**CHAOCIPHER REVEALED:**

**DECIPHERING EXHIBIT #1 in “SILENT YEARS”**

© Moshe Rubin, 8 August 2010

**ADDRESS:** Rechov Shaulson 59/6, Jerusalem 95400 ISRAEL; mosher@mountainvistasoft.com.

**ABSTRACT:** Chaocipher is a method of encryption invented by John F. Byrne in 1918 who tried unsuccessfully for more than three decades to interest the US Signal Corp and Navy in his system. In 1954, Byrne presented four Chaocipher-encrypted messages as challenges in his autobiography “Silent Years”. Although numerous non-governmental cryptanalysts attempted to solve the challenge messages over the years, none succeeded (the success of official government agencies is currently unknown). This paper presents the decipherment of Exhibit 1 found in “Silent Years” together with points of interest.

**KEYWORDS:** Chaocipher, John F. Byrne, Silent Years, Exhibit 1

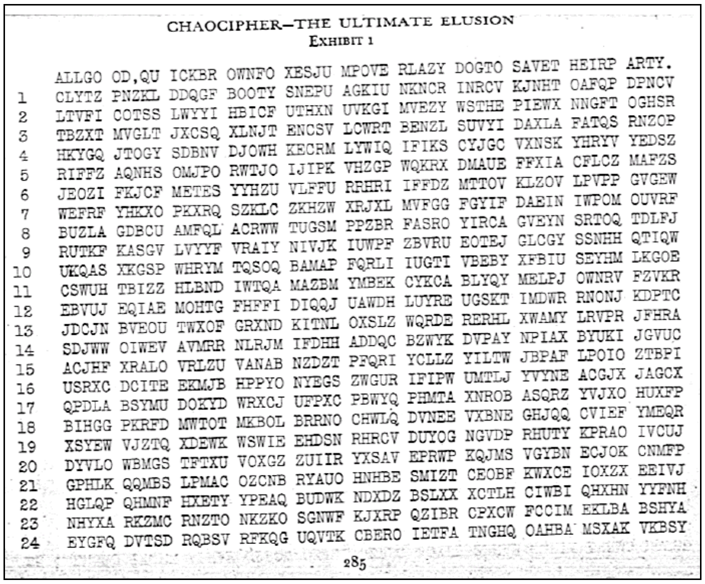
## Introduction

This paper is the logical continuation of a previous paper entitled “Chaocipher Revealed: The Algorithm” [1]. In that paper we described how John F. Byrne’s Chaocipher works from an algorithmic point of view. The reader is strongly urged to read that paper before proceeding with this one; the current paper will only make sense after reading the previous one.

In this paper we present the decipherment of the first of four challenge exhibits presented in Chapter 21 of Byrne’s autobiographical “Silent Years” [2].

## Basic Information about Exhibit 1

The ciphertext of Exhibit 1 begins on page 285 in “Silent Years” (see Figure 1). The initial unnumbered line is the plaintext “ALLGOODQQUICK…” for the next 100 lines of ciphertext (see Figure 1). In all, there are 248 lines of ciphertext, extending until page 294 (see Figure 2). All ciphertext lines are presented as lines of eleven 5-letter groups and are numbered from 1 through 248, for a total of 13,615 characters.



