Excerpts from article submitted to Cryptologia on
22 February 2005,
please see: http://www.dean.usma.edu/math/pubs/cryptologia/

## Table of Contents

Page intentionally blank

# BREAKING GERMAN ARMY CIPHERS

Geoff Sullivan[1] and Frode Weierud[2]

ADDRESS: (1) 64 Tennyson Road, Headless Cross, Redditch, Worcs., B97 5BJ, UNITED KINGDOM. Email: geoff@blueangel.demon.co.uk – URL: http://www.hut-six.co.uk/
(2) Le Pre Vert, 1041 Rte de Mategnin, F-01280 Prevessin-Moens, FRANCE. Email: Frode.Weierud@cern.ch – URL: http://cryptocellar.org/

ABSTRACT A large number of encrypted German Army radio messages, from 1941 and 1945, have survived the end of the Second World War to the present day. Most of these messages are enciphered on the three-wheel, steckered *Wehrmacht* Enigma. We present an account of a ciphertext-only cryptanalysis of these messages and give details of the Enigma procedures used in the networks.

KEYWORDS: Enigma, German Army Ciphers, cryptanalysis

## INTRODUCTION

This is the first report of an on-going cryptanalytical project, which can best be described by the title Breaking German Army Ciphers. The project has its origins in an attempt to devise good, computerised cryptanalytical techniques that can solve authentic Enigma messages. By this we mean Enigma messages that are shorter than the authorised limit of 250 letters, enciphered on a standard three-wheel, steckered *Wehrmacht* Enigma machine. The project would never have got off the ground without access to a sufficiently large number of authentic messages with which to develop and refine our technique.

By lucky circumstances a large number, in excess of 500, of encrypted German Army radio messages (*Funkspruch*)[1] from 1941 and 1945 have survived the end of the Second World War to the present day. The majority of these messages are Enigma while a few are in a hand cipher that we suspect is a variant of *Doppelkastenschlüssel*, Double Playfair. These messages are being catalogued and transcribed. Good progress is being made in breaking the Enigma keys and transcribing the message plaintext. It is hoped that the entire collection can be published in the near future, but the nature and volume of this task is beyond the scope of this paper, which deals only with the technical issues of breaking the messages and reporting the Enigma procedures in use. Because we have no prior knowledge of the content of these messages, we cannot use techniques based on the Turing-Welchman Bombe, the electromechanical key finding machine, developed during the war at the Government Code and Cypher School (GC & CS) at Bletchley Park. Our attack is therefore of the variety called a ciphertext-only attack and is based on statistical techniques.

## THE MESSAGE FORMS

The German Army messages are written in pencil on printed message forms. Two examples are shown in Appendix E. We do not have access to the originals but only to photocopies. As the message forms seem to be made from some type of greyish, perhaps recycled, paper the photocopies are sometimes very dark and the contrast is poor. The content can best be described as dark grey pencil marks on light grey paper, and therefore transcribing them is at best a painstaking process. Furthermore, the various radio/cipher operators all have slightly different handwriting even though

[1] The 1941 messages are on forms designed to be used with *Fernspruch* (telephone/telegraph message), *Funkspruch* (radio message), and *Blinkspruch* (Morse lamp message). On all the 1941 message forms *Fernspruch* and *Blinkspruch* have been crossed out, leaving only *Funkspruch*. The 1945 messages are on dedicated Funkspruch forms.

they have all been trained to take down Morse code in lower case letters using what seems to be a standardised script. Hence the first step in the codebreaking process is to decipher the operator hieroglyphs and at best make educated guesses at faint or nearly illegible letters. The final hurdle in recovering correct plaintext from faulty ciphertext has to do with bad radio reception or poor operators. When plaintext finally appears, we often discover letter errors that can only be explained by incorrect Morse code reception. Due to the statistical techniques we employ, we are nevertheless able to break messages starting from somewhat faulty ciphertext.

