Chaocipher: Exhibit 6
by Jeff Calof[1] & Moshe Rubin[2]
(6 January 2015)[3]

The Chaocipher timeline has, until now, reflected five distinct "Exhibits", or challenge messages. The first four Exhibits were created by John F. Byrne and presented in the final chapter of his autobiography *Silent Years: An Autobiography with Memoirs of James Joyce and Our Ireland.* Byrne's Exhibits were unique for a challenge message as they didn't ask for a decipherment to plaintext (except for a singular short phrase). Rather, Byrne provided all the plaintext and challenged his readers to determine his encipherment method used to create the ciphertext. His challenge was never solved and the solutions to his four Exhibits, i.e. the encipherment schema used, remained a mystery for Exhibits 1 & 4 until 2010 (following the donation of Byrne's materials to the National Cryptologic Museum (NCM) by his daughter-in-law, Patricia Byrne, and the publication of the classic Chaocipher algorithm by Moshe Rubin).

The encipherment schemas for Exhibits 2 & 3 were also part of the donated materials. Jeff Calof discovered Byrne's hand-written notes for those Exhibits on a visit to the NCM in May, 2013 but, as they were not clearly laid out, the mystery continued until Esa Peuha independently arrived at the solution (which differed from the algorithm used for Exhibits 1 & 4) and published his results in October, 2013.

Chaocipher Exhibit 5 had a different genesis. Cryptologia founding editors Louis Kruh and Prof. Cipher Deavours met with John Byrne (son of Chaocipher creator John F. Byrne) in 1989 and were the first verified non-family individuals to learn the classic algorithm in nearly 35 years. Though unable to reveal the encipherment schema due to a non-disclosure agreement, they published a set of 3 challenge messages as Exhibit 5 in their article ''Chaocipher Enters the Computer Age When its Method is Disclosed to *Cryptologia* Editors,'' *Cryptologia*, 14(3):193–197. Unlike the first four Exhibits, the messages of Exhibit 5 divulged no plaintext though Kruh and Deavours did identify their source material. This too went unsolved for 23 years until Jeff Calof found their solution document at the NCM containing the plaintext along with their takeoff\keying patterns and encipherment algorithm (a variant of Byrne's). With co-authors Moshe Rubin and Jeff Hill, he published the article "Chaocipher Exhibit 5: History, Analysis, and Solution of *Cryptologia's* 1990 Challenge", *Cryptologia*, 38(1):1-25.

With the five known Chaocipher Exhibits all in the "solved" column, it would seem that Byrne's Chaocipher has exhausted its mysteries. Yet such is not the case, for along with the Kruh and Deavours's solution document for their *published* Exhibit 5, an earlier draft article (never published) with an entirely separate set of challenge messages was discovered at the NCM. Also written by Kruh and Deavours, it differs markedly from the Exhibit 5 they eventually presented in *Cryptologia*. As an homage to, and continuation of, the Chaocipher timeline Calof, Hill, and Rubin have christened it going forward as "Exhibit 6".

Beginning with three short explanatory paragraphs (with numerous misspellings of Byrne's name), it then leads into a list of 50 short "in-depth" encipherments, each about 25-30 characters in length. By comparison, the published Exhibit 5 consists of three "in-depth" encipherments running from 121 to 162 characters. Unlike the discovered solution document for the published Exhibit 5, this document does not provide the keyword, takeoff patterns, or encipherment schema used for the 50 rows, nor does it provide its plaintext source.

