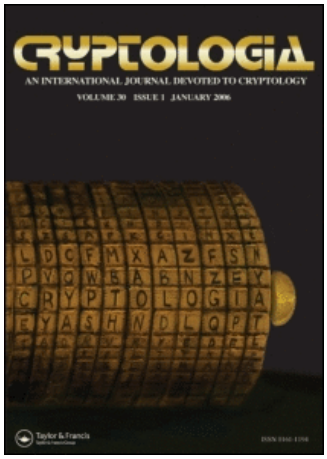

Cryptologia
Publication details, including instructions for authors and subscription information:
http://www.informaworld.com/smpp/title~content=t725304178

G-312: AN ABWEHR ENIGMA

David H. Hamer [a]
[a] 66 Academy Court, Bedminster NJ 07921 USA. Email: dhamer@eclipse.net. URL: http://www.eclipse.net/?dhamer/..

Online Publication Date: 01 January 2000
To cite this Article: Hamer, David H. (2000) 'G-312: AN ABWEHR ENIGMA', Cryptologia, 24:1, 41 - 54
To link to this article: DOI: 10.1080/0161-110091888772
URL: http://dx.doi.org/10.1080/0161-110091888772

G-312: AN ABWEHR ENIGMA

David H. Hamer

ADDRESS: 66 Academy Court, Bedminster NJ 07921 USA. Email: dhamer@eclipse.net. URL: http://www.eclipse.net/~dhamer/.

ABSTRACT: G-312, an *Abwehr* Enigma in the collection of The Bletchley Park Trust[1] is presented together with details of its internal mechanism and wheel wiring.

KEYWORDS: Enigma, *Abwehr* Enigma, cyclometric stepping, multi-notch machines.

INTRODUCTION

G-312, an *Abwehr* Enigma, is in the collection of The Bletchley Park Trust. Since very little information about this Enigma variant is available in the current literature it is perhaps appropriate to review the outcome of a detailed examination of this particular example of the wartime output of *Chiffriermaschinen Gesellschaft Heimsoeth und Rinke* of Berlin.

For an overview of *Abwehr* cryptographic operations and Bletchley Park's involvement see "The *Abwehr* Enigma" by Peter Twinn in [4].

CONVENTIONS

In this description of G-312 the following conventions have been adopted. In operational terms the four wheels are numbered right to left as seen from the machine operator's viewpoint - thus the right-hand movable wheel is designated "wheel 1". Similarly, any other relational references are 'as seen' by the operator of the machine. When referring to specific wheels - such as when discussing wiring or notches - the wheel designation will be as marked on the wheels themselves - such as "Wheel I", "Wheel II", etc.

[1] The Mansion, Bletchley Park, Milton Keynes MK3 6EF, UK. URL: http://www.bletchleypark.org.uk or: http:// www.cranfield.ac.uk/ccc/bpark/.

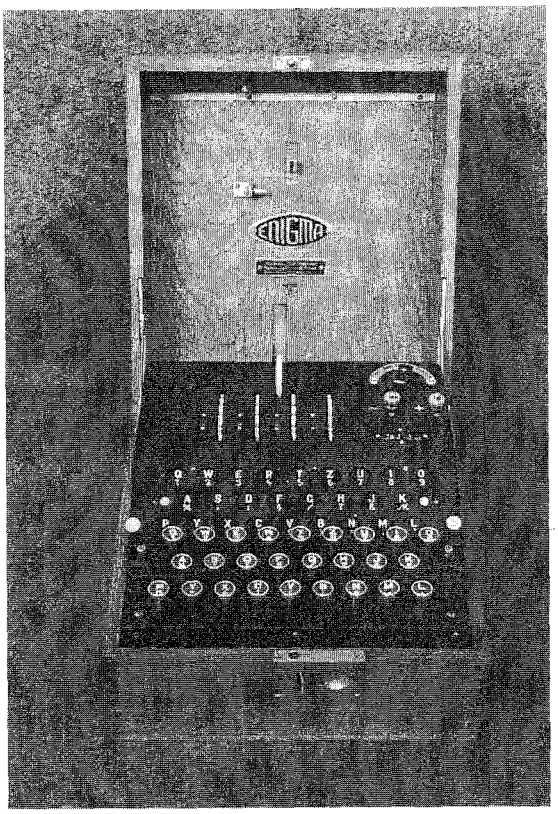

Figure 1. G-312 The *Abwehr* Enigma.

