BREAKING THE LAST "H.M.S. HURRICANE" INTERCEPT

INTRODUCTION

In a 1995 letter to the editors of the journal *Cryptologia*,[1] Ralph Erskine included a transcription of a page from a Royal Navy HF/DF operator's report that he had found in the U.K. National Archives. The HF/DF report had been appended to a report dated 25th November, 1942, by the Commanding Officer of the Royal Navy destroyer H.M.S. Hurricane of Escort Group B1, concerning their just-completed escort of Convoy HX 215. The page gave the texts of three radio messages that the HF/DF operator had intercepted during that crossing, on the 19th and 21st November. It was evident that the three intercepts, judging by their formats and by the circumstances of their interception, were almost certainly German Navy messages, probably sent to or from U-boats, and enciphered with the four-wheel Model M4 Enigma machine.

I began trying to break these messages about ten years ago; but in 2006 Stefan Krah's distributed-computing M4 Project made the first two breaks, on the second and third of the intercepts. Since then, I've continued trying to break the remaining message, until some recent help from Michael Hörenberg finally enabled me to do it. I've already given the solution in a previous article; this article will explain the method used for the break, and also give some additional background and analysis.

[1] Ralph Erskine, letter to the editor, *Cryptologia* Oct. 1996 Vol. XX, No.4

1. THE SOFTWARE

General Description: Bombe-Simulator Plus Hillclimber

The software I used to break the message is a combination of a Turing Bombe simulator and a hillclimber program. The Bombe uses input from a menu based on a possible alignment of a crib with a portion of the ciphertext, and looks for any setting of the Enigma wheels at which the ciphertext letters in the menu will decipher to the corresponding letters in the crib. When it finds such a setting, called a "stop", the hillclimber then tries to decipher the whole message, using the information from the stop as a starting point.

Special Feature Of The Bombe-Simulator

The Bombe portion of the program incorporates a special feature that as far as I know did not exist in the actual Turing Bombes of WWII. It is designed to reduce the number of false stops when running weak menus – i.e., menus with no loops and two or more letter-chains. An ordinary Bombe stop will find a number of the plugboard connections, or "*Steckers*". Often, some of these will not be confirmed – for example, it might have found that 'A' was steckered to 'J', but could not confirm that 'J' was steckered to 'A'. The special cross-checking feature of my program would then force the issue by feeding the assumption that 'J' was steckered to 'A' back into the system and seeing if it led to a contradiction. I've found that the great reduction in false stops that this feedback produces makes it possible to run menus that would otherwise have been too weak to be of any use. A secondary advantage is that it seems to find more of the plugboard connections.

How Stops Are Handled By The Hillclimber

The information from a stop consists of the plugboard connections, the wheel order, and the core prestart positions of the wheels – i.e., their positions just before the first letter of the crib. If the crib/ciphertext alignment is not at the beginning of the message, the hillclimber adjusts the prestart positions to what they would be just before the message beginning, by counting back from the position of the crib in the message. Then, starting with these core wheel positions and the plugs found by the bombe, the hillclimber tries to decipher the whole message at all possible ring settings, doing an abbreviated hillclimb at each ring setting to find any plugboard connections that the bombe did not find. If the score for the best decryption of the hillclimb is higher than the top score of previous hillclimbs, then the Enigma settings and the decryption are stored in memory to be written to an output text file at the end of the program run. Additionally, if the score is above a certain threshold, the settings and the decryption are accepted as a possible "solution" and immediately written to the output file.

2. THE SEARCH FOR A CRIB

Strategy: Look For Cribs In U-Boat War Diaries

Breaking an Enigma message with a Bombe-simulator requires a crib, so when I first started trying to break the H.M.S. Hurricane intercepts some years ago , I did some research to try to narrow down the possibilities as to the originators of the messages.

The radio frequency that H.M.S. Hurricane was monitoring when it intercepted the three signals had been assigned by the Kriegsmarine to the radio circuit, or "*Schaltung*," called "*Amerika I*," which was used for the radio traffic of U-boats in the western half of the North Atlantic. I learned that on November 19, 1942, there were 23 U-boats operating more or less in that area: U-43, 84, 106, 183, 184, 224, 262, 264, 383, 445, 454, 460, 518, 521, 522, 524, 606, 608, 611, 623, 624, 663 and 753. It seemed probable that the intercepted messages had been sent either to or from one or more of those boats. Since H.M.S. Hurricane's HF/DF report gave the times of reception of the three intercepts (and, in one case, what looked like a message serial number), I thought that searching the war diaries (*Kriegstagebücher*, or KTBs) of those U-boats would be useful.

