

SECRET

IL 3642
Report #P-87
#7 July 1944SUBJECT: Fish Notes
TO : CO, SSA, War Dept.

1. Enclosed are Bream decks to be used for trying out the dragging machine, together with document indexing tapes and giving wheel patterns and cribs. I think all of this is self-explanatory. On the broken decks the plain text has been written in at the point where the break was made, so if you prefer to work with no clues except those furnished by the crib list I suggest that these stretches be erased before work is started (or, in the alternative, that you work only from tapes). Duplicate decodes are furnished to enable you to check results. Motor patterns are not included (although the number of 37 dots is given in each case) and it might be good practice to derive those for each day you succeed in breaking. The chi patterns are included, although superfluous for this experiment. The number of unbroken decks is few because in most cases the failure to read creates a strong suspicion that the chis are not set correctly. This is the reason no unbroken Jellyfish decks are being sent. Most of them have been worked over so thoroughly as to make it fairly certain that there is something wrong with the decks. On the unbroken messages enclosed herewith it is believed reasonably likely that the decks are correct. You will note that some of the best cribs are shorter than 10 letters. If too many random stops are produced alternative runs can be made with varying assumptions as to word-spacers. In this traffic the crib, unless part of a compound word, must be preceded by 8 or 9 and must be followed by 8, 9 or +.

2. The difficulties with current traffic continue. July Tarpon has been broken. The limitation is $\chi_1 + \chi_2 + P_5$. 437 has 25 dots. The patterns have been in force from the beginning of the month to the present. July Gurnard is still unbroken. No July Jellyfish has been solved although one day (13 July) looked promising for a while. However, there was not enough traffic to complete the solution. Bream is now also changing patterns daily. 13 July was solved statistically. 437 had 21 dots. 18 July was solved through a crib from Tarpon. 437 had 26 dots. 21 July was also solved statistically and 437 had 18 dots. A statistical solution has yielded the Bream chi and psi patterns for 20 July but this was only accomplished today and the motor patterns are not yet out. The number of dots in 437 is estimated at 27. It is believed that Codfish no longer uses Bream patterns because attempts to set Codfish messages on some of the solved Bream days have been unsuccessful.

3. It looks as though new security measures in the West require a daily change of pattern whereas in the East the χ limitation is considered good enough. Stickleback has probably added P_5 to its limitation for July but does not use the full limitation on all occasions. A similar phenomenon was observed

ARMY

SECRET

DECLASSIFIED
Authority NND 963016
By SP NAVA, Dala

in June Gurnard which on a few occasions omitted P₅ from its limitation. The group QTQNN in operator's chat apparently means "no auto-key". A watch is being kept for identity of QEF numbers among QTQNN messages. Stickleback, however, has been off the air for some time but has just come back. The new station is west of Galatz. The mystery about the new attachment (paragraph 5, Report #F-61) is unsolved. It was mentioned on Bream so cannot be the Y₁ limitation as had been suggested. However, if used on Bream it can have no cryptographic significance because the Bream days broken have been perfectly normal. The Germans call the attachment "2x".

4. The Fish information contained in Monthly Information Letter #3 and annexes was turned over to Mr. Newman. His comments are as follows:- "The starting and converging of rectangles is taking up a great deal of our time and energy at the moment so we were glad to see that you are thinking along these lines. We would be interested to know how long an IBM run on a block of nine takes. We are hoping to have a new attachment on Colonus soon which will print a rectangle in about a quarter of an hour; a further mechanical method of making a start would be of great help."

5. Pursuant to requests contained in SSA 2101 I enclose TRUMB/ZIP/EF 4 of 26 July 1944. This brings frequency data up to the moment and gives figures as to the amount of drift. On the Air keys the call signs are set forth and should present no difficulty. On the Army keys the M serials and rows refer to the call-sign book commonly known as the E book. There is, however, no use in sending this to you because it is used with an additive which changes daily. It would be practically impossible to recover this on Fish traffic alone. If you want the E book plus a daily cable as to the additive please advise. Logs for 3 days each on 4 different links are also enclosed. The final enclosure sets forth identified or suspected Q code values.

