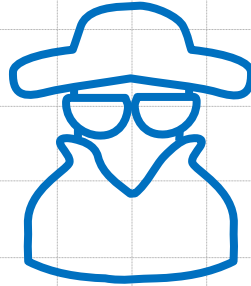


German Spy Ciphers in World War II



Euro HCC Bratislava, 2017

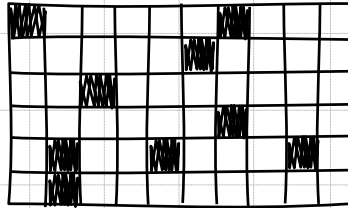
Klaus Schmeh
www.schmeh.org

Encryption based on a crossword puzzle

Cleartext

ENGLAND MUST CONCENTRATE FORCES TO WIN THE WAR

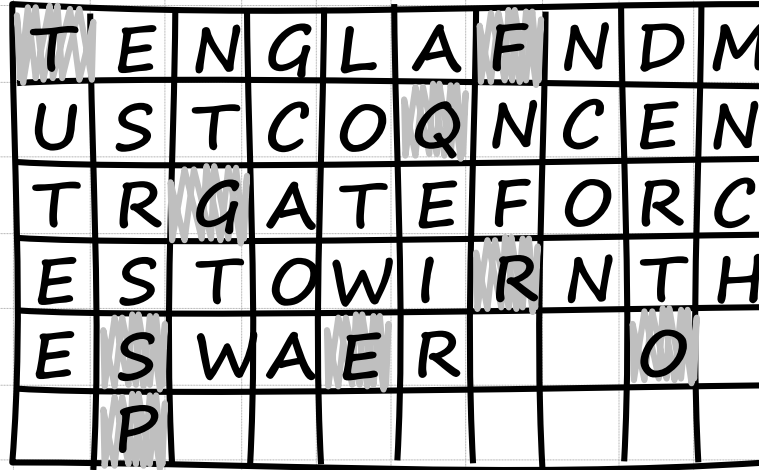
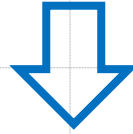
Crossword puzzle



Key word

EMBANKMENT

ENGLAND MUST CONCENTRATE FORCES TO WIN THE WAR



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	L	R	N	T	H
E	S	W	A	E	R			O	
	P								

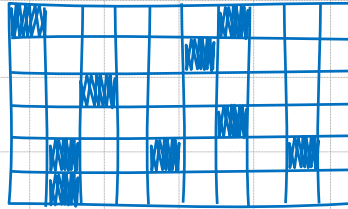
A B E E K M M N N T

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 TUTE E NCONA QEIRE SRSSP
 FNFRL OTWED ERTOM NCH

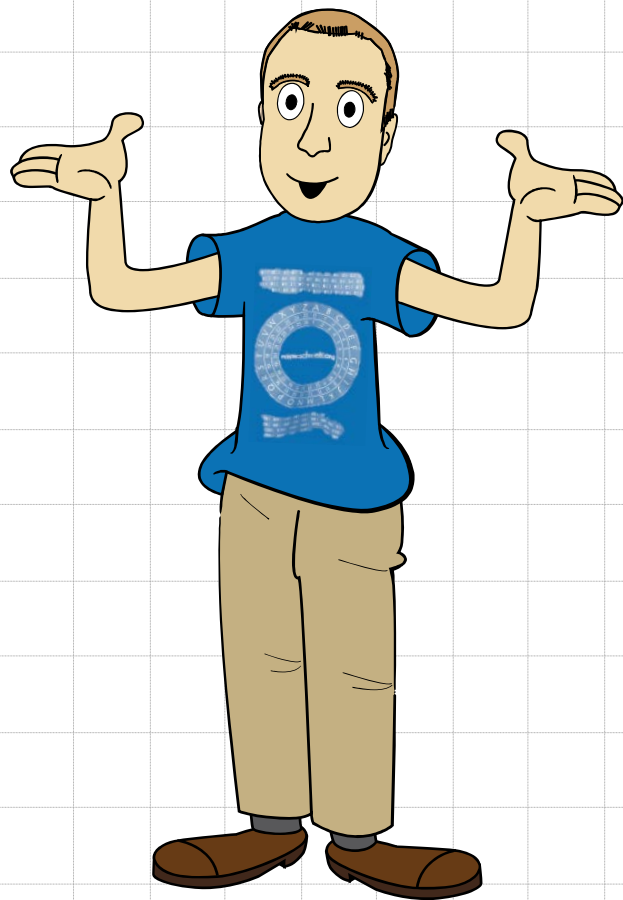
Encryption based on a crossword puzzle



Used by German spies from 1936 on.