The messages are from two periods, June to October 1941 and April 1945. The messages from 1941 all appear to be from the campaign against Russia, Operation Barbarossa. The units all belong to *Heeresgruppe Nord* (Army Group North) and many of the messages are from *Panzergruppe* 4 (Tank Group 4) and SS *Panzer* T (*Totenkopf* – Death's Head) Division. Other messages concern *Armeekorps* XXXXI (Army Corps 41) and *Armeekorps* LVI (Army Corps 56) and various infantry divisions and regiments. The messages may be of interest to historians studying the history of German military units and to local historians in Lithuania, Latvia and the areas south of St. Petersburg (Leningrad). The messages contain many place names and it is to some extent possible to follow the advance of the German forces though this area.

The 1945 messages deal with a dark chapter in German history, the Nazi concentration camps. The collection consists of a total of 258 messages of which 48 are multi-part messages, three of these being five-part messages. The messages, which are divided into an incoming and an outgoing batch, seem to come from the communication centre of Flossenbürg concentration camp. KL[2] Flossenbürg was built in the spring of 1938 on the German-Czech border northeast of the town of Weiden [12]. The majority of the messages are between KL Flossenbürg[3] and *Amtsgruppe D*[4] of the *SS-Wirtschafts- und Verwaltungshauptamt* (WVHA)[5] situated in Oranienburg near Berlin [15]. Some messages are addressed to other concentration camps e.g. Buchenwald, Gross Rosen, and Flossenbürg's *Außenlager*.[6]

We have identified two Enigma keys that are explicitly mentioned in a few messages dealing with cipher security and the transfer of Enigma machines and keys. The principal key for this traffic was the *KL-Maschinenschlüssel* [7] while on a few occasions we have identified an additional key that presumably is the key referred to as the *SS-Querverkehr-Maschinenschlüssel* 13A.[8] The messages deal with various administrative matters including the transport of prisoners to and from KL Flossenbürg. In April 1945 KL Flossenbürg received prisoners from other camps that were being closed due to the Russian advances on the eastern front. At the same time it was confronted with the advancing American forces in the west and the forced closure of many of its *Außenlager.*

---

[2] KL = *Konzentrationslager* (concentration camp). The usual German abbreviation is KZ, but in the SS (*Schutzstaffel*) communications KL is used instead.

[3] Most of the messages are signed by the camp commander, *SS-Obersturmbannführer* Maximilian Kögel. Max Kögel hanged himself in his cell in Schwabacher prison on 27 June 1945, exactly 24 hours after his capture.

[4] *Amtsgruppe D* – Department D, was the office responsible for the concentration camps under the leadership of *SS-Gruppenführer* Richard Glücks.

[5] WVHA – SS Economic and Administrative Main Office, under the command of *SS-Obergruppen-führer* Oswald Pohl.

[6] *Außenlager* = sub-camp – camp or commando attached to Flossenbürg where the prisoners worked in various industries. Flossenbürg had more than 100 *Außenlager*.

[7] *KL-Maschinenschlüssel* = Concentration Camp Machine (Enigma) Key. The key we have broken is either Nr. 12 or Nr. 13. This is most likely the key Bletchley Park (BP) called Grapefruit and which they broke only once on 21 August 1944 [9, p. 487].

[8] *SS-Querverkehr-Maschinenschlüssel* = SS Cross-Traffic Machine Key. This is probably the key BP called Medlar; first broken on 29 May 1944 and rarely broken afterwards [9, p. 487].

KL Flossenbürg was not an extermination camp and it had very few Jewish prisoners. Nevertheless, more than 30,000 people were killed or died in this camp where the inmates were mainly political prisoners, criminals, so-called "antisocial elements", homosexuals, Jehovah's Witnesses, and foreign prisoners of 30 different nationalities. From April 1944 until the last days of its existence in April 1945 KL Flossenbürg was increasingly used as a Nazi execution camp. Several of the messages are execution orders or final reports about completed executions. Perhaps the historically most significant of these is the four-part message Nr. 69 sent at 16:33 on 9 April 1945 from Walter Huppenkothen.[9] The message is marked *Geheim* and is addressed to *SS-Gruppenführer* Glücks who is kindly requested to immediately inform the chief of *Gestapo, SS-Gruppenführer* Müller, by telephone, telex or through messenger that his mission has been completed as ordered. The mission he had accomplished was the summary execution of the last prominent members of the German resistance movement connected with the assassination attempt on Hitler on 20 July 1944. In the early morning of 9 April 1945 Admiral Wilhelm Canaris, General Hans Oster, *Heereschefrichter*[10] Dr. Karl Sack, *Hauptmann*[11] Ludwig Gehre and pastor Dietrich Bonhoeffer were hanged in the courtyard at KL Flossenbürg.

