German Spy Ciphers of World War II

Mediocre Encryption Methods Developed by Amateurish Intelligence Agencies

Klaus Schmeh

Independent Scholar, klaus@schmeh.org

Abstract. As espionage played a major role in World War II, spy ciphers were in wide use. Creating ciphers for agents operating in hostile environments was a major challenge. On the one hand, spies required easy-to-use and secure encryption methods; on the other hand, working with cipher equipment was usually prohibitive due to the suspision it might have risen. In addition, a spy cipher had to be much more individual and adapted to the needs of a particular user than, say, a military encryption system. This paper will focus on German spy ciphers in World War II. As will be shown, the German secret services used at least 25 different spy ciphers during WW2. The quality of these encryption methods was, at best, mediocre. A major problem was that the German intelligence and cryptology efforts were spread to several organisations not cooperating with each other. This paper confirms that neither cryptology nor intelligence work in the Third Reich reached the highest level.

Key words: spy cipher, Enigma, David Kahn, crossword encryption, columnar transposition, dictionary code, steganography, cipher disc

1 Introduction

The standard work on intelligence history of the Third Reich is David Kahn's book *Hitler's Spies* (Kahn 2000). Kahn, who is also considered the world's leading expert on crypto history, writes that he originally thought that Hitler's secret services were as good as his army, which was regarded the best in the world. However, during research for his book, Kahn more and more realized that intelligence work under Hitler was quite amateurish and poorly organized. Apart from the Abwehr, Germany's most important intelligence organisation, several other secret services were involved in espionage. The existence of different authorities, which were not cooperating and even competing with each other, considerably weakened German intelligence efforts. All in all, David Kahn rates Hitlers spies as not very successful.

While the history of spies in the Third Reich is well researched since Kahn's book, no systematic treatise of the ciphers these spies used has ever been published in the scientific community. This paper is a first attempt to change this. Based on information provided in books, research articles and archive material, the author has compiled a list of about 25 German spy ciphers. A few of them will be described in detail in this publication. The remaining ones will be listed, along

with references leading to more comprehensive information about them. Virtually all sources the author has found about German spy ciphers describe these methods from an enemy's point of view (usually the sources are British or American). It should be a target of future research to find material of German origin.

Developing ciphers for agents operating in a hostile environment was, of course, different from usual cipher design. Spies required easy-to-use, unconspicious and secure encryption methods. The use of cipher machines or crypto devices was usually prohibitive due to the suspision this equipment might have risen. Even with today's crypto knowledge it is hard, if not impossible, to develop a cipher that would have worked especially well under these conditions. Things were complicated further by the fact that many spy ciphers had to be adjusted to the individual needs of a certain user. For instance, a codebook had to contain the vocabulary the spy in question was expected to use and, of course, it had to be written in a language the spy understood.

2 A Columnar Transposition Based on a Crossword Puzzle

Let's now look at a first example. In the Friedman Collection (Friedman undated) a German WW2 spy cipher using a crossword puzzle as key is described. Like all other encryption methods covered in this paper, this one is only known from descriptions created by enemy specialists (in this case by US cryptologists). We therefore don't know which German intelligence organisation developed this cipher and what the design criteria were. The cipher was introduced in 1936. It is a simple columnar transposition.

To use this cipher one needs a book containing several crossword puzzles and several text pages. An ordinary puzzle magazine taken from a newspaper stand will do. Both sender and receiver need a copy of this book. The sender takes a crossword puzzle (say, the one on page 4) from the book and writes his message (say, ENGLAND MUST CONCENTRATE AL FORCES TO WIN THE WAR) into the white boxes. Black boxes are filled with meaningless letters (nulls):

Now the sender chooses a text page (say, page 12) and notes the initials of the first 18 words. These letters are numbered according to their position in the alphabet:

G R E C V V A N G H M I L R B N F I
6 15 4 3 17 18 1 13 7 8 12 9 11 16 2 14 5 10

Now the content of the crossword is read out column-wise (including the nulls in the black boxes). The column corresponding with letter number 1 is taken first, then the column corresponding with letter number 2 and so on. Here's the result:

NETOC LCWGR GCFEN TMLHU DETEA
ESBOR SFWDA HNENT OCRAA IATN.