GENERAL DESCRIPTION

The *Abwehr* Enigma (Figure 1) is in general appearance, similar to the better-known Service machines [1] - but there are several differences, which are immediately apparent. First, it is somewhat more compact - its overall dimensions measure $25 \times 27 \times 16.5$ cm. compared with the Service machine's $28 \times 34 \times 15$ cm. The slight increase in the height of the case over that of the Service Enigma is due to the fact that in the *Abwehr* variant the lampboard has a slight front-to-back slope, which makes it easier to read the output. There is no plugboard.

The keyboard (Figure 2) has the expected 26-key QWERTZU layout but each key carries an additional symbol. The lampboard echoes the keyboard. The top panel, in addition to the usual cut-outs for the wheels, the accumulator terminals and the power source switch, carries a mechanical digital counter which can be zeroed by means of a small crank [normally carried in the lid but missing on G-312] which is inserted through a hole in the right side of the case.

Figure 2. The keyboard and lampboard of G-312.

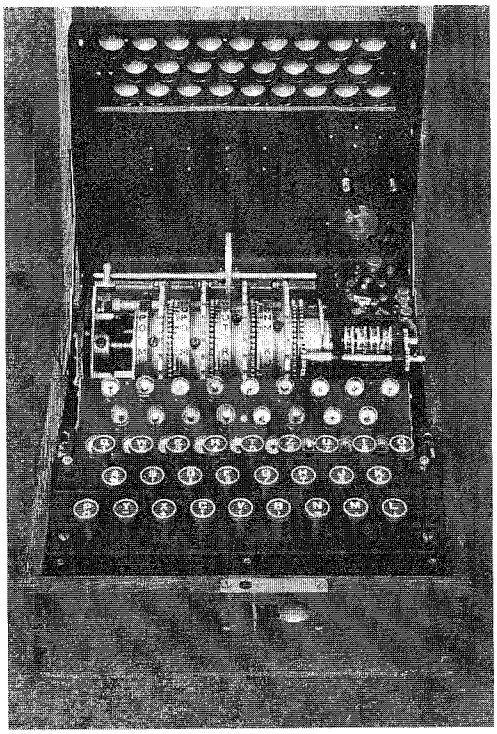

Figure 3. G-312 with inner lid open.

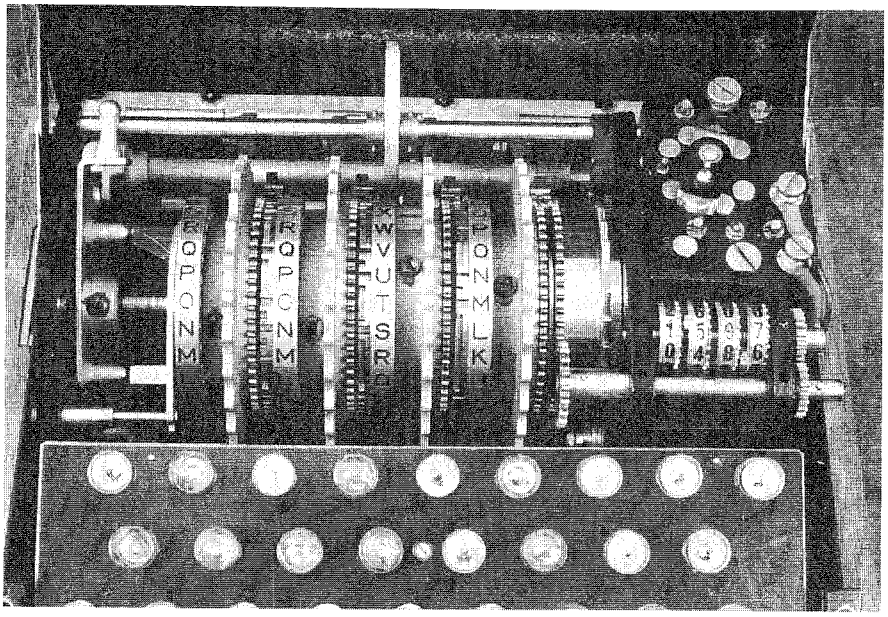

Figure 4(a). Interior details – wheels, counter, etc.

