Copy 8 of 8 copies SECRET IL 3706
Report #F-75
12 August 1944

SUBJECT: Fish Notes
TO : CO, SSA, War Dept.

1. Receipt is acknowledged of SSA 2639. No copies of June Gurnard decodes are available but a few July samples are enclosed. (Retained B-III-C-2). I am sure these will do just as well.

2. The following ΔD count is based on 10 June Gurnard messages:-

/	112	R	89	A	93	D	87
9	124	C	82	U	130	F	103
H	108	V	87	Q	100	X	92
T	95	G	101	W	89	B	71
O	112	L	89	5	156	Z	90
M	106	P	96	8	105	Y	97
N	97	I	90	K	84	S	106
3	116	4	90	J	114	E	89

3. Two new links have been solved or partially solved. Whiting (formerly Koenigsberg-Riga) of 1 August has been broken statistically. The exact number of μ_{37} dots is not yet known, but it is high and therefore the fact that no other day can be set on the X patterns is convincing evidence of a daily change. The limitation is $X_2 + \psi'_1$. Whiting was read a long time ago but has been very quiet until quite recently. July X wheels have been statistically recovered on Perch, a newly classified key between Berlin and Lyck, East Prussia. Although the ψ's are not yet out it is known that during July the patterns did not change daily. The limitation is X_2. There has been practically no August traffic.

4. Tarpon continued to be read on the same patterns through the end of July but August is unsolved. July Gurnard was finally broken on a crib of 21 July. μ_{37} had only 18 dots and this is apparently the only reason for the difficulties which were encountered in the statistical work. Other July days have been set on the patterns. However, Gurnard of 5 August was solved statistically and other August days will not set. Since μ_{37} had 28 dots the daily change is now in effect on Gurnard as well. Since my last report the only Bream days solved are 29 July and 1 August. Both solutions were statistical. The number of μ_{37} dots was 26 and 16 respectively. The X patterns are practically out on Bream of 7 August. No August Jellyfish has been read but one more July day (the 25th) was broken on a Tarpon crib. μ_{37} had 25 dots. A true July Stickleback depth was found and anagrammed but the key has not yet been resolved. The difficulties lead to the belief that the number of dots in μ_{37} is low. No work has been done on Grilse or Codfish.

5. In paragraph 13 of Report #F-71 I mentioned a modification of the cribbing procedure. This requires further elaboration in two respects.

SECRET

6. In the first place, the intervals used to illustrate the method were ineptly chosen. If these intervals were actually employed the tests would not be independent because in the 32nd position we would be comparing positions 32, 63, 94, 125 and 156, four out of five of which have already been compared. If, to avoid this, we used a series of intervals the differences between which were all different multiples of 31, say Δ31, Δ93, Δ186 and Δ310 we would still not have complete independence. At the first position we would be comparing positions 1, 32, 94, 187 and 311 and 93 positions later we would again find 94 and 187 entering into the score. To achieve complete independence the differences, ranged in ascending order, must constitute a series of multiples of 31 such that (after inserting zero as a first term) the first differences of these multiples form a series of integers all of which are different and such that the sum of no sequence in the series is equal to any of the integers or the sum of any other sequence. The sum of these first differences should be a minimum so as to reduce the available text as little as possible. Only the following series of first differences will satisfy these conditions:- 1352, 2513, 2531 and 3152. The last of these is the one that happens to have been chosen for standard procedure here. It derives from Δ93, Δ124, Δ279 and Δ341. These 4 differences are put on both crib and message tape and the fifth level is reserved for control symbols. All that has to be counted is the number of positions where there is a dot on all 4 levels. However, the procedure of tape-making and running is not nearly so simple because of mechanical limitations. A description of the methods actually used has been drafted, is being revised and will be forwarded when complete.

7. In the next place, I did not mean to imply that this method which examines 5 positions simultaneously is more powerful than the method first described which looks separately at all intervals which are multiples of 31, but only that it was more powerful than previous methods which had proved practicable. It can easily be proved that scoring of all intervals is equivalent to writing $(\Delta Z_2 + \Delta P_2 + \overline{\overline{P}}_5)$ on a width of 31 and summing the squares of the deviations of the column totals from ½ the depth. The expected score in both cases is a function of the message length and $(b - \frac{1}{2})^2$. A tabulation of minimum crib lengths needed to get only one chance in a million of hitting, at random, the expected right score is as follows:-

M 37 dots	Crib length
28	170
26	211
24	253
22	325
20	410
18	550
16	710
14	950
12	1400
10	2180

The formula used for these calculations is derived by partial integration of the formula developed in Uspensky "Introduction to Mathematical Probability", Chapter XVI, Problem 1. The question, for a given number of motor dots, is "What is the minimum message length (or column length) necessary so that, in the random case, the sum of the squares of the deviations from ½ the depth has only 1 chance in a million (or any other set figure) of being as great as the expected sum of the squares of the deviations in the non-random case". If the distribution of the sum of the squares of the deviations were normal this would be relatively simple. As a matter of fact, the error introduced by assuming it to be normal is precisely the same as the error made in calculating by the method outlined in Report #F-46 which disregards the lack of independence of the data (referred to in paragraph 10 of that report).

8. Please send one additional set of the photographs sent as Annex C to Supplement to Monthly Information Letter #3. Mr. Kenworthy's report on the captured Sturgeon machine has not yet been prepared.

Walter J. Fried
Capt. Signal Corps

Encl. - decodes
188, 183, 184, 185,
186, 176, 182