Copy 8 of 8 copies.

TOP SECRET CI/WJ

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

Report #F 22
17 April 1944

1. March Bream furnished the greatest volume of decodes in the history of the section, over one and one-half million letters of plain text having been turned out.

2. The March Jellyfish wheels have finally been broken and a few messages have been read. They have fulfilled all expectations with respect to intelligence value. The circuit uses the X_2 and P_5 limitations precisely as does Bream. The χ_{37} patters contained 22 dots. This is quite favorable so that it is probable that a substantial amount of March traffic can be read if time permits. Work on the April Jellyfish wheels is in progress and they look hopeful. The plain language~~s~~ characteristics (judged from only a handful of decodes) seem a little better than the Berlin end of Bream but not so good as the Rome end. (The Rome operators have bad habits which make that end of the circuit much easier to read and Bream work always starts on the messages originating from Rome. The difference is more important to Mr. Newman's section than to Maj. Tester's.)

3. The April Bream wheels are broken but χ_{37} has only 17 dots and this makes it difficult to set the ψ patterns and read messages. At present only about 50% of the de-chies are being read, although it is anticipated that the percentage will increase later in the month. This type of situation revives interest in the machine we contemplated for setting ψ patterns by dragging probable words. Mr. Welchman has just advised that it has been decided to proceed with this project but before this was known the people here were urging me to suggest that we go ahead as quickly as possible. The value of the machine method, as an adjunct to the hand methods employed, is that the very fact that makes the latter difficult adds to the sensitivity of the former. This may be slight but less contraction of the ψ s will cause some reduction in the number of stops and may make it feasible to work with probable words shorter than 10 letters.

4. In working on April Bream, Maj. Tester's section, for the first time, derived the ψ patterns without a depth. In theory, no plain text assumption applied to a de-chi can be disproved (unless long enough to repeat a portion of the cycle of the shortest ψ wheel) because the resultant ψ ' key is always possible. But actually there is a high probability of the assumption being wrong unless it produces a substantial number of repeats and anti-repeats in the ψ ' key. Although sure cribs are not available, familiarity with the traffic proved a help in this process which, in any event, is most difficult and requires a high degree of skill and a good deal of training and backbround. Once an assumption has been fitted into a position which yields a likely stretch of ψ ' key, efforts are made to extend this forward and backward.

ARMY

TOP SECRET

After enough ψ' is recovered to give about 20 elements of each of the ψ patterns, these can be projected forward or backward (or both if text is available in both directions) to their next respective cycles and will overlap sufficiently to give a small stretch of the ψ key. This has to be slid back and forth in an effort to find plain text because the exact number of intervening dots in M_T is unknown. Furthermore, since ψ' key, rather than ψ, is needed, additional assumptions must be made and tested as to various possibilities of extension. These projected stretches of ψ key are bordered by areas in which 4 of the ψ patterns are known so that, after the stretch has been properly located and extended, additional text can be found, fore and aft, on 2 generatrices (again with proper extensions). This method can be used before enough of the ψ patterns are recovered to overlap on all 5 wheels at the next cycle but with the necessity of reading on 2 generatrices superimposed upon the problem of locating the stretch and determining the extensions it is even more difficult. In practice what is done is to look for a new and independent break at approximately the right interval and to confirm it or expand it, or both, with the aid of the pattern fragments. It should be observed that the P_5 limitation is a help rather than a hindrance in this type of work because in working forward it limits the places where a motor dot has to be tried and in working backward it sometimes determines the fifth plain text impulse. This is true as against no limitation at all; the X_2 limitation alone would be even more of a help. In theory this method could be used on a number of different messages and the ψ pattern fragments thereafter combined but in practice, if the fragments are large enough to piece together successfully, it would almost necessarily be easier to proceed by extending and projecting as described above. Actually the solution was achieved wholly on one message.

5. The enclosure "Breaking the ψs in the P_5 Era" includes the section's own description of the foregoing procedure but is devoted primarily to the recovery of ψ patterns with the aid of a depth. When it was written they had never actually been recovered without a depth.