The encipherer sends this ciphertext to the recipient, along with the information that the crossword puzzle was taken from page 4 and the text from page 12. With this information (and wih the book) the recipient can decrypt the message.

It goes without saying that this method is not very secure. A skilled cryptanalyst can certainly break it without knowing the crossword puzzle and the text used as key.

3 A Columnar Transposition

The next cipher was used by German agents in Mexico, Brazil, and Chile (Bratzel, Rout 1989; p. 135, Kahn 1996, p. 629). It is again a rather weak columnar transposition. The Nazis supplied this system until spring 1941.

T	S	E	I	N	C	T	L	A	T	E	U	I	D	U	I	T	V	R	L
14	13	4	6	11	2	15	9	1	16	5	18	7	3	19	8	17	20	12	10
L	E	A	R	N	E	D	X	N	A	M	E	X	D	E	S	T	R	O	Y
E	R	X	G	R	E	E	N	E	X	N	U	M	B	E	R	X	A	V	D
X	T	H	I	R	T	E	E	N	X	D	A	M	A	G	E	D	X	T	H
R	E	E	X	W	E	E	K	S	X	A	G	O	X	I	N	X	V	I	C
I	N	I	T	Y	X	W	H	E	R	E	X	N	O	R	W	E	G	I	A
N	X	S	T	E	A	M	E	R	X	W	A	S	X	T	O	R	P	E	D
O	E	D	X	A	T	X	S	A	M	E	X	T	I	M	E	X	D	E	S
T	R	O	Y	E	R	X	D	A	M	A	G	E	D	X	O	N	X	S	T
E	R	N	X	A	N	D	X	D	I	E	S	E	L	X	E	N	G	I	N
E	X	W	I	L	L	X	B	E	X	R	E	A	D	Y	X	I	N	X	T
W	O	X	W	E	E	K	S	X	X										

Fig. 1. Josef Starziczny, a German spy operating in Brazil, used a simple columnar transposition.

One of the spies using this system was Josef Starziczny, the leader of the German spy network in Brazil. Prior to leaving Germany, Starziczny was handed a copy of the book *No Antro da Vida* to use as the key to encipher his radio messages exchanged with the Abwehr post in Hamburg. The following cleartext is an Englsh translation of an original message Starziczny encrypted:

```
LEARNED NAME DESTROYER GRENE NUMBER AVD THIRTEEN DAMAGED THREE
WEEKS AGO IN VICINITY WHERE NORWEGIOAN STEAMER WAS TORPEDOED AT
SAME TIME DESTROYER DAMAGED ON STERN AND DIESEL ENGINE WILL BE
READY IN TWO WEEKS.
```

The first enciphering step was to find the page in the book from which he would take the key letters. Starziczny determined this by multiplying the number of the month (January=1, February=2, ...) by 8 and adding 20, and then adding the day of the month. For the February 24 message given below, the page number was 60, from (2 x 8) + 20 + 24. On this page he noted the first letter of each of the first 20 text lines. He then numbered these letters in their alphabetical order. Under this key he wrote his message horizontally, with words divided by X's (see Fig. 1). He received the following ciphertext by reading out the letters columwise in the order of the column numbers:

```
NENSE RAADE XEETE XATRN LEDBA XOXID LDAXH EISDO NWXMN DAEWE AERRG
IXTTX YXIWX MMONS TEEAS RENWO EOEXX NEKHE SDXBS YDHCA DSTNT NRRWY
EAEAL EOVTI IEESI XERTE NXERR XOLEX RINOT EEWDE EEWMX XDXKA XXXRX
MMIXX TXDXE RXNNI EUAGX AXGSE EEGIR TMXXY RAXVG PDXGN.
```

It is clear that this columnar transposition was far from unbreakable at the time it was used.

4 A Dictionary Code

The telegram shown in Fig. 2 (today kept by the British National Archive) was sent by a German businessman named Ottomar Müller from Buenos Aires, Argentina, to a company named NLT Technico in Hamburg, Germany (Censorship Manual 1944, p. 65).

