Modern Cryptanalysis of the *Truppenschlüssel*

Abstract *Truppenschlüssel* (troop cipher) was a manual cipher used by the German Army during World War II. Based on more than a hundred authentic messages which survived the war, a cryptanalysis is performed. The exact encryption procedure is investigated via two plaintext-ciphertext compromises. A specific ciphertext-only breaking tool is developed, utilizing the hill climbing technique. This leads to successful breaks of most of the messages.

Keywords Ciphertext-only, cryptanalysis, *Doppelkasten, Doppelkastenschlüssel*, double boxes, double Playfair, field cipher, German Army, NI cipher, radio message, seriation, trigram statistics, *Truppenschlüssel*, two-box cipher, two-square cipher, unicity distance, unsolved ciphers

1. Introduction

Truppenschlüssel (TS — troop cipher) was a manual field cipher used by German front line troops during World War II. It is a simplified version of *Doppelkastenschlüssel* (DK — double box cipher or double Playfair) used by the German *Wehrmacht* from army groups down to company level (David 1996, 60). Field units of the Wehrmacht, which were not equipped with a higher-grade machine cipher, normally the well-known Enigma — see Hamer, Sullivan, and Weierud (1998) — used various manual ciphers. Furthermore, in cases where Enigma was not available or damaged, such a field cipher provided a manual backup technique (*Ersatzschlüssel* — replacement cipher) for the German Army (*Heer*).

As described by Sullivan and Weierud (2005, 193), by lucky circumstances a large number (approximately 600) of encrypted German Army radio messages from Operation Barbarossa, the German invasion of the Soviet Union during World War II, have survived. They stem from different units of Army Group North (*Heeresgruppe Nord*, abbreviated *HG Nord*), mostly from Tank Group 4 (*Panzergruppe 4*), during the first few months (June to October 1941) of their advance through the Baltic countries toward Leningrad. The majority of these messages use Enigma, while approximately 136 are in a manual cipher that Sullivan and Weierud (2005, 193) suspected was a variant of DK.

When these messages were analysed in 2003, and also later when the authors started their attack on the messages in 2015, the knowledge of Wehrmacht manual ciphers was limited. The only manual systems known to have been used by the German Army were *Doppelwürfel* (DW — double transposition),[1] DK, and *Rasterschlüssel* (RS — stencil cipher). Of these only DK was known to have been used in 1941 and this system was therefore used as an entry point in attacking the manual cipher messages from Operation Barbarossa. It was first in 2020 that one of the authors discovered that the messages were enciphered with the, until then, unknown cipher system *Truppenschlüssel* (TS).

Inspired by the codebreaking project described here and partly based on its results concerning the analysis of the German field cipher procedures, one of the authors subsequently performed detailed research to clarify which hand-operated ciphers were used by the Wehrmacht before and during World War II. His brand-new results, illustrating the surprisingly diverse development history of Wehrmacht manual ciphers between 1936 and 1945, will be published by Weierud in a (forthcoming) companion article.

[1] In official German documents it is often described as *Doppelwürfelverfahren* (DWV — double transposition system). Many of the manual ciphers were described as systems, *Verfahren*. Other examples are *Heftschlüsselverfahren* (HSV), *Wehrmacht-Handschlüsselverfahren* (WHSV) — another double transposition cipher, and *Kastenschlüsselverfahren* (KSV), to mention a few.

2. Historical Background

During World War II, the German Wehrmacht used various manual ciphers. The Navy (*Kriegsmarine*) had e.g., *Reserve-Hand-Verfahren R.H.V.* (reserve hand procedure) (Sebag-Montefiore 2000, 213; Morris 1993, 238) and *Werftschlüssel* (dockyard cipher) (Meulen 1995a, 1996), while the Army and Air Force used *Heftschlüsselverfahren* (Meulen 1995b), *Doppelkastenschlüssel* (David 1996), and later *Rasterschlüssel* (RS44) (Cowan 2008). The DK can be interpreted as an extension of the well-known classical Playfair cipher, invented as early as 1854 by the English scientist Sir Charles Wheatstone. In contrast to the single Playfair square, DK utilizes not one but two adjacent squares. Hereby, the combinatorial complexity and the key space is enhanced. Compared to Playfair, DK nearly doubles the key size. Nevertheless, it remains a monoalphabetic, digraphic, substitution cipher.

The German Wehrmacht developed different variants of manual ciphers during the war; some used only a single substitution stage but most used two cascaded stages, as described by e.g., Schick (1987). Additionally, a seriation of the plaintext was often performed, meaning an arrangement of the plaintext in lines of constant length, mostly 17 or 21 letters, followed by encipherment of vertical adjacent letter-pairs as bigrams.

In contrast to Enigma ciphertexts, early manual cipher messages, as intercepted by the British, showed no indicator. They were therefore designated “NI cipher” by the Allies, short for Non-Indicator (David 1996, 56). Other designations were “double boxes” (Schick 1987, 35) or “two-square cipher” (USAIS 1990). As reported by several sources, e.g., (Schick 1987, 35; USAIS 1990, 12; David 1996, 63), DK was broken by the Allies regularly and fairly easily, provided that cribs were known (David 1996, 69), or if a sufficient amount of text was available, then by anagramming with the aid of a bigram frequency count (Currer-Briggs 1993, 214). As described by Welchman (1982, 57), at Bletchley Park it was the British Brigadier (then Colonel) John H. Tiltman (1894–1982) and his team who successfully attacked German manual ciphers (Bauer 2013, 63). American cryptanalysts also broke them. According to Joseph S. Schick (1987, 35), who served with the 849th SIS (Signal Intelligence Service): “The solution of a single message was not too difficult.” The most comprehensive account of the allied breaking of DK is to be found in the American Signal Intelligence Report “Double Playfair System” (SIS 1943).[2] This report has much more information about DK and the cryptanalytical process, however it mainly deals with the latest version of DK, *Nachrichtenschlüssel 42* (NS42 — Message cipher 42).

In March 1944, the Germans introduced a new manual cipher called *Rasterschlüssel 44* (stencil cipher 44). It utilized irregular grids and a transposition rather than a substitution, and partly replaced the previous manual cipher procedures by August 1944 (Cowan 2004, 25). RS 44 proved to be significantly stronger, but also more difficult for the German cipher clerks to handle.

Unfortunately, none of the references above give a good explanation of the DK manual cipher system as we shall see later. The reason for this is that the various authors base their accounts on cryptanalytical information obtained while breaking different versions of a same cipher. DK went through several modifications during the period it was in use from its introduction on 1 March 1941 to its final days in the autumn of 1944, when it was replaced by RS44 on 1 September 1944.

None of these references were important for the study and cryptanalysis of the TS messages from June to October 1941, however they did help us to get a better feeling for the problem. The only important documents were the German DK cipher instructions; the first draft of the instructions (OKH 1940) from December 1940 and the preliminary instructions (OKW 1941) from December 1941.

[2] The report was kindly offered to the authors by a reviewer. For this we are most grateful.