The message forms give a unique glimpse into Enigma history; there are no other examples of messages in such volume known to the authors. There are reported to be around 250 *Luftwaffe* intercepts in the Bletchley Park Trust Archive, but these Army message forms are different since they originate from the Enigma operators complete with all headings and annotations. For cryptological historians they are of great interest because for the first time it is possible to analyse in detail how the German army radio/cipher operators performed, how well they respected security regulations and what errors they made.

[9] *SS-Standartenführer* Walter Huppenkothen was chief of the *Gruppe E – Spionageabwehr* (Group E – counter-espionage) in the RSHA department IV, Gestapo.
[10] *Heereschefrichter* = Chief Army Judge.
[11] *Hauptmann* = Captain.

**SUMMARY**

Figure 11 shows a summary of the message form contents. Multi part messages are each counted in arriving at the message numbers, since they are separately enciphered. The number of messages unbroken does not include messages yet to be processed on broken days, however since only a few other keys have been found in addition to the main key, we do not expect these figures to increase much. A number of messages on another cipher, Double Playfair, are distributed in the 1941 set, mostly for the months of June and July, and these will be dealt with as a separate project. Hand ciphers were in use as a reserve cipher on Enigma networks and were occasionally used on the Russian Front [8, p. 670].

| Date | Number of Enigma message parts | Total message length | Unbroken |
|---|---|---|---|
| June 1941 | 42 | 5440 | 2 |
| July 1941, Batch A | 8 | 1139 | 1 |
| July 1941, Batch B[12] | 50 | 4755 | — |
| August 1941 | 114 | 12337 | 3 |
| Sep. 1941, Batch A/B[13] | 220 | 24970 | 1 |
| Sep. 1941, Batch C[14] | 5 | 577 | 5 |
| October 1941 | 18 | 2687 | 0 |
| April 1945 | 332 | 50717 | 0 |
| Total | 789 | 102622 | 12 |

Figure 11. Summary of Enigma messages from 1941 and 1945.

German Army Enigma procedures were assumed to be better than those of the Air Force, however the procedures we find in the 1941 messages are no better than the situation described by Welchman for the Air Force Enigma procedures [17]. GC & CS only broke three Army keys before 1942 [8, p. 69], one being Vulture from the Russian Front; perhaps this marked a turning point in the bad habits of Enigma operators on units at the front. However, the difficulty of reading good intercepts from the Eastern front was significant. We note a considerable difference in the quality of the messages on the forms. Incoming messages often have serious garbles, even though they are within the working distance of the radio networks. Outgoing messages have fewer errors only attributed to operator ciphering or transcription errors. By 1945 the Enigma procedures used in the message forms had improved considerably, Cillies had vanished. However, the increased security measures of intra-day wheel rotations and the CY procedure offered little increase in security and few problems for Bletchley Park [10, p. 109]. In our case the loss of wheel crash was only a minor problem and CY did not seriously divide the messages. The average number of message parts (*Teile*) per day was higher in the 1945 messages and this favoured our statistical attack. However, longer runs were sometimes required since we had no knowledge of the wheel-orders.

[12] July, Batch B has message numbers that differ from Batch A and it is possible they are on a different key. The messages have not yet been transcribed and hence no break has so far been attempted.

[13] As the messages in both Batch A and B are on same key they have been combined.

[14] Batch C contains messages, both Enigma and hand cipher, from a different radio network than the other 1941 messages. All our attempts to break these Enigma messages have failed. We therefore suspect the use of an Enigma machine with differently wired wheels.

