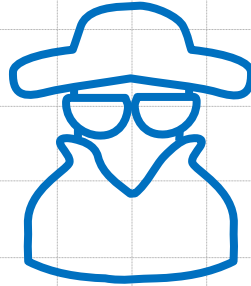# German Spy Ciphers in World War II

Euro HCC Bratislava, 2017
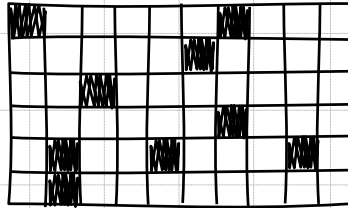
Klaus Schmeh
www.schmeh.org

Encryption based on a crossword puzzle

Cleartext
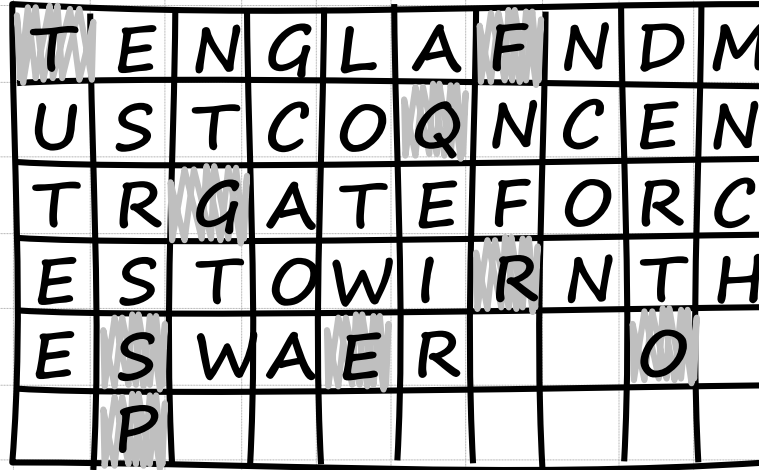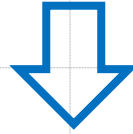ENGLAND MUST CONCENTRATE FORCES TO WIN THE WAR