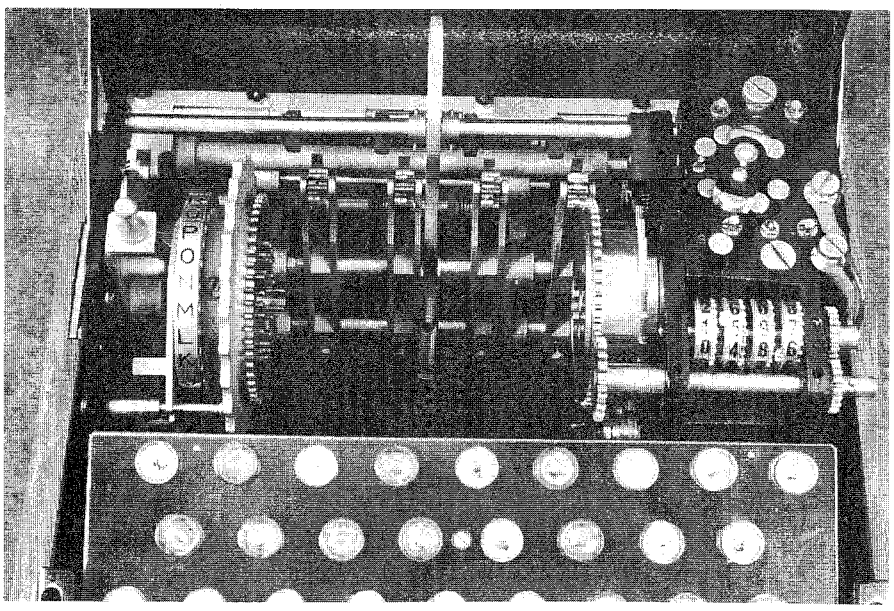

Figure 4(b). Wheels removed – showing stepping mechanism.

The large curved lever above the four thumb wheels is the lock/unlock lever for the geared stepping mechanism. This lever is placed in the 'unlocked' (up) position to allow the setting of the wheel positions prior to use but it must be returned to the 'locked' (down) position to render the machine operational. Movement of this lever controls the engagement and disengagement of the gears and pinions.

Opening the inner lid (Figure 3)reveals that there is no 'lamp test' position on the lampboard - only the 26 operational lamps.

A general comment: G-312 is a very well-constructed machine and exhibits a degree of workmanship, attention to detail and precision that is a 'cut above' that found in Service Enigmas.

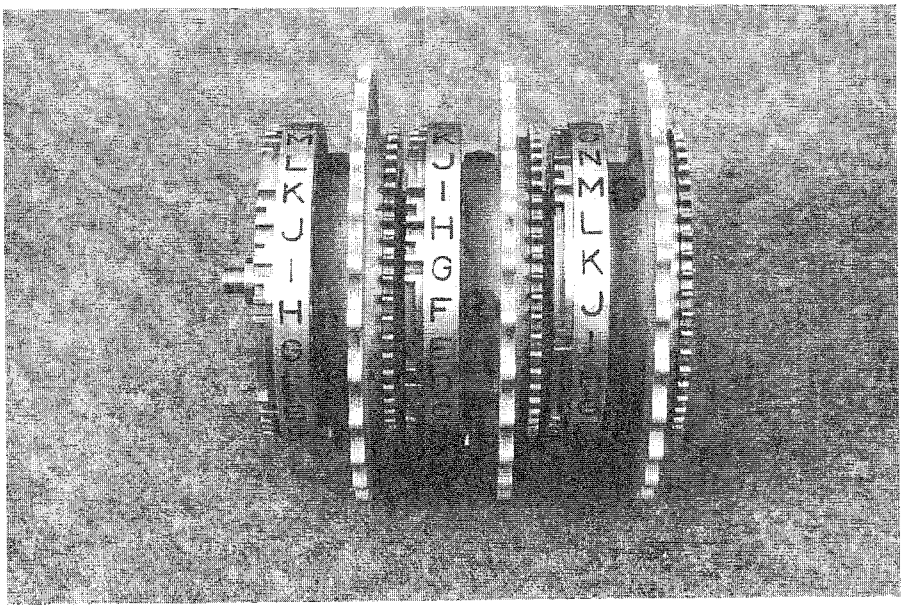

Figure 5. The three removable wheels and spindle.

THE WHEELS

In Figure 4(a), from right to left, we see the *Eintrittwalze* (ETW), the three removable and interchangeable wheels and the *Umkehrwalze* (UKW). With the exception of the ETW all of the wheels have settable index rings and all four move during the encipherment/decipherment operation. The three central wheels may be removed as a unit, with their spindle (Figure 5), as in the Service Enigma. The steppable UKW normally remains in the machine (Figure 4(b)).

The wheels (Figure 6 (a) and (b)) are significantly different from those of other Enigma variants. First, they are smaller. The outside diameter of the *Abwehr* wheel is approximately 8.5 cm. compared with that of approximately 10 cm. for the Service machine wheel.