Source: Friedman Collection

Details are not known.



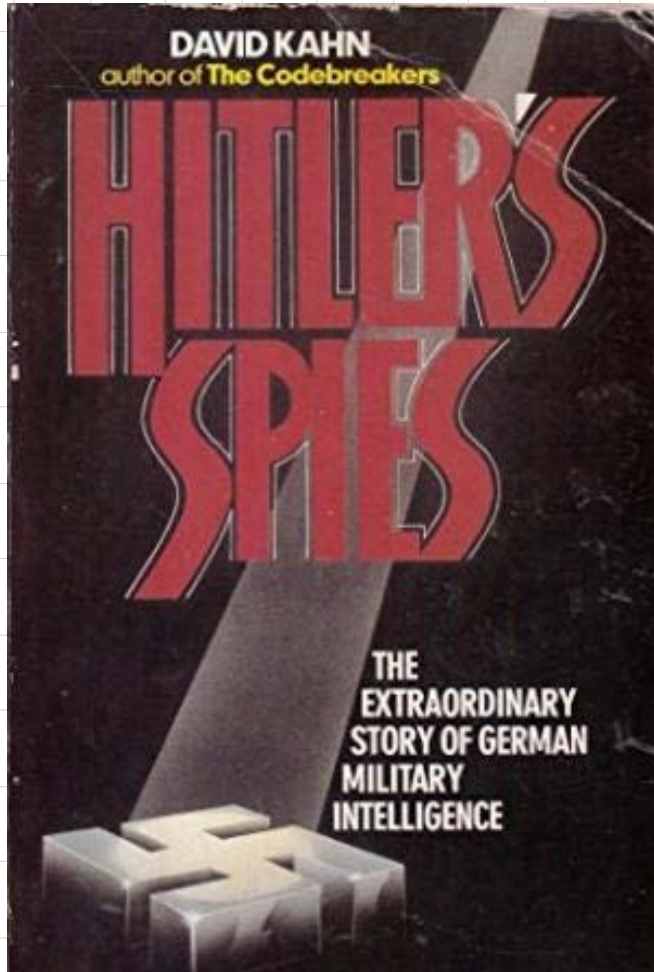
Klaus Schmeh

Cryptology Consultant

Journalist

Blogger

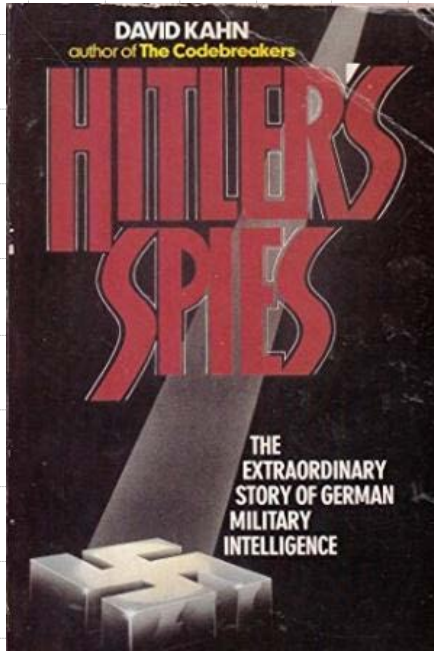
www.schmeh.org



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

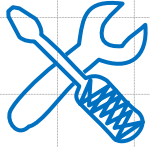
All sources I found refer to enemy
descriptions of the methods

What I found

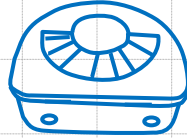
About 25 German WW2 spy ciphers

But there must be more

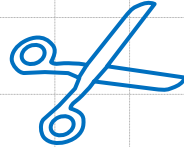
Spy Cipher Requirements



secure and
easy to use



machines and devices
prohibitive



tailored to the
spy's need

Spy cipher design is ...

