Cryptologia
Publication details, including instructions for authors and subscription information:
http://www.tandfonline.com/loi/ucry20

Captured *Kriegsmarine* Enigma Documents at Bletchley Park

Ralph Erskine

Available online: 08 Jul 2008

To cite this article: Ralph Erskine (2008): Captured *Kriegsmarine* Enigma Documents at Bletchley Park, Cryptologia, 32:3, 199-219

To link to this article: http://dx.doi.org/10.1080/01611190802088318

Cryptologia, 32:199–219, 2008

ISSN: 0161-1194 print
DOI: 10.1080/01611190802088318

Taylor & Francis
Taylor & Francis Group

Captured *Kriegsmarine* Enigma Documents at Bletchley Park

RALPH ERSKINE

Abstract This paper lists Enigma-related *Kriegsmarine* documents captured by the British during the Second World War and describes the formation and functions of Naval Section VI, which dealt with captured documents in the British Government Code and Cypher School.

Keywords captured documents, Enigma, Government Code and Cypher School, Hut 4, Hut 8, *Kriegsmarine*, Naval Section VI, No. 30 Assault Unit, No. 30 Commando, Pinch

Introduction

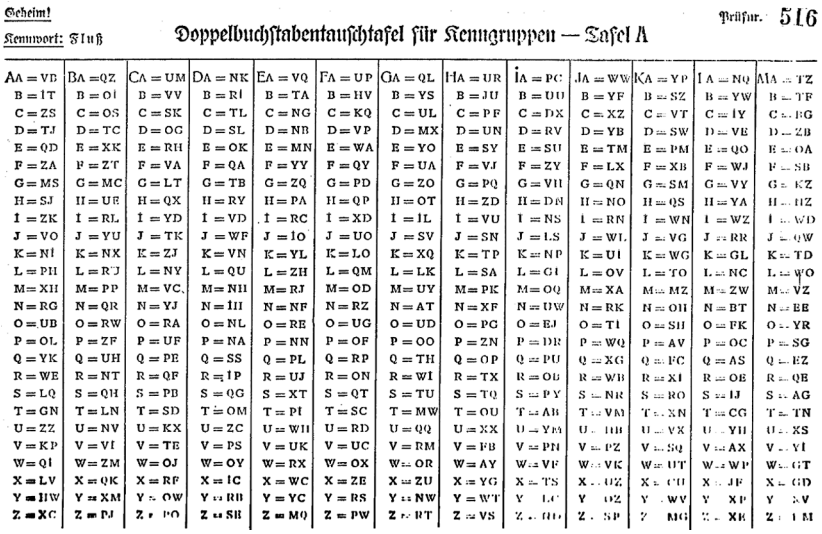
The document in the Appendix lists virtually all the important Enigma-related *Kriegsmarine* documents captured by the British during the Second World War. Many of them were critical to the success of the naval cryptanalysts in the Government Code and Cypher School (GCCS) at Bletchley Park in solving the principal naval Enigma cipher, *Heimische Gewässer* (home waters—codenamed Dolphin by the British, and later renamed Hydra by the *Kriegsmarine*), from 1 June 1941 onwards. The document was an appendix to a memorandum written on 21 June 1944 by Frank Birch, the head of Hut 4 (Naval Section) at Bletchley [6]. The memorandum was written in response to "CXG 746 of June 12," which was almost certainly sent by a GCCS liaison officer in the United States, following a query to him from the US Navy.

GCCS's Need for Captured Documents

GCCS needed captured documents in order to solve naval Enigma essentially for three purposes. First, to gain some insight into the contents of Enigma signals so as to be able to devise cribs (probable plaintext) for menus for the Turing/Welchman bombes (high-speed key-finding machines for Enigma). Next, to acquire detailed statistics about the linguistic content of naval Enigma signals, so as to refine cryptanalytical techniques. Lastly, to derive cribs from various manual ciphers, such as the *Wetterkurzschlüssel* (weather short signal book) used by the U-boats.

The need for good cribs is self-evident, but without actually seeing the plaintext of a substantial number of signals, Hut 4 and the naval cryptanalysts were working almost entirely in the dark: initially, Hut 4's self-styled " 'certain cribs' even became a standing joke" with the naval cryptanalysts [36, p. 27]. In August 1940, Birch deluded himself by believing that Hut 4 was producing cribs "of 90% certainty,"

Address correspondence to Ralph Erskine, c/o Parliament Buildings (Room 228), Stormont, Belfast BT4 3SW, Northern Ireland, U.K.



Geheim! Prüfnr. 516

Kennwort: Fluß

Doppelbuchstabentauschtafel für Kenngruppen — Tafel A

AA = VB	BA = QZ	CA = UM	DA = NK	EA = VQ	FA = UP	GA = QL	HA = UR	IA = PC	JA = WW	KA = YP	LA = NQ	MA = TZ
B = IT	B = OI	B = VV	B = RI	B = TA	B = HV	B = YS	B = JU	B = UU	B = YF	B = SZ	B = YW	B = TF
C = ZS	C = OS	C = SK	C = TL	C = NG	C = KQ	C = UL	C = PF	C = DX	C = XZ	C = VT	C = IY	C = BG
D = TJ	D = TC	D = OG	D = SL	D = NB	D = VP	D = MX	D = UN	D = RV	D = YB	D = SW	D = VE	D = ZB
E = QD	E = XK	E = RH	E = OK	E = MN	E = WA	E = YO	E = SY	E = SU	E = TM	E = PM	E = QO	E = OA
F = ZA	F = ZT	F = VA	F = QA	F = YY	F = QY	F = UA	F = VJ	F = ZY	F = LX	F = XB	F = WJ	F = SB
G = MS	G = MC	G = LT	G = TB	G = ZQ	G = PD	G = ZO	G = PQ	G = VH	G = QN	G = SM	G = VY	G = KZ
H = SJ	H = UE	H = QX	H = RY	H = PA	H = QP	H = OT	H = ZD	H = DN	H = NO	H = QS	H = YA	H = HZ
I = ZK	I = RL	I = YD	I = VD	I = RC	I = XD	I = IL	I = VU	I = NS	I = RN	I = WN	I = WZ	I = WD
J = VO	J = YU	J = TK	J = WF	J = IO	J = UO	J = SV	J = SN	J = LS	J = WL	J = VG	J = RR	J = QW
K = NI	K = NX	K = ZJ	K = VN	K = YL	K = LO	K = XQ	K = TP	K = NP	K = UI	K = WG	K = GL	K = TD
L = PH	L = RJ	L = NY	L = QU	L = ZH	L = QM	L = LK	L = SA	L = GI	L = OV	L = TO	L = NC	L = WO
M = XH	M = PP	M = VC	M = NH	M = RJ	M = OD	M = UY	M = PK	M = OQ	M = XA	M = MZ	M = ZW	M = VZ
N = RG	N = QR	N = YJ	N = HI	N = NF	N = RZ	N = AT	N = XF	N = UW	N = RK	N = OH	N = BT	N = EE
O = UB	O = RW	O = RA	O = NL	O = RE	O = UG	O = UD	O = PG	O = EJ	O = TI	O = SH	O = FK	O = YR
P = OL	P = ZF	P = UF	P = NA	P = NN	P = OF	P = OO	P = ZN	P = DR	P = WQ	P = AV	P = OC	P = SG
Q = YK	Q = UH	Q = PE	Q = SS	Q = PL	Q = RP	Q = TH	Q = OP	Q = PU	Q = XG	Q = FC	Q = AS	Q = EZ
R = WE	R = NT	R = QF	R = IP	R = UJ	R = ON	R = WI	R = TX	R = OU	R = WB	R = XI	R = OE	R = QB
S = LQ	S = QH	S = PB	S = QG	S = XT	S = QT	S = TU	S = TQ	S = PY	S = NR	S = RO	S = IJ	S = AG
T = GN	T = LN	T = SD	T = OM	T = PI	T = SC	T = MW	T = OU	T = AB	T = VM	T = XN	T = CG	T = TN
U = ZZ	U = NV	U = KX	U = ZC	U = WH	U = RD	U = QQ	U = XX	U = YM	U = HH	U = VK	U = YH	U = XS
V = KP	V = VI	V = TE	V = PS	V = UK	V = UC	V = RM	V = FB	V = PH	V = PZ	V = SQ	V = AX	V = YI
W = QI	W = ZM	W = OJ	W = OY	W = RX	W = OX	W = OR	W = AY	W = VF	W = VK	W = UT	W = WP	W = GT
X = LV	X = QK	X = RF	X = IC	X = WC	X = ZE	X = ZU	X = YG	X = TS	X = UZ	X = CU	X = JE	X = GD
Y = HW	Y = XM	Y = OW	Y = RB	Y = YC	Y = RS	Y = NW	Y = WT	Y = LC	Y = OZ	Y = WV	Y = XP	Y = XV
Z = XC	Z = PJ	Z = PO	Z = SB	Z = MQ	Z = PW	Z = BT	Z = VS	Z = GU	Z = SP	Z = MG	Z = XR	Z = IM

Figure 1. Page 1 of bigram table A from the "Fluss" set.

but that they were being ruined by Alan Turing and Peter Twinn,[1] both of whom he considered to be brilliant but "not practical." However, he had completely misunderstood the nature of the problem—it was Birch who was not practical in this context. He had wanted Turing and Twinn to use cribs with "100,000 possible answers," but doing so would have taken at least eight months—if there had been enough bombes and staff, both of which were in extremely short supply.