Over the years I've bought microfilm copies of the KTBs of some but not all of the relevant U-boats from the U.S. National Archives. I hoped that by comparing the times of reception and/or serial numbers of the intercepts to those of the radio messages recorded in the KTBs (allowing for the one-hour difference between the Greenwich time kept in Royal Navy ships and the German Legal Time kept on Kriegsmarine vessels), I might find a crib for at least one of the intercepts. I thought that even if the plaintext of the message was not recorded, there might at least be an entry stating that the boat had sent or received a message at one of the times in question; and that I could then guess the address and/or signature that would appear at the beginning of the message.

The "Looks" And "Schröder" Messages

My strategy came tantalizingly close to success with two of the messages; but a combination of my own mistakes and a little bad luck prevented a break. In the KTBs of U-264 (Looks) and U-623 (Schröder) I found two radio messages whose times of reception led me to believe that they might be the plaintexts of the second and third intercepts, respectively.

In the case of the "Looks" message, I had trouble re-arranging the plaintext from the way it appears in the KTB to the form it would take as typed into the Enigma machine. I thought that the address "BDUUU", or a variant thereof, would appear along with the signature, as for example "BDUUUVVVJLOOKSJ" or "JLOOKSJANANBDUUU." I didn't know at the time that in October 1941, an order had been sent out to the effect that from then on, the signature would be omitted in all messages from B.d.U. ("*Befehlshaber der Unterseeboote*", or Commander-in Chief of Submarines); and that the address was to be omitted in all messages to B.d.U. I never tried just "VONVONJLOOKSJ" as a message beginning, and because I couldn't

find an arrangement of the plaintext that did not result in a crash when aligned with the ciphertext, I abandoned it. Shortly thereafter, that message was broken by Stefan Krah's M4 Project.

After the "Looks" message was broken, I told Stefan that I had found the message in U-264's KTB, and that I had also found what I thought might be the plaintext of the third intercept in U-623's KTB. In the meantime, while the M4 project proceeded with their ciphertext-only attack, I tried the crib "VVVJSCHROEDERJAUFGELEITKURS" at the beginning of the message, and when that failed, "AUFGELEITKURSFUENFFUENF" at the 15th letter of the ciphertext, also without success. When Stefan's group broke the message two weeks later, I found that an incorrect ciphertext letter at the ninth position had prevented my solving it with the first crib; and that a mistake of mine in how my program handled the wheel positions for cribs in the middle of a message had prevented success with the second. I then turned to the remaining intercept; but without much hope – I did not have a crib for that message, and until I found one, I would have to rely on guesswork. I thought that Stefan's project would almost certainly beat me to that solution, as well.

Attempts On The Remaining Message

In the absence of a good crib for the remaining intercept, I started trying to guess the signature of the message, using the names of the relevant U-boat commanders. For example, for U-43 I might try "VONVONJSCHWANTKEJ"; for U-753, I might try "VVVJMANNSTEINJ." At first, I would also include the address "BDUUU" or one of its variants, until I learned that this would probably not be present. From time to time, as I began to run out of names to try, I would order another microfilm reel from the National Archives; but as the price kept increasing, this became more and more infrequent.

Attempts Based On "Offizier" Theory

When the distributed-computing efforts of the M4 Project also failed to break the remaining intercept, I began to think that the reason might be that it was a double-enciphered "Offizier" message. I wrote a special version of my software to deal with this possibility, and started using cribs like "VVVJBARGSTENJOFFIZIER" or "VONVONJWISSMANNJOFFZ." I didn't have any luck with this approach, either.

3. FINDING THE CRIB

Joining Michael's Project, And Learning Of His Efforts

It was Michael Hörenberg who finally provided me with the crib I had been looking for. When I learned of his "Breaking German Navy Ciphers" project to break the messages recovered from U-534, I volunteered to help with the translation of the decrypts into English. Michael and I began comparing notes, and I learned that he had also been working on the unbroken H.M.S. Hurricane intercept, along much the same lines that I had. He had obtained from his sources many of the same KTBs that I had, plus a few others that I didn't have; but together, we still didn't have those of all of the likely U-boats.

Joint Theory About The "0924/19/221" Message

In the KTBs of U-43, U-183, U-460 and U-608, we found an entry of just the second paragraph of a particular radio message, with the time/date/serial number "0924/19/221":

> *2) Schäfer, Rasch, Struckmeier melden ob Boote nach Ergänzung weiter maschinell und personell verwendungsbereit für Einsatz gegen Geleitzüge. Wenn ja, Schnoor ansteuern und dazu voraussichtliches Eintreffen melden. Für Schwantke gilt gleiches nach Beendigung seiner Geleitverfolgung.*
>
> [2) Schäfer (U-183), Rasch (U-106), and Struckmeier (U-608) report whether their boats after refueling will be ready, mechanically and in personnel, for action against convoys. If so, head for Schnoor (U-460) and report expected time of arrival. The same applies to Schwantke (U-43) after the end of his convoy pursuit.]

