	4	.
35	4	5	.
45	6	.	.
55	7	.	.
65	10	.	
75	12		
85	17		
95	26		
	5	15	25 - - - %

(3) Subtract a slight amount for middle wheel distance, roughly 2 half decibans per multiple of 26 (e.g. 10 if distance is between 4.20 and 5.6). Not used for comparisons "at 26", i.e. with middle letter the same. ("Comparisons at 676" are those with only the first trigram letter the same.)

(4) To the number of repeats in addition to the tetra, add 1 for a bigram and 6 for a trigram. Table gives approximately 3 half decibans per coincidence (so modified), to be added, of course.

(5) Subtract for length of overlap; table gives approximately 15 for each 100 letters of overlap to be subtracted.

Examples:

(a) UUW = UUB + 0.14 Score: 7(4)/94

(b) MWC = MWF + 0.5 Score: 11(5)/99

Message	Category	Length	D Dummy Percentage	Position Of Tetra
UUW	XVI	96	35	27 (10-30)
UUB	V	108	5	41 (β)
MWC	VI	236	5	47 (β)
MWF	V	104	65	52 (β)

Both of these matches being at 26, step (3) is omitted.

Step	Example (a)		Example (b)	
(1)	UUW XVI 10-30:	14	MWC VI β :	23
	UUB V β	22	MWF V β :	22
		36		45
	Correction 36. . . .	38	Correction	(none)
(2)	5% - 35%	-4	5% - 65%	-10
		34		35
(4)	3 add'l repeats . .	9	13* add'l repeats ..	37
		43		72
(5)	Overlap 94:	-14	Overlap 99:	-15
	FINAL SCORE. . . .	29	FINAL SCORE. . . .	57

Now 20 log 26 = 27 approximately, so that 27 should be subtracted from these (division by the a priori probability of 1/26), in order to find odds (in half decibans) that line-up is correct. Thus example (a) has slightly better than an even chance of being right, while (b) has odds of about 30 to 1 of being right.

Below are listed the outstanding matches found for the day's traffic. A heptographic repeat or better is virtually certain to be right, though some allowance must always be made for a garbled indicator letter. A hexagraphic repeat would be very good at 676, and since the one found is at 26 we can likewise put it in the virtually certain class. The one pentagraphic repeat at 26 has the remarkable score of $17^{(5)xx}/111$, that is, two bigrams and 8 single letters repeated in addition to the pentagraph. Of the four tetras at 26, the second and fourth are at least 30 to 1 shots by their Roms scores (57 and 65). Including the cribbed pair, we thus get the following virtually certain equations on the EW alphabet:

T = J + 9
O = P + 1
U = E + 9
F = P + 15
X = A + 16
Q = C + 9
C = F + 5
I = V + 4
X = K + 8

No turnover between these intervals since comparisons are at 26.

* 6 for trigram plus 7 singles)

The EW alphabet may be determined by these, except for six missing letters, by scritching (Exhibit 7A). However, for the purpose of showing how two competing alphabets may be "counted" on the deciban sheets, we shall pretend that the PNI/PNV match did not exist; without it, another likely alphabet may be found. Of course in practice one begins scritching long before the list is complete, and moreover this day's traffic was unusually rich in repeats. Usually it is necessary to use the less likely matches. With less traffic (used to be about 300 a day) or a double-notch end wheel, it is much more difficult.

LIST OF OUTSTANDING MATCHES FOUND IN DOLPHIN 28 MAY

12 - gram: IQT = IOJ + 1.9

9 - gram: HZO = HTP + 1.1

Heptagrams: RIU = RPE + 1. 9
ZGF = ZOP + 3. 15

Hexagram: JAX = JAA + 0.16 (at 26)

