Copy 3 of 8 copies

TOP SECRET/SECRET

L 3657-A
Report #F-86
29 September 1944

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

1. The following days have been solved since my last Fish report:-

Key	Date	M37 dots	Method
Gurnard	6 Sept.	25	R
	7 Sept.	28	R
	9 Sept.	25	R
	11 Sept.	26	R
	14 Sept.	22	R
	15 Sept.	28	R
Codfish	28 Aug.	25	R
Stickleback	13 Sept.	20	R
	15 Sept.	25	R
	20 Sept.	24	D
	23 Sept.	16	D
	24 Sept.	21	D
Bleak	13 Sept.	16	D
Bream	30 Aug.	17	C
	6 Sept.	18	C
	7 Sept.	16	C
	9 Sept.	23	R
	11 Sept.	19	C
Whiting	12 Sept.	15	D
	19 Sept.	16	D

2. There seems to be a growing tendency on some links to abandon the P_5 limitation on certain occasions. This is apparently done when conditions are such that there are likely to be reception difficulties. The dropping of this portion of the limitation is indicated by QTQNH (see Report #F 67, paragraph 2) but this cannot always be relied on. As a result of this change solutions through depths are once again likely to become an important factor. There have recently been some refinements of theory on methods of key resolution which have produced very effective results. I will try to obtain write-ups or, if these are not available in the near future, will send a description of the latest procedure. The improvements lie in the application of accurate probability theory whereas the older methods, which simply counted agreements and disagreements, utilized approximate probabilities.

3. A recapitulation of the limitations recently employed on the various links may be useful.

Jellyfish	$X_2 + P_5$
Bream	$X_2 + P_5$
Codfish	$X_2 + P_5 + \Psi_1$
Gurnard	$X_2 + P_5$ (Berlin uses X_2 only quite frequently)
Grilse	X_2 ordinarily, $X_2 + P_5$ on other occasions
Tarpon	$X_2 + P_5 + \Psi_1$
Stickleback	$X_2 + \Psi_1$ (believed to be using P_5 also on frequent occasions - but never solved with P_5)
Whiting	$X_2 + \Psi_1$
Bleak	X_2
Perch	X_2 (reasonably certain although solution never completed)

TOP SECRET/SECRET

4. Enclosed is up-to-date chart of Fish links.

5. Enclosed is rough description, prepared by one of the people in Maj. Tester's section, showing how go-backs are used in psi setting or psi recovery. The statistical theory of go-back recognition and location has been fully elaborated but there are no write-ups except for some scattered notes in Maj. Tester's research log. However, pure statistical methods have not been found too useful and the usual procedure is to endeavor to exploit a break by trying to find the same plain text on the other side of the go-back. It will be noted that the illustration used in the enclosure represents an instance where the P_5 limitation was dropped.

6. With reference to paragraph 4 of Monthly Information Letter No. 5, there is no approved method of appraising a rectangle in advance. Theoretically the deviations from average of the scores in the individual cells should furnish an index of significance but it is not believed that any test based on such deviations would be sharp enough to be useful. The enclosure contains answers to the questions of paragraph 7. With respect to the last two sentences of this paragraph, I am sorry that I did not explain more fully. I agree that it is by no means obvious ab initio. However, I assumed that anyone trying to follow this would have in mind the cribbing theory developed in Report #F 46 (IL 3601) and with this as a background I think it is obvious. Annex C to Letter No. 5 has been delivered to Mr. Newman but neither he nor any of his assistants has as yet had an opportunity to study it.

