MysteryTwister C3

THE CRYPTO CHALLENGE CONTEST

Flawed Usage of a OTP Cipher by the BND

Author: Jörg Drobick

June 2015 (Update September 2015, thanks to Bart13)

Introduction (1/2)

During the cold war (more specific from the 1960s to 1989) the foreign intelligence agency of Germany (BND) established so-called stay-behind units, whose task was to let themselves be overrun in case of war (German: Überrollagenten). Radio messages were encrypted with a method that first changes the plaintext into a numbertext (series of digits) using a substitution matrix, and then encrypts this text with a one-time pad (OTP). The OTP is a symmetric encryption system that is theoretically secure and cannot be broken if used correctly.

First, the key sequences of this cipher were called worm rows, then in the 1980s they were called OTP too: The key taken out of these sequences must have the same length as the numbertext. For the security of the OTP method it is essential that once a OTP key is used, it must not be used a second time.

Introduction (2/2)

The stay-behind agents of the BND initially got a great number of keys, but after 10 years the very same key tables were given out anew, which corrupted the security of the method and let some specific phrases of the radio messages become public.

This challenge is about the effect on the security by using the same OTP more than once.

Remark: The 'scheme' of the substitution table is the same in GRANIT and in this cipher, and the used alphabet contained 28 characters in each case. The differences were: The BND always used the same table ('DEIN STAR' for German, and 'ZA OWIES' for Polish speaking agents), the characters weren't exactly the same, and for GRANIT the text was shortened through substitution by a codebook before performing the substitution with the table.

The Method (1/3)

In this OTP method, at first the plaintext is changed into a numbertext with a substitution table. Before that we substitute every German umlaut with its 2 letters, every ’ß’ with ’ss’, and ’ ?’ with ’..’. Digits in the plaintext will be tripled to mark them (e.g. 13 –> 111333). Additionally, specfic abbreviations are used just as in the original radio messages (details on page 10).
The used substitution table is the standard table ’DEIN STAR’:

	0	1	2	3	4	5	6	7	8	9
	D	E	I	N			S	T	A	R
4	B	C	F	G	H	J	K	L	M	O
5	P	Q	U	V	W	X	Y	Z	.	,

At the end of every radio message as much zeros are added as we need to make the number of digits divisible by 5.

The Method (2/3)

For encrypting, the first unused row of the OTP is chosen. The first column of that row is the so-called key-id (German: Kenngruppe), which is not used for encrypting and marks the starting point for the key. Out of the given sequence we use as key a sequence of the same length as the numbertext. For example, if somewhere we have the sequence '34901 35728 94503...' and the key-id is '35728', the key starts with '94503 ...'.

Every radio message is divided into groups of 5 digits. The first group contains the 3-digit long agent number of the receiver and the 2-digit long length of the message (= number of groups without the first group).
The second group is the key-id as explained earlier, and the rest of the groups form the actual radio message which has to be decrypted.

The Method (3/3)

Now we encrypt the numbertext by subtracting the individual digits of the key from the ones of the text modulo 10.
For example, if we have the numbertext '43789 56371' and the key '94503 20754' we get the ciphertext as follows:

```
      43789 56371
  -   94503 20754
  ---------------
      59286 36627
```

In this case the radio message will be '00703 35728 59286 36627', where 007 is the agent number and the actual message contains three groups of 5 digits.

Challenge Description (1/3)

Five radio messages with identical key-ids were picked up, which obviously all use the same OTP as key. Your task is to compute the OTP and recover the plaintext, for which you need at least 2 of the radio messages. The remaining ones can be used for validation. As solution, please submit the first four words of the first message in capital letters and without spaces or special characters.

```
Message 1:
053 22 15315 04033 19214 20480 74981
       27315 65785 20716 39434 71296
       73709 75909 67278 47474 32995
       00346 87146 93088 40907 97538
       17065 57315
```

Challenge Description (2/3)

```
Message 2:
054 19 15315 21830 98123 55553 83124
       00474 58915 17766 49433 66222
       19796 75085 17136 66603 91776
       51453 67788 52081 59513

Message 3:
055 19 15315 90139 70834 82108 27106
       09336 29097 78330 66017 51684
       24404 30034 60797 44547 75368
       64089 68508 90813 40903
```

Challenge Description (3/3)

```
Message 4:
056 29 15315 90813 17044 96901 31052
       34252 14724 87019 31816 47156
       55061 96603 79652 51353 22125
       42474 82732 03897 47267 06763
       10653 14883 38505 58261 30818
       26309 71271 39789 57800

Message 5:
171 17 15315 06114 64556 92268 10164
       46517 27034 95833 12707 33877
       01696 01235 62306 06671 62688
       02348 38550 09390
```

Hints

Because the OTP was used multiple times the radio reconnaissance and the decrypting service of the former GDR found out the following phrases which appeared in the messages:

- Brief 4 öffnen/ausfüllen/nächsten Treff übergeben
- Gezeichnet: „Zentrale/Führung/Ihr Betreuer“
- Frequenzen: 3638/4115 kHz
- Aktionstrupps
- (TRO) Treffort
- (NTR) Neutraltreff
- (ATRO) Ausweichtreffort
- „das Ost-West-Verhältnis ist so gespannt, dass in Kürze mit Angriffshandlungen des Warschauer Pakts gerechnet werden muss, deshalb alle Geräte und Schalteinrichtungen auf Brauchbarkeit überprüfen“
- „Handeln Sie weiter nach Auftrag . . . “
- „Freuen uns, dass Sie die Situation gut überstanden haben, Dank für Verbindungsaufnahme.“

Links

- https://en.wikipedia.org/wiki/Bundesnachrichtendienst
- Website with nearly all codes and encryption mechanisms used in the former GDR (only German): http://scz.bplaced.net/m.html#bndotp
- Challenges zum Thema GRANIT: https://www.mysterytwisterc3.org/en/challenges/level-ii/double-column-transposition-GRANIT-part-1