Pentagrams:		Banburismus Score
1.	MGQ = MGC + 0. 9 (at 26)	$17^{xx}/111$
2.	ALO = AVJ + 4. 4	6/60
3.	BXL = BBE + 1. 25	$14^{x}/124$
4.	BYM = BBE + 0. 20	8/176
5.	DDN = DJE + 2. 1	8/72
6.	HPK = HRW + 1. 23	7/43
7.	IVS = IZZ + 2. 10	8/62
8.	KKY = KDD + 2. 11	6/69
9.	LVO = LRM + 12.6	$10^{x}/136$
10.	MEY = MWC + 4. 8	$10^{x}/129$
11.	OOK = OSH + 1. 5	12/184
12.	ORT = ONP + 0. 1	not made
13.	VSS = VKU + 2. 9	not made
14.	MIR = MIN + 7. 3	impossible
15.	EAC = EAJ + 5. 12	impossible

Tetragrams at 26:	Banburismus Score	Roms Score
1. UUW = UUB + 0. 14	$\frac{5^{④}}{45} \cdot \frac{2}{49}$	29

2. MWC = MWF + 0. 5	$\frac{1}{35} \cdot \frac{10}{64}$	57
3. LSH = LSM + 0. 2	$\frac{8}{82}$	not made
4. PNI = PNV + 0. 4	$\frac{24}{231}$	65

Two Tetragrams at 676*:

IAN = ICB + 1. 14	$\frac{13}{200}$	48

Two Trigrams at 26:

LRR = LRM + 0. 19	$\frac{15}{200}$	46

Cribbed:

KAX = KAK + 0. 8	$\frac{16}{176}$	not made

(That is, one of these was cribbed by a re-encodement, and by repetitions and reciprocals, enough letters were found in the other - at the distance 8 - to fill it in completely with plain text consisting largely of numerals.)

In Exhibit 6A the intervals given by these equations (with I = V + 4 omitted) are given spacially, and the scritch sheet (Exhibit 7A) is laid out by sliding the first of these along the alphabet, and recording those not conflicting with reciprocity or the requirement that no letter be enciphered by itself. The possible turnovers are marked in vertical red lines (none coming between F and Q). Eleven possible skeleton alphabets are thus found, reciprocal values being entered. Five of these are eliminated by the A - K - X relation, #10 on the sole grounds that no possible turnover is left. Two more are eliminated by the E - U interval, and one by J - T, leaving three: #1, 2, and 6.

In #6 there are only two places where the A-K-X sequence may be entered, A under V and A under W. The latter puts K under E, hence E under K, hence U under T (by E - U), hence T under U, when we find J conflicting with X under L (by J - T). Hence only A under W is possible,

* Granting this one, the following tetra at 676 becomes virtually one at 26:

IAJ = ICB + 1. 24	$\frac{15}{180}$	16 (at 676) 43 (at 26)

and these are entered in red. But this eliminates all possible turnovers except N/O, and since this is only for wheel VI which also has a turn Z/A, it is also impossible. Hence only #1 and #3 remain.

In #1, A - K - X can be entered in two places, and these are rewritten in lines 16 and 17. Line 16 goes out from E - O. In line 17, turnover Z/A is knocked out, leaving only wheel 3 as possible; E - O and J - T are drawn in without contradiction. All conditions are satisfied though 8 letters are missing. This we call alphabet I.

In #2, A - K - X can be entered in only one place, and this is rewritten in line 21. Only the turnover E/F remains, i.e. wheel 2. J - T can now be entered in one way only, and all conditions are satisfied. This we call alphabet II. It is seen to violate the condition I = V + 4 which we ignored.

In line 16 we have added the I = V + 4 in black to show the extent of completion with the virtually certain intervals. The very good penta #3 (L = E + 25) and the two trigrams at Z6 (R = M + 19) are already satisfied. The relatively poor tetra #1 (W = B + 14) is impossible. The somewhat better tetra #3 (H = M + 2) is possible. The LAM/ICB/IAJ combination can be reinforced by placing E and N as indicated in red. If we don't care to rely on H = M + 2 to finish the alphabet we can "count" the three alternatives on the G, H, S, and Z deciban sheets. The result is given in Exhibit 8 (on the Z-sheet for checking purposes). Thus one places the Z in the alphabet in question under the center Z, and records the deciban value over the letter matched (here U, V, R, etc.). Plus values are encircled; others are negative. Thus the scores + 30 for Z over G, + 6 for Z over H, and - 80 for Z over S point conclusively to Z over H, and this confirms H = M + 2.