7. Construction of Block H, which was built to take care of Mr. Newman's new machinery and the overflow of his section, was completed a week or so ago. Colossus 5 has been installed in the new building and is in operation. Colossus 6 has also been installed but is not yet connected. Mr. Newman's section now consists of 20 male civilians (at least 10 of them with honors mathematical degrees from Oxford or Cambridge), 1 U. S Navy officer, 2 U. S. Army non-commissioned officers and 186 W.R.N.S. women (including 1 officer) especially chosen for this work. Maj. Tester's section consists of 21 officers (including 2 U. S. Army officers), 77 other tanks, 26 A.T.S. women (including 2 officers) and 12 male civilians, a total of 136 people. About 30 of these are engaged on registration of traffic. There are 6 mechanics and 37 machine operators. There are about 20 people who break dechies and anagram depths. In addition there are 34 setters whose principal function is to carry a break back to the beginning of a message and compute the settings for the machine operators. The remaining 9 people in the section have a variety of miscellaneous jobs.

8. The SSA technical paper entitled "Hand-Transposition Systems" has been distributed as suggested but I have received very few comments as yet. I read it with a great deal of interest and thought it was, for the most part, well written and presented. I have made note of a number of typographical errors but will defer calling attention to these until after my return. I think the paper raises an interesting question of general application, namely, "Should cryptographic and cryptanalytic write-ups of this nature be presented as mathematical treatises when such treatment is not essential to a full understanding

of the subject matter." My own opinion is in the negative and I think that this particular write-up tends to be too formal. Not all cryptanalysts are mathematicians and I see no virtue in symbolic formulation where the thought can be accurately and succinctly expressed in ordinary language. Page 8 furnishes an instance. The proposition proved is so obvious from its mere statement in words that the algebraic presentation seems to add nothing. In a treatise on pure mathematics rigorous proofs of apparently self-evident theorems is doubtless necessary but it does not follow that the same degree of precision need be carried over to a field that is essentially practical.

9. A rather different approach to some of the problems considered in the paper seems conceptually simpler and at the same time more fruitful. In the first place, it is easily shown that a depth of n with K_s unknown is exactly equivalent to a depth of (n-1) with known K_s. In the first case we consider the (n-1) independent differences (or combinations) as being subjected to transposition whereas in the second the transposition can be applied directly to the letters. If we have a group of letters in depth and represent them as follows:-

A + + - - -
B + - - + +
C - + + + -

it is easy to think of the transposition as being applied to the columns as units. If all 5 columns are different and we know both plain and cipher equivalents the transposition key is uniquely determined whereas if 2 or more columns are identical unique determination is impossible. With a column length of 2 (which represents a depth of 3 when K_s is unknown) unique determination is obviously impossible because only 4 different columns are possible and there are 5 positions. To me this is much simpler than the proof contained on pages 34 and 35. Also, from this viewpoint it becomes immediately apparent that the probability of a unique determination of transposition key from a depth of 4 is $\frac{8!}{2^5 \cdot 3!}$; and for a depth of (n+1) it is $\frac{2^n!}{2^{5n} \cdot (2^n-5)!}$.

Similarly, the probability of obtaining a transposition key with one ambiguity (or with any number of ambiguities) can be immediately computed.

Walter J. Fried
Capt. Signal Corps

Encl. - 1 chart
1 sheet cross-section paper
3 pages

CALCULATION OF ODDS OF BEST SCORE IN A RUN

Consider a X_1, X_2 run for the sake of argument. Let the best bulge be B_1 and second best B_2 (not agreeing on either wheel). Then not allowing for competition the factor in favor of the best reading being right is

$$\frac{25}{\sqrt{N}} \; E^{2B_1^2/N}$$

where N is the text length. This is the same formula, essentially, as in significance test IV. Possibly the 25 ought to be increased a little, say to 35, since b is known in this case.

The odds on the best reading being right allowing for competition are

$$\frac{\frac{25}{\sqrt{N}} \; E^{2B_1^2/N}}{\frac{25}{\sqrt{N}} \; E^{2B_2^2/N} + 1269q}$$

Where q = probability of right score being below B_2.

i.e.

$$\frac{E^{x_1^2/2}}{E^{x_2^2/2} + 1269\, q.\, \frac{\sqrt{N}}{25}}$$

X_1, X_2 being the σ-ages of best and 2nd best readings.