Crossword puzzle

Key word
EMBANKMENT

ENGLAND MUST CONCENTRATE FORCES TO WIN THE WAR

T	E	N	G	L	A	F	N	D	M
U	S	T	C	O	Q	N	C	E	N
T	R	G	A	T	E	F	O	R	C
E	S	T	O	W	I	R	N	T	H
E	S	W	A	E	R			O	
	P								

EMBANKMENT

T	E	N	G	L	A	F	N	D	M
U	S	T	C	O	Q	N	C	E	N
T	R	G	A	T	E	F	O	R	C
E	S	T	O	W	I	R	N	T	H
E	S	W	A	E	R			O	
	P								

EMBANKMENT

T	E	N	G	L	A	F	N	D	M
U	S	T	C	O	Q	N	C	E	N
T	R	G	A	T	E	F	O	R	C
E	S	T	O	W	I	R	N	T	H
E	S	W	A	E	R			O	
	P								

ABEEKMMN NT

G	N	T	N	A	E	F	L	D	M
C	T	U	C	Q	S	N	O	E	N
A	G	T	O	E	R	F	T	R	C
O	T	E	N	I	S	R	W	T	H
A		E			S		E	O	
					P				

GCAOA NTGTW TUTEE NCONA QEIRE SRSSP
FNFRL OTWED ERTOM NCH

Encryption based on a crossword puzzle
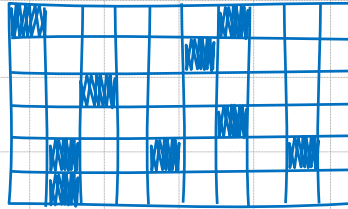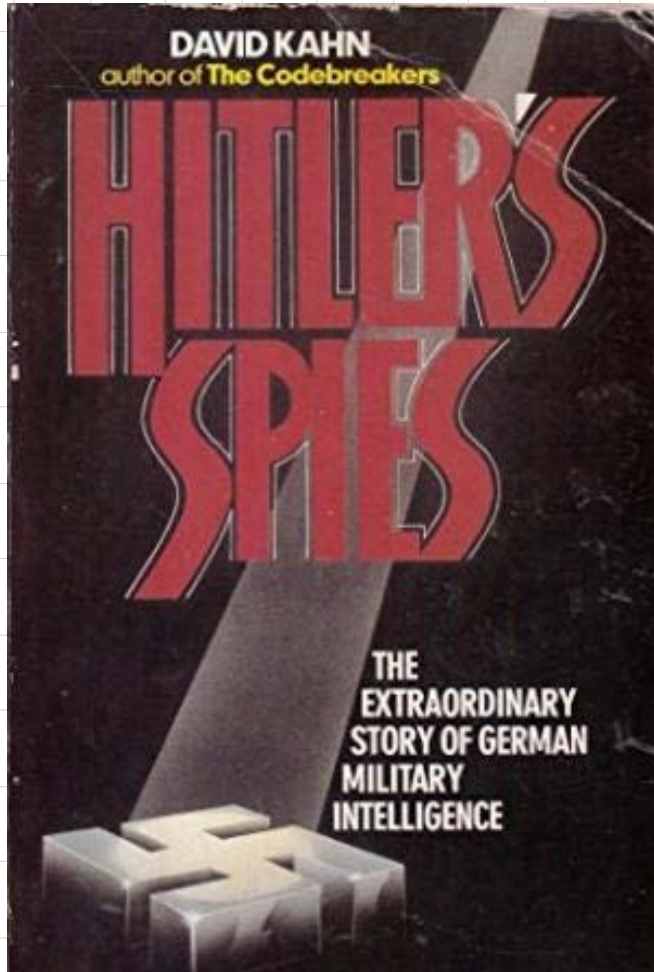

Used by German spies from 1936 on.

Source: Friedman Collection

Details are not known.
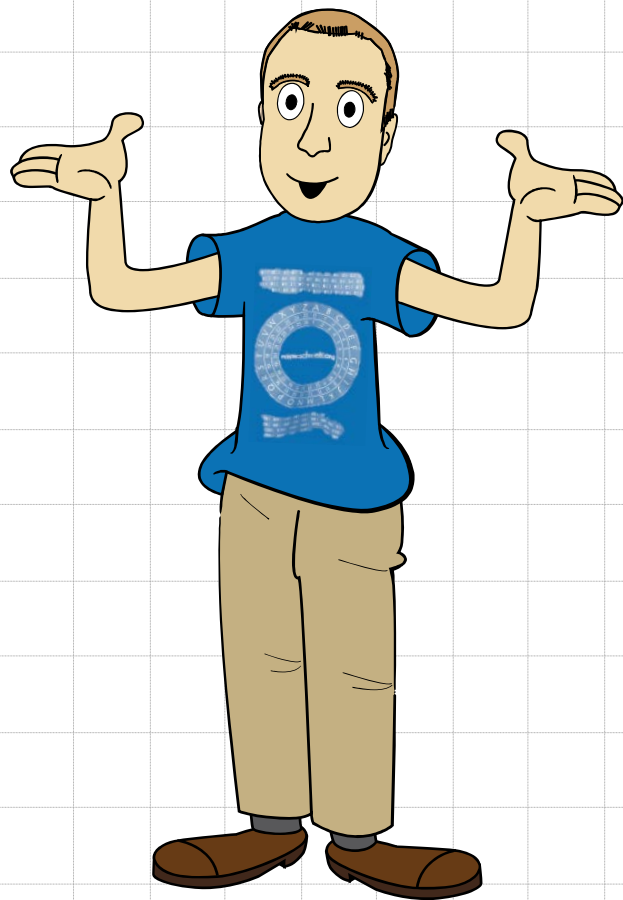
Klaus Schmeh

Cryptology Consultant

Journalist

Blogger

www.schmeh.org

DAVID KAHN
author of **The Codebreakers**

HITLER'S SPIES

THE EXTRAORDINARY STORY OF GERMAN MILITARY INTELLIGENCE

Germany took great effort in espionage in WW2 ...