- different from other codemaking
- difficult

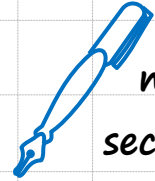
Two Approaches



cryptographic
codes



steganographic
codes

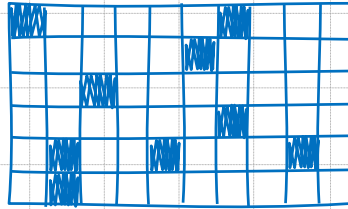


microdot
secret ink

technical
steganography

out of scope

We have seen a
cryptographic code



Let's now look at a
steganographic one

Westerlinck Code

mentioned in a British
censorship manual

Every word stands for a number:

- 1 syllable: 1
- 2 syllables: 2
- 3 or more syllables: 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

L O N
'Apres une charmante' 'mais tout aussi' ereintante 'nuit nous etions'
D O N
'fort enchanter hier' 'de voir Londres' 'but provisoire de destination. Esperons'
O U
'toutefois que' realisation totale 'de nos reves' 'comblera vite les'
T B I
'malheureux et decevants' 'sorts precedents. Ce' 'Congo tout desire'
E N A
's'atteindra esperons' 'le tout prochainement. Toutefois' 'nous avons encore'
T T E
'surement des attentes' 'penibles en perspective seulement' 'la nature humaine'
N D E
'est un contradictoire melange' 'de multiples desirs' 'sont rarement satisfaits.'
Z A
'Eternels ennuyeux problemes philosophiques !' 'A present varions !'
U T R
'Aujourd'hui soleil et' 'temperature charmante nous jouissons' 'pleinement de ce'
E S N
'beau spectacle printanier' 'dependant mes pensees' 'sont et demeurent'
O U V E
'a la "praia"' 'Estoril cote d'' 'eternel soleil luisant!' 'Nous aurions desire'
L L E
'rester la-bas seulement' 'selon une vieille' 'et exacte parole' populaire
S
'Aspirer est autre' chose chose que posseder. etc..

LONDON TOUT BIEN
ATTENDEZ AUTRES
NOUVELLES

Everything okay in
London, wait for
other news.

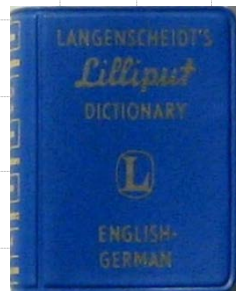
Codebook

mentioned in a British censorship manual

Octubre 1 de 1940 - No. de caja 781
NLT TECHNICO HAMBURG
NAN HAELET ANGEBOT 264/6 BEREITS GESGHEITERT 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 HAELE ANGEBOE 264/6 BEREITS GESCHEITERT DAHER BISHER
ANNEHMEN OHNE DIESE 244 UND 1345 BIS HOECHSTENS 112/3 NOCH
AUSSTEHEN LEZTE 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

TRANSLATION

47600

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** (flasks); each pipe, a bomber and each flask a fighter, i.e. 50 fighters and 20 bombers - 50 flasks 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 sira sira

North West
South West
Northern
From the North of
To the North
Meridional
From the South of
To the South

ardo ardos
sira sira
aixa

iga
ar

esse

encia

Divisions
Concentrations
Camps
Garrison
General Staff

French type, Frenchman
American type, American
English type, Englishman
Like the other Allies
South African
Portuguese
Mentioned
Rifles
Highway
Railway line
Water ways, canals
Always
Frontier

Types of Planes

Martin
Flying Fortress
Congo Island
Hurricane
Spitfire
Boston Bomber
Wellington Bomber
Douglas
Recent model
Old model
Pictories
General
Admiral
Colonel
Repair aerodromes
Aerodromes
The enemy's intentions
The difficulty of supplies
Contagious diseases
Hunger
Plans

mercaderia (merchandise)
necessidade
barris
pedido
embalagem, lata
(packing, tin)
desejo, podendo
tem pressa, recolho
diga-me (tell me)
favor, favores
disponivel (disposable)
impossivel (impossible)
oportunidade
pastilhas
interessante
comprimidos, bom, bom
preco, condicoes
especificas, conveniencia
especies, pacotes