The first paragraph of the message was not entered in those KTBs, presumably because it did not concern those boats. We thought that if the whole message was a long one, it might have been sent in two parts, and the missing first part might be the unbroken intercept. In the transcription in Ralph Erskine's letter, the intercept was marked "T.O.R. 1152/19/221." The serial numbers matched, and we thought that the "1152" was the time of reception of the message. (The "0924" entered in the KTBs was the time of origin of the message.)

The missing first part of the message was not in any of the KTBs that Michael and I had, and enquiries I had made several years ago on a few U-boat-related Internet forums had come up empty. We both decided to try to get two more KTBs, those of U-106 (the one boat mentioned in the above message whose KTB we didn't have) and U-518. My order from the U.S. National Archives was expected to take six weeks or more to arrive; but Michael managed to obtain copies of the KTBs from his sources in just a few days. He very graciously sent me scans of the relevant pages, and suggested that we co-ordinate our efforts in order to avoid both of us covering the same ground.

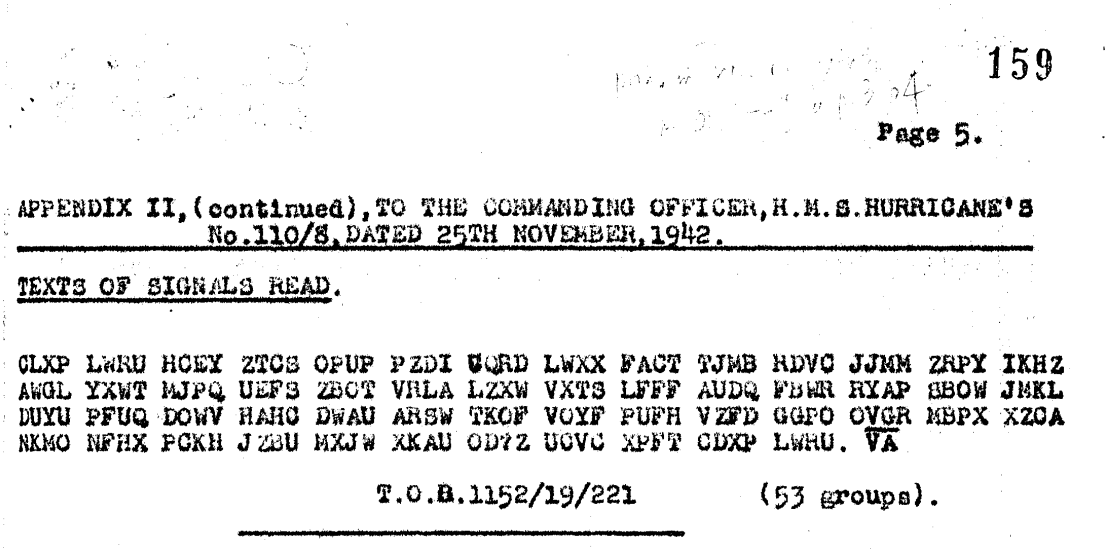
We Abandon Our Theory, And Adopt A New One

Both of the KTBs contained the missing first paragraph of the message — U-518's had just the first paragraph, and U-106's had the whole message. The first paragraph read:

> *1. Wißmann Marqu. BC 22 ansteuern.*
>
> [1. Wissmann (U-518) head for Naval Square BC 22.]

We started looking for arrangements of this plaintext that would not crash with the ciphertext, and even ran a few menus on our Bombe-simulator programs; but we soon realized that our theory of a two-part message could not be correct. On the one hand, the entire message, including both paragraphs, was not long enough to have required splitting it into two parts; and on the other hand, it was too long to have been the unbroken intercept.

I noticed, however, that Rasch's reply to this message, in the next entry in U-106's KTB, had the time/date serial number "1152/19/231", which was a very close match with the "1152/19/221" on the unbroken intercept. (I had previously seen this same message in U-460's KTB; but there it was entered without the time/date/serial number group.) We thought it possible that the "221"on the intercept might be the result of a Morse error in transmission or reception, or perhaps a mistake on the part of the clerk who typed the original report; and as to the "1152" on the intercept, I had reason to believe that it was not, in fact, the time of reception; but rather the time of origin.



159

Page 5.

APPENDIX II,(continued),TO THE COMMANDING OFFICER,H.M.S.HURRICANE'S No.110/S,DATED 25TH NOVEMBER,1942.

TEXTS OF SIGNALS READ.

CLXP LWRU HOEY ZTCS OPUP PZDI UQRD LWXX FACT TJMB RDVC JJMM ZRPY IKHZ
AWGL YXWT MJPQ UEFS ZBOT VRLA LZXW VXTS LFFF AUDQ FBWR RYAP SBOW JMKL
DUYU PFUQ DOWV HAHC DWAU ARSW TKOF VOYF PUFH VZFD GGPO OVGR MBPX XZOA
NKMO NFHX PCKH JZBU MXJW XKAU ODYZ UCVC XPFT CDXP LWRU. VA

T.O.B.1152/19/221 (53 groups).