Turing invented a sequential statistical scoring system (later known as Banburismus) based on Bayes' theorem [26] to overcome the lack of bombes available for solving naval Enigma.[2] When operative, Banburismus cut down the number of naval rotor orders to be tested from 336 to between three and sixty, by enabling Hut 8 (naval Enigma cryptanalysis) to find which rotors were in the right-hand and middle slots of the three-rotor naval Enigma (M3) [2, p. 11; 36, p. 23]. Pairs of messages from the same day with the same first two letters in their *Verfahrenkenngruppe* ("procedure indicator group," but actually the message key) had to be compared at all positions from -25 to $+25$ by sliding one against the other [31, p. 19]. Hut 8 therefore needed to hold the current bigram tables used for enciphering naval Enigma indicators in Dolphin—either a captured set or one that had been reconstructed cryptanalytically. Each set contained nine reciprocal bigram tables, A to J (I was omitted) (for an example of a bigram table, see Figure 1). Ideally, 400 messages were required on a given day in order to employ Banburismus [2, p. 11]. With only 300 messages, Banburismus was still feasible, but some parts of it became "much more difficult" [31, p. 25].

Hut 8 also required detailed statistics about the content of the considerable amount of dummy traffic, since dummy signals distorted the application of Banburismus. Although dummy signals began with 30 to 60 letters of plain (but

[1]Peter Twinn had joined GCCS as its first mathematician in February 1939.

[2]No full description of Banburismus has appeared in print. However, for an outstanding article on it, which includes a Banburismus bombe menu, see [32]. The best archival account is [31], which includes considerably more detail than [2, pp. 94–109] and [36, pp. 20–24], including some of the tables used. [2] contains some statistically significant typos.

generally nonsensical) plaintext, their endings were a series of consonants, which gave a completely different repeat rate: if dummy traffic was not marked up and taken into account, Banburismus became difficult and sometimes impossible [2, pp. 26, 30].[3] Hut 8 therefore also needed a month's Enigma keys in order to analyse the relevant traffic and build up statistics on dummy signals.

First Captures

The capture of *Schiff 26* in April 1940 yielded the *Steckerverbindung* (plugboard connections) and *Grundstellung* (basic starting position for the rotors each day) for 23 and 24 April 1940, and a log giving the plaintext of signals for 25 and 26 April, which provided good cribs [36, p. 26]. The naval cryptanalysts used this material to read the traffic for 22 to 27 April. The first break was into the traffic for 23 April, which was solved on 11 May.[4] The signals for 22, 26, and 27 April were broken by Joan Clarke (later Joan Murray), with the help of the first bombe, Agnus, which lacked the diagonal board invented by Gordon Welchman. [36, p. 26; 41, p. 113] Clarke was a young mathematician recruited by Welchman, who had arrived at BP on 17 June, and was immediately put on to testing bombe answers, despite receiving only "the sketchiest of the introductions to the ENIGMA." A "column" menu was used. This took a cipher letter associated with its assumed plain equivalent for a single position of the fast rotor, treating that rotor and the *Stecker* as a set of non-reciprocal *Stecker*. The identity of the fast rotor was then irrelevant, which reduced the rotor orders to be tested from 210 to 42 for the rotors held by Hut 8 [40, p. 43], since the British did not capture rotor VIII until August [28, p. 957]. For this important work, Clarke was being paid the princely sum of £2 (then about $8) a week [41, p. 113].

Unfortunately, the capture of *Schiff 26* had been handled very badly. It should have been kept secret, but most of the sailors at Scapa Flow, the Royal Navy's base in the Orkneys, heard about it. Worse still, due to a series of errors, *Schiff 26* seems to have been looted before it could be examined carefully by naval intelligence [8, p. 43]. A subsequent naval inquiry cast doubt on the naval intelligence report [8, p. 43] into the looting, claiming that the officer who wrote it was "overwrought" [55, p. 75], but that appears to be an unwarranted criticism of a model intelligence report, perhaps because it had revealed the navy's shortcomings. After the war, Birch wrote that naval Enigma might have been "continuously forthcoming from [May 1940] on—a whole year earlier than in the event" if the looting had not taken place [8, p. 42]. While that view must remain speculative, it represents a reasonable scenario.

The first break using Banburismus did not take place until November 1940, when after months of work Hugh Foss broke 8 May (which became known as "Foss's Day" in his honour) despite the fact that others had already given it up. He found the "*Grundstellung* alphabets" for the middle and fast rotors (the mappings of all 26 letters of the alphabet at the second and third letters of the *Grundstellung*), and used them to derive a special bombe menu [2, p. 26; 36, p. 30; 41, p. 115]. Menus from Banburismus were different from those derived from cribs. The first Banburismus menu produced 256 stops, none of which was correct. Eventually, the staff in the bombe room asked a junior cryptanalyst to explain what was

[3]For a table showing the probability of repeats in *Kriegsmarine* Enigma traffic and in random German text, see [2, p. 96].

[4]The decrypts are in [25]; for the first decrypt, see [16].

being attempted and, to solve the problem, then fitted Agnus with a special "Banbury Circuit," which led to a good "stop" [58, p. 2].

Unsuccessful attempts were made in diving operations to recover Enigma documents from U-13, which had been sunk on 31 May 1940 off Lowestoft, and various plans to effect a "pinch" were proposed. Commander Ian Fleming (later the creator of James Bond), who was an assistant to the director of naval intelligence, put forward a hare-brained scheme to board a German air-sea rescue vessel by crash-landing a captured Heinkel 111 bomber with an armed crew, who were supposed to overpower the Germans and seize the ship's documents. Fortunately, this was never put into effect, since its chances of success were minimal, and it might have caused the Germans to increase Enigma's security. Hut 4 then proposed that *Schiff 26* should be sent under a German flag with a boarding party to seize a German aircraft security vessel, the *Bernhard Von Tschinsky*, in the Channel. Again, the proposal was not implemented; it too was impractical – in particular, the narrow waters of the Channel militated against it [22, p. 15]. Hut 4 later supplied detailed information in connection with the planning for the captures of the *München* and *Lauenburg* in May and June 1941. In a post-war internal history, Frank Birch described the capture of the latter as a "masterpiece of cooperation between Naval Section and the Navy."

"Einsing"

The February 1941 keylist captured from *Krebs* enabled the current bigram tables (called *Bach* by the *Kriegsmarine*) to be reconstructed. The first step was to read the individual messages in February and March with a method known as "Einsing," which was used to solve messages when the bigram tables were not known [41, p. 114]. About 90%. of non-dummy signals contained *EINS*, which was the most common four-letter word in *Kriegsmarine* Enigma traffic. In Einsing, *EINS* was enciphered at all 16,900 Enigma positions, using the relevant rotor order and *Stecker*.

The day's traffic was then searched for groups of letters that could be encipherments of *EINS*. Thus if XIDP was the result of encyphering *EINS* at rotor starting position UCL, and XIDP occurred in a message on that day's traffic, an Enigma was set up at UCL (with the day's *Stecker* and rotor order (*Walzenlage*)) and the cipher text entered. If the resulting plaintext read *EINS VIER*, for example, UCL was clearly correct (as happened in about one case in four), but if it read *EINS* XGWU, say, it was wrong and the *EINS* could be discounted as being random [2, p. 24; 36, p. 25]. If correct, UCL could then be used to derive up to three bigrams, since the bigram tables were reciprocal (see e.g. "FB" and "HV" in Figure 1). The captures of the keys for June and July 1941 (P/248 and 251 here) also greatly helped Banburismus.

