BREAKING GERMAN ARMY CIPHERS

Geoff Sullivan[1] and Frode Weierud[2]

ADDRESS: (1) 64 Tennyson Road, Headless Cross, Redditch, Worcs., B97 5BJ, UNITED KINGDOM. geoff@blueangel.demon.co.uk, http://www.hut-six.co.uk/ and (2) Le Pre Vert, 1041 Rte de Mategnin, F-01280 Prevessin-Moens, FRANCE. Frode.Weierud@cern.ch, 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. The messages are being catalogued and transcribed, while the original message forms are being scanned for electronic archiving. Good progress is being made in breaking the Enigma keys and

[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.

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 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. The provenance of the messages is not entirely clear. They were initially believed to be German Army messages but the decoding shows that they are all of SS or *Waffen-SS* origin. We received them from our good friend and fellow researcher, Michael van der Meulen. He obtained the messages and some other documents from *Oberstleutnant* (Lieutenant Colonel) Waldemar Werther's estate on the latter's death in the late 1980's. How Waldemar Werther came in possession of the messages is not known.

During the Second World War Lt. Colonel Werther was a signal intelligence (Sigint) officer in the German Air Force (*Luftwaffe*). His main responsibility was deciphering of Russian signals. Immediately after the war he had several civilian jobs until he in 1953 started to work for the French intelligence service, SDECE.[2] He seems to have been attached to their Sigint organization, GCR,[3] working on Soviet and East German problems. He stayed with the French for about four years until he joined the newly created German Air Force Sigint organization in 1957 [16].

As the messages have their origin with SS units it is inconceivable that Lt. Colonel Werther received them through normal, official *Luftwaffe* channels. The most likely scenario is that he obtained the messages after the war, probably during his post-war signal intelligence service or though friends he had made during the war.

The message forms seem to be made from some type of coloured, perhaps recycled, paper and the photocopies are sometimes very dark and the contrast is

[2] SDECE = *Service de Documentation Extérieure et de Contre-espionnage* – External Documentation and Counterespionage Service; the French foreign intelligence service at the time.

[3] GCR = *Groupement des Contrôles Radioélectrique* – Radioelectronic Communications Group.

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 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 through 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[4] 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[5] and *Amtsgruppe D*[6] of the *SS-Wirtschafts- und Verwaltungshauptamt* (WVHA)[7] situated in Oranienburg near Berlin [15]. Some messages are addressed to other

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

[5] 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.

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

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

concentration camps e.g. Buchenwald, Gross Rosen, and Flossenbürg's *Außenlager*.[8]

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* [9] while on a few occasions we have identified an additional key that presumably is the key referred to as the *SS-Querverkehr-Maschinenschlüssel* 13A.[10] 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.*

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.[11] 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*[12] Dr. Karl Sack, *Hauptmann*[13] Ludwig Gehre and pastor Dietrich Bonhoeffer were

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

[9] *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].

[10] *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].

[11] *SS-Standartenführer* Walter Huppenkothen was chief of the *Gruppe E – Spionageabwehr* (Group E – counter-espionage) in the RSHA department IV, Gestapo.

[12] *Heereschefrichter* = Chief Army Judge.

[13] *Hauptmann* = Captain.

hanged in the prison courtyard at KL Flossenbürg.

Other messages of historical interest are the message reporting to *SS-Gruppenführer* Müller on the execution of General Friedrich von Rabenau and the order to execute Simone Michel-Lévy, a female French resistance fighter who received posthumously the distinction Chevalier de la Légion d'Honneur, together with two other female prisoners. Until now the fate of General von Rabenau was largely unknown. It was suspected he was executed at Flossenbürg, but the message from *SS-Sturmbannführer* Kurt Stawizki is the first firm evidence that he was murdered at Flossenbürg on 15 April 1945. The order to execute the three French female prisoners, Simone Michel-Lévy, Hélène Lignier and Noémie Suchet was sent to Flossenbürg on 5 April 1945. However the executions appear to have taken place on 15 April, two days later than the day officially recorded as the date of execution. These messages, together with some supplementary information, are now being published in full on our Web pages.

The 1941 messages are not as exciting historically as the Flossenbürg messages. They deal mainly with the logistics of the units under the command of Army Group North and their real historical value is difficult to asses. Military historians, who would like to get a detailed view of the logistical operations and associated problems in this part of the campaign against Russia, might find these messages of great interest.

For the historians of cryptology the situation is clear: 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 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.

FINDING THE KEYS

In his article, "Ciphertext-Only Cryptanalysis of Enigma", James Gillogly presents an ingenious method for breaking messages enciphered on the *Wehrmacht* Enigma [6]. This is based on identifying the correct wiring positions by looking through the self-steckered letters of the plugboard; the Index of Coincidence was used to detect the correct wheel positions. However, the method is rarely successful for short messages. With an empty plugboard, on average, only one in twenty letters will pass through the machine correctly. We set out to devise a method that would succeed with the authorised message limit of 250 letters.

Initial trials were carried out on a small set of *Luftwaffe* messages; these were the only genuine messages available at this time. A hill climbing[14] technique was used to search for the correct *Stecker* arrangement; this process is repeated for each possible message setting (i.e. set of wheel starting positions) and each fast wheel ring setting. Furthermore the process needs to be applied to each wheel-order. We chose not to attempt to handle a slow wheel movement due to the middle wheel ring setting. The chance of this occurring is only about one in three for the maximum allowable message length and would probably cause our method to fail. The hill climb consists of systematically selecting pairs of letters, which are then plugged together. A trial decrypt is carried out and tests applied to determine if the connection is good; if there is an increase in plaintext output the connection is retained, otherwise the original arrangement is restored. We need to consider the chosen pair of letters and also other letters that may already be connected to them. For example, if we have *Stecker* connections B/W, E/J and M/S already made, this can be represented by the letter arrangement:

```
AWCDJFGHIEKLSNOPQRMTUVBXYZ
```

If we are at the point where the 2nd and 16th are the two selected letters, we need to test two additional possible *Stecker* arrangements:

```
ABCDJFGHIEKLSNOWQRMTUVPXYZ
APCDJFGHIEKLSNOBQRMTUVWXYZ
```

The arrangement from this set of three giving the best plaintext output is retained. Pairs of letters are selected by their position in the sequence, which gives 325 possible pairs, however over 600 trial decrypts are required at each machine setting since on average there are about two *Stecker* arrangements to test for each selected pair.

PLAINTEXT DETECTION

The first trials used the Index of Coincidence to detect improved plaintext fragments in the trial decrypt. It was found that this was most efficient in finding the first four *Stecker* connections. *Stecker* connections five to ten were found more easily by using a count of log-trigrams in the decrypt.[15] Initially a database of

[14] The Stochastic Hill Climbing technique used here has been described in Gillogly, Jim. 1995. Shotgun Hill-Climbing. *The Cryptogram*. LXI(6): 12-13. Further use of this technique to attack other machine ciphers is decribed in [4, 14].

[15] The product of the characteristic frequencies of trigrams appearing in the decrypt is an estimate of the plain text content [13, p. 77]. It is more convenient to construct a frequency table with log frequencies and to sum these to derive a score for the decrypt.

plain German text was used to generate a trigram frequency table. A significant improvement in success was achieved by assembling a database from raw Enigma decrypts. Around 40 decrypts obtained from various sources were available and these were supplemented with fresh decrypts as they became available. A typical letter frequency order for raw Enigma plaintext compared with standard German is:

Enigma: `ENXRSIATUOLFDGMBZQKHWPVYCJ` (100 Enigma decrypts)

German: `ENIRSADTUGHOLBMCFWZKVPJYQX` (H. F. Gaines, 1939 [5])

Note the promotion of X in particular which is used as a full stop, abbreviation point and other punctuation; also Q that is frequently used in place of the ligature CH. This also contributes to a reduction in the frequency of C and H. N-gram frequencies also differed from standard German. For example the trigrams AQT (*acht*) and NAQ (*nach*) are both common in Enigma decrypts and normally absent in German. Figure 1 shows the ten most frequent Enigma trigrams and the ten most common in two samples of German.

	1	2	3	4	5	6	7	8	9	10
Enigma	EIN	INS	FUE	ZWO	ULL	IER	NUL	UNG	ENF	VIE
German 1	SCH	DIE	NDE	CHE	UND	ICH	TEN	DEN	EIN	END
German 2	EIN	ICH	NDE	DIE	UND	DER	CHE	END	GEN	SCH

Figure 1. Comparison of the 10 most frequent Enigma and German language trigrams. German 1 is from a text sample of 80,000 characters, German 2 from F. L. Bauer [1].

The high Enigma frequencies are dominated by numbers which are frequently used in dates, times, military units and quantities, but not all Enigma messages contain numbers. The Enigma frequencies were taken without regard to word divisions, a necessary requirement for our use. More Enigma trigram frequencies are listed in Appendix C.

IMPROVEMENTS IN THE ATTACK

The first improvement to the hill climb was to introduce a second pass to the system. The first pass used the Index of Coincidence as a detector. The second pass was simply a repeat of the procedure using the final *Stecker* from the first pass as a starting point, but using log-trigram scoring for plaintext detection. The problem of when to switch between IC and log-trigram scores was eliminated with this arrangement. The run time now increased to about 1200 trial decrypts. Further improvements were added by allowing optional log-unigram

or log-bigram scores to replace the IC score for the first pass. This gave some improvement in the success rate; more success was achieved by using log-bigram scores on the first pass and log-trigram for the second.

FIRST SUCCESS

The first break we achieved into the Army Messages was the message FHPQX[16] dated 13 July 1941. This was with the two-pass hill climb. The actual plaintext we obtained:

```
YLVP RONX PANZ XGRU PPEX VIER XSIE HDDI EDSI EGFR IEDT ONIX DIVX STCN RSEI
TXEI NSZW OXSI EBEN XEIN ZBYN SNUL LNUL LXUH RMIT ANFA ENOL LAMU NTER KUNF
TSRA UMXK ANNN EFRE INFL IESZ ENXD AXDR ITTE XIYX CDIV XUND XAQT EXPA NZXD
IVXB GMNI EREN UNDR ANMB
```

This immediately revealed a lot of information about the network we are dealing with. It confirmed our suspicion that the first group is the *Kenngruppe* and not part of the message text. The *Kenngruppe* consists of three letters, in this case PQX, which are taken from a daily cipher table, arranged in random order and prefixed with two randomly chosen letters. Four groups of three letters were used for each day. This first group is sent in the clear as part of the message. Furthermore, we have confirmation that the message belongs to a unit of the German Army, this one is addressed to *Panzergruppe* 4 SS T (*Totenkopf*) Division. A possible crib for use with a Turing-Welchman Bombe can be seen in the message: SIEGFRIEDSIEGFRIEDTONIXDIVX. This was to make an appearance in several messages, although the position within the message varied. With its several repeated letters, this crib would enable a moderately strong menu to be constructed in many situations.