CHAOCIPHER—THE ULTIMATE ELUSION

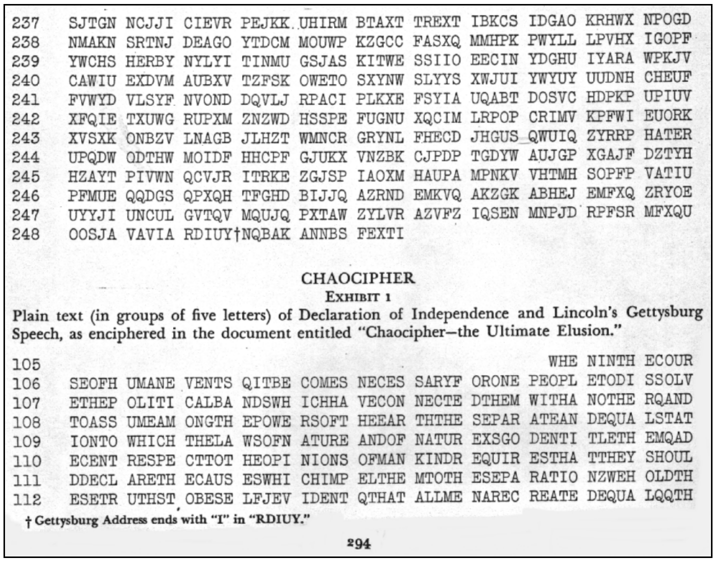
EXHIBIT 1

```
     ALLGO OD,QU ICKBR OWNFO XESJU MPOVE RLAZY DOGTO SAVET HEIRP ARTY.
1    CLYTZ PNZKL DDQGF BOOTY SNEPU AGKIU NKNCR INRCV KJNHT OAFQP DPNCV
2    LTVFI COTSS LWYYI HBICF UTHXN UVKGI MVEZY WSTHE PIEWX NNGFT OGHSR
3    TBZXT MVGLT JXCSQ XLNJT ENCSV LCWRT BENZL SUVYI DAXLA FATQS RNZOP
4    HKYGQ JTOGY SDBNV DJOWH KECRM LYWIQ IFIKS CYJGC VXNSK YHRYV YEDSZ
5    RIFFZ AQNHS OMJPO RWTJO IJIPK VHZGP WQKRX DMAUE FFXIA CFLCZ MAFZS
6    JEOZI FKJCF METES YYHZU VLFFU RRHRI IFFDZ MTTOV KLZOV LPVPP GVGEW
7    WEFRF YHKXO PKXRQ SZKLC ZKHZW XRJXL MVFGG FGYIF DAEIN IWPOM OUVRF
8    BUZLA GDBCU AMFQL ACRWW TUGSM PPZBR FASRO YIRCA GVEYN SRTOQ TDLFJ
9    RUTKF KASGV LVYYF VRAIY NIVJK IUWPF ZBVRU EOTEJ GLCGY SSNHH QTIQW
10   UKQAS XKGSP WHRYM TQSOQ BAMAP FQRLI IUGTI VBEBY XFBIU SEYHM LKGOE
11   CSWUH TBIZZ HLBND IWTQA MAZBM YMBEK CYKCA BLYQY MELPJ OWNRV FZVKR
12   EBVUJ EQIAE MOHTG FHFFI DIQQJ UAWDH LUYRE UGSKT IMDWR RNONJ KDPTC
13   JDCJN BVEOU TWXOF GRXND KITNL OXSLZ WQRDE RERHL XWAMY LRVPR JFHRA
14   SDJWW OIWEV AVMRR NLRJM IFDHH ADDQC BZWYK DVPAY NPIAX BYUKI JGVUC
15   ACJHF XRALO VRLZU VANAB NZDZT PFQRI YCLLZ YILTW JBPAF LPOIO ZTBPI
16   USRXC DCITE EKMJB HPPYO NYEGS ZWGUR IFIPW UMTLJ YVYNE ACGJX JAGCX
17   QPDLA BSYMU DOKYD WRXCJ UFPXC PBWYQ PHMTA XNROB ASQRZ YVJXO HUXFP
18   BIHGG PKRFD MWTOT MKBOL BRRNO CHWLQ DVNEE VXBNE GHJQQ CVIEF YMEQR
19   XSYEW VJZTQ XDEWK WSWIE EHDSN RHRCV DUYOG NGVDP RHUTY KPRAO IVCUJ
20   DYVLO WBMGS TFTXU VOXGZ ZUIIR YXSAV EPRWP KQJMS VGYBN ECJOK CNMFP
21   GPHLK QQMBS LPMAC OZCNB RYAUO HNHBE SMIZT CEOBF KWXCE IOXZX EEIVJ
22   HGLQP QHMNF HXETY YPEAQ BUDWK NDXDZ BSLXX XCTLH CIWBI QHXHN YYFNH
23   NHYXA RKZMC RNZTO NKZKO SGNWF KJXRP QZIBR CPXCW FCCIM EKLBA BSHYA
24   EYGFQ DVTSD RQBSV RFKQG UQVTK CBERO IETFA TNGHQ OAHBA MSXAK VKBSY
```

285

Figure 1. The first page of Exhibit 1 showing the initial plaintext and subsequent ciphertext lines.

Immediately following the 248 lines of ciphertext are the corresponding plaintext lines, beginning on page 294 (see Figure 2).



```
237  SJTGN NCJJI CIEVR PEJKK UHIRM BTAXT TREXT IBKCS IDGAO KRHWX NPOGD
238  NMAKN SRTNJ DEAGO YTDCM MOUWP KZGCC FASXQ MMHPK PWYLL LPVHX IGOPF
239  YWCHS HERBY NYLYI TINMU GSJAS KITWE SSIIO EECIN YDGHU IYARA WPKJV
240  CAWIU EXDVM AUBXV TZFSK OWETO SXYNW SLYYS XWJUI YWYUY UUDNH CHEUF
241  FVWYD VLSYF NVOND DQVLJ RPACI PLKXE FSYIA UQABT DOSVC HDPKP UPIUV
242  XFQIE TXUWG RUPXM ZNZWD HSSPE FUGNU XQCIM LRPOP CRIMV KPFWI EUORK
243  XVSXK ONBZV LNAGB JLHZT WMNCR GRYNL FHECD JHGUS QWUIQ ZYRRP HATER
244  UPQDW QDTHW MOIDF HHCPF GJUKX VNZBK CJPDP TGDYW AUJGP XGAJF DZTYH
245  HZAYT PIVWN QCVJR ITRKE ZGJSP IAOXM HAUPA MPNKV VHTMH SOPFP VATIU
246  PFMUE QQDGS QPXQH TFGHD BIJJQ AZRND EMKVQ AKZGK ABHEJ EMFXQ ZRYOE
247  UYYJI UNCUL GVTQV MQUJQ PXTAW ZYLVR AZVFZ IQSEN MNPJD RPFSR MFXQU
248  OOSJA VAVIA RDIUY†NQBAK ANNBS FEXTI
```

CHAOCIPHER

EXHIBIT 1

Plain text (in groups of five letters) of Declaration of Independence and Lincoln's Gettysburg Speech, as enciphered in the document entitled "Chaocipher—the Ultimate Elusion."

```
105                                                        WHE NINTH ECOUR
106  SEOFH UMANE VENTS QITBE COMES NECES SARYF ORONE PEOPL ETODI SSOLV
107  ETHEP OLITI CALBA NDSWH ICHHA VECON NECTE DTHEM WITHA NOTHE RQAND
108  TOASS UMEAM ONGTH EPOWE RSOFT HEEAR THTHE SEPAR ATEAN DEQUA LSTAT
109  IONTO WHICH THELA WSOFN ATURE ANDOF NATUR EXSGO DENTI TLETH EMQAD
110  ECENT RESPE CTTOT HEOPI NIONS OFMAN KINDR EQUIR ESTHA TTHEY SHOUL
111  DDECL ARETH ECAUS ESWHI CHIMP ELTHE MTOTH ESEPA RATIO NZWEH OLDTH
112  ESETR UTHST OBESE LFJEV IDENT QTHAT ALLME NAREC REATE DEQUA LQQTH
```

† Gettysburg Address ends with "I" in "RDIUY."