3. Cryptanalysis

When (re)starting the cryptanalysis of the messages suspected to have been manually enciphered, Michael van der Meulen's extraordinary collection of authentic German messages of Army Group North, to which he gave us full access, was the basis of this codebreaking project. Of approximately 600 messages from 1941, nearly 500 were identified as Enigma ciphertexts. The rest were obviously not Enigma. Although suspected to be a variant of *Doppelkastenschlüssel* (DK), this was uncertain. Therefore, as a first step toward the intended breaking of the messages, it was essential to clarify the exact enciphering technique. In order to break the messages, it is first mandatory to investigate precisely the method being used. To achieve this, a study of the DK was seen as a good starting point.

3.1 Doppelkasten Studies

DK existed in several known variants, all utilizing two cipher squares with the 25 letters of the alphabet, skipping J, randomly arranged in a 5 × 5 box.

The usual preamble (*Spruchkopf*) of an Enigma message consists of the time of day, the message length, and six letters, which represent the enciphered message key. A typical example was given by Sullivan and Weierud (2005, 202) as 1130 – 146 – BIU AVL –. Here, the time when the message had been encrypted, is 11:30 a.m., the number of letters is 146, and the enciphered message key, also called the message indicator, is BIU AVL. While the lion's share of the *HG Nord* radio messages proved to be Enigma ciphertexts, which could largely be broken by Sullivan and Weierud (2005), and later by Ostwald and Weierud (2017), more than 100 are different. First, they have a different preamble with a missing indicator. Moreover, they did not break with the aid of our Enigma-breaking tool, which was quite successful in breaking the Enigma messages. A further analysis indicated that the letter count for these messages is always even, while Enigma messages show both even and odd lengths. A Fourier transform of the ciphertexts clearly showed a period of two, thus indicating a bigram substitution. Several repeats were found in the ciphertexts, sometimes with lengths of up to 14 letters, and mostly with even distances. A particularly impressive example (Fig. 1) is message No. 218 of 17 July 1941.

0025 - 82 -
TNIDR AONZU CZPKH LGRFB
HPONN EYOIT GSUBG EGHNF
RUBED PISEB NDGIV ITDQI
LKLS**P SHEBB ONXPT NBEPS**
HEBBO NXPTN BE

Figure 1. Message No. 218 of 17 July 1941.

It is not important that the preamble here erroneously indicates a length of 82 instead of the actual 92 letters, but that at the end of this ciphertext a noticeable repeat can easily be spotted, namely the letters P SHEBB ONXPT NBE. Such an occurrence is virtually impossible for any Enigma ciphertext, and it is a strong indicator of a manual cipher being used. Both the even length of 14 letters of the repetition, and the starting positions, namely 65 and 79, corresponding to this length, substantiate the suspicion of a digraphic cipher. Nevertheless, it is still not entirely clear exactly how it worked. Theoretically, it could be the Playfair cipher, the origin of all bigram substitution ciphers. On the other hand, that is rather unlikely because it is known that the German Army during World War II adapted Playfair to "Double Playfair" by introducing a second square.

Two relevant documents from that time were available when the codebreaking project was carried out. Both were formerly classified as secret (*Geheim!*). The first one (OKH 1940), of 2 December

1940, originates from the Army High Command (*Oberkommando des Heeres*, abbreviated *OKH*). It is entitled as a draft (*Entwurf*) of the cipher instructions (*Schlüsselanleitung zum Doppelkastenschlüssel*). The second one (OKW 1941), of December 1941, was issued by the Supreme Command of the Armed Forces (*Oberkommando der Wehrmacht*, abbreviated *OKW*), and is entitled "Provisional Cipher Instructions" (*Vorläufige Schlüsselanleitung zum Doppelkastenschlüssel*). Both documents identically describe the *Doppelkasten* procedure (OKW 1941, 3–5), which is summarized in the following.

DK is a manual encryption technique using substitution. The key is changed at midnight. It consists of two boxes (*Kästen*), each of which contains a randomly scrambled alphabet that omits the letter J. The line length for the plaintext is fixed at 17 letters. Within the plaintext the letter J, if necessary, is substituted by II (double-I). The minimum text length is unlimited; the maximum length is 500 letters. As an example (Fig. 2) the following daily key is presented in the booklet.

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

Figure 2. Example key as given in the German instructions (OKW 1941, 4).

Enciphering of successive bigrams is done by finding the first letter of each bigram in the first box, and the second letter in the second box. At this juncture two cases must be distinguished. In case #1 the two letters are in the same row, while in case #2 they are in different rows. In the first case, here called the "in-line case," the first letter of the ciphertext bigram is the letter to the right of the plaintext letter in the second box, and the second letter of the ciphertext bigram is the letter to the right of the plaintext letter in the first box. For instance, the plaintext bigram PE, when enciphered once through the two boxes, yields LW. In the second case, if the two plaintext letters are in different rows, here called the "cross-over case," they can be interpreted as forming two diagonal vertices (corner points) of a rectangle. The remaining two vertices (taken from right to left) then indicate the corresponding cipher bigram. As an example, the plaintext letters RT are enciphered as AF. These two cases, however, do not represent the final result of the enciphering. The cipher instructions (*Schlüsselanleitung*) of OKH (1940, 5) treat the obtained bigram as just an intermediate result and encipher it once more using the same procedure. Doing this, AF is transformed to IY, and the previously mentioned LW to HX, yielding the final ciphertext bigrams.

Furthermore, the German booklet illustrates a typical preamble (*Spruchkopf*), – 1512 – 54 – IWE –, being composed of the time of origin 15:12 (or 3:12 p.m.), the number of letters 54, and the discriminant (*Kenngruppe*) IWE. After that, the following plaintext (Fig. 3) is given for illustration.

```
FEINDLIQERANGRIFF
AUFSTRASZEADORFST
RIQBEHAUSE
NABGEWEHRT
```

Figure 3. Example of plaintext with seriation as given in the German instructions (OKW 1941, 5).

The German plaintext reads *Feindlicher Angriff auf Straße Adorf Strich Behausen abgewehrt*, translated "Enemy attack on road A-village to B-town repulsed." Here some well-known and commonly used German Army transcriptions can be seen, such as substituting the frequent bigram *ch* by Q, and the traditional letter *ß* (a ligature of 's' and 'z') by SZ. Furthermore, we see that the plaintext is ordered in lines of 17 letters, the last part being shorter has been divided into two lines of ten letters each. This is a basic cryptographical measure, which is further described in the German instructions.