Banburismus

GCCS had five bombes in June 1941, of which only one was generally available for Hut 8 work [2, p. 31]. To test all 336 rotor orders in full using a single bombe would have taken almost seven days, since on average a bombe could carry out about 50 runs each day. Without Banburismus, up to seven bombes might therefore have been needed to break a Dolphin key within 24 hours. The value of the bigram tables can also be seen from what happened when they were changed in June and November 1941. In June, the captured keys advanced Hut 8's ability to break Dolphin currently

by about two months, since it made reconstructing the tables, which had changed on 15 June 1941, a simple task [2, p. 31]. Without the tables, Hut 8 would have been forced to run a number of cribs on all 336 rotor orders, which would have been very difficult with so few bombes available for attacking all *Wehrmacht* Enigma. In early December, all GCCS's bombes had to be devoted to attacking the Dolphin key for 30 November [36, p. 57]. Fortunately, GCCS had 16 bombes then, although four were out of commission, due to maintenance problems [27, p. 748]. Although Hut 8 began to build up the tables quite quickly with the help of the bombes, the lack of the full tables made it impossible to resume Banburismus until January 1942, after a new *Kenngruppenbuch* (indicator book) and the *Strom* bigram tables from *Geier* reached Hut 8 on 1 January. This saved Alan Turing from having to start the laborious task of reconstructing the new book, with its 17,576 trigrams [36, p. 58].

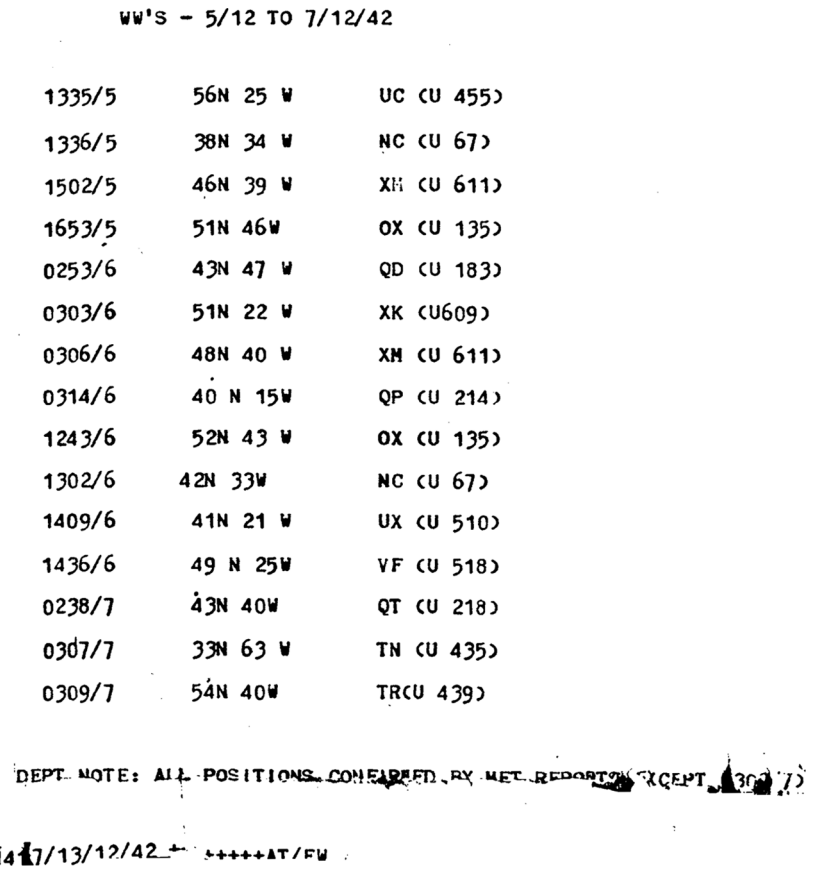
Banburismus required each day's traffic to be sent as it arrived to Bletchley's Hollerith (punched card) section under Frederic Freeborn, who recorded it and sorted the results to find all repeated groups.[5] Huge numbers of cards were required, since a card was made for each trigram in a signal: 500 signals with an average length of 150 letters therefore needed about 75,000 cards. Banburismus was crucial to Hut 8's speedy solutions of Dolphin until June 1943, when about 70 three-rotor bombes were in service [10], making it possible to run cribs on all 336 rotor orders if necessary; it was officially abandoned in September 1943 [2, p. 61]. Banburismus was generally only useful against the first day of a pair. In naval Enigma, the inner settings (rotor order and *Ringstellung*) were valid for two days (or occasionally one or three, mainly depending on whether it was a 31 day month). Once the first day of a pair had been solved with the help of Banburismus, it yielded the rotor order, so that Banburismus did not have to be used against the second day for that purpose. The second day of a pair was "always broken on a crib, usually very quickly" [2, p. 13]. From mid-1942 Banburismus was also employed against *Süd*, a key used in the Mediterranean [38, p. 7], even though it did not use the *Kengruppenbuch* indicating system or bigram tables [21, p. 233]. Banburismus could not be used to attack the four-rotor Enigma (M4), since about 7800 (26×300) messages would have been required in a day's traffic, and no traffic in an M4 cipher ever approached that figure.

Cribs from the *Wetterkurzschlüssel*

Hut 8 also derived cribs from manual ciphers. Thus weather observations by a U-boat were encoded with the *Wetterkurzschlüssel*, before being enciphered on Enigma. The *Kriegsmarine* shore control then deciphered and decoded the signal and sent it to a central meteorological station which rebroadcast the data as ship synoptics, after enciphering it with additive tables in a cipher called "Germet 3" by Bletchley (and also known by it as "the DAN meteorological cipher").[6] Since Germet 3 was being solved by Bletchley's meteorological subsection in Hut 10 from February 1941 onwards [37], Hut 8 had a good source of plaintext for bombe menus—but only when it held the relevant edition of the *Wetterkurzschlüssel* [2, p. 43]. Hut 8 derived cribs for bombe menus for Dolphin by using the captured *Wetterkurzschlüssel* (P 169 in the present list) to convert the Germet 3 data into the

[5]The procedures used in Freeborn's section for Banburismus, are described in [61]. My thanks to Brian Oakley for sending me this paper.

[6]On Germet 3, see [24].



WW'S - 5/12 TO 7/12/42

1335/5	56N 25 W	UC (U 455)
1336/5	38N 34 W	NC (U 67)
1502/5	46N 39 W	XH (U 611)
1653/5	51N 46W	OX (U 135)
0253/6	43N 47 W	QD (U 183)
0303/6	51N 22 W	XK (U609)
0306/6	48N 40 W	XH (U 611)
0314/6	40 N 15W	QP (U 214)
1243/6	52N 43 W	OX (U 135)
1302/6	42N 33W	NC (U 67)
1409/6	41N 21 W	UX (U 510)
1436/6	49 N 25W	VF (U 518)
0238/7	43N 40W	QT (U 218)
0307/7	33N 63 W	TN (U 435)
0309/7	54N 40W	TRCU 439)

DEPT NOTE: ALL POSITIONS CONFIRMED BY MET REPORTS (EXCEPT [illegible])

1417/13/12/42 +++++AT/FW

Figure 2. ZTPGU 1 (Source: PRO DEFE 3/705).

"plaintext" of the weather short signals sent by the U-boats. The fact that the "plaintext" was actually coded text was irrelevant.

The first edition of the *Wetterkurzschlüssel* was replaced on 20 January 1942 [56], depriving Hut 8 of an important source of cribs. When M4 took effect on Triton, the Atlantic U-boats' cipher (codenamed Shark by Hut 8), on 1 February, the result was the Shark black-out until mid-December 1942 [5, pp. 110–114, 152–157; 27, pp. 228–233, 747–752]. This ended only after Lt. Anthony Fasson and Able Seaman Colin Grazier,[7] with a 16-year old Naafi canteen assistant, Tommy Brown, recovered the second edition of the *Wetterkurzschlüssel* (P 936 in the list below) from U-559 after it was forced to surface following a prolonged attack. For some unknown reason, the documents from U-559 did not reach Hut 8 until 24 November, but they enabled Hut 8 to break into Shark on 13 December 1942 with the help of the data from Hut 10's Germet 3 decrypts (see Figure 2 for the resulting Shark decrypt, ZTPGU 1 [63]).[8] Sadly, Fasson and Grazier drowned,

[7]For photographs of Fasson and Grazier, see [55].

[8]Hugh Alexander, who was head of Hut 8 at the time, gives 7 November 1942 as the end of the Shark Black-out [2, pp. 38, 43]. However, this is definitely an error—he is probably referring to the earliest date for which Hut 8 read some of the back traffic.