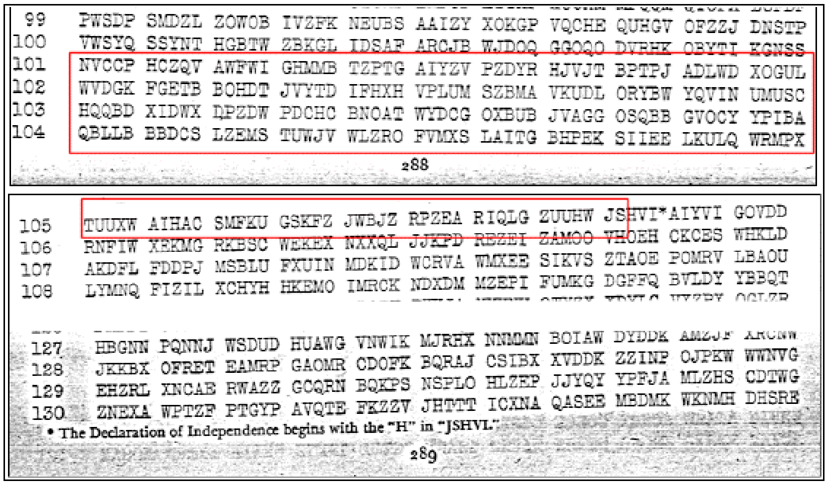
294

Figure 2. Page 294 of "Silent Years" showing transition between ciphertext and plaintext sections

According to Byrne, the Exhibit 1's underlying plaintext consists of the following:

- Lines 1-100: 100 repetitions of the 55-letter phrase "ALLGOODQQUICKBROWNFOXESJUMPOVERLAZYDOGTOSAVETHEIRPARTYW". The plaintext is not shown on page 294, but can be seen at the top of page 285 (Figure 1). Byrne substituted the letters 'Q' and 'W' for comma and period, respectively.

- Lines 101-105: 262 characters whose plaintext is not disclosed. Byrne writes that these lines “are devoted to a few introductory words to the two great historic documents that follow”. The plaintext is not shown on page 294 (see Figure 3 for the corresponding ciphertext).



```
 99  PWSDP SMDZL ZOWOB IVZFK NEUBS AAIZY XOKGP VQCHE QUHGV OFZZJ DNSTP
100  VWSYQ SSYNT HGBTW ZBKGL IDSAF ARCJB WJDOQ GGOQO DVBHK OBYTI KGNSS
101  NVCCP HCZQV AWFWI GHMMB TZPTG AIYZV PZDYR HJVJT BPTPJ ADLWD XOGUL
102  WVDGK FGETB BOHDT JVYTD IFHXH VPLUM SZBMA VKUDL ORYBW YQVIN UMUSC
103  HQQBD XIDWX DPZDW PDCHC BNOAT WYDCG OXBUB JVAGG OSQBB GVOCY YPIBA
104  QBLLB BBDCS LZEMS TUWJV WLZRO FVMXS LAITG BHPEK SIIEE LKULQ WRMPX
                                 288

105  TUUXW AIHAC SMFKU GSKFZ JWBJZ RPZEA RIQLG ZUUHW JSHVI*AIYVI GOVDD
106  RNFIW XEKMG RKBSC WEKEX NXXQL JJKPD REZEI ZAMOO VHOEH CKCES WHKLD
107  AKDFL FDDPJ MSBLU FXUIN MDKID WCRVA WMXEE SIKVS ZTAOE POMRV LBAOU
108  LYMNQ FIZIL XCHYH HKEMO IMRCK NDXDM MZEPI FUMKG DGFFQ BVLDY YBBQT

127  HBGNN PQNNJ WSDUD HUAWG VNWIK MJRHX NNMMN BOIAW DYDDK AMZJF XRCNW
128  JKKBX OFRET EAMRP GAOMR CDOFK BQRAJ CSIBX XVDDK ZZINP OJPKW WWNVG
129  EHZRL XNCAB RWAZZ GCQRN BQKPS NSPLO HLZEP JJYQY YPFJA MLZHS CDTWG
130  ZNEXA WPTZF PTGYP AVQTE FKZZV JHTTT ICXNA QASEE MBDMK WKNMH DHSRE
 * The Declaration of Independence begins with the "H" in "JSHVI."
                                 289
```

Figure 3. Ciphertext lines 101-105 corresponding to the “hidden” plaintext

- Lines 105-248: The full text of the Declaration of Independence followed by the Gettysburg Address[1].

- Line 248: The last 17 letters of this line correspond to plaintext that Byrne does not disclose (see Figures 2 and 4 for ciphertext).

The challenge to a would-be cryptanalyst, then, is to:

1. Determine the starting alphabets of Exhibit 1
2. Discover the hidden plaintext in lines 101-105
3. Reveal the final 17 characters of the exhibit

## Types of Cryptanalytic Attacks

Before proceeding further, a brief overview of what is known of Chaocipher to date, and its relation to other historical ciphers will help in understanding the methods used to solve Exhibit 1.

The task facing a cryptanalyst may vary in difficulty, depending on the information the cryptanalyst has at his disposal [11]. The direction and efforts of a cryptanalyst may vary significantly based on the available information. The following paragraphs list the most common scenarios a cryptanalyst may face when attacking a cipher message:

### Ciphertext-only / system unknown

In this case the cryptanalyst has one or more ciphertext messages belonging to a cryptographic system whose underlying algorithm is unknown to the cryptanalyst. He has no idea what the corresponding

[1] On page 282 of “Silent Years” Byrne writes “*In both the cipher and plain texts of the Gettysburg Speech, there was an error of omission of the fourth character in the eighth group of five letters in line 239. At this point 35 characters were left out, these being a comma followed by the words ‘but it can never forget what they did here*’”. Since they are missing from both the plaintext and the ciphertext, no harm is done.

plaintext is. This is conceptually the hardest case a cryptanalyst will encounter. Before he can decipher the messages, he must first determine the underlying system, a task that may be extremely difficult.