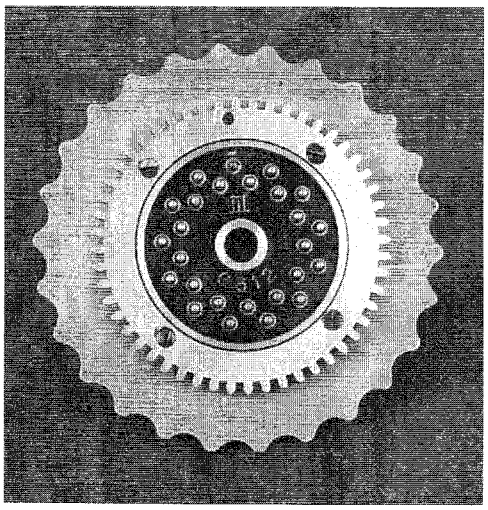

Figure 6(a). Wheel – 'pin' side with stepping gear.

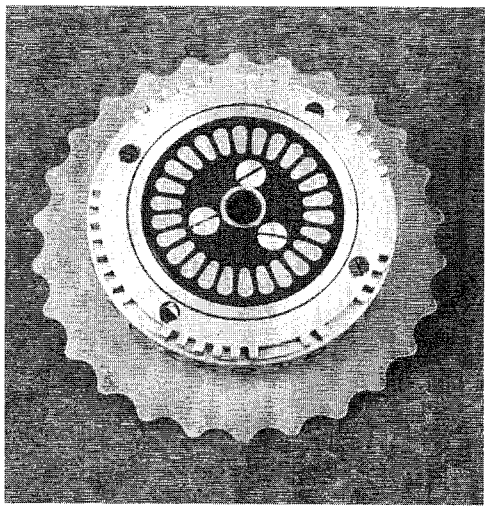

Figure 6(b). Wheel – 'plate' side with notches.

The central, wired block is also proportionately smaller, which necessitates a concentric arrangement of the spring contacts on the 'pin' side of each wheel together with an elongation of the 'plates' on the other side. This arrangement is clearly visible also on the ETW and UKW (Figures 7 and 8). The wheel alphabets are 'staggered' thus: $^{A}_{B}\ ^{C}_{D}\ ^{E}_{F}\ \ldots$

The wheel wirings for G-312 are given in Table 1. Following convention these have been determined with *Ringstellung* = A, where appropriate. Alphabets run clockwise as viewed down the axis of the machine looking 'through' the ETW. It is perhaps surprising, given the overall complexity of the machine, that the diagonal of the *Eintrittwalze* is found to be QWERTZU ...

The location and number of the notches on each of the three wheels are also given in Table 1. Because of the notch configuration[2] this *Abwehr* machine was identified as the "11-15-17' by BP and the U. S. agencies. The 'offset' between a notch location and its associated 'turnover' displayed in the window is -8 as in the Service and other Enigma variants.

[2]A typographical error in Peter Twinn's chapter in [4] gives the number of notches as 11-15-19.

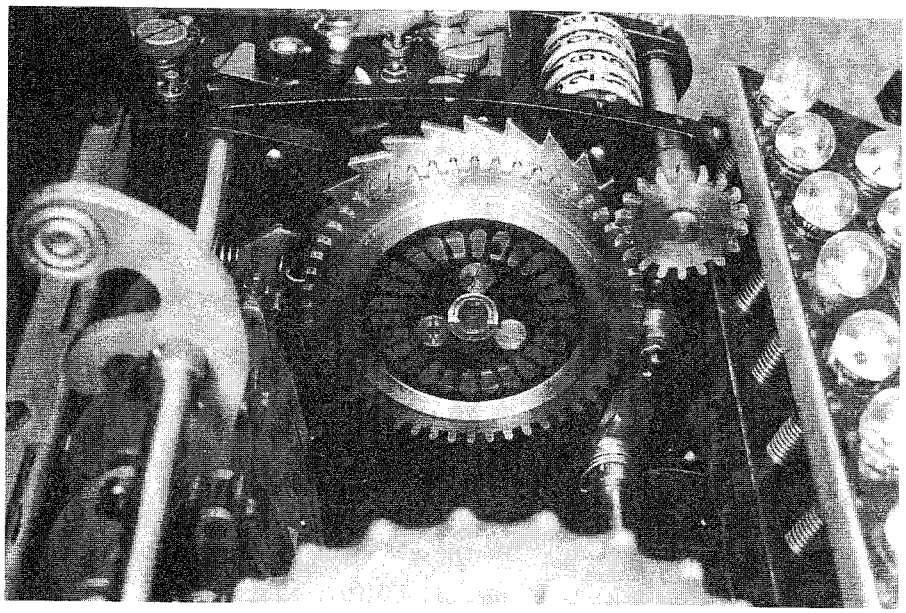

Figure 7. *Eintrittwalze* with stepping lever, gears, and pinions.