## APPENDIX E: THE MESSAGE FORMS

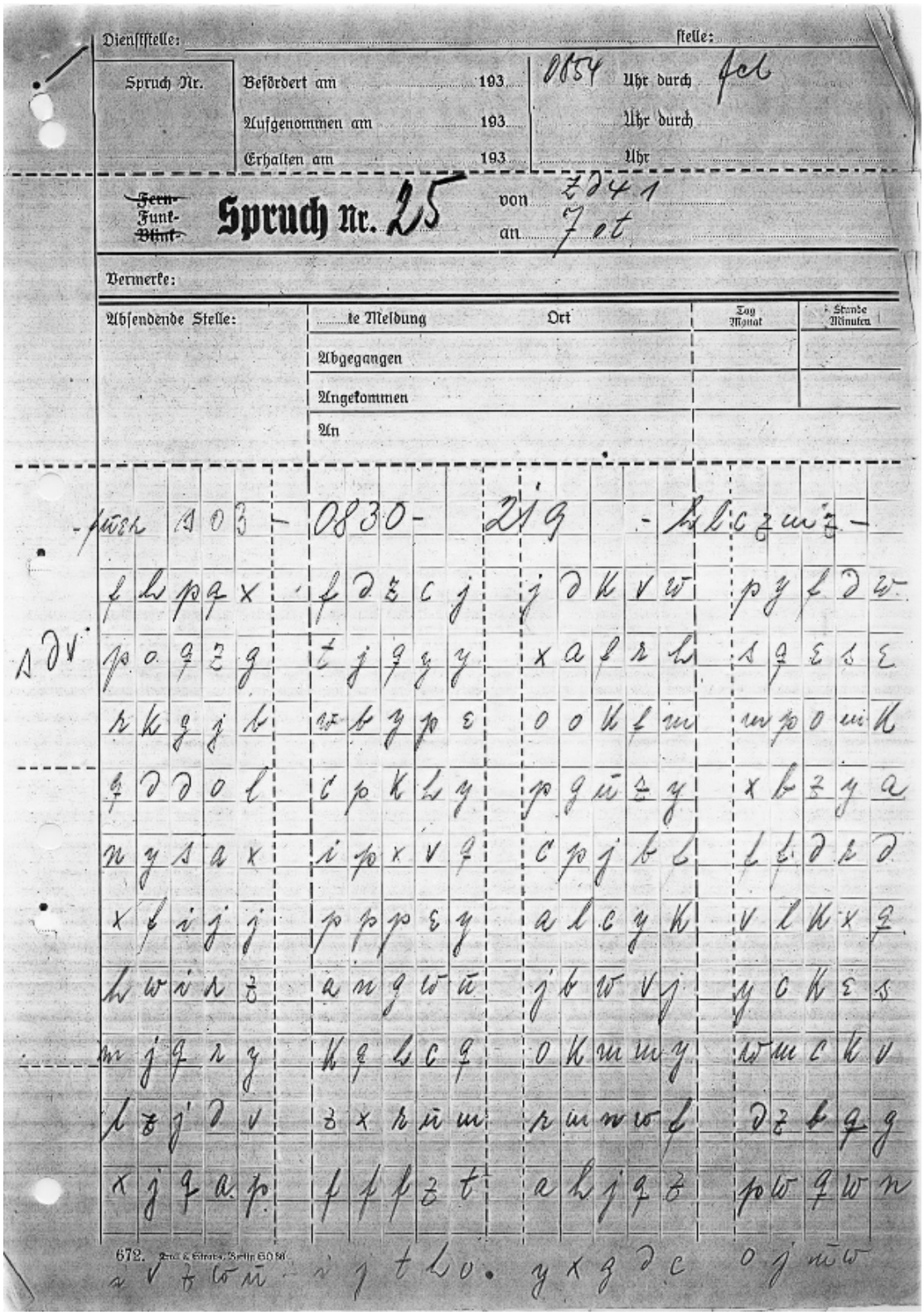


Figure 20. *Funkspruch* form for message number 25, from 13 July 1941. A few message forms, like this example, have the message key written in the margin – SDV. At most this would imply a fast ring setting but was of little use for our analysis.

