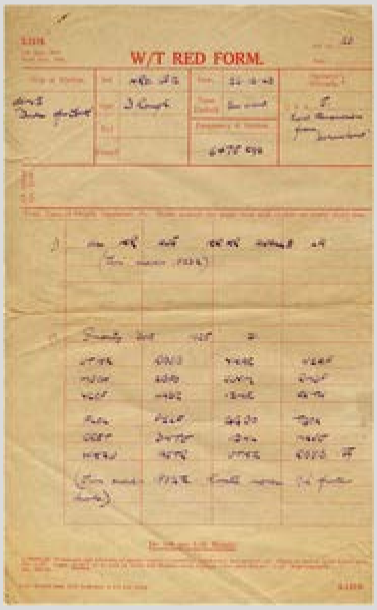
Scharnhorst’s Last Message?

The ciphertext message below is suspected to be the last message from the German battlecruiser *Scharnhorst*. The message was intercepted by one of the the radio officers, D. Rough, on board the English battle ship *Duke of York* in the evening of 26 December 1943. The message, which was transmitted in Morse code, was received on a HRO receiver and written out on the customary W/T Red Form. The Red Form has been found among the papers of Edward Thomas who was the intelligence officer on board the *Duke of York*. Today the Red Form is owned by the collector Mr. Colin Waghorn and I am grateful for his permission to publish this historical document here.



W/T RED FORM.

In December 2007 Geoff and I were contacted by the Bombe Rebuild Project to hear if we could help with breaking this message. The rebuilt Bombe at BP did not have the necessary Naval Enigma rotors and they wondered if our E-Breaker program would be able to do the job. Unfortunately, we don’t have a Naval Enigma version of this program and both Geoff and I were too busy with work and other tasks to envisage starting yet another codebreaking project. We kindly asked for permission to give the message to Dan Girard, who since then has been trying to break the message with a Bombe simulator using cribs from the plaintext message. Here is a report on his attempts so far:

> *I’ve had no success with the Scharnhorst message. I’ve tried the "vierneunneunzwo" crib in various positions; also "steuereauftanafjord," "steuereaufjtanafjordj," "steuerenachtanafjord," "steuerejtanafjordjan," etc.; and, at the beginning of the message, the signatures "vvvjscharnhorstj," "vonvonjscharnhorstj," and "vonvonscharnhorst." I’ve also tried "mueckevvvjscharnhorst" as a crib. The other urgency codewords, “biene” and "wespe," and the variants "bine," “mucke” and "muke" all result in crashes when placed before the signatures, so I didn’t try those.*
>
> *Nothing has worked. Of course, until the message is broken there’s no way of*

> *knowing whether this was due to garbled ciphertext letters or because the cribs were either incorrectly aligned or wrongly worded.*

A good account of what happened during the *Scharnhorst* battle has been given by Patrick Beesley in his book *Very Special Intelligence*. Here is an extract from page 216 that describes the final hours of the battlecruiser *Scharnhorst* and the transmission of its last message:

> At 4.17 p.m., *Duke of York* gained radar contact with the enemy and at 4.50 opened fire. Once again *Scharnhorst* was taken by surprise. At 4.56 she signalled to Gruppe Nord-Flotte: ‘Most Immediate. 72 degrees 39 North, 26 degrees 10 East. Heavy battleship. Am in action.’ Bey evidently mistook some of Burnett’s cruisers for battleships because at 5.22 he signalled that he was ‘surrounded by heavy units.’ The situation soon became hopeless. At 6.02 a signal went off to ‘Admiral of the Fleet and the Commander-in-Chief. *Scharnhorst* will ever reign supreme,’ and this was followed at 6.25 by one to Hitler, ‘We shall fight to the last shell.’ *Scharnhorst*’s last signal was made at 7.25, stating that she was steering for Tanafjord at 20 knots. It seems unlikely that she was still capable of this speed because, shortly before she had reported it as only 15 knots, and within another twenty minutes, after repeated hits from *Duke of York*’s 14-inch guns, from the lesser armament of the cruisers and from eleven of the many torpedoes fired at her by the British destroyers, she sank. Despite every effort only thirty-six survivors could be rescued.