Figure 1. Part of the scan of the original HF/DF report from H.M.S. Hurricane.[2]

[2] From The National Archives of the UK: ref. ADM 199/717 (Reproduced by permission.)

Several years ago, Ralph Erskine had shown me a scan of the actual page from H.M.S. Hurricane's HF/DF report containing the intercepts, which he had found in the U.K. National Archives. He explained that the document he had found was a poor carbon copy, and that many of the letters were hard to read. For example, it was often hard to tell whether a letter was a 'C' or an 'O'; or what looked like an 'X' might really be a 'K'. Also, a few letters seemed to have been corrected by overtyping, so that it was not clear which letter was the correct one. This is why the version of the ciphertext that I used differed slightly from the one in Ralph's letter to *Cryptologia* – mine was based on my own examination of the scan he had provided me.

One of the overtyped letters was in the time/date stamp on the unbroken message. In Ralph's letter, it is transcribed as "T.O.R. 1152/19/221"; but in the scan of the original it looks as if the 'R' in "T.O.R." had been overtyped with an 'O', making it "T.O.O." ("Time of Origin"). That would explain why the time/date stamp for this message differs from those of the other two, which end in just "/19Z" and "/21Z", without a serial number. It seemed that in those intercepts, the original time/date/serial number group transmitted by the German radio operators had been missed by the operator on H.M.S. Hurricane; but that the one for this message had been picked up (with the one error in the serial number). The length of the message in the KTB seemed an approximate match with that of the intercept, so Michael and I were fairly confident that we had found our crib.

We each began to look for ways that the plaintext might have been arranged by the German radio operator for encryption with the Enigma. Michael decided to test the theory that the message would begin with the sender's signature, as was the usual practice; and began to try the initial crib "VVVJRASCHJBOOTKLARXBEIJSCHNOORJETWAZWOSIEBEN" on his Bombe simulator. I decided to test the possibility that the signature had been put at the end of the message, as was occasionally done. I would first try the initial crib "BOOTKLARXBEIJSCHNOORJETWAZWO" with my Bombe-plus-hillclimber program.

4. DRAWING UP THE MENUS

Dividing The Crib

The task of drawing up the menus for input into the Bombe simulator from the crib/ciphertext alignment is done by hand, as I haven't worked out a way of automating that process.

My Bombe simulator can only handle one set of assumptions about the relative wheel positions at the various menu links per run of the program. This means that for short cribs of thirteen or fourteen letters (the minimum number of links my program usually needs, unless the menu is a strong one), it would need 26 or 28 runs to cover all of the turnover possibilities for the middle and slow wheels. For this reason, longer cribs are better, if they are available, so that the turnover possibilities can be covered with fewer runs.

The first thing is to divide the crib/ciphertext into several sections, and then draw up several different menus, skipping different sections each time, and assuming a middle wheel turnover

somewhere within the skipped sections. The links for each menu are taken only from the crib/cipher letter-pairs in the sections not skipped. The divisions I made for the above crib will illustrate this.

The crib-divisions for Menus 1, 2, 2a, 3 and 3a are for wheel orders with a single-notch wheel (1-5) as the fast wheel. The ring settings and prestart positions for all of the wheels are assumed to be at 'Z'.

Crib-division for Menu 1; assuming no middle wheel turnover until somewhere after the 18th letter:

```
Crib:         BOOTKLARXBEIJSCHNO----------
Ciphertext:   HCEYZTCSOPUPPZDICQ----------
Slow Wheel:   ZZZZZZZZZZZZZZZZZZ----------
Middle Wheel: ZZZZZZZZZZZZZZZZZZ----------
Fast Wheel:   ABCDEFGHIJKLMNOPQR----------
```

Crib-division for Menu 2; middle wheel turnover between the 8th and 19th letters, and no slow wheel turnover:

```
Crib:         BOOTKLAR----------ORJETWAZWO
Ciphertext:   HCEYZTCS----------RDLWXXFACT
Slow Wheel:   ZZZZZZZZ----------ZZZZZZZZZZ
Middle Wheel: ZZZZZZZZ----------AAAAAAAAAA
Fast Wheel:   ABCDEFGH----------STUVWXYZAB
```

Crib-division for Menu 2a; middle and slow wheel turnover between the 8th and 19th letters:

```
Crib:         BOOTKLAR----------ORJETWAZWO
Ciphertext:   HCEYZTCS----------RDLWXXFACT
Slow Wheel:   ZZZZZZZZ----------AAAAAAAAAA
Middle Wheel: ZZZZZZZZ----------BBBBBBBBBB
Fast Wheel:   ABCDEFGH----------STUVWXYZAB
```

Crib-division for Menu 3; middle wheel turnover anywhere before the 10th letter, and no slow wheel turnover:

```
Crib:         --------XBEIJSCHNOORJETWAZ--
Ciphertext:   --------OPUPPZDICQRDLWXXFA--
Slow Wheel:   --------ZZZZZZZZZZZZZZZZZZ--
Middle Wheel: --------AAAAAAAAAAAAAAAAAA--
Fast Wheel:   --------IJKLMNOPQRSTUVWXYZ--
```

