

TOP SECRET

4061  
Report #F-118  
21 November 1944SUBJECT: Fish Notes  
TO : CO, SSA, War Dept.

1. Enclosed is Sixta non-Morse report for week ending 16 November 1944.
2. Enclosed is Dragon report for week beginning 10 November 1944. A few explanations may be helpful. Obviously Dragon is most helpful on low dottage messages because these are difficult by hand methods. But aside from this Dragon works much better with low dottage because the settings at the correct stop are more likely to be unique or almost unique. If the dottage is high the psi patterns contain many self-matching stretches and as a result a multiplicity of settings are possible. This tendency is aggravated by the fact that the high dottage causes many deletions so that only short stretches are available for matching. Extending the break found by the machine is likely to be very difficult - in fact, this is the most difficult part of the hand process. Consequently Dragon saves virtually no time when the dottage is high. The probability of random stops is lower with high dottage because there are fewer different stretches of pattern. However, the probability of such stops with a 10 letter crib is so low that this is an insignificant factor. Although the danger of missing a correct stop is increased with low dottage (see Report #F-111) this also is not an important factor.
3. The wheel-breaking experiments tried on Dragon were not very successful. The idea of setting up artificial psis and getting a stop if there are either 3 deletions or an agreement on the artificial patterns does not seem too useful because the probability of an agreement on all 5 artificial patterns is too low. What is really needed for wheel-breaking is a machine method of dragging a crib and scoring anti-repeats (and near anti-repeats) in the derived psis as well as the deletions. The scoring would be similar to that described in Monthly Information Letter No. 6, paragraph 5.
4. The suggestion of Dr. Cocombes for testing the consistency of a pair of breaks becomes important in high dottage cases where the possible alternative settings are many. If, for example,  $\psi 1$  were uniquely set for both breaks, the interval (in terms of unextended psi) between the two breaks can be determined because the dottage is known. If the distance is great the determination may be off by 43 in one direction or the other. The possible intervals for all pairs of settings on the other psi wheels can now be checked against the  $\psi 1$  figure. Usually all wheels can be uniquely set by this method, even though there isn't a unique pair on any impulse to begin with.
5. One of the new Dragons being built here will provide for cribs of up to 15 letters. This may prove highly useful where one of the chi settings is doubtful.
6. The following are all Fish solutions subsequent to those listed in Report #F-108, IL 3992. This list includes those mentioned by Mr. Small in Report #F-116, IR 4054.

TOP SECRET



# TOP SECRET

4061  
118  
Page 2

Key	Date	<i>N</i> 37 dots		Key	Date	<i>N</i> 37 dots		
Stickleback	27 Oct.	16	R	Gurnard	27 Oct.	25	R	
	1 Nov.	16	R		3 Nov.	24	D	
	2 Nov.	16	R		4 Nov.	24	D	
	3 Nov.	20	R		5 Nov.	25	D	
	5 Nov.	24	R		7 Nov.	26	R	
	7 Nov.	26	R		8 Nov.	27	D	
	11 Nov.	21	R		9 Nov.	27	R	
Jellyfish	30 Oct.	25	R	11 Nov.	27	R		
	15 Nov.	23	R	12 Nov.	27	R		
	16 Nov.	23	R	13 Nov.	28	R		
Bream	4 Nov.	26	R	Codfish	2 Nov.	22	D	
	7 Nov.	21	R		3 Nov.	24	R	
	8 Nov.	25	R		4 Nov.	26	C	
	9 Nov.	18	C		Whiting	28 Oct.	19	R
	11 Nov.	24	R			2 Nov.	19	R
Lumpsucker	17 Nov.	24	R	3 Nov.	25	C		
	5 Nov.	26	D	8 Nov.	25	R		
	18 Nov.	26	D	28 Oct.	16	D		

7. Production continues to increase. October surpassed all records but November is already far ahead. Through the 19th the plain text letters produced exceeded 2,800,000 whereas for the corresponding period in October the figure was under 2,200,000. During October Maj. Tester's section solved an average of about 20 dechis a day. Now they frequently top 30 and a few days ago the solutions numbered 48. On each of 2 recent days over a quarter of a million letters of plain text were turned out. During the last 2 weeks of Sept. Mr. Newman's section required an average of 11 days to produce a dechi (from time of interception) and the minimum time was 7 days. During the first week in November the maximum time was 6 days, the average  $4\frac{1}{2}$  and the minimum 2.

