Copy 8 of 8 copies.

MOST SECRET CX/MSR 1-3367

SUBJECT: Fish Notes — Report #F 7
TO : CO, SSA, War Dept. — 23 March, 1944

1. As Capt. Seaman has doubtless explained, Mr. Newman's section handles the machine work on this problem and Maj. Tester's the hand work. Since I am visiting both groups my reports on the techniques observed cannot follow the order employed in the actual work of solution. It might be well, therefore, to indicate the usual procedure applicable to the Bream traffic (or any other traffic using the P_5 limitation).

2. At the beginning of the month the X patterns must first be recovered by statistical methods. This is handled by Mr. Newman's section. The methods used are known at A. H. and have been reported on by Capt. Seaman. I will report further at a later date. Next the X patterns have to be set on a message which is one of a pair in depth. The setting is also done by Mr. Newman's section. Some of the mathematics involved will be recapitulated in my next Fish report. In this operation both messages can obviously be used if one is not long enough. After this has been done the de-chi is sent to Maj. Tester's group to find the ψ patterns. This is not simple because the so-called depths are not true depths by reason of the P_5 limitation. The ψ patterns emerge with plain text in the two messages and also lead to M_ψ. This must then be resolved into μ_{61} and μ_{37}. This last step is described in paragraph 3. Later in the month when both X and ψ patterns are known, Mr. Newman's people take all messages of sufficient length, set the X patterns wherever possible, and send the de-chies to Maj. Tester. Depths are now not required because agreement with known patterns furnishes the check by which plain text assumptions are verified. Both the original recovery of the ψ patterns and the setting of known patterns will be described in due course. The setting of the ψ patterns again yields M_ψ which must be resolved as heretofore. When the day's motor patterns have already been found, this last is a simple problem because it is only a matter of finding the starting point. One of the real difficulties of this entire problem arises from the fact that it never reduces to mere decoding. Each message requires independent cryptanalysis unless it is on the same day as one already solved, on the same circuit, in the same direction and with the same GEP number - in other words, unless it would have been in depth with a solved message were it not for the P_5 limitation. Identical GEP numbers in opposite directions mean nothing because different tables of settings are used at the two ends of the circuit. The tables are also different for each day.

3. The method used to determine μ_{61} and μ_{37} from M_ψ is fundamentally the same as the old method with which A. H. is familiar. However, since M_ψ and M_β are not identical the problem is now more difficult and ordinarily requires at least 400 - 500 letters of text. M_β is first derived from M_ψ by carrying down all values where $\bar{X}_2 + \bar{P}_5 = x$. The other positions must be left blank because there is no way of knowing whether the cross in M_ψ derives from a cross in M_β or from the limitation. The broken M_β pattern is written on a width of 61 and

ARMY SECRET

Report #7 7 (continued)

and crosses placed in the κ_{61} pattern wherever required. In the first instance no dots are placed in the κ_{61} pattern unless the evidence supporting them is very strong indeed. Efforts are then made to match the column patterns. Successive assumptions are made as to the number of dots in κ_{61} and inconsistencies used to disprove each wrong assumption. It is best to work with a section of columns under a heavy band of crosses in Ψ_2. This procedure is exactly the same as we have heretofore used except that it is made more difficult by the breaks in the columns and by the increase in the number of assumptions to be disproved. The number of dots in κ_{61} now ranges from 10 to 30 whereas a few months ago the range was only 11 to 19. Of course 24 dots are never used. The number of dots in κ_{37} is invariant throughout the month (or other key period) in order to preserve the ab = 1/2 relation. However, this fact furnishes almost no assistance in recovering the motor patterns because, by the time the information could be used, the task will be virtually completed.

4. The number of dots in κ_{37} has varied widely in recent months. For March Dream it is 24. This high a number facilitates solution from several viewpoints. First, it aids in recovering and setting the X wheels. 24 dots means that b must equal .74 which is very good. Second, it helps in recovering and setting the Ψ patterns because the techniques employed depend on finding significant motor dots and it therefore helps to have a high proportion.

Walter J. Fried
Captain, Signal Corps