As explained in *Very Special Intelligence* most of the messages from *Scharnhorst* and Admiral Northern Waters were quickly broken and decoded at Bletchley Park (BP). The messages were enciphered on the 3-rotor Naval Enigma machine M3 and most of them were using the *Allgemein* (general) settings from the Enigma key *Heimisch*. *Heimish*, later renamed *Hydra* and called Dolphin by BP, was the Enigma key used by U-boats and surface ships in German home waters, in the North Sea, and the Atlantic. A few of the signals were enciphered using the *Offizier* setting of the *Heimisch* key. These signals were usually decoded but with a delay of two to three weeks. One *Offizier* signal that was transmitted on 18 December 1943 and that instructed the Battlegroup with *Scharnhorst* to take ‘preparatory measures so that departure would be possible at any time’ seems to have been broken with a delay of only two days.

Ciphertext and suspected plaintext

W/T Red Form

```
Ship or Station:     | Set: H.R.O. No. 2  | Date: 26.12.1943      | Operator's
                     | Opr.: D. Rough.    | Time  : See below     | Remarks:
HMS "Duke of York"   |                    | Ended                 | QSA:  5
                     | To:                | Frequency & System:   |   Last
transmission
                     | From:              |    6475 kc/s          |   from
Scharnhorst
----------------------------------------------------------------------------
```

```
----------

        1)      de KR ANA KR.KR AN ALLE LA
                  ( Time ended: 1823Z )

        2)      Priority dots.   1925   21.

                UTKZ RBSB YKAE NZAP
                MSCH ZBFO CUVM RMDP
                YCOF HADZ IZME FXTH
                FLOL PZLF GGBO TGOX
                GRET DWTJ IQHL MXVJ
                WKZU ASTR UTKZ RBSB

                ( Time ended: 1832Z. Erratic morse. Nil further
                  heard. )
```

BP Decode Teleprint

```
        VX
        ADM(1)                                                          128
        TO I D 8 G
        FROM N S                                     ZIP/ZTPG/200000
        6475 KC/S       T O O 1925                   TOI 1830/26/12/43

        FROM:  SCHARNHORST                                             7157
N
                                                                       2830
E
           AM STEERING FOR TANAFJORD. POSITION IS SQUARE AC 4992,
           SPEED 20 KNOTS.
        (DEPT. NOTE: THIS WAS THE LAST TRANSMISSION MADE BY
               SCHARNHORST)

        0645/13/1/44+EE/AM
```

Facsimile of the Red Form and the BP Decode (*PDF format*)

The Red Form shows two messages labeled 1) and 2). The first message seems to be an emergency warning to everybody (*An Alle*) that a KR KR message – *Kriegsnotmeldung* (war emergency message) was to be expected. The regulations for the use of a war emergency message was very strict: *Kriegsnotmeldungen dürfen nur bei unmittelbarer Gefahr und höchster Notlage für Schiff und Besatzung abgegeben werden* — War emergency messages must only be transmitted when immediate danger and the highest emergency exist to ship and crew. The transmitting station uses the callsign ANÄ, which is an Umlaut callsign — Umlautfunkname. These callsigns, which could not be enciphered, were usually given to fixed land stations. If it was exceptionally given to *Scharnhorst* for this engagement is not known. Nor is the meaning of LA understood. It could be a frequency reference as the German naval frequencies were given two letter designators, however the frequency lists I have access to shows *la* as 109 kHz and the frequency 6475 kHz is not listed.

The second message is the suspected last message from *Scharnhorst*. It starts of with some priority dots and then gives the time of origin, 1925, and the number of cipher groups, 21. A quick look at the message shows that it has 24 groups. If the error in group count is due to the cipher operator on *Scharnhorst* or the radio operator on the *Duke of York* is impossible to say. The message is in the standard Naval Enigma format with the two first 4-letter groups being respectively the Schlüsselkenngruppe (Cipher Indicator Group) and the Verfahrenkenngruppe (Procedure Indicator Group), both being repeated as the two last groups of the message. For further information please see the General Naval Enigma Procedure – Der Schlüssel M Verfahren M Allgemein.

As can been seen from the BP decode the last message from Scharnhorst was decoded on 13 January 1944, almost three weeks after it was transmitted. What does this mean? The most obvious reason is that this message was transmitted in the *Offizier* key and BP had difficulties in breaking this key. As the battle was over there would not have been a great urgency in breaking the message and this could also account for the delay. Another possibility is that BP's intercept stations failed to receive this message and that they first got a copy after the *Duke of York* was back in harbour. In this case the decoding of the message could also easily have been delayed by two, three weeks.