Examples of this scenario are the Japanese Purple cipher [12] and the German Lorenz cipher [13] during World War II. In both instances Allied cryptanalysts were able to discover how the cryptographic system worked using analytic and deductive methods only [14]. Once that was determined, they were able to devise a general solving method enabling them to determine the specific message keys. The general solving method allowed them to decipher ciphertext messages on a continuous basis.

**Ciphertext-only / system known**

Somewhat easier than the previous case, here the cryptanalyst has only ciphertext messages (i.e., no known plaintext), but he does know the underlying cryptographic system. In this case, the cryptanalyst needs "only" to discover the keys for the ciphertext messages.

This is the most common case facing a cryptanalyst. This will occur whenever the cryptanalyst knows the underlying system and has ciphertext messages with no other information. The aforementioned Japanese Purple and German Lorenz cases moved from ciphertext-only / unknown system to ciphertext-only / known system once the system was deduced.

In regards to Chaocipher, Kruh and Deavour's Exhibit 5 [15] can qualify as a case of ciphertext-only / system known. This exhibit contains three ciphertext messages for which the following information is given:

- All three messages are "in-depth", meaning that they all begin with the identical starting alphabets.
- The underlying plaintexts for these messages are taken from Stewart C. Easton's book, *Rudolf Steiner: Herald of a New Epoch* [16].

Although the exact corresponding plaintexts are not known, the cryptanalyst is in a somewhat better position of knowing where to find the plaintexts.

**Known-plaintext / system unknown**

Here we have a case where the cryptanalyst has both ciphertext messages and their corresponding plaintexts, but the system is unknown. As in the case of "ciphertext-only, system unknown", the cryptanalyst must ascertain the underlying cryptographic system before he can tackle other ciphertext-only messages. The cryptanalyst has a decided advantage: knowing both the ciphertext and its corresponding plaintext can suggest novel candidate ideas, something the cryptanalyst might never have thought of had he had only the ciphertext.

The most important example of this case in our discussion is Chaocipher before the algorithm was revealed: Byrne provided a plethora of ciphertext and its corresponding plaintext, while challenging everyone to deduce the underlying system. Although no information is available regarding official government agencies (e.g., NSA, GHCQ), it is known that numerous non-governmental cryptanalysts unsuccessfully attempted to deduce the system over the years.

**Known-plaintext / system known**

This is one of the best situations to be in. In this case, the cryptanalyst knows how the underlying cryptographic system works, and has a quantity of ciphertext and its corresponding plaintext. If the entire plaintext is known, then the challenge is to deduce the message key. If only a portion of the plaintext is known, the challenge is to decipher the entire plaintext and, hopefully, deduce the message key.

The quintessential example from our point of view is Chaocipher as is stands today: the underlying cryptographic system is known, and there is a plethora of ciphertext and plaintext. In our case, there are patches of plaintext that are not known, so the challenge is to deduce the message key (i.e., the starting alphabets) and decipher the entire message.

Another famous example is the German Enigma cipher, which was solved by the British at Bletchley Park for a portion of World War II. The underlying system was known to the Allies, and the cryptanalysts had highly probable plaintext (known as "cribs") for portions of the ciphertext. Assuming a candidate crib was correct, the cryptanalyst was facing a known system / known plaintext scenario.

It is important to realize that even a known-plaintext / known system case can be challenging and difficult to solve.

| | | Underlying system | |
|---|---|---|---|
| | | **Unknown** | **Known** |
| **Material Available** | **Ciphertext only** | Japanese Purple, German Lorenz | The most common case if collateral information is not available. |
| | **Known plaintext** | Chaocipher before the underlying system was revealed | Chaocipher after the underlying system was revealed, Enigma with known cribs. |

Table 1. Summary of scenarios a cryptanalyst may face, with illustrative examples

## Solving Exhibit 1 as a Known-Plaintext / Known System Problem

In the present case of Exhibit 1 in "Silent Years", we know how the underlying system works, and we have a plethora of ciphertext and its corresponding plaintext. Based on the previous section, we qualify for the known-plaintext / known system scenario. In our case we almost know the entire plaintext – there are 262 plaintext characters within the body of the exhibit and another 17 characters at its end which we need to solve.

To date several researchers, including the author, have solved this fundamental cryptanalytic problem (see [4] for a clear explanation of how to solve the Chaocipher known-plaintext problem). Such a discussion is outside the scope of this paper and will be discussed in a future paper.

## The Starting Alphabets

Assuming we have solved the known-plaintext problem and have deciphered Exhibit 1, we will discover that the starting alphabets are:

```
Left  (ct) starting alphabet: BFVGUHWJKNCPEDQRSTIXYLMOZA
Right (pt) starting alphabet: CMOPRTUVJXAYZNBQDSEFGHLWIK
```

or any of the other 25 *rotated forms*. By "rotated form" we mean shifting the left and right alphabets a specific number of positions in tandem. There are 26 such rotated forms, of which the first three shifted examples are:

```
                                     ↓
Left (ct):  FVGUHWJKNCPEDQRSTIXYLMOZAB (one position counterclockwise)
Right (pt): MOPRTUVJXAYZNBQDSEFGHLWIKC
                                     ↑

                                    ↓
Left (ct):  VGUHWJKNCPEDQRSTIXYLMOZABF (two positions counterclockwise)
Right (pt): OPRTUVJXAYZNBQDSEFGHLWIKCM

                                   ↓
Left (ct):  GUHWJKNCPEDQRSTIXYLMOZABFV (three positions counterclockwise)
Right (pt): PRTUVJXAYZNBQDSEFGHLWIKCMO
                                   ↑
```

All 26 starting alphabet pairs are equivalent and will decipher Exhibit 1 correctly[2].