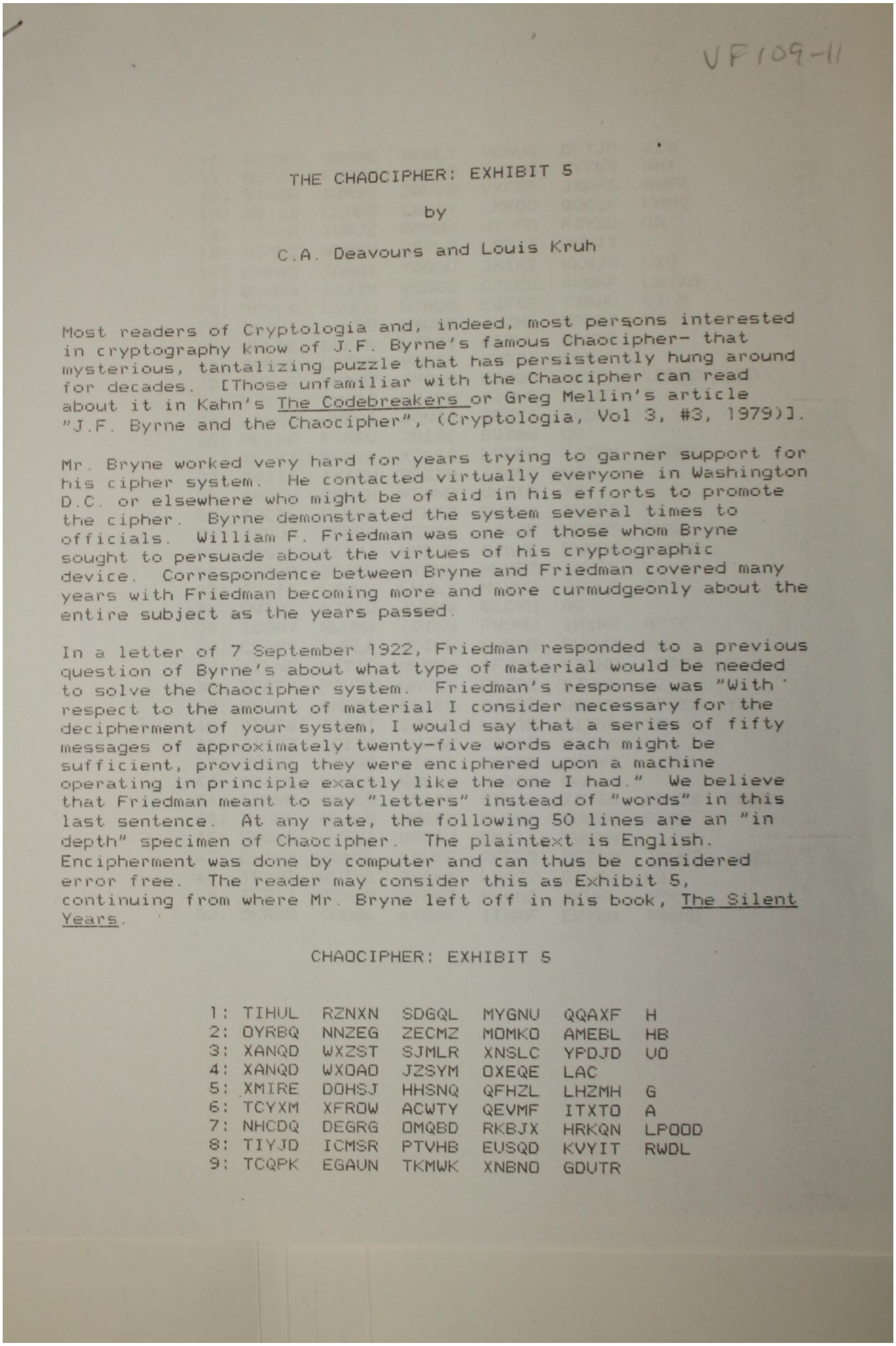
The following photographs are of the actual, printed documents prepared by Lou Kruh and Prof. Cipher Deavours as found in the donated Byrne Family files at the National Cryptologic Museum in Ft. Meade, MD. Take note that certain letters (e.g., D & O or U &V) may appear nearly identical to the naked eye.

[1] Jeff Calof's email address: jcalof@yahoo.com

[2] Moshe Rubin's email: mosher@mountainvistasoft.com

[3] This paper can be found at http://www.chaocipher.com/chaocipher-024.htm

As was discovered with the published Exhibit 5, in several instances those letters were juxtaposed between the printed output and the Cryptologia publication. The “VF 109-11” in the upper-right corner is not by Kruh and Deavours but the NCM’s own marking reflecting their filing system.