The completed alphabet is written in line 25, and in line 24 we have put a completed version of alphabet II with the following comparative results:

	I	II
12 - gram	yes	yes
9 - gram	yes	yes
7 - gram	both yes	both yes
6 - gram	yes	yes
Pentagram at 26	yes	yes
Pentagram at 676	2 yes' (#7, 3, 11)	2 yes' (#4,6)
	9 no	10 no
Tetragram at 26	3 yes (#2, 3, 4)	1 yes (#2)
	1 no (#1)	3 no (#1,3,4)
Two tetras at 676	yes	yes
Tetra at "virtually 26"	yes	no
Two trigrams at 26	yes	no
Cribbed pair	yes	yes

Recalling that we agreed to ignore one of the tetras at 26 (#4), we might not regard I as conclusively better than II. To make it conclusive, the two were counted (on all 26 deciban sheets), the results - with duplications omitted - being entered in Exhibit 9. The method is the same as for Exhibit 8. The results of + 146 for I and - 370 for II show (by converting from half-decibans back to odds) that I has relative odds of 10^{7} for and II has relative odds 10^{18} against. These must be divided by the a priori odds (pretty colossal) of any random alphabet being correct, but at least it shows that I is 10^{25} times more probably than II.

We have thus found the end-wheel alphabet, and the fact that the end-wheel is 3. Proceeding now to the middle wheel, we first list the outstanding matches at 676 [illegible] in agreement with the end-wheel alphabet, with the implied equation (turnover known!).

12-gram	IQT = IOJ + 1.9	Q = O + 1
9-gram	HZO = HTP+1.1	Z = T + 1
Heptas	RIU = RPE +1.9	I = P + 1
	ZGF = ZOP +3.15	G = O +4
Pentas	ALO = AVJ + 4.4	L = V +4
	BXL = BBE + 1.25	X = B + 2
	OGK = OSU + 1.5	O = S + 1
Two tetras	IAN = ICB + 1.14	A = C + 2

From the EW Tetra Square we can quickly locate all tetras in agreement with the EW alphabet. These being "virtually at 26", they stand a very good chance of being correct, but may now be ROMSed if necessary to determine their relative values. We find the following:

1.	DRW = DIE + 0. 16	R = I + 1
2.	DQM = DIE + 0. 13	Q = I + 1
3.	ERN = EUC + 4. 19	R = U + 5
4.	JIF = JKJ + 1. 18	I = K + 2
5.	LMJ = LRM + 1. 14	M = R + 1
6.	JMG = JBO + 3. 3	M = B + 3
7.	NEF = NJO + 4. 14	E = P + 2
8.	LRR = LPY + 1. 21	R = P + 2

The first two are incompatible, but #2 violates the virtually certain Q = 0 + 1, and hence we may discard it. #1 and #8 together give the pattern PIR, confirming the virtually certain I + P + 1, and hence we adopt them. The virtually certain intervals and this additonal R are entered on Exhibit 6B. We use the pattern SOQ. . G to start the scritch sheet. Observe that no turnovers are allowed between any of the recorded intervals (assuming their correctness). When the further certain patterns are applied, 12 of the 14 possibilities are immediately eliminated, leaving line 2 (alphabet I) and line 7 (alphabet II).

PIR fits into I in six places (11-15-20), but all go out except ℓ. 15. But here TZ will fit in only two places, both violating B-X. Consequently, II is correct but incomplete. TZ, SX, and CA are still to be applied. Rather than eliminate step by step we may hazard some of the tetra intervals. #1 and #8 have been used, and #2 thrown out. #4 and #5 have been confirmed and #6 denied. There remain #3 (R = U + 5) and #7 (E = J + 5). These are added in ℓ.21, drawing in TZ. B - X may be added in two ways (11 22 and 24), and C - A in two ways to each of these. Thus four alphabets are possible, with wheel possibilities reduced to 2 or 5. It may be completed by burrowing into less likely matches. The ones used were

OUL = ONP + 0.21		U = N + 1
OLP = OSH + 4.15		L = S + 4
VSS = VRR + 1.16		S = R + 2
VZO = VAX + 2.3		Z = A + 2
VPG = VKU + 5.25		P = K + 6
TFH = TVJ + 0.14		F = V + 1
WAK = WEP + 2.16		A = E + 3
EEO = EXP + 1.1		E = X + 1
HYU = HGU + 2.0		Y = G + 2

Unfortunately, the scores were not recorded.