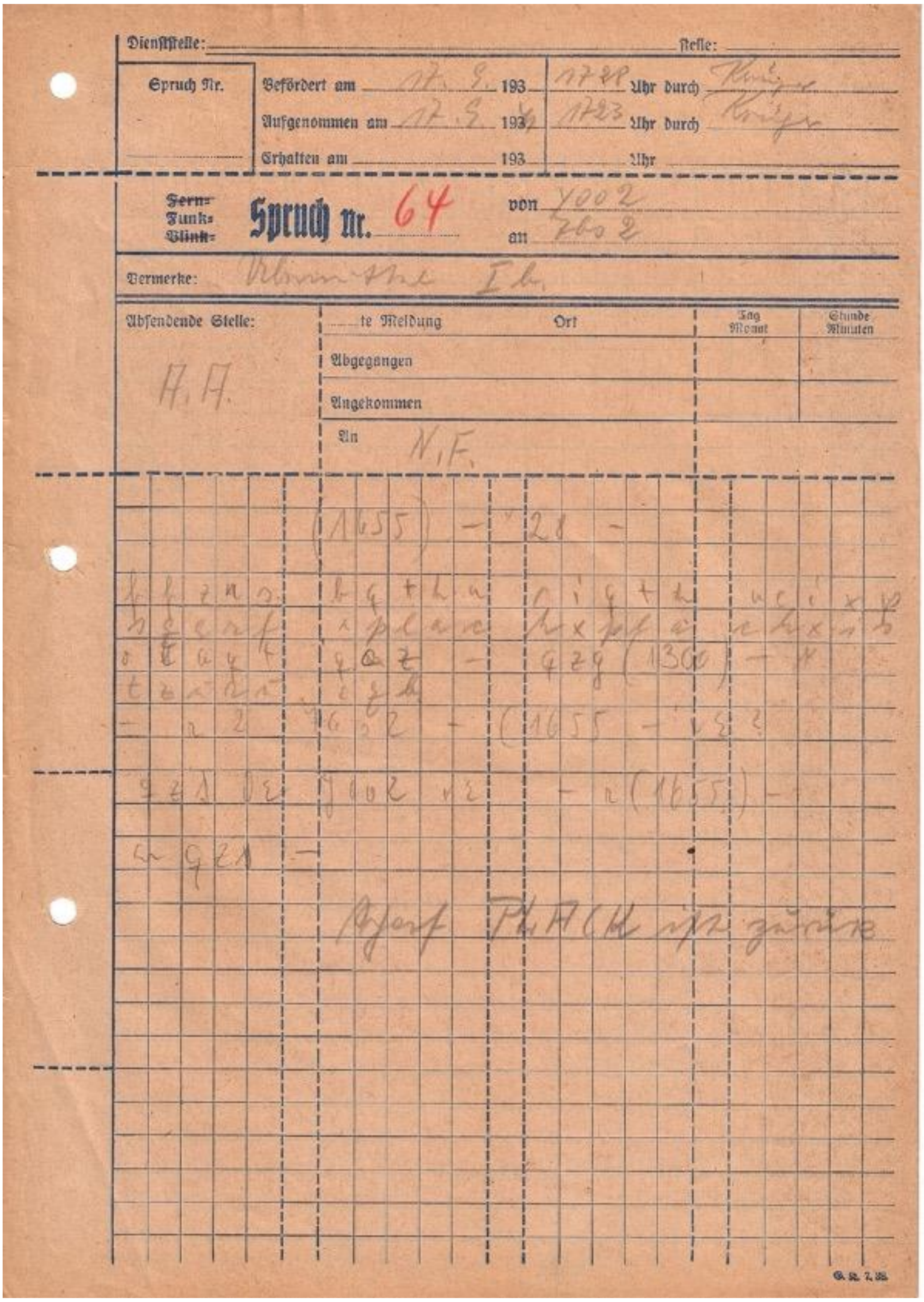
The aim is to form bigrams from the vertically aligned letters of two-by-two lines. In the case of Figure 3, for example, FA and EU are the first two bigrams to be enciphered.

This measure is a known procedure called seriation, e.g., by Fouché Gaines (1956, 207) and David (1996, 61). It is intended to strengthen the ciphertext against cryptanalytical attacks. The idea is that by seriation frequent plaintext bigrams such as ER, EN, and EI are broken up, and the ciphertext bigrams then become slightly more randomized. In fact, seriation is not a very strong cryptographic measure. The American codebreaker Charles David (1996, 63), who successfully broke DK as a member of the Army Signal Corps from 1942 and onwards, states that the bigrams after seriation now reflected "the individual frequencies of disconnected German letters taken two at a time." Furthermore, he describes a twofold substitution as being used at that time by the Germans.

Unfortunately, the available documents and publications do not match concerning the exact definition of how to choose the horizontal neighbours (left-hand or right-hand), how to read out the cipher letters from the boxes (sequence from left to right or right to left), what line length should be used for seriation, and how many cipher stages were cascaded (one or two). For instance, the German instructions define the right-hand neighbours as the ciphertext letters, while David (1996, 62) writes: "If the two letters of a bigram to be encrypted lie along the same line in both boxes, we take the letters immediately to the left as cipher values." Furthermore, the instructions define lines 17 letters long as being used for seriation, while David (1996, 64) observed a line length of 21 letters. Did the Germans not use the same procedure for all parts of their armed forces, or did they alter or modify it during the war? What we did not know during the codebreaking project, but know now, is that the reason for this discrepancy is entirely due to the time frame. In 1944 the seriation length had been increased to 21 letters and this is what David experienced. All evidence shows that the same procedure was used by all parts of the Wehrmacht that adopted these systems.

David (1996, 74) reported that contrary to the double encipherment utilized in the first months of 1944: "With the invasion of Normandy in June 1944, much of the enemy traffic began to be enciphered only singly, the second, double, encipherment being omitted." As we now know, the reason for this is that before the invasion the situation was static and very few troop communications would have taken place. After the invasion this changed overnight and the troops started to use another variant of their manual cipher system, designated *Truppenschlüssel 42a* (TS 42a), which turns out to be a modified version of the original *Truppenschlüssel* (TS). While David's report is mainly focused on the year 1944, the messages of *HG Nord* stem from the German eastern campaign of 1941. Moreover, different levels within the military hierarchy, say companies or commands, could have used different enciphering procedures.

3.2 Unravelling the Truppenschlüssel



Dienſtſtelle: ſtelle:

Spruch Nr.	Befördert am 17. 9. 193	1728 Uhr durch	Krüger
	Aufgenommen am 17. 9. 1941	1723 Uhr durch	Krüger
	Erhalten am 193	Uhr	

~~Fern~~- Funk- ~~Blink~~- **Spruch Nr.** 64 von Y002 an Zbo2

Vermerke: Ukrainethe Ib

Abſendende Stelle: A.A.

…te Meldung	Ort	Tag Monat	Stunde Minuten
Abgegangen			
Angekommen			

An N.F.

(1655) – 28 –

hhzns bqthu aiqth ucixp
bgerf xplac hxpfa chxnb
otayf qaz – qzg (1300) – 4
tzaza zgh
– n 2 6 2 2 – (1655 – 1 8 ?
9 2 1 0 2 9 0 0 2 1 2 – n (1655) –
4 9 2 1 –

Abruf PLACK ist zurück

G.K. 7.38

Figure 4. A rare message sheet of 17 September 1941, showing both ciphertext and plaintext.

Fortunately, two very special message sheets are available, which contain both the received ciphertexts and the deciphered plaintexts. The messages were transmitted on 17 September 1941. Figure 4 shows a scan of one of these message sheets.