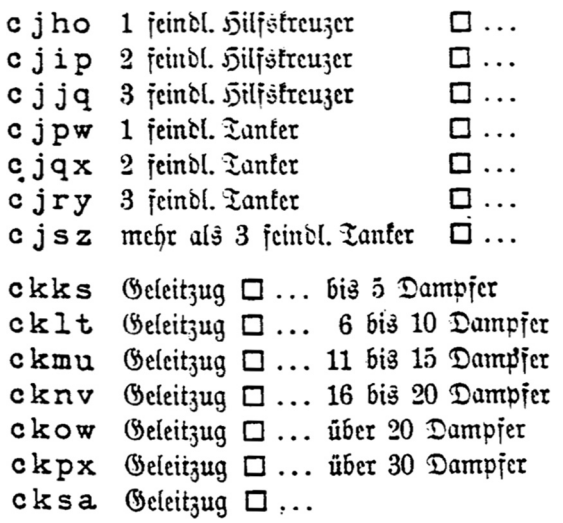
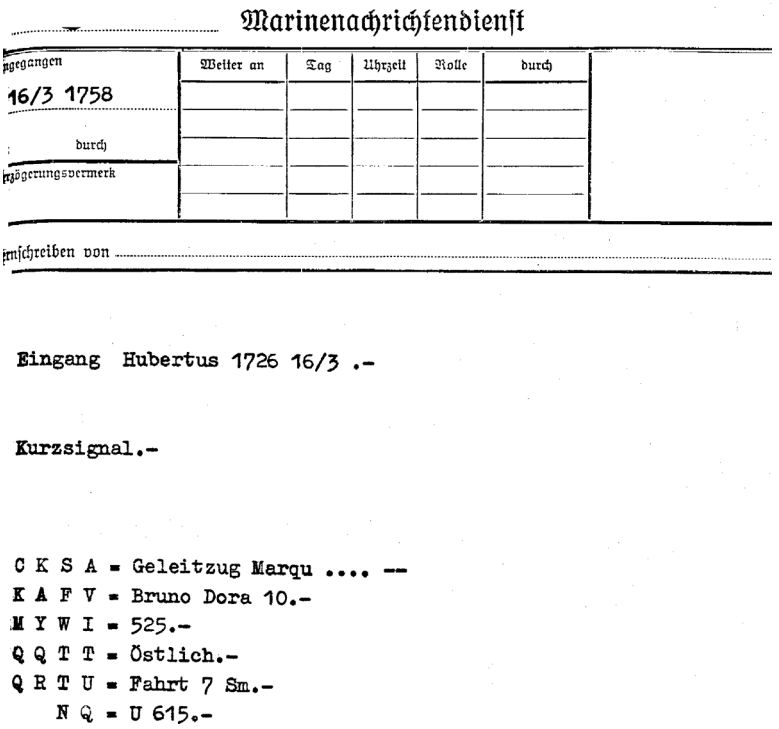


Figure 3. Excerpt from section III (*Feindmulgen*-enemy reports) of the *Kurzsignalheft*.

when U-559 sank suddenly. They had been trying to recover equipment, almost certainly a four-rotor Enigma. But Hut 8 had not needed an M4, making their deaths even more poignant, since Hut 8 had reconstructed the wiring of M4's new rotor and reflector (*Beta* and thin reflector B (*Bruno*)) at the end of 1941 [39; cf. 2, p. 36]. Unfortunately, even after the cryptanalysts' success in reconstructing M4's rotors, for some reason a Confidential Admiralty Fleet Order (CAFO) had required that "every effort should be made to capture" an Enigma [42]. Fasson and Grazier were awarded the George Cross (Britain's second highest medal for bravery) posthumously, while Brown became the youngest person to receive the George Medal [33, p. 226; 55, pp. 218–221].

When Hut 8 learned that the second edition of the *Wetterkurzschlüssel* was to go out of force on 10 March 1943, it despondently advised the Admiralty that it might be blind against Shark for "some considerable period, perhaps extending to months". Fortunately, it re-entered Shark within nine days using the *Kurzsignalheft* (P 255 below), which had also been seized by Fasson and Grazier. The *Kurzsignalheft* was a one-part short signal book comprising about 120 pages, arranged by subjects such as enemy sightings, positions, numbers and times (see Figure 3 for an excerpt from the *Kurzsignalheft* about convoy sightings. Note the group "cksa" (the square symbol means "naval [*Kriegsmarine*] grid square" [17]) and its use in Figure 4). Hut 8 used the text of signals encoded with the *Kurzsignalheft* to solve Shark for 90 out of the 112 days from 10 March to 30 June, mostly with cribs from short signals containing sighting reports of convoys.[9] With the help of the *Kurzsignalheft* and its detailed knowledge of past short signals, it guessed some of the letters used in "B bar" short signals such as the signal of 16 March 1943 from U 615 set out in Figure 4, and used them as very short cribs. In fact, the traffic for 16 March was broken on 18 March [49, p. 77]—the first Shark day to be solved after

[9]For examples of the way in which these short signals would have provided cribs, see [15, pp. 172, 173]; [53].



Marinenachrichtendienst

gegangen	Weiter an	Tag	Uhrzeit	Rolle	durch
16/3 1758					
durch					
zögerungsvermerk					

mschreiben von

Eingang Hubertus 1726 16/3 .-

Kurzsignal.-

C K S A = Geleitzug Marqu .... --
K A F V = Bruno Dora 10.-
M Y W I = 525.-
Q Q T T = Östlich.-
Q R T U = Fahrt 7 Sm.-
N Q = U 615.-

Figure 4. Beta short signal of 16 March 1943 from U 615 (commanding officer, Kapitänleutnant Ralph Kapitzky).

the third edition of the *Wetterkurzschlüssel* had come into force, depriving Hut 8 of "weather" cribs. The Atlantic shore direction-finding stations helped to provide Hut 8 with information about the positions of convoys and U-boats when using B bar cribs [2, p. 50]. But solutions of Shark were sometimes a week or more late; some 1943 days were not broken until 1945,[10] while a few were never solved.

Gap in the List

The list only covers documents, and not equipment. It therefore contains no reference to the three *Kriegsmarine* Enigma rotors (VI to VIII) captured by the British, which apparently had no PG numbers allocated to them.[11] Secondary sources have revealed that rotors VI and VII were taken from the survivors of U-33, when it was sunk near Ailsa Craig in the Irish Sea in February 1940, and that rotor VIII was captured in August 1940 [28, p. 957], although we know nothing about where or how it was seized. No primary source exists in any public archive about the capture of rotor VIII.

The documents listed below feature "P" numbers. However, the series was generally known as "PGs" (said to mean "pinched from the Germans"). There was a

[10]E.g. 2 June 1943 and 9 and 10 September 1943 were broken on 15 and 21 June 1945, respectively [49].

[11]Information from Naval Historical Branch (NHB), Ministry of Defence, Portsmouth.

similar but smaller series for captured Italian naval documents (''PIs''), and an even smaller set for captured Japanese naval documents (''PJs'') [1].

GCCS's "Pinch Committee"

Considerable thought was given by a ''pinch committee'' at GCCS to capturing a second ''Greek'' rotor (*Gamma* and its associated thin reflector C (*Cäsar*)) for M4 in 1943. GCCS knew that a *Kriegsmarine* radio station at Gabès, Tunisia, held those rotors, and believed that a raid on the station would be well worthwhile. It also proposed a dive against U-205, which had been sunk off Cyrene, Libya, on 17 February 1943. It is not clear whether the *Kenngruppenbuch* and *Zuteilungsliste* (allocation list) listed below (P 1568) were captured from U-205 as a result of such a dive, or in some other way.[12] Hut 8 could not solve *Cäsar*'s and *Gamma*'s wiring for several weeks after they were introduced on 1 July 1943. No M4 Shark traffic for July was solved until 19 July, when Hut 8 recovered the key for 16 July [49, p. 112]. It then used that key to solve their wiring. It should not have been necessary to do so, since they had in fact already been captured in North Africa. But they had not been sent back to England, because it was thought that GCCS already held all the rotors needed to break Shark [2, p. 61]!

