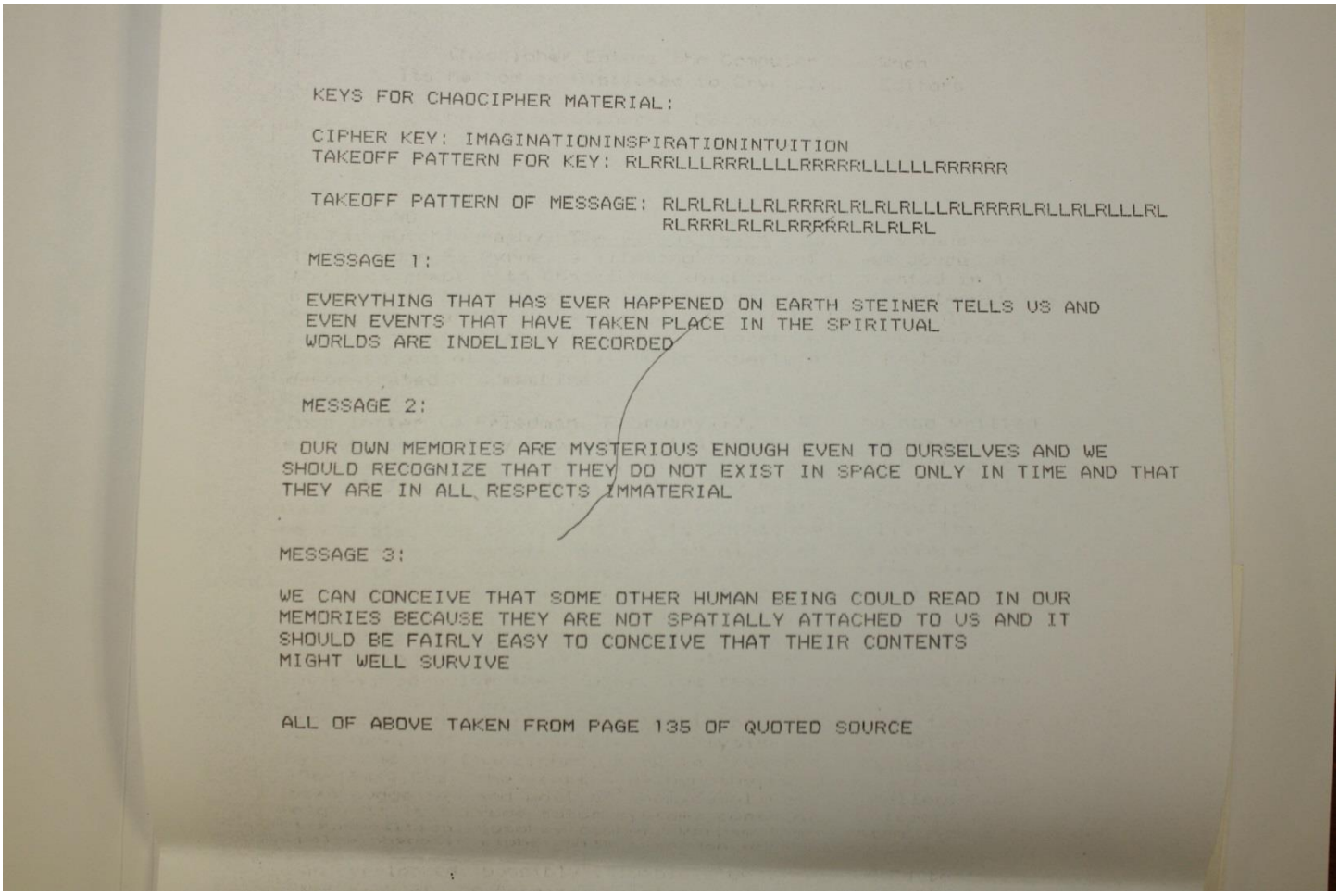
Chaocipher: Exhibit 5 Solution
by Jeff Calof
(3/22/14)



KEYS FOR CHAOCIPHER MATERIAL:

CIPHER KEY: IMAGINATIONINSPIRATIONINTUITION
TAKEOFF PATTERN FOR KEY: RLRRLLLRRRLLLLRRRRRLLLLLLRRRRR

TAKEOFF PATTERN OF MESSAGE: RLRLRLLLRLRRRRLRLRLRLLLRLRRRRLRLLRLRLLLRL
RLRRRLRLRLRRRRRLRLRLRL

MESSAGE 1:

EVERYTHING THAT HAS EVER HAPPENED ON EARTH STEINER TELLS US AND
EVEN EVENTS THAT HAVE TAKEN PLACE IN THE SPIRITUAL
WORLDS ARE INDELIBLY RECORDED

MESSAGE 2:

OUR OWN MEMORIES ARE MYSTERIOUS ENOUGH EVEN TO OURSELVES AND WE
SHOULD RECOGNIZE THAT THEY DO NOT EXIST IN SPACE ONLY IN TIME AND THAT
THEY ARE IN ALL RESPECTS IMMATERIAL

MESSAGE 3:

WE CAN CONCEIVE THAT SOME OTHER HUMAN BEING COULD READ IN OUR
MEMORIES BECAUSE THEY ARE NOT SPATIALLY ATTACHED TO US AND IT
SHOULD BE FAIRLY EASY TO CONCEIVE THAT THEIR CONTENTS
MIGHT WELL SURVIVE

ALL OF ABOVE TAKEN FROM PAGE 135 OF QUOTED SOURCE

The photograph above is of the actual, printed document prepared by Prof. Cipher Deavours and Louis Kruh (with John Byrne) as found in the donated Byrne Family files at the National Cryptologic Museum in Ft. Meade, MD.