Removing garbles and re-formatting the plaintext we have:

```
FHPQX AN X PANZ X GRUPPE X VIER X SIEGFRIED SIEGFRIED TONI X DIV X STEHT
SEIT X EINS ZWO X SIEBEN X EINS EINS NULL NULL X UHR MIT ANFAENGEN AM
UNTERKUNFTSRAUM X KANN NIQT EINFLIESZEN X DA X DRITTE X INF X DIV X UND X
AQTE X PANZ X DIV X BLOQIEREN UND RAUM BELEGT HALTE X DIV X KDR X
```

The progress of this message break is mapped out in Figure 2, which is a diagnostic re-run of the original break, with the wheels and fast ring at the correct position. Column one is the message trial decrypt number. The score is shown in the second column. The third column of up to 26 characters is the *Stecker* pattern in reciprocal form; correct *Stecker* letters only are shown. This figure

[16] We use the first group of the message, in this case FHPQX, to identify each message. This first group is either the *Kenngruppe* or the first cipher group, depending on the prevailing procedures.

illustrates the great difficulty of finding the first few *Stecker* connections. Some of the self-steckered letters, BCFJPS are temporarily lost and correct *Stecker*-pairs are acquired very slowly. For the first pass the score system used was the Index of Coincidence, for the second pass a count of log-trigrams was used, the apparent decrease in the score at step 609 is where the score changes to log-trigrams at the start of the second pass. Finally the first few letters of the decrypt at each stage are given showing only those letters that agree with the actual plaintext. Curiously, the *Stecker* to E took some time to find.

```
1    2    3                          4
-------------------------------------------------------------------------------------------------------
0000 3812 .BC..F...J.....P..S.......-   P        P                    F  E         X           I S
0004 3992 DBCA.F...J.....P..S.......-   PA       P                    F  E      D  X           I S
0056 4019 D.CA.F...J.....P..S.......-   PA       P                    F  E      D  X             S
0060 4111 DBCA.F...J.....P..S.......-   PA       P                    F         D  X             S
0066 4124 D.CA.F...J.....P..S.......-   PA       P                    F         D  X             S
0067 4133 D.CA.F...J.....P..S.......-   PA       P                    F         D  X             S
0068 4181 DBCA.F...J.....P..S.......-   PA       P                    F         D  X             S
0072 4216 D.CA.F...J.....P..S.......-   PA       P                    F         D  X             S
0086 4229 D..A.F...J.....P..S.......-    A       P                    F         D  X
0098 4278 D.CA.F...J.....P..S.......-   PA       P                    F         D  X             S
0105 4291 D..A.F...J.....P..........-    A       P                              D  X             S
0109 4299 D.CA.F...J.....P..........-   PA       P                              D  X
0161 4365 D.CA.F...J.....P..........-   PA       P                              D
0166 4453 D.CA.F.........P..........-   P        P                        T     D  X
0219 4479 D.CA...........P..S.......-   P                                 T     D  X             S
0228 4580 D.CA.F.........P..S.W.U...-   P      U P                        F     T     D  X       S
0235 4624 D.CA.F.........P..S.W.U...-   P      U P                        F     T     D  X       S
0243 4703 D.CA.F..M...I..P..S.W.U...-   P      U P            I   I  F    T     D  X  C       S
0246 4747 D.CA.F..M...I..P..S.W.U...-   P      U P            I   I  F    T     D     C       S
0247 4765 D.CA.F..M...I.....S.W.U...-                         I   I  F    T        X  C       S
0249 4800 D.CA.F..M...I.....S.W.U...-                         I   I GF    T        X  C       S
0253 4857 D.CA.F..M...I.......W.U...-                         I            T        X  C
0254 4922 D.CA.F..M...I.......W.U...-                         I            T        X  C
0263 5023 D.CA.FY.M...I.......W.U.G.-                       D I           DT        X  C
0271 5177 D.CA.FY.M.N.IK......W.U.G.- N                     D I           DT N      X  CN   I       W
0290 5247 DBCA.FY.M.N.IK......W.U.G.- N                     D I           DT NI     X  CN   I       W
0294 5252 DBCA.FY.M.N.IK......W.U.G.- N                     D I           DT NI        CN   I       W
0295 5278 DBCA.F..M.N.IK......W.U...- N                       I            T NI        CN   I       W
0399 5546 DBCA.F..M.N.IK......W.U...- N                       I            T NI        CN   I       W
0421 5598 DBCA.F..M.N.IKZ.....W.U..O-ON    Z         I        I            TONI        CN   I   I   W
0504 6261 DBCA.F..M.N.IKZ.V...WQU..O-ON    Z         I        I            TONI   V    CN   I   I   W
0569 6520 DBCA.F..M.N.IKZPV..XWQUT.O-ONXP  ZX  U P XVI       DI             ONI D VX TCN   ITX I  ZW
0609 0216 DBCA.F..M.N.IKZPV..XWQUT.O-ONXP  ZX  U P XVI       DI             ONI D VX TCN   ITX I  ZW
0660 0258 DBCA....MJN.IKZPV..XWQUT.O- NXPANZX  U   XVI    I   DI           TONI D VX  CN   ITX I  ZW
0783 0262 DBCA.F..MJN.IKZPV..XWQUT.O-ONXPANZX  U P XVI    I   DI           TONI D VX TCN   ITX I  ZW
0785 0444 DBCAHF.EMJN.IKZPV..XWQUT.O-ONXPANZX  U PEXVIE   IE  DIE   E    E TONI DIVX TCN  EITXEI  ZWO
0867 0465 DBCAHF.EMJN.IKZPV..XWQUT.O-ONXPANZX  U PEXVIE   IE  DIE   E    E TONI DIVX TCN  EITXEI  ZWO
0878 0550 DBCAHF.EMJNRIKZPVL.XWQUT.O-ONXPANZX RU PEXVIER  IE  DIED  E  RIE TONI DIVX TCNR EITXEIN ZWO
0880 0620 DBCAHF.EMJNRIKZPVLSXWQUT.O-ONXPANZX RU PEXVIER SIE  DIEDSIE FRIE TONI DIVXSTCNRSEITXEINSZWO
0892 0782 DBCAHFYEMJNRIKZPVLSXWQUTGO-ONXPANZXGRUPPEXVIERXSIEHDDIEDSIEGFRIEDTONIXDIVXSTCNRSEITXEINSZWO
```

Figure 2. Hill climb on the message FHPQX from 13 July 1941.

PROCESSING MESSAGE BREAKS

The information we get from a successful hill climb is a set of *Stecker* connections, the wheels' core wiring position and a turn-over point for the middle wheel.

A successful hill climb usually gives all ten plugboard connections. On a few occasions one connection has been found to be incorrect. A few breaks have been what we call partial breaks, with some errors in the decrypt, but usually it is an all or nothing situation. To get the daily machine settings we need first to check that all the *Stecker*-pairs are correct and then to find the ring positions. Missing or incorrect *Stecker* connections are found using a graphical Enigma simulator. The fast wheel ring is sometimes not quite correct, as we will explain later. It can be verified by setting up a graphical Enigma simulator with the wheel-order (*Walzenlage*), *Stecker* and the wheels at the correct core wiring position, with the letter rings on all wheels set to the neutral position – A. The fast ring setting is then verified by trial and error, observing the plaintext output. This is sometimes easy but depends on identifying the correct turn-over from the output text. All three ring positions can be found using the indicator information in the message preamble.

As an example we will use the second break we obtained for 17 August 1941:[17]

Wheel-order	Wire	Turn-over	Stecker
524	YVF	**P [18]	EBFDACLIHJPGSRUKYNMWOVTXQZ

The message header is:

1130 -- 2tle - 1tl.[19] 146 - BIU AVL --

This is the first part (1tl.) of a two part (2tle.) message timed at 11:30.

BIU is the *Grundstellung* of the machine and AVL is the enciphered message key. The operator has set his wheels to BIU and enciphered the message start setting. This gave the letters AVL entered as the second trigram of the indicator. We need to find which ring positions give the core wiring position YVF when AVL is enciphered with the window set to BIU. This is simply a question of trying all possible settings using a computer program.

For this example we have three results, only one of which can be correct:

Possible solutions	1	2	3
Ring positions	FNZ	LOF	OZE
Start positions	DIE	JJK	MUJ

[17] The first message break, from 13 July 1941, started from the first cipher group, the *Kenngruppe* and since there was also a wheel turn-over near this point, we selected the second message break for this example.

[18] The turn-over occurs when the core wiring position, starting from F, reaches P; the other two wheels are irrelevant except in dud-busting mode.

[19] 2tle – 1tl. Stands for "Zwei Teile – Teil Eins" = Two parts – Part one.

The correct solution can easily be found by trial decrypt of the message, but in this case we have an example of a type of Cilli – DIE for the first result, which gives a clue that this may be the correct solution. We will say more about Cillies later. Having found the ring positions, it should now be possible to decrypt all messages for the day that are on the same key. Frequently we found duds: messages that do not decode because there is an error in the indicator. This may be due to an operator's ciphering or transcription error, a Morse reception error, or our transcription error due to the message forms being difficult to read. In cases where the message indicator does not decrypt to give the correct start position, a dud-buster can be applied. This is a simple software routine to test all 17576 wheel positions for the message in question. Decrypting all the messages from a day can be quite straightforward, however some formidable problems have been found. A few messages have letters missing with one or more characters lost on reception. In difficult cases this has occured at several places within a message. The decrypt immediately becomes garbled at this point. Knowledge of German and Morse is helpful to sort out these situations. Other, simpler, problems sometimes appear: for example a *Stecker* cable plugged into an incorrect socket. We have also seen evidence of machine faults, probably caused by a partially open circuit *Stecker* cable or contact. Fortunately these problems have been overcome and it has been possible to decrypt almost all messages when a daily key is broken. Messages have also been noted using a previous day's key; sometimes these are easy to spot from the time or indicator. A dud-busting run can often resolve these problems. On a few occasions a message that fails dud-busting and is believed to be on a different key has required a fresh attack.

MORE IMPROVEMENTS IN THE ATTACK

The two-pass procedure was producing a steady stream of breaks into the 1941 messages, but not all messages could be broken. The success rate, for suitable length messages, was between 20 and 50%; some groups of days were more difficult than others. We had a preference for messages with around 180 letters, they were long enough to succeed and not so long as to give extended run times or encounter problems with a slow wheel turn-over. It was noted that many breaks occurred with a fast wheel ring setting that was incorrect, but only slightly so. This observation led us to believe that the hill climbs were starting due to a chance arrangement of decrypt characters in the early stages. It appeared that the 26 fast ring positions that we examine gave a stochastic kick to the hill climbs. It was decided to re-run some of the failed messages starting at the second cipher letter rather than the first. If this failed, the third letter would be used as the start point and so on. This, we hoped, would kick the hill climb back into

synchronization. This did the trick and opened up previously difficult, unbroken messages. An offset of up to 25 could be specified for the attack. Further examination of this technique showed that for the 25 offsets, breaks could frequently be obtained for between three and ten different offset settings. However, there was no way to pre-determine which offsets would succeed. Nevertheless the technique was invaluable in increasing our output.

WHEEL-ORDERS

Only a few messages are available for June and July 1941, but almost two week's traffic is available for August. After breaking several days in this month, the wheel-orders listed in Figure 3 were noted.