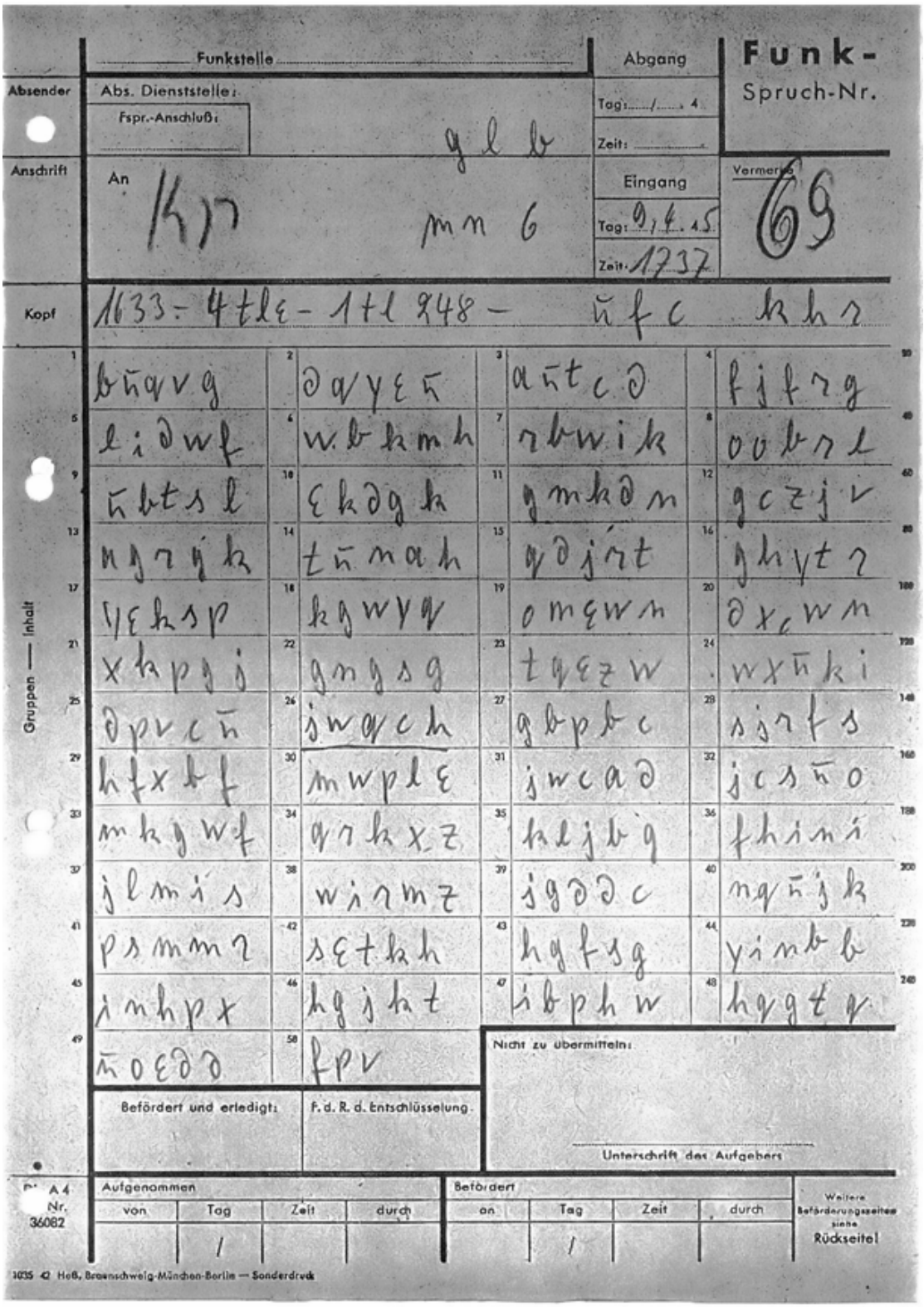


Figure 21. *Funkspruch* form for message number 69, from 9 April 1945. Part one of a four-part message sent by *SS-Standartenführer* Walter Huppenkothen.

```
Befordert am: 13.07.1941   Uhr: 0854  Durch: fcl
Sent on     :              At :       By   :

Funkspruch Nr.: 25    Von/An : ZD41 / JOT
Message No.   :       From/To:

Remarks:

Absendende Stelle   :           An:
Transmitting Station:           To:
-----------------------------------------------------
fuer SO3    0830 - 219 - HLC ZMZ