Message Broken

The M4 Message Breaking Project started a break on this message on 27 May 2008 at 22:39:21. Less than 24 hours later, on 28 May 2008 at 18:16:21, the message was broken. The German plaintext does indeed correspond to the English plain text in the BP teleprint. The raw German plaintext is:

```
steuere j tanafjord j an standort qu aaa ccc vier neun neun zwo
fahrt zwo nul sm xx scharnhorst hco
```

Written out in full it becomes:

```
Steuere Tanafjord an. Standort Qu. AC 4992,
Fahrt 20 sm [Seemeilen].
Scharnhorst
```

The Enigma key for Scharnhorst's Last Message:

```
UKW         : B
Wheel Order : 368
Stecker     : AN, EZ, HK, IJ, LR, MQ, OT, PV, SW, UX
Rings       : AHM
Message key : UZV
```

The full details are given in the M4 Project Report on the Scharnhorst break. By studying Ralph Erskine's notes on Breaking Naval Enigma (Dolphin and Shark) and The *Kenngruppenbuch* Indicator System, and using Geoff Sullivan's Enigma M3 or Enigma M4 simulators you should be able to verify for yourself that the decode is correct.

Dan Girard was indeed only a hair's breadth from breaking this message with his Turing Bombe simulator. Here is his story:

> *Since "steuerejtanafjordj" is one of the cribs I had tried with my bombe simulator,*

> *it’s obvious that I must have made a mistake somewhere; and sure enough, on re-checking the menus I had drawn up for this crib, I find that I had misread one of the links from the diagram I had made. I had drawn up seven different menus from the crib, in order to allow for different turnover possibilities; and it was just my bad luck that the only one of the seven on which I made the mistake was the one which had the right turnover assumption. This is embarrassing!*
> *I’ve checked on the "vierneunneunzwo" crib, and it turns out that one of the positions I tried it in was the correct one; but unfortunately for me I had assumed that since there was a comma between "4992" and "speed" in the translated decrypt, there would be one in the German plaintext, as "vier neun neun zwo y fahrt...;" and I included the "y" in the crib. I’ve just re-run the relevant menu, omitting that link, and found that it would have worked.*

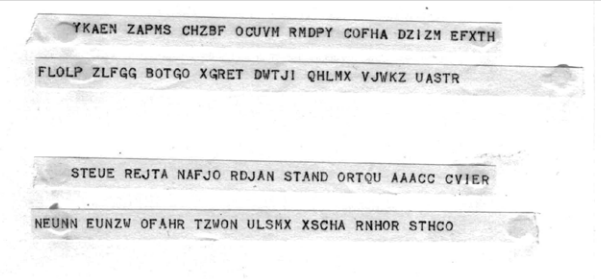
This shows yet again that selecting cribs and constructing menus is indeed more of an art than a science; an art where the codebreakers at Bletchley Park were the real masters. We should all stand in awe of their achievements.

Closing the circle

Yesterday, 30 April 2010, I received the following good news from Paul Kellar at BP:

> *Hello everybody*
>
> *This is the last link in the chain from the original Red Form.*
> *We have made the rotors 6,7 and 8 for our Typex (which, as you know, we have previously*
> *converted to behave like an Enigma, as they did at BP).*
> *This would output both the original and the decrypt on paper tape which, like a telegram*
> *was gummed to a message form. It groups letters by fives, as you see.*
> *Using the settings from Frode's group we have decoded the original message to reproduce*
> *the decoded output as seen 66 years ago.*
>
> *Thanks, everybody!*
>
> *Regards*
> *Paul*

And this is how the Scharnhorst messages would have looked like when it was decoded at BP in January 1944.



```
YKAEN ZAPMS CHZBF OCUVM RMDPY COFHA DZIZM EFXTH
FLOLP ZLFGG BOTGO XGRET DWTJI QHLMX VJWKZ UASTR

STEUE REJTA NAFJO RDJAN STAND ORTQU AAACC CVIER
NEUNN EUNZW OFAHR TZWON ULSMX XSCHA RNHOR STHCO
```

Acknowledgments

We should first of all like to thank the Bombe Rebuild Team who immediately thought of us when they realized they were not in a position to attack this message. Of the team we should like to particularly thank John Harper, Paul Kellar, Mike Hillyard, and John Borthwick, who sent us the copies of the Red Form and the teleprint with the BP Decode. Special thanks goes to John Gallehawk, who through his thorough and persistent search in the National Archives at Kew discovered the BP Decode teleprint. Futhermore, we are most grateful to Dan Girard who stepped into our shoes to do the work Geoff and I had neither the time nor the energy to do. Finally we should like to thank the owner of the Red Form, Colin Waghorn and his partner Dr. Rebecca Hill. And as always we are most grateful to have Ralph Erskine as our friend and mentor, who is always there to hold our hands when the sea gets rough.

