

4061 Report #F-118 21 November 1944

SUBJECT: 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 pais 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 pais 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. Coombes 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, φ 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 φ 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.



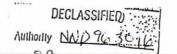
TOP SECRET

4061 118 Page 2

Key	Date		H 37 dots		Key	Date) 37 dots	
Stickleback	27 0	at.	16	R	Gurnard	27	Oct.	25	
	1 N	ov.	16	R		3	Nov.	2	
	2 N	ov.	16	R		4	Nov.	24	D
· ·	3 N	lov.	20	R		5	Nov.	25	D
	5 N	OV.	24	R		7	Nov.	26	R
	7 N	OV.	26			8	Nov.	27	D
	11 N	OV.	21	R		9	Nov.	27	R
Jellyfish	Control Section 1	at.	25	R		11	Nov.	27	R
	15 N	ov.	28	R		12	Nov.	27	R
		OV.	28	R		13	Nov.	28	R
Bream		lov.	26	R	Codfish	2	Nov.	22	D
av m agr samma	1000000000	ov.	21	R		3	Nov.	24	
		ov.	25	R		4	Nov.	26	Ö
		ov.	18	C	Whiting	28	Oct.	19	Ř
		ov.	24	R		- 2	Nov.	10	R
		ov.	24	R		3	Nov.	25	Ö
umpsucker		ov.	26	D	Grilse	ě	Nov.	25	Ř
was a company	THE PARTY OF THE P	ov.	26	Ď	Block	28	Oct.	ĩs	Ď

- 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 42 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: $X_0 = A$; $X_0 + Y_1 = B$; $A_0 + P_0 = C$; $X_2 + Y_1 = P_0 = D$. 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 Mon-Morse Army Callsigns (up to 31/10/1944) and Frequencies Corrected to 20th November 1944." In GCCS 8788 I advised that this was in course of preparation. However, the 1 November change in Army call-sign procedure delayed its production







7-118 Page 3

and it has just arrived from Knockholt today.

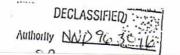
11. Enclosed is current list of abbreviations used to designate the various Fish links.

12. Efforts are being made to read a Barbel (Maval 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.





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 suxiliary. The method at present employed very briefly is this:
 - (a) Set the deletion switch at 3.
 - (b) Plug up a set of artificial γs designed to set somewhere on each wheel the commonest 8 sequences of γs which arise.
 - (c) Hun a 10 letter crib (for shorter cribs the artificial ψ s should be different)
 - (d) When the machine stops it will be because
 - (a) the ψ 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 ψ wheels according to whether the dottage is probably low or probably high.

Note: In cases where may 20 consecutive Ψ s have been obtained in a hand break, it might be best to plug these up, replacing 20 of the artificial Ψ 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 89ROEM94



TOP SEUNET 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



DECLASSIFIED Authority NAD 96 30 16

TOP SECRET

IR 4061 F-118 Page 6

QX/MSS SECURITY

ULF RA/ZIP/NMS.14.

ON NON-MORSE ARMY LINKS.

It has for some time past been clear that FUNDAMENT has the same meaning as QSO. 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. Frecisely similar references were made to QSG.

As references to Schluesselzusatz 40 occur in the Schluesselfernschreibverschrift, 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 GEP of 13.9. Berlin asked "habt Ihr einen G-Zusatz
40 zur Verfuegung? Fundament 40 ? ... Also Ihr habt Keinen 40 G-Zusatz
mehr gut ... danke sehr ... einen Fundament ... Also habt Irh
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 Schluesselzusaetse 42A and 42B. A reference to "42A" was made on the Shad log for October 22nd, but the subsequent QEF was unfortunately not decoded.

However, decodes are available for traffic which has been preceded by references to FUNDAMENT or to QEC, and these have shown that the similar references to "QTQ" and "QTQ NH" 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 Movember 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, a greed that he was using "FUNDAMENT A".

Again, on Remora for October 20th, 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:-

References to QSG A and B do not normally occur on Bream. 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.





_... 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 l 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.

NIT QTQ = QSG B = Limitation Chi 2 + Psi l.