Of course, such very rare plaintext-ciphertext compromises are extremely valuable in order to investigate the unknown details of an encryption technique. As can be seen in Figure 4, both the ciphertexts and plaintexts have been written in lowercase. Here (Fig. 5), for greater clarity, uppercase letters are used for the transcribed ciphertexts, and lowercase letters for the transcribed plaintexts, in in the respective lines below.

```
    (1655) — 28 —

FFZNS BQTHN CIQTH NCIXP
sqarf xplac hxpla chxis
OOAQT QAZ
tzuru eqb
```

```
    (1720) — 126 — TNDGL
                   ceost
XSBYQ CHBHS KYQCH BHSKR
ufxhe nning xhenn ingxn
CERTI ENRVO HMNGM RFENK
aqrxg ereat eanbo rderu
QSAGV OHGWK ZFWEN BHQFA
ngheu tebil xobeg inspx
HRWZY CHAHR WZYCH THBHP
reima nnxre imann xeing
NZHSY PRCKI NZGOR ZSENR
etrof fenxk radme ldern
KEUZV TPZUW AWPSZ BFZNS
iqtda xplac hxssx sqarf
B
x
```

Figure 5. Transcribed ciphertexts (uppercase) and plaintexts (lowercase) of 17 September 1941.

The emended plaintexts (with ‘x’ interpreted as a space) read “*Scharf[ührer] Plach Plach ist zurück.*” (Corporal Plach is back.) and “*O[ber]stu[rm]f[ührer] Henning Henning. Nachr[ichten]geräteanforderung heute bei Oberinsp[ektor] Reimann Reimann eingetroffen. Kradmelder nicht da. Plach, SS-Scharf[ührer].*” (Lieutenant Henning. Request for radio equipment arrived today with Senior Inspector Reimann. Dispatch rider not available. SS Corporal Plach.) Neither the semantic nor the intelligence value of these messages are important for the codebreaker, but the relationships between the ciphertext and plaintext letters are.

First and foremost, it is obvious that in contrast to the descriptions in the available instructions and publications, here no seriation has been carried out. Quite the contrary, the natural order of the letters has been retained, and simply every two consecutive letters of the plaintext were used as bigrams for enciphering. Another very important item can also be examined via these compromises. If it is really *Doppelkasten*, then the following can be checked. Enciphering any bigram, symbolically written as 12, with 1 and 2 representing any letter, yields a ciphertext bigram, which can be symbolically written as 34. In cross-over cases, which provide the majority of all cases, the following reciprocal relationship must be fulfilled: if 12 yields 34, then enciphering of 43 must yield 21, or short, if ‘12–34’ then ‘43–21’. To verify this characteristic, suitable bigram pairs must be detected in the given plaintext-ciphertext compromises. Fortunately, at least two of them occur, namely ‘kr–IN’ and ‘ni–RK’ as well as ‘qt–EU’ and ‘ue–TQ’. They are marked respectively by solid and dotted underlines in Figure 5.

For further verification of the exact enciphering technique, we tried to reconstruct the key used for these messages and succeeded without the aid of computers, using only paper and pencil via trial and error. For that, it was necessary to detect and correct some garbles in the ciphertexts. For instance, the plaintext bigram ‘sq’, which occurs twice, is in one case related by ‘sq–BF’ and in the other case by ‘sq–FF’ (marked with undulating lines in Figure 5). Only one of the two inconsistent relations can be true. The recovered key squares are given in the following Figure 6.

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

Figure 6. Recovered key squares of 17 September 1941.

After that, it became evident that for the *HG Nord* messages of 1941 no seriation had in fact been applied. Moreover, no two-stage digraphic substitution, as described for the year 1944, had been used, but rather only a single stage. Incidentally, for the intended computerized solution of DK messages, a double stage variant would not be harder to solve than a single encipherment, so long as the same key squares were used for both stages. Only the use of different pairs of key squares for a two-stage DK would be substantially harder to break. To the authors' knowledge, the latter was never used by the Germans. Though they certainly knew that such a procedure would be significantly stronger, they also were aware that it was too complicated and thus far from being field approved (*feldtauglich* or *truppenbrauchbar*).

In conclusion, the field cipher as used by *HG Nord* in 1941, is a monoalphabetic substitution cipher based on bigrams that are taken consecutively from the plaintext. No seriation takes place. For encipherment two square boxes, each with a size of 5 × 5, are used. Each of the boxes is randomly filled with the letters of the alphabet, omitting the letter J. A bigram is enciphered by finding its first letter in the left-hand square and its second letter in the right-hand square. The encipherment takes place as previously assumed and described. Much later we found out that this procedure was named *Truppenschlüssel* (TS). Decipherment is, of course, the reversal of encipherment. In order to ease the decipherment work, the instructions recommend moving the first square to the right of the second square. Hence for the cipher clerk, the decipherment operation thus becomes almost the same as for encipherment. The only difference he needs to observe is that in the in-line case for decipherment the letters to the left are read out, while for encipherment it is the letters to the right. Nevertheless, operation is eased by moving the first square to the right of the second square, because then the order of using the two squares is always left to right, and moreover, in the cross-over cases, the decipherment and encipherment steps remain identical.

The key space can be determined via the number of different possibilities for filling in the letters of the alphabet into the two key squares. Each square with its size of 5 × 5 generally allows for 25! different alphabets, two independent squares then consequently allow for 25! × 25! arrangements. For reasons of symmetry, several arrangements yield redundant keys. In total the previous number must be divided by 5! × 5 × 5, i.e., 3000, resulting in 25! × 25! / 3000 or approximately 156 bits. As derived by Shannon (1949, 660), and, e.g., defined by Menezes, van Oorschot, and Vanstone (1996, 246), the expected unicity distance of a cipher is approximately H/D, where H is the logarithm of the number of possible keys, and D is the plaintext redundancy (in bits/character). With H ≈ 156 bits for this field cipher, and D ≈ 3.2 bits for *HG Nord* texts, this results in a unicity distance of around 49 letters. This is quite similar to the figure given by C. A. Deavours (1977, 49) for a foursquare cipher of a little more than 45 letters.

4. Breaking Tool

After clarification of the exact enciphering procedure used by *HG Nord* in 1941, the next goal was to break their messages. While only a very few plaintexts directly derived from this cipher are known, many German plaintexts from the eastern campaign were already available to the authors from breaking of hundreds of Enigma ciphertexts. Nevertheless, we do not really have access to cribs concerning the unsolved messages. Therefore, we decided to implement a computerized ciphertext-only attack on the manual cipher. Assuming the message content of Enigma and manual cipher messages are similar, then known Enigma plaintexts should be an excellent starting point for generating suitable statistics files for use with the manual cipher texts. However, one important difference between Enigma and the field cipher plaintexts must be considered, namely that with the *Truppenschlüssel* the letter J is omitted and substituted by II (double-I). It was an easy task to modify existing Enigma text bases in this way and generate statistics for the suspected plaintexts.

For computerized automatic breaking of the ciphertexts, a hill climbing technique was implemented. Starting with two randomly initiated key boxes, a trial decryption of a given ciphertext was performed. The closeness of the resulting candidate text to plaintext was measured with a trigram count of the candidate text. This has been found to be a good compromise. Trigrams are superior to, e.g., bigrams and are less affected by garbles than tetragrams or even hexagrams (Ostwald and Weierud 2017, 411), while tetragrams proved efficient for solving *ungarbled* Playfair ciphers (Cowan 2008, 75).

