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
<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>E</th>
<th>E</th>
<th>K</th>
<th>M</th>
<th>M</th>
<th>N</th>
<th>N</th>
<th>N</th>
<th>T</th>
</tr>
</thead>
<tbody>
<tr>
<td>G</td>
<td>N</td>
<td>T</td>
<td>N</td>
<td>A</td>
<td>E</td>
<td>F</td>
<td>L</td>
<td>D</td>
<td>M</td>
<td></td>
</tr>
<tr>
<td>C</td>
<td>T</td>
<td>U</td>
<td>C</td>
<td>Q</td>
<td>S</td>
<td>N</td>
<td>O</td>
<td>E</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td>A</td>
<td>G</td>
<td>T</td>
<td>O</td>
<td>E</td>
<td>R</td>
<td>F</td>
<td>T</td>
<td>R</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>O</td>
<td>T</td>
<td>E</td>
<td>N</td>
<td>I</td>
<td>S</td>
<td>R</td>
<td>W</td>
<td>T</td>
<td>H</td>
<td></td>
</tr>
<tr>
<td>A</td>
<td>E</td>
<td>S</td>
<td>E</td>
<td>O</td>
<td></td>
<td></td>
<td>P</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- GCAOA NTGTW TUTEE NCONA QEIRE SRSSP
- FNRL 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 focuses 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 design is ...
• different from other codemaking
• difficult
Two Approaches

cryptographic codes

steganographic codes

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
<table>
<thead>
<tr>
<th>Letter</th>
<th>Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>122</td>
</tr>
<tr>
<td>B</td>
<td>131</td>
</tr>
<tr>
<td>C</td>
<td>111</td>
</tr>
<tr>
<td>D</td>
<td>132</td>
</tr>
<tr>
<td>E</td>
<td>133</td>
</tr>
<tr>
<td>F</td>
<td>211</td>
</tr>
<tr>
<td>G</td>
<td>333</td>
</tr>
<tr>
<td>H</td>
<td>113</td>
</tr>
<tr>
<td>I</td>
<td>212</td>
</tr>
<tr>
<td>J</td>
<td>121</td>
</tr>
<tr>
<td>K</td>
<td>122</td>
</tr>
<tr>
<td>L</td>
<td>213</td>
</tr>
<tr>
<td>M</td>
<td>123</td>
</tr>
<tr>
<td>N</td>
<td>113</td>
</tr>
<tr>
<td>O</td>
<td>112</td>
</tr>
<tr>
<td>P</td>
<td>211</td>
</tr>
<tr>
<td>Q</td>
<td>221</td>
</tr>
<tr>
<td>R</td>
<td>311</td>
</tr>
<tr>
<td>S</td>
<td>312</td>
</tr>
<tr>
<td>T</td>
<td>313</td>
</tr>
<tr>
<td>U</td>
<td>311</td>
</tr>
<tr>
<td>V</td>
<td>323</td>
</tr>
<tr>
<td>W</td>
<td>222</td>
</tr>
<tr>
<td>X</td>
<td>223</td>
</tr>
<tr>
<td>Y</td>
<td>231</td>
</tr>
<tr>
<td>Z</td>
<td>332</td>
</tr>
</tbody>
</table>

**SNOW IN NOVEMBER:** 113 = N

**WEATHER IS NICE:** 211 = P
Everything okay in London, wait for other news.
Codebook
mentioned in a British censorship manual

Sent by German businessman Ottomar Müller from Buenos Aires to NLT Technico in Hamburg
From a German-English dictionary:
264/6 (page 264, word 6): pier
112/3 (page 112, word 3): December
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
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
Airways
?Frontier

mercadoria (merchandise)
necessidade
bogris
pedido
enbalagens, lata
(packing, tin)
desejo, podendo
tem pressa, recolho
diga-me (tell me)
favor, favorável
disponível (disposable)
impossível (impossible)
ansejo, oportunidade
pastilhas
interessante
comprimidos, boa, bom
preço?, condições
garantia, conveniência
cópias, pacote

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
remessa (remittance)
pimenta
Franco Belga
Portuguese escudos
Angolares
Madeira
cinho 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)
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
Queridísimas Amigas,

1. Me parece que hay una eternidad desde cuando no nos hemos visto y desde cuando no tengo noticias tuyas,

5. Como he prometido escribirte tan pronto

7. tenga llegado en algún sitio para poder esperar

9. noticias que tengo tanto impaciencia de tener

11. que as ya casi una obsesión para mí, pero es 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 dbvis prito kecqq kokik kyiwm zuarj alyia qtxvi vxzya szgou skiqn rbqjq mogex ezdnf vusda zurop ixklo cmnbl grdhz smwch kufej pzljej hbord wkkhku vthjk sfwda jepmu izvig kzlau rdrxx mdecs spozv eeeod dlmdz nqmia pidwg xdcyy mvkso hmml ii impwq nkipa mljvm qsbb glevn sktlq tn.

178
Eekao parwo xiavy pejux lhnhj pbqdd vdxxb mdiia gwmmn zbivm abuws dwoug djozl ylaug loaea ilihj swjft oetad tjisin avaqn sodwb wzaxe zvoxg xpgzv adurm shvxx xfmug pdpvq dqwtu fryok xfcvp ydzwm ofwfl uzfne qsslo evl.

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

140
dmxkb kqnvh zzeek beoop ygcca yvepv tykmtp iykfl zkacz uxiyd kruwy vnjvp xyeqg jpmfo abzpt mjtdy zvzky bjdge vdyd zeejw zumjp ivsna gsmzg dltxb gjjqqj fnpta mgted skijj.

229
fpoxa tijyp qrerq znqst zasnk zarvq hhsww vlhfg pyhgq yuirf fsgoi twgdg sbphc fkkza bpegh jzujn wtsxp ijamg tzezd hhzdtn ulvwv tizoc axkye lhmndn sffzo omrhb zpith hklsw anvdr ynhqg syrgi ltxos wabom dzwlb byaav sjomn qqszq adddu greao alhon lxzgj iwpnf uzgui jgmya ksqfw szj1.
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