Exhibit 5 was published in Cryptologia Volume 14, Issue 3, 1990 in the article “Chaocipher Enters the Computer Age when its Method is Disclosed to Cryptologia Editors”. It was comprised of 3 distinct messages, all which were stated to be taken from Stewart C. Easton’s book, *Rudolf Steiner: Herald of a New Epoch*:

MESSAGE 1:

MHRMC DEGBC WWQFN SDDQC UJHYH YNPYT QCXVR CSFUX QZZLH VVWIV SBFDF
QGEXV NXEAN SDEJF RVKYA RVRED QDEKZ QENIL QXVEV DXBZP URCQY QSHYY
VPLXP IKMGX Q

MESSAGE 2:

ENWSC EAQGI VIDEM WUMSN ZMNTV UFDLB JKKMR HHSNB KTJBH VPTWH FMQQJ
PGRWF FVJMD HFUZO XEOZT MKZSA MJYRL SQSXU ZYEKR JBFRE SGGFX FEGXL
PWTWL ZAVIM TBDTQ BLVRZ VEMMT LXITZ

MESSAGE 3:

JZHAS QNRTK TTLZD YOWLN VDMWN YHSMG XJMGZ QTHRI WTIFL XYHTK BOXUY
EANJU DXNVO GFZHM JEGRD GGPUG SXVBA CBEPK WHVSB IJGOH KVKAI BBNKF
HFFLS FMIIN TTXJX UHWQA PTSNB TBBNK FUCBP IONQS MVEHU XTLMR RA

As confirmed by Jeff Calof, the three plaintext messages in the NCM document exactly match the respective number of ciphertext letters in each of the three Exhibit 5 messages as found on Page 135 of the Easton's book. Moshe Rubin successfully set-up the starting Plaintext & Ciphertext Alphabets following the Cipher Key and its Takeoff Pattern Key.

Moshe also generated the accurate ciphertext for each message by following the "Takeoff Pattern of Message". It was discovered that for Messages 1 & 2, their respective published ciphertexts in Cryptologia contained transcription errors:

In Message 1, at letter position 82, the accurate ciphertext letter should be "O"… but was published as the ciphertext letter "D".

MESSAGE 1:

MHRMC DEGBC WWQFN SDDQC UJHYH YNPYT QCXVR CSFUX QZZLH VVWIV SBFDF
QGEXV NXEAN SDEJF RVKYA RVRED Q**D**EKZ QENIL QXVEV DXBZP URCQY QSHYY
VPLXP IKMGX Q

In Message 2, there were two transcription errors. At letter position 11, the accurate ciphertext letter should be "U"… but was published as the ciphertext letter "V". At letter position 13, the accurate ciphertext letter should be "O"… but, as with Message 1, was published as ciphertext letter "D".

MESSAGE 2:

ENWSC EAQGI **V**I**D**EM WUMSN ZMNTV UFDLB JKKMR HHSNB KTJBH VPTWH FMQQJ
PGRWF FVJMD HFUZO XEOZT MKZSA MJYRL SQSXU ZYEKR JBFRE SGGFX FEGXL
PWTWL ZAVIM TBDTQ BLVRZ VEMMT LXITZ

The result of these transcription errors is that anyone trying to decipher the two Messages would have only gotten a partially accurate plaintext solution. It is not known how the transcription errors arose, though the most likely cause was determined to be a result of the printout itself. Created on an Impact Printer (likely Deavours's), the letters "O" and "D", as well as "U" and "V", are nearly indistinguishable to the naked eye. Whomever was creating the final Cryptologia proof for the Exhibit 5 article (back in 1990) likely misinterpreted these letters from the submitted draft; or, the submitted draft itself already contained these same errors which carried over into the proof and ultimately into publication.

What seems certain is that neither Deavours nor Kruh verified the draft, proof, or published ciphertext for accuracy by attempting their own decipherment. If this had been done (as Moshe Rubin discovered), they would have quickly realized the error and made the correction.

For further details and a complete overview of Exhibit 5, see the article "Chaocipher Exhibit 5: History, Analysis, and Solution of Cryptologia's 1990 Challenge" by Jeff Calof, Jeff Hill, and Moshe Rubin in Cryptologia Volume 38, Issue 1, 2014 at http://www.tandfonline.com/toc/ucry20/current.