6. SSA 2200 has just been received. I am completely at a loss to understand the opening sentence which reads "Received F-61 which answers SSA 2101 as to Fish status." I can find nothing in my Report #F 61 which answers any question in SSA 2101. The suggestion that tapes could be regenerated is not applicable to any of the Fish material that has heretofore been sent to you. None of this had been worked on here and consequently original tapes had not been perforated. If, in the future, any traffic is sent to you on which tapes have been prepared here, it will be possible to send the originals or make duplicates. If no tapes have been prepared I would be reluctant to request that this be done unless we gave plenty of advance notice so that idle moments could be utilized to do this work. I suggest, therefore, that you endeavor to give me some idea now as to what you are likely to want during the next 5 or 6 weeks. It seems to me that emphasis should be on rectangle analysis rather than on setting. Setting problems seem useful primarily as a means of testing equipment reasonably well adapted to do the job. I would not include the IC plate machine

SECRET

DECLASSIFIED

Authority NWD 96 30 16
By SB NANA, Dala

SECRET

pg 3
3642
Report #P-67

in this category and from the little I know about the 70 mm. comparator I doubt whether it qualifies for inclusion. When the IC film machine is ready the situation will be substantially different. Possibly you would like to work on some solved Green or Jellyfish traffic. With this you would have the advantage of being able to check your results but the disadvantage of contributing nothing to operations. In any event please give us as much advance notice as possible as to future requirements. With respect to the final question in SSA 2200 - GOCG has a photostat of the T52C handbook. I was about to arrange to get a copy to send you with a report I am writing on some aspects of the permutation machine problem. You realize, I am sure, that the machine covered by T 52C is not the machine described in Report #7 45.

7. An outline of current procedure at Knockholt may help to clarify the tape situation discussed in the preceding paragraph. There are 3 methods of reception, namely, undulator tape, hand and teletype tapes. The first is the most accurate and reliable. Teletype tapes are the exception rather than the rule and can be obtained only when conditions are very good. Even then these tapes are never worked with. The working tapes are perforated from the Red Forms after checking against undulator tapes. The only function of the teletype tapes is to resolve ambiguities and at the moment the complete discontinuance of this type of reception is under consideration. Obviously working tapes are prepared only on traffic that is being currently processed.

Walter J. Fried
Capt. Signal Corps

Encl. - 6 pages
4 envelopes
7 pages
4 bundles of logs
5 pages

SECRET

DECLASSIFIED
Authority NWD 96 38 12
By SB NWA, Dala

ARMY

SECRET

1. e 4
IL 3643
Report #7-57

BRKAM

A. BROKEN DECHI'S.
(PRINTED DECHI, DECHI TAPE AND DUPLICATES DECODE)

<u>Tape No.</u>	<u>Motor Key Date.</u>	<u>Wheels.</u>	<u>No. of Dots '137' Wheel.</u>
167	3rd June.	A	27
277	22nd "	B	21
279	22nd "	B	21
283	22nd "	B	21
285	22nd "	B	21
287	23rd "	B	21
297	23rd "	B	21
302	24th "	B	21
310	21st "	B	21
318	26th "	B	21
325	29th "	B	21
326	29th "	C	21

B. UNBROKEN DECHI'S.

<u>Tape No.</u>	<u>Motor Key Date.</u>	<u>Wheels.</u>	<u>No. of Dots '137' Wheel.</u>
157	29th June.	B	21
261	18th "	A	27
121	25th "	B	21
134	26th "	B	21
135	24th "	C	21

THESE UNBROKEN DECHI'S ARE THE BEST WE CAN PROVIDE.
NONE CAN BE TAKEN AS BEING DEFINITELY SET ON ALL FIVE WHEELS.

ARMY

SECRET

DECLASSIFIED
 Authority NWD 96 30 14
 By SB NARA, Dalh