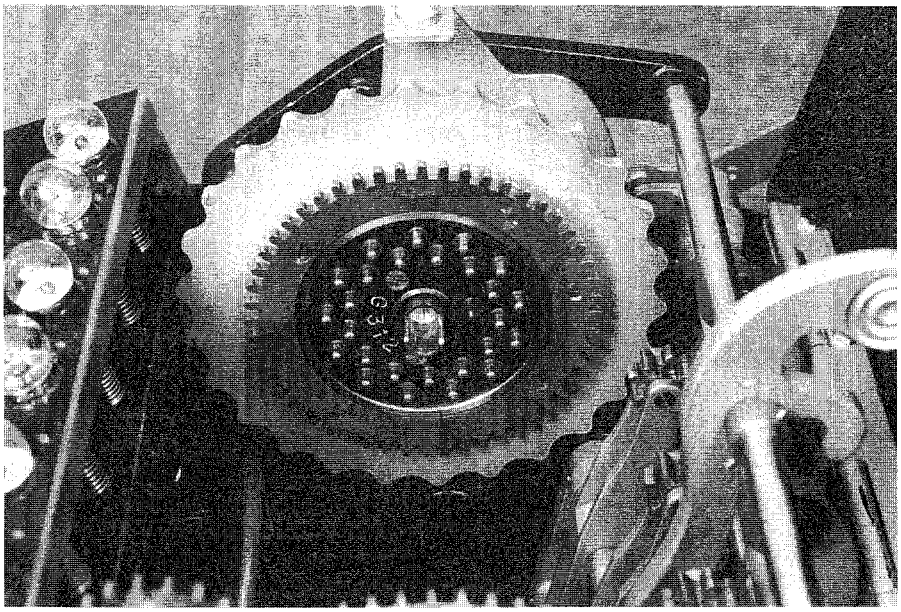

Figure 8. *Umkehrwalze* with stepping gear, pinions, and locking lever.

The wheel classes[3] for this set of wheels are shown in Table 2.

Wheel	ABCDEFGHIJKLMNOPQRSTUVWXYZ	Notch	Window
I	DMTWSILRUYQNKFEJCAZBPGXOHV	ACDEHIJKMNOQSTWXY (17)	SUVWZABCEFGIKLOPQ
II	HQZGPJTMOBLNCIFDYAWVEUSRKX	ABDGHIKLNOPSUVY (15)	STVYZACDFGHKMNQ
III	UQNTLSZFMREHDPXKIBVYGJCWOA	CEFIMNPSUVZ (11)	UWXAEFHKMNR
UKW	RULQMZJSYGOCETKWDAHNBXPVIF		
ETW	QWERTZUIOASDFGHJKPYXCVBNML		

Table 1. Wiring of Wheels, *Umkehrwalze* and *Eintrittwalze* for G-312.

Notes:

1. The Notch column gives the location of the notches on the alphabet ring - the Window column indicates the letter appearing in the window when the notch is engaged in its turnover position.
2. Alphabets progress clockwise as viewed along the wheel axis from the ETW. All wheels are in their neutral position, *Ringstellung* = A.
3. UKW = *Umkehrwalze*; ETW = *Eintrittwalze*

Wheel	Class 1.2	Class 1.3
I	3.23	4.22
II	6.20	2.24
III	2.24	2.2.6.16
UKW	10.16	1.5.20

Table 2. Wheel classes for G-312.

STEPPING MECHANISM

The *Abwehr* machine uses a system of gears and notches to achieve stepping of the wheels, unlike all other known Enigma variants which use a lever, pawl and ratchet arrangement. These two quite different systems have been described previously by Deavours [2] and Hamer [5], respectively.

Details of the *Abwehr* Enigma's geared system are evident in Figure 7. With the large central lever in the forward (locked) position, when a key is depressed the stepping lever on the left turns the large gear, which has 52 teeth and is concentric to the ETW, via the ratchet. This in turn causes the smaller gear, on the right, to advance the digital counter by one position. The larger gear is also meshed with a pinion that is in turn meshed with the driving gear of wheel 1, which thus advances one position with each keystroke.