For each cycle the key boxes were modified slightly, bearing in mind not to change the boxes too heavily, and a new trial decryption was performed. Next, a trigram count of the new candidate text was taken, with an increased count indicating that it came closer to plaintext. In this case the modified key boxes were retained for the next cycle. However, if the count decreased, then the previous key boxes were restored and a different modification tried. After investigation of several different techniques and strategies for modifying the key squares and the subsequent hill climbing, it was found that the variations of the squares should be kept rather simple and ultra-fast. Accordingly, within each 5 × 5 box only letters from rather small subunits of just four or five letters (quadruples and quintuples) are systematically permutated, such as quads (2 × 2), rows, columns, and diagonals. In addition, all possible swaps of two lines, columns, or diagonals are tested in order to increase the plaintext score. Once again, the well-known KISS principle proved valid: “Keep it simple, stupid.” Don’t try to implement highly sophisticated techniques. Moreover, don’t waste time. Use the high speed that a PC offers for performing relatively simple operations.

A problem frequently observed in hill climbing is the tendency of converging to a local maximum and to stay there, thus missing the global maximum. This was also seen in the early versions of the authors’ hill climber. To overcome the problem, two cascaded program stages were added, similar to the well-known Shotgun hill climbing techniques. The first stage controls the internal hill climber and checks if it is resting on a possibly local maximum. Then it applies a kick of varying intensity to the key squares, meaning a random swap of several letters in each of the two squares. This procedure ensures that the hill climber walks away from a local maximum and searches for other peaks, while preserving a great deal of a key that is possibly partly correct. After finding another maximum, or unluckily finding the original maximum again, the intensity of the kick is boosted in order to force the hill climber to continue its search in another region. If nothing helps, and the global maximum cannot be found, then from time to time a complete reset takes place, meaning a restart with totally refreshed randomized key squares. This is controlled by a second (outer) stage.

Most up-to-date commercially available PCs possess multi-core processors. In the authors’ case of a PC with an Intel i7-3770 processor running at 3.4 GHz, four independent cores were available. Together with hyper-threading technology, this allowed for eight instances of the program running in parallel. Initially, these instances were completely independent of each other. Figuratively, they represented eight individual explorers, traveling through the world looking for Mount Everest. After a while, it was realized that this technique might not be optimal. In real mountain climbing the advantages of a rope team are well-known. Why not also try this for codebreaking? For that, the eight instances were synchronized via a central data pool, called the headquarters (HQ). Now, each of the explorers continuously reported its position and height to the HQ, and, from time to time, each explorer compared its own height with the global record as stored in the HQ. In cases where the record was higher than its own height, it jumped to the higher region. In this way, the rope team always came together after a period of individual exploring, always focusing again on the most promising regions. Experiments demonstrated that this technique indeed strengthened the efficiency of the hill climber.

For checking and further optimisation of the design of the breaking tool, several test runs on artificial self-made ciphertexts were analysed. As a first check of the breaking ability, parts of the key boxes were correctly predetermined and fixed, in order to ease hill climbing. This is comparable to giving it a head start or, figuratively, to dropping the explorers deliberately in India or China, rather than in South America, to ease finding the top of Mount Everest. Furthermore, rather long artificial ciphertexts were used initially, comprising several hundred letters. After the first successful solutions, the number of correctly predetermined and fixed key letters was reduced, until the key was correctly recovered without any head start. After that, the ciphertext lengths were reduced until they assumed reasonable values, which are defined by the given message lengths.

5. Decryptions

At this stage of the codebreaking project it had not yet been determined how often the keys were changed, although in the German instructions (OKW 1941, 3) a daily key change at midnight was specified. However, David (1996, 74) reported: “The enemy changed its boxes every three hours of every day.” As we now know from recent research results (Weierud, forthcoming), changes this frequent were not in operation in 1941, but were first introduced more than a year later when *Nachrichtenschlüssel 42* (Message cipher 42) came into service.

Enigma messages use an individual message key (*Spruchschlüssel*), which is different for each message of a day. Whether the manual cipher also used something like that was unclear. But the obviously identical keys for both known plaintexts of 17 September 1941 were an indication that this might not be the case. If so, then all messages of a single day could be assembled by the codebreakers in order to get a sufficiently long combined ciphertext. By the way, this would not have been so easy if seriation had been utilized during encryption.

The first attack on a real *Spruch* was done on 1 October 2015, combining the six messages of 7 July 1941 to yield a total ciphertext length of 848 letters. After a run time of less than ten minutes the first break of such a manual cipher message of *HG Nord* succeeded and partly garbled plaintext flashed up, beginning with: *Eins Drei x Kolonne benoetigt dingend Zwo x Racken x Neun Komma Sieben Fuenf x del x Yto Nall x und x Zwo x Sqlaeuqe yus Dqvisionsreserve x*. Emended: *Eins Drei x Kolonne benoetigt dringend Zwo x Decken x Neun Komma Sieben Fuenf x mal x Zwo Null x und x Zwo x Sqlaeuqe aus Divisionsreserve x.* Translated: 13th convoy urgently needs two tyre casings 9.75 times 20 [i.e., the rim width times the rim diameter, both in inches] and two tubes out of the division’s reserve.

Certainly, more important than the intelligence about flat tyres gained from the recovered plaintexts is the confirmation that all the six messages broke with the same key. That allows for combination of individual ciphertexts and parts of the same day, and it eases breaks. In the following days and weeks several other messages were broken, in total 94 out of approximately 136 suspected or proven manual cipher messages. The first break of an individual message succeeded on 9 November 2015. It is the one and only message known of 30 July 1941. Its length is 228 letters (Fig. 7). The breaking software needed less than two and a half hours to solve it.

```
DSCBE SNVYQ ELKAM EWQPA
SQRGR AAQUE LAPQU EKQPD
QKQDW OFRUE FTCIM KUUMK
UUQPC AGUAG ZROAA QZRDX
ESCTF DQGES ORCAQ DVOPD
QMPDQ KRRAQ NURSV DURQR
BRWNN GWILA YQQDV OGQVS
FGREI IFTKZ RSGIQ KFTLK
IDAQN PDQDS YQECH PUKBX
FDIQC AQDVO QDVOI LKADS
DHYQP DQKPD QKQLO QZLQK
QLOQZ LGK
```

Figure 7. A singular message of 30 July 1941.

One of the shortest combined ciphertexts that could be broken originates from 14 July 1941. Three messages are known from that day (Fig. 8), with lengths of 128, 24, and 42 letters, in total 194 letters.

```
      1450 — 128 —         |       1825 — 24 —         |        2100 — 42 -
                           |                           |
DFEDL OQAFA MNCCY FLOPD    | PZUBV SYWLQ RPERM GWZIA   | NZIOR MQRKE PGCRS DLSRV
WTQRS FWRPS YYPTS BLCTX    | FALC                      | PDPUQ RGCWD FZRXL YGSGQ
FAZYK ZRFYZ WVVUR WMKUN    |                           | FG
VULQP DURVS BWSVW TOTCS    |                           |
SZNGZ IHAHC VVLRE BLQPM    |                           |
FZRXL TRWLC NTRPG HAQQB    |                           |
SVVQP DLU                  |                           |
```

Figure 8. Three messages of 14 July 1941.

