opy 8 of 8 copies TOP SECRET

3892-A
Report #F-101
14 October 1944

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

1. The following days have been solved since my last Fish report:-

Key	Date	Ψ_{37} dots	Method
Broem	24 Sept.	20	Crib
	25 Sept.	22	Rectangle
	28 Sept.	21	R
	3 Oct.	27	R
Gurnard	19 Sept.	15	C
	22 Sept.	26	R
	23 Sept.	25	R
	24 Sept.	21	C
	2 Oct.	21	R
Bleak	19 Sept.	24	D
	26 Sept.	18	D
	6 Oct.	24	Dragon
Whiting	11 Sept.	23	D
	3 Oct.	27	R
Stickleback	28 Sept.	20	R
	29 Sept.	23	R
Shad	22 Sept.	20	D
	26 Sept.	15	R(chis),D(psis)
	30 Sept.	24	R
	9 Oct.	27	D
Bullhead	28 Sept.	16	R
	8 Oct.	28	R
Jellyfish	7 Oct.	27	R
Grilse	3 Oct.	27	C

2. Shad is a Belgrade link which uses Stickleback patterns and limitation. Bullhead is a Finnish link to a place called Rovaniemi. Its limitation is $X_2 + P_5 + \Psi_1$ but the P_5 is sometimes dropped.

3. In the solution of Shad of 26 September the chi patterns were derived from a very long message but the psis could not be recovered because of the low number of Ψ_{37} dots. However, a depth was found and anagrammed yielding 100 elements of key. X_2 was removed in 31 different positions and the resultant patterns examined to see which was the most likely looking Ψ_2'. It was known that the number of motor dots must be low so the approximate point where Ψ_2 should start to repeat was known. This aided identification and actually the correct pattern turned out to be the first one tried. Some motor values were not derivable and this assisted the further work on other impulses. Impulse 5 was worked on next because it involved fewest trials on X_5. It would seem that it might have been easier to go next to impulse 1. Although this would have meant 41 trials of X_1 settings, a longer repeat in Ψ_1 would have been available. Also, since the limitation was $X_2 + \Psi_1$, after completion of this wheel all elements of the limitation would have been known.

TOP SECRET

4. The Shad solution of 9 October was completed on 9 October within 10 hours of the receipt of the messages constituting the depth. The statistical solution of Bullhead of 28 September with only 16 motor dots was facilitated by reason of the fact that the operator had, for some unknown reason, tapped out / about 500 times in succession.

5. I have obtained a write-up of the new theory which is being applied in breaking key. This is the procedure referred to in paragraph 2 of Report #F-96. However, the document would be virtually impossible to understand without a great deal of preliminary explanation. Mr. Small is studying it and in due course it will be sent on to you with such additional material as is necessary to make it clear. Since you are not working on this phase of the problem I don't imagine there is any urgency about forwarding it. Bleak chi and psi patterns of 6 October were derived by this method from less than 200 elements of key. Experimental work is also being done in resolving key by rectangling.

6. During September over 2½ million letters of plain text were produced by the Fish section. September interception was about 40 million letters (exclusive of Sturgeon type links) but a large portion of the traffic is contained in transmissions too short to be subjected to statistical treatment. A general idea as to how transmission lengths run can be gleaned from the following table which is for the week ending 1 October 1944.

Length	No. of transmissions
0 - 1499	4448
1500 - 1999	351
2000 - 2499	212
2500 - 3649	274
3650 - 5999	291
6000 - 9999	176
10,000 plus	83
Total	5835

Except in rare instances nothing whatever is done with transmissions of under 2000 letters. Although the weekly tabulations, of which the foregoing is a typical sample, are not expressed in terms of numbers of letters falling into the various categories, it would seem as though at least half of the total letters intercepted are contained in transmissions under this minimum length. All statistics of this kind are kept in terms of transmissions rather than messages because messages are commonly run together and the number contained in a transmission can only be determined after solution.

7. During the week ending 8 October Mr. Newman's section decried 182 transmissions. This is the largest weekly total to date. After daily changes of patterns were introduced there was an immediate substantial decline in production followed by a gradual rise and it is particularly noteworthy that this record surpasses the best that was achieved while patterns remained in force for monthly periods.

8. Dragon has produced 19 solutions in the first week of operations. Not only is this a substantial contribution to p roduction (the number of transmissions per week currently set on psis by Maj. Tester's section being between 80 and 100) but it has made possible the reading of many messages which could not have been solved by hand because of the low number of motor dots. The time of the machine has not been entirely devoted to operations because a lot of experimenting is still going on. Runs are being made to determine empirically the number of stops and trials to be expected on cribs of various lengths. This is not hard to calculate for random psi patterns but for actual patterns with varying values of b experiment will probably furnish the most reliable statistics. Dragon has not yet been used in connection with recovery of psi patterns but probably will be tried for this purpose in the near future. A problem now receiving consideration is how best to use Dragon when it is suspected that one of the chi patterns is incorrectly set. What is then desired is to make a run on 4 impulses only. This can be done by forcing a constant match on one Baud through modification of the dechi tape but it would be much easier if the machine itself could be adapted to eliminate any desired impulse. The engineers here, with the help of Sgt. Collins and your circuit diagrams, expect to look into this problem shortly but you may receive a cable asking for suggestions.