... but was not very successful

One reason: Germany had several intelligence agencies, which did not cooperate
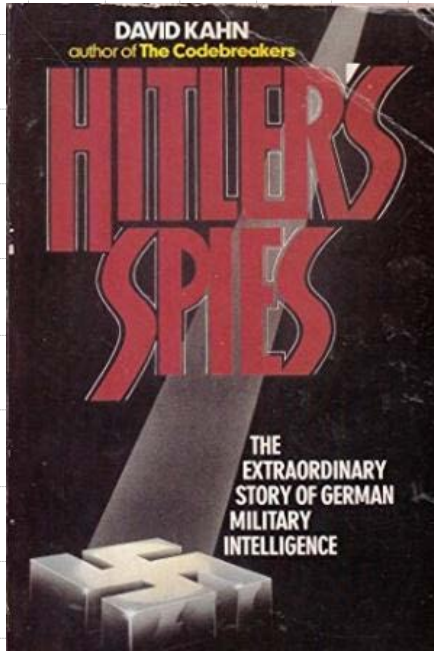
German espionage is now well researched

However, little is known about German spy ciphers

This presentation focusses on German spy ciphers

My sources

Crypto history literature

British National Archives

Bundesarchiv

Friedman Collection

Cryptologia

NSA publications

All sources I found refer to enemy descriptions of the methods

What I found

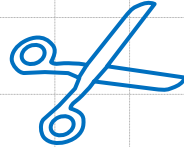About 25 German WW2 spy ciphers
But there must be more

Spy Cipher Requirements
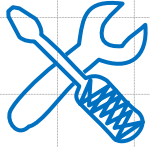
secure and
easy to use
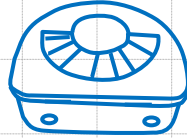
machines and devices
prohibitive

tailored to the
spy's need

Spy cipher design is ...

- different from other codemaking

- difficult

Two Approaches

cryptographic
codes

steganographic
codes
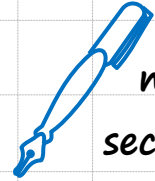
microdot
secret ink

technical
steganography

out of scope

We have seen a
cryptographic code
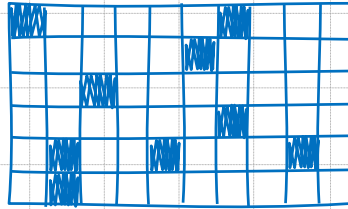
Let's now look at a
steganographic one

Westerlinck Code

Every word stands for a number:

- 1 sylable: 1
- 2 sylables: 2
- 3 or more sylables: 3

SNOW IN NOVEMBER: 113

WEATHER IS NICE: 211

Westerlinck Code

A=122
B=131
C=111
D=132
E=133
F=211
G=333
H=113
I=212
J=121
K=122
L=213
M=123

N=113
O=112
P=211
Q=221
R=311
S=312
T=313
U=311
V=323
W=222
X=223
Y=231
Z=332

SNOW IN NOVEMBER: 113=N

WEATHER IS NICE: 211=P

Westerlinck Code

LONDON TOUT BIEN
ATTENDEZ AUTRES
NOUVELLES


Everything okay in
London, wait for
other news.

Codebook

mentioned in a British censorship manual

Octubre 1 de 1940 – No. de caja 781

NLT TECHNICO HAMBURG

NAN HAELT ANGEBOT 264/6 BEREITS GESCHEITERT DAHER BISHER

ANNEHMEN OHNE DIESE 244 UND 1345 BIS HOECHSTENS 112/3 NOCH

AUSSTEHEN LETZTE POSITION 4992.

Sent by German businessman Ottomar Müller
from Buenos Aires to NLT Technico in Hamburg

Codebook
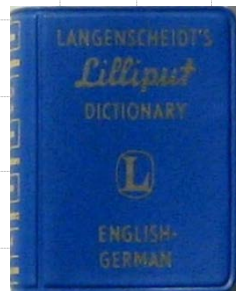
Octubre 1 de 1940 — No. de caja 781

NLT TECHNICO HAMBURG

NAN HAELT ANGEBOT 264/6 BEREITS GESCHEITERT DAHER BISHER

ANNEHMEN OHNE DIESE 244 UND 1345 BIS HOECHSTENS 112/3 NOCH

AUSSTEHEN LETZTE POSITION 4992.

