8 Example 2

Now we go through an example step by step and produce a complete solution for the ciphertext

```
ZIDPV USABH HEABG RZMOP UWVJD MLPCS PFTSH ISJMR RFSKU KHUAT
SFDNB GWTAN CSZZW HPHNP DDSAX GTRGY OZPKO EAGRG YSGQD KKNIT
DWFZZ INSYH UTSZR KJDVJ JLJIJ MQHCB RINYI
```

Aligning Known Plaintext

We believe the plaintext contains "Oberleutnant zur See" as the rank of the sender, that is we assume a crib near the end of the message, and assume that at most 20 letters follow, containing the name. The scheme

```
      RGYSGQDKKNITDWFZZINSYHUTSZRKJDVJJLJIJMQHCBRINYI
[ 89] xstopxoberleutnantxzurxseex
[ 90]  xstopxoberleutnantxzurx=eex
[ 91]   x=topxoberleutna=txz=rxseex
[ 92]    xstopxoberleutnantxzurxseex
[ 93]     xstopxoberleut=antxzurxseex
[ 94]      xstopxoberleutnantxzu=xseex
[ 95]       xstopxoberleutnan=x=urxseex
[ 96]        xstopxoberleutnantxzurxseex
[ 97]         xstopxoberleutnantxzurxseex
[ 98]          xs=opxoberleutnantxzurxseex
[ 99]           xstopxoberle==nantxzurxseex
[100]            xstopxoberleutnantxzurxseex
[101]             xstopxoberleutnantxzurxseex
[102]              xstopxoberleutnantxzurxseex
[103]               xstopxoberleutnantxzurxseex
[104]                xstopxoberleutnantxzurxseex
[105]                 xstopxoberleutnantxzurxseex
[106]                  xstopxobe=leutnantxzurxseex
[107]                   x=topxoberleutnantxzurxseex
[108]                    xstopxoberleutnantxzurxseex
[109]                     xstopxoberleutnantxzurxseex
      RGYSGQDKKNITDWFZZINSYHUTSZRKJDVJJLJIJMQHCBRINYI
```

gives 12 hits for the negative pattern search among the 21 considered positions: 89, 92, 96, 97, 100, 101, 102, 103, 104, 105, 108, 109—at least a slight reduction for manual cryptanalysis.

Constructing a TURING Graph

Somewhere along the way we test position 103 and consider the crib

```
FZZINSYHUTSZRKJDVJJLJIJMQHC
xstopxoberleutnantxzurxseex
```

We derive the cycle diagram in Figure 7.

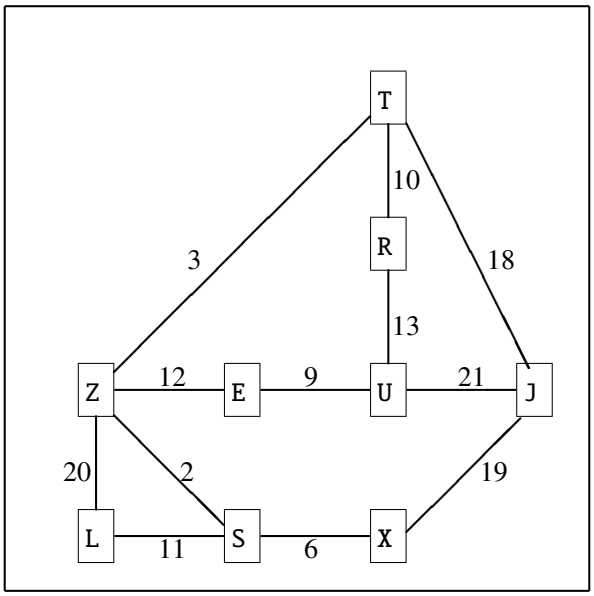

Abbildung 7: TURING *cycles for Example 2*

Therefore as "menu"—the chunk of known plaintext to be examined—we use the sequence of length 20 starting from position 104 (that corresponds to the edge with label 2):

```
ZZINSYHUTSZRKJDVJJLJ
STOPXOBERLEUTNANTXZU
```

To exhaust all the rotor orders, starting positions, and plug connections for this chunk of known plaintext we use Jean-François Bouchaudy's TURING Bombe Simulator, to be found at `http://cryptocellar.web.cern.ch/cryptocellar/simula/jfb/BP12.zip`.