20.08.1941	—	24.08.1941	—	28.08.1941	—
21.08.1941	341	25.08.1941	415	29.08.1941	134
22.08.1941	423	26.08.1941	321	30.08.1941	421
23.08.1941	251	27.08.1941	132	31.08.1941	243

Figure 3. Wheel-orders used for August 1941.

Here we see evidence that the 'non-crashing' rule under which wheels were never used in the same position on adjacent days. This immediately reduces the workload from 60 to 32 wheel-orders when searching for the key of an adjacent day. If both adjacent days are known, the number of possible wheel-orders can be as low as 13. There is also a possibility that a wheel-order is never repeated within a month, but the sample was too small at this time to be sure. However, a few repeated wheel-orders were later found, one of these being for 24 August 1941, which caused some delay in breaking that day.

FURTHER IMPROVEMENTS IN THE ATTACK

Messages for September 1941 were available for most days. Breaking into this month and then using non-crashing wheel-orders to reduce the workload was possible for the first time. It was decided to use an extended three-pass hill climb; although this suffered from an extended running time, it was bearable due to the reduced number of wheel-orders left to be processed after the initial break. The three passes used the Index of Coincidence, bigram and trigram scoring, in that order, which increased the success rate to around 75% for a single message. This gave a success rate for each day of nearly 100% provided

three or more messages were available for the day. In a few cases it was necessary to use the offset procedure described previously; nevertheless, almost the entire month was broken within a few weeks.

A few other ideas were tried to improve the attack, one of these being Yoxallismus, which is described in Appendix A. Other ideas involved preferential attacks on the *Stecker* in frequency order ENXR, but this gave no increase in the success rate. Figure 2 illustrates the difficulty of correctly detecting the first few *Stecker* connections.

STECKER

With messages available for most days in September 1941, we were able to break most of this month and recover almost the entire key sheet for the month. This key sheet is reproduced in Appendix D.

It may be expected that the most convenient way to select the *Stecker*-pairs for a calendar month would be to draw these randomly from a set of 325 bigrams, or a set of 300 if consecutive *Stecker* are to be avoided. However, the distribution of *Stecker* connections shows that there is a preference for certain pairs. In the set of 250 *Stecker*-pairs for the 25 days broken at the time of the examination, only 160 different connections have been selected. For a random selection we would expect to have around 200 different pairs over 25 days, if drawn from a set of 325. On average, around 35 bigrams would need to be drawn to obtain ten with unique letters, perhaps this was too tedious to consider.

Figure 4 shows the *Stecker* connections in graphical form for six days in September. The missing days between 8 and 17 September either have no message available or were unbroken. The *Stecker* for 10 September 1941 is particularly striking. The messages for 16 September 1941 remain unbroken at the time of writing and it may be possible that some of the *Stecker* for this day can be guessed. This day has only two messages of lengths 67 and 101; the latter is within reach of our method and we have otherwise never been defeated on a day with at least three messages available, and only very rarely on days with just one or two available.

We found a few instances of consecutive *Stecker* in the 1941 and 1945 messages. Evidently there was no particular rule to avoid them on these networks. The CSKO[20] circuitry added to Bletchley Park's Bombes to eliminate solutions containing consecutive *Stecker* is presumed to apply only to certain *Luftwaffe* networks.

[20] CSKO = Consecutive Stecker Knock-Out.

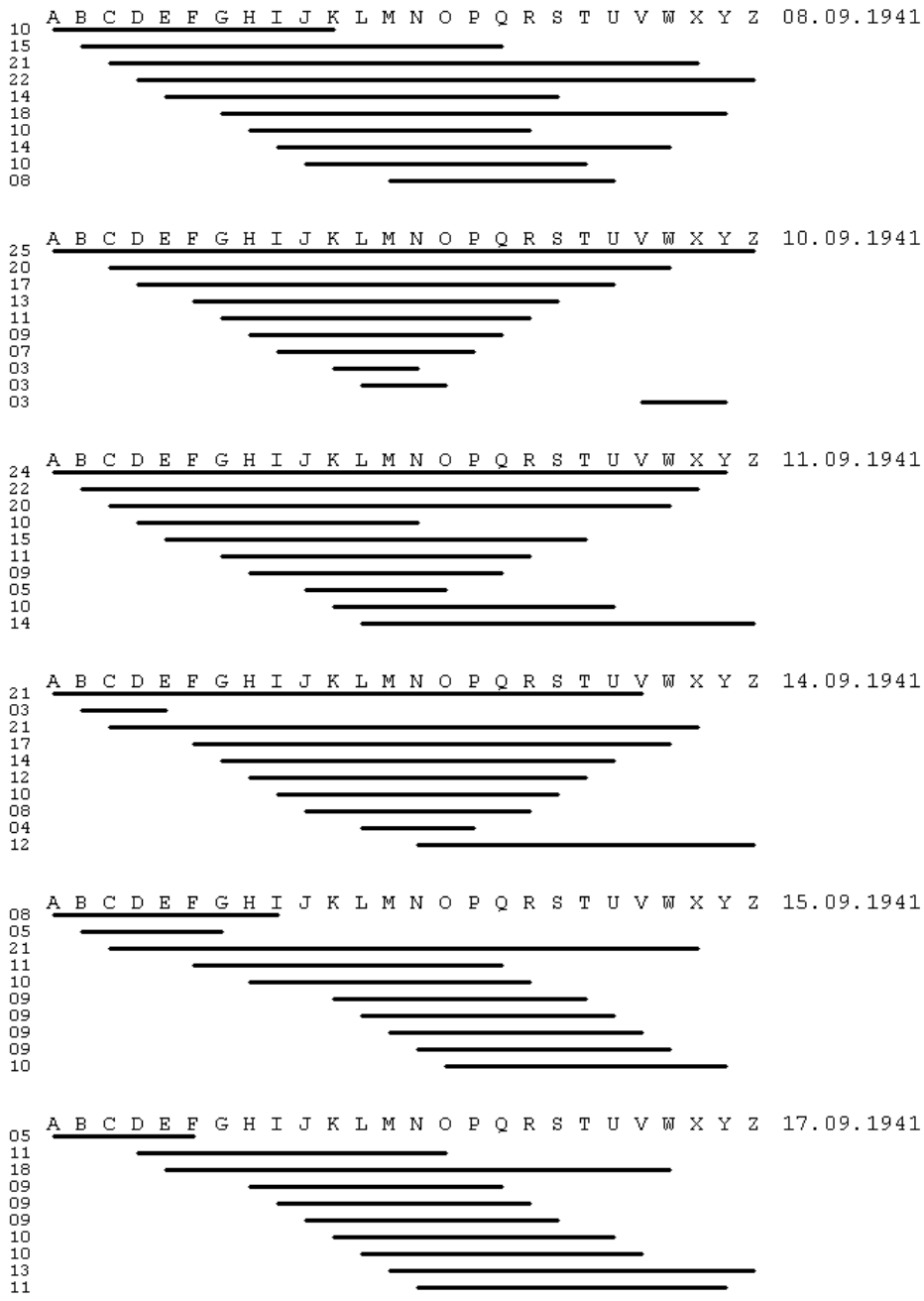

Figure 4. *Stecker* connections for six days in September 1941.[21]

[21] A horizontal line, e.g. the first line in the top graph illustrates the *Stecker* connection A linked to K. The number in the lefthand column gives the distance between the connected letters.

CRIBS

After most of the messages of August 1941 were broken, the few remaining messages proved difficult. The offset procedure gave solutions to some difficult messages, but a few days remained unbroken. Surely we have enough material for a crib for a Turing-Welchman Bombe?[22] An examination of the broken messages from August 1941 showed one often recurring text. Messages were frequently signed XROEMEINSBERTA which had already made an appearance 11 times in the month, in messages sent by Ib to N.F.[23]

The messages for 25 August 1941 were unbroken. The result of an examination of the headers of these messages is shown in Figure 5.

Indicator	From	To	Length	Remarks
ONRWP	N.F.	Ib	73	
FMITY	N.F.	Ib	57	
MUITY	N.F.	Ib	93	
ATBWC	Ib	N.F.	145	1tl.
SPTYI	Ib	N.F.	138	2tl.
BEGPU	I	N.F.	47	

Figure 5. Message headers from 25 August 1941.

ATBWC and SPTYI is a two-part message; it is possible that the second part, SPTYI, ends with our crib.

BEGPU is also possibly a message from Ib; the hand written information on some message forms sometimes lack in detail or has errors.

Fitting the crib to these two ciphertexts:

```
SPTYI     VAWZJDYJXDAUYR
Crib      XROEMEINSBERTA
BEGPU     VFDLLJBPRYASSN
```

There are no letter crashes in either message. The longest possible menu for the two messages is for the message SPTYI shown in Figure 6.

BEGPU only gives a menu with a maximum of five letters. However, the menu from SPTYI is rather short with no closed loops and is expected to give

[22] For an introduction to Bombes and the construction of menus, see [2,3, and 18].

[23] Ib = Ib *Armeekommando*. N.F. = *Nachrichtenführer*. On the *Funkspruch* forms which contain original hand written messages, the message serial numbers from Ib were written in blue pencil, while those numbered from N.F. were written in red pencil. Clearly it was not only Gordon Welchman who required a supply of coloured pencils [18, p. 87].

many Bombe stops per wheel-order. Running this on a Letchworth Bombe would not have been practicable in 1941, however it is all that we have to work with. The solution we used was to modify a software Bombe[24] to automatically feed the stops to a short hill climb process, since Bombe stops would only give seven *Stecker*-pairs for this menu. This program was successful in finding the key; a total of 3600 outputs from the Bombe's "machine gun"[25] stage were processed by the hill climb. Finding good cribs is a difficult process; looking at the messages that we had broken it is clear that there are cribs in some messages and information about the network is valuable in selecting cribs. However, they can change even over a period of a few days. Some cribs may have a short lifetime and re-appear days later. Further they can be corrupted by garbles due to operator error or bad reception. There is a further complication in that the message text style can vary.

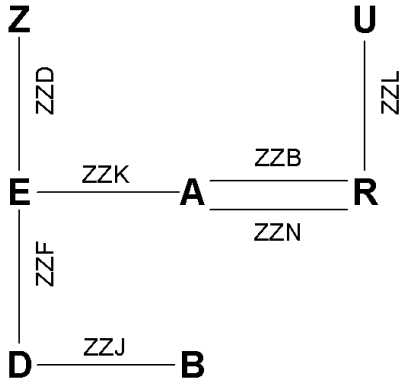

Figure 6. Menu for SPTYI. Bletchley used wheel positions ZZZ as the zero reference point, hence the first constatation A/R is at the second wheel position ZZB.

For example, the following variations were noted as the ending text of messages signed by Friedrich Hartjenstein[26]:

[24] The modified Bombe dragged a crib through a specified part of the message. At all non-crashing positions, the longest possible menu was run according to the Turing-Welchman process. The run was repeated for all relevant middle wheel turn-overs at each crib position. Data from the stops was processed by a simplified hill climb (the menu was expected to be weak). We called this modified program Wren, after the W.R.N.S. (Women's Royal Navy Service – 'Wrens') who tended and fed the Bombes.