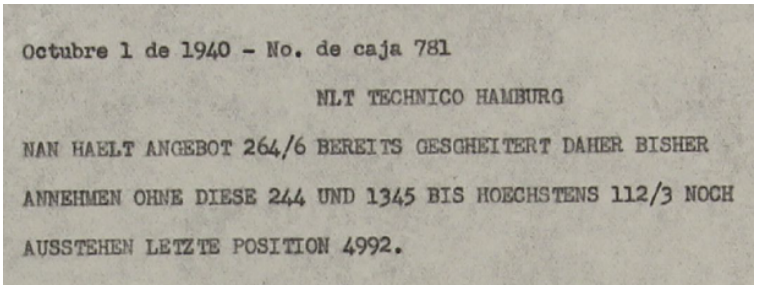

Fig. 2. This telegram was sent by German spy Ottomar Müller from Buenos Aires to Hamburg.

Here's the English translation of the telegram:

```
NLT TECHNICO, HAMBURG, OCTOBER 1, 1940
NAN HOLDS THAT OFFER 264/6 ALREADY FALLEN THROUGH, THEREFORE
UP UNTIL NOW ASSUME THAT WITHOUT THIS, 244 AND 1345 STILL
OUTSTANDING UNTIL AT LATEST 112/3. LAST POSITION 4992.
```

This telegram has the appearance of a commercial note. It contains several code numbers, which was quite common for a business telegram of the time. The meanings of the code numbers were listed in a codebook.

According to (McGaha 2009), Ottomar Müller was hired in 1940 by the Hamburg-based company Schmitt & Co., which operated as a cover organisation for the Abwehr. NLT Technico probably was a codename of this company. Müllers task was to provide reports on British ships entering and leaving Buenos Aires.

The telegram was forwarded to British crypto experts, who recognized that it was a spy message. The two code numbers containing a slash were derived from a German-English dictionary (e.g., 264/6 means page 264, word number 6). Using this dictionary the cryptanalysts found out that 264/6 stands for pier and 112/3 for December. The meanings of the numbers 244, 1345 and 4992 are unknown. They might refer to ships.

Possibly, the secret message only consists of the five code numbers, while the rest of the telegram is meaningless. If this is correct, the message reads "Pier 244 1345 December 4992" – whatever this means.

5 A Steganographic Code

The next method, the so-called Westerlinck Code, ist steganographic in nature (Censorship Manual 1944, pp. 94, 104). It can be used to hide an arbitrary message in an arbitraty cover text. For this method it is important to distinguish whether a certain word has one (1), two (2) or more than two (3) syllables. The cover text is devided into groups of three words with every group being interpreted as a three-digit number. For instance, the word group SNOW IN NOVEMBER stands for 113, while the words WEATHER IS NICE represent the number 211. As is obvious, 27 different numbers (111 to 333) can be coded this way.

Each three-digit number is identified with a letter of the alphabet. In Fig. 3 the following scheme is used: A=122, B=131, C=?, D=132, E=133, F=?, G=?, H=?, I=212, J=?, K=?, L=213, M=?, N=113, O=112, P=?, Q=?, R=311, S=312, T=313, U=311, V=323, W=?, X=?, Y=?, Z=332. The hidden message shown is LONDON TOUT BIEN ATTENDEZ AUTRES NOUVELLES.

It is clear that a message written in the Westerlink Code is hard to detect. However, coding a message is time-consuming, which makes this method only suitable for short texts.

6 A Cipher Disk

A number of German spies who were sent to England between September 1940 and January 1941 were equipped with cipher discs to encrypt their radio transmissions back to Germany (Jakobs 2014). One of theses spies was WW1 veteran Josef Jakobs (1898-1941). His cipher disc was numbered 9. Two other discs of the same kind confiscated from German spies bore numbers 6 and 7.