> In a virtual machine on a 2.93 GHz Intel Core-i7 processor it needed 5 minutes for all 60 rotor orders and produced exactly one solution in "WELCHMAN mode" (the diagonal board, see later).

Using only the rotors I, II, and III and disabling the diagonal board—that we haven't introduced yet—we get 6 "solutions" in a few seconds

```
(1)                I II III KFX
(2)                I II III WHV
(3)                II I III ZYN
(4)                III I II JXS
```

```
(5)                 III II I IES
(6)                 III II I QSV
```

Exploring Solution (1)

Let us try the first proposed solution. We begin by decrypting the ciphertext with a ring setting that causes no stepping of the middle rotor for the next 20 positions, and no plugs in the plugboard. Missing plugs will be detected by the following considerations.

> The assumption on the ring setting is somewhat optimistic. It it fails for all of the solutions, we have to try harder, experimenting with shorter cribs or guessing the ring setting of the fast rotor.

We use the rotor order I (slow), II (middle), III (fast), and the start positions KFX. This gives the trial decryption

```
ZZINSYHUTSZRKJDVJJLJIJMQHCBRINYI
XPMEJJXPGQBMIVVUKRSISPTNFVAZEQTG
```

This doesn't look like plaintext, but we have not yet explored the plugs. We start with the plug connection $\tilde{\mathtt{Z}}$ of Z, the letter with the maximum number of edges in the graph. We try all 26 possible connections, see Table 1.

Only line X is compatible with the cycle, giving $\tilde{\mathtt{Z}} = \mathtt{X}$. For a manual check of the other cycles we use the complete description of the combined rotor substitutions $\varphi_2, \ldots, \varphi_{21}$ given in Table 2. The "plugged" cycles fit "unplugged" ones:

$$\tilde{\mathtt{Z}} \xrightarrow{3} \tilde{\mathtt{T}} \xrightarrow{10} \tilde{\mathtt{R}} \xrightarrow{13} \tilde{\mathtt{U}} \xrightarrow{9} \tilde{\mathtt{E}} \xrightarrow{12} \tilde{\mathtt{Z}} \quad \text{fits} \quad \mathtt{X} \xrightarrow{3} \mathtt{I} \xrightarrow{10} \mathtt{Y} \xrightarrow{13} \mathtt{F} \xrightarrow{9} \mathtt{L} \xrightarrow{12} \mathtt{X}$$

$$\tilde{\mathtt{Z}} \xrightarrow{2} \tilde{\mathtt{S}} \xrightarrow{6} \tilde{\mathtt{X}} \xrightarrow{19} \tilde{\mathtt{J}} \xrightarrow{21} \tilde{\mathtt{U}} \xrightarrow{9} \tilde{\mathtt{E}} \xrightarrow{12} \tilde{\mathtt{Z}} \quad \text{fits}$$

$$\mathtt{X} \xrightarrow{2} \mathtt{Z} \xrightarrow{6} \mathtt{F} \xrightarrow{19} \mathtt{N} \xrightarrow{21} \mathtt{F} \xrightarrow{9} \mathtt{L} \xrightarrow{12} \mathtt{X}$$

$$\tilde{\mathtt{T}} \xrightarrow{10} \tilde{\mathtt{R}} \xrightarrow{13} \tilde{\mathtt{U}} \xrightarrow{21} \tilde{\mathtt{J}} \xrightarrow{18} \tilde{\mathtt{T}} \quad \text{fits} \quad \mathtt{I} \xrightarrow{10} \mathtt{Y} \xrightarrow{13} \mathtt{F} \xrightarrow{21} \mathtt{N} \xrightarrow{18} \mathtt{I}$$

Therefore the cycle conditions hold indeed.

However we didn't need to check them because reading off the plug connections from the first loop, row "X" in Table 1, we get $\tilde{\mathtt{Z}} = \mathtt{X}$, $\tilde{\mathtt{S}} = \mathtt{Z}$, and this already is a contradiction.