## The Deciphered Plaintext

Deciphering the entire exhibit produces the following plaintext:

Lines 1-100: All lines consist of the plaintext
"ALLGOODQQUICKBROWNFOXESJUMPOVERLAZYDOGTOSAVETHEIRPARTYW"

Lines 101-105:
"ZENSHRINEDINTHISARCANUMQTOWHICHNONEWHODOESNOTPOSSESSTHEKEYMAYENTE
RQTHEDECLARATIONOFINDEPENDENCEANDLINCOLNXSBEAUTIFULORATIONATGETTYS
BURGAREHEREREJINFORMEDWITHANINVISIBLEQINTANGIBLEANDIMPERCEPTIBLESO
ULWJWFWBYRNEQANDMAPHJAGEFRWBEGUNAUGUSTSIXTEENQONENINETHREESEVENWZ"

Lines 105-248: The Declaration of Independence and the Gettysburg Address

Line 248: CORDIALTHANKSTOLO

Lines 101-105, when correctly spaced and punctuated, read as follows:

> "*Enshrined in this arcanum, to which none who does not possess the key may enter, the Declaration of Independence and Lincoln's beautiful oration at Gettysburg are here re-informed with an invisible, intangible and imperceptible soul. J.F.Byrne, and MAPHJAGEFR. Begun August sixteen, one nine three seven.*"

The final 17 characters of Exhibit 1 in line 248 read 'CORDIALTHANKSTOLO'.

## Discussion of the Plaintexts

[a] Lines 101-105 tell us that Byrne began enciphering Exhibit 1 on Monday, August 16th, 1937. Byrne alludes to something using the phrase "MAPHJAGEFR". At the time of writing it is not clear what this refers to. It might refer to a person, or it could be an acronym of a larger phrase.

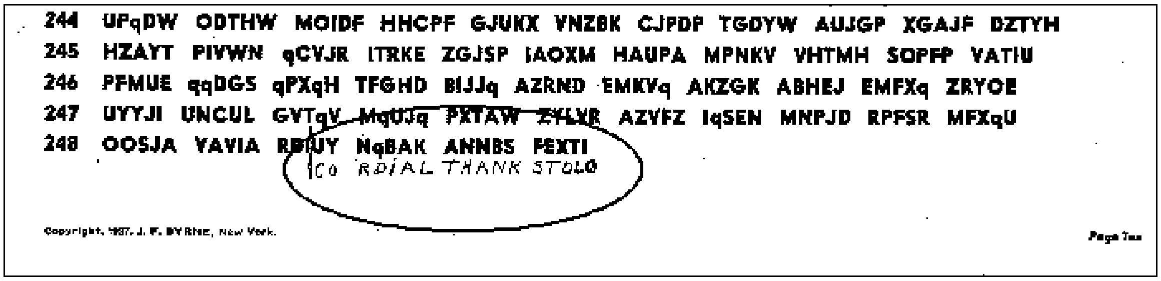
In a July 2010 correspondence with Dr. Fritz Senn, a world-renowned expert on the writings of James Joyce, the author asked whether "MAPHJAGEFR" could be a Joyce-like phrase known to Byrne similar to the style of writing found in Joyce's "Finnegans Wake". The theory was that Byrne, a close friend and colleague of Joyce, might have wanted to acknowledge his Joycean connections in some way. Dr. Senn

[2] This is because the alphabets, when kept together in tandem, are invariant under rotation.

replied *"I cannot see any Joycean echo in "MAPHJAGEFR". It rings no bell in Finnegans Wake (I am also not sure what kind of interest, if any, Byrne took in Finnegans Wake). What I vaguely thought of is the word "joggerfry" in Ulysses: slang for geography. But unlikely.*"

[b] In "Silent Years" page 277 Byrne writes that, on November 18, 1937, he sent his first letter to one Admiral Bowen of the US Navy Department. It is further known that the Navy had recently published a tender for submitting cryptographic systems for use by the Navy. One can assume that Byrne already began his preparations for his submission in August, enciphering his Exhibit and preparing his pamphlet "Chaocipher -- The Ultimate Elusion" [6]. By November he was ready to submit his letter to the Navy together with his pamphlet.

[c] As mentioned above, the last 17 characters read "CORDIAL THANKS TO LO". This plaintext was known even before the Chaocipher algorithm was publicized; it can be seen handwritten in Byrne's 1937 pamphlet as declassified by NSA [7] (see Figure 4):



```
244  UPqDW  ODTHW  MOIDF  HHCPF  GJUKX  VNZBK  CJPDP  TGDYW  AUJGP  XGAJF  DZTYH
245  HZAYT  PIVWN  qCVJR  ITRKE  ZGJSP  IAOXM  HAUPA  MPNKV  VHTMH  SOPFP  VATIU
246  PFMUE  qqDGS  qPXqH  TFGHD  BIJJq  AZRND  EMKVq  AKZGK  ABHEJ  EMFXq  ZRYOE
247  UYYJI  UNCUL  GVTqV  MqUJq  PXTAW  ZYLVR  AZVFZ  IqSEN  MNPJD  RPFSR  MFXqU
248  OOSJA  YAVIA  RBUUY  NqBAK  ANNBS  FEXTI
                  CO RDIAL THANK STOLO
```

Copyright, 1937, J. F. BYRNE, New York.