A delicate balance always had to be struck when deciding whether or not to organise a pinch. Thus in 1942, when Shark was not being read during the long blackout, it was apparently decided that the risk of compromising the ability to read Dolphin was too great to allow a special pinch of Shark material to be attempted. Although the Admiralty issued CAFOs on the need for pinches of ''codes or ciphers,'' they emphasized the need to keep the capture of an enemy vessel secret, if necessary by sinking it.[13]

Naval Section VI and No. 30 Assault Unit

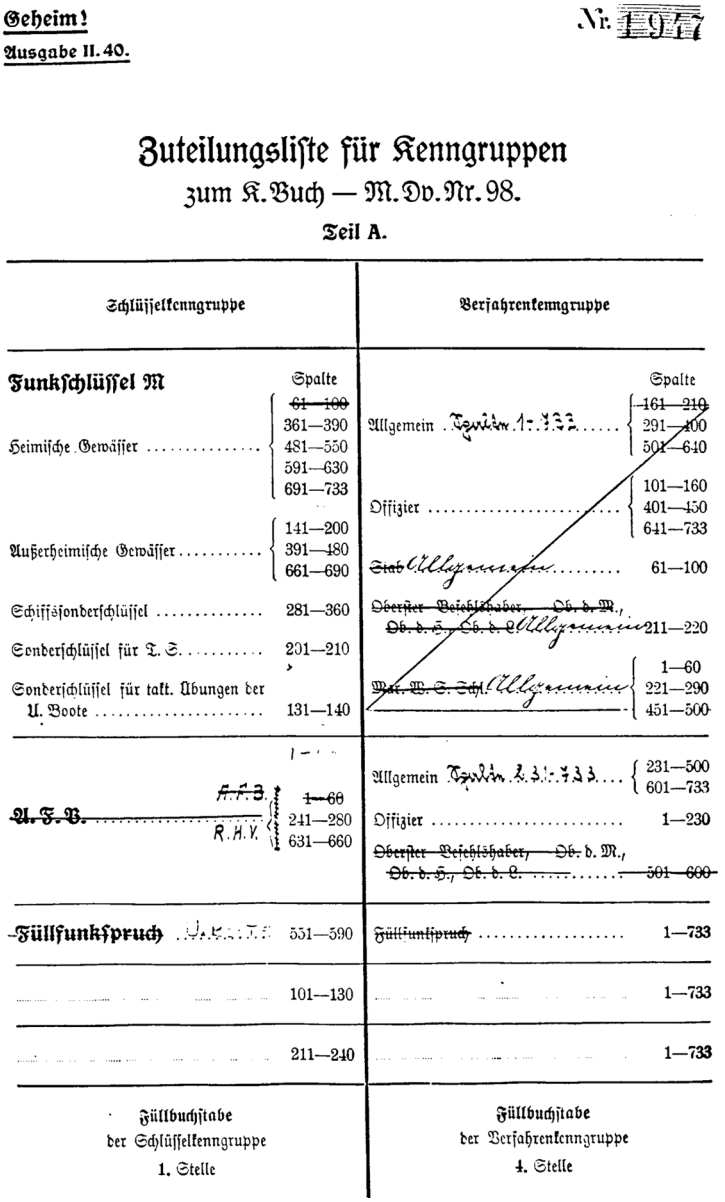
With success in breaking naval Enigma came problems in interpreting the language and abbreviations used, as had happened in early 1940 with *Luftwaffe* Enigma decrypts [57, p. 35].[14] Naval Section therefore set up a team of experts to translate and interpret the decodes; the experts then expanded their activities and derived technical intelligence about the enemy's weapons and equipment. They had to serve both GCCS and the Royal Navy.

In November 1941, Valerie Travis (the daughter of Edward Travis, who was later appointed as the operational head of Bletchley's services section) became responsible for all the captured documents received by Naval Section, while a Technical Intelligence subsection (Lieutenant-Commander Geoffrey Tandy and two others) carried out research and vetted, promulgated and

[12]See Figure 5 for a *Zuteilungsliste*.

[13]CAFO 879 of 7 May 1942 [51, p. 28].

[14]Hut 3 had not known the significance of such basic terms as *Fliegerkorps* (air corps—a flexible organisation comprising between 300 and 700 aircraft of all types, which usually controlled all the air units in a sector).



Geheim!
Ausgabe II. 40.

Nr. 1947

Zuteilungsliste für Kenngruppen
zum K. Buch — M. Dv. Nr. 98.

Teil A.

Schlüsselkenngruppe	Spalte	Verfahrenkenngruppe	Spalte
Funkschlüssel M	~~61—100~~	Allgemein	~~161—210~~, 291—400, 501—640
Heimische Gewässer	361—390, 481—550, 591—630, 691—733	Offizier	101—160, 401—450, 641—733
Außerheimische Gewässer	141—200, 391—480, 661—690	~~Stab~~ Allgemein	61—100
Schiffssonderschlüssel	281—360	~~Oberster Befehlshaber, Ob. d. M., Ob. d. H., Ob. d. L.~~ Allgemein	211—220
Sonderschlüssel für T. S.	201—210	~~Mar. W. S. Schl.~~ Allgemein	1—60, 221—290, 451—500
Sonderschlüssel für takt. Übungen der U. Boote	131—140		
~~A. F. B.~~ R. H. V.	~~1—60~~, 241—280, 631—660	Allgemein	231—500, 601—733
		Offizier	1—230
		~~Oberster Befehlshaber, Ob. d. M., Ob. d. H., Ob. d. L.~~	~~501—600~~
~~Füllfunkspruch~~	551—590	~~Füllfunkspruch~~	1—733
	101—130		1—733
	211—240		1—733
Füllbuchstabe der Schlüsselkenngruppe 1. Stelle		Füllbuchstabe der Verfahrenkenngruppe 4. Stelle	

Figure 5. *Zuteilungsliste* in *Kenngruppenbuch* seized from U 110.

issued equivalents of technical terms in the languages handled by Naval Section (German, Italian, Portuguese, Spanish and French). In 1942, the Admiralty assigned Naval Section the task of making its dictionaries of foreign terms, and of exploiting pinches.

Naval Section VI (NS VI) seems to have been established as such in mid-summer 1942. Its functions were:

(a) to provide expansions of abbreviations and technical equivalents;
(b) to keep, catalogue, index and distribute captured documents;

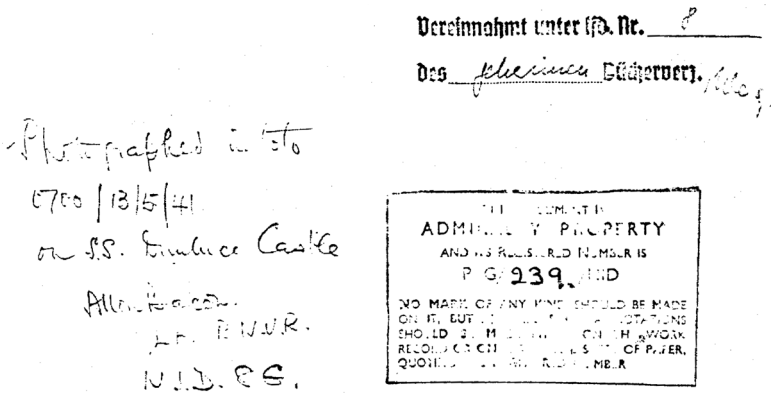


Figure 6. Annotation by Lt. Allon Bacon on *Kenngruppenbuch* seized from U 110.

(c) to examine messages to elucidate any difficulties, and provide information about enemy personnel, equipment and manufacturers.[15]

NS VI proved its worth sufficiently to have its activities endorsed in December 1942 by Commodore E. G. N. Rushbrooke, who had succeeded Admiral John Godfrey as the Director of Naval Intelligence. He issued a directive that all captured documents arriving in the Admiralty were to be screened by a representative of Naval Intelligence Division (NID) 12A (NS VI's cover name in the Admiralty) and NID 1/PW (the NID section that dealt with intelligence from prisoners of war). They were to be split into two groups: items for NID 12A only (code and cipher documents, although this was not spelled out), and those of interest to the Admiralty or other departments. NID was then to list all those in the second group, after which the list was to be circulated within the Admiralty. All the documents were to be transferred to NS VI, after they had been seen inside the Admiralty [52]. Following the December 1942 directive, NS VI acquired all the documents held by NID 1/PW, various Admiralty technical departments, and the Office of Strategic Reserves, and new photographic equipment was installed at GCCS to help NS VI meet its new responsibilities. The December directive was amplified in September 1943, to make NS VI responsible for helping to translate captured documents, if requested by NID [13, p. 10]. In early 1944, NS VI was also given the duty of registering all captured documents. By September 1944, NS VI comprised 24 staff.

Ian Fleming had been impressed by the results of *Abwehr* intelligence assault parties, *Marine Einsatz Kommando*, in Yugoslavia and Greece in 1941. He therefore persuaded Godfrey to propose the creation of a similar British inter-service group. Although the War Office and Air Ministry were less than enthusiastic, the Joint Intelligence Committee and Chiefs of Staff approved the creation of an intelligence assault unit to seize intelligence material of value to the three services. A unit with Royal Navy, Royal Marines and army sections was formed, and designated No. 30

[15]On NS VI, see [3], [51] and, for a somewhat jaundiced account (Tandy seems to have lacked good personnel skills), [9].