Therefore solution (1) was a false alarm. This observation leads to WELCHMAN's **plug condition** expressing the fact that the plug substitution is an involution:

> *If $\tilde{a} = b$, then also $\tilde{b} = a$ for each pair of letters $a, b \in \Sigma$.*

Exploring Solution (2)

We try the second proposed solution. As before we begin by decrypting the ciphertext, starting from position 103, rotor order I, II, III. Because V is the turnover point of Rotor III we have to turn Rotor II back by one position in order to get the correct start positions WGV. The trial decryption gives

$\tilde{Z}$	$\xrightarrow{2}$	$\tilde{S}$	$\xrightarrow{11}$	$\tilde{L}$	$\xrightarrow{20}$	$\tilde{Z}$
A		C		V		W
B		L		H		G
C		A		M		B
D		F		N		R
E		G		K		U
F		D		Z		E
G		E		T		A
H		O		R		N
I		V		C		P
J		M		A		T
K		U		W		V
L		B		I		F
M		J		P		C
N		S		Q		J
O		H		L		S
P		R		O		Y
Q		Y		X		D
R		P		J		Q
S		N		F		I
T		W		U		K
U		K		G		H
V		I		B		M
W		T		E		Z
X		Z		D		X
Y		Q		S		L
Z		X		Y		O

Tabelle 1: Example 2—Possible plug connections for the first cycle

Substition in rotor position	Substitution table A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
φ_2: KFX	C L A F G D E O V M U B J S H R Y P N W K I T Z Q X
φ_3: KFY	D C B A Y S L J X H O G N M K Z R Q F V W T U I E P
φ_4: KFZ	N X E F C D P S M Q U Y I A V G J T H R K O Z B L W
φ_5: KFA	B A X V N Y K Q O Z G M L E I U H T W R P D S C F J
φ_5: KFB	U D L B M Z O Y V S T C E Q G W N X J K A I P R H F
φ_5: KFC	Z U O T X H L F P Y Q G V S C I K W N D B M R E J A
φ_5: KFD	J D U B Y Q R X S A T P O Z M L F G I K C W V H E N
φ_5: KFE	R C B W H L O E J I M F K S G U T A N Q P X D V Z Y
φ_{10}: KFF	M Z H X W P T C Y R O U A Q K F N J V G L S E D I B
φ_{11}: KFG	M I V Z T N K L B P G H A F R J S O Q E W C U Y X D
φ_{12}: KFH	F Z R W V A T I H Y O X N M K U S C Q G P E D L J B
φ_{13}: KFI	J S U G W Y D K L A H I R P Q N O M B V C T E Z F X
φ_{14}: KFJ	V Y O W F E H G K S I P T R C L U N J M Q A D Z B X
φ_{15}: KFK	F R W K Y A M P X V D N G L Q H O B U Z S J C I E T
φ_{16}: KFL	B A I V J S H G C E Q O N M L T K U F P R D Z Y X W
φ_{17}: KFM	R J I O K Y M X C B E P G Q D L N A Z W V U T H F S
φ_{18}: KFN	R Q S P U H L F N K J G T I Z D B A C M E W V Y Z O
φ_{19}: KFO	W V E K C N X Z O R D Y P F I M S J Q U T B A G L H
φ_{20}: KFP	T M P X Z I H G F Q U S B R Y C J N L A K W V D O E
φ_{21}: KFQ	C T A V M N Y Z J I Q O E F L X K W U B S D R P G H

Tabelle 2: Example 2—Combined rotor substitutions for rotor order I, II, III without turnover of Rotor II. Calculated using the online Enigma simulation at `http://enigmaco.de/`.

```
ZZINSYHUTSZRKJDVJJLJIJMQHCBRINYI
STOPXOBERLEUTNANTXZURXSEEXJAEGER
```

—a perfect result. We see that indeed V is the true turnover point of Rotor III, that means that the ring setting of this rotor is A. Moreover all letters except F and W occur, proving that they are unplugged, and the only possible plug connection could be between F and W.

From position 103 we go back for 26 positions and start with the rotor setting WFV. We get

```
RGYOZPKOEAGRGYSGQDKKNITDWF
ISTXLEUCHTTONNEXKNULLNEUNX
```

This proves that also F and W are unplugged. The only key element yet unknown is the ring setting of rotor II.

