Copy 8 of 8 copies

SECRET

I/L 599-A
Report #P-55
2 July 1944

IL 3599

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

1. Enclosed are Mr. Newman's comments on the Fish information contained in Monthly Information Letter # 2 and Annexes B and F. Although I don't feel competent to enter into the mathematical phases of the discussion my feeling about the Jacobs method is that it confuses the eventual goal of a rectangle with a high overall score with the means to that goal which is the matching of rows and columns. It seems to me that the Jacobs test is "Which pair of rows (or columns) if matched (or mismatched) will contribute most heavily to the final score" rather than "Which pair are the most likely match (or mismatch)". Since combining of rows and columns results from the data produced by the test it would seem that the second question is the proper one. It may be demonstrable that the answers to the two questions are identical but if this is so how can the accurate method be theoretically fallacious? At any rate it yields probabilities which are essential when several messages are being worked on. A possible advantage of the Jacobs method is that it involves no assumption as to the a priori probability - but the same argument could be used in favor of matching by cross-producting excesses. Mr. Newman advises that some time ago they considered a method similar to the IBM method but using only 6 rows at a time. However, their calculations showed that it wasn't sharp enough and this is the occasion for the question in paragraph 4 of his notes. In the IBM method why do you use blocks of 9 instead of 8? Presumably this sharpens the results but doesn't it increase the danger of error if the rows which are used twice happen to be abnormal? And, of course, it increases substantially the number of tests required. The people here would like to know the time factors involved in the IBM procedure.

2. I mentioned in Report # P-50 that the Jellyfish patterns changed on 14 June. The wheels were broken on traffic of 18 June (through a crib from Bream) but only messages of that day could be set. This led to the suspicion that the wheel patterns were changing daily but since 137 only had 20 dots it was by no means certain. However, 24 June has now been solved (also through a Bream crib) and the patterns are different. This time 137 had 28 dots and messages as short as 1100 letters of 24 June have been set. No other day can be set on these patterns so it is reasonably certain that they are now changing daily. As a result, principal reliance is now being placed on attempted solution through cribs although rectangle analysis on this link has not been abandoned.

ARMY

SECRET

3. Grilse, a new link between Berlin and somewhere in Northern France, was solved for the first time a few days ago. The solution was statistical on a single message of 10,000 letters. It is the only long message of that day (21 June) and no other messages can be set. Attempts to set 5 long messages of other days have been unsuccessful so it looks as though the patterns change daily here as well. The limitation is $\bar{I}_2 + \bar{P}_5$. 37 had 27 dots. Thus far traffic on this link has been very light. There were only 15 messages of 1500 letters or more during the entire month of June.

4. Bream wheels changed on 22 June and have been solved. 37 had 21 dots. Messages of subsequent days are being set on these patterns. No effort has yet been made to set Codfish traffic on the new wheels.

5. Gurnard patterns continued in force without change up to the end of June.

6. Stickleback traffic seems to have been discontinued for some time but has shown signs of revival during the last few days. Some Key messages were being run up until a few days ago.

Walter J. Fried
Capt. Signal Corps

Encl. - 1 page

SECRET

TO:- Captain Fried
FROM:- M.H.A. Newman.
FROM:- 28th June, 1944.

Notes on 'Solution of a Rectangle' and other paper.

1. We are very interested to have your experimental evidence that the same pattern is yielded by different starts. We are not quite sure how the starts were made, and should very much like to know about this.

2. We should be grateful to have the reasons why Pte. Jacobs thinks 'accurate scoring', i.e. presumably the 'slide-rule' method based on the formula

$$\frac{1+\zeta^{\theta+\theta'}}{\zeta^{\theta}+\zeta^{\theta'}}$$

for combining rows, is theoretically fallacious. It is surely a straight deduction from Bayes' Theorem. Perhaps he means 'accurate converging', which we would agree is logically attackable? In any case we should be interested to hear the argument.

3. The problem solved in Annex B seems to be rather what we call the 'preliminary flag', for making a good start, than the convergence of the rectangle. As the American experiments have strikingly confirmed, a single rectangle can give only a partial solution. To pick up other messages, and hence gradually to get the complete wheel, we need to know which characters to believe and which to doubt, i.e. we want probabilities as the values of $f_i + g_j$ not, ± 1 merely. This is done in the converging process.

Our present practice is as follows:

A flag is first made on what appear at sight to be the best 8 or so rows, the answers to this process giving x or . or 'doubtful'. This 'partial wheel' is taken as the starting point for crude convergence, and the results are run as partial wheels on Colossus, to pick up other messages. With their help, crude converging is continued on Colossus. 'Accurate converging' is now rarely done. We have also used the flagging of the 'skeleton rectangle' as starting point, i.e. the rectangle marked -1, 1, or 0 as $\theta_i < -k, > k$ or between $\pm k$ for some suitable k. This can be flagged rapidly for the whole rectangle and has given good results.

4. The IBM procedure seems a practical and interesting one. Have calculations been made of how the expected 'bulges' on 9 rows compare with the standard deviation?

ARMY

SECRET