The partially garbled plaintexts read: *Bitte uz Angaoe ob Beutebetrhwbstoff verwendungsfaehig x Wenn iia kann Nertellung wie besproqen durqgefueirt werden x Hartiienstei x Hartiienstein* (Request statement about usability of looted petrol. If yes then distribution may be performed as discussed. Hartjenstein.) *Meldung bereits abgegangen*. (Report [has] already [been] sent.) *Ntpaeqtrosz bisher niqt evotroffen x Hahn l Fahn y.* (Luggage train [has] not yet arrived. Hahn.)

6. Practical Experiences

The process of emending the raw decrypts is fascinating. Nearly every single garble tells its own story. Was it simply a human error during the enciphering process or was it perhaps enciphered and transmitted by different persons? Errors could then have been caused by a cipher clerk with a poor handwriting and a radio operator misreading the ciphertext on the message form. Or was the Morse code erroneously received? Say the receiver missed an initial dit for the letters F or H, resulting in an erroneously heard R or S. There exist many reasons and possible explanations for garbles. Moreover, depending on the rows and columns of the two letters of each bigram in the cipher boxes, a single ciphertext garble sometimes causes only a single plaintext garble, be it in the first or the second letter, and while in other cases both plain letters are affected.

Besides the main challenge of breaking the ciphertexts, the process of emending the raw decrypts can also be pretty challenging. Even for a native speaker, who, thanks to the practice with the Enigma messages of *HG Nord*, already has some experience and specific knowledge concerning all the military phrases, abbreviations, names of persons and locations involved, and the wording used within the German military messages, it is sometimes quite hard. An illustrative example for some obstacles during emending is given by the curious story of Message No. 210 SNDNX of 16 July 1941. The key for that specific day was recovered via four combined messages of that day, namely SNDNX (length = 118), ZHRIQ (90), SQOKQ (122), and HCYCW (144). This resulted in a total length of 472 letters. (An odd-looking JN at the end of the last message was initially omitted by the codebreakers, thus reducing its length by two letters. Later it was detected that these letters should read WN.)

The recovered raw decrypts of all four messages showed garbles. In three of them about 10 to 20 were found, but the first message, No. 210 SNDNX, contained even more. Its raw decrypt, as determined by the breaking software, is *Rhrvi gzxia nstep tuenf xkkbo stwae rtsxs agori iexsx qlkax fnauq bvffh gcyvf palte nxwer fermw rsqna qfree gabed ekstr aszex harti ienst eon*. At first, the text is nearly unreadable, though the inspection of the last 14 characters proves the successful break. Success is confirmed by the name, previously known from other decrypts, of Captain (*Hauptstuf*) *Hartjenstein*. After substituting the letter 'j' within his name by 'ii', according to the rules, it is written *Hartiienstein*. His signature can be spotted at the end of the raw decrypt and it provides evidence for a break.

In the next step of emendation, spaces were inserted where they seemed appropriate, and the text could be further emended. ------- - ------- *Fuenf x km x ostwaerts x Sagoriie x Sagoriie x Auf Befehl angehalten x Weitermarsq naq Freigabe der Strasze x Hartiienstein.* (... 5 km east of *Zagorye* stopped as ordered. To proceed after the road has opened. *Hartjenstein*.) But the initial words still remained unreadable and proved very hard to unravel. After lots of speculation and assisted by a special ungarbling tool which utilizes the *HG Nord* text database or alternatively a common German text database, it was finally found out that "*Naqsqubdienste*" (supply services) might be the first word. Compared to the raw decrypt: "*Rhrvigzxianste,*" there are not many similarities apart from five of the last six letters. So the emendation might be called pure speculation. But a very interesting criterion exists that proves the correctness of the decipherment.

The first twenty letters of the ciphertext read SNDNX FKCNE HROSY LCHVE. They directly decipher to the heavily garbled phrase "*Rhrvigzxianstep Tuenf.*" The supposed plaintext reads "*Naqsqubdienste x Fuenf.*" When now re-enciphering this suspected plaintext with the recovered key one gets the ciphertext HENDN XFKCR HROSF ICHVE. Now, a phase shift of both ciphertexts, the original one from the message sheet and the re-enciphered one, can be seen (Fig. 9).

Original ciphertext:	`S NDNXFKC NE HROS YL CHVE`
Presumed ciphertext:	`HE NDNXFKC R HROS FI CHVE`
Original plaintext:	`R hrvigzx ia nste pT uenf`
Presumed plaintext:	`Na qsqubdi e nste xF uenf`

Figure 9. Original and partly shifted message of 16 July 1941.

By simply inserting one letter after the first letter, thus changing S to HE, the resulting shifted ciphertext suddenly produces a meaningful plaintext. This cannot be accidental but provides good evidence supporting the emendation. Presumable a reception error occurred for the first letter S, and the following E, which is only a single dit in Morse, was missed.

None of the samples mentioned above as examples of human errors providing possible reasons for garbles, e.g., reception or Morse errors, are fictional, but each and every one mentioned stem from the SNDNX message of 16 July 1941. The reason for success in breaking such a message with so many garbles is due to the German regulation to encipher all messages of a day with identical keys. SNDNX indeed broke after it had been combined with the three other messages of that day, forming a total ciphertext with a length of 472 letters. If the Germans had decided to use more than one, say four different keys per day, and one had to attack SNDNX as an isolated message, then the breaking attempt would probably have failed. As recently discovered (Weierud, forthcoming), this procedure was indeed introduced by the Wehrmacht more than one year later, in November 1942, when a new variant of DK came into service, called *Nachrichtenschlüssel 42* (Message cipher 42).

7. Conclusion

During the eastern campaign of the German Wehrmacht in 1941, its *Heeresgruppe Nord (HG Nord)* enciphered secret messages for the most part with the Enigma machine, but in some cases with the aid of a manual cipher. As we now know, this cipher was called *Truppenschlüssel* (troop cipher). By good fortune, approximately 600 authentic message sheets of *HG Nord* survived the war and were made available to the authors. After the successful breaks of most of the Enigma ciphertexts, the majority of the 136 manual cipher messages could also be broken. To do so, a cryptanalysis was performed resulting in a modern ciphertext-only breaking tool utilizing the hill climbing technique. The ensuing software was further improved during the project, resulting in an acceleration of the breaking speed by nearly a factor of ten. While the first break initially required about ten minutes, in several re-break experiments, utilizing the latest software version, solution times between ten seconds and two minutes were observed.

The successful breaking of nearly one hundred authentic ciphertexts gives further insight into the habits, tactics, and parlance of the German Wehrmacht during the early phase of their eastern campaign in 1941. The newly recovered plaintexts, and especially the newly detected idiomatic expressions, allow one to extend a previously existing text database specific *HG Nord* and to improve the corresponding statistics. Using these, the ability to break Enigma messages of that time could also be improved.

