MysteryTwister C3

THE CRYPTO CHALLENGE CONTEST

Typex – Part 2

Authors: Kelly Chang, Richard M. Low, Mark Stamp

April 2013

During World War II, the British used a cipher machine known as Typex that was based on the commercial version of the Enigma cipher [1].

Please refer to the first part of this challenge for an explanation of the functionality of the Typex cipher.

Challenge

Here we assume that one new rotor is used but you (the cryptanalyst) do not have physical access to the rotor. Your goal is to recover the wirings of this unknown rotor using a known-plaintext attack. To slightly simplify the attack, we assume that the key is known, the wirings of all other rotors/stators are known, and the rightmost (i.e., fast) rotor is the unknown rotor. Consequently, the only unknown is the wiring of the rightmost rotor. In terms of the simulator, the key used to generate the ciphertext was

```
01834 00000 AAAAA
```

where rotor "8" represents the new (unknown) rotor.

Your challenge is to determine the wiring (i.e., permutation) of this mysterious new rotor. Give your answer in the same format as the rotor wirings that appear in the simulator (see the array "`rot`" in the `Typex.c` simulator). For example, the identity rotor is denoted

```
ABCDEFGHIJKLMNOPQESTUVWXYZ
```

As another example, the rotor

```
YSDZTFOWPLCUXNJIHBEGAVQRMK
```

indicates that, in the forward orientation, the rotor maps the letter `A` to `Y`, the letter `B` to `S`, the letter `C` to `D`, and so on.
For this challenge, the relevant pair of plaintext and corresponding ciphertext is contained in the files

```
alicePlain.txt and aliceCipher9.txt
```

respectvely.

References

[1] M. Stamp and R. M. Low, *Applied Cryptanalysis: Breaking Ciphers in the Real World*, Wiley-IEEE Press, 2006

[2] http://en.wikipedia.org/wiki/TypeX

[3] http://www.cryptomuseum.com/crypto/uk/typex/index.htm