[25] For information about the Bombe and the "machine gun", see [3, p. 237].

[26] *SS-Obersturmbannführer* Friedrich Hartjenstein was commander of *SS Totenkopf Nachschubdienste* (supply service – logistics) in 1941, one of several infamous personalities that appear in the messages. In 1943, he became *Lagerkommandant* (Camp Commander) of KL Auschwitz II Birkenau and then *Lagerkommandant* of KL Natzweiler. After the war he was sentenced to death by the French, a sentence which was later commuted to life imprisonment. He finally died of a heart attack in a French prison.

```
XNDXNDXHARTJENSTEINX
XGEZXHARTJENSTEINX
XHARTJENSTEINX
XHARTJENSTEIN
XHARTJENSTEINXHARTJENSTEIN
XGEZXHARTJENSTEINXHAUPTSTUFX
```
[27]

The SS crib, mentioned previously, also had variations. This strong crib capable of viable Bombe menus has the problem of variable positions within the messages:

```
SIEGFRIEDXSIEGFRIEDTONIXDIVX
SIEGFRIEDSIEGFRIEDTONIXDIVX
SIEGFRIEDSIEGFRIEDXTONIXDIVISION
SIEGFRIEDSIEGFRIEDTONIDIVX
SIEGFRIEDSIEGFRIEDTONIDIV
```

Having now had the opportunity to examine a number of contiguous Enigma messages, it is clear that the art of cribbing was a remarkable achievement. We never attempted to break another message with a guessed crib. Fortunately our hill climb success rate increased with the September messages.

CILLIES

Having found the daily machine settings for wheel-order, *Ringstellung* and *Stecker*, it is a simple process, at least in theory, to read all messages on the same key for the day in question. We have already mentioned the sometimes considerable difficulties that occur due to duds and garbled or missing letters. However, having fully decrypted a day with several messages, we begin to see the operators' procedures and the errors that were made in using Enigma. The messages for 22 August 1941 will serve as a good example. The indicators, start and end positions, and the operator's name, where known, are shown in Figure 7.

We note that two operators, Krüger and Beyer, were each prone to use the first three letters of their name for either the indicator or the message key. Krüger was especially prone to this habit. BEN is also used twice as a message start position, probably derived from the word *sieben*, since SIE is also present. Trigrams taken

[27] The meaning of GEZ is *gezeichnet* – signed.

from common words are often encountered. For example DIE paired with EID has been noted on other days.

Msg. No.	Kenngruppe	Indicator	Start	End	In[28]	Out	Operator
31	AGGKR	XMB JXM	BEN	CHX	08:45	09:50	
32	FDHOW	FKQ CZQ	ALP	APJ	10:00	10:29	
33	KMFVY	KMP SBG	WAS	XHM	12:45	13:01	Krüger
34	FLFYV	WBH AIE	RAS	SFZ	14:55	14:00	Krüger
35	BCRKG	FUY PEX	JRP	JYZ	14:05	15:48	Krüger
36	GRBLQ	CGL ANX	WAS	XMS	15:45	16:06	Krüger
37 1tl.	FMBLQ	XMS HUT	BEN	CNH	18:30	18:53	Krüger
37 2tl.	XFLQB	CNH ESW	GRA	GUD	18:30	18:53	Krüger
38	HOBQL	GUD ALX	WER	XLY	20:20	20:36	Horn
39	SOLBQ	XLY RPR	QWE	QZN	20:40	20:55	Horn
33a[29]	RMBLQ	BMU RNH	WER	XNB	08:00	08:20	tjmk
34a	KRBLQ	WOS JTD	BEY	CHO	09:45	09:59	Beyer
35a	BEWOH	KRU MYD[30]	BEY	CGL	14:30	14:36	Krüger
36a	RXBQL	KSE MKN	SIE	SLG	18:10	18:40	Horn
37a	HOBQL	BEY EBZ	KRU	KYG	18:15	18:40	Krüger
39a	ERQZP	N.I.[31]			20:30	21:10	

Figure 7. Enigma message settings for 22 August 1941.

Here we have a startling sequence of Cillies starting with the message timed at 14:36 with the indicator KRU provided by the operator. The final wheel positions were not changed before enciphering the message key of a following message for a considerable number of messages as shown on Figure 8.

A further alarming feature of this day's messages can be seen in the first message of the day, timed at 08:20. The indicator BMU is identical to this day's *Ringstellung.* This leaves this day's key in an even more vulnerable position given knowledge of the poor procedures (see Appendix B). More examples of this particular bad habit, known as "Herivel tip", are given below. Often the indicator setting was chosen by moving one or more of the wheels by a few steps in either direction from the positions at the end of the previous message. There

[28] 'In' is the time stamp attached to the message by its originator and sent in plain as part of the message preamble. 'Out' is the time of radio transmission/reception entered on the message form.

[29] A number of messages on the same key have the same message numbers. This is probably due to two or more operators working on messages in parallel and not correlating their message numbers. To distinguish between the messages we have added the suffix 'a' to one of these sets.

[30] Message 35a has the indicator KRU UZR written on the message form. A correction has been added to change the second trigram to MYD. The operator had set the wheels to KSU in error to encipher the message key.

[31] N.I. = No Indicator. This message has no indicator, and only a 5-letter *Kenngruppe* in the message preamble rather than in the cipher groups, indicating that this is a hand cipher, probably *Doppelkastenschlüssel* – Double Playfair which was in use at this time. A variation of this procedure was to include the *Kenngruppe* as the first group of the message text.

is one probable example here where the first message timed at 08:20 ends at position XNB. The indicator for the second message at 09:50 is XMB JXM; the middle wheel was moved back by one position to select the next *Grundstellung*. Some messages from July 1941 show this habit of minor adjustments to the wheel position more frequently, a procedure probably preferred by other operators. Krüger *et al.*, tended to leave the wheels as found. Keyboard Cillies can also be seen in the table. WAS, WER and QWE are used as the message key in several messages. Most of the messages for this day have keys formed on Cillies.

Time	Kenngruppe	Indicator	Message end	Length
14:36	BEWOH	KRU MYD	CGL	39
16:06	GRBLQ	CGL ANX	XMS	286
18:53	FMBLQ	XMS HUT	CNH	202
18:53	XFBLQ	CNH ESW	GUD	81
20:36	HOBQL	GUD ALX	XLY	168
20:55	SOBLQ	XLY RPR		87

Figure 8. Message ends for 22 August 1941.

One variation of Cilli mentioned by Gordon Welchman [18, p. 102], known as JABJAB, appears to be absent in these Army messages. This is where the indicator setting and message setting are identical, requiring only the fast wheel to be moved back three positions to encipher the message after enciphering the message key. One regulation we found to be observed was the authorised message limit of 250 letters. Only a few instances of violation of this rule were observed, one being a two-part message of lengths 322 and 280 from October 1941. Some messages, especially in 1945 had short final parts, of eleven letters in one example, to comply with the regulation.

HERIVEL TIPS

"Herivel tip" is the name given to a particular operator habit, anticipated by John Herivel while working in Hut 6 in the early (pre-Bombe) days of breaking *Luftwaffe* keys. The first message from a station on the network after a key change would frequently have an indicator which gave a *Grundstellung* near to the *Ringstellung* for the key period. Examination of a few days' messages from August 1941 shows that the Army Enigma operators also seem to be guilty of this habit, as shown in Figure 9.

For example in the message ATSMI, the wheel setting chosen to encipher the first message is SIE. The operator has assembled the wheels with the letters

TWE showing in the windows, which is close to the *Ringstellung* setting SVD. He has then enciphered the start position SIE to get TPG. The message indicator is TWE TPG. The offset column shows how far the wheel position was moved from the *Ringstellung* letter position to encipher the message key. The message key is also given; this shows a preference for particular trigrams rather than a random selection as required by the regulations.

Date	Kenngruppe	Indicator	Rings.	Start	Offset			Operator
16.08	ATSMI	TWE TPG	SVD	SIE	+1	+1	+1	mac
17.08	ANJSZ	EPC SJR	FNZ	GBT	-1	+2	-3	tjn
21.08	XHFBR	XGV IYZ	WGR	GLA	+1	0	+4	Horn
22.08	RMBLQ	BMU RNH	BMU	WER	0	0	0	tjmk
23.08	YYGPR	IQF LRH	IQF	DAN	0	0	0	sjn
24.08	FDKMV	OTA EJJ	OTA	BEN	0	0	0	Beyer
26.08	AXBSR	ABN PDH	XBM	SIL	+3	0	1	mon
28.08	SPJBV	ZYG QXQ	CWJ	ROT	-3	+2	-3	Krüger
30.08	GRXYJ	RYD ZMG	RYD	FUT	0	0	0	Horn
31.08	GEUPY	VIQ OVZ	UHP	GUT	+1	+1	+1	Beyer

Figure 9. Herivel tips for August 1941.

1945 MESSAGES

With most messages from 1941 either broken or waiting to be processed on broken daily keys, we were eager to see how the batch from 1945 would turn out. Did the procedures change, and would we still be able to use our methods and database from 1941? The first thing to note is the different message forms in use in this period (Appendix E). By now the *Fraktur* font had disappeared.[32] The forms are marked Ln., which could be an abbreviation for *Luftnachrichtendienst* or *Luftnachrichtentruppen.* This would be bad news; since 1944, messages on many *Luftwaffe* networks were enciphered with *Uhr*[33], the non-reciprocal *Stecker* attachment, and UKWD,[34] Enigma's re-wireable reflector. This situation would be difficult to deal with without very good cribs, which we did not have. However, if these were Army messages, then we might be lucky and only need to deal with the CY procedure that was introduced in September 1944; UKWD was probably only introduced on one Army network, Greenshank.[35] We will return

[32] After 1941, Hitler had declared the once glorified *Fraktur* font to be "Un-German" and ordered all printers to change to Antigua as soon as possible [17].

[33] Enigma *Uhr* is an attachment with a 40 position rotary switch. It connects to the Enigma plugboard instead of the normal *Stecker* cables and it allows the operator to select easily among 40 different *Stecker*.

[34] UKWD = *Umkehrwalze* D – reflector D.

[35] See [10, p. 107–109].

to the CY procedure later. The first hurdle was to transcribe the messages and get reasonably error-free ciphertext. The cipher operators' hand scripts were significantly different from the 1941 batches, and proved to be difficult to transcribe until a short familiarisation period improved the situation.[36] The forms were still of poor quality in places. The first day's traffic to be transcribed was from 3 April 1945 and consisted of 15 message parts, five of which were of a suitable length to attack.

It was some days before the first break appeared (our previous session, in December 2003, yielded 17 days broken from the 1941 batch in just under 3 weeks). Until the break we were very suspicious that these messages could indeed be using either *Uhr* or UKWD, but the first break confirmed we were still dealing with Army messages enciphered on the standard *Wehrmacht* machine. The first message out was the one with *Kenngruppe* PVRDP. It was apparent from this that the first group was no longer used for the *Kenngruppe* (discriminant), but was the first true cipher group. The signatory, with the rank of *Hauptmann*, indicated that the messages were probably still German Army, but unlike the 1941 messages, could not be from SS units.

