Copy 8 of 8 copies

SECRET

I/L 3605-A
Report # F-50
21 June 1944

IL 3605—

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

1. During the period when Bream was off the air a few Codfish messages were set and thereafter read. It has just been discovered that ψ_1 one back also contributes to the motor. The limitation is $\psi_1 + \bar{X}_2 + \bar{P}_5$. When these 3 elements combine to produce a dot a motor cross is compelled.

2. Gurnard has been solved by the cribbing method described in Report #F-46 (IL 3601). The process was somewhat reversed since the crib was about 2000 letters long and a portion of it was found in a Gurnard message of only 800 letters. Runs were made at intervals of 31, 62 and 93 and although the scores were very strong they were then checked by a further run at interval 124. The day solved was 19 June. μ37 has 24 dots. The limitation is $\bar{X}_2 + P_5$ (which, of course, had been assumed). Both messages were from Berlin.

3. Jellyfish patterns changed again on 14 June and the new wheels have not yet been broken. Statistical and cribbing methods are both being tried.

4. The ψ_1 limitation makes inapplicable the cribbing technique as heretofore used. An alternative possibility which can be used with this limitation, or without any limitation, is $(\Delta P_{45} + \Delta Z_{45})_{\Delta 598}$. The probability of dot is again $b^2 + (1 - b)^2$ at the correct setting. Impulses 4 and 5 are chosen simply because the product of their cycles is lowest. Multiple intervals can also be run if the crib is long enough. Obviously this method needs much longer cribs but simpler tapes are used so much preliminary time is saved. A crib of almost 2000 letters is required to yield a score of 4 or 5σ. There seems no reason why runs cannot be made on other pairs of impulses as well and the scores combined. IC equipment can, of course, be used for all these procedures.

5. The Ψ_1 limitation would seem to have a slight adverse effect on the results expected from the dragging machine. (I am assuming that it can incorporate X_2 or $X_2 + P_5$ limitation). However, it merely means that some random stops must be eliminated by hand testing.

ARMY

SECRET

6. A statistical method to differentiate between ordinary Fish and permuted traffic would be to run $(\Delta Z_{ij})_{\Delta ij}$. Δ_{ij} means differenced at an interval equal to the product of the cycles of two X wheels. Impulses 1 and 2 would be best from the viewpoint of the bulge in ΔP but of course the cycle is longest. Again all ij pairs could be tried (also all available multiple intervals) and all available long messages could be run. The strength of the test depends on the value of b and the plain language characteristics. Probably about 40,000 letters would be required to proe duce significant results but this figure might vary widely. Mr. Newman points out that a positive result would safely lead to the conclusion that the traffic was regular Fish but that it would be highly dangerous to conclude that it was permuted because the scores were random.

Walter J. Fried
Capt. Signal Corps