Crib-division for Menu 3a; middle and slow wheel turnover anywhere before the 10th letter:

```
Crib:         --------XBEIJSCHNOORJETWAZ--
Ciphertext:   --------OPUPPZDICQRDLWXXFA--
Slow Wheel:   --------AAAAAAAAAAAAAAAAAA--
Middle Wheel: --------BBBBBBBBBBBBBBBBBB--
Fast Wheel:   --------IJKLMNOPQRSTUVWXYZ--
```

Wheel orders with one of the double-notched wheels 6, 7 or 8 as the fast wheel require a separate set of crib/ciphertext divisions, with the skipped sections coming at intervals of 13 letters instead of 26. For example:

Crib-division for Menu 4; middle wheel turnovers after the 8th and 21st letters, and no slow wheel turnover:

```
Crib:         BOOTKLAR-----SCHNOORJ-------
Ciphertext:   HCEYZTCS-----ZDICQRDL-------
Slow Wheel:   ZZZZZZZZ-----ZZZZZZZZ-------
Middle Wheel: ZZZZZZZZ-----AAAAAAAA-------
Fast Wheel:   ABCDEFGH-----NOPQRSTU-------
```

Crib-division for Menu 4a, middle and slow wheel turnover after the 8th letter:

```
Crib:         BOOTKLAR-----SCHNOORJ-------
Ciphertext:   HCEYZTCS-----ZDICQRDL-------
Slow Wheel:   ZZZZZZZZ-----AAAAAAAA-------
Middle Wheel: ZZZZZZZZ-----BBBBBBBB-------
Fast Wheel:   ABCDEFGH-----NOPQRSTU-------
```

Crib-division for Menu 5, middle wheel turnovers after the 3rd and 16th letters, and no slow wheel turnover. (The asterisks indicate a section that was not used in the menu, because there were enough links in the other two sections.):

```
Crib:         ***-----XBEIJSCH-----ETWAZWO
Ciphertext:   ***-----OPUPPZDI-----WXXFACT
Slow Wheel:   ZZZ-----ZZZZZZZZ-----ZZZZZZZ
Middle Wheel: ZZZ-----AAAAAAAA-----BBBBBBB
Fast Wheel:   ABC-----IJKLMNOP-----VWXYZAB
```

Crib-division for Menu 5a, middle wheel turnover after the 3rd and 16th letters, middle and slow wheel turnover after the 16th letter:

```
Crib:         ***-----XBEIJSCH-----ETWAZWO
Ciphertext:   ***-----OPUPPZDI-----WXXFACT
Slow Wheel:   ZZZ-----ZZZZZZZZ-----AAAAAAA
Middle Wheel: ZZZ-----AAAAAAAA-----CCCCCCC
Fast Wheel:   ABC-----IJKLMNOP-----VWXYZAB
```

Crib-division for Menu 5b, middle and slow wheel turnover after the 3rd and 16th letters, middle wheel turnover after the 16th letter:

```
Crib:         ***-----XBEIJSCH-----ETWAZWO
Ciphertext:   ***-----OPUPPZDI-----WXXFACT
Slow Wheel:   ZZZ-----AAAAAAAA-----AAAAAAA
Middle Wheel: ZZZ-----BBBBBBBB-----CCCCCCC
Fast Wheel:   ABC-----IJKLMNOP-----VWXYZAB
```

Crib-division for Menu 6, middle wheel turnovers before the 7th letter and between the 13th and 20th letters, no slow wheel turnover:

```
Crib:         -----LARXBEIJ-----ORJETWAZ--
Ciphertext:   -----TCSOPUPP-----RDLWXXFA--
Slow Wheel:   -----ZZZZZZZZ-----ZZZZZZZZ--
Middle Wheel: -----AAAAAAAA-----BBBBBBBB--
Fast Wheel:   -----FGHIJKLM-----STUVWXYZ--
```

Crib-division for Menu 6a, middle wheel turnover before the 7th letter, middle and slow wheel turnover between the 13th and 20th letters:

```
Crib:         -----LARXBEIJ-----ORJETWAZ--
Ciphertext:   -----TCSOPUPP-----RDLWXXFA--
Slow Wheel:   -----ZZZZZZZZ-----AAAAAAAA--
Middle Wheel: -----AAAAAAAA-----CCCCCCCC--
Fast Wheel:   -----FGHIJKLM-----STUVWXYZ--
```

Crib division for Menu 6b, middle and slow wheel turnover before the 7th letter, middle wheel turnover between the 13th and 20th letters:

```
Crib:         -----LARXBEIJ-----ORJETWAZ--
Ciphertext:   -----TCSOPUPP-----RDLWXXFA--
Slow Wheel:   -----AAAAAAAA-----AAAAAAAA--
Middle Wheel: -----BBBBBBBB-----CCCCCCCC--
Fast Wheel:   -----FGHIJKLM-----STUVWXYZ--
```