A few days later we obtained a break into a second message from April 1, at 95 letters one of the shortest messages to be broken.[37] The wheel-orders for these two days are 523 and 423. Wheel-orders so similar just two days apart would probably not have been used in 1941. However, from early 1944 the basic wheel-order was cycled through its three possible rotations at predetermined times during each day. Figure 10 shows the recovered keys for 3 April 1945.

The longer messages, those that approach the maximum allowed length of 250 letters, use the CY procedure. This required the slow wheel to be moved manually at a randomly selected point in the message. On deciphering the message, the bigram CY would appear. This was followed by another bigram, the first letter of this being the new slow wheel position to be used to decrypt the remainder of the message. The second letter was the next letter in the alphabet included as a check against transmission errors, e.g. CYPQ – where P is the new slow wheel position. The CY procedure created no particular problems for Bletchley Park. We frequently found that the portions of the message text before and after the CY position were each of suitable length to attack with success. Some assistance was provided by the operator having marked the CY position on the form, however it was typically at around 150 letters and hardly likely to give us many problems. Also notable in Figure 10 is the absence of Cillies. This must

[36] A large number of the cipher and teleprinter operators in the concentration camps were young women from the SS female auxilliary unit, *SS-Helferinnen*.

[37] Our record is a message broken at 78 letters.

No.	1st Group, Length	CY position	Indicator	Start	End	CY Start	CY End
Wheel-order with rotation. *Stecker*: AN BX CU DW EV FT GK HP IQ JR							
00:00 – 11:59 Hours, Wheel-order: 423 Ringstellung LBS							
8	UKHNL 131		JXM RBY	EPE	EUU		
9	PVRDP 145		JXP FSE	DIO	DOD		
11	UZUUE 95		RBN IIX	EBP	FGG		
12:00 – 17:29 Hours, Wheel-order: 342 Ringstellung SLB							
12 1tl.	NJHCE 246	122	IUJ GTK	FRE	FWA	LWA	LBQ
12 2tl.	YFBKT 19		GRM TZD	FPV	FQO		
13 1tl.	HDCTD 239	146	BRD AVW	HOU	HUO	NUO	NXZ
13 2tl.	ZEQOT 47		DQA SUZ	HMS	HON		
14	LRCTF 248	155	YGA JRM	TXB	TDE	ZDE	ZHP
17:30 – 23:59 Hours, Wheel-order: 234 Ringstellung BSL							
15	LRUFY 62		DQF VZJ	BIN	CLX		
16 1tl.	HKAKW 243	166	UYB YMX	XCP	XID	DID	DLY
16 2tl.	UPVBC 117		ZCI OCX	YDM	YHZ		
17 1tl.	MEMAD 247	156	XLM WXW	YPN	ZWR	HWR	HZA
17 2tl.	XQJHR 239	145	BGT FCB	YHD	YNW	FNW	FQI
18	QJJNH 176	124	EHP OZJ	SBN	SGL	WGL	WHH

Figure 10. Message keys for 3 April 1945 showing the wheel-order rotation and CY settings.

be due to the directive, given in September 1944, to use the Enigma machine itself to encipher text to generate random indicator settings.[38] The dropping of the *Kenngruppe* was another security feature introduced in 1943[39] and, along with the CY and wheel rotation, we see real examples in the 1945 messages. We also noted that cribs for these particular messages would probably be more difficult. The occurrences of military units and place names, which must be a good source of cribs, were reduced.

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

[38] See [10, p. 109].

[39] See [10, p. 106].

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[40]	50	4755	—
August 1941	114	12337	3
Sep. 1941, Batch A/B[41]	220	24970	1
Sep. 1941, Batch C[42]	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 [18]. 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.

[40] 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.

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

[42] 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.

SOFTWARE

We used the C programming language to produce all the software for this project. Microsoft Visual Studio 6.0 was used to compile the programs. Of several compilers available to the authors this produced the fastest running code and a useful number of Intel machines were available. Compilers with more advanced optimizing features were also considered. Intel's C++ 7.0 compiler and the Interactive Optimizer (CodePlay Technology, intended for computer game applications) were tried with little benefit.

-i *file*	Input cipher filename.
-o *file*	Optional output filename.
-k	Use Sinkov unigram statistics on first pass (default use I.C.).
-kb	Use Sinkov bigram statistics on first pass (default use I.C.).
-l n	Read at most n letters from the ciphertext file (default read all)
-y	Use Yoxallismus on first pass.
-w 123	Use wheel-order 123 only (default use all 60 wheel-orders).
-u *file*	Dud-bust mode. File contains a fixed *Stecker*.
-u2 *file*	Dud-bust mode. File contains a starter set of *Stecker*.
-n *file*	File contains list of wheel-orders to exclude.
-nw *file*	File contains list of wheels to exclude in each position.
-d *file*	File contains raw decrypts for frequency table generation.
-r	Restart job at last uncompleted wheel-order.
-t a; -t ab	Test mode. Fix slow/slow-medium wheels at A/AB.
-z n	Offset run, start at nth cipher-text letter (if $n < 0$, message is padded).
-zs n	Offset run, start at nth *Stecker* position.
-mail *file*	Report results by email. File contains email script details.

Command line options in the program Ebreaker.

It was found that only badly written code was improved. About 90% of the processing time involved just a few lines of code, which was hard to optimize further. Assembler was tried but a small gain on AMD processors was lost on Intel processors, where the compiler performed better. There is always a greater gain by paying attention to the algorithm. The initial two-pass program run time was around 10-15 minutes per wheel-order on Pentium P4 machines. This increased to up to 70 minutes for the later program; the run time depends on the processor speed and the message length.[43] During this project, development

[43] An analysis of one machine output (Intel P4 1.8GHz) which operated from 14 March 2004 to 25 April

of improved techniques was continuous. A set of 40 test messages was used to check any amended software before it was run on any unbroken message. It was known that at least 80% of the test messages should break. Further utilities were developed to produce Figures 2 and 12, which assisted our development work. While we are not intending to release any software developed in this project – we would prefer that others try their own development, (using the previously unpublished messages in Appendix F) – we will describe the command line to illustrate the features that we used.

The program, which we call Ebreaker, has a number of command line options, which may be freely mixed as appropriate. See above.

A number of tools were added to our M4 graphical Enigma simulator, which we hope to release this year. Tools for ring finding, dud-busting, CY decoding, wheel-order rotation and dealing with synchronization problems were added.

APPENDIX A: YOXALLISMUS

Yoxallismus is the name given to the procedure invented by Leslie Yoxall, a Bletchley Park cryptanalyst. It was used to recover *Stecker* connections for the *Offizier* keys. These were Naval messages, intended to be read by an officer only and were doubly encrypted. It is said that Leslie Yoxall's original break was with an *Offizier* message of just 80 letters. The inner encryption of *Offizier* differs from the daily outer key in the *Stecker* and in that it uses just 26 different, predefined wheel settings. The process is therefore similar to what we require in recovering *Stecker* at a particular wheel setting. Yoxallismus was examined as a possible method of assisting the early stages of the hill climb. The procedure requires that the *Stecker* to E be identified first. A process known as Dottery[44] can achieve this, but with a computerized system it is easy to apply every possible *Stecker* to E in turn and select the best scoring result. In the following example for message SOEFI from 27 August 1941, the *Stecker* of E is assumed to be H. The letter H is encrypted at the message start position for the entire length of the message with the plug board empty. The output text is recorded. This is aligned under the original cipher message and a count of vertical bigrams recorded at each position in the message. The results for the example message are shown in Figure 12.

2004: a total of ten breaks were achieved. The message length range was 90–180 letters (average 137) and the run time ranged between 24–55 minutes (average 39) per wheel order. There being no mechanism for detecting a break, each run was for the full course of specified wheel orders. In a few cases , where a break failed, an offset run was required. In a few exceptional cases this required many re-runs at different offsets.

[44] Dottery and Yoxallismus, methods for recovering *Stecker*, require the wheel-order, wheel positions and *Ringstellung* to be known. An explanation of these procedures can be found in [11, Appendix 1].

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A		01			01				01	02			02	01								01	02		04	
B											02		01	01		01		01		01	01		01		01	
C							01			02		01		01	01		01	01	01			02		01		
D							01				01			01	01		01	03	01	01				01		
E										01	01		01						02				01	01	01	01
F						01	02									01	01	01						01		01
G								01		01	01	01	01					01	01				02			
H										01	02												01			
I												02	02		01						01	01	01	01	01	
J										01		01	01			02				02			01		02	01
K												02		02	03				01					01		01
L													01	01		02		02	01	01				01		
M															01							01				
N																03						01	04	01		01
O																					01	01		01	01	
P																	01			02	01	02	01			01
Q																		01			03	02	01		01	01
R																			01	04	01	01			01	01
S																			01		01					
T																					02		01	01	01	
U																					03	01			02	
V																						01	01	01	02	
W																								01		01
X																										
Y																										01
Z																										

Figure 12. Bigram count for message SOEFI with *Stecker* E/H. This process would be repeated for each *Stecker* to E.

In addition to the assumed *Stecker* to E, we have identified three other probable connections but they are not necessarily correct. Experience has shown that a message length of around 150-200 letters may have a bigram count of four or more indicating a probable *Stecker*. In this case we correctly assume the *Stecker*-pairs E/H, A/Y, N/W and R/T. Twelve of the encryptions of E have come out on just three ETW[45] positions. This example is better than average, often only one or two *Stecker*-pairs are implied in messages of this length; however, bigram scores have been noted up to seven in some messages. The reason we get high counts in some of the cells is due to the high frequency of E, which occurs 26 times in the plaintext of this message of length 180, or about 14%. If the *Stecker* to E is enciphered at every position, some of these will coincide with positions where the plaintext is E. In this case the vertical bigram gives the *Stecker* required to obtain the correct encryption of E. Since E is frequent, there is a likelihood of high counts emerging at correct *Stecker*-pair cells. Figure 13 shows the decrypt score for each of the 26 runs for letters connected as *Stecker* to E. In each case the implied *Stecker*-pairs giving a count of at least four are set and the message decrypted and scored using log-bigrams. Clearly, E/H is most likely to be the correct solution.

[45] ETW = Eintrittwalze, the stationary entry plate.

This example of Yoxallismus has given four *Stecker*-pairs at the cost of only 52 message decrypts. This is significantly more efficient than the example given for the first break on FHPQX, which obtained four correct *Stecker* connections after around 500 message decrypts. Unfortunately the process does not work sufficiently well with many short messages. For example, for September 1941, with twenty-five days broken, only four of the 25 breaks exceeded 200 letters, four were 100 or fewer and the average length was 148. With fewer correct *Stecker* identified, the scores in Figure 13 become much less discriminating. Often several incorrect *Stecker* to E give scores higher than the correct *Stecker*. Since we need to carry out this process for each message setting and fast ring setting, there is no advantage if many results need to be processed. However, work continues on this approach to find better statistical tests to improve the discrimination of Figure 13.