In April of 1941, a dead man was found in a public air raid shelter in Cambridge. He had committed suicide. He was identified as Jan Willem Ter Braak

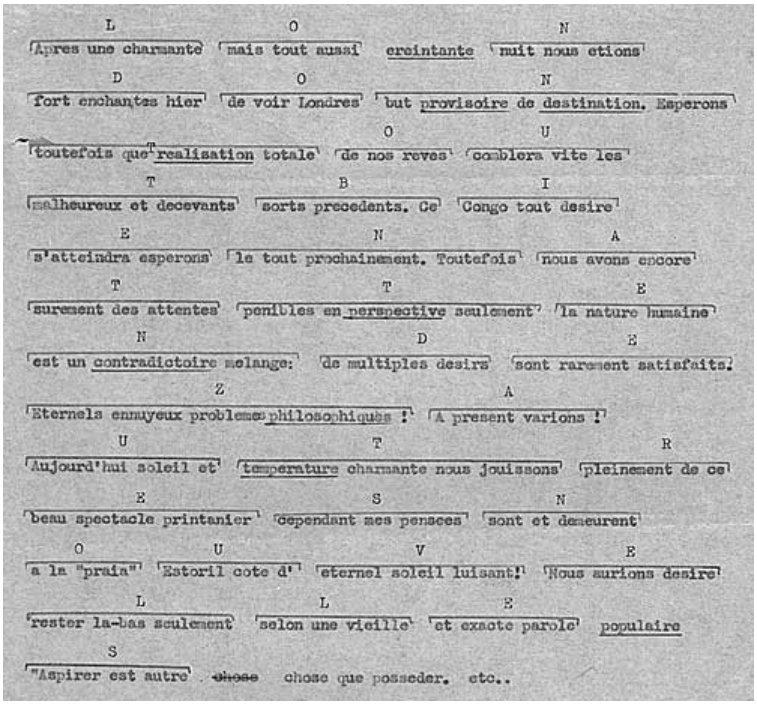

Fig. 3. This letter contains a hidden spy message coded in the Westerlinck Code.

(real name Engelbertus Fukken), who had lived as a German spy in Cambridge for several months. Having run out of funds and with no fresh supply from Germany, Fukken decided to shoot himself. It is quite likely that he had used cipher disc number 8.

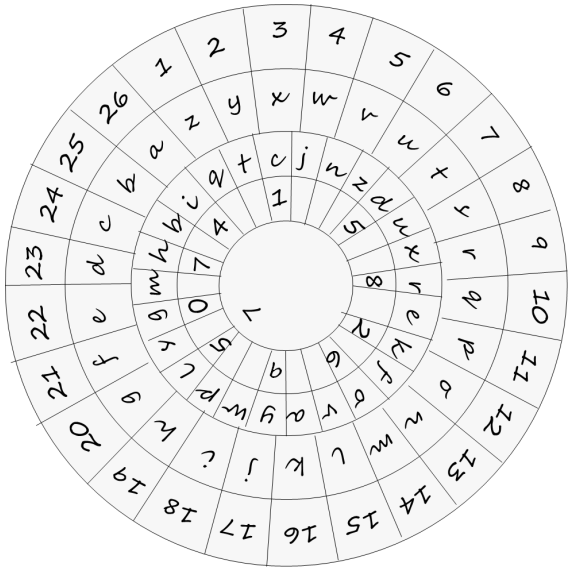

Fig. 4. Cipher discs of this kind were used by German spies in England. It is not known how exactly such a disc was to be used.

Cipher disc number 7 is shown in Fig. 4. It is not known how exactly it was to be used.

7 An Unknown Cipher

As David Kahn reports in his book *Hitlers Spies*, the Abwehr recruited a spy code-named "Koehler" in New York City. This Koehler might be identical with Nazi spy Walter Koehler, who is described in an online article published in 2016 (Johnson 2016). Apparently, David Kahn was not aware of this person, when he wrote his book.