VF109-11

THE CHAOCIPHER: EXHIBIT 5

by

C.A. Deavours and Louis Kruh

Most readers of Cryptologia and, indeed, most persons interested in cryptography know of J.F. Byrne's famous Chaocipher- that mysterious, tantalizing puzzle that has persistently hung around for decades. [Those unfamiliar with the Chaocipher can read about it in Kahn's The Codebreakers or Greg Mellin's article "J.F. Byrne and the Chaocipher", (Cryptologia, Vol 3, #3, 1979)].

Mr. Bryne worked very hard for years trying to garner support for his cipher system. He contacted virtually everyone in Washington D.C. or elsewhere who might be of aid in his efforts to promote the cipher. Byrne demonstrated the system several times to officials. William F. Friedman was one of those whom Bryne sought to persuade about the virtues of his cryptographic device. Correspondence between Bryne and Friedman covered many years with Friedman becoming more and more curmudgeonly about the entire subject as the years passed.

In a letter of 7 September 1922, Friedman responded to a previous question of Byrne's about what type of material would be needed to solve the Chaocipher system. Friedman's response was "With respect to the amount of material I consider necessary for the decipherment of your system, I would say that a series of fifty messages of approximately twenty-five words each might be sufficient, providing they were enciphered upon a machine operating in principle exactly like the one I had." We believe that Friedman meant to say "letters" instead of "words" in this last sentence. At any rate, the following 50 lines are an "in depth" specimen of Chaocipher. The plaintext is English. Encipherment was done by computer and can thus be considered error free. The reader may consider this as Exhibit 5, continuing from where Mr. Bryne left off in his book, The Silent Years.

CHAOCIPHER: EXHIBIT 5

```
1: TIHUL  RZNXN  SDGQL  MYGNU  QQAXF  H
2: OYRBQ  NNZEG  ZECMZ  MOMKO  AMEBL  HB
3: XANQD  WXZST  SJMLR  XNSLC  YPDJD  UO
4: XANQD  WXOAO  JZSYM  OXEQE  LAC
5: XMIRE  DOHSJ  HHSNQ  QFHZL  LHZMH  G
6: TCYXM  XFROW  ACWTY  QEVMF  ITXTO  A
7: NHCDQ  DEGRG  OMQBD  RKBJX  HRKQN  LPOOD
8: TIYJD  ICMSR  PTVHB  EUSQD  KVYIT  RWDL
9: TCQPK  EGAUN  TKMWK  XNBNO  GDUTR
```

```
10:  BCQXD   OGMPE   MKBLT   YUAUQ   DPTJR   JZH
11:  MSQEJ   KMEYK   JQSXG   QJDHB   YYEKQ   NHX
12:  YIMEH   ZZRVC   ZAHYZ   VYFZP   JXAFS   GQFE
13:  DVIIX   LLUBE   LWWQY   LMFOD   QQCSK   KHMQ
14:  TPUSB   SWAJZ   SPMBH   HTSFO   RXYED   DA
15:  SYMEZ   WGNPH   QEPLZ   LSZIT   DPYIT
16:  KMPNS   TOABI   TQGSU   JMXRZ   KKNJN   UXV
17:  DVHPA   XKJZN   VSDCQ   CJLEG   AWONP   LNIXG
18:  TCYCS   WGOOH   UJRDB   EGFXP   TTRHU   CJLY
19:  TLQYI   LXKSU   WMWAE   JUZHI   WPQNT   TI
20:  OKLAE   CKPKN   LTSGY   AISUL   NIFFR   Y
21:  DVRHS   LOCDS   VJQXC   FPAZT   OFV
22:  DVINE   VMEMJ   JMCFR   OJMQH   HBVGV   LCBGD   LBD
23:  VISSL   XWQIE   DRIPN   MZONC   OWNMT   Y
24:  JISRX   QMPQI   QGNSJ   GDZFQ   MEDKC
25:  OKLNC   FSRRC   ZRIRC   BWXBW   CO
26:  TPZEY   GGMVA   XZKSQ   LYBEB   TXTRM   YEDHK
27:  DVIIX   IXIPH   BPZXQ   XTMBG   NEQ
28:  AHPEV   CEUYH   RTANP   GKZIR   TS
29:  TCCTS   OLEBN   BFHID   BURNI   IVPPZ   UC
30:  JISUA   CDUPG   EZPKS   VXUOE   VWBBS   BVSA
31:  SYGYE   ZEEJJ   VGBYF   BJGNC   BMNRU   XQPUN
32:  TCRBD   XCAPM   NTPHK   HKNFZ   JNHIK   L
33:  DVIIX   LKBKH   LUJLY   NIVOY   AGULA   ZZY
34:  DVIUT   QJXIO   ZVMRW   BLCYH   QC
35:  TCGHV   HLNNJ   IDIKU   FNUNU   IHXNR   APTC
36:  OKLBX   QNFLP   YDIKL   OHMTH   PWUWM   SH
37:  JIYNE   WKTIS   MLDKV   SFZGH   VZRHV   DBBXJ   Y
38:  BPAEX   PQVQV   WAVDG   EBESZ   XJHAK   FZ
39:  DVIQE   GMDMT   RTIEM   BACBT   WQYUU   GTXXN   YX
40:  DTGFW   TSCNI   DOAVR   LCPAE   AIXRQ   YM
41:  JIYSS   COITP   XYJNP   QZZOZ   MIZOM
42:  DVIBX   GVFQP   QIQXT   OMDAR   MPBYG   KXTW
43:  IDAYS   NYRVC   BBBKU   UUDGZ   WABAA
44:  TCRVF   CCAER   NDIXR   OTHJX   XZTGG   QDSTB   FENB
45:  YHAPC   NUQLS   MHRBY   MVDKR   NDNMC   PDQN
46:  MASXQ   WVXWA   UAOIV   BMTIX   YWONN
47:  DVINS   PRNDL   LBUKC   RFEFS   METGM   JNLNT   XHGZ
48:  TCQNO   QUTHK   TVGHA   LVAJS   CIUSQ   MQ
49:  TCBXI   SZAOK   OYQNT   PKQOD   JKUKP   ZFK
50:  BKRBO   COBBL   KYOQP   IINKF   EUYEN   JRGMD
```

