MysteryTwister C3

THE CRYPTO CHALLENGE CONTEST

SIGABA – PART 2

Author: Mark Stamp

October 2010

Sigaba Encryption

The Sigaba machine was the American counterpart of the German Enigma machine in World War 2. But in contrast to the Enigma no successful attack on the Sigaba was conducted during its service lifetime.
The used system of rotors and wirings was far more complex than that of the Enigma.

The effective key space of the Sigaba has $2^{95.6}$ possible keys and even nowadays attacks can not significantly reduce this key space. But it has to be mentioned that the full key space only was used within the POTUS-PRIME communication, between the American president and the British prime minister. (POTUS $\hat{=}$ President Of The United States, PRIME $\hat{=}$ PRIME Minister)

Challenge

Decrypt the ciphertext (*lincolnCipher.txt*) which was encrypted with the Sigaba cipher. It can be found in the zip-archive for this challenge (*mtc3-stamp-06-sigaba2.zip*). Furthermore, there is a piece of known plain text (*lincolnInitPlain.txt*) in the archive.

An implementation of the Sigaba-Encryption can be found in the zip-archive as well (*Sigaba_code.zip*).
Note, that the full key space of $2^{95.6}$ was used in the given challenge.

Challenge

The solution for this challenge consists of the order of the 15 rotors (5 chipher , 5 control and 5 index rotors), the orientation of the 5 cipher and the 5 control rotors (0 means forward, 1 means reverse) and the initial settings of all of the 15 rotors.

If the rotors would be ordered *0,1,2,3,4,5,6,7,8,9,0,1,2,3,4*, all the cipher and control rotors would turn forward, the cipher and control rotors would all be initiated with *A* and the index rotors with *0*, the key would be:
012345678901234000000000AAAAAAAAAA00000.