Commando (later No. 30 Assault Unit) [29; 43]. One of its main objectives was the capture of German and Italian Sigint material, including Enigma rotors, and the daily key settings for Enigma ciphers.[16]

In the fall of 1944, plans were made to establish about five joint British-American Target Intelligence Committee (TICOM) units, which were also charged with seizing Sigint documents. NID 24 was therefore established to share in translating them, and to act as an intermediary between NS VI and any Admiralty sections interested in German documents. A final directive of 10 March 1945, formally recognised this position [22, p. 10].

Conclusion

Unlike the British Army, the Royal Navy established good procedures to ensure that captured Sigint documents reached GCCS quickly, without being delayed by local commands. The creation of 30 AU was a very innovative step, although relatively few of the documents captured by it seem to have been of much benefit to GCCS. Without the documents captured by the Royal Navy, Hut 8's breaks into Dolphin and Shark would have been considerably delayed, with incalculable consequences. But ultimately, only the bravery and sacrifice of men such as Anthony Fasson and Colin Grazier made the major breaks into naval Enigma possible.

About the Author

Ralph Erskine is a retired barrister who has written extensively on signals intelligence in WWII. He is a member of the editorial board of *The Journal of Intelligence History*.

[16]For lists of targets for No. 30 Assault Unit, see The National Archives of the United Kingdom, Public Record Office (PRO), Kew, Surrey, ADM 223/349 (targets in Germany) and PRO ADM 223/501 (targets in 1944–1945).

Appendix

List of Captured Documents

DETAILS OF CAPTURE	DOCUMENTS CAPTURED	REMARKS
	VORPOSTENBOOT 2623[17]	
Captured in position 62° 37′ N, 4° E by H.M.S. Griffin at 1030 hours on 26 April, 1940[18]	P/115/NID Schlüsselzettel for 23rd, 24th, 25th and 26th April 1940 Cypher message pads[19]	Traffic for April was broken in June 1940
	VORPOSTENBOOT KREBS	
Sunk in Operation "CLAYMORE" (Attack on Lofoten Islands) 4th March 1941[20]	P/138/NID Schlüsseltafeln M-Allgemein Schlüsseltafel "Heimische Gewässer" Kennwort: HAU Cypher keys for home waters	These keys enabled us to read the traffic of February, 1941 and to reconstruct the bigram tables then in force.
	WETTERBEOBACHTUNGSSCHIFF MÜNCHEN	
Sunk in Northern North Sea by H.M.S. Somali on 9th May 1941[21]	P/168/NID Schlüsseltafeln M-Allgemein[22]	These keys enabled us to read currently the traffic on June 1941 ZTP/1218, T.O.O. 0017/1/6/41, was teleprinted at 0237/1/6/41[23]

(*Continued*)

[17]The *Kriegsmarine* seems never to have had a *Vorpostenboot* (patrol boat) 2623 in service. The vessel captured was almost certainly *Schiff 26* (and is so referred to in a number of Bletchley and *Kriegsmarine* documents), which was seized at this time [54], [59] (I am indebted to R. M. Coppock for these references). *Schiff* 26 was the captured *Julius Pickenpack*.

[18]On the capture of *Vorpostenboot 2623* (*Schiff 26*), see [30]; [50]; also [33, pp. 116–117]; [55, pp. 73–76]. Although [2, p. 24] and [36, p. 26] refer to it as "the Narvik pinch", the capture took place 60 miles west of the Norwegian port of Älesund, which is about 450 miles south-west of Narvik. Ålesund is at 62-28 N, 6-12 E. Narvik is 68-28 N, 17-26 E.

[19]*Schlüsselzettel* were cipher message pads on which the plaintext and ciphertext were written down. For an example in a *Kriegsmarine* manual, see [46, p. 14].

[20]On the capture of *Krebs*, see [33, pp. 130–136]; [55, pp. 116–118]; on the raid, Operation Claymore, see [12]; [35].

[21]On the capture of *München*, see [33, pp. 156–159]; [55, pp. 127–130].

[22]These were the general Dolphin keys for June. They arrived at Bletchley on 10 May 1941.

[23]ZTP/1218 is in DEFE 3/2 at the PRO. Although the translated decrypt was teleprinted (ZTP stood for "Naval Enigma, teleprint") to Naval Intelligence Division 8G in the Admiralty within a few hours, it is uncertain whether the time of origin in decrypts employed DGZ ("*Deutscher Gesetzlicher Zeit*"—German legal time, which was GMT + 1 hr., except during summer), which was used by the U-boats, or Greenwich mean time (as adjusted for summer time), so that a simple subtraction is not possible. The captured keys, indicator book (see the captures from U-110) and bigram tables enabled Hut 8 to read Enigma currently for all of June.

DETAILS OF CAPTURE	DOCUMENTS CAPTURED	REMARKS
	P/169/NID Wetterkurzschlüssel (Ausgabe 1940) M.Dv.Nr. 443 OKM, Berlin, 1940 Weather short signal book[24]	Our first sight of the German weather short signal book. This enabled us to read these signals.
	U 110	
Captured in position 60° 28′ N, 32° 40′ W by H.M.S. Bulldog on 9th May 1941[25]	P/239/NID Kenngruppenbuch[26] M.Dv.Nr. 98 Indicator Book[27] P/240/NID Der Funkschlüssel M Allgemeine Bestimmungen M.Dv.Nr. 32/3 OKM, Berlin, 1941 Instructions for use of machine P/241/NID Der Funkschlüssel M Verfahren M Offizier und M Stab M.Dv.Nr. 32/2 Instruction for cyphering messages for 'Officers' and 'Staff Officers'[28]	

(*Continued*)

[24]P 169 was the first edition of the *Wetterkurzschlüssel*. It reached Bletchley on 10 May 1941.

[25]On the boarding of U-110, see [4]; [33, pp. 161–168]; [55, pp. 133–140].

[26]P 239 was photographed by Lt. Allon Bacon, a member of NID8G, before being flown to London. See Figures 5 and 6 for copies of pages seized from U-110 and his annotation about having photographed PG 239 on SS *Dunluce Castle*, which was used at Scapa Flow as an accommodation ship. P 239 to 255 reached Bletchley on 13 May 1941.

[27]The *Kenngruppenbuch* contained a random list of indicators for Enigma and *Reservehandverfahren* (an emergency reserve hand cipher). These designated the specific cipher being used (such as Hydra or Triton); thus in late 1940, the indicators in columns 361 to 390 (with others) were reserved for Hydra—see the column headed "Schlüsselkenngruppe" in Figure 5. They also provided a source of message keys for Enigma, to prevent the operator from choosing easily guessed combinations, such as ABC or IJN (a keyboard diagonal), etc. For the instructions for using the *Kenngruppenbuch*, see [20, 44].

[28]Offizier signals were doubly enciphered, first by officers only, using the inner settings (rotor order and ring settings) from the *Allgemein* (general) key and plugboard connections from special monthly *Offizier* keylists, and then by a rating, with the *Allgemein* daily key for the cipher in question [47]. For an *Offizier* keylist, see [21, p. 229]. *Stab* (staff) signals were doubly enciphered with their own special settings (unlike *Offizier*, they did not use any *Allgemein* settings). Hut 8 only solved one *Stab* key [2, p. 74].

DETAILS OF CAPTURE	DOCUMENTS CAPTURED	REMARKS
	P/242/NID Doppelbuchstaben-tauschtafeln für Kenngruppen Kennwort: BACH Zu M.Dv.Nr. 98 Bigram substitution tables for encoding indicators[29]	
	P/243/NID Anweisung zur Änderung der Schlüssel M Heimische Gewässer auf Stichwort[30]	
	P/246/NID Schlüsseltafeln M-Allgemein	These keys enabled us to read all the traffic of April, 1941[31]
	Schlüsseltafel "Heimische Gewässer" Kennwort: PIL Cypher keys for home waters	
	P/247/NID Schlüsseltafeln M-Offizier Kennwort: PIL Cypher keys for messages intended to be read only by officers	Our first decypher of an 'Offizier' message[32]

(*Continued*)

[29]The Bach (brook) bigram tables took effect on 1 July 1940. They were replaced by the *Fluss* (river) set on 15 June 1941, which was succeeded by *Strom* (stream) in November 1941, followed by *Mündung* (mouth (of a river)) on 1 March 1943, and *Quelle* (source) on 16 July 1944 [23, p. 55]. With nine tables in each set, reconstructing them was very time-consuming. For Op-20-G procedures for doing so, see [7, pp. 1–11, 79]. Two different dates have been given for the start of *Strom*: 29 November 1941 [2, p. 35]; [36, p. 57] and 1 November 1941, in a US Navy history [23, p. 55]. Since the US Navy was not breaking Dolphin in November 1941, 29 November seems the more probable date.

