MysteryTwister C3

THE CRYPTO CHALLENGE CONTEST

Enigma Messages with Repeated Letters – Part 2

Author: George Lasry

October 2013

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 letter with an Enigma machine.

It is known that Reflector B was used, the Rotor order was 145, the Ring settings were CEN, and 10 Steckerboard plugs were used. Therefore, only 6 letters are not "steckered".

You need to provide the Message Key settings (the rotors starting positions) from left to right, 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 initial position of the right rotor (Rotor #5).

Hints

1. The ciphertext is the same as in the first part of this series.
2. This challenge could be solved in two phases. For the second phase, one of the tools mentioned below could be helpful.

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
- Ideas (and code) for cryptanalysis of the Enigma using modern methods:
  http://practicalcryptography.com/cryptanalysis/breaking-machine-ciphers/cryptanalysis-enigma/

Useful links

- An Enigma breaking software for Windows and Linux (C source code available): `http://www.bytereef.org/enigma-suite.html`
- Description of the Turing Bombe: `http://www.ellsbury.com/bombe1.htm`