6. It should be easily possible to use the machine for dragging probable words to assist in the initial steps involved in recovering ψ patterns without depths. If a 10 letter word were dragged through a de-chi the machine would be set to show all positions where 3 or more repeats were yielded in the ψ' key, that is, it would stop if the ψ patterns were contracted down to 7 or below. I have discussed this suggestion with Maj. Tester and Mr. Newman and they both feel it would be a great help in getting started. Mr. Welchman advises that there would be no difficulty in adapting the machine to accomplish this provided it is borne in mind during construction. I calculate the number of random stops as about 1 in 450. If the P_5 limitation is incorporated (so that there could be no contraction where a motor cross were compelled by X_2 and P_5) the number of random stops is reduced to about 1 in 720. (These calculations have not been checked here - suggest this be done.) It is true that the requirement of at least 3 repeats will cause a good number of correct positions to be missed. This involves no loss however,

because if a hand assumption yielded less than this number it would not be regarded as good enough to go ahead with. For this procedure (as well as for the primary function of the machine) the inclusion of the P_5 limitation would be useful but not at all essential if it involves any constructional difficulties. Hand elimination of stops rendered illegal by the P_5 limitation is relatively simple and rapid. From my talk with Mr. Welchman I conclude that the machine will be constructed so that this limitation can be wired in if required but that it will not be an integral part of the mechanism.

7. Mr. Newman's section, with the aid of Colossus, is now able to carry out by statistical or mechanical methods, all steps in the solution except the initial recovery of the ψ patterns.

8. The motor can, in theory at least, be derived statistically by writing into a 61 x 37 rectangle all positions where there is a / in the ΔD test. These probably result from motor dots. The technique used is exactly the same as for the recovery of μ_{37} and μ_{61} from M, except that the entries in the rectangle represent probabilities rather than certainties. Without the X_2 limitation the method has been successfully used on a depth of just over 2. The X_2 limitation (and also the X_2P_5) makes the necessary depth 4 times as great because the procedure is based on comparison of columns and elimination of half the data from each reduces the available comparisons to ¼. Mr. Newman thinks that with the limitations it might be done with a depth of 6. This obviously limits the applicability of the method. In any event Maj. Tester's methods seem less laborious. Entries in the rectangle need not necessarily be confined to /. + is sometimes used (Δ89) and sometimes U (Δ+M). A combination can also be used. The characteristics which serve as criteria are determined by a frequency study of the ΔD text of the individual message being analyzed.

9. The setting of a known motor pattern is quite another matter. This is easily done after the X patterns have been set, by setting up μ_{37} and μ_{61} on the Colossus machine and running through in all 2257 positions. It is not even necessary to make a ΔD tape because the machine operates with a ΔZ tape and ΔX patterns set up on the X wheels. The machine records all /s in ΔD which coincide with motor dots. It looks at 5 positions simultaneously on each of the 5 impulses and takes less than 10 minutes to try all settings and record those on which the count exceeds a predetermined criterion. Here again / is the usual test, not the only one. Plans are under way for runs which will count / against motor dots together with some other letter (not 8 however) against motor crosses. Self-match of "slide" causes some difficulty in this operation. The P_5 limitation does not eliminate this method although it increases the length of message required. In general, however, if the message is long enough to set the X patterns, there is a good chance that it is long enough, even with the P5 limitation, to set the motor.

MY

10. After the motor is set the ψ patterns can also be set with Colossus. They are extended by the motor and 2 ψ wheels at a time are tried at all possible starting positions. Ideally, ψ_1 and ψ_2 should be run against the de-chied message because $P_1 = P_2$ is a very strong plain text characteristic. A number of considerations make this ideal procedure impracticable (and sometimes impossible). It is impracticable with present equipment because it takes too long to set up new patterns on the machine. Two sets of patterns can be set up on the existing Colossus and it is possible to switch either one into use. However, at the moment, both Bream and Jellyfish ΔX patterns are set up. Therefore the procedure would be to make a run which would require that $\Delta P_1 = \Delta P_2$. This is not as sharp but is still good enough. When the new Colossus arrives (about June first) this practical difficulty will be remedied. In fact Colossus #2 could do the whole job itself because it will hold 5 alternative sets of patterns. The impossibility of proceeding in the manner indicated arises when the P_5 limitation is present. It is then necessary to set ψ_5 first and the best run is $P_4 = P_5$. For the reason stated above $\Delta P_4 = \Delta P_5$ would be the actual run. After After ψ_4 and ψ_5 are set short runs are made on other ψ wheels with ψ_5. Different plain text characteristics must, of course, be locked for on the various types of runs. All of the material set forth in this paragraph is, to some extent, theoretical because Colossus has never been used to set the ψ wheels. Some of the older machines have been used but the fact that it has all been thought out and developed furnishes another instance of the advance planning which seems to account for a great deal of the cryptanalytic success which has been achieved here. Because of the possibility of corruption (and its devastating effect when the P_5 limitation is employed) this type of run is limited to 800 letters at a time. The correct solution is found through matching up the high scores. Experience shows that about 1 letter in 800 is garbled on the fifth impulse.