9. There has been some slip-up or other in deciphering the message on which you originally broke April Gurnard (your message # 10). I am informed that it will be typed in a few days. Enclosed is deciphered version of the other message (your # 92) qn which you have sent a complete solution.

10. Enclosed is full text of material on plates of the Sturgeon-type machine at Knockholt. This was requested in SSA 4355.

11. About 4 months ago Mr. Welchman was placed in charge of all captured cipher machines. Enclosed is his inventory of all items which have arrived here since that time. The most interesting are the T 52c and T52d. Although they are badly smashed efforts are being made to reconstruct them. There seem to be at least 7 different T52 models which have been solved or seen or referred to in traffic or captured documents and I have been trying to dig out what information is known about each of them. However, the situation is very confused and it will have to be studied further before an intelligible report can be prepared. Several notions that had developed from the traffic have been shattered by the physical evidence of the machines. It is found, for example, that the captured T52c is also T52a/b and can be transformed from one to another by a switch. Also the Germans have changed designations because this T52c is definitely not the same as the old T52c which was the "pentagon" model. (See "pentagon" in Cryptographic Dictionary). The most interesting fact about the T52d is that it contains a switch marked KTF which throws in the auto-key element. (KTF = klartext funktion). Without the auto-key this model seems to be the one described in Report #F 46 (IL 3601). When the KTF switch is thrown on the motor relations of the wheels are altered. The tetrad is eliminated and which wheels drive which is now dependent on the plain text. It seems that 4 different sets of motor relations are possible (but always with each wheel driven by two of the others) so it looks as though at least 2

plain-text impulses enter into the picture. All of these conclusions are extremely tentative. The tetrad, whose purpose was to avoid the possibility of a short cycle, is not needed when the periodicity is eliminated by the auto-key. There is no switch for eliminating the motor action as was suggested in Report #F-46 (IL 3601). The non-motorized traffic was probably transmitted on another model - very likely the new T52c.

Walter J. Fried
Capt. Signal Corps

Encl. - 12 pages
1 page
2 pages

TOP SECRET

COPY

TOP SECRET

To: Miss Mortimer, Station 'X'.

From: Mr. H.C. Kenworthy, F.O.R.D.E., Knockholt.

Date: 1st October, 1944.

Ref: 38/1741/

Dear Miss Mortimer,

Re: PLATE DETAILS OF MACHINE.

I think these are the details Colonel Rowlett requires:-

Lable on left hand side:

Siemens & Halske
Type T typ 52b V 220 ac
No.34388 Lokal 2 x 60 =
Alphab 32 50 Bd Ausfg. 1° 41

On the right is a Switch plate marked:

Aus
Klar Geheim Tastatur Loschstreifen.

Yours sincerely,

(sgd) H.C. KENWORTHY.

TOP SECRET

TOP SECRET

TOP SECRET 2.10.44

Attached is a list of captured machines which have now been put in my store room in Block H.

W. G. Welchman

A.D.(Mch).

Distribution
Director
D.D.4.
D.D.(N.S.)
D.D.(A.S.)
D.D.(M.M.)
D.D.(C.S.A.)
D.D.(C.T.)
A.D.(C.C.H.)
Capt. Fried (3)
Lt. Eachus
I.E.
File

TOP SECRET

TOP SECRET

3.10.44.

INVENTORY OF CAPTURED MACHINES

IN BLOCK H. STORE ROOM

1. Italian Alpha Machine. No. 00069/0. In good condition.

2. 5 German "E" Machines. (3 Wheel Machines) Nos. A 6941, A 8828, A 00289, A 10596, A 14710. All very badly damaged.
Also two sets wheels I to V badly damaged.
Machine No. A 00289 has special 30-way plugboard for printing attachment.

3. 3 German "E" Machines (Naval 4 Wheel Machines) Nos. M 6305, M 6383, M 16233. All very badly damaged.

4. German Teleprinter Cypher Machine. Type 52c. No. 53041. Manufactured 1944. Damaged and incomplete. No wheels and wiring connections cut. Also badly damaged switchboard.

5. German Teleprinter Cypher Machine. Type 52d (?). No. 21305. Manufactured 1945. Almost completely destroyed.

6. Teleprinter No. 076. Incomplete and very badly damaged.

7. 62 "T" Machines. Nos. 241-258, 260, 266-270, 301-340, each machine complete with one set of 5 wheels.
Also 5 wheels No. T 265.
All in perfect condition.

8. Hagelin Machine. Type B 21 1. No. 460. In good condition.

9. 12 Hellschreiber Machines. Type THS/24a-32. Nos. 3155/6, 2769, 2889, 3110, 3501, 3654, 3928, 4190, 4396, 4426, 4618, 4768.
Machine No. 3155/6 incomplete, remainder in perfect condition.
Also one spare Hellschreiber Motor.

10. Keyboard, Printer etc. Marked MZSE No.187. Badly damaged. Presumably printing attachment, for use with "E" machines.

11. Small unidentified 24-way switch.

TOP SECRET