MysteryTwister C3

THE CRYPTO CHALLENGE CONTEST

Reserve Hand Procedure – Part 1

Author: Michael Hörenberg

February 2013

The Reserve Hand Procedure, (German: Reservehandverfahren (RHV), Marine Dienstvorschrift Nr. 929/1) has been used by the German navy during World War 2 in cases when no working Enigma machine was available. Messages encrypted with the RHV could not be distinguished from Enigma messages. The method is based on transposition and substitution. In order to encrypt a message, the following pieces of information that used to be secret were necessary:

- 25 (or more) bigram substitution tables and the order of their application.
- The number sequence that defined the order of the transposition groups (it varied in each message in length and order).

An example (without indicator groups)

We want to decrypt the following message:
Ciphertext: `MRQE KHUG XHUK QLML QNRD KPIP EADL`

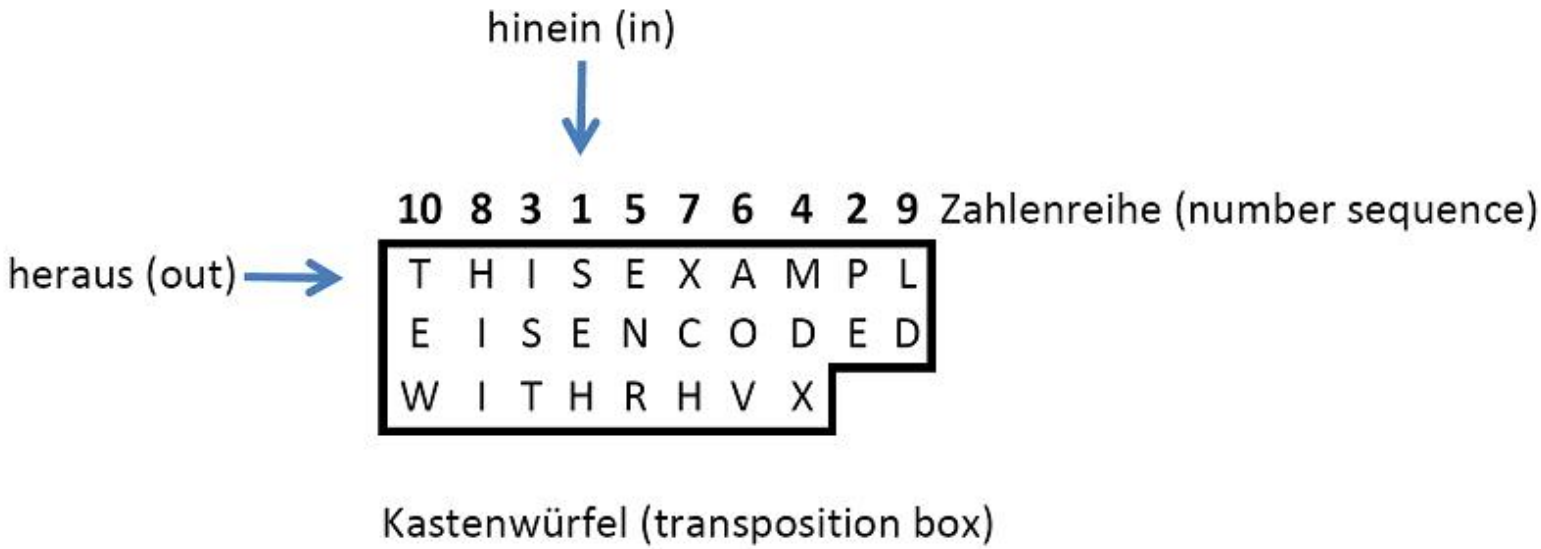
At first, the substitution needs to be reversed.
The groups of four characters are called "radio groups" because they have been transmitted using Morse code. With these groups the so called "book groups" are built using bigram substitution tables.
Therefore, one radio group is written under the other and then they are grouped in pairs vertically. If the last letters cannot be grouped vertically, they are combined horizontally.

It is required that the number of letters in each message can be divided by 4. (If this is not the case, the message is padded with random consonants).
The pairs of letters are now transformed into book groups by using the corresponding bigram substitution table that is given above the column.
In this example, the radio group MK (marked in yellow) is replaced by the book group SE as it is defined in the bigram substitution table 5.

FUNKGRUPPEN (radio groups)				BUCHGRUPPEN (book groups)			
Tauschtafelfolge (table sequence)							
5	**17**	**2**	**21**				
M	R	Q	E	S	E	H	P
K	H	U	G	E	I	S	T
X	H	U	K	M	D	X	E
Q	L	M	L	N	R	A	O
Q	N	R	D	V	X	C	H
K	P	I	P	H	I	I	L
E	A	D	L	D	T	E	W

Bigram	Bigram	Table
MK -->	SE	5
XQ -->	MN	5
QK -->	VH	5
EA -->	DT	(5)!
RH -->	EI	17
...	...	...

In the next step, the transposition is undone. The number sequence is written above the "transposition box" and determines the order in which the book groups are filled in vertically. The plaintext can be read horizontally from the transposition box.



Kastenwürfel (transposition box)

In the example, we get the following plaintext:
`THIS EXAMPLE IS ENCODED WITH RHV`

In order to create a message, you do the steps described before in reverse order:
Create transposition box → write plaintext horizontally → read book groups vertically → create radio groups using bigram substitution tables.

The key, which consists of the table and number sequence, has been transmitted by indicator groups at the beginning and end of each message.

The complete procedure can be looked up in [1]. In the following challenge, the key is known and it is not necessary to extract it from the message, i.e., the indicator group at the beginning and end of the message has already been deleted.

Challenge

You need to solve the following task:
Table sequence: 3 19 8 24
Number sequence: 13 7 4 8 15 1 6 11 5 2 14 10 9 12 3
Ciphertext:

```
MINB BNYG DJFJ SWAP DSKH ZLVH OFZW DQJB UXEA UQSX
PGST NIQC QXOB SURK PSXZ AHNI YPHF ZQBB RSKR SQBY
DBKL MDQZ QYOM TMRW BUHM
```

The solution is the last word of the plaintext, without blanks. Use only capital letters. The plaintext is in English.
Additional files: RHV-TABLES.zip (25 bigram substitution tables)

Sources

[1] www.enigma.hoerenberg.com

[2] en.wikipedia.org/wiki/Reservehandverfahren