A	B	C	D	E	F	G	H	I	J	K	L	M
789	770	773	816	792	761	783	1024	834	858	826	757	794

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
818	831	771	771	816	753	786	807	792	766	773	790	787

Figure 13. Bigram scores for 26 Yoxallismus runs for each *Stecker* to E.

APPENDIX B: FMBLQ – A PENCIL AND PAPER ATTACK

Referring back to the messages in Figure 7 and 8, suppose we make an assumption that the *Ringstellung* is BMU, which is identical to the indicator for the first message of the key period. We also make assumptions that some of the messages have message keys enciphered with the wheels left in position from the end of the previous message encryption. Moving back from the indicator *Grundstellung* position by the length of the message may, in some cases, reveal the message key of the previous message. If some of the message keys are Cillies we may also, with luck, be able to identify one or two right hand wheels.[46] Referring to Figure 7, it is not very clear in what order some of the messages were enciphered. We suspect that two Enigma machines were in use on this station. Probably there would be more messages available from other stations on this key and this would increase the cryptanalysts chance of success.

Figure 14 shows the results of moving back from the *Grundstellung* of several messages for a few selected wheel-orders. We have good fortune here and find

[46] See [11, Appendix 4]. Note that usually several messages would be needed to identify wheels, the method may not work for all cases. For example the second indicator XMS alone cannot distinguish between wheels 3, 4 or 5 in the fast position.

that wheel-order 123 has given all five probable message starts that look like keyboard or other Cillies. We may need to apply up to twenty selected right hand wheel pairs to exhaust all possibilities.

Message Grundstellung	Length	Wheel-order					
		123	124	125	132	134	135
CGL	39	BEY/CFY	BDY	BDY	CEY	CEY	CEY
XMS	286	WAS	WAS	WAS	XBS	XBS	XBS
CNH	202	BEN/CFN	CGN	BEN/CFN	CFN	CGN	CFN
GUD	81	GRA	GRA	GRA	GRA	GRA	GRA
XLY	137	WER/XFR	XGR	XGR	XGR	XGR	XGR

Figure 14. Assumed message starts from several *Grundstellungs.*

Message	Indicator	Message End	Message Length	Message Key
BEWOH	KRU MYD	CGL	39	BEY
GRBLQ	CGL ANX	XMS	286	WAS
FMBLQ	XMS HUT	CNH	202	BEN
XFLBQ	CNH ESW	GUD	81	GRA
HOBQL	GUD ALX	XLY	137	WER

Figure 15. Message keys for five messages from 22 August 1941.

Wheel 2 is the middle wheel and this falls on a slow wheel turn-over at position E for several messages and could easily be missed.[47] For example the start position CFN is the same as BEN due to the double step lead in [7]. Often only the fast wheel can be identified, a slow wheel turn in a favourable position is needed to identify the middle wheel. The slow wheel cannot be determined since there is no wheel to its left to kick over. In this case we do not know whether the slow wheel is 1, 4 or 5, so it will be necessary to try each in turn. An incorrect wheel would be very quickly found in the next stage. If a fast wheel cannot be identified then all 60 wheel-orders will need to be considered. If the assumption of the *Ringstellung* is wrong, then another position will need to be tried. We assume that the message keys of Figure 15 apply, and the actual wheel-order 423 is used for the rest of this example.

We choose a message of good length; FMBLQ looks ideal at 202 letters. Setting the *Ringstellung* to BMU and running a bigram count from BEN gives

[47] The five Enigma wheels I – V have turn-over positions at Q, E, V, J and Z respectively. Clearly this is a bad design feature which was partially addressed when the three new Naval wheels VI-VIII, each having two diametrically placed turn-over points at M and Z, were introduced. Unfortunately this is not an ideal choice. If we applied our hill climb attack on a Naval message, then only 13 ring positions, rather than 26, would need to be considered for wheels VI – VIII in the fast position.

the results shown in Figure 16 (with luck the *Stecker* E/L can be found by Dottery). This has identified a further possible connection M/P with a bigram count of five. C/M or C/U and H/S may possibly be worth trying but with counts of three have less chance of being correct.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	01	01	01		01		02	01			01			02	01			02	02					02		
B				01		01	01			01				02	01					01		01				
C						01			02		01	01	03		02	02	01	02		01	03			01	01	01
D						02	01		01	01		01	02	01		02			02	02		01		01	01	
E												01		02				02		02	01	01	01		01	
F								02	01	01							01	01		02	02			01	01	
G							01							01				01	02		01	01			01	
H													01	01	01	01			03		02	01				01
I										01						01	01		02	01	01		01		01	
J											01				01		01	02		01					01	
K											01	02		01	02		01				01				01	
L														01			01			01	01			01		01
M													01		01	05		01	01	01		01		01	02	01
N															02					01			01		01	
O															02			01					01	01		
P																	01		02	01		01	01			
Q																		01	01	02	01		01	01		
R																		02		01						01
S																			01	01	01		01	02	01	01
T																										
U																					01	01	02	01	01	
V																							01	01	01	01
W																									01	01
X																								02	01	01
Y																										02
Z																										

Figure 16. Bigram count for FMBLQ with *Stecker* E/L.

If the assumptions made are correct, then we now have 15 possible letter transpositions. For example, for KRU MYD BEY, we see that M goes to B at wheel position KRV and Y goes to E at KSW and D goes to Y at KSX.[48] We have two plugboard connections E/L and M/P and need to find others. If we set up our Enigma simulator, real Enigma or TypeX machine with wheel-order 423, Rings BMU and plug connections E/L, M/P, we set the wheels to CNH and try enciphering a message key having a known *Stecker* letter:

Wheels	Input	Expected output	Actual output
CNH	ESW	GRA	BNR

Since we have assumed E for the first letter is correctly steckered, the *Stecker* B/G is implied. This is added to the plugboard and we continue to look for other

[48] Remember that the wheels step before the keyed letter is enciphered and a middle wheel turn-over occurs at the second position.

plugs:

Wheels	Input	Expected output	Actual output
XMS	BEN	HUT	SWP

With the *Stecker* of B and E known, this implies *Stecker*-pairs H/S and U/W. We continue, adding plug connections as they are found:

Wheels	Input	Expected output	Actual output
CGL	WAS	ANX	AKX

Here A has come out correct in the first position and X has come out correct in the last position, suggesting that both A and X to be self-steckered. But A being self-steckered implies *Stecker* N/K for the second letter.

Wheels	Input	Expected output	Actual output
KRU	BEY	MYD	MZO

M in the first place is a confirmation of the correct *Stecker*. In the second place we have the *Stecker* Y/Z.

Wheels	Input	Expected output	Actual output
KRU	BEY	MYD	MYI

In the third place we have the *Stecker* D/I.

We now have the *Stecker* connections E/L, M/P, B/G, H/S, X/X, A/A, K/N, Y/Z, D/I and U/W with no contradictions and have exhausted the possibilities of finding further letters from this set of indicators.

A trial decode of FMBLQ gives:

```
XMUYL PYPKX TDGKL CRMQG
ANROE MXVIE GANQO NXRUE
```

The third word looks like VIER, but we don't yet have the plug connection for T. Since it is on the cipher side we can only try each of the unassigned letters. The connection T/Q gives success:

```
XMUYL PYPKX TDGKL CRMQG VXSXJ GXFNC
ANROE MXVIE RANTO NXROE MJUEQ JSBQS
```

We note that J occurs three times, on both sides, in the word after the second ROEM. A good fit looks like FUENF and this requires the connection F/J.

We now have all ten plugboard connections and can fully decode the message:

```
XMUYL PYPKX TDGKL CRMQG VXSXJ GXFNC
ANROE MXVIE RANTO NXROE MFUEN FSEQS
```

We have fully broken this message using information given away by the bad procedures, using only a pencil and paper attack. If a contradiction were found at any stage a new set of assumptions would need to be made and the work repeated. We used Yoxallismus to obtain the first plug connection, but it can also be found by trial and error or by using information given away by the self-steckers. This is more or less how Enigma was broken at Bletchley Park before the Bombes were delivered in the summer of 1940. However, the workload could be significant: Welchman states that sometimes the key was broken in the first shift after a key change, sometimes at the end of the day, and sometimes never [18, p. 104].

So how much luck was involved in our break? For the ten days listed in Figure 9 there are two other days, 17 and 23 August, each with four suitable message indicators, on which a break may be possible. The remaining days have too few suitable messages. For 17 August it is not possible to determine the fast wheel, but for the the 23rd the fast wheel is identified as Wheel I. This leaves twelve possibilities for the two slow wheels. A decode of one indicator for 23 August gives an opening into the *Stecker*:

Input	Expected output	Actual output
TCR	GUT	FFT

This could imply the *Stecker* R/R and T/T. It is also possible that the correct *Stecker*-pairing is R/T. This is indeed the position and a further three *Stecker*-pairs can then be derived from the four indicators. The connections found are A/I, C/G, E/P, R/T, U/U, YY and Z/Z. Four *Stecker*-pairings are unlikely to give much readable plain text. Decrypting the message and removing letters of uncertain *Stecker*:

```
LXGBP ZTLIO KSOTW DAKEY
--TR- E---- ---E- ----G
```

The message may begin with AN, but ANX is more usual. Therefore we are possibly looking for a German word with TR in the 3rd and 4th position. If the word is a proper noun or there are garbles in the cipher, the situation may be

lost. A search through our Enigma word database yields only six words with TR: BETRIEB, EINTREFFEN, GETRENNT, TRUPPEN, STRASSE, STRIQ.

Betrieb is actually a good fit with three matching letters:

```
LXGBP ZTLIO KSOTW DAKEY
--TR- E---- ---E- ----G
BETRI EB
```

From this break the remaining *Stecker* can be found leading to a complete solution.

For the messages of 17 August, with all 60 wheel-orders and several *Ringstellung* to trial, the situation is not so easy. But this was the prospect at BP before the Bombes were operational [18, p. 110].

A break into the first *Stecker*:

Input	Expected output	Actual output
VHZ	EID	AID

We have possible *Stecker* H/H, I/I, Z/Z and D/D. The actual correct pairing is found to be H/I. This leads to the recovery of four *Stecker*-pairs. A decode also shows few plain fragments. We note from the middle of the third group a fragment corresponding to XVIEREINSXVIER and this leads to the recovery of the complete *Stecker*.

```
SMDAX NOOYH RCZGV VZCBI GIBGW HMXKR
UXNMM ELDLA YBXDI ERPIN QXVJE RIESA
----- ----- --XVI EREIN SXVIE R----
```

APPENDIX C: ENIGMA TRIGRAM FREQUENCIES

A	B	C	D	E	F	G	H	I	J	K	L	M
6.09	2.20	0.72	2.90	12.91	3.03	2.81	1.88	6.16	0.41	1.99	3.90	2.72
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
8.41	4.42	1.47	2.02	6.87	6.23	5.41	4.47	1.38	1.68	6.98	0.89	2.05

Figure 17. Single letter frequency distribution in Enigma decrypts from 1941 (frequencies in %).