Page Ten

Figure 4. The last 17 plaintext characters from Byrne's 1937 pamphlet as declassified by NSA

It is believed that Rosario Candela, a famous American architect who had a passionate interest in cryptography [8], donated the pamphlet, which was subsequently declassified by NSA [6]. One can speculate that Byrne sent Candela, a known cryptographic expert at the time, a copy of his 1937 pamphlet. Candela probably tried to account for all ciphertext letters in Exhibit 1 and discovered there were 17 extra ciphertext characters at the end. When asked about the discrepancy, Byrne probably divulged the underlying plaintext, which was then written in by hand by Candela.

[d] Line 248 refers to someone named "LO". It is not known whether these are the initials of someone (e.g., "Laurence Olivier") or a nickname (e.g., "Loretta") [3]

## Errata in Exhibit 1 in "Silent Years"

If you attempt to decipher Exhibit 1 as found in "Silent Years", with the alphabets provided above, you will run into plaintext garbles beginning with the ciphertext group "XZCGM" on line 184, 11th group. Comparing that group with the same group in Byrne's 1937 pamphlet "Chaocipher: The Ultimate Elusion" [6] shows that the group should really be "ZXCGM", not "XZCGM". This pairwise transposal occurred when the pamphlet was typeset for publication in "Silent Years". If this is corrected, the entire exhibit deciphers correctly to the end. It should be noted that Byrne, in his pamphlet, enciphered Exhibit 1 perfectly (with the exception of one ciphertext error [17]).

Similarly, the typesetters introduced three plaintext errors in "Silent Years":

Line 155: OP**H**EV ENTTH EPOPU *should be* OP**R**EV ENTTH EPOPU<br>
Line 164: INTIM ESOF**F** EACEQ *should be* INTIM ESOF**P** EACEQ<br>
Line 174: OFTHE **R**ENEF ITSOF *should be* OFTHE **B**ENEF ITSOF

Deciphering Exhibit 1 shows that Byrne correctly used the plaintexts “PREVENT, “PEACE”, and “BENEFITS”.

For the record, Byrne’s plaintext and ciphertext for Exhibit 1 were perfect with no errors. The “Silent Years” typesetters introduced four errors (three in the plaintext and one in the ciphertext) when preparing the book for publication.

## Deriving Starting Alphabets from a Keyword

In his papers related to Exhibits 1 and 4, Byrne describes a system of key distribution for Chaocipher. Although not explained clearly, the papers do refer to the sender and receiver deriving the starting left (ct) and right (pt) alphabets based on a key phrase.

Byrne’s alphabet derivation method for Chaocipher requires the sender and receiver to possess two pieces of pre-distributed secret information:

(a) a secret phrase of length N
(b) a left/right alphabet pattern of length N

An *alphabet pattern* is a sequence of references to the left (L) and right (R) alphabets, and denotes which alphabet should be used for locating a plaintext character. For example, if the sender alternated between the R and L alphabets when locating subsequent plaintext characters, the alphabet pattern would be written as “RL”, repeating the pattern over again and again until enciphering is completed.

The process of deriving the starting alphabets begins with both the left (ct) and right (pt) alphabets consisting of the straight alphabet “ABCDEFGHIJKLMNOPQRSTUVWXYZ”, with both alphabets being positioned with ‘A’ at the zenith. The sender/receiver enciphers the key phrase by the method described in [1], with the alphabet pattern telling us which alphabet to use to locate the plaintext character (the pattern is reused repetitively until the keyphrase is finished). The left/right alphabets generated by the aforementioned enciphering are the alphabets used at the start of the exhibit.

When using the left/right alphabet pattern to generate the starting alphabets the encipherer suspends the usual assumption that plaintext letters are always located in the right-hand alphabet (plaintext letters are always located in the right-hand alphabet when enciphering an actual message[3]). Thus, when enciphering the key phrase, the plaintext letter may be located in either alphabet according to the left/right alphabet pattern. Note that regardless of the alphabet used to locate the plaintext, the left and right alphabets are always permuted as per the Chaocipher algorithm [1].

The following section will fully explain how this is done for Exhibit 1.

## Deriving the Exhibit 1 Starting Alphabets

Reading Byrne’s Chaocipher papers for Exhibit 1, we know the key phrase is “THINKTHINK” and the left/right alphabet pattern is “RLLRLLRRLR”. Here is how to derive the starting alphabets.

[3] It is currently believed, however, that exhibits 2 and 3 in “Silent Years” may have been enciphered using alternating plaintext alphabets within the messages themselves. This is thought to be the case because of the “pt/ct identities < 9” phenomenon detected in them that does not occur in exhibits 1 and 4 [9].

We begin with both alphabets as standard alphabets:

```
        +            *     ↓
 Left : ABCDEFGHIJKLMNOPQRSTUVWXYZ
Right : ABCDEFGHIJKLMNOPQRSTUVWXYZ
```

The key phrase plaintext letter in position 1 is “T” while the corresponding left/right alphabet pattern letter is “R” (referring to the right-hand alphabet) so we encipher the letter “T” by locating it in the right-hand alphabet, reading the ciphertext letter off of the left-hand alphabet.