Below is a transcription of the 50 rows of ciphertext. Though great care has been taken for accuracy, it is possible those same juxtaposed errors (D vs O, and U vs D) have been introduced by the authors.[4] Readers are encouraged to verify each row against the photographs before pursuing any cryptanalysis.

```
1:   TIHUL RZNXN SDGQL MYGNU QQAXF H
2:   OYRBQ NNZEG ZECMZ MOMKO AMEBL HB
3:   XANQD WXZST SJMLR XNSLC YPDJD UO
4:   XANQD WXOAO JZSYM OXEQE LAC
5:   XMIRE DOHSJ HHSNQ QFHZL LHZMH G
6:   TCYXM XFROW ACWTY QEVMF ITXTO A
7:   NHCDQ DEGRG OMQBD RKBJX HRKQN LPOOD
8:   TIYJD ICMSR PTVHB EUSQD KVYIT RWDL
9:   TCQPK EGAUN TKMWK XNBNO GDUTR
10:  BCQXD OGMPE MKBLT YUAUQ DPTJR JZH
11:  MSQEJ KMEYK JQSXG QJDHB YYEKQ NHX
12:  YIMEH ZZRVC ZAHYZ VYFZP JXAFS GQFE
13:  DVIIX LLUBE LWWQY LMFOD QQCSK KHMQ
14:  TPUSB SWAJZ SPMBH HTSFO RXYED DA
15:  SYMEZ WGNPH QEPLZ LSZIT DPYIT
16:  KMPNS TOABI TQGSU JMXRZ KKNJN UXV
17:  DVHPA XKJZN VSDCQ CJLEG AWONP LNIXG
18:  TCYCS WGOOH UJRDB EGFXP TTRHU CJLY
19:  TLQYI LXKSU WMWAE JUZHI WPQNT TI
20:  OKLAE CKPKN LTSGY AISUL NIFFR Y
21:  DVRHS LOCDS VJQXC FPAZT OFV
22:  DVINE VMEMJ JMCFR OJMQH HBVGV LCBGD LBD
23:  VISSL XWQIE DRIPN MZONC OWNMT Y
24:  JISRX QMPQI QGNSJ GDZFQ MEDKC
25:  OKLNC FSRRC ZRIRC BWXBW CO
26:  TPZEY GGMVA XZKSQ LYBEB TXTRM YEDHK
27:  DVIIX IXIPH BPZXQ XTMBG NEQ
28:  AHPEV CEUYH RTANP GKZIR TS
29:  TCCTS OLEBN BFHID BURNI IVPPZ UC
30:  JISUA CDUPG EZPKS VXUOE VWBBS BVSA
31:  SYGYE ZEEJJ VGBYF BJGNC BMNRU XQPUN
32:  TCRBD XCAPM NTPHK HKNFZ JNHIK L
33:  DVIIX LKBKH LUJLY NIVOY AGULA ZZY
34:  DVIUT QJXIO ZVMRW BLCYH QC
35:  TCGHV HLNNJ IDIKU FNUNU IHXNR APTC
36:  OKLBX QNFLP YDIKL OHMTH PWUWM SH
```