EIN	194	INS	137	FUE	108	ZWO	90	ULL	90	IER	89	NUL	87	UNG	83
ENF	80	VIE	80	XEI	78	REI	76	UEN	71	DER	67	AQT	63	ERX	60
SIE	59	GEN	58	DRE	55	EBE	55	VER	53	UND	53	STE	49	STA	49
ENX	47	SCH	47	EST	46	EQS	46	BER	46	STO	45	TRI	45	STR	42
ERE	41	IEB	41	QTX	40	ERS	40	SEQ	40	NGE	39	XST	38	TEN	38
NAX	37	XAQ	37	BEN	37	DIV	36	TER	36	RIQ	36	GUN	36	ROE	36
EGE	36	AND	36	RIN	35	TAN	35	LLX	34	ENS	34	OEM	34	END	34
EHR	33	INA	33	NSX	32	XZW	32	NST	32	TOP	32	KOM	32	TEI	32
RIE	32	NDE	32	RST	31	IQT	31	BES	30	NAQ	30	RAU	29	XDR	29
XVI	29	XBE	29	ORD	29	KLA	29	ERT	28	MIT	28	AUS	28	XRO	28
XMO	28	ANN	28	SSE	28	ABE	28	NFX	27	XFU	27	AUF	27	INX	26
VOR	26	LAM	26	ENI	26	IEG	26	IVX	25	NEU	25	LLE	25	CHE	25
ANZ	24	WOX	24	EIX	24	VON	24	XDI	24	ANG	24	ETZ	23	GES	23
ERP	23	RUN	23	EUN	23	XIN	23	SSI	23	LEG	23	ERB	23	NGX	22
LNU	22	NOR	22	XVO	22	XKO	22	UEH	22	DIE	22	XGE	22	XSC	22
ERA	22	XMA	22	XHA	22	ERU	21	OST	21	ROS	21	ETR	21	LLN	21
PFL	21	ING	21	TTE	21	ELD	21	ENA	21	XKA	21	QSX	20	ERV	20
ITT	20	NGS	20	WES	20	MOR	20	LIQ	20	ERN	20	LEN	20	ZUM	20
ERK	20	ORI	20	RPF	20	ESE	20	ENE	20	EME	20	GAB	20	XPA	20
IEX	19	NDX	19	WAX	19	ORT	19	ART	19	XSI	19	LEI	19	RDE	19
EGU	18	SET	18	BET	18	ARS	18	SPR	18	DOR	18	UER	18	GER	18
MAR	18	IEN	18	XAN	18	ELL	18	ERF	18	EGF	18	MME	18	NIE	18
AGE	18	IED	18	STU	17	EIT	17	NXS	17	OSS	17	GFR	17	MUN	17
TON	17	DEN	17	PAN	17	AMM	17	MEL	17	FRI	17	ERI	17	NNE	17
FLE	17	ERD	17	RTA	17	ENT	16	MER	16	ORO	16	CHO	16	ZEN	16
NEN	16	ARM	16	ERL	16	EHL	16	SZE	16	EFE	16	NBE	16	SGA	16
ONX	15	ANX	15	TEX	15	ERW	15	IST	15	EQT	15	AXS	15	NSS	15
WOS	15	NFS	15	BOR	15	UHR	15	ESP	15	DUN	15	WON	15	ENN	15
SEN	15	RAN	15	AXM	15	AUM	15	INM	15	TEL	15	FEL	15	NEI	15
USG	15	INF	15	FFE	15	SXA	15	NSA	15	TRA	15	NMA	15	FZX	14
UNX	14	EMX	14	AKX	14	SZW	14	SFU	14	SXS	14	KOR	14	RSQ	14
XBO	14	XUN	14	NSN	14	UNI	14	SEI	14	MEI	14	QTE	14	ITE	14
ETE	14	HNE	14	IGE	14	SBE	14	RBE	14	GED	14	TSC	14	LXA	14
NNA	14	BEZ	13	RYY	13	ZYX	13	STX	13	IQX	13	ORW	13	XNU	13
SNU	13	UST	13	MOT	13	ALT	13	RXS	13	ONS	13	BIS	13	IES	13
EDS	13	RAS	13	XAR	13	EIQ	13	ORP	13	TUN	13	TIN	13	REN	13
NAN	13	SVI	13	WEG	13	GEF	13	NZE	13	TXE	13	LTE	13	XSE	13
HRE	13	EID	13	XNA	13	NSZ	12	ERZ	12	KFZ	12	OKX	12	LFX	12
NSV	12	XZU	12	ONU	12	INU	12	NAU	12	EXS	12	ASS	12	RPS	12
EIS	12	RES	12	NXR	12	TAR	12	XPO	12	XNO	12	RXN	12	ONN	12
ALL	12	EIL	12	HEI	12	ELF	12	BEF	12	AXE	12	NTE	12	FSE	12
LIE	12	LDE	12	IDE	12	IND	12	GEB	12	TXA	12	RXA	12	OWA	12
DNA	12	ENZ	11	TYY	11	TRX	11	ELX	11	NIX	11	RKU	11	QFU	11
SAU	11	HAU	11	TZT	11	ETT	11	TST	11	SST	11	FST	11	UPT	11
HAR	11	NIQ	11	AUP	11	PRO	11	NUN	11	SIN	11	CHN	11	JEN	11
ENM	11	SQL	11	XEL	11	NXK	11	MXK	11	RVI	11	XUH	11	FEH	11
ZUG	11	NSF	11	OFF	11	TAF	11	SXE	11	MXE	11	XVE	11	RVE	11
RUE	11	RTE	11	NSE	11	PPE	11	INE	11	NXD	11	XKD	11	UEB	11
OMA	11	AJA	11	XSZ	10	AQX	10	LEX	10	MZW	10	HOW	10	LXU	10
PRU	10	NNU	10	RFU	10	LIT	10	TXS	10	EBS	10	DUR	10	PTR	10

Figure 18. Frequencies of the 400 most frequent trigrams in 20,000 letters of Enigma decrypts from 1941.

APPENDIX D: RECOVERED ENIGMA KEY SHEET FOR SEPTEMBER 1941

Tag	Walzenlage			Ring	Steckerverbindungen	Kenngruppen[49]
01	II	V	IV	ZGL	BN CL DQ EX FP HU IS JT MZ OY	zae umg wue
02	IV	III	II	RIT	AH BO DP EX FN JQ KS LR MU TZ	cxy hqs diz bes
03	V	II	I	FOX	AO CZ DR EM HT IY JX LV NS UP	ace cek soh khq
04	I	IV	II	VMH	AG BE DZ FP HY IS JW LU MV OX	pca hou dpu hyz
05	IV	V	III	JEP	AP DS EH GO IW JX KR LZ MU NQ	chk nwk cgo fev
06	III	II	V	BYJ	AX BH ET FK GY IR JZ MS OU QW	dns dkz
07	II	I	IV	HLS	BL CM DH EJ FR IP KQ NS UZ WY	qoj kpx
08	IV	II	V	QUD	AK BQ CX DZ ES GY HR IW JT MU	wij tsa
09	(unbroken)[50]					hrg
10	I	II	IV	WOA	AZ CW DU FS GR HQ IP KN LO VY	tor dvy hpp tgo
11	V	III	I	EIV	AY BX CW DN ET GR HQ JO KU LZ	asy hnx mqu grs
12	(unbroken)					hut ibw
13	(unbroken)					try
14	II	IV	III	IXM	AV BE CX FW GU HT IS JR LP NZ	tkb fmh ati nvz iai
15	I	V	II	ZPH	AI BG CX FQ HR KT LU MV NW OY	kuy utj kut anp
16	(unbroken)					afu egp
17	III	V	I	XDY	AF DO EW HQ IR JS KU LV MZ NY	diy abl cid ndu
18	II	III	V	FMK	AX CO DP EQ FR GS IZ JU KW LV	cos blv hol vbb
19	V	IV	II	OAT	BM DQ EO FP GR HS IT KV LU XZ	des wmh itz kdp
20	III	I	IV	UJE	AR BJ EQ FV HT IY LW MX NZ OP	tsf dmp
21	I	III	V	CWQ	AB CX EO FP GU IS JW KM LR QV	oki utd bkq zda nrz
22	III	II	I	RGN	AI BM CQ DF EP GR HV LS NW OZ	amc jgc
23	V	I	IV	MBV	CJ DK EO GU HQ IM LR NT SZ VX	dnu elp irv ebp smc
24	II	III	I	SZI	AQ BO CM DP EW FT HS JZ KX LU	gvt bjp fax pqx neh
25	V	IV	III	GQU	AK BP CL DF GR JQ MT OX UW VZ	vyz awt gjl
26	I	V	IV	JWC	BF CX DG HQ JZ KP MS NU OT VY	abv fmy
27	(unbroken)					fpx qbh qix ptz
28	V	III	IV	DKR	AZ BK DP GS HT IQ JW LY OV RU	dtm xrp
29	II	V	I	PTF	BL CM DP FN GI HS JV OU RZ TW	wlg dif clw
30	I	III	II	ANX	AN BQ EY FK GS HM IU OW PV ZX	lcj dlt

Figure 19. Enigma key sheet for the month of September 1941.[51]

[49] Four *Kenngruppen* are expected for each day, it is possible that garbles account for the extra groups on some days.

[50] Three days remain unbroken at the time of writing while two days have not yet been attacked. These days have very few messages, all of which are short. It is possible that some have slow wheel turn-over or they simply failed to break. We are determined to complete this job!

[51] The original German key sheet would have been slightly different. The days were listed in the reverse order with the last day of the month at the top of the sheet. This allowed the cipher operator to cut off and burn the key settings for the elapsed days. Furthermore, the *Wehrmacht* Enigma had numbers on the rings instead of letters; therefore the Ringstellung was given as three numbers instead of three letters.

