MysteryTwister C3

THE CRYPTO CHALLENGE CONTEST

The SIGABA Challenge – Part 1

Author: George Lasry

February 2020

SIGABA Encryption Machine

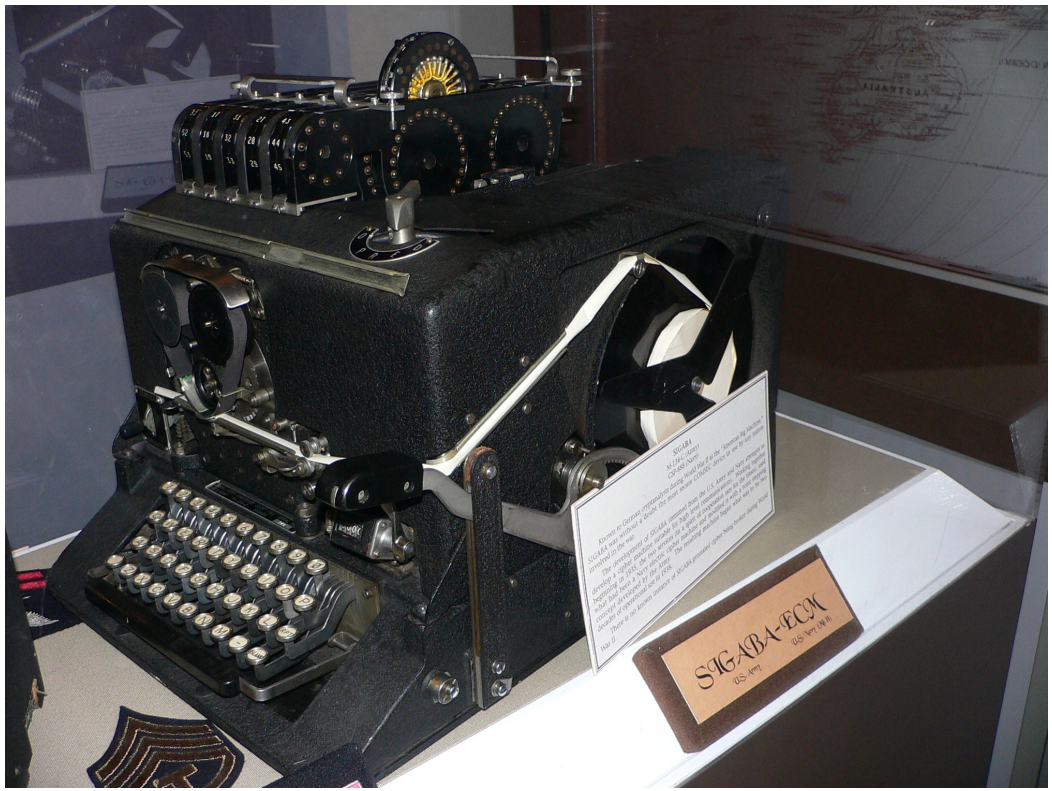

Figure: SIGABA at the National Cryptological Museum – Fort Meade, USA – Source: Wikipedia

Introduction

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 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. In this challenge, you need to recover the plaintext from a ciphertext and a partial crib (a known-plaintext fragment). The rotor selection, order, and orientation are unknown. The starting position of some of the rotors is known, as follows:

- All *cipher* and *control* rotors are at position A.

The plaintext was extracted from Shakespeare writings. It consists of the concatenation of two plaintext segments, extracted from different places. The first segment, with 100 letters, is given as a crib. The letter Z is used to represent a space.

The answer to the challenge are the last 10 letters of the full plaintext (including Z-placeholders, in capital letters).

Challenge (2/2)

The ciphertext:

```
GSZQEMAGFULNFZHHRVUTCUEXUFBMPDGOROJRPMAUDOZMJWJCVH
YCBZDELOWKVLYJLSZBQJXWXLRWOIMBVUTBAVRHPPPYQDTIURLV
IQGIZSEVGXOYCMGESFOXDLPFTUQQCRDSRNFDTBDDULFJKQGXZB
XKKIMSBSIUZSZNOOLCFRRVTODXFQRRXLDEMSLORKXUCGDKCZKY
ULDORUGEGDLTTROBUIVWJTBVHYWOKANYJCGQUYGPHSMWJRILZP
SQJOXKKMEGMWQKXWVKF
```

The plaintext starts as follows:

```
AHZFOULZSHREWDZNEWSZBESHREWZTHYZVERYZHEARTZIZDIDZN
OTZTHINKZTOZBEZSOZSADZTONIGHTZASZTHISZHATHZMADEZME
```

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. HistoCrypt-2019-SIGABA.pdf
   ➥ a paper describing the device and a new known-plaintext attack