[4] In fact, a re-review of these 50 lines by the authors revealed that in the published article "Chaocipher Exhibit 5: History, Analysis, and Solution of *Cryptologia's* 1990 Challenge", two such transcription errors were made (and here now corrected). Line 32, first 5-letter sequence published as TCRBO, and Line 39, second 5-letter sequence published as GMOMT. In both instances, the letter D was incorrectly transcribed as O based on use of scanned copy of actual source document. For this short paper, an enhanced PDF of the photograph taken at the NCM aided in the correct verification.

```
37:  JIYNE WKTIS MLDKV SFZGH VZRHV DBBXJ Y
38:  BPAEX PQVQV WAVDG EBESZ XJHAK FZ
39:  DVIQE GMDMT RTIEM BACBT WQYUU GTXXN YX
40:  DTGFW TSCNI DOAVR LCPAE AIXRQ YM
41:  JIYSS COITP XYJNP QZZOZ MIZOM
42:  DVIBX GVFQP QIQXT OMDAR MPBYG KXTW
43:  IDAYS NYRVC BBBKU UUDGZ WABAA
44:  TCRVF CCAER NDIXR OTHJX XZTGG QDSTB FENB
45:  YHAPC NUQLS MHRBY MVDKR NDNMC PDQN
46:  MASXQ WVXWA UAOIV BMTIX YWONN
47:  DVINS PRNDL LBUKC RFEFS METGM JNLNT XHGZ
48:  TCQNO QUTHK TVGHA LVAJS CIUSQ MQ
49:  TCBXI SZAOK OYQNT PKQOD JKUKP ZFK
50:  BKRBO COBBL KYOQP IINKF EUYEN JRGMD
```

Foundational efforts to decipher these 50 lines have begun but as yet yielded no success. To date, the following has been determined:

- The 50 lines do not appear to have been created based on the same settings (i.e., same keyword and progressive, alternating encipherment wheel patterns) Kruh and Deavours used for their published Exhibit 5. Moshe Rubin attempted to decipher Line 1 using those settings, but no plaintext came through. He also attempted an enciphering operation, using straight alphabets instead; again, the results were negative.

- The 50 lines were probably enciphered based either on the 'classic' Chaocipher algorithm Byrne used for Exhibits 1 & 4, or on Kruh and Deavours's advanced keying algorithm used for Exhibit 5 (see the next section for more details). Given that Kruh and Deavours were not aware of the algorithms used for Exhibits 2 & 3, it is improbable that either of these were used for the Exhibit 6 encipherments.

With no knowledge of the source material, plaintext, or encipherment schema, Exhibit 6 offers students of cryptanalysis the greatest Chaocipher challenge yet. Jeff Calof reached out to Prof. Deavours at his Kean University email address for additional information on its creation but received no reply.

For greater details and a complete overview of Exhibits 5 & 6, 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 [3].

For a more cursory overview of the "Chaocipher: Exhibit 5 Solution", see Progress Report 23 at The Chaocipher Clearing House http://www.mountainvistasoft.com/chaocipher/chaocipher-023.htm [4].

