

MysteryTwister C3

THE CRYPTO CHALLENGE CONTEST

THE THIRD ENIGMA M4 MESSAGE

Author: Michael Hoerenberg

September 2011

In 2006 the so-called "M4 Message Breaking Project" [1] under the direction of Stefan Kraus aimed at decrypting three ENIGMA-M4 messages from the time of World War II.

This variant of the ENIGMA was used from 1942 on to communicate with German submarine boats [2]. Because of the huge key space of the ENIGMA-M4 (equivalent to a 86 bit binary key) the calculations were distributed on many participants in the World Wide Web.



ENIGMA-M4 [3]

Within the first days after the project was launched, there was the first report of success: After more than 60 years a message by lieutenant commander Hartwig Looks (U264) was decrypted. Just a few weeks later, the second message was decoded. This success caused a stir in professional circles.

Up to now, it has not been possible to decrypt the third message. The project has been discontinued.

It is your task to decrypt the third message.

The third message

APPENDIX II (continued), TO THE COMMANDING OFFICER, H.M.S.
HURRICANE'S
No. 110/S, DATED 25TH NOVEMBER, 1942.
TEXTS OF SIGNALS READ

CLXP LWRU HCEY ZTCS OPUP PZDI UQRD LWXX FACT TJMB HDVC JJMM ZRPY IKHZ
AWGL YXWT MJPQ UEFS ZBCT VRLA LZWX VXTS LFFF AUDQ FBWR RYAP SBOW JMKL
DUYU PFUQ DOWV HAHC DWAU ARSW TXCF VOYF PUFH VZFD GGPO OVGR MBPX XZCA
NKMO NFHX PCKH JZBU MXJW XKAU OD?Z UCVC XPFT CDXP LWRU VA

T.O.R.1152/19/221 (53 GROUPS).

Source: [4]

References

[1] http://www.bytereef.org/m4_project.html

[2] [http://en.wikipedia.org/wiki/M4_\(cipher\)](http://en.wikipedia.org/wiki/M4_(cipher))

[3] <http://de.wikipedia.org/wiki/Enigma-M4>

[4] <http://members.fortunecity.com/jpeschel/erskin.htm>