The Stickleback, hiting and Shad evidence is scanty, but since 4/11, when SB gave "ER QJB FUNDAMENT RR FUNDAMENT BBB" there have been no further log references, and all RBPs decoded on Stickleback have been on Chi2+Psil, 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.

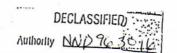
It would therefore seem possible to predict fairly accurately the limitation in force on these links, provided always that atmospherics do not swamp vital log chat.

There is however, one drawback - the existence of some QEFs having triple limitation -Chi2Psil P5. One November Codfish QEP only has been deceded on this. It was preceded by a ten minute QEX 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 Psil 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 Psil and brought "QSG B = QTQ" to mean Chi2Psil 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 preduction of it very unreliable.





TOP SERVE S Page 8

PROBABLE MEANING OF CURRENT LIMITATION CHAT

Link	Current Chat	Probable Meaning	Confirmed from Decode.
ANGIER	QTQ NN	Chi 2 Chi 2 Pai 1	
ANGELPISH	No evidence.		
BASKER	No chat since 26/10 when QTQ NN given.		
BLEAK	QTQ NN QTQ	Chi 2 Chi 2 Psi 1	Yes
REAM	CIC NH	Chi 2 Chi 2 P5	Yes
BUILHRAD	Very little evidence In Catober - QTQ NN QTQ	Chi 2 Psi 1 Chi 2 Psi 1 P5	Yes
CHUB	No evidence, probably resemble Codfish and Gurnard.	8	
CODFISH	QTQ NN = QSG A QTQ = QSG B (NB: Occasionally Chi 2 Psi l' has been employed. This has n predictable on log evidence).	Chi 2 Chi 2 Psi 1 P5 ot been	Yes
DACE	FUNDAMENT A FUNDAMENT B	Chi 2 Chi 2 Psi 1	
DEVILPISH	Probably using a different mac	hine.	
FLOUNDER	No chat. Probably resembles Co	ofish.	
GRILSE	QTQ NN = QSG A QTQ = QSG B (NB: Prior to 30th October the QSG A, B, on Grilse. Before t indicated Chi 2 Psi 1, and QTQ Psi 1 P5.)	his date QTQ NN	es to
GURNARD	QTQ NN = QSO A QTQ = QSO B (NB: Occasionally Chi 2 Psi 1 employed. This has not been p log evidence.		Yes



			PA	ge v	Confirmed
IAnk	Current Chat	Proba	ble	Meaning	from Decode.
J ELLYFISH	QTQ NH = FUNDAMENT A QTQ = FUNDAMENT B	Chi 2 Chi 2		1	Insufficient evidence.
LAMPERN	Inactive since 3rd November. Probably resembles Whiting.				10 A
Lumpsucker	QTQ NN = FUNDAMENT A QTQ = PUNDAMENT B	Chi 2 Chi 2		1 (Most	Insufficient usual) evidence
MULLET	No evidence.	у.			
PERCH	QTQ NN (Most usual) QTQ	Chi 2 Chi 2		1.	
POLLACK	(Inactive since November 12th) QTQ NN QTQ				
REMORA	QTQ NN = FUNDAMENT A QTQ = FUNDAMENT B	Chi 2 Chi 2		1	
RUDD	(Inactive since 4th October) Probably resembles Bullhead.				
SHAD	(Inactive since 27th October) QTQ NN QTQ	Chi 2 Chi 2		1	Yes
Shapper	Probably using same key as ANGLER.				
SOLE	Probably using a different mach	nine.			
SQUID	QTQ NN = FUNDAMENT A QTQ = FUNDAMENT B	Chi 2 Chi 2		1.	
STICKLEBACK	QTQ NN = PUNDAMENT A QTQ = FUNDAMENT B	Chi 2		1 (Most	usual) Yes
TORRUT	QTQ NN QTQ				
WHITING	QTQ NN - FUNDAMENT A QTQ = FUNDAMENT B	Chi 2 Chi 2		1	Yes
Distribution	n •=			SIXTA. 19.11.4	4.
W/Cdr.Oeser. Lt.Col.Walls Lt.Col.Gadd	Capt.Fried, U.S.Ar Capt.Cowan Dr.Hewman (4)	my.		1091101	,
Major Crant Major Tester	· (3) TOO OFFINE	2			
Major Tester Morgan	r (for Mr.				
- M					