FHPQX FDZCJ JDKVW PYFDW
POQZG TJQYY XAFRH SQESE
RKGJB WBYPE OOKFM MPOMK
QDDOL CPKHY PGUZY XBZYA
NYSAX IPXVQ CPJBF FFDRD
XFIJJ PPPEY ALCYK VLKXQ
HWIRZ ANGWU JBWVJ YCKES
MJQRY KQHCQ OKMMY WMCKV
LZJDV ZXRUM RMNWF DZBQG
XJQAP FFFZT AHJQZ PWQWN
IVZWU IJTHO YXGDC OJUW
```

Figure 22. Transcript of Message Nr. 25 of Figure 20.

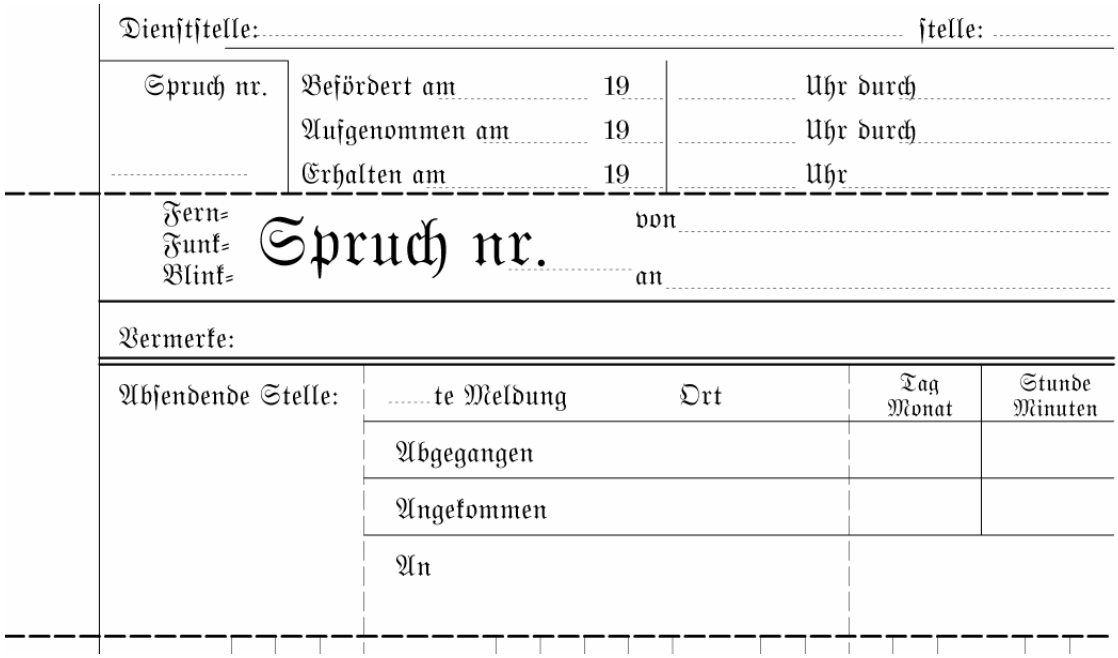


Figure 23. Reconstructed message form from 1941. Several printing works produced these forms, for example: G Braun GmbH Karlsruhe and Kroll & Straus, Berlin SD 36, (Fig. 20).