Using the Chaocipher enciphering method as described in [1], the ciphertext letter is “T”, and the permuted alphabets will now be:

```
        +            *↓
 Left : TVWXYZABCDEFGUHIJKLMNOPQRS
Right : UVXYZABCDEFGHWIJKLMNOPQRST
```

The next key phrase plaintext letter is “H” while the corresponding left/right alphabet pattern is “L” (directing us to locate the plaintext letter in the left-hand alphabet). Locating the letter “H” in the left-hand alphabet, we read off the ciphertext letter in the right-hand alphabet, giving us “I”. Permuting the left and right alphabets as usual (i.e., as per [1]) we get:

```
                     ↓
        +            *
 Left : HJKLMNOPQRSTVIWXYZABCDEFGU
Right : JKMNOPQRSTUVXLYZABCDEFGHWI
```

The next key phrase plaintext letter is “I” while the left/right alphabet is “L”. Locating the letter “I” in the left-hand alphabet we see the resulting ciphertext letter is “L” and the permutated alphabets are now:

```
        +            *
 Left : IXYZABCDEFGUHWJKLMNOPQRSTV
Right : YZBCDEFGHWIJKAMNOPQRSTUVXL
```

We can summarize all the steps in the following table:

| Keyphrase Letter (plaintext) | Left/Right Alphabet | Ciphertext Letter | Permuted Alphabets | |
|---|---|---|---|---|
| | | | Left | Right |
| --- | --- | --- | ABCDEFGHIJKLMNOPQRSTUVWXYZ | ABCDEFGHIJKLMNOPQRSTUVWXYZ |
| T | R | T | TVWXYZABCDEFGUHIJKLMNOPQRS | UVXYZABCDEFGHWIJKLMNOPQRST |
| H | L | I | HJKLMNOPQRSTVIWXYZABCDEFGU | JKMNOPQRSTUVXLYZABCDEFGHWI |
| I | L | L | IXYZABCDEFGUHWJKLMNOPQRSTV | YZBCDEFGHWIJKAMNOPQRSTUVXL |
| N | R | K | KMNOPQRSTVIXYLZABCDEFGUHWJ | OPRSTUVXLYZBCQDEFGHWIJKAMN |
| K | L | O | KNOPQRSTVIXYLMZABCDEFGUHWJ | PRTUVXLYZBCQDSEFGHWIJKAMNO |
| T | L | Y | TIXYLMZABCDEFVGUHWJKNOPQRS | ZBQDSEFGHWIJKCAMNOPRTUVXLY |
| H | R | B | BDEFVGUHWJKNOCPQRSTIXYLMZA | WIKCAMNOPRTUVJXLYZBQDSEFGH |
| I | R | D | DFVGUHWJKNOCPEQRSTIXYLMZAB | KCMNOPRTUVJXLAYZBQDSEFGHWI |
| N | L | V | NCPEQRSTIXYLMOZABDFVGUHWJK | JXAYZBQDSEFGHLWIKCMNOPRTUV |
| K | R | B | **BFVGUHWJKNCPEDQRSTIXYLMOZA** | **CMOPRTUVJXAYZNBQDSEFGHLWIK** |

The permuted alphabets following the last step are the starting alphabets for enciphering Exhibit 1.

In truth there are many key phrases, with their own corresponding left/right alphabet patterns, which will produce the same starting alphabets. For instance, a keyphrase of “TILNOYHIVK” with a left/right pattern of “RRRRRRRRRR” (i.e., the plaintext letters are taken only on the right alphabet) will produce the same alphabets.

Byrne’s scheme of alternating alphabets, then, is simply a means of using an easily remembered keyphrase for generating the starting alphabets.

## Discovering the Keyphrase

In the previous section we disclosed that the keyphrase Byrne used to prepare the starting alphabets was “THINKTHINK” and the left/right alphabet pattern was “RLLRLLRRLR”. This information was found in Byrne’s Chaocipher papers. An important question to ask is: given only the starting alphabets, can a cryptanalyst discover the keyphrase and alphabet pattern analytically?

An early correspondent following the Chaocipher algorithm disclosure, Carl Scheffler, wrote a program that searches for all keyphrases up to 20 characters long that will produce the starting alphabets using only the left alphabet as the plaintext alphabet. Carl reduced the search space significantly by working backwards from the starting alphabets, continually attempting to reduce the ‘ring entropy’ [4] until he arrived at straight alphabets.

This search results in the single keyphrase “TILNOYHIVK” (with an alphabet pattern of “RRRRRRRRRR”) that will transform two straight alphabets (left and right) into the starting alphabets. He assumed the keyphrase was readable English, which this keyphrase is not. ‘Enciphering’ this keyphrase using Chaocipher with the starting alphabets results in the output “THIKKTBDNB”.

Writing one keyphrase under the other:

**T**IL**N**OY**HI**V**K**

T**HI**K**KT**BD**N**B

he glimpsed the keyphrase “THINKTHINK”. This means that Byrne alternated between alphabets, using the pattern “RLLRLLRRLR” (or the equivalent “LLLRLLRRLR”). Carl is to be commended on the excellent deductive work.

## The Cryptographic Indicator System for Exhibit 1 is Incomplete

In order for a valid recipient of the Exhibit 1 message to decipher it without prior knowledge of the starting alphabets, there must be a previously agreed upon ‘cryptographic indicator system’ in place. Here are the definitions of the terms ‘indicator’ and ‘indicator system’ as defined by the British in 1943 [5]:

INDICATOR :

One or more letter or figure or letter-and-figure groups (either sent in clear or enciphered on a separate system and placed at the beginning and/or end of a message, or in the body of it) indicating the key … used or … the starting- point or starting-point and finishing-point.

INDICATOR SYSTEM :

System by which key or starting-point indicators are enciphered or concealed.

Indicator systems are essential to any real-life cryptographic system; they allow the prompt deciphering of messages received from several different correspondents in a high-volume environment. For such an indicator system to work with Chaocipher the following needs to happen:

1. The sender decides on a keyphrase (e.g., “THINKTHINK”) and on an alphabet-alternating pattern (e.g., “RLLRLLRRLR”). The keyphrase and alphabet pattern is chosen by the sender and can differ from one message to another.
2. The sender uses the keyphrase and the alphabet pattern to generate the starting alphabets.
3. The sender enciphers the plaintext to produce the ciphertext.
4. The sender somehow embeds both the keyphrase and the alphabet pattern within the message (this is known as the ‘indicator’) together with the ciphertext. The indicator should be encoded so that an enemy cryptanalyst cannot deduce the keyphrase and alphabet pattern and hence cannot compute the starting alphabets.
5. The sender transmits the message, which is received by the recipient.
6. The recipient extracts the keyphrase and alphabet pattern from the message, using them to generate the starting alphabets.
7. The recipient uses the starting alphabets to decipher the ciphertext.