Totals: 5 menus for the 210 wheel orders with a single-notch fast wheel, 8 menus for the 126 wheel orders with a double-notch fast wheel; 13 in all. Of these, I only needed to actually run ten. Menus like 3a, 5b and 6b, which assume a slow wheel turnover before the first section used in each menu, produce stops equivalent to those produced by menus like 3, 5 and 6, which assume no slow wheel turnover. The only difference is in the start positions, and the part of my software that tests the bombe stops adjusts for this when making its trial decipherments.

Failure On The First Attempt

Unfortunately, after all of the menus based on these divisions had been run, the message remained unbroken. It was possible that the crib/ciphertext alignment was wrong; but it was also possible that one or more incorrect ciphertext letters had defeated the Bombe simulator, as had happened with the Schröder message.

Strategy For A Second Attempt

I tried again, this time using as a crib slightly more of the message beginning: "BOOTKLARXBEIJSCHNOORJETWAZWOSIBENX". I drew up the crib/ciphertext divisions so that each one would have at least sixteen links available for use in a menu. I could then draw up eight different menus for each division, systematically omitting a different pair of links from the available ones each time, and still have enough links left for my Bombe-simulator. If there was only one incorrect ciphertext letter in the crib/ciphertext alignment, then eventually a menu omitting that letter would be run that would also have the correct assumptions for the wheel positions.

To illustrate how the menus are actually drawn up from the crib/ciphertext division, here's the first of the divisions of the longer crib, with the links that will be used in the first menu marked with '+':

```
                  +++++++                  ++++++ +
Crib:          BOOTKLARX-----------------WOSIBENX
Ciphertext:    HCEYZTCSO-----------------CTTJMBRD
Slow Wheel:    ZZZZZZZZZ-----------------ZZZZZZZZ
Middle Wheel: ZZZZZZZZZ-----------------AAAAAAAA
Fast Wheel:    ABCDEFGHI-----------------ABCDEFGH
```

The first two crib/ciphertext letter-pairs, B/H and O/C, are omitted from this menu in case one of them has an incorrect ciphertext letter. I also omitted the link at the 'N' in "SIBEN", as I did in all my menus, because I was not sure if the ciphertext letter was an 'R', as I thought it appeared to be in the scan of the original, or an 'H', as it is given in Ralph's letter to *Cryptologia*. (Similarly, though it doesn't appear in this crib/ciphertext division, I omitted the link at the seventeenth letter of the ciphertext from any menus it would otherwise have appeared in; because while the ciphertext letter there is given as a 'U' in Ralph's letter, in the scan of the original it looked to me like a 'C' typed over a 'V'.)

The next step is to diagram the crib/ciphertext links, to see how they can be connected into chains, and if possible, into loops. Since Enigma encipherment is reciprocal, it doesn't matter whether the crib or ciphertext letter is mentioned first in each link. . Figure 2 shows the first few links to be diagrammed: H – B at wheel position ZZA, B – M at ZAE, B – E at ZAF, E – O at ZZC, O – T at ZAB, and T – Y at ZZD. Figure 3 shows the full diagram of the crib division, and the first menu derived from it.

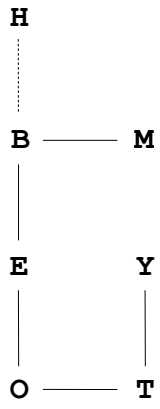
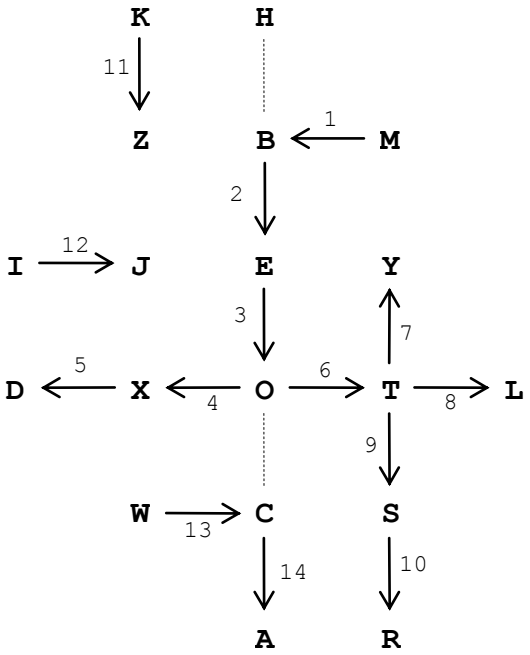


Figure 2. Beginning of the menu diagram.