[3] For an explanation of the derivation of wheel classes from rod squares see [6].

Each wheel is equipped with a number of notches on its index ring - these and their locations are shown in Table 1. The notches on the left side of each wheel can be seen in Figure 5. Notches are also clearly visible in Figure 4(a) where their relationship with the pinions can also be seen. The number of notches, 11, 15 and 17 respectively, is selected as being relatively prime - to each other and to 26.

The pinions associated with wheels 2, 3 and 4 differ from that associated with wheel 1 in that each of the first group has alternating long and short teeth (Figure 4(b)). Each pinion 'straddles' the gap between a pair of wheels - one end aligned with the driving gear of the wheel to its left, the other aligned and ready for engagement with a notch of the wheel to its right. Each pinion is free to rotate. A pinion is driven when its 'long' tooth engages a notch of the wheel to its right and it, in turn, drives forward the wheel on its left. This process is repeated for wheels 3 and 4 (UKW) - thus every wheel except wheel 1 is controlled and driven by the notches on the index ring of the wheel to its right[4].

It would not be appropriate to attempt to compare the level of security afforded by the *Abwehr* Enigma with that of the other Enigma variants, since many factors other than machine design contribute to the overall cryptographic effectiveness of any cryptosystem. Nor is it productive to speculate on the myriad reasons which might lie behind the *Abwehr's* decision to adopt a design that is so different from that used by the other German military services. It might, however, be interesting to compare a couple of features of the *Abwehr* Enigma with those of another well-researched Enigma variant - the 4-wheel Naval M4 [1, 3].

First: the *Abwehr* Enigma is a true, four-wheel machine. During the encipherment/decipherment processes all four wheels move. Within the same sense, the M4 is not a true four-wheel machine in that, like the Commercial Enigma and the Swiss 'K' and Japanese 'T' machines [6], the fourth, left-hand wheel may be considered to be a 'settable' *Umkehrwalze* which, once the initial message setting has been made, does not move again unless reset manually. Offsetting this 'stepping' advantage of the *Abwehr* Enigma is the fact that the Naval machine has the usual *Stecker* board while the *Abwehr* variant is without *Steckers*.

Second: the arrangement of the notches, and their number, in the *Abwehr* Enigma results in a much more complex and 'randomized' movement of the wheels during operation. This arrangement - as previously stated the number of notches per wheel is relatively prime to that of each of the other wheels and to 26 - produces much more frequent wheel movement without the consequent

[4]This is in contrast to normal Enigma stepping in which the movement of a wheel is controlled by the notch(es) of the wheel to its right but driven by its own stepping lever. The 'double stepping' anomaly is a direct consequence of this simpler system.

reduction of the cycle length[5] which occurs in the Navy Enigmas. For example, an M4 with two-notch wheels [Wheels VI, VII and VIII each have two notches] in the 'fast' and 'middle' positions will have the length of its cycle reduced from 16,900 to 4,056.

The stepping movement of the *Abwehr* Enigma is truly cyclometric. It does not have the 'double stepping' anomaly of the regular Enigma [5] and so, in the course of a complete machine cycle, there are no 'missing' four-letter combinations. The cycle length is therefore $2^{64} = 456,976$ [7].

An illustration of the complexity of the stepping sequence of the *Abwehr* machine is provided in Table 3, which compares the movement of the wheels during ten keystrokes of G-312 and a similar sequence on a Naval M4. Note the occurrence of a 'lobster' between positions 4 and 5 in the G-312 sequence[6].

Wheels: III, II, I	G-312	M4
Start	NZAM	NZAM
1	NZAN	NZAN
2	NZAO	NZAO
3	NABP	NZAP
4	NACQ	NZAQ
5	OBDR	NZBR
6	OBDS	NZBS
7	OCET	NZBT
8	OCEU	NZBU
9	OCFV	NZBV
10	ODGW	NZBW

Table 3. First ten wheel movements - *Abwehr* and Naval M4.

[5]Here, 'cycle length' is defined as the number of characters or keystrokes required to return to a particular setting of the wheels - e. g., from AAAA to AAAA. Because of the 'double stepping' anomaly inherent in the normal Enigma stepping this is reduced, in both the 3-wheel and 4-wheel variants, from an 'ideal' of 17,576 to 16,900 when using single-notch wheels.

[6]The term 'lobster' - attributed to Dilwyn Knox - is used to describe a situation where all four wheels move together. For a detailed discussion of this term, the associated expression 'crab' and their contribution to the cryptographic weakness of the *Abwehr* Enigma, see Deavours [2] and Twinn in [4].

