9 Example 3

Since Example 2 turned out to be quite simple, we analyze one more example. The ciphertext is

```
CZSTQ GJYNF ZYOLR TLXBR YXJCE MONAS XIPHU CXSAD BGEEQ ROBPI
QMUDP LWYDD GRCMC MJLGW TWBDK BHCPM UMEIB TMCUR DOVPU XNGBZ
QRBKD RPCKL XQKYM CSLGP NHIGD LOHBM PYPNV MTZVU EBDCZ AZLSX
OSZHL GSSZN MBBWS FDTUW IAXEH HLQGR LXMVA MXLWF QGOOA RZXUH
VUAWM KQDXH ZOIJI AMXCI TQNUM ZTZIW CKSBH HRZBH HRNZE WZCGV
BQ
```

and we are quite sure that the plaintext begins with “Befehl X des X Fuehrers X Stop X”. We align this with the ciphertext:

```
CZSTQ GJYNF ZYOLR TLXBR YXJCE
BEFEH LXDES XFUEH RERSX STOPX
```

Negative pattern search yields no contradiction. From positions 1 to 20 we derive the TURING graph whose largest connected component is shown in Figure 8. It has three cycles that overlap, two of them of length 2. Running the Bombe Simulator in “TURING mode” for these three cycles yields about $1500 \approx 60 \cdot 26$ solutions, as expected. The (lexicographically) first of them is

Rotor order	I II III
Start position	ZPB

Table 3 describes the transformations $\varphi_2, \ldots, \varphi_{20}$.

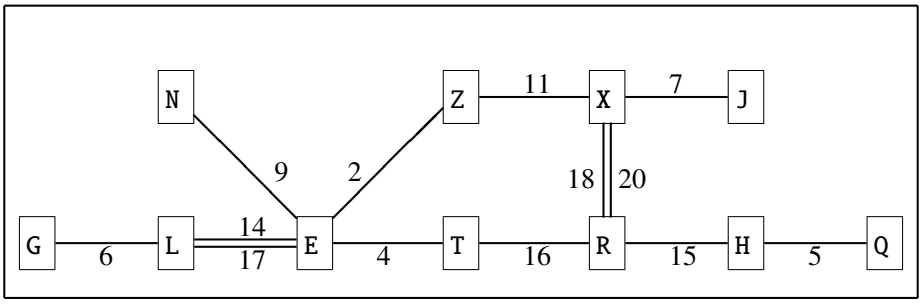

Abbildung 8: TURING *graph for Example 3, largest connected component*

Now we consider the E-L-E cycle and the E-Z-X-R-T-E cycle, see Table 4. The L-E cycle has 6 compatible plug connections for E and L. The E-Z-X-R-T-E cycle boils this number down to 1. The third cycle, X-R-X, fits into the picture, because $\varphi_{20}\tilde{\mathtt{X}} = \varphi_{20}\mathtt{I} = \mathtt{B} = \tilde{\mathtt{R}}$.

Again the WELCHMAN conditions rule out this solution because of the contradiction in the first row: $\tilde{\mathtt{L}} = \mathtt{B}$ in column 2, $\tilde{\mathtt{R}} = \mathtt{B}$ in column 6. And indeed, running the Bombe Simulator in “WELCHMAN mode” yields a unique solution:

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: ZPB	N G E S C I B R F W X U O A M Y Z H D V L T J K P Q
φ_3: ZPC	M J S H Q O K D W B G V A U F Z E Y C X N L I T R P
φ_4: ZPD	F L H N I A T C E R X B Y D Z Q P J V G W S U K M O
φ_5: ZPE	V D G B J T C K U E H Y W Z S R X P O F I A M Q L N
φ_6: ZPF	P T I U J Z Q M C E Y S H W X A G V L B D R N O K F
φ_7: ZPG	R D I B M Q U V C Y O T E X K Z F A W L G H S N J P
φ_8: ZPH	Q L F T K C P R Z S E B X W U G A H J D O Y N M V I
φ_9: ZPI	D X J A L Q I S G C U E W R Z V F N H Y K P M B T O
φ_{10}: ZPJ	S W X L R U Q T O M Y D J Z I V G E A H F P B C K N
φ_{11}: ZPK	P E O H B Z Q D N R W Y U I C A G J X V M T K S L F
φ_{12}: ZPL	R M S Y L U T Q P X Z E B V W I H A C G F N O J D K
φ_{13}: ZPM	J P S G Y N D Z Q A T U V F X B I W C K L M R O E H
φ_{14}: ZPN	B A Z W Y R I O G T U X Q V H S M F P J K N D L E C
φ_{15}: ZPO	H M S Y O R L A T U P G B X E K W F C I J Z Q N D V
φ_{16}: ZPP	K F D C R B S T U N A P V J Z L X E G H I M Y Q W O
φ_{17}: ZPQ	B A V L Y S U O K M I D J P H N Z X F W G C T R E Q
φ_{18}: ZPR	N I J Q T U M W B C V S G A Y X D Z L E F K H P O R
φ_{19}: ZPS	Q P K R U J Z N L F C I W H T B A D Y O E X M V S G
φ_{20}: ZPT	V I G L Z P C M B N S D H J Y F X U K W R A T Q O E

Tabelle 3: Example 3—Combined rotor substitutions for rotor order I, II, III without turnover of Rotor II. Calculated using the online Enigma simulation at `http://enigmaco.de/`.