8. Epilogue

Since the first draft of this article was written in 2016 no further work or cryptanalytical studies have been undertaken. The only exception is a parallel study into Wehrmacht manual cipher systems that one of the authors started in 2020 and which now is in its final stages. This research allowed us to finally identify the manual cipher we have attacked in this article as being the field cipher *Truppenschlüssel* (TS).

In the meanwhile, others, such as Dunin et al (2021), have made further studies and developed new methods for attacking Playfair ciphers that might very well be adapted to attack and solve the remaining unbroken TS messages from Operation Barbarossa. An up-to-date list of the messages is available here: https://cryptocellar.org/bgac/1941-msg-list.html

In total 94 of the 136 TS messages have been broken, of which seven were solved through plaintext-ciphertext compromises. The remaining 42 messages are still unbroken. Their message lengths vary from 14 letters for the shortest message to 152 for the longest with a mean length of 77 letters.

In a recent test with a more modern PC (Intel i9-10900 with ten cores) and the latest version of the software, a rerun of the messages from 7 July 1941 needed only seven seconds until the key was found. The initial break of these messages took almost ten minutes (505 s).

9. Appendix

For illustration and general information, some ciphertexts of *HG Nord* mentioned in this paper, are given in order of appearance, together with the recovered keys (all “normalised,” i.e., with the letter A always at the first position), and the “raw” (not emended) plaintexts.

Ciphertexts	Daily keys	Raw plaintexts
Message No. 218 of 17 July 1941		
TNIDR AONZU CZPKH LGRFB	AXFRH FRHZP	Einshfenfxcmxcxtgran
HPONN EYOIT GSUBG EGHNF	BWONI NUIBV	atennoqniqteingetrof
RUBED PISEB NDGIV ITDQI	PLUES OETXA	fenxzeitpunktunbesti
LKLSP SHEBB ONXPT NBEPS	YMQGT YGQLW	mmtxhartiiensteinxha
HEBBO NXPTN BE	ZKVDC KDSMC	rtiiensteinx
Message No. 64 of 17 September 1941		
FFZNS BQTHN CIQTH NCIXP	ATLMD OLMHZ	Sqarfxplachxplachxis
OLAQT QNZ	CXUYV TUKWA	tzurueqb
	GPSFO PQFSD	
	KIZBW GVBXI	
	NHQRE EYNCR	
Message No. 65/74 of 17 September 1941		
TNDGL XSBYQ CHBHS KYQCH	ATLMD OLMHZ	Ceostufxhenningxhenn
BHSKR CERTI ENRVO HMNPM	CXUYV TUKWA	ingxnaqrxgereateanfo
RFENK QSAYV OHGRI ZFWEN	GPSFO PQFSD	rderungheutebeixober
BHQFA HRWZY CHAHR WZYCH	KIZBW GVBXI	inspxreimannxreimann
THBHP NZHSG PRCKI NZGOR	NHQRE EYNCR	xeingetroffenxkradme
ZSENR KEUZV TPZUW AWPSZ		lderniqtdaxplachxssx
FFZNS B		
	sqarfx	
Message No. 283 of 30 July 1941		
DSCBE SNVYQ ELKAM EWQPA	ASDQR CNEIX	Bestandanxartxmuniti
SQRGR AAQUE LAPQU EKQPD	HPCOZ BSOHZ	onxdleinullxiiulixvi
QKQDW OFRUE FTCIM KUUMK	LUEKX UFRQL	ereinhxnullaqtnullnu
UUQPC AGUAG ZROAA QZRDX	TBVIG TADPK	lluhrxfritzxheinzxgr
ESCTF DQGES ORCAQ DVOPD	YFMNW MVGWY	anatenxpanzerxeinsvi
QMPDQ KRRAQ NURSV DURQR		ewvierxeinsfuemnxcxi
BRWNN GWILA YQQDV OGQVS		zcmgranplxnxeinsnefn
FGREI IFTKZ RSGIQ KFTLK		xaufqplagzuenderlaeq
IDAQN PDQDS YQECH PUKBX		seinssiebenxdohoelzu
FDIQC AQDVO QDVOI LKADS		enderxeinseinsaqtxbe
DHYQP DQKPD QKQLO QZLQK		tonxviervierxroehler
QLOQZ LGK		xroehlnr
Message No. 204 of 14 July 1941		
DFEDL OQAFA MNCCY FLOPD	AKLXO AUKMG	Bitteuzangaoeobbeute
WTQRS FWRPS YYPTS BLCTX	GWBFP IDWBY	betrhwbstoffverwendu
FAZYK ZRFYZ WVVUR WMKUN	NUSYC ZNVOF	ngsfaehigxwenniiakan
VULQP DURVS BWSVW TOTCS	QIRHE RLSCH	nnertellungwiebespro
SZNGZ IHAHC VVLRE BLQPM	ZVTDM QTEPX	qendurqgefueirtwerde
FZRXL TRWLC NTRPG HAQQB		nxhartiiensteixharti
SVVQP DLU		ienstein
Message No. 205 of 14 July 1941		
PZUBV SYWLQ RPERM GWZIA	AKLXO AUKMG	Meldungbereitsabgega
FALC	GWBFP IDWBY	ngen
	NUSYC ZNVOF	
	QIRHE RLSCH	
	ZVTDM QTEPX	

Message No. 206 of 14 July 1941

```
NZIOR MQRKE PGCRS DLSRV         AKLXO AUKMG      Ntpaeqtroszbisherniq
PDPUQ RGCWD FZRXL YGSGQ         GWBFP IDWBY      tevotroffenxhahnlfah
FG                              NUSYC ZNVOF      ny
                                QIRHE RLSCH
                                ZVTDM QTEPX
```

Message No. 210 of 16 July 1941

```
SNDNX FKCNE HROSY LCHVE         APNVY HPVRY      Rhrvigzxiansteptuenf
QQZZU HTLPS ZEDCS TFBEF         CQIUZ NCXKB      xkkbostwaertsxsagori
CRUDM FWQVC UIHWN IVGUN         SDRHK SEDLZ      iexsxqlkaxfnauqbvffh
OURAI NRSOS VIISD EWNQB         TLEGB AOFWT      gcyvfpaltenxwerfermw
EHCIR WQNOR OBOKD RESWA         WXFOM UIGQM      rsqnaqfreegabedekstr
HSCKU PYPOW CRHRO SUU                            aszexhartiiensteon
```

Message No. 215 of 16 July 1941

```
ZHRIQ DRIGF ZTQQN HQGQQ         APNVY HPVRY      Rlnkxlnkxistxkusowxk
NHQGU DWFDC ZMUDC SLLAR         CQIUZ NCXKB      usowxseqsxkmxscedwes
WSUDV WUSHB UDVWU HSBQQ         SDRHK SEDLZ      tlxsagwsyaxsagoskaxk
OFPRH WDTPS WDFIU LAANE         TLEGB AOFWT      eineausfaellexxathia
FYUBA ANVFC                     WXFOM UIGQM      bvmathuhtx
```

