MysteryTwister C3

SIGABA CSP-2900 – Part 1

Author: Nils Kopal
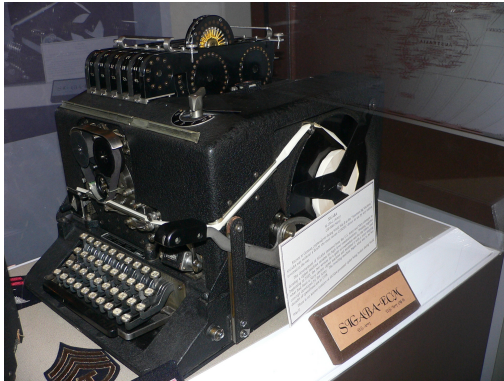
July 2021

SIGABA Encryption Machine

Figure: SIGABA at the National Cryptological Museum – Fort Meade, USA – Source: Wikipedia

Introduction (1/2)

The SIGABA is an electromechanical encryption device used by the US during WWII and in the 1950s. Also known as ECM Mark II, Converter M-134, as well as CSP-888/889, the SIGABA was considered highly secure, and was employed for strategic communications, such as between Churchill and Roosevelt.

The model CSP-888/889 (Navy name) was later adjusted and then called CSP-2900. This series of challenges deals with the modified version CSP-2900.

Introduction (2/2)

The SIGABA encrypts and decrypts with a set of five rotors, and implements irregular stepping, with two additional sets of rotors generating a pseudo-random stepping sequence. Its full keyspace, as used during WWII, was in the order of $2^{95.6}$. It is believed that the German codebreaking services were not able to make any inroads into the cryptanalysis of SIGABA.

A functional description of the SIGABA is given in the additional zip file, as well as a simulator, and a method for cryptanalysis.

Challenge (1/2)

This challenge is part of a series of challenges with SIGABA CSP-2900. In this challenge, you need to recover the plaintext from a ciphertext (320 characters) and a known-plaintext fragment (120 characters). The rotor selection, order, and orientation, as well as the starting position of the rotors are unknown.

The solution to this challenge can be found at the end of the (unknown) plaintext between two "X".
Example plaintext: "XONETWOX" $\rightarrow$ Solution: "ONETWO".
Please enter the solution without any spaces.

Challenge (2/2)

The ciphertext:

```
EXRQOQQZCVOFMDSTYEMELWOBZLTYJPLRCUJYMGXOTNAKIQUTAVMUZ
COZYOWSVFIHPVLWEIPOCAIMUOYQKMZITFSJSHQQHZTZOWZOIDUXIE
OARMSOMUAQPCAKWGFWALGGYFYAHAWJRIBSIEIEUFYRBKREEDJYCZN
IKELWTCZEJDLQVXFYNMYFFOYQDDNLDZMTKSFQXTXLBQWJAXTECFNF
PJOPTQKUORLQNYUPYUFTPSCRVPZWDXZPNNKKCAJSCCOKOVXNMXEZX
WEMDRPUGGYOZTCNWTWQIGQKMAVRZANVBVBYTFNAMBOKBLWMKJEUVA
KX
```

The plaintext starts as follows:

```
SIGABAWASSIMILARTOTHEENIGMAINBASICTHEORYINTHATITUSEDA
SERIESOFROTORSTOENCRYPTALLLETTERSOFTHEPLAINTEXTINTOAD
IFFERENTLETTER
```

Author: Nils Kopal

MysteryTwister C3
THE CRYPTO CHALLENGE CONTEST

Additional Files

The attached zip file includes:

1. Sigaba.java + Sigaba.jar
   - ➡ Java source code and according executable of a simulator, used to create the challenges
2. README.txt
   - ➡ text file with instructions to run the simulator
3. sigaba_funcational.pdf
   - ➡ a paper describing the device