11. Maj. Tester's section has derived the X and ψ patterns for March Stickleback (X_2 limitation but not P_5) but has had no time to devote to efforts to read the traffic.

1 Encl. - 2 pages

Walter J. Fried
Capt. Signal Corps

ARMY

Copy 8 of 8 copies.

SECRET

BREAKING THE Ψ S IN THE P5 ERA.

In previous months, the process of wheelbreaking has always consisted in key analysis, either by Turing's method, or subsequent methods rendered effective by the introduction of the X_2 limitation. However, the introduction of the (X_2P_5) limitation (hereafter referred to as P_5) has made it virtually impossible for us to obtain key and the process of wheelbreaking has undergone a very radical change.

Whereas, the solution of the X wheels and the Ψ wheels resulted from the same process before P , we now use two entirely different processes to obtain the two sets of wheels. The X wheels are obtained by statistical methods from the cipher text (based on clear and motor characteristics) and the Ψ s are only investigated subsequent to the solution of the Xs. I propose here to deal only with the method employed for obtaining the Ψ patterns.

A 'depth' is set on the X wheels by statistical methods. By a depth we now mean two messages whose initial settings are the same. In the course of encoding the X wheels and the motor wheels remain in depth but the Ψ wheels will diverge according to the limitations imposed on their movement by (X_2P_5). The two legs of the depth are written out underneath each other in their de-Xs form (preferably on a width of 62) and the X_2 component of the limitation is written over the top (it should be remembered at this stage we do not know if our X_2 is inside out). We then attempt to break into one leg of the depth, using methods employed in the normal day to day reading of de-Xs. When a break is obtained which gives a reasonable expectation of being correct (i.e. works on limitation, involves dots in the motor, changy Ψs, and probable clear) we drag the inferred Ψ characters through the other leg of the depth in the neighbourhood of the corresponding position on the de-X. (It should be noted that, if our break occurs N from the beginning of the message, where N is less than 300, say, then we would expect our Ψs to have diverged by not more than $\frac{1}{2}\sqrt{N}$ from each other). When the Ψs are picked up on the other leg, the process becomes very similer to the old game of anagramming a depth, since clear obtained from one leg will give us new Ψ characters which will in their turn enable us to anagram the other leg, (c.f. in anagramming a depth, obtaining clear on one gives us new K-characters which enable us to anagram the other leg). There are, however, two important differences, one being to our disadvantage, the other to our advantage. In the first place in anagramming a depth we can very easily make two breaks-in and then join them. This is far more difficult in our present problem since a new break-in involves a new drag of the Ψ s in order to be able to use both legs of the depth. On the other hand, we can jump on our Ψ s and this is very useful indeed. Suppose, for example, we have obtained twenty Ψ characters. If we put in our patterns again on the width corresponding to the wheel length we will obtain four new Ψ characters, flanked by Ψ characters about which we know four of the signs. We use these <u>certain</u> Ψ characters to get in again lower down the message and use the additional evidence we get from further anagramming to help us to push on our first break. We may well be called upon to 'jump' four or

ARMY

TOP SECRET

five times before we complete our ψ wheel patterns and, in fact, in March, 1943, we had six separate patches of the de-χ which we were using to complete our knowledge of the patterns. (Note. If we know n ψ characters, and we put these in at the correct intervals, we obtain (n – 16) new complete ψ characters, flanked by 10 ψ characters about which we know 4 signs).

The final point which arises is this:- Is a depth absolutely necessary for breaking the ψ patterns? It is true that we only need use the second leg of the depth in order to confirm and extend our original break-in and that subsequently all the work can be done (and has been done) on only one message. However, the task of getting an original break-in on a single message long enough and certain enough to render 'jumping' effective seems to me to be a very great one. One can, however, say this. The chance of success would be dependent very considerably on two unrelated factors, (1) the nature of the clear and (2) the number of dots in μ 37. With an operator who regularly uses 9++M89 as his stop, with a μ37 consisting of 26 dots and with the original break-in occurring in the address, then certainly it could be done. With an operator who varies his stop between +M98 and +M89, with 16 dots in μ37 and if the break-in occurred in a long patch of hand, then certainly it could not be achieved. Somewhere between these two extremes lies the critical point.