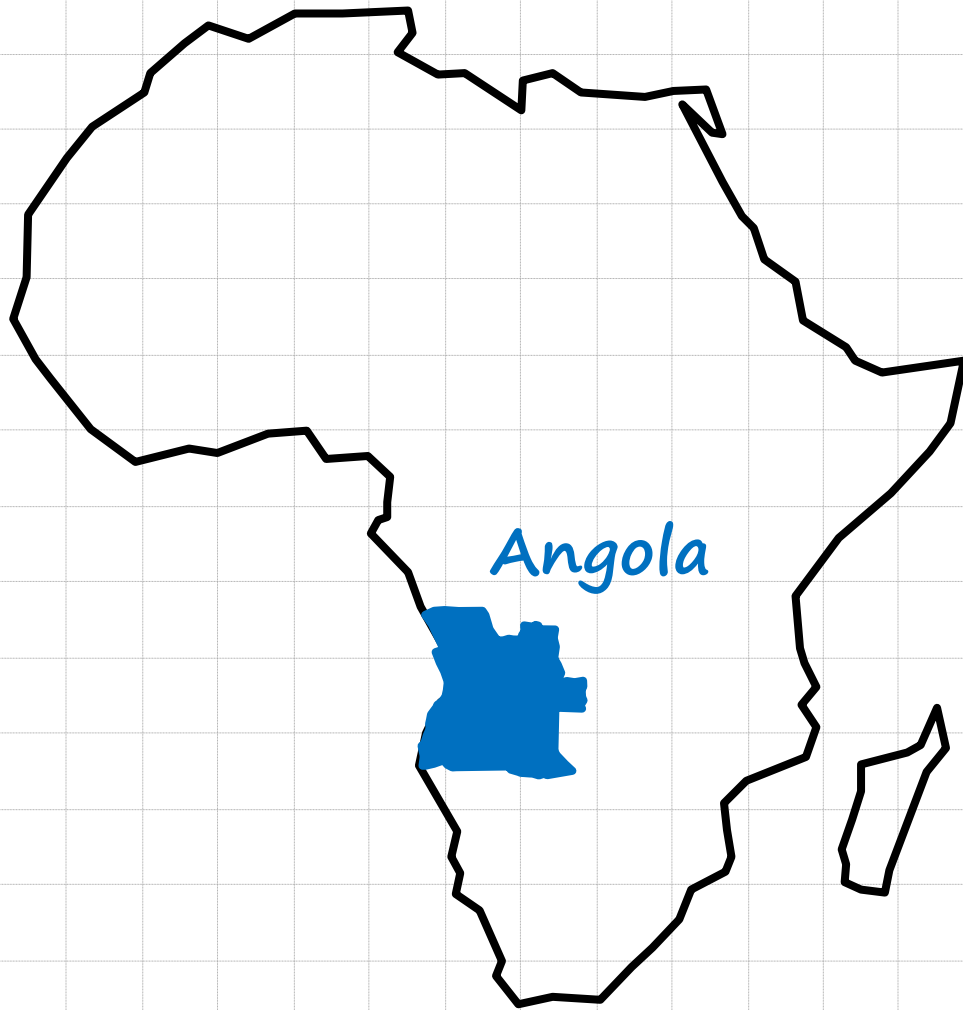
remessa (remittance)
planeta
Franco Belga
Portuguese escudos
Angolares
Madeira
vinho branco (white wine)
vinho tinto (red wine)
preto, novo (black, new)
branco, velho (white, old)
azeite (oil)
milho (maize)
trigo (corn, wheat)
azeitonas (olives)
entruga
cargos (charge, duty)
vontade (will, desire)
difficil (difficult)
difficilissimo (very difficult)
facil (easy)
intencoes (intentions)