8. Many keys now vary their limitations and as many as 3 different limitations have been observed on some links on a single day. Records are being kept and various studies being made. For the purpose of such records the limitations are designated as follows:  $X_2 = A$ ;  $X_2 + \psi_1 = B$ ;  $X_2 + P_5 = C$ ;  $X_2 + \psi_1 + P_5 = D$ . C and D never seem to be mixed but just about all other combinations of 2 or 3 limitations have appeared on the same day. Both C and D have lately been very rare. D was used on 1 Codfish message of 3 November and on 1 of 4 November and since then it has not appeared on any link. Bream is the only link that has used C in November. The enclosure entitled "Log Procedure Relating to the Use of 'Limitation' on Non-Morse Army Links" sets forth what is known about the manner in which the operators indicate the limitation employed.

9. Enclosed is up-to-date chart of Fish net-works.

10. Enclosed is document entitled "Guide to Non-Morse Army Callsigns (up to 31/10/1944) and Frequencies Corrected to 20th November 1944." In GCCS 8758 I advised that this was in course of preparation. However, the 1 November change in Army call-sign procedure delayed its production

# TOP SECRET

DECLASSIFIED  
Authority NWD 963816

TOP SECRET

4061  
F-118  
Page 3

and it has just arrived from Knockholt today.

11. Enclosed is current list of abbreviations used to designate the various Fish links.

12. Efforts are being made to read a Barbel (Naval link, Berlin-Oslo) depth of 3. It has been established that it is not Tunny so it is now assumed to be Sturgeon. The hope is that the T52C machine was used (only 256 possible alphabets) and that if this is the fact it will be possible to read a depth of 3. It is not believed here that it is possible to read a depth of 3 on the T52D (960 alphabets).

Walter J. Fried  
Capt. Signal Corps

Encls.

TOP SECRET

DECLASSIFIED  
Authority NND 963876



TOP SECRET

4061  
-118  
Page 4

DRAGON

Report No 4

Week beginning Friday 10th November, 1944

1. Production

12 messages broken. The machine was not used during the equivalent of three complete days, mainly owing to lack of suitable material. The material altogether during this week has not been good Dragon material.

2. One shift was spent on wheel-breaking experiments but without success: I shall be surprised if a satisfactory Dragon wheel-breaking technique can be worked out, though for low dottage days the machine should prove a useful auxiliary. The method at present employed very briefly is this:

- (a) Set the deletion switch at 3.
- (b) Plug up a set of artificial  $\psi$ s designed to set somewhere on each wheel the commonest 8 sequences of  $\psi$ s which arise.
- (c) Run a 10 letter crib (for shorter cribs the artificial  $\psi$ s should be different)
- (d) When the machine stops it will be because
  - (a) the  $\psi$ s set on the artificial wheels (very rare)
  - (b) there are three deletions.

The merits of any possible break may then be assessed by eye according to:

- (a) The number of wheels it sets on
- (b) The number of deletions.

The relative assessment of these 2 factors will vary according to the estimated dottage and it is proposed to have two sets of artificial  $\psi$  wheels according to whether the dottage is probably low or probably high.

Note: In cases where say 20 consecutive  $\psi$ s have been obtained in a hand break, it might be best to plug these up, replacing 20 of the artificial  $\psi$ s - any possible break which gives settings within this stretch might be of special interest.

3. Dr. Coombes has suggested a small electrical computator which quickly tests the consistency of breaks at any distance apart. It frequently happens that (e.g.) two plausible  $\psi$ ROEM91

TOP SECRET

TOP SECRET

4061  
118  
Page 5

breaks both impossible to "push" and (say) 1053 letters apart are abandoned and other runs made in the hope of better things, without recourse to any form of consistency test, because the work involved is rather more than the Dragon breakers can undertake. Dr. Coombes' machine is designed to make this test quickly. It would enable us to exploit more seven and eight letter cribs, the bother of whose ambiguous settings have hitherto outweighed the great merits of their high frequency of occurrence. This machine might perhaps be used on wheelbreaking problems at the stage mentioned in the "Note" to 2 above, and would of course be useful to hand breakers as well.

4. A statistical analysis of Whiting Riga language has now been made.

Mr. Small.

A. McIntosh

TOP SECRET

DECLASSIFIED  
Authority NND 963016



TOP SECRET

IR 4061  
F-118  
Page 6

OX/MSS SECURITY

UIFRA/ZIP/NMS.14.

LOG PROCEDURE RELATING TO THE USE OF "LIMITATION"  
ON NON-MORSE ARMY LINKS.