Already in 1981, David Kahn had published five encrypted messages written by Koehler in the scientific magazine, *Cryptologia* (Kahn 1981). Koehler sent these messages to his contact person at the Abwehr in February 1944. David Kahns publication is not based on Koehlers original messages, but on a letter quoting these kept by the British National Archive in London. Here it is (the numbers indicate the length of the respective message):

```
An
```

```
Abwehrleitstelle Frankreich
Paris Funkstelle
Sofort vorlegen!
Betr.: Koehler

237
Ybtat mqfvo dvbis prito kecqg kokik kyiwm zuarj
alyia qtxvi vxzya szgou skiqn rbqjq mogex ezdnf
vusda zurop ixklo cmnbl grdhz swmch kupef pzlej
hbord wkkhu vthjk sfwda jepmu izvig kzlau rdrxx
mdecs spozv eeeod dlmdz nqmia pidwg xdcyy mvkso
hmmii impwq nkipa mljvm sqsbb glevn sktlq tn.

178
Eekao parwo xiavy pejux lhnjh pbqdd vdvxb mdiia
gwwmn zbivm abuws dwoug djozl ylaug loaea ilihj
swjft oetad tjisn avaqn sodwb wzaxe zvoxg xpgzv
adurm shvxx xfmuq pdpvq dqwtu fryok xfvcp ydzwm
ofwfl uzfne qsslo evl.

137
tziqb lqqxs kinod mbvil sukms syarh mhzvp tvswm
ayddg rixyy omfzm ugfzz aznqe ljuyi ygwuo qmdbi
vcxgz rmzno pessh gpoyx qqlei xmaoj buugz czfdl
yzmkp gsmfm dteze oxmos.

140
dmxkb kqnvh zzeek beoop ygcca yvepv tykmt iykfl zkacv
uxiyd kruwy vnjvp xyeqp jpmfo abzpt mjtdy zvzky bjgze
vdtyd zeejw zumjp ivsna gsmzq dltxb qjqqj fnpta mqted
skijj.

229
fpoxa tijyp qrerq znqst zasnk zarvq hhsmw vlhfg pyhqc
yuirf fsgoi twgdg sbphc fkfza bpegh jzujn wtsxp ijamg
tzdto hxzdn uivww tizoc axkye lhmdn sfzjo omrhb zpith
hklsf anvdr ynhqk syrgi ltxos wabom dzwlb byava sjomn
qqszs adddu greao alhon lxzgi iwpnf uzgui jgmya ksqfw
zsjl.
```

In spite of two blog posts the author of this work has published asking his readers for help (Schmeh 2017; Schmeh 2013), the solution of these cryptograms is still unknown. However, as German spy ciphers of WW2 were not the best, there is still a good chance to break the Koehler cryptograms.

8 Other German Spy Ciphers

There are many more spy ciphers used by the Germans in World War II. The following list contains all the ones the author of this work is aware of:

- A German spy captured in the UK used a steganographic code that would hide a message in a love letter (Censorship Manual 1944, p. 19).
- The same spy used a dictionary code (Censorship Manual 1944, p. 22).
- A German agent named Janssens used a steganographic method to hide a message in a letter (Censorship Manual 1944, p. 59).
- A German secret service used a substitution cipher for messages sent by spies from the USA to German contact persons in Spain (Censorship Manual 1944, p. 67).
- For the same purpose a code based on a codebook was used (Censorship Manual 1944, p. 68).
- A German spy in Angola used a codebook containing Spanish codewords, which made a cipher message look like a Spanish text (Censorship Manual 1944, p. 72, Schmeh 2016).
- German spies in the Middle East used an encryption method based on a cipher slide (Censorship Manual 1944, p. 86).
- The same spies made use of a similar method in order to encrypt letters sent by mail (Censorship Manual 1944, p. 87).
- Another steganographic spy method was used by the Germans (Censorship Manual 1944, p. 89).
- Another German spy is cipher based on marked letters in a hand-written text (Censorship Manual 1944, p. 93).
- A similar method is mentioned in the same source (Censorship Manual 1944, p. 96).
- A German spy in Southern Spain used a simple cipher named CCG (Hinsley, Stripp 1993).
- German agents in Europe and Africa used the so-called ABC key (Mowry 1989, p. 15).
- The same source reports on a simple encryption method named Procedure 40 (Mowry 1989, p. 17).
- The same source reports on another spy cipher named Procedure 62 (Mowry 1989, p. 17).
- German spies in Brazil used a cipher based on a book and a grille (Bratzel, Rout 1989, p. 135).
- German spy Werner Walthemat, who was captured in Rio de Janeiro before he became active, used a simple transposition cipher named Comb Code (Bratzel, Rout 1989, p. 137).
- German spy Guillermo Kunsemueller, who operated in Chile, used a cipher based on a book and a cipher slide (Bratzel, Rout 1989, p. 138).
- German spy Kurt Frederick Ludwig used a codebook especially designed for him (NYT 1942).