**ACKNOWLEDGEMENTS**

The authors are most grateful to Michael van der Meulen for giving us access to his collection of German Army messages. His help and co-operation continues to be a crucial and inspiring factor for the success of this codebreaking project. Without him we probably would not have embarked on such an undertaking. We are equally indebted to the former *Oberstleutnant* (Lieutenant Colonel) Waldemar Werther and his wife Hetty, now unfortunately both deceased. Waldemar Werther was instrumental in saving these messages from destruction at the end of the Second World War, and later he made sure the material would survive his death. On his death in the late 1980's, his widow Hetty followed his wishes and transferred the Army messages to Michael van der Meulen. We are most thankful to Erik Brache and John Molendijk for their continuing help in supplying us with the necessary computing power to break these messages. We thank Jim Reeds for providing a software implementation of a Welchman-Turing Bombe, which we automated further in case its use became necessary to complete the job. Ralph Erskine provided help with documents. David Hamer supplied a number of Enigma decrypts to augment our starter set of decrypts. Philip Marks provided guidance on our first break into the messages from 1945. His 2001 Cryptologia paper was also a useful reminder of the Army Enigma key procedures that we would meet. We thank David, Philip, Ralph Erskine and Wes Freeman for proofreading the manuscript and for useful discussion.

## REFERENCES


1. Bauer, F. L. 2000. *Decrypted Secrets*. Berlin: Springer-Verlag.
2. Davies, Donald W. 1999. The Bombe – A Remarkable Logic Machine. *Cryptologia.* 23(2):108-138.
3. Davies, Donald W. 1999. Effectiveness of the Diagonal Board. *Cryptologia.* 23(3):229-239.
4. Freeman, Wes, Geoff Sullivan and Frode Weierud. 2003. Purple Revealed: Simulation and Computer-Aided Cryptanalysis of Angooki Taipu B. *Cryptologia*, 27(1):1-43.
5. Gaines, H. F. 1956. *Cryptanalysis*. Dover Publications.
6. Gillogly, J.J. 1995. Ciphertext-Only Cryptanalysis of Enigma. *Cryptologia.* 19(4):321-413.
7. David H. Hamer. 1997. Enigma: Actions Involved in the “Double Stepping” of the middle Rotor. *Cryptologia*, 21(1):47-50.
8. Hinsley, F. H. with R. C. Knight, E. E. Thomas, C. F. G. Ransom. 1981. *British Intelligence in the Second World War, Volume 2.* London: HMSO.
9. Hinsley, F. H. with R. C. Knight, E. E. Thomas, C. F. G. Ransom. 1984. *British Intelligence in the Second World War, Volume 3, Part 1.* London: HMSO.
10. Marks, Philip. 2001. Umkehrwalze D: Enigma’s Rewirable Reflector – Part I. *Cryptologia.* 25(2):101–141.
11. Sebag-Montefiore, H. 2000. *Enigma: The Battle for the Codes*. London: Weidenfeld and Nicholson.
12. Siegert, Toni. 1996. *30000 Tote mahnen! Die Geschichte des Konzentrations-lagers Flossenbürg und seiner 100 Außenlager von 1938 bis 1945* [30000 Dead Urge Us to Remember! The History of the Concentration Camp Flossenbürg and Its 100 Sub-Camps from 1938 to 1945]. Weiden: Verlag der Taubald’schen Buchhandlund GmbH.
13. Sinkov, A. 1966. *Elementary Cryptanalysis.* Washington DC: The Mathematical Association of America.
14. Sullivan, Geoff. 2002. Cryptanalysis of Hagelin Machine Pins Wheels. *Cryptologia*, 26(4):257-273.
15. Tuchel, Johannes. 1994. *Die Inspektion der Konzentrationslager 1938 – 1945. Das System des Terror* [The Inspectorate of the Concentration Camps 1938 – 1945. The System of Terror]. Berlin: Edition Hentrich.
16. 1997. *Five Centuries of German Fraktur*. Winchester MA: Walden Font. (http://www.waldenfont.com/downloads/gbpmanual.pdf)
17. Welchman, Gordon. 1997. *The Hut Six Story*. Kidderminster UK: M & M Baldwin.

## BIOGRAPHICAL NOTES

Geoff Sullivan is a computer programmer and electronics engineer working on the design of scientific instruments. His main interest in cryptography is the computer simulation and computer cryptanalysis of historic cipher machines.

Frode Weierud is employed by the European Organization for Particle Physics (CERN) in Geneva. He works as a programmer in one of the equipment groups. Cryptography has been his main interest for more than 35 years. His cryptological research is focused on cipher machines and cryptanalytical techniques.