The two alphabets could be used to make up a menu for the bombe. But

in order to avoid frequent "boxing stops", a double input on the main chain is used, and this causes electrical difficulties.

//s// A. H. Clifford,
Lt. USNR
Station X, England

June 8, 1943

EXTRACT FROM BANBURY SCORE SHEET (LETTER E)

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	
	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	
WEE	3	1	2	1	1	2	1	2	2	3	2	2	0	3	2	0	1	0	2	2	2	1	1	0	2	60/132 65%
	59	58	57	56	55	54	53	52	51	50	49	48	47	46	45	44	43	42	41	40	39	38	37	36	35	
	0	3	2	1	8X	3	1	7X	3	2	2	0	2	0	1	0	3X	2	2	0	1	1	0	3	2	104 5%
WEP	60					60					60					60					60					

E - 8 - 31

EXHIBIT 2

EXTRACT FROM DECIBAN SHEET

(Encircled values are positive. The rest are negative)

	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	1	2	
FW F	1	4	1	(2)	4	1	(8)	2	(4)	(1)	2	2	(1)	3	5	0	6	(3)	3	6	1	(5)	(2)	1	4	E	4	2 - -
WE P	4	1	11	7	7	11	4	4	(3)	11	7	11	4	11	4	4	1	(16)	7	1	(3)	7	4	1	11	E	-	7 - -

	2	1	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	
FW P	- -	1	4	E	4	2	7	4	4	2	2	4	2	(4)	(1)	2	2	(1)	4	(1)	(1)	(1)	2	(1)	(2)	7	6	1	(2) P
WE P	- -	1	11	E	-	7	3	7	6	3	6	3	3	(1)	2	2	5	(2)	1	5	4	5	1	-	-	3	3	6	(1) P

EXHIBIT 3

EXTRACT FROM FREEBORN CATELOG

Regis. Number	Indicator Trigram	Text	Position In Message
469	E U C	S L L U I Z O Y F T T	06 05
117	E Z V	I A L U I Z M S K J M	02 14

EXHIBIT 4
(Omitted)

EXHIBIT 5
(Omitted)

EXHIBIT 6A

INTERVALS ON END WHEEL

F - - - - C - - - - - - F O - Q
A - - - - - - - K - - - - - - - X
E - - - - - - - - U
J - - - - - - - - T

EXHIBIT 6B

INTERVALS ON MIDDLE WHEEL

S O Q - - G
T Z
P I R
V - - - L
B - X
C - A

EXHIBIT 7A

SCRITCH SHEET FOR END WHEEL

Cut On		2	4	6	1	3	5/6
		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	I F D C P O R Q					
	2	L H G F E C S R U P O Q					
JT	3	M H F C T S V P O Q					
EU	4	N I F G C U T W P O Q					
AKX	5	Q R M F Y X A C P O					
AKX	6	V Q S K N D X F Z Y B C A L P O					
EU	7	M X P O S Q U A E D G F K C					
AKX	8	C A V P O Q H G J F					
AKX	9	C B W P O Q I H K F					
AKX	10	D C Y P O O K J M F					
AKX	11	C Z P O Q L K N F					
	12						
	13						
	14						
	15	#1					
EU	16	E I F A D C U M K P O R Q X U					
I	17	W I F K D C L E J X P O R Q U T A M					
	18	W N I F K D C L E J X B P O R Q U T Y A M V					
	19						
	20	#2					
II	21	N L X H G F E Z V C A S R U P O I Q K D J					
	22						
	23						
II	24	N M L X H G F E T Z V C B A S R U P O I Q K Y D W J					
I	25	W N I F K D S Z C L E J X B P O R Q G U T Y A M V H					

