TURING BOMBE ENIGMA I

Author: Michael Hoerenberg

October 2011

You intercepted two ENIGMA I messages. Both messages date from the same day. Intelligence services told you the initial plaintext of the first message: FROMXHEADQUARTERXTOX

The message header contains: the date, the number of characters, the rotor position to decipher the message key and the encrypted message key. The first 5 characters of a message are the so called indicator group. The indicator group does not contain any plaintext, instead it identifies the message.

Use a TURING BOMBE to find out the ENIGMA key of the day and decipher the second message. To solve this challenge send us the complete plaintext of the second message (only upper-case characters, no blanks).

Hint

The key of the day contains the reflector, the rotor order, the rings and the plugs.

Don't worry about the ring position. The ring position doesn't matter (AAA). Reflector B.

The messages

First message:
05.10.2011 - 171 - OKF VMI -
KHLPTWOXKCMSHXKPTKKOZWSYDRJCBLYKFPUQYLO
JNTOJLPPUKMJQPZWARLVQJDRMXDTBVQQNJHYZCK
WGLOGUPJOLPWXYOUPNDWHNGBXLKSSSAVXHDJLSN
TLPLOGPLGIMZPRPHTFWQLBMGYGYJYNLXVGSMQQW
OLKWNBUNNIGVSSI

Second message:
05.10.2011 - 14 - ABC DUO -
YFVBNVUWNIXBNP

Links

http://www.ellsbury.com/bombe1.htm

http://en.wikipedia.org/wiki/Bombe

http://users.telenet.be/d.rijmenants/en/enigmasim.htm

http://frode.web.cern.ch/frode/crypto/Shaylor/bombeapp.html