

L 3657-A Report #F-98 29 September 1944

TEJECT: Fish Notes

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

Date	M 37 dots	Method
6 Sept.	25	R
7 Bepte	28	R
	20	R
		R
18 Sant.	28	R
28 AUG.	25	Ŕ
13 Sept.	20	RRR
15 Sept.	25	R
20 Sept.	24	D
	16	D
	31	D
	16	D
	17	C
o Sept.	16	C
	93	
11 Sept.	19	Ĝ
18 Sept.	15	R C D
19 Sept.	16	D
	6 Sept. 7 Sept. 9 Sept. 11 Sept. 14 Sept. 15 Sept. 15 Sept. 15 Sept. 20 Sept. 23 Sept. 24 Sept. 25 Sept. 26 Sept. 27 Sept. 7 Sept. 9 Sept. 11 Sept. 12 Sept. 13 Sept. 14 Sept. 15 Sept. 16 Sept. 17 Sept. 18 Sept.	6 Sept. 28 7 Sept. 28 9 Sept. 25 11 Sept. 26 14 Sept. 28 18 Sept. 28 18 Sept. 20 15 Sept. 20 15 Sept. 24 23 Sept. 24 23 Sept. 16 24 Sept. 16 30 Aug. 17 6 Sept. 16 9 Sept. 16 9 Sept. 18 11 Sept. 16 9 Sept. 19 12 Sept. 19 13 Sept. 19

2. There seems to be a growing tendency on some links to abanden the P. 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 QTQNE (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 Bresm Codfish Gurnard Grilse Tarpon Stickleback	X <sub>2</sub> + P <sub>5</sub> X <sub>2</sub> + P <sub>5</sub> X <sub>3</sub> + P <sub>6</sub> (Berlin uses X <sub>2</sub> only quite frequently) X <sub>4</sub> erdinarily, X <sub>5</sub> + P <sub>5</sub> on other occasions X <sub>5</sub> + P <sub>5</sub> + P <sub>6</sub> X <sub>6</sub> + P <sub>6</sub> X <sub>7</sub> + P <sub>6</sub> X <sub>7</sub> + P <sub>6</sub> X <sub>7</sub> + P <sub>7</sub> X <sub>8</sub> + P <sub>7</sub> X <sub>8</sub> + P <sub>8</sub> X <sub>9</sub>
Shiving Blesk	Xg + 1
Perch	(secondary cortain elthough solution never



TL 3857-A eport #F-96 Page 2

- 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 endeaver 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 Ps 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 initic. However, I assumed that anyone trying to follow this would have in mind the cribbing theory developed in Report #F 46 (IL 5601) 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 B, 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 Eavy officer, 2 U. S. Army non-commissioned officers and 186 W.R.M.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 135 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 amagram 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.
- 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 crypt-analysts 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 unknown is exactly equivalent to a depth of (n-1) with known K. 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 ++---

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 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

 $\frac{8!}{8^5 \cdot 3!}$ ; and for a depth of (n+1) it is  $\frac{8^n!}{2^{5n} \cdot (8^n-5)!}$ 

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

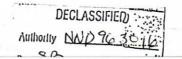
Walter J. Fried Capt. Signal Corps

Encl. - 1 chart

1 sheet cross-section paper

3 pages







L 3857-A 1-96 Page 4

## CALCULATION OF ODDS OF BEST SCORE IN A RUN

Consider a  $X_1$ ,  $X_0$  run for the sake of argument. Let the best bulge be  $B_1$  and accord best  $B_0$  (not agreeing on either wheel). Then not allowing for competition the factor in fevor of the best reading being right is

25 E2B12/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 resding being right allowing for competition are

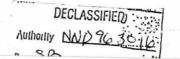
Where q = probability of right score being below Bg.

1.0.

X1. X2 being the -ages of best and 2nd best readings.

The q/N can be replaced by a constant for a given link and day with a fairly small error, remembering that if X<sub>2</sub> is high it doesn't matter even if q is taken as 0 or 1. Empirically, q/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.





OURNAND Traffic 7th Sept. 1944 Fal wheels for a La-Chi. X2 only. Example of a 'Go-back' used to set 28 dots in 57 Motor. Ilaitation:

Ext. Pal Do-Chi Clear

YDAUY81 EURBB/F1.2 IP/H3BINEBCIL-UNBFFB-AKUNDYARNFRR 0000000411884EM4X44X11BCCJC

Class

EXT. Pel

147ZMBZ1+94WCMIMBETSUKVY+PJJWOQFTXJCVM+SYOFOTAADHBU 9URTERDDAMFPOSTARSBELEUT+N89 NK/BBCCBSQRIWY/VERDSGCGGAXAMU

Recognition of Co-Back

The X2 limitation above. With the X2 alone being used as limitation, it was known that motor dots could only occur under X2 crosses fell in depth, several click Colour on the other side of the Autopause, as in the energie by the finding of the two ecour-crange of "SUNTERS". The two atretches of De-Chi were then written out in depth, each with The X2 limitation above. With the X2 slone being used as limitation, it was known that enced 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 Fsi behaviour Usually by normal method of finding likely alear and then looking for the same In these positions, it could be assumed with fair certainty that differenced De-Chi was the same as differenced clear. for keys whose 57 motor had as many as 28 dots.

However, recognition is diffi-Here it is helpful to use the Z2 limitation as This has been useful in bresking De-Chis with Go-backs have also been recognized by sliding differenced Do-Chi stretches one Chi-wheel. difficult clear or which are arongly set on against each other and looking for elicks. sult if the 37 motor has very few dots.

DECLASSIFIED Authority NND 96

TOPECHE TO IL 3857-A

his may help to explain the first annex. It is due to Sgt. Jecobs.

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

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

paugal (expe val s)

$$P(x/s) = y_2 = \sqrt{\frac{1}{2\pi 6}} e^{-\frac{(x-s)^2}{26^2}}$$

$$\frac{s_{1/2}}{s_{1/2}} = \frac{(x-s)^2}{2s^2} - \frac{(x-r)^2}{2s^2} = \frac{-s-x}{s^2} \times \frac{s^2-x^2}{2s^2} = \text{Inverse odds}$$

$$\frac{excess}{s} = \frac{x - r}{\sqrt{N/2}} = \frac{2 \, 3}{\sqrt{N}}$$

$$T_{N_1} = T_2 \sqrt{\frac{\pi N}{2}} C \frac{425^2}{N}$$

$$\frac{1}{25}$$
  $\frac{25}{N}$   $\frac{251^2}{N}$  , they say

(So they are saying y2 = 80/H)

Don't know why.

Small is going to look into this.