[30]"Instructions for changing Cipher M [naval Enigma] home waters [Dolphin] on a code word." The *Stichwort* procedure modified Enigma daily keys following a possible cipher compromise, by adding numbers derived from a varying key to the rotor order, ring settings and plugboard connections. The procedure became more and more complicated as the war went on, but for one version, see [18, p. 44]. Despite these complications, it did not present problems to the codebreakers, since it generally only modified the original settings. Once they knew that a *Stichwort* had taken effect, they then only had to test eight rotor orders and 26 different Stecker combinations—a far cry from a completely new key.

[31]Only nine April 1941 Dolphin daily keys had been solved before 10 May.

[32]"Our first decypher of an 'Offizier' message" is slightly misleading, since P 247 is not an actual decrypt. The PIL Offizier keys were in force in April 1941. The first decrypt using them is probably ZTP 540 [62], which sent the text of a signal of 21 April 1941 to NID 8G on 14 May 1941.

DETAILS OF CAPTURE	DOCUMENTS CAPTURED	REMARKS
	P/248/NID Schlüsseltafeln M-Offizier Kennwort: EIF Cypher keys for messages intended to be read only by officers	These were the June keys for 1941 which enabled us to read currently the traffic for that month
	P/251/NID Schlüsseltafeln M-Allgemein Schlüsseltafel "Heimische Gewässer" Kennwort: EIF Cypher keys for home waters	"
	P/252/NID Signalschlüsseltafel für den Funksignaldienst (Funksignaltafel) 1939 M.Dv.Nr. 114 E Bar keys	
	P/255/NID U-Bootskurzsignalheft[33] M.Dv.Nr. 299 1940 U-boat short signal book Schlüsseltafel II Kennwort: BREMEN[34] 2nd part of cyphering keys Schlüsseltafeln I und II Kennwort: DRESDEN[35]	With this we began to read the U-Boat short signals
Captured and sunk 72°N, 4°W 28/6/41[37]	WBS LAUENBURG[36]	

(*Continued*)

[33]On the *U-Bootskurzsignalheft* (a short signal book for U-boats only), see [14, p. 68].

[34]Bremen was *Schlüsseltafel* (cipher table) II in the *U-Bootskurzsignalheft*. It contained a list of special *Grundstellungen* for use with the *U-Bootskurzsignalheft*.

[35]Dresden was *Schlüsseltafel* (cipher table) I in the *U-Bootskurzsignalheft*. It contained a list of message keys for use with the *U-Bootskurzsignalheft*.

[36]On the capture of *Lauenburg*, see [33, pp. 177–181]; [55, pp. 146–149].

[37]*Lauenburg* was captured in the general area of Jan Mayen. For photographs of the capture, see [60].

DETAILS OF CAPTURE	DOCUMENTS CAPTURED	REMARKS
	P/389/NID Schlüsseltafeln M-Allgemein Schlüsseltafel "Heimische Gewässer" Kennwort: WEL Cypher keys for home waters[38]	These keys were current for July, 1941
	VORPOSTENBOOT GEIER[39]	
Sunk in West Fjord 4 miles west of TRACY light on 26th December, 1941[40]	P/661/NID Doppelbuchstaben-tauschtafeln für Kenngruppen Kennwort: UFER Zu M.Dv.Nr. 92 Bigram substitution tables for encoding indicators P/662/NID Doppelbuchstaben-tauschtafeln für Kenngruppen Kennwort: STROM Bigram substitution tables for encoding indicators P/666/NID Kenngruppenbuch M.Dv.Nr. 98 1941 Indicator Book	These were reserve tables and have not yet been used[41]
	LOFOTEN RAID OF DECEMBER 1941[42]	
	P/668/NID Der Schlüssel M Verfahren M-Allgemein M.Dv.Nr. 32/1 1940[43]	

(*Continued*)

[38]P 389 reached Bletchley on 2 July 1941.

[39]*Geier* (*V* [Vorpostenboot] 5904) was sunk during Operation Anklet, on which see [34], [55, pp. 196–197].

[40]West Fjord (Vestfjorden) is below the Lofotens, and south-west of Narvik.

[41]The *Ufer* (bank – of a river) bigram tables (P 661 above) never came into service.

[42]This was apparently Operation Anklet.

[43]These instructions would not have helped Hut 8 much at this stage. It would be surprising if they had not been captured earlier, in view of the huge haul of documents taken from U-110, in particular.

DETAILS OF CAPTURE	DOCUMENTS CAPTURED	REMARKS
	Instructions for cypher ratings on the drafting of messages	
	U 559	
Sunk in position 60 miles N.E. of Port Said by H.M.S. Pakenham and aircraft on 30th October 1942	P/936/NID Geheimer Wetterundseeschlüssel der Kriegsmarine Teil 2 Wetter kurzs chlüssel (2 Auflage) M.Dv.Nr. 443 1941 Weather short signal book	
	P/937/NID Geheime Marinefunknamenliste (G.F.L.) M.Dv.Nr. 82 1940 Secret call sign book	Out of force 7/9/42
	P/938/NID Geheime Marinefunknamenliste (G.F.L.) M.Dv.Nr. 82 1942[44] Secret call sign book	In force 7/9/42
	P/942/NID Kurzsignalheft 1941 M.Dv.Nr. 96	
	Kenngruppenheft Nr. 1.	Out of force 1.12.42
	Kenngruppenheft Nr. 2. Short signal book.[45]	In force 1.12.42

(*Continued*)

[44]The *Geheime Marinefunknamenliste* (Secret call sign book) contained a list of call-signs of *Kriegsmarine* units, including shore stations. Call-signs were generally enciphered – the cipher changed every two hours. Shore stations were allocated call-signs with letters containing umlauts (e.g., SÜP for Wilhelmshaven in 1943). For a translation of the instructions from the *Geheime Marinefunknamenliste*, see [48]. U-boats did not use call-signs as such in their radio signals.

[45]*Kenngruppenheft* 2 contained a list of *Kenngruppen* (indicators) and the message keys for Enigma beta (B bar) signals to which the *Kenngruppen* referred.

DETAILS OF CAPTURE	DOCUMENTS CAPTURED	REMARKS
	P/967/NID Begleitbuch für den Schlüssel M Prüfnummer: 3210[46]	
	U 205	
Sunk in position 32° 56′ N, 22° 01′ E by H.M.S. Paladin on 17th February 1943[47]	P/1568/NID Kenngruppenbuch M.Dv.Nr. 98 Zuteilungsliste Kennwort; FORELLE Indicator book[48]	

References

1. Accession Lists of Captured Documents. ULTRA/ZIP/NS/PU/I/1-16 (Italian); PU/J/1-39 (Japanese); PU/G/1-62 (German). PRO HW 8/116.
2. Alexander, C. H. O'D. Cryptographic History of Work on the German Naval Enigma. PRO HW 25/1.
3. Alford, V. 1993. Naval Section VI. In *Codebreakers: The Inside Story of Bletchley Park*, edited by F. H. Hinsley and A. Stripp. Oxford: Oxford University Press.
4. Balme, sub-lieutenant D. E. 11 May 1941. Boarding Primrose [U-110]. PRO ADM 1/11133.
5. Beesly, P. 2000. *Very Special Intelligence: The Story of the Admiralty's Operational Intelligence Centre 1939–1945*. London: Greenhill.
6. B[irch], F. 21 June 1944. DD (NS) Memorandum No. 45. National Archives and Records Administration, College Park (NACP), Md., RG 38, Naval Security Group, Crane, Indiana, Intelligence Records of Inactive Naval Stations 1941–1945, Box 55, 3200/3.
7. Bigram Change. NACP RG 38, Radio Intelligence Publications (RIPs), Box 168, RIP 401.
8. Birch, F. 2004. *The Official History of British Sigint 1914–1945 Volume 1 (Part 1)*. Milton Keynes: Military Press.
9. Blacker, C. 1993. Recollections of *temps perdu* at Bletchley Park. In *Codebreakers: The Inside Story of Bletchley Park*, edited by F. H. Hinsley and A. Stripp. Oxford: Oxford University Press.
10. British 3-Wheel Bombes. PRO HW 25/31.

[46]For an example of such a log book for M4 No. 15835, see [19, p. 238].

[47]On this capture, see [55, pp. 227–230]. U-205 had attacked convoy TX1 northwest of Derna, Libya, and was then sunk by South African aircraft of No. 15 Squadron and the destroyer HMS *Paladin* [11].