Important Information for the Cryptanalyst

Before tackling Exhibit 6, a potential cryptanalyst should be aware of the Chaocipher systems used in challenge exhibits to date. The following table shows the methods used for enciphering the different exhibits.

Exhibit	Method Used	Author	Comments
1	Classic	John F. Byrne	Plaintext letter is always found in right alphabet
2	Rogue variant	John F. Byrne	Solved by Esa Peuha, nonstandard variants
3	Rogue variant	John F. Byrne	
4	Classic	John F. Byrne	Plaintext letter is always found in right alphabet
5	Advanced	Deavours and Kruh	Plaintext letter from right or left alphabets, based on takeoff key
6	???	Deavours and Kruh	Probably used the Exhibit 5 advanced method

It turns out that John F. Byrne used one flavor of the Chaocipher system (‘classic’) for Exhibits 1 and 4, and ‘rogue’ variants for Exhibits 2 and 3 [2]. In the case of Deavours and Kruh’s Exhibit 5, on the other hand, they used a more complex Chaocipher system (‘advanced’).

Leaving Exhibits 2 and 3 out of the discussion for the moment, it seems probable that Deavours and Kruh enciphered Exhibit 6 using the same ‘advanced’ system as Exhibit 5 (or a slight variant) to encipher Exhibit 6.

The ‘Classic’ Chaocipher System

The ‘classic’ Chaocipher system is identical to the one described in reference [1] and [5]. The major feature to pay attention to is that, when enciphering a message, the plaintext letter is always located in the right alphabet and the ciphertext letter in the left alphabet.

The ‘Advanced’ Chaocipher System

The ‘advanced’ Chaocipher system is identical to the ‘classic’ system except in one important detail: when enciphering a message, the plaintext will be located in either the right or left alphabet, depending on a predetermined ‘takeoff key’. The takeoff key is a finite ordered set of two denotations of ‘right’ and ‘left’. The key is used cyclically to decide which alphabet should be used for finding the plaintext letter, with the other alphabet being used to find the ciphertext letter.

A complete description of the advanced Chaocipher system can be found in reference [3], which must be bought from the publishers of Cryptologia. Therefore, we will provide a contrived description of the advanced Chaocipher system for the benefit of the reader.

In the following example we encipher the input text “SENDMONEY”. For the initial conditions we provide left and right starting alphabets, the alignment of these two alphabets relative to each other, the left and right zeniths, and, importantly, a plaintext disk pattern (“takeoff key”). Here is the detailed output of enciphering the input text, with the plaintext alphabet dictated by the “takeoff key”:

```
Session options
===============
        Left starting alphabet:         BGSXMLJWQDKZAIPRHFVCYOETUN
        Right starting alphabet:        RYUJBDAKVFGOWIPLCZXENHMTQS
        Left zenith:                    B
        Right zenith:                   R
        PT takeoff key:                 RLRRLLLRRRLLLLRRRRRLLLLLLRRRRRR
        Command line input:             SENDMONEY
        Mode:                           encipher


Input text has 9 characters

(      0) leftAlphabet:  BGSXMLJWQDKZAIPRHFVCYOETUN
(      0) rightAlphabet: RYUJBDAKVFGOWIPLCZXENHMTQS
(      0) Plain disk is the RIGHT disk

(      0) pt(S) = ct(N)

(      1) leftAlphabet:  NGSXMLJWQDKZABIPRHFVCYOETU
(      1) rightAlphabet: RYJBDAKVFGOWIUPLCZXENHMTQS
(      1) Plain disk is the LEFT disk

(      1) pt(E) = ct(T)

(      2) leftAlphabet:  EUNGSXMLJWQDKTZABIPRHFVCYO
(      2) rightAlphabet: QSYJBDAKVFGOWRIUPLCZXENHMT
(      2) Plain disk is the RIGHT disk

(      2) pt(N) = ct(V)

(      3) leftAlphabet:  VYOEUNGSXMLJWCQDKTZABIPRHF
(      3) rightAlphabet: HMQSYJBDAKVFGTOWRIUPLCZXEN
(      3) Plain disk is the RIGHT disk

(      3) pt(D) = ct(S)

(      4) leftAlphabet:  SMLJWCQDKTZABXIPRHFVYOEUNG
(      4) rightAlphabet: AKFGTOWRIUPLCVZXENHMQSYJBD
(      4) Plain disk is the LEFT disk

(      4) pt(M) = ct(K)

(      5) leftAlphabet:  MJWCQDKTZABXILPRHFVYOEUNGS
(      5) rightAlphabet: FGOWRIUPLCVZXTENHMQSYJBDAK
(      5) Plain disk is the LEFT disk

(      5) pt(O) = ct(Y)

(      6) leftAlphabet:  OUNGSMJWCQDKTEZABXILPRHFVY
(      6) rightAlphabet: JBAKFGOWRIUPLDCVZXTENHMQSY
(      6) Plain disk is the LEFT disk

(      6) pt(N) = ct(A)

(      7) leftAlphabet:  NSMJWCQDKTEZAGBXILPRHFVYOU
(      7) rightAlphabet: KFOWRIUPLDCVZGXTENHMQSYJBA
(      7) Plain disk is the RIGHT disk

(      7) pt(E) = ct(I)

(      8) leftAlphabet:  IPRHFVYOUNSMJLWCQDKTEZAGBX
(      8) rightAlphabet: NHQSYJBAKFOWRMIUPLDCVZGXTE
(      8) Plain disk is the RIGHT disk

(      8) pt(Y) = ct(F)

(      9) leftAlphabet:  FYOUNSMJLWCQDVKTEZAGBXIPRH
(      9) rightAlphabet: JBKFOWRMIUPLDACVZGXTENHQSY

Final ciphertext = "NTVSKYAIF"
```