The $q\sqrt{N}$ can be replaced by a constant for a given link and day with a fairly small error, remembering that if X_2 is high it doesn't matter even if q is taken as 0 or 1. Empirically, $q\sqrt{N} = 12$ or 8 or so. It doesn't make too much difference for most practical purposes. It was intended to drew up several charts to cover the variations from Fish to Fish and with number of motor dots, but there has always been something more important to do.

TOP SECRET

Example of a 'Go-back' used to set Psi wheels for a De-Chi. GURNARD Traffic 7th Sept. 1944
28 dots in 37 Motor. Limitation: X2 only.

```
X2         .XXX..X..X..X..XXX..XXXX.X...X..XXX..X..X..X..XXX..
De-Chi     YD4UY8JECRBB/FL+ZIP/N3BLMBSQIL+UNSFFB+AKUMDY4MNFWRJ
Clear                          9UNTER9DAMPF9STARK9BELECT+N89
Ext. Psi                       DC00000AMJT884MMM4X44X11BCCJQ

X2         ..XXX..X..X..X..XXX..XXXX.X...X..XXX..X..X..X..XXX.
De-Chi     14JZMBZ1+94NCMIMMN+T3NKVY+PJJMOQPTXJCVM+3VOFOTAADN8U
Clear                          9UNTER9DAMPF9STARK9BELECT+N89
Ext. Psi                       MK/888883QRYNW/VEEOSGG84XANMU
```

TOP SECRET

Recognition of Go-Back

Usually by normal method of finding likely clear and then looking for the same clear on the other side of the Autopause, as in the example by the finding of the two occurrence of "9UNTER9". The two stretches of De-Chi were then written out in depth, each with its X2 limitation above. With the X2 alone being used as limitation, it was known that motor dots could only occur under X2 crosses. Where X2 crosses fell in depth, several clicks in differenced De-Chi were observed. Also there were numerous cases of the differenced de-Chi letter at a X2 cross in one stretch being the complete reverse of the corresponding position in the other stretch under a X2 dot. One would expect this Psi behaviour for keys whose 37 motor had as many as 28 dots. In these positions, it could be assumed with fair certainty that differenced De-Chi was the same as differenced clear.

Go-backs have also been recognized by sliding differenced De-Chi stretches against each other and looking for clicks. Here it is helpful to use the X2 limitation as well, even if there is also P5 limitation. This has been useful in breaking De-Chis with difficult clear or which are wrongly set on one Chi-wheel. However, recognition is difficult if the 37 motor has very few dots.

Note to IL 3857-A

This may help to explain the first annex. It is due to Sgt. Jacobs.

J.N.Seaman

$B_1 = x - r$

Normal curve. random (exp. val. = r)

$$P(x/r) = y_1 = \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{(x-r)^2}{2\sigma^2}}$$

gaugal (exp. val s)

$$P(x/s) = y_2 = \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{(x-s)^2}{2\sigma^2}}$$

$$y_1/y_2 = e^{\frac{(x-s)^2}{2\sigma^2} - \frac{(x-r)^2}{2\sigma^2}} = e^{\frac{-s-r}{\sigma^2}x + \frac{s^2-r^2}{2\sigma^2}} = \text{Inverse odds}$$

$$\frac{\text{excess}}{\sigma} = \frac{x - r}{\sqrt{N/2}} = \frac{2B_1}{\sqrt{N}}$$

$$\therefore y_1 = \frac{1}{\sqrt{2\pi}\sqrt{N/2}} e^{\frac{-2B_1^2}{N}}$$

$$y_2/y_1 = y_2\sqrt{\frac{\pi N}{2}}\, e^{\frac{+2B_1^2}{N}}$$

$$\doteq \frac{25}{\sqrt{N}} e^{\frac{2B_1^2}{N}}, \text{ they say}$$

(So they are saying $y_2 \doteq 20/N$)

Don't know why.

Small is going to look into this.