It has for some time past been clear that FUNDAMENT has the same meaning as QSG. This was especially brought out by references on Stickleback in September, when chat often occurred, before traffic was sent, as to whether FUNDAMENT 40 or FUNDAMENT 42 was to be used. Precisely similar references were made to QSG.

As references to Schlüsselzusatz 40 occur in the Schlüsselfernschreibverschrift, and as Zusatz 42 is known to be used on Non-Morse Army links (Tunny) it seemed very probable that FUNDAMENT referred to the encoding machine in use. This theory was substantiated by chat in a decoded Stickleback QEP of 13.9. Berlin asked "habt Ihr einen G-Zusatz 40 zur Verfügung? Fundament 40? .... Also Ihr habt Keinen 40 G-Zusatz mehr ..... gut .... danke sehr .... einen Fundament .... Also habt Ihr noch einen vierzigen .... gut ... gut". H.Gr.Suedukraine replied in clear "RR 1 FUND 40".

By the end of September these references to FUNDAMENT 40 had died out on Stickleback, and were replaced by references, as current on other links, to FUNDAMENT A and B. It is known from decode evidence (SB 3010, GDB 6414) that the two types of cypher attachment are Schlüsselzusatz 42A and 42B. A reference to "42A" was made on the Shad log for October 22nd, but the subsequent QEP was unfortunately not decoded.

However, decodes are available for traffic which has been preceded by references to FUNDAMENT or to QSG, and these have shown that the similar references to "QTQ" and "QTQ NN" which also precede traffic, do in fact refer to the same thing - the type of encoding machine, or, in other words, the limitation, in use.

Log evidence giving the two terms in close apposition can be cited:-

On Jellyfish for November 3rd, JP gave "QSU NN QTQ. ER FUN. A. ER QSW NN QTQ", and, in reply to "ER QTQ NN" from JB, said "QWP RR A." JP, admonished presumably for using the wrong terminology, agreed that he was using "FUNDAMENT A".

Again, on Remora for October 29th, RAV made "FUNDAMENT?" and Berlin replied "FUNDAMENT A". RAV then gave "RR NN QTQ".

A study of decodes available for the second half of October and the beginning of November, in conjunction with log evidence, revealed the following:-

1. Bresm.

References to QSG A and B do not normally occur on Bresm. Log references are confined to "QTQ NN" and "QTQ". "QTQ NN" was found to refer to QEPs which decoded on Chi 2 only limitation, and "QTQ" to those which were on Chi 2 and P5.

TOP SECRET

DECLASSIFIED

Authority NND 963846



TOP SECRET

4061

F-118

Page 7

Bleak, Codfish, Gurnard, Stickleback, Whiting and Shad.

On all these links, references to QSG A and B, and also to QTQ, are made; and they are all known to use Chi 2 or Chi 2 plus Psi 1 limitation. Log Chat on Bleak for 25th - 28th October, on Codfish for 25th - 28th October and 2nd - 4th November on Gurnard for 16th October, prove the equation

QTQ NN = QSG A = Limitation Chi 2 only.

MIT QTQ = QSG B = Limitation Chi 2 + Psi 1.

The Stickleback, Whiting and Shad evidence is scanty, but since 4/11, when SB gave "ER QJE FUNDAMENT RR FUNDAMENT BBB" there have been no further log references, and all QEPs decoded on Stickleback have been on Chi2+Psi1, indicating that instructions about limitations do hold good until a further statement is made, and do not merely refer to the next QEP or the rest of one day's traffic. This point has also been proved on Bream and on Codfish.

It would therefore seem possible to predict fairly accurately the limitation in force on these links, provided always that atmospherics do not swamp vital log chat.

There is however, one drawback - the existence of some QEPs having triple limitation - Chi2Psi1 P5. One November Codfish QEP only has been decoded on this. It was preceded by a ten minute QRX and some unrecorded chat; but other chat on this day fitted the theory of QTQ NN = QSG A = Chi2 only, suggesting that a 3rd Q-signal meaning "Add P5" exists. Gurnard for 27th October, however, shows conflicting evidence, as messages following "QTQ" were decoded on Chi2 Psi1 P5 and those after "QTQ NN" were on Chi 2 Psi 1. There were no unusual Q- signals on this day, and unfortunately no day was broken between 16th and 27th. The only chat of an unusual kind between these two dates occurred on 23rd. GDB asked QDZ what limitation he was using and GDZ gave "QZS QSG ROT B. ER QZS QSG ROT RR ER B." Shortly afterwards GDB gave "ER MIT QTG MIT QTB ve ER QTQ ER QSW QSG B". Thus it may be that the Rot reference stopped "QSG A = QTQ NN" up to Chi2 Psi1 and brought "QSG B = QTQ" to mean Chi2Psi1 P5. In November the situation was normal, with only 2 limitations in use.