APPENDIX E: THE MESSAGE FORMS

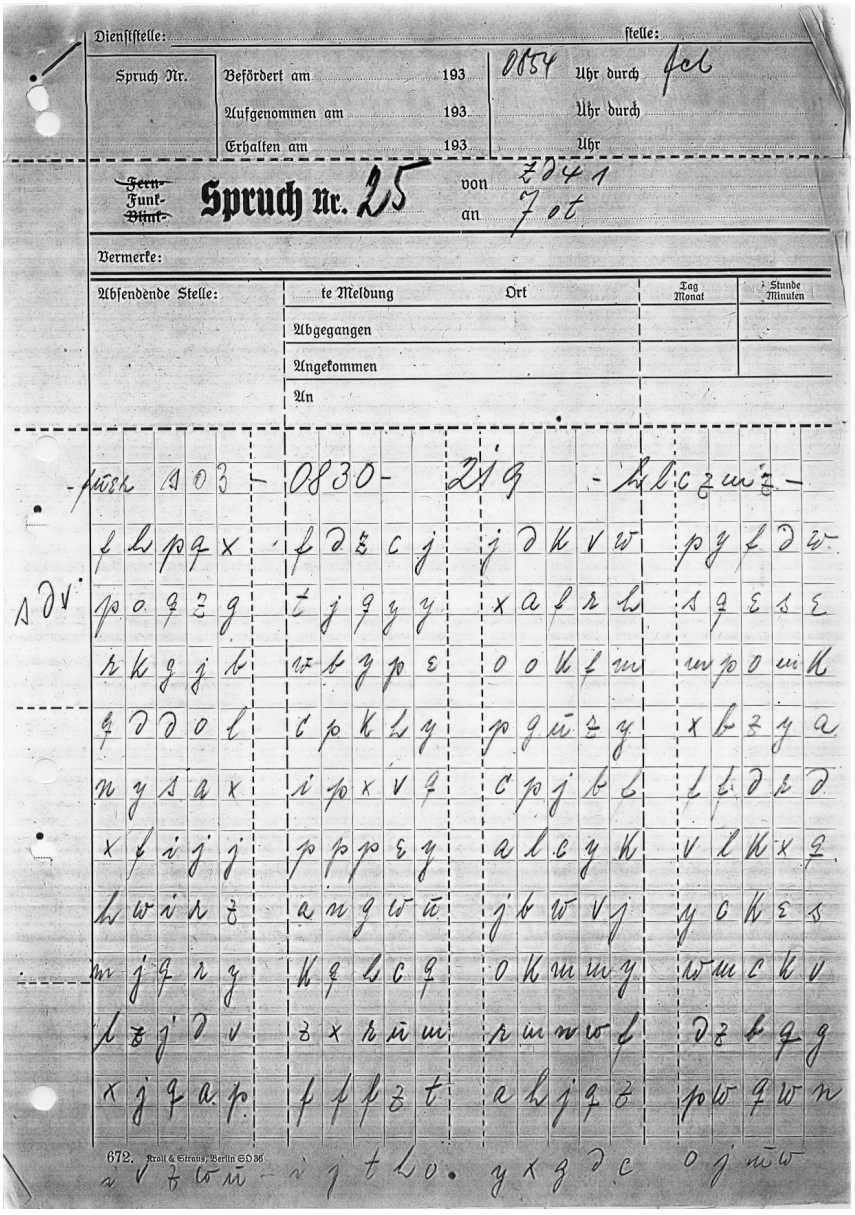

Figure 20. *Funkspruch* form for message number 25, from 13 July 1941. A few message forms, like this example, have the message key written in the margin – SDV. At most this would imply a fast ring setting but was of little use for our analysis.

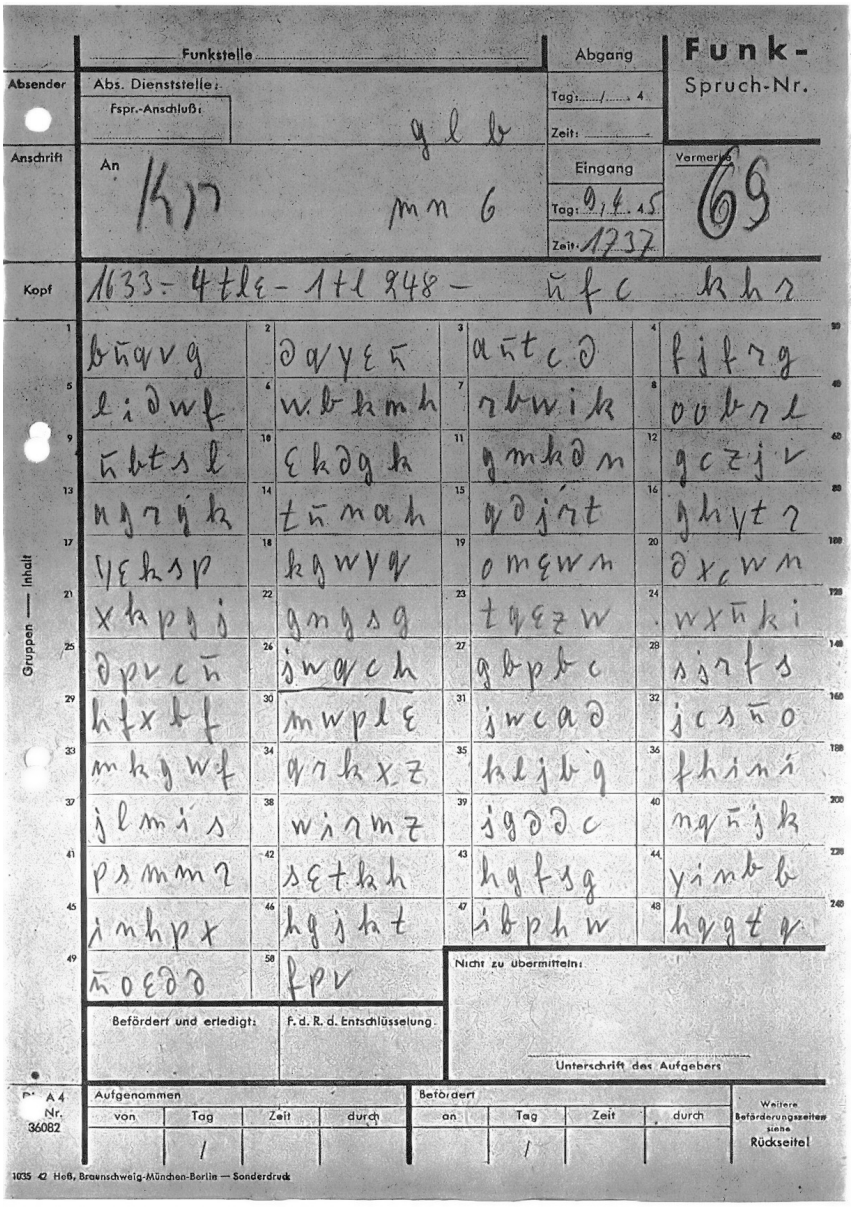

Figure 21. *Funkspruch* form for message number 69, from 9 April 1945. Part one of a four-part message sent by *SS-Standartenführer* Walter Huppenkothen.

```
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.

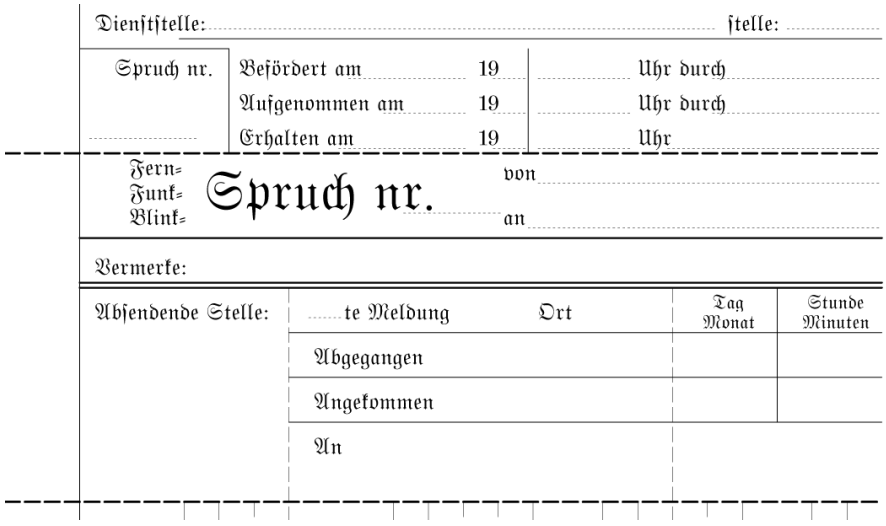

Figure 23. Reconstructed message form from 1941. Several printing works produced these forms, for example: G Braun GmbH Karlsruhe and Kroll & Straus, Berlin SD 36, (Figure 20).

APPENDIX F: FIVE EASY PIECES IN THE KEY OF E

Below are five original German Army Enigma messages from 1941. These have never been published before. They are given in increasing order of difficulty of breaking (for our method). All have been enciphered on the standard 3-wheel, steckered *Wehrmacht* Enigma, using Wheels I – V with ten *Stecker*, and are presented here as a challenge for those wishing to make their own attempt at breaking the messages. The message length given in the heading is as found on the forms. It is sometimes incorrect, however there are no letters missing from within the messages. There is nothing unusual about the messages and there are no intentional clues to them in this paper.

I
- 186 - DOQ VHZ -

PBNXA SMDAX NOOYH RCZGV
VZCBI GIBGW HMXKR RVQCF
JCZPT UNSWA DDSTI GQQCS
AGPKR XXLOM GFXAP HHMRF
SDKYT MYPMV ROHAS QYRWF
WVAVG CCUDB IBXXD YZSAC
JSYOT MWUCN WOMHH JPYWD
CCLUP GSWCL MBCZS SYXPG
MGMQX AUFUL NOZEQ ENHEI
ZZAKL C

II
- 241 - SDV RUD -

TAZUK DVNNF AZOUV YYSXO
ZLRJO TMMXK AWPVU TTUXS
LAQOX GQUKX XKXAL URHGR
SUOHD FJTRE TLFKD MGDXE
MWIXX INTLG EDKVL RTJFX
RFOIE NNIRR WFKTI BVFVE
LLAWR GJNVB YHBZS CJVTZ
PDBGV PBNNA LNAKX OUOJG
WLJXO UXHDS HXJOU HVBVF
DOLMN LYNVC MRGKK YTOCP
DUEVN FMIPT GGJYA YBDES
P

III
- 149 - TLS CMU -

FTMKV DRJMG FBUDK LZCTR
FLTUU IWVJL OYKYX GDCKJ
TMDFB WNLZQ JAXHP GGKFG
SBZOQ KQKUK TINMH BAJOO
AUILA QVFTK LSTMM XGAQL
CNHUW LFHKA ULTXT BIVIF
EWWDY PUCNS TPJHR OBWHE
KYUSB CANYC W

IV
- 83 - ADJ JNA -

LMHNX WEKLM UERDS EVHLC
JSQQK VLDES ANEVT YEDGI
ZQDOD RMDKG SXGSQ SHDQP
VIEAP IENLI CLZCL LAGWC
BJZD

V
- 167 - MRJ LLT -

KLIBM ERJAR WMMHJ STHOY
OOIQB HSSZU EOOKF TASXN
XVYWE SCTCH NRNBL ZPEBH
XPAQE DFNYS XHMNI HRARO
UNBMD ZRZDN WTGUI UCBZN
ZTFJA EKOMJ AZILN RKVFD
UNIEW ILZVL KQYYJ ANKXG
NNNHT EMAVD FXKAY MLWCV
QDFWX LO

Figure 24. Five original German Army Enigma messages from 1941.

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 Lt. Colonel Waldemar Werther and his wife Hetty, now unfortunately both deceased. Waldemar Werther was instrumental in saving these messages from destruction and 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 Bracke 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*. New York: 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 Konzentrationslagers 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 Buchhandlung 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. van der Meulen, Michael. 1996. Cryptology in the Early Bundesrepublik. *Cryptologia*. 20(3): 202-222.

17. 1997. *Five Centuries of German Fraktur*. Winchester MA: Walden Font. (`http://www.waldenfont.com/downloads/gbpmanual.pdf`.)

18. 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.