From a German-English dictionary:

264/6 (page 264, word 6): pier

112/3 (page 112, word 3): December

unknown codebook

Another Codebook

Used by a German spy in Angola

Angola

During WW2
Portuguese colony

Portugal: neutral in
WW2, but involved in
trade with military
goods

British military expressions (gun, tank, troup, …)

Spanish code words

Divisions	mercadoria (merchandise)
Concentrations	necessidade
Camps	barris
Garrison	pedido
General Staff	embalagem, lata
	(packing, tin)
French type, Frenchman	desejo, podendo
American type, American	tem pressa, recolho
English type, Englishman	diga-me (tell me)
Like the other Allies	favor, favores
South African	disponivel (disposable)
Portuguese	impossivel (impossible)
Munition dump	ensejo, oportunidade
Rifles	pastilhas
Highway	interessante
Railway line	comprimidos, boa, bom
Water ways, canals	preco?, condicao
Airways	garantia, conveniencia
?Frontier	espécies, pacote

Types of Planes

Martin	remessa (remittance)
Flying Fortress	pimenta
Consolidated	Franco Belga
Hurricane	Portuguese escudos
Spitfire	Angolares
Boston Bomber	Madeira
Wellington Bomber	vinho branco (white wine)
Douglas	vinho tinto (red wine)
Recent model	preto, novo (black, new)
Old model	branco, velho (white, old)
Factories	azeite (oil)
General	milho (maize)
Admiral	trigo (corn, wheat)
Colonel	azeitonas (olives)
Repair aerodromes	entrega
Aerodromes	encargo (charge, duty)
The enemy's intentions	vontade (will, desire)

47 6( )

The strength of the military forces will be denoted by the word TONELADA (Ton). Each ton represents 1,000 men; 10,000 men - 10 tons, 5,000 men - 5 tons, half a ton - 500 men.

Guns will be denoted by the word QUILO (Kilo), each 200k. represents one piece, i.e. 18 guns - 3,600k.

Anti-aircraft guns will be denoted by the words METROS DE FASENDA (Metres of material), each metre represents one piece or each 4 metres one battery, i.e. 3 anti-aircraft guns - 3 metres of material; 4 batteries - 12 metres of material.

Machine-guns will be denoted by the word GARRAFA (bottle), each bottle represents a machine-gun. i.e. 8 machine-guns - 8 bottles.

Aeroplanes will be denoted by the words TUBOS (pipes) and FRASCOS (flagons); each pipe a bomber and each flagon a fighter, i.e. 50 fighters and 20 bombers - 50 flagons and 20 pipes. Transport planes will be denoted by the words GRANDES TUBOS (big pipes) and reconnaissance planes by the word GRANDES (big ones).

The following words will be denoted by a word which ends with these suffixes:-

Fortifications still under construction   ardo   ardos
Fortifications built   aixa   aixo
                                            aixas

North West   iga
South West   ar
Northern
From the North of)
To the North   )   esse
Meridional   )
From the South of)   encia
To the South   )

PIMENTA UTO IAS

Flying fortress arrived
[at] destination.