APPENDIX - ENIGMAS AT BLETCHLEY PARK

During the course of gathering information about G-312 for this paper an inventory of the Enigma-related material at Bletchley Park was created. For the benefit of researchers and others with an interest in BP's collection of Enigma machines and artefacts the following list has been compiled. Some of these items are on public display and are so indicated. For access to the archived material prior permission should be obtained from the Bletchley Park Trust authorities.

Army/GAF Enigma - A16991/jla/43

This machine is on public display, in the BP Mansion. It is a standard, wooden-case model complete and in working condition and is fitted with metal-engraved Wheels VI, VII and VIII from Navy Enigma M1332 and *Umkehrwalze B*. The plug board has a QWERTZU layout

Army/GAF Enigma - A16992/jla/43

The 'twin brother' of the machine above. Fitted with metal-engraved Wheels III and V [1-26] from A18131 and a second Wheel V marked A16801. The *Umkehrwalze* is B. This machine is currently in the BP archive and has been modified [a GC&CS or GCHQ experiment?] by the addition of a small plugboard on the left side of the case that appears to have been used to alter the wiring of the *Umkehrwalze*. (Figure 9).

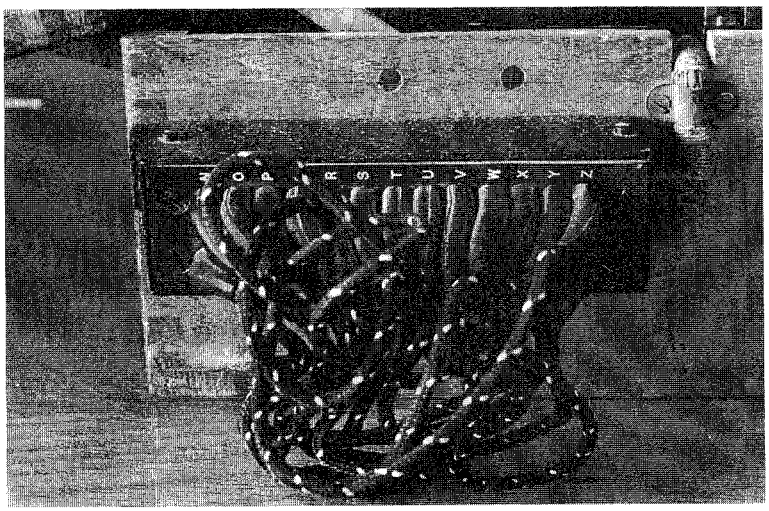

Figure 9. Detail of plugboard attached to left side of A16992.

Navy Enigma M3 - M1322

Fitted with standard, A-Z, Navy Wheels II, IV and V from M1332 and *Umkehrwalze* B. The plugboard carries both A-Z and 1-26 markings. An unusual feature of this M3 is the two-piece hinged lid, which covers the lampboard and the wheel compartment. This machine is on public display in a 'hands-on' environment - visitors are encouraged to decrypt a real Enigma message, which is displayed nearby, and are given detailed instructions on how to do so.

Navy Enigma M4 - M3097

On public display. Navy wheels - A-Z engraved metal - I, II and II from M3887. The 'gamma' wheel is from M5520 and a 'thin C' reflector is in place. This M4 is one of the Navy machines equipped with a 'numbered' keyboard, with 1-9 sharing the top row of keys and the zero sharing the P key in the bottom row.

Abwehr Enigma - G-312

A rare example, on public display in the BP mansion. Fitted with Wheels I, III and V indexed to this machine. A full description of this machine is in the body of this paper.

OTHER ENIGMA ARTEFACTS

Navy Wheels: A wooden case marked M1332 contains Wheels II, IV and VI from M3887, Wheels III, VII and → from M3097 and Wheel VII from M3889. All of these wheels are metal-engraved, black, except for the → which has red lettering. Public display.

Navy Wheels: Another wooden case, 15796, containing Wheels I, III, IV, V and VI from M15796 and Wheel II from M15788. Wheel VII from M15796 is displayed alongside - 'exploded' to display its internal wiring. Public display.

Army/GAF Wheels: three wheels in a box marked A00093/43E. Normal wiring. Archive.

Army/GAF Wheels: A wooden box marked M983 contains two wheels [engraved 1-26] marked A6008 I and III. These have non-standard internal wiring [see Table 4] and each has its turnover notch filled with a dark, pitch-like substance. Public display.