MENU:

```
 1  MB ZAE
 2  BE ZAF
 3  EO ZZC
 4  OX ZZI
 5  XD ZAH
 6  OT ZAB
 7  TY ZZD
 8  TL ZZF
 9  TS ZAC
10  SR ZZH
11  KZ ZZE
12  IJ ZAD
13  WC ZAA
14  CA ZZG

Not used:

   BH ZZA
   OC ZZB
```

Figure 3. Complete diagram of the first division of the crib/ciphertext, and the first menu derived from it.

Although the links B-H at wheel position ZZA and O-C at ZZB will not be used in this menu, they are included in the diagram because they would be used in the other seven menus based on this division of the crib/ciphertext.

The first two letters in each menu link are the crib/ciphertext pair, in either order; the last three are the wheel core positions (again assuming rings set to ZZZ).

With one 10-letter chain, one chain with two links, and two with one link; and with no loops, this is a fairly weak menu. However, with the special feedback feature of my Bombe simulator, along with the Diagonal Board of the Turing-Welchman Bombe, it is nevertheless still usable.

5. THE BREAK

Success On The Second Attempt

With eight times as many menus to run as before, I expected the tests on the second, longer crib to take more than a week; but luckily, the message broke on the very first run, using the menu above on just the 210 wheel orders with a single-notched fast wheel. The Bombe had reached 374 stops, and on one of them, the hillclimber found settings that produced a solution:

```
B Beta 613 NBNE  AA BQ CR DI EJ ID JE KW LL MT OS PX QB RC SO TM UZ WK XP YY
ZU

B Beta 613 ZZDG NAQL  BQ CR DI EJ KW MT OS PX UZ GH

BOOTKLARXBEIJSCHNOORBETWAZWOSIBENXNOVXSECHSNULCBMXPROVIANTBISZWONULXDEZXBENOE
TIGEGLMESERYNOCHVIEFKLHRXSTEHEMARQUBRUNOBRUNFZWOFUHFXLAGWWIEJKCHAEFERJXNNTWWW
FUNFYEINSFUNFMBSTEIGENDYGUTESIWXDVVVJRASCH
```

The combination of ring setting ZZDG and message key NAQL is only one of many equally valid such combinations. With the “Greek” and slow wheel rings still at “ZZ”, and the prestart position of the slow wheel changed from ‘A’ to ‘B’, there are 17 more possibilities for the ring setting and prestart position of the middle wheel:

Rings	**Key**
ZZDG	NBRL
ZZEG	NBSL
ZZFG	NBTL
ZZGG	NBUL
ZZHG	NBVL
ZZIG	NBWL
ZZJG	NBXL
ZZKG	NBYL
ZZLG	NBZL
ZZMG	NBAL
ZZNG	NBBL
ZZOG	NBCL
ZZPG	NBCL
ZZQG	NBEL
ZZRG	NBFL
ZZSG	NBGL
ZZTG	NBHL

Since we have no other messages on this day’s key to use as a check to positively identify the ring setting for the middle wheel, it’s impossible to know which of these is the right one. Moreover, since the rings on the “Greek” and slow wheels have no effect on the encipherment process, the actual ring settings for these wheels in the daily Enigma key cannot be worked out from a single message. Working these out would require at least one more message enciphered with that day’s key, plus the bigram table that was used to encipher the indicator groups.

The decrypted plaintext shows that it had, in fact, been an incorrect ciphertext letter that had prevented success with the first set of menus. The menu with the correct wheel-turnover assumptions had unfortunately included the bad link. (This was at the 21st ciphertext letter, 'L', which a re-encipherment of the corrected plaintext shows should be 'O'. The incorrect ciphertext 'L' makes what should be "JSCHNOORJ" come out as "JSCHNOORB".)

Advantage Of The Bombe-Feedback Feature

In order to illustrate the advantage of the special feedback feature of my Bombe-simulator, I did two test runs of the menu on wheel order B Beta 613 only – the first with the feedback feature turned off, and the second with it on. The first run took about 1 minute and 21 seconds to test all 456,976 wheel start positions, and produced 99 stops, including the correct one:

```
B Beta 613 NBNE  BQ DI EJ LL MT OS RC SO TM XP YY
```

The Bombe identified seven of the ten stecker-pairs: BQ, DI, EJ, MT, OS, RC, and XP; plus two of the self-steckered letters: LL and YY; leaving three stecker-pairs for the hillclimber to find out of the remaining ten letters. Notice that here, only two of the stecker-pairs are confirmed: MT/TM and OS/SO.

The second run, with the feedback turned on, took only 21 seconds, and produced just 4 stops, including the right one:

```
B Beta 613 NBNE  AA BQ CR DI EJ ID JE KW LL MT OS PX QB RC SO TM UZ WK XP YY
ZU
```

A bonus by-product of the feedback feature's process of confirming the stecker-pairs from the ordinary stop was the identification of two additional stecker-pairs, KW and UZ, and another of the self-steckered letters, AA; leaving only one stecker-pair for the hillclimber to find, out of just five remaining letters.