Cipher disk
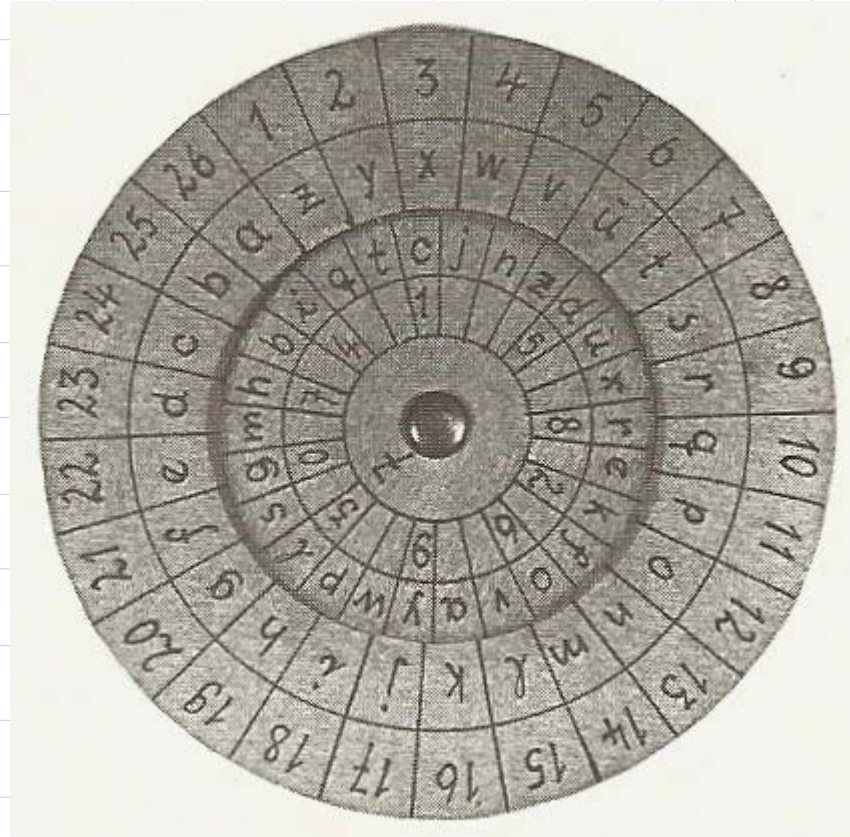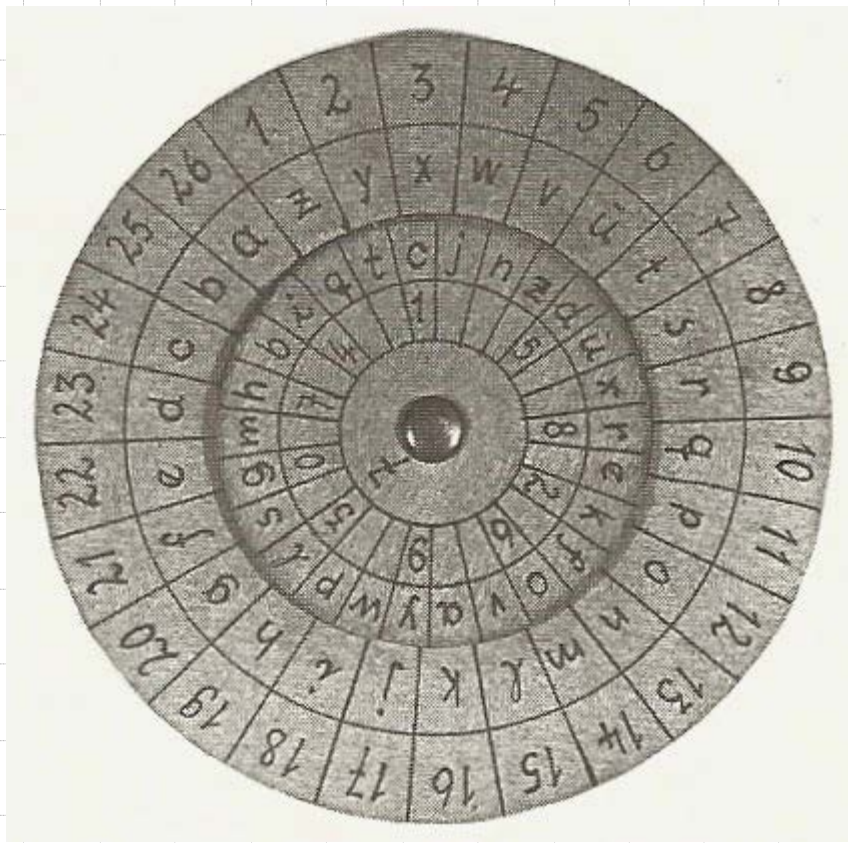
Josef Jakobs
(1898–1941)

German spy in
Great Britain

Steganographic code

mentioned in a British
censorship manual

Cleartext

CONVOY LEAVING LONDON FOR NEAPOLY THE 25/1 COMPOSED OF
TROUPS HIGHLY TRAINED FAR MOUNTAIN WARFARE
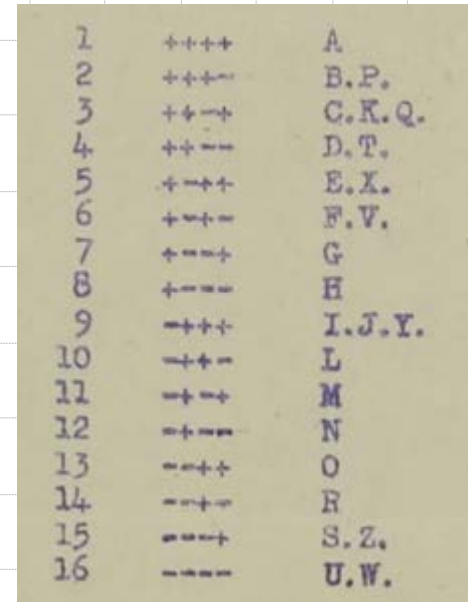
Coded cleartext