9 Conclusion and Outlook

As the previous chapters have shown, German intelligence organisations developed very different spy ciphers in World War II. Some of these methods are cryptographic, others steganographic in nature. The cryptographic methods described in this paper are mediocre, at best. The steganographic techniques used by German spies were certainly harder to break, but they were not suited for longer messages.

All in all, this paper confirms two well-known facts. First, German cryptology in WW2 was not the best (otherwise the Allies would not have been capable of breaking the Enigma and the Lorenz machine). Second, German intelligence work in WW2 was not the best (as stated by David Kahn in his book about Hitler's spies).

This paper, which needs to be limited to ten pages, is of course only a first view on German spy ciphers in WW2. Future research should go into more detail about the ciphers described here and try to find more encryption methods used by German spies in WW2. In addition, German sources for these ciphers should be found, in order to better understand their origin and the motivation of their developers. And finally, WW2 spy ciphers from other countries should be researched, as well. The author hopes that this paper will stimulate further research into these topics.

10 Acknowledgments

The author would like to thank Max Baertl and Thomas Bosbach, whose comments on the blog *Klausis Krypto Kolumne* provided helpful input for this paper.

References

Anonymous *The National Archives' reference KV-2-2424.* (1944)

Anonymous *A Life Torn to Shreds.* http://www.josefjakobs.info/2014/11/a-life-torn-to-shreds.html (2014)

Anonymous *FBI Photographer Bares Spy Secrets.* New York Times, February 12 (1942)

Bratzel, J. F.; Rout, L. *Abwehr Ciphers in Latin America.* Cryptologia 1983/2, p. 135 (1989)

Friedman, W. *The method of encipherment according to the crossword puzzle system used by the nazi intelligence service.* William Friedman Collection A69065 (undated)

Hinsley, F. H.; Stripp, A. *Codebreakers. The Inside Story of Bletchley Park.* Oxford University Press, Oxford (1993)

Johnson, D. A. *Walter Koehler & J. Edgar Hoover.* http://warfarehistorynetwork.com/daily/wwii/walter-koehler-j-edgar-hoover/ (2016)

Kahn, D.: *German Spy Cryptograms.* Cryptologia 1981/2, p. 65 (1981)

Kahn, D.: *Hitler's Spies.* Da Capo Press, Boston (2000)

Kahn, D.: *The Codebreakers.* Scribner, New York (1996)

McGaha, R. L. *The Politics of Espionage.* Dissertation at the College of Arts and Sciences of Ohio University, Columbus, p. 185 (2009)

Mowry, D. P. *The Cryptology of the German Intelligence Services.* NSA, Fort Meade, p. 15 (1989)

Schmeh, K. *An unusual cipher from a WW2 intelligence officer.* http://scienceblogs.de/klausis-krypto-kolumne/2016/12/13/an-unusual-cipher-from-a-ww2-intelligence-officer/ (2016)

Schmeh, K. *The Top 50 unsolved encrypted messages: 47. Encrypted messages of a Nazi spy.* http://scienceblogs.de/klausis-krypto-kolumne/2017/02/19/the-top-50-unsolved-encrypted-messages-47-encrypted-messages-of-a-nazi-spy/ (2017)

Schmeh, K. *Top-25 der ungelösten Verschlüsselungen Platz 16: Verschlüsselte Botschaften eines Nazi-Spions.* http://scienceblogs.de/klausis-krypto-kolumne/2013/07/05/top-25-der-ungelosten-verschlusselungen-platz-16-verschlusselte-botschaften-eines-nazi-spions/ (2013)