$\tilde{\mathtt{E}}$	$\xrightarrow{14}$	$\tilde{\mathtt{L}}$	$\xrightarrow{17}$	$\tilde{\mathtt{E}}$	$\xrightarrow{2}$	$\tilde{\mathtt{Z}}$	$\xrightarrow{11}$	$\tilde{\mathtt{X}}$	$\xrightarrow{18}$	$\tilde{\mathtt{R}}$	$\xrightarrow{16}$	$\tilde{\mathtt{T}}$	$\xrightarrow{4}$	$\tilde{\mathtt{E}}$
A		B		A		N		I		B		F		A
B		A		B		G		Q		D		C		H
C		Z		Q	†									
D		W		T	†									
E		Y		E		C		O		Y		W		U
F		R		X	†									
G		I		K	†									
H		O		H		R		J		C		D		N
I		G		U	†									
J		T		W	†									
K		U		G	†									
L		X		R	†									
M		Q		Z	†									
N		V		C	†									
O		H		O		M		U		F		B		L
P		S		F	†									
Q		M		J	†									
R		F		S	†									
S		P		N	†									
T		J		M	†									
U		K		I	†									
V		N		P	†									
W		D		L	†									
X		L		D	†									
Y		E		Y		P		A		N		J		R
Z		C		V	†									

Tabelle 4: Example 3—Possible plug connections for the first two loops

Rotor order	III II I
Start position	BMX

with the plugs A-Z, C-X, E-V. A trial decryption with these plugs and ring settings AAA shows parts, but not all of the known plaintext:

```
EUEHLXHECXGFEHRERLXZTOPX
 *     * * **      * *
(B)EFEHLXDESXFUEHRERSXSTOPX
```

To get on we use a second connected component of the TURING graph, see Figure 9.

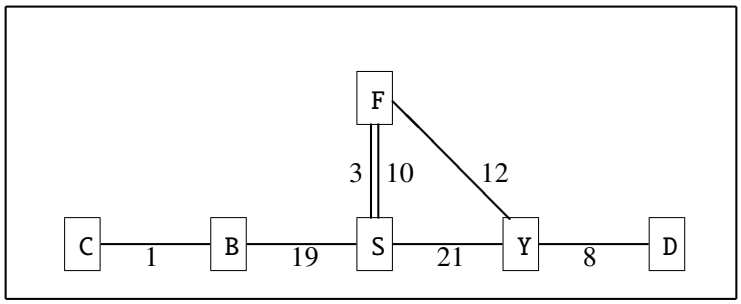

Abbildung 9: TURING *graph for Example 3, second connected component*

Trying the cycle S-F-S with φ_3 and φ_{10} using all the plugs for S that are yet free gives two possible solutions: S-U-S and U-S-U. The second one violates the WELCHMAN condition for S. The first one yields the plugs S-S and F-U. Furthermore we get $\tilde{\mathtt{Y}} = \varphi_{12}\tilde{\mathtt{F}} = \varphi_{12}\mathtt{U} = \mathtt{B}$, and $\tilde{\mathtt{D}} = \varphi_8\tilde{\mathtt{Y}} = \varphi_8\mathtt{B} = \mathtt{W}$.

Up to now we identified the plugs A-Z, B-Y, C-X, D-W, E-V, F-U. Trial decryption yields the perfect plaintext

```
EFEHLXDESXFUEHRERSXSTOPX
```

So we try to decrypt the complete ciphertext with the rotor order III II I, the ring settings AAA, the plugs A-Z, B-Y, C-X, D-W, E-V, F-U, and the start positions BMW, and get

```
BEFEH LXDES XFUEH RERSX STOPX IMXFA LLEXZ XZTXU NWAHR SQEIN
LIQEN XFRAN ZOESI SQENX ANGRI FFSXS INDXD IEXWE STBEF ESTIG
UNGEN XJEDE RXZAH LENMA ESSIG ENXUE BERLE GENHE ITXZU MXTRO
TZXZU XHALT ENXST OPXFU EHRUN GXUND XTRUP PEXMU ESSEN XVONX
DIESE RXEHR ENPFL IQTXD URQDR UNGEN XSEIN XSTOP XHEIL XHITL
ER
```

> Befehl des Fuehrers STOP Im Falle z. Zt. unwahrscheinlichen franzoesischen Angriffs sind die Westbefestigungen jeder zahlenmaessigen Ueberlegenheit zum Trotz zu halten STOP Fuehrung und Truppe muessen von dieser Ehrenpflicht durchdrungen sein STOP Heil Hitler

We observe that the slow rotor didn't step during this decryption. In general the a priori probability for its stepping was 257 letters of text divided by 676 possible positions of the other two rotors ≈ 0.38.