We go back for another 26 letters and start with the rotor positions WEV. This gives the trial decryption

```
FDNBGWTANCSZZWHPHNPDDSAXGT
SHKTDFEEFXMAMPPGAGRJIXKMXN
```

and the end rotor positions XFV instead of WFV. Something must have happened in between, and this could only be the stepping of Rotor I. The position of Rotor II then must have been E. Because of the double stepping of Rotor II the rotor start positions for this section of text must be VDV. Let's try this:

```
FDNBGWTANCSZZWHPHNPDDSAXGT
XHDREIZEHNXSTOPXERLOSCHENX
```

This is correct plaintext and proves that Rotor II has turnover point E, corresponding to ring setting A.

We conclude that the rotor start positions for the complete text are VCW, and get the decryption

```
ZIDPVUSABHHEABGRZMOPUWVJDMLPCSPFTSHISJMRRFSKUKHUATS
MELDUNGXVONXFREGATTEXGERMANIAXSTOPXPLANQUADRATXQELF

FDNBGWTANCSZZWHPHNPDDSAXGTRGYOZPKOEAGRGYSGQDKKNITDWF
XHDREIZEHNXSTOPXERLOSCHENXISTXLEUCHTTONNEXKNULLNEUNX

ZZINSYHUTSZRKJDVJJLJIJMQHCBRINYI
STOPXOBERLEUTNANTXZURXSEEXJAEGER
```

or, written in a more readable form,

> Meldung X von X Fregatte X Germania X Stop X Planquadrat X Qelf X Hdreizehn X Stop X Erloschen X ist X Leuchttonne X Knullneun X Stop X Oberleutnant X zur X See X Jaeger

A Note on the Technical Realization: WELCHMAN's Diagonal Board

To systematically explore WELCHMAN's plug conditions we consider the connected component of the TURING graph that we used. Assume it consists of the set $M = \{s_1, \ldots, s_r\}$ of letters. When the bombe stops it also provides the plug connection of the selected letter, say s_1 with $\tilde{s}_1$, and allows to derive the set of plug connections $\tilde{M} = \{\tilde{s}_1, \ldots, \tilde{s}_r\}$.

For the false "solution" (1) we had $M = \{\mathtt{E,J,L,R,S,T,U,X,Z}\}$, and the provided or derived plug connections

$$\tilde{\mathtt{E}} = \mathtt{L},\ \tilde{\mathtt{J}} = \mathtt{N},\ \tilde{\mathtt{L}} = \mathtt{D},\ \tilde{\mathtt{R}} = \mathtt{Y},\ \tilde{\mathtt{S}} = \mathtt{Z},\ \tilde{\mathtt{T}} = \mathtt{I},\ \tilde{\mathtt{U}} = \mathtt{F},\ \tilde{\mathtt{X}} = \mathtt{F},\ \tilde{\mathtt{Z}} = \mathtt{X}.$$

We observe two kinds of contradictions:

1. $\tilde{\mathtt{U}} = \mathtt{F}$, $\tilde{\mathtt{X}} = \mathtt{F}$: Two letters in M cannot be connected to the same letter in $\tilde{M}$.
2. $\tilde{\mathtt{E}} = \mathtt{L}$, $\tilde{\mathtt{L}} = \mathtt{D}$, hence $\eta\mathtt{E} = \tilde{\mathtt{E}} \in M \cap \tilde{M}$ and $\eta^2\mathtt{E} \neq \mathtt{E}$. In the same way $\tilde{\mathtt{S}} = \mathtt{Z}$, $\tilde{\mathtt{Z}} = \mathtt{X}$, $\eta^2\mathtt{S} \neq \mathtt{S}$, and $\tilde{\mathtt{Z}} = \mathtt{X}$, $\tilde{\mathtt{X}} = \mathtt{F}$, $\eta^2\mathtt{Z} \neq \mathtt{Z}$.

Checking for these contradictions in software is easy. WELCHMAN's ingenious idea was to imagine and construct a simple device, the diagonal board, that was attached to the bombe and prevented stops in situations that contained contradictions to the plug conditions.

The improved bombe, called TURING-WELCHMAN Bombe, provided only very few false positives. Moreover it not only used the letters in the cycles but also "non-cycle" letters connected to a cycle, in other words, a complete connected component of the TURING graph. In fact it even worked when the graph didn't have any cycles.