East
From the East of
To the East
West
To West of
To the West

osto, osta
ando

Dams
Airfields
Technical military offices
Deposits of combustibles
Concentration of white forces
Concentration of native forces
Merchant ship
Warship
From 1,000 to 2,000 tons
" 2,000 to 3,000 tons
" 3 to 4,000 tons
" 4 to 5,000 tons
" 5 to 6,000 tons
" 6 to 8,000 tons
" 8 to 10,000 tons
More than 10,000 tons
Departure, departed
Arrival, arrived
Onwards
Infantry
Airforce troops
Engineers troops
Coastal artillery
War material
Blimets
Destinations
By Atlantic Islands
In good condition
Parachutists
Tanks
American tanks "M.4"
Battalions
Regiments

ancia ancias
ogo isto
enho, enho
i
arde, arda
encomenda, encomens
certa, certas
eco
encia
icias
eria
ivel
inho
inha
ente
er
aco uto
ito or v. falar
erc, ivo or v. informar
ado, ado
alta, asse or v. avisar
oes
titulos, ontos ana
es, es, ais
uno, use, usa, las
anta
ons
dolares
libras
libras esterlinas
Tons of coconut
(toneladas de cocoate)
dozenas de coiro
(dozens of skins)



During WW2
Portuguese colony

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

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

Divisions
Concentrations
Camps
Garrison
General Staff

French type, Frenchman
American type, American
English type, Englishman
Like the other Allies
South African
Portuguese
Munition dump
Rifles
Highway
Railway line
Water ways, canals
Always
?Frontier

Types of Planes

Martin
Flying Fortress
Consolidated
Hurricane
Spitfire
Boston Bomber
Wellington Bomber
Douglas
Recent model
Old model
Factories
General
Admiral
Colonel
Repair aerodromes
Aerodromes
The enemy's intentions

mercadoria (merchandise)
necessidade
barris
pedido
embalagem, lata
(packing, tin)
desejo, podendo
tem pressa, recolho
diga-me (tell me)
favor, favores
disponivel (disposable)
impossivel (impossible)
consejo, oportunidade
pastilhas
interessante
comprimidos, boa, bom
preco?, condicao
garantia, conveniencia
especies, pacote

remessa (remittance)
pimenta
Franco Belga
Portuguese escudos
Angolares
Madeira
vinho branco (white wine)
vinho tinto (red wine)
preto, novo (black, new)
branco, velho (white, old)
azeite (oil)
milho (maize)
trigo (corn, wheat)
azeitonas (olives)
entrega
encargo (charge, duty)
vontade (will, desire)

Spanish code words

TRANSLATION

4760

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 FASENIA (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 GARRAPA (bottle), each bottle represents a machine-gun. i.e. 8 machine-guns - 8 bottles.

Aeroplanes will be denoted by the words TUBOS (pipes) and FASUCOS (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).

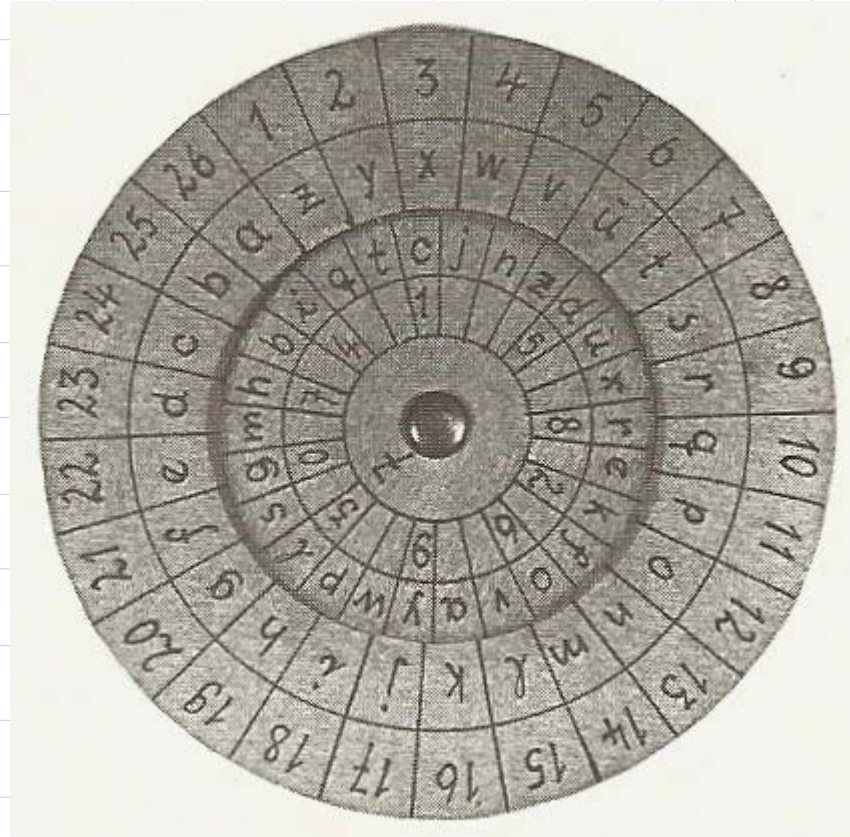
The following words will be denoted by a word which ends with these suffixes:-