The comparative rarity of this triple limitation, and the possibility that arrangements about it are made in cypher, make it difficult to find log evidence for known instances, and would make production of it very unreliable.

TOP SECRET

DECLASSIFIED

Authority NND 963016



## PROBABLE MEANING OF CURRENT LIMITATION CHAT ON ARMY LINKS.

<u>Link</u>	<u>Current Chat</u>	<u>Probable Meaning</u>	<u>Confirmed from Decode.</u>
ANGLER	QTQ NN QTQ	Chi 2 Chi 2 Psi 1	
ANGELFISH	No evidence.		
BASKER	No chat since 26/10 when QTQ NN given.		
BLEAK	QTQ NN QTQ	Chi 2 Chi 2 Psi 1	Yes
REAM	QTQ NN QTQ	Chi 2 Chi 2 P5	Yes
BULLHEAD	Very little evidence In October - QTQ NN QTQ	Chi 2 Psi 1 Chi 2 Psi 1 P5	Yes
CHUB	No evidence, probably resembles Codfish and Gurnard.		
CODFISH	QTQ NN = QSG A QTQ = QSG B (NB: Occasionally Chi 2 Psi 1 P5 has been employed. This has not been predictable on log evidence).	Chi 2 Chi 2 Psi 1	Yes
DACE	FUNDAMENT A FUNDAMENT B	Chi 2 Chi 2 Psi 1	
DEVILFISH	Probably using a different machine.		
FLOUNDER	No chat. Probably resembles Codfish.		
GRILSE	QTQ NN = QSG A QTQ = QSG B (NB: Prior to 30th October there were no references to QSG A, B, on Grilse. Before this date QTQ NN indicated Chi 2 Psi 1, and QTQ indicated Chi 2 Psi 1 P5.)	Chi 2 Chi 2 Psi 1.	
GURNARD	QTQ NN = QSG A QTQ = QSG B (NB: Occasionally Chi 2 Psi 1 P5 has been employed. This has not been predicatable on log evidence.	Chi 2 Chi 2 Psi 1	Yes



# TOP SECRET

4061

118

Page 9

<u>Link</u>	<u>Current Chat</u>	<u>Probable Meaning</u>	<u>Confirmed from Decode.</u>
JELLYFISH	QTQ NN = FUNDAMENT A QTQ = FUNDAMENT B	Chi 2 Chi 2 Psi 1	Insufficient evidence.
LAMPERN	Inactive since 3rd November. Probably resembles Whiting.		
LUMPSUCKER	QTQ NN = FUNDAMENT A QTQ = FUNDAMENT B	Chi 2 Chi 2 Psi 1 (Most usual)	Insufficient evidence
MULLET	No evidence.		
PERCH	QTQ NN (Most usual) QTQ	Chi 2 Chi 2 Psi 1.	
POLLACK	(Inactive since November 12th) QTQ NN QTQ		
REMORA	QTQ NN = FUNDAMENT A QTQ = FUNDAMENT B	Chi 2 Chi 2 Psi 1	
RUDD	(Inactive since 4th October) Probably resembles Bullhead.		
SHAD	(Inactive since 27th October) QTQ NN QTQ	Chi 2 Chi 2 Psi 1	Yes
SNAPPER	Probably using same key as ANGLER.		
SOLE	Probably using a different machine.		
SQUID	QTQ NN = FUNDAMENT A QTQ = FUNDAMENT B	Chi 2 Chi 2 Psi 1.	
STICKLEBACK	QTQ NN = FUNDAMENT A QTQ = FUNDAMENT B	Chi 2 Chi 2 Psi 1 (Most usual)	Yes
TURBOT	QTQ NN QTQ		
WHITING	QTQ NN = FUNDAMENT A QTQ = FUNDAMENT B	Chi 2 Chi 2 Psi 1	Yes

SIXTA.

19.11.44.

Distribution:-

W/Cdr. Oeser.

Lt. Col. Wallace

Lt. Col. Gadd.

Major Grant

Major Tester (3)

Major Tester (for Mr. Wood)

Major Morgan

Major M

Capt. Fried, U.S. Army.

Capt. Cowan

Dr. Newman (4)

File (4).

# TOP SECRET

DECLASSIFIED

Authority NND 963016