Further Information

- The Sinking of the *Scharnhorst* by Norman Fenton, BBC World War II History
- If you are interested in seeing detailed plans of how and where the battle took place then you should have a look at the book German Capital Ships and Raiders in World War II by First Sea Lord Eric Groove.
- In his book, Enigma: The Battle for the Code, Hugh Sebag-Montefiore has a good description of sinking of the *Scharnhorst* in Chapter 24.

For more information about our codebreaking projects see our Web Portal: **Breaking German Wehrmacht Ciphers**.

Back to Frode’s CryptoCellar

Site visitors:
Statcounter

Breaking German Wehrmacht Ciphers

S.1319.

Est. May, 1925.
Revd. Nov., 1931.

Ref. No. 23.

Page

W/T RED FORM.

Ship or Station.	Set	H.R.O. No 2.	Date.	26.12.43	Operator's Remarks.*
HMS "Duke of York"	Opr.	D Rough.	Time Ended§	See below.	Q. S. A. 5. Last transmission from "Scharnhorst"
	To†		Frequency & System.		
	From†		6475 Kc/s.		

All before the Text.

Text, Time of Origin, Signature, etc. Write ACROSS the page, code and cypher on every third line.

i) de KR ANĀ KR.KR ANALLE LA

(Time ended:- 1823Z.)

ii) Priority Dots. 1925 21.

UTKZ	RBSB	YKAE	NZAP
MSCH	ZBFO	CUVM	RMDP
YCOF	HADZ	1ZME	FXTH
FLOL	PZLF	GGBO	TGOX
GRET	DWTJ	1QHL	MXVJ
WKZU	ASTR	UTKZ	RBSB. Ā

(Time ended:- 1832Z. Erratic morse. Nil further heard.)

Do not use Left Margin.

G 03556/25. *Constancy and reliability of signals, quality of operating, interference, atmospherics, etc. †Name of Station; if not known leave blank. §G.M.T. to be used on Home and Mediterranean Stations, other users indicate "Zone" Time employed.
Sta. 1/30.
Sta. 103/31.

128

VX
ADM(1)
TO I D 8 G
FROM N S

ZIP/ZTPG/200000

6475 KC/S   T O O 1925   TOI 1830/26/12/43

7157 N
2830E

FROM: SCHARNHORST

AM STEERING FOR TANAFJORD . POSITION IS SQUARE AC 4992.
SPEED 20 KNOTS.

(DEPT. NOTE: THIS WAS THE LAST TRANSMISSION MAAX MADE BY
SCHARNHORST)

0645/13/1/44+EE/AM

back to index
M4 Project
M4 Project Blog

This is the third break of the M4 Project:

Ciphertext (stripped of indicator groups):

```
ykaenzapmschzbfocuvmrmdpycofhadzizmefxthflolpzlfggbotgoxgretdwtjiqhlmxvjwkzuastr
```

Plaintext (as seen in the server logs):

```
Date: 2008-05-28 18:16:31
Score: 1863727
UKW: B
W/0: 368
Stecker: ANBJEZHKLRMQOTPVSWUX
Rings: AGM
Message key: UYV

ilpgureitanaffordianstandortquaadcccvberneunneunzwefahrtzwonulshexscharxhorsthco
```

Plaintext (with adjusted rings and message key):

```
UKW: B
W/0: 368
Stecker: ANEZHKIJLRMQOTPVSWUX
Rings: AHM
Message key: UZV

steuerejtanafjordjanstandortquaaacccvierneunneunzwofahrtzwonulsmxxscharnhorsthco
```

Result:

```
Steuere Tanafjord an. Standort Qu. AC 4992, Fahrt 20 sm [Seemeilen].
        Scharnhorst
```

Translation:

A suspected plaintext had already been located in a BP Decode Teleprint [see Scharnhorst message]. Our break confirms that this is indeed the correct plaintext.

```
VX
ADM(1)                                                            128
TO I D 8 G
FROM N S                                    ZIP/ZTPG/200000
6475 KC/S       T O O 1925                  TOI 1830/26/12/43

FROM:  SCHARNHORST                                               7157 N
                                                                 2830 E
   AM STEERING FOR TANAFJORD. POSITION IS SQUARE AC 4992,
   SPEED 20 KNOTS.
(DEPT. NOTE: THIS WAS THE LAST TRANSMISSION MADE BY
              SCHARNHORST)
```

0645/13/1/44+EE/AM

Contact:

Stefan Krah <website @ bytereef.org>