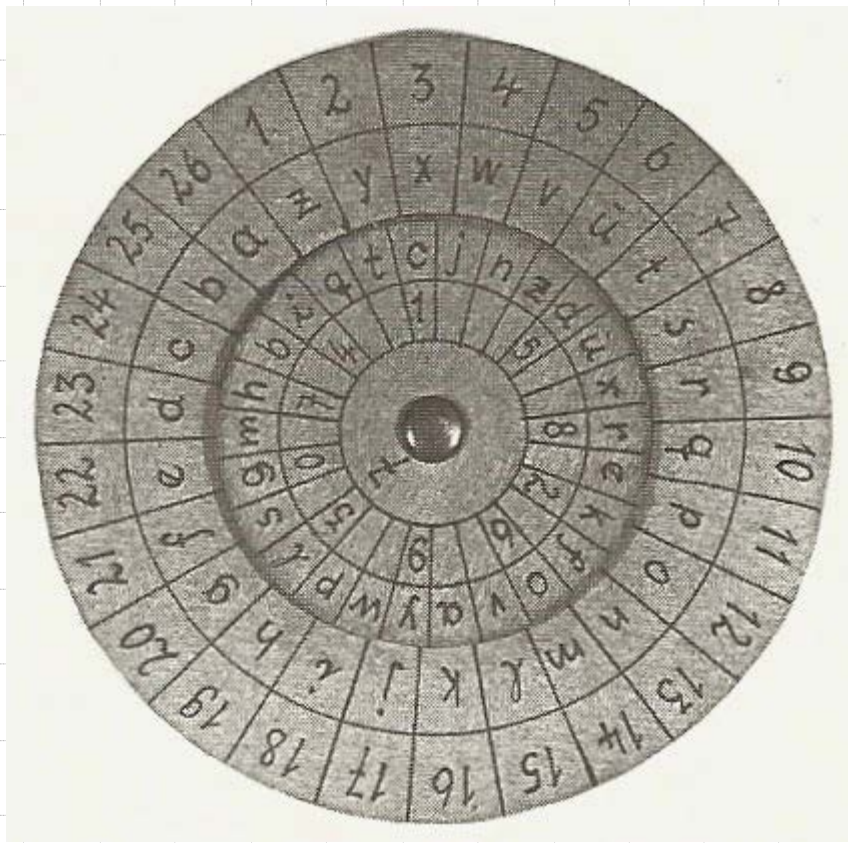
Fortifications still under construction	ardo ardos
Fortifications built	aixa aixs aixas
North West	iga
South West	ar
Northern	
From the North of }	esse
To the North }	
Meridional }	
From the South of }	encia
To the South }	