[48]Although *Forelle* (trout) is described as an "Indicator book," "allocation list" is probably a better translation, since a *Zuteilungsliste* allocated specified columns in the *Kenngruppenbuch* to a named cipher (see note 27). The *Forelle Zuteilungsliste* was in force for about nine months from 10 February 1943, and apparently came into force again on 15 October 1944.

11. Campaign Summaries of World War 2 North African Campaigns, Part 2 of 2. 1943. http://www.naval-history.net/WW2CampaignsNorthAfrica2.htm (accessed 9 January 2008).
12. Captain (D.) 23 June 1948. Sixth Destroyer Flotilla. Report. Supplement to the *London Gazette*.
13. D[irector] N[aval] I[intelligence]. 18 September 1943. Directive. In "Evolution of Technical Intelligence." PRO HW 50/15/14.
14. Erskine, R. 1999. "*Kriegsmarine* Short Signal Systems—and How Bletchley Park Exploited Them," *Cryptologia*, 23(1):65–92.
15. Erskine, R. 1988. "Naval Enigma: The Breaking of Heimisch and Triton," *Intelligence and National Security*, 3(1):162–183.
16. Erskine, R. 1997. "The First Naval Enigma Decrypts of World War II," *Cryptologia*, 21(1):42–46.
17. Erskine, R. 1992. "The German Naval Grid in World War II," *Cryptologia*, 16(1):39–52.
18. Erskine, R. 1988. "Ultra and Some U.S. Navy Carrier Operations," *Cryptologia*, 19(1):81–96.
19. Erskine, R. and F. Weierud. 1987. "M4 and its Rotors," *Cryptologia*, 11(4):235–244.
20. Erskine, R. and M. Smith, eds. 2001. *Action This Day: Bletchley Park from the Breaking of the Enigma Code to the Birth of the Modern Computer*. London: Bantam Press.
21. Erskine, R. and P. Marks. 2004. "Naval Enigma: Seahorse and other Kriegsmarine Cipher Blunders," *Cryptologia*, 28(3):211–241.
22. Evolution of Technical Intelligence. PRO HW 50/15/14.
23. German Naval Ciphers. NACP RG 457, Entry 9032, Historic Cryptographic Collection, Pre-World War I Through World War II ("HCC"), Box 1393, Nr. 4457.
24. German Naval Meteorological Cypher. Met 65. NACP HCC Box 187, Nr. 874.
25. German Naval Section GC and CS: Z serials 1-199. PRO ADM 223/620.
26. Good, I. J. 1979. "Studies in the History of Probability and Statistics. XXXVII. A. M. Turing's Statistical Work in World War II," *Biometrika*, 66(2):393.
27. Hinsley, F. H., with E. E. Thomas, C. F. G. Ransom, and R. C. Knight. 1981. *British Intelligence in the Second World War: Its Influence on Strategy and Operations*, Vol. 2. London: Her Majesty's Stationery Office.
28. Hinsley, F. H., with E. E. Thomas, C. A. G. Simkins, and C. F. G. Ransom. 1988. *British Intelligence in the Second World War: Its Influence on Strategy and Operations*, Vol. 3, Part 2. London: Her Majesty's Stationery Office.
29. History of 30 Commando (latterly called 30 Assault Unit and 30 Advanced Unit). PRO HW 8/104.
30. HMS *Griffin*. 26–28 April 1940. Report of proceedings. PRO ADM 199/476.
31. Home Waters Enigma. 8 June 1943. NACP RG 38, RIPs, Box 172, RIP 610, vol. E-8, pp. 19–35.
32. Hosgood, S. All You Ever Wanted to Know about Banburismus but were Afraid to Ask. http://tallyho.bc.nu/~steve/banburismus.html (accessed 9 January 2008).
33. Kahn, D. 1991. *Seizing the Enigma: The Race to Break the German U-Boat Codes, 1939–1945*. Boston: Houghton Mifflin.
34. Lofoten Islands 2nd Raid 26/27th Dec 1941. http://www.combinedops.com/lofoten_2.htm (accessed 9 January 2008).
35. Lofoten Islands Raid – 3/4 Mar 1941. http://www.combinedops.com/Lofoten_Islands_Raid.htm (accessed 9 January 2008).
36. Mahon, A. P. The History of Hut Eight 1939–1945. PRO HW 25/2. Note that the pagination differs from the retyped copy in NACP HCC, Box 1423, Nr. 4685.
37. McVittie, G. C. 8 February 1941. Diary entry with "Autobiographical Sketch" prepared for Royal Society of Edinburgh. Archives Centre, Churchill College, Cambridge, RLEW.
38. Mediterranean Enigma. 26 May 1943. NACP RG 38, RIPS, Box 172, RIP 610, Vol. E-8, pp. 1–18.

39. Memorandum No. 3, Schlüssel M (Form M 4). NACP RG 38, RIPs, Box 169, RIP 403.
40. Murray, J. Fall 1975. "A Personal Contribution to the Bombe Story," *NSA Technical Journal*, 20(4):41–46.
41. Murray, J. 1993. Hut 8 and Naval Enigma—Part I. In *Codebreakers: The Inside Story of Bletchley Park*, edited by F. H. Hinsley and A. Stripp. Oxford: Oxford University Press.
42. NID. 7 May 1942. CAFO 879. In "Report on British Procedures for Capturing and Exploiting Enemy Naval Documents." PRO HW 8/103.
43. Nutting, D. C. and T. J. Glanville, eds. 1997. *Attain by Surprise: The Story of 30 Assault Unit Royal Navy/Royal Marine Commando and of Intelligence by Capture*. Chichester: David Colver.
44. Oberkommando der Kriegsmarine. 1939. Kenngruppenbuch. M. Dv. Nr. 98. Copy held by author. For a translation, see "Book of Indicator Groups (K. Book)." NACP HCC, Box 622, Nr. 1681.
45. Oberkommando der Kriegsmarine. 1940. *U-Bootskurzsignalheft*. M. Dv. Nr. 299. Copy held by author.
46. Oberkommando der Kriegsmarine. 1941. Der Schlüssel M - Verfahren M Allgemein. M. Dv. Nr. 32/1. For a translation, see "Translated 1940 Enigma General Procedure." http://www.codesandciphers.org.uk/documents/egenproc/eniggnix.htm (accessed 9 January 2008).
47. Oberkommando der Kriegsmarine. 1941. Der Schlüssel M - Verfahren M Offizier M und Stab. M. Dv. Nr. 32/2. Bundesarchiv-Militärarchiv, RMD 4/32/2. For a translation, see "Translated 1940 Enigma Offizier and Staff Procedure." http://www.codesandciphers.org.uk/documents/officer/officerx.htm (accessed 9 January 2008).
48. Oberkommando der Kriegsmarine. 1942. Geheime Funknamenliste. M. Dv. Nr. 82. Translation of the Instructions for Use of the Geheime Funknamenliste. 1942. NACP HCC, Box 622, Nr. 1670.
49. Op-20-GM-1-C-3 war diary. NACP RG 38, Records of the Naval Security Group Central Depository, Crane, IN, CNSG Library, Box 113, 5750/176.
50. Port minesweeping officer, Lyness. 20 May 1940. Minute. PRO ADM 199/476.
51. Report on British Procedures for Capturing and Exploiting Enemy Naval Documents. PRO HW 8/103.
52. S/NID 142. 24 December 1942. In "Evolution of Technical Intelligence." PRO HW 50/15/14.
53. Sale, T. Making the Enigma ciphers for the film Enigma. http://www.codesandciphers.org.uk/enigmafilm/index.htm (accessed 9 January 2008).
54. Schiff 26 und Schlüsselsicherheit. 21 May 1940. KTB 2/SKL. Naval Historical Branch (NHB), Ministry of Defence, Portsmouth.
55. Sebag-Montefiore, H. 2000. *Enigma: The Battle for the Codes*. London: Weidenfeld and Nicolson.
56. Signals 1946/8 January and 1917/17 January 1942. NHB, microfilm, reel 18.
57. Smith, M. 1998. *Station X: The Codebreakers of Bletchley Park*. London: Channel 4 Books.
58. Squadron-Leader Jones' Section. PRO HW 3/164.
59. Verlust Schiff 26 und 37 und Schlüsselsicherheit. 3 May 1940. KTB 2/SKL. NHB.
60. Wetterbeobachtungs-Schiff Lauenburg. http://www.warcovers.dk/greenland/wbs3_1.htm (accessed 9 January 2008).
61. Whelan, R. The Use of Hollerith Equipment. PRO HW 25/22, and in "Report on IBM Operations and Overseas Interception." NACP HCC, Box 1126, Nr. 3621.
62. ZTP 540. 14 May 1941. PRO DEFE 3/1.
63. ZTPGU 1. 13 December 1942. PRO DEFE 3/705.