EXHIBIT 7B

SCRITCH SHEET FOR MIDDLE WHEEL

Out On	5/6 ↓	A	B	C	D	2 ↓ E	F	G	H	I	4 ↓ J	K	L	6 ↓ M	N	O	P	1 ↓ Q	R	S	T	U	3 ↓ V	W	X	Y	Z
BX	1	S	O	Q			G	F								B		C		A							
I	2	U		S	O	Q		H	G							D		E		C		A					
PIR	3				S	O	Q	I		G						E		F		D							
PIR	4							M	S	O	Q			G		I		J		H							
PIR	5							N		S	O	Q			G	J		K		I							
PIR	6							P			S	O	Q			L	G	M		K							
II	7							V		N		L	K	P	I	R	M	S	O	Q			G				
TZ	8							Y								U		V		T	S	O	Q			G	
VL	9							Z										W		U		S	O	Q			G
BX	10	G						A								W		X		V			X	O	Q		
BX	11		G					B								X		Y		W				S	O	Q	
BX	12			G				C		U						Y	T	Z	V	X	P	I	R		S	O	Q
CA	13	Q			G			D								Z		A		Y						S	O
BX	14	C	Q			G		E								A		B		Z							S
I	15	U		S	O	Q		H	G	K	P	I	R		V	D	J	E	L	C		A	N				
VL	16	U		S	O	Q		H	G	L		P	I	R		D	K	E	M	C		A					
VL	17	U		S	O	Q		H	G	M			P	I	R	D	L	E	N	C		A					
BX	18	U		S	O	Q		H	G	W						D	V	E	X	C		A	P	I	R		
BX	19	U		S	O	Q		H	G	X						D	W	E	Y	C		A		P	I	R	
TZ	20	U		S	O	Q		H	G	Y						D	X	E	Z	C		A			P	I	R
	21				T	Z		V		N	U	L	K	P	I	R	M	S	O	Q	D	J	G				E
	22		F		T	Z	B	V	X	N	U	L	K	P	I	R	M	S	O	Q	D	J	G		H		E
	23																										
	24		W		T	Z		V		N	U	L	K	P	I	R	M	S	O	Q	D	J	G	B	Y	X	E
	25																										

EXHIBIT 8
(Omitted)

EXHIBIT 9

COUNT OF THE TWO ALTERNATIVE ALPHABETS

		I	II		I	II		I	II		I	II
A	M	3	6	EP	11	5	J X	3	9	N O	6	-
	E	7	3	O	5	7	O	4	10	O P	9	9
	J	-	5	K	8	5	N	2	4	T	25	16
	K	7	7	I	6	7	K	3	3	W	8	1
	N	3	11	FM	13	3	S	1	10	Q	4	4
	H	6	3	N	1	2	L	2	7	R	2	5
	R	1	4	U	13	5	K S	3	2	S	9	2
B	K	4	5	P	6	6	Y	4	8	P X	8	11
	L	7	3	R	7	7	U	2	3	V	4	6
	W	10	7	Z	7	4	R	7	6	S	3	11
	S	13	4	Y	17	10	N	7	11	Q S	1	1
	X	8	2	G H	6	5	P	3	2	R T	-	3
	G	1	8	X	-	8	W	6	4	X	6	4
	Q	4	1	S	9	7	O	4	4	Z	7	14
C	T	-	2	H X	6	3	L R	17	17	W	10	8
	V	17	11	U	1	5	Q	4	2	S X	7	1
	Y	7	10	N	8	8	Z	4	1	T	19	3
	K	15	1	J	-	11	P	6	2	W	4	4
	P	3	3	R	4	9	N	1	5	Z	5	4
	H	4	3	W	4	6	M R	39	6	U Z	1	1
	L	1	4	Y	6	3	N	5	13	W	1	7
	Z	5	3	P	5	11	X	12	-	Y	1	3
D	K	6	-	M	3	2	P	21	7	V Z	3	3
	O	4	1	I U	9	19	S	4	-	W Z	1	6
	U	2	21	O	12	7	N U	5	3	X Y	6	6
	V	11	16	W	15	3	R	2	16			
	N	-	3	Z	12	10	X	2	9			

FINAL SCORE: I + 146
II - 370