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

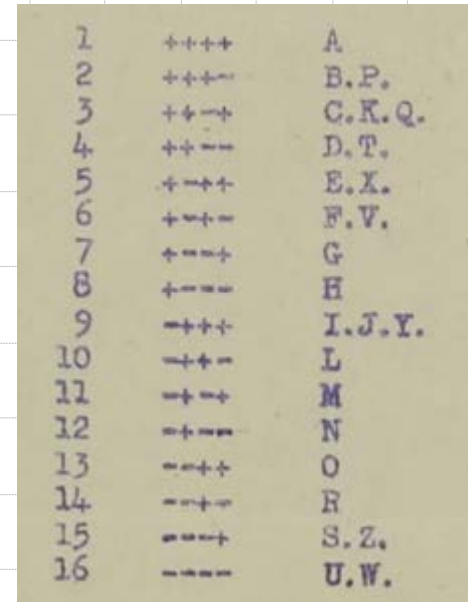
COMV LIV LOND NAPOL CC 251 HIGH
TH TRROP LIGT ART TANKS MOUNT

Steganographic code

mentioned in a British
censorship manual

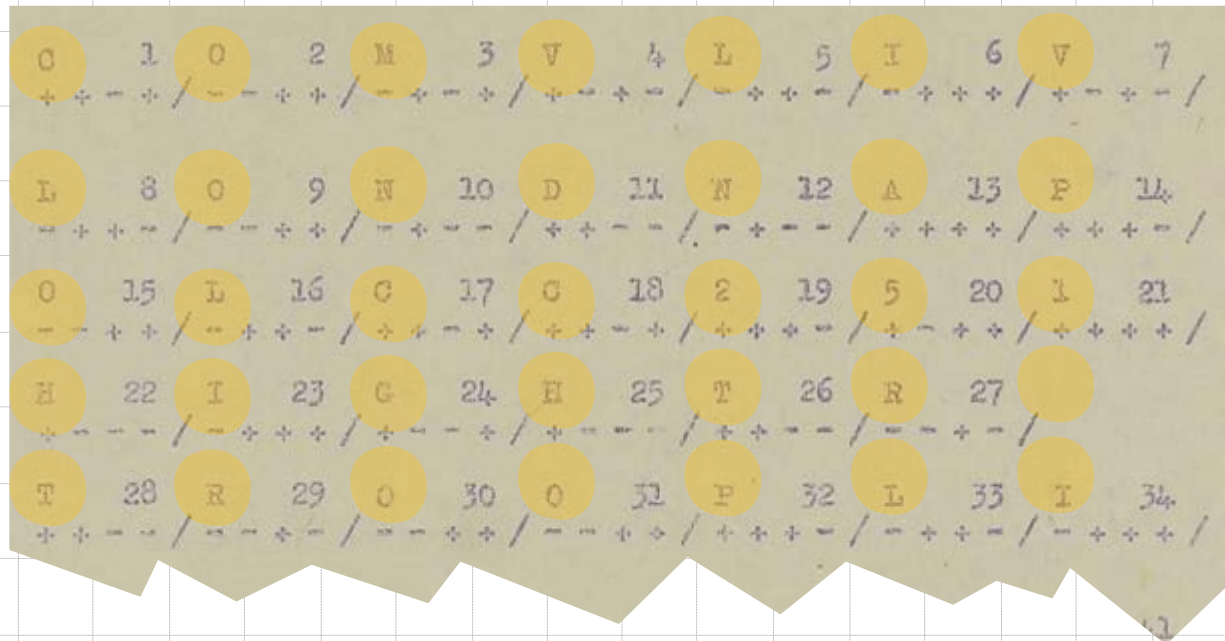
Coded cleartext

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



1	++++	A
2	+++-	B.P.
3	++-+	C.K.Q.
4	++--	D.T.
5	+--+	E.X.
6	+--+	F.V.
7	+---	G
8	+-++	H
9	+-+-	I.J.Y.
10	-+++	L
11	-++-	M
12	-+-+	N
13	-+--	O
14	--++	R
15	--+-	S.Z.
16	----	U.W.

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

London, 26.1.44.

Queridísima Amiga

1
Me + parece + que hay + una eternidad desde + cua-
2
ndo + no nos + hemos visto + y desde cua-
3

4
ndo + no tengo noticias + tuyas.

5
Como + he prometido escribirle + tan + pronto

6
tenga + llegado + en algún + sitio para poder + esperar
7

8
noticias + que tengo tanto impaciencia + en tener
9

10
que es + ya casi una + obsesión + para mí, pero es
11

12
una + obsesión dulce y + consolante

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 kecgg 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 abuwz dwoug djozl ylaug loaea ilihj
swjft oetad tjisn avagn sodwb wzaxe zvoxg xpgzv
adurm shvxx xfmug pdpvq dqwtu fryok xfvcp ydzwz
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 mjt dy zvzky bjgze
vdytd zeejw zumjp ivsna gsmzq dltxb qjqjq fnpta mqted
skijj.

229

fpoxa tijyp qrerq znqst zasn timer zarvq hhsnw vlhfg pyhqc
yuirf fsgoi twgdg sbphc fkfza bpegh jzujn wtsxp ijamg
tzdto hxzdn uivvw tizoc axkye lhmdn sfzjo omrhh zpith
hklsf anvdr ynhqk syrgi ltxos wabom dzwlz byava sjomn
qqszs adddu greao alhon lxxgi 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