Wheel	ABCDEFGHIJKLMNOPQRSTUVWXYZ	Notch	Window
I	LVAWDKEJGMIHORNSQYPBZCFTXU	Y	Q
III	WYKEXFINHQOPJRLTMSACVGBUZD	D	V

Table 4. Wiring of Wheels A6008 I and III: *Ringstellung* = A.

Wooden case from Enigma M16264 has been modified to contain 27 mechanical digital counters [A-Z + totalizer] probably constructed by GCHQ to perform statistical character analysis. The Enigma keyboard has been replaced by a standard 'British' QWERTY typewriter unit. The assembly is fitted with a modern, 13 amp. UK standard electrical plug. Archive item. (Figure 10).

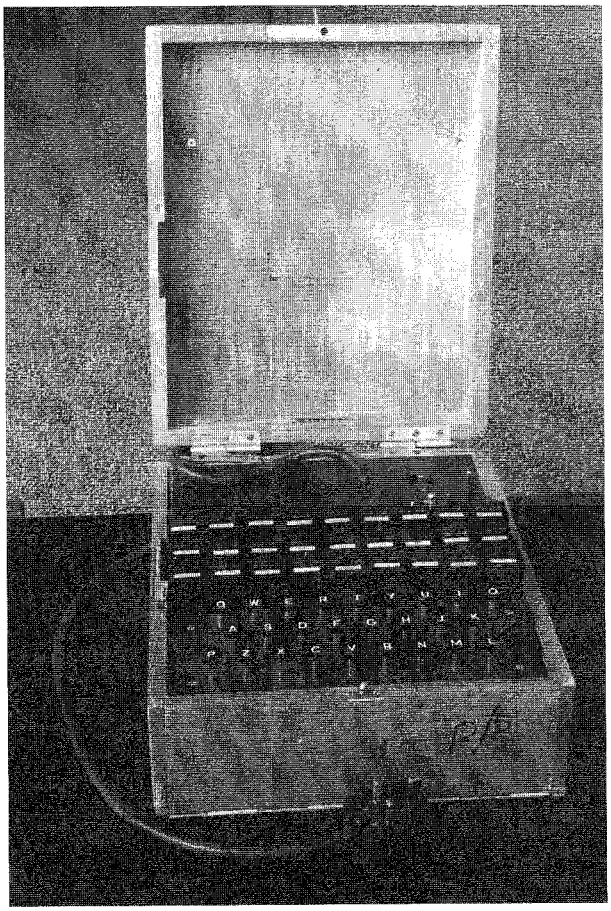

Figure 10. Digital counting device mounted in the case of M16264.

ACKNOWLEDGEMENTS

My thanks are due to Tony Sale, Trustee and Director of Museums, The Bletchley Park Trust, for providing access to G-312 and much other material in the BP collection. Also at BP; Margaret Sale's help was and is invaluable; and both John Gallehawk and Cliff Horrocks are due thanks for their counsel and support. My colleagues in the Crypto Simulation Group[7]; Ralph Erskine, Philip Marks, Geoff Sullivan and Frode Weierud were, as always, more than supportive.

REFERENCES

1. Deavours, Cipher A. and Louis Kruh. 1985. *Machine Cryptography and Modern Cryptanalysis*. Norwood MA: Artech House

2. Deavours, Cipher A. 1997. Lobsters, Crabs and The *Abwehr* Enigma. *Cryptologia*. 21(3): 193-199.

3. Erskine, R. and Frode Weierud. 1987. Naval Enigma: M4 and its Rotors. *Cryptologia*. 11(4): 235-244.

4. Hinsley, F. H. and Alan Stripp. 1993. *Codebreakers - the Inside Story of Bletchley Park*. Oxford University Press.

5. Hamer, D. H. 1997. Enigma: Actions Involved in the "Double Stepping" of the Middle Rotor. *Cryptologia*. 21(1): 47-50

6. Hamer, D.H., Geoff Sullivan and Frode Weierud. 1998. Enigma Variations: An Extended Family of Machines. *Cryptologia*. 22(3): 211-229.

7. Unpublished email exchange between the author, Frode Weierud and Geoff Sullivan.

BIOGRAPHICAL SKETCH

David Hamer, having more or less retired from 'real work', finds himself busier than ever pursuing cryptographic artefacts and knowledge on both sides of the Atlantic.

[7]For information about the Crypto Simulation Group and examples of computer simulations [including downloadable software] visit the CSG pages at the web site listed at the head of this article.