Message No. 216 of 16 July 1941

```
SQOKQ NBENY OFYVX UZOCZ         APNVY HPVRY      Dnbefritzheinrichmun
CFVIU HWAQG ILZTE EGCEW         CQIUZ NCXKB      iinxostrowxostrowxsi
CDDFA ROSWD AWVRK BQUZH         SDRHK SEDLZ      qergestelltundzwokrl
UUPRY RKVYC EGAXV FHEXD         TLEGB AOFWT      onnenzurabholungnaqd
QVOWY FYPLW AHDDT SFCST         WXFOM UIGQM      ortinmarsqgssetztxsa
KVNKO SDCDI ZTKVN COIDK                          urzstesxrxsturzbeche
DE                                               rf
```

Message No. 217 of 16 July 1941

```
HCYCW AIHIK CUZCW NOLGD         APNVY HPVRY      Anabtroemeinsbertaxd
CNYPB BUFWR SXVFC HOKEN         CQIUZ NCXKB      iparztxmeldungueberp
WNDAW NAXZT AIRAD RUKAL         SDRHK SEDLZ      ersverlustenyvdemstt
VRPQI KCUED WFDCE WTIAI         TLEGB AOFWT      ndpcmeinsseqsxsieben
GPERD BCUDC IRZKB CCKXF         WXFOM UIGQM      xvdskfinsxfehlzkzeig
FIKYH CDSNP ABVFO FHRNQ                          exzrankeqhgtngeinscb
ARFCE WTIAI QPAIP RDIDH                          estxsiebenxrennerxre
HIJN                                             nnfp
```

Acknowledgments

The authors are deeply grateful to the support of Michael van der Meulen, who gave us access to his collection of authentic German Wehrmacht messages. His noble gift constituted the base of the codebreaking project described. Special thanks go to Bernhard Richt for our always inspiring crypto talks. We are grateful to Philip Marks for his very thorough review of the final draft. We should also like to thank one reviewer who provided valuable comments and help with improving the article.

References

Bauer, F. L. 2013. *Decrypted Secrets: Methods and Maxims of Cryptology.* Berlin: Springer.

Cowan, M. J. 2004. Rasterschlüssel 44 – The epitome of hand field ciphers. *Cryptologia* 28(2): 115–148. doi: 10.1080/0161-110491892827.

Cowan, M. J. 2008. Breaking short Playfair ciphers with the simulated annealing algorithm. *Cryptologia* 32(1): 71–83. doi: 10.1080/01611190701743658.

Currer-Briggs, N. 1993. Army Ultra's poor relations. In *Codebreakers: The Inside Story of Bletchley Park*, edited by F. H. Hinsley and Alan Stripp, 209–230. Oxford: Oxford University Press.

David, C. 1996. A World War II German army field cipher and how we broke it. *Cryptologia* 20(1): 55–76. doi: 10.1080/0161-119691884780.

Deavours, C. A. 1977. Unicity points in cryptanalysis. *Cryptologia* 1(1): 46–68. doi: 10.1080/0161-117791832797.

Dunin, E., M. Ekhall, K. Hamidullin, N. Kopal, G. Lasry, and K. Schmeh. 2021. How we set new world records in breaking Playfair ciphertexts. *Cryptologia*. doi: 10.1080/01611194.2021.1905734. Published online: 13 Aug 2021.

Fouché Gaines, H. 1956. *Cryptanalysis: A Study of Ciphers and Their Solution*, New York: Dover Publications.

Hamer, D. H., G. Sullivan, and F. Weierud. 1998. Enigma variations: An extended family of machines. *Cryptologia* 22(3): 211–229. Accessed October 6, 2021. doi: 10.1080/0161-119891886885. http://cryptocellar.org/pubs/enigvar.pdf

Meulen, van der, M. 1995a. Werftschlüssel – A German navy hand cipher system Part I. *Cryptologia* 19(4): 349–364. doi: 10.1080/0161-119591884006.

Meulen, van der, M. 1996. Werftschlüssel – A German navy hand cipher cystem Part II. *Cryptologia* 20(1): 37–54. doi: 10.1080/0161-119691884771.

Meulen, van der, M. 1995b. The book cipher system of the Wehrmacht. *Cryptologia* 19(3): 247–260. doi: 10.1080/0161-119591883926.

Menezes, A. J., P. C. van Oorschot, and S. A. Vanstone 1996. *Handbook of Applied Cryptography*. Boca Raton: CRC Press.

Morris, C. 1993. Navy Ultra's poor relations. In *Codebreakers: The Inside Story of Bletchley Park*, edited by F. H. Hinsley and Alan Stripp, 231–245. Oxford: Oxford University Press.

OKH (Oberkommando des Heeres). 1940. *Schlüsselanleitung zum Doppelkastenschlüssel*, Entwurf. Bestand Rückgabe TICOM, S8: T-16. Politisches Archiv des Auswärtigen Amts, Berlin. Accessed October 6, 2021. https://cryptocellar.org/wmc/schluesselanleitung-dk-1940.pdf

OKW (Oberkommando der Wehrmacht). 1941. *Vorläufige Schlüsselanleitung zum Doppelkastenschlüssel*, M.Dv. Nr. 158. RG 457, Entry A1 9032, Box 7, NR. 57. NARA, College Park, MD. Accessed October 6, 2021. https://cryptocellar.org/wmc/schluesselanleitung-dk-1941.pdf

Ostwald, O. and F. Weierud. 2017. Modern breaking of Enigma ciphertexts. *Cryptologia* 41(5): 395–421. 10.1080/01611194.2016.1238423. Accessed October 6, 2021. https://cryptocellar.org/pubs/enigma-modern-breaking.pdf

Schick, J. S. 1987. With the 849th SIS – 1942–45. *Cryptologia* 11(1): 29–39. doi: 10.1080/0161-118791861767.

Sebag-Montefiore, H. 2000. *Enigma: The Battle for the Code.* London: Weidenfeld & Nicolson.

Shannon, C. E. 1949. Communication theory of secrecy systems, *Bell System Technical Journal*, 28 (Oct):656–715. Accessed October 6, 2021. http://pages.cs.wisc.edu/~rist/642-spring-2014/shannon-secrecy.pdf

SIS (Signal Intelligence Service). 1943. Double Playfair System. RG 457, Entry A1 9032, Box 1299, NR. 3890. NARA, College Park, MD.

Sullivan, G. and F. Weierud. 2005. Breaking German army ciphers. *Cryptologia* 29(3): 193–232. Accessed February 14, 2021. doi: 10.1080/01611190508951299. https://cryptocellar.org/pubs/bgac.pdf.

USAIS (US Army Intelligence School). 1990. "Chapter 7: Solution of polygraphic substitution systems," in *Basic Cryptanalysis*, Field Manual No. 34-40-2. Washington DC: US Government Printing Office. Accessed February 14, 2021. http://www.contestcen.com/ArmyFieldManual.pdf.

Weierud, F. Forthcoming. The development of Wehrmacht manual ciphers, 1936–1945. *Cryptologia*.

Welchman, G. 1982. *The Hut Six Story: Breaking the Enigma Codes.* London: Allen Lane.