Each Bombe stop has to be tested by the hillclimber portion of the program, and the more work the hillclimber has to do, the longer each run takes. Reducing the number of stops, and at the same time increasing the number of stecker-pairs found by each stop, is obviously a big time-saver.

The Role Of Luck In The Break

It had been just my good fortune to have been the one to guess the right arrangement of the plaintext to use as a crib, instead of Michael; it could just as easily have been the other way around.

In fact, the break involved a considerable amount of luck, starting with the finding of the message plaintext in the war diary, just below the message that we had mistakenly thought might have been the right one. I was also fortunate that I had not used more of my guess for the

plaintext arrangement than I did: the text of the message as it is entered in the war diary gives the expected date of the rendezvous with Schnoor as “27.11.”, which I had guessed would be rendered in the Enigma plaintext as “ZWOSIBENXELFX”; but it actually turned out to be “ZWOSIBENXNOVX” instead. If I had used “ELF” in my crib, instead of stopping with “ZWOSIBENX”, the Bombe simulator would not have found the right stop.

Another bit of luck was the fact that there was only one wrong letter in the portion of the ciphertext that aligned with the crib: if several incorrect letters had been scattered throughout that part of the ciphertext, the Bombe would have failed.

6. POST-BREAK ANALYSIS

Tests With Hillclimbing Alone

Out of curiosity as to whether a ciphertext-only hillclimbing attack could have broken the message, I did some tests with a stand-alone hillclimber program, testing only the correct wheel order, ring setting and message key. In addition to my version of the ciphertext and the version in Mr. Erskine’s letter, I also tested a “perfect” ciphertext, made by re-enciphering the plaintext with all of the garbled letters corrected; and, for comparison, the Looks and Schröder messages, truncated to 196 letters (the length of the Rasch message).

The truncated Schröder message broke on the first hillclimb, starting from an empty plugboard; and another 9631 times out of 20 thousand restarts from random sets of plugboard connections. The truncated Looks message did not break on the first hillclimb; but it did break 9761 times out of the same number of restarts.

As expected, the results for the Rasch message were not as good. The hillclimber failed to break any of the three versions of the ciphertext on the first hillclimb. The results for the random restarts were a little surprising: in its best configuration, the hillclimber broke the “perfect” version just 567 times out of 20 thousand restarts, and the “Erskine” version 245 times; but it only broke my version, which actually has fewer incorrect letters than the “Erskine” version, just 51 times. In the next-best configuration of the hillclimber, the number of breaks decreased to 504 for the “perfect” version, and all the way down to 25 for the “Erskine” version; but actually increased to 85 for my version. I have no explanation for this.

Statistical Comparison

An examination of the statistics for the decrypted plaintexts gives some indication of why the hillclimber had so much more trouble with the Rasch message than with the Looks and Schröder messages.

Message	Index of Coincidence	Bigram Score	Trigram Score
Truncated Looks Message	0.0551020	8194971	4893508
Truncated Schröder Message	0.0613291	8252177	4682246
Rasch Message ("Perfect" version)	0.0488749	7498743	3883935
Rasch Message (My version)	0.0464155	7177481	3480091
Rasch Message ("Erskine" version)	0.0449503	7033458	3258581

The Index of Coincidence (I.C.) for even the "perfect" version of the Rasch message is quite low, and still lower for the other two versions. Similarly, the bigram and trigram scores for all three versions of the Rasch message are considerably lower than those of the Looks and Schröder messages. My hillclimber was configured to do one pass using the I.C. for scoring, a second pass with bigram scoring, and two or more passes with trigram scoring. The relatively flat letter-distribution indicated by the low I.C. would have made it difficult for the first pass to get a good start in correctly identifying the first few plugboard connections, and the low n-gram statistics of the underlying plaintext would have made it difficult for subsequent passes to recover from a poor start.

I expected that the atypical statistics of the Rasch message had caused similar difficulty for Stefan Krah's M4 Project, accounting for their failure to break it after having had such rapid successes with the Looks and Schröder messages. Stefan has since told me that he has done some tests with his hillclimber software and n-gram files, using the correct wheel order, rings and message key, and that it needs an average of about 30 restarts to break the full ciphertext. He said that the M4 Project had originally done 15 walks through the full M4 keyspace with the whole message, but then switched to tests on smaller blocks of the message, in case there were letters missing somewhere in the ciphertext. They had just been unlucky that the solution had not come up before they stopped their runs on the full ciphertext.

Final Thought

When Rasch received the "0924/19/221" message, to which the "1152/19/231" message was his reply, he had evidently been anxiously awaiting orders for some time. After entering the first message in his war diary, he added this comment, which also sums up my reaction to the message break:

> *Endlich! Das war ein sehr erfreulicher F.T.*
>
> [At last! This was a very pleasant radiogram.]