Here is a brief description of the first two enciphering steps.

- Before commencing enciphering
  - Align the left and right alphabets using their respective zeniths, such that that "B" in the left alphabet corresponds to "R" in the right alphabet.
- Enciphering the first plaintext letter "S"
  - The first letter in the takeoff pattern is "R", denoting that the plaintext letter should be found in the right ("R") alphabet
  - Find the plaintext letter "S" in the right alphabet
  - Note the corresponding ciphertext letter in the left alphabet, i.e., "N"
  - Permute the left and right alphabets as per the Chaocipher method (see references for exact instructions)
- Enciphering the second plaintext letter "E"
  - The second letter in the takeoff pattern is "L", denoting that the plaintext letter should be found in the left ("L") alphabet
  - Find the plaintext letter "E" in the left alphabet
  - Note the corresponding ciphertext letter in the right alphabet, i.e., "T"
  - Permute the left and right alphabets as per the Chaocipher method (see references for exact instructions)
- Continue with the remaining letters, using successive takeoff key letters to determine which alphabet to locate the plaintext letter in. When the takeoff key is exhausted, begin from the start of the key again.

When working on Exhibit 6, it is a likely consideration to believe it was enciphered using the 'advanced' Chaocipher system used in Exhibit 5.

References

[1] John F. Byrne's Chaocipher Revealed: An Historical and Technical Appraisal by Moshe Rubin, Cryptologia, Volume 35, Issue 4, October 2011. Freely accessible online at http://www.tandfonline.com/doi/abs/10.1080/01611194.2011.606751?journalCode=ucry20&

[2] Decoding Chaocipher Exhibits 2 & 3 by Esa Peuha (PDF). Retrieved April 23, 2014. Accessible online at http://www.chaocipher.com/chaocipher-022.htm

[3] Chaocipher Exhibit 5: History, Analysis, and Solution of Cryptologia's 1990 Challenge by Jeff Calof, Jeff Hill & Moshe Rubin, Cryptologia, Volume 38, Issue 1, January.

[4] "Chaocipher: Exhibit 5 Solution" by Jeff Calof (PDF). Retrieved 12/3/14. Accessible online at http://www.mountainvistasoft.com/chaocipher/chaocipher-023.htm

[5] Chaocipher Revealed: The Algorithm by Moshe Rubin (July 2, 2010), accessible at http://www.mountainvistasoft.com/chaocipher/ActualChaocipher/Chaocipher-Revealed-Algorithm.pdf