MysteryTwister C3

THE CRYPTO CHALLENGE CONTEST

Sigaba – Part 1

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 but for this challenge a part of the key is known. It is known, that the initial settings of the 5 cipher rotors is **ABCDE** and the one of the 5 control rotors is **ZYXWV**. Furthermore the order of the 5 index rotors is **01234** and the first index rotor is initialised with **4**.

Challenge

Decrypt the ciphertext (*WWIIcipher.txt*) which was encrypted with the Sigaba cipher and can be found in the zip-archive for this challenge. Furthermore there is a piece of known plain text (*WWIIinitPlain.txt*) in the archive as well an an implementation of the Sigaba-Encryption (*Sigaba_code.zip*).

The solution for this challenge consists of the order of the 5 chipher and the 5 control rotors, the orientation of the 5 cipher and the 5 control rotors (0 means forward, 1 means reverse) and the initial settings of the remaining 4 index rotors.

If the cipher and control rotors would be ordered *0,1,2,3,4,5,6,7,8,9*, all the cipher and control rotors would turn forward and the remaining 4 index rotors would be intialised with *6*, the key would be: **01234567890000000006666**.