MysteryTwister C3
THE CRYPTO CHALLENGE CONTEST

Enigma Messages with Repeated Letters – Part 3

Author: George Lasry

February 2014

Introduction

This series of Enigma challenges is about messages which contain only repeated single letters ("GG") or repeated groups of letters (like "ALPHAALPHA"), encrypted by the Enigma I, which uses 3 rotors selected out of 5.

The challenges are of an increasing level of difficulty, the easiest is pen-and-paper only, others may be solved using existing tools, the most difficult one may require programming and/or special adaptations of existing tools or software code available on the Internet.

Challenge

The attached ciphertext is the result of encrypting a plaintext message consisting of repeating the same pair of letters.
The original message could have been
ABABABABABABABABABABABABABABABABABABABABAB.

It is known that reflector B was used, the rotor order was 145, the ring settings were ABC, and no Steckerboard plugs were used.

You need to provide the Message Key settings (the rotors starting positions), first the left, then middle, then right value, in capital letters. E.g. UKG – if U is the starting position of the left rotor (Rotor #1), K is the starting position of the middle rotor (Rotor #4), and G is the middle position of the right rotor (Rotor #5).

Hint

This challenge can be solved using the open-source program CrypTool 2.

Useful links

- A general description of the Enigma and successful attacks in WWII:
  http://en.wikipedia.org/wiki/Enigma_machine
- Another informative site about the Enigma and its internal functioning:
  http://users.telenet.be/d.rijmenants/en/
- An Enigma simulator:
  http://users.telenet.be/d.rijmenants/en/enigmasim.htm

Useful links

- Ideas (and code) for cryptanalysis of the Enigma using modern methods: http://practicalcryptography.com/cryptanalysis/breaking-machine-ciphers/cryptanalysis-enigma/
- An Enigma breaking software for Windows and Linux (C source code available): http://www.bytereef.org/enigma-suite.html
- Open-source program for Windows that allows for the cryptanalysis of Enigma messages: http://www.cryptool.org/en/cryptool2-en