COMV LIV LOND NAPOL CC 251 HIGH
TH TRROP LIGT ART TANKS MOUNT

Steganographic code

mentioned in a British
censorship manual

Coded cleartext
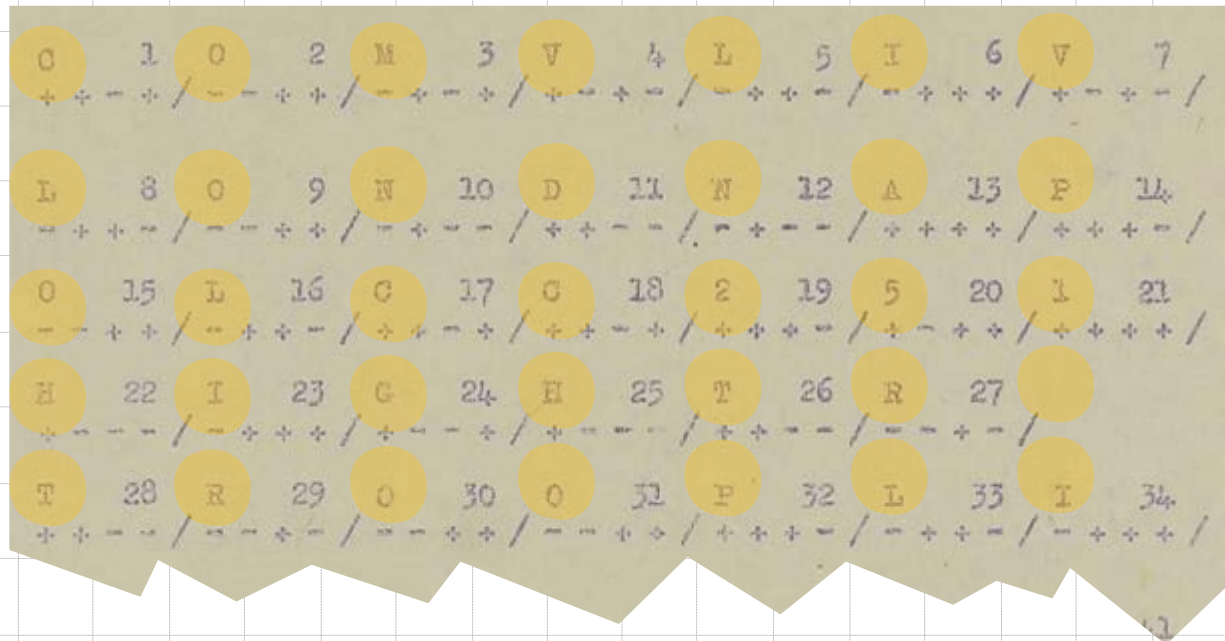
COMV LIV LOND NAPOL CC 251 HIGH
TH TRROP LIGT ART TANKS MOUNT

Binary code

Coded cleartext

COMV LIV LOND NAPOL CC 251 HIGH
TH TRROP LIGT ART TANKS MOUNT

Love Letter

COMV LIV LOND NAPOL CC 251 HIGH TH TRROP LIGT ART TANKS MOUNT

Five Unsolved Messages

Created by a German
spy in New York

```
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.
```

Conclusion and Outlook

German spy ciphers
were not especially good

Crypto codes were
not secure

Steganographic worked
but were complicated

This confirms:

1. German cryptography in WW2 was only mediocre

2. German intelligence in WW2 was only mediocre

Conclusion and Outlook

Further research is necessary:

- Find more German WW2 spy ciphers

- Find out more about German WW2 spy ciphers

- Research WW2 spy ciphers of other nations