Exhibit 1 fulfills all of the steps above except for (4); in Exhibit 1 there is no evidence of the indicator (i.e., keyphrase and alphabet pattern) being transmitted via the ciphertext message. Indeed, Byrne did not embed the indicator within Exhibit 1. A future paper will show, however, that Exhibit 4 fulfills all requirements of a true indicator system.

## Conclusions

It is evident that Byrne was meticulously careful when enciphering Exhibit 1; any errors in the plaintext and ciphertext in Exhibit 1 were introduced by the typesetters when preparing “Silent Years” for publication. While the unknown plaintext reveals some information about Byrne’s thoughts, references to “MAPHJAGEFR” and “LO” will require literary research to determine what they refer to.

In Exhibit 1 we see Chaocipher as a full-fledged cryptosystem. What remains to be seen in Exhibit 4 is how Byrne envisioned his cryptographic indicator system.

## Acknowledgements

I would like to take this opportunity to thank Jeff Calof for the excellent proofreading feedback he provided and for his willingness to meticulously check several draft versions. I am indebted to him for his continual demand for readability and clarity, targeting both the professional and casual readers.

## References

[1] The Chaocipher Clearing House. 2010. “*Chaocipher Revealed: The Algorithm*”, can be seen at: http://www.mountainvistasoft.com/chaocipher/ActualChaocipher/Chaocipher-Revealed-Algorithm.pdf, Retrieved 2010-08-02.

[2] Chapter 21 of “Silent Years”, can be seen at: http://www.mountainvistasoft.com/chaocipher/ActualChaocipher/Chaocipher-Revealed-Algorithm.pdf

[3] Wikipedia has a list of personal names referred to as “LO” (http://en.wikipedia.org/wiki/LO. Retrieved 2010-07-21.

[4] Carl Scheffler’s Chaocipher articles can be found on his web site: http://www.inference.phy.cam.ac.uk/cs482/projects/chaocipher/

[5] Government Code and Cipher School. 1944. *Cryptographic Dictionary*. Secret Document, Bletchley Park. NARA: RG457, box 1412, item 4559. Accessible on-line at http://www.codesandciphers.org.uk/documents/cryptdict/page45.htm. Retrieved 2010-08-02.

[6] A copy of Byrne's 1937 pamphlet "Chaocipher – The Ultimate Elusion", as declassified by NSA, can be seen at:
http://www.mountainvistasoft.com/chaocipher/nsa-foia/foia-contents.htm .
The specific page showing the specific group on line 184 can be found at:
http://www.mountainvistasoft.com/chaocipher/nsa-foia/The-Ultimate-Elusion.08.cropped.gif .

[7] The last page of the declassified 1937 pamphlet can be seen at:
http://www.mountainvistasoft.com/chaocipher/nsa-foia/The-Ultimate-Elusion.10b.cropped.gif. Retrieved 2010-08-02.

[8] Wikipedia article about Rosario Candela, http://en.wikipedia.org/wiki/Rosario_Candela. Retrieved 2010-080-2.

[9] The Chaocipher Clearing House. Progress Report #1.
http://www.mountainvistasoft.com/chaocipher/chaocipher-001.htm. Retrieved 2010-08-03.

[10] Wikipedia article, *Known-Plaintext Attack*. http://en.wikipedia.org/wiki/Known-plaintext_attack. Retrieved 2010-08-04.

[11] Wikipedia article, *Cryptanalysis*.
http://en.wikipedia.org/wiki/Cryptanalysis#Types_of_cryptanalytic_attack. Retrieved 2010-08-05.

[12] Wikipedia article, *Purple (cipher machine)*. http://en.wikipedia.org/wiki/Purple_code. Retrieved 2010-08-05.

[13] Wikipedia article, Lorenz cipher. http://en.wikipedia.org/wiki/Lorenz_cipher. Retrieved 2010-08-05.

[14] The Chaocipher Clearing House, *Progress Report #12*.
http://www.mountainvistasoft.com/chaocipher/chaocipher-012.htm. Retrieved 2010-08-05.

This page discusses one of the most fascinating declassified reports affording a view into the world of real-life cryptanalysis. The report, entitled "*Preliminary Historical Report of the Solution of the "B" Machine*" and written by William F. Friedman, describes in wonderful technical detail how the Americans cryptanalyzed the highest Japanese diplomatic cipher, codenamed "PURPLE". It resides on Frode Weierud's excellent CryptoCellar web site (http://cryptocellar.org/). This document is a must-read for any serious student of classical cryptanalysis.

[15] John Byrne, Cipher A. Deavours and Louis Kruh. *Chaocipher enters the computer age when its method is disclosed to Cryptologia editors*. Cryptologia, 14(3): 193-197. Can be ordered at http://www.informaworld.com/smpp/content~db=jour~content=a741902642. Retrieved 2010-08-06.

[16] Easton, Stewart C. 1980. *Rudolf Steiner: Herald of a New Epoch*. Spring Valley, NY: Anthroposophic Press.

[17] On page 1 of NSA's declassified copy of "Chaocipher – The Ultimate Elusion" you can see Byrne's handwritten correction of line 4, group 6 from "LWYIQ" to "LYWIQ". Byrne's correction can be seen at:
http://www.mountainvistasoft.com/chaocipher/nsa-foia/The-Ultimate-Elusion.01.cropped.gif. Retrieved 2010-08-06.