John F. Byrne's Chaocipher Revealed: An Historical and Technical Appraisal

MOSHE RUBIN[1]

Abstract Chaocipher is a method of encryption invented by John F. Byrne in 1918, who tried unsuccessfully to interest the US Signal Corp and Navy in his system. In 1953, Byrne presented Chaocipher-encrypted messages as a challenge in his autobiography *Silent Years*. Although numerous students of cryptanalysis attempted to solve the challenge messages over the years, none succeeded. For ninety years the Chaocipher algorithm was a closely guarded secret known only to a handful of persons. Following fruitful negotiations with the Byrne family during the period 2009-2010, the Chaocipher papers and materials have been donated to the National Cryptologic Museum in Ft. Meade, MD. This paper presents a comprehensive historical and technical evaluation of John F. Byrne and his Chaocipher system.

Keywords ACA, American Cryptogram Association, block cipher encryption modes, Chaocipher, dynamic substitution, Greg Mellen, Herbert O. Yardley, John F. Byrne, National Cryptologic Museum, Parker Hitt, *Silent Years*, William F. Friedman

1 Introduction

John Francis Byrne was born on 11 February 1880 in Dublin, Ireland. He was an intimate friend of James Joyce, the famous Irish writer and poet, studying together in Belvedere College and University College in Dublin. Joyce based the character named Cranly in Joyce's *A Portrait of the Artist as a Young Man* on Byrne, used Byrne's Dublin residence of 7 Eccles Street as the home of Leopold and Molly Bloom, the main characters in Joyce's *Ulysses*, and made use of real-life anecdotes of himself and Byrne as the basis of stories in Ulysses. Byrne was an eclectic person: he was a very strong chess player who won numerous tournaments in Dublin [24], while being knowledgeable in the writings of Spinoza [2, pp. 178-185].

Byrne left Ireland for the United States in 1910, residing over the years in different boroughs within New York City. During that time he was employed as a reporter, editorial writer, financial editor [23, p. 257], and daily columnist, contributing at different times to the Daily News Record, the New York Times, Poor's Manual, and the Wall Street Journal. He also wrote for numerous magazines and newspapers abroad, occasionally writing under the pseudonym of J. F. Renby [44].

In 1953 Byrne published his autobiographical *Silent Years: An Autobiography with Memoirs of James Joyce and Our Ireland* [2]. While adding much insight about the Irish struggle at the turn of the 19th century and of Byrne's intimate acquaintance with James Joyce, the primary reason for publishing the book was to be on record regarding 'Chaocipher', a cryptographic system he invented in 1918 [56].

Chaocipher was to take up much of Byrne's energies until his death in April 1960. From about 1920 to 1950 Byrne tried unsuccessfully to interest U.S. military and government agencies to adopt Chaocipher.

[1] Address correspondence to Moshe Rubin, Rechov Shaulson 59/6, Jerusalem, Israel 95400. E-mail: moshe.rubin@gmail.com

The purpose of this paper is to summarize what is currently known about John F. Byrne and his Chaocipher invention.

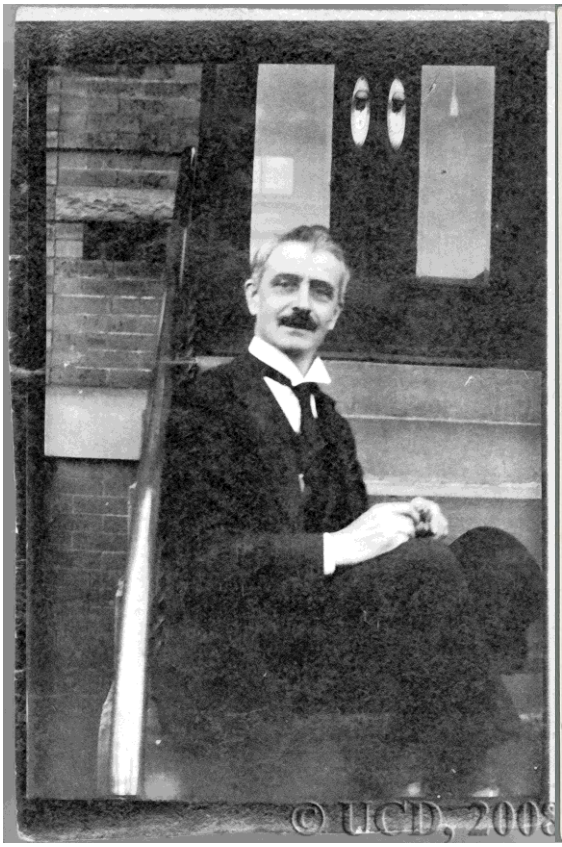


Figure 1: Photograph of John F. Byrne (circa 1924). Reproduced with kind permission of Helen Curran Solterer.

Figure 2: Photograph of John F. Byrne (date unknown[2]). Reproduced with kind permission of Helen Curran Solterer.

2 1918 to 1953: From Invention to Publication

Throughout the period of 1918 – 1953 Chaocipher was unknown to the general public. During this time John F. Byrne contacted numerous agencies and personages, demonstrating his system when possible. As Byrne probably requested confidentiality regarding Chaocipher, the cipher was known only to Byrne himself and a select number of military and government persons.

In 1918 Byrne conceived the concept of Chaocipher, doing most of the design in his head, seldom committing his thoughts to paper. In June 1919 he went to Washington to consult with Marcellus Bailey[3], a

[2] According to the Irish Virtual Research Library and Archive, the back of the photo says "La Bergerie 1917". In this photograph, however, Byrne is most visibly older than the photograph to its left (i.e., circa 1924) so one of the datings may be inaccurate. For information about the photos, see [28].

[3] Marcellus Bailey (1840 – January 16, 1921) was an American patent attorney who, with Anthony Pollok, helped prepare Alexander Graham Bell's patents for the telephone and related inventions (from Wikipedia).

well-known patent attorney. Bailey advised him to prepare blueprints before applying for a patent. The blueprints were finished six months later, but initial estimates for producing a working machine varied from $5,000 - $20,000 [2, p. 267] ($65,500 - $262,000 in 2010 costs)[4].

In 1920, based on the advice of a lawyer friend of his, Byrne sounded out the State Department in Washington with the hope of being able to interest them in Chaocipher, only to have his papers returned with the explanation that the department "does not feel that it can undertake to pass upon the value of an invention of this sort" [2, p. 272].

Besides a reference to a secret-cipher transcript he smuggled into London for Irish rebels [2, p. 119, 134 ff], there seems no other evidence that Byrne was interested in ciphers. This makes it all the more interesting that Byrne's first known foray into cryptography produced a cipher more sophisticated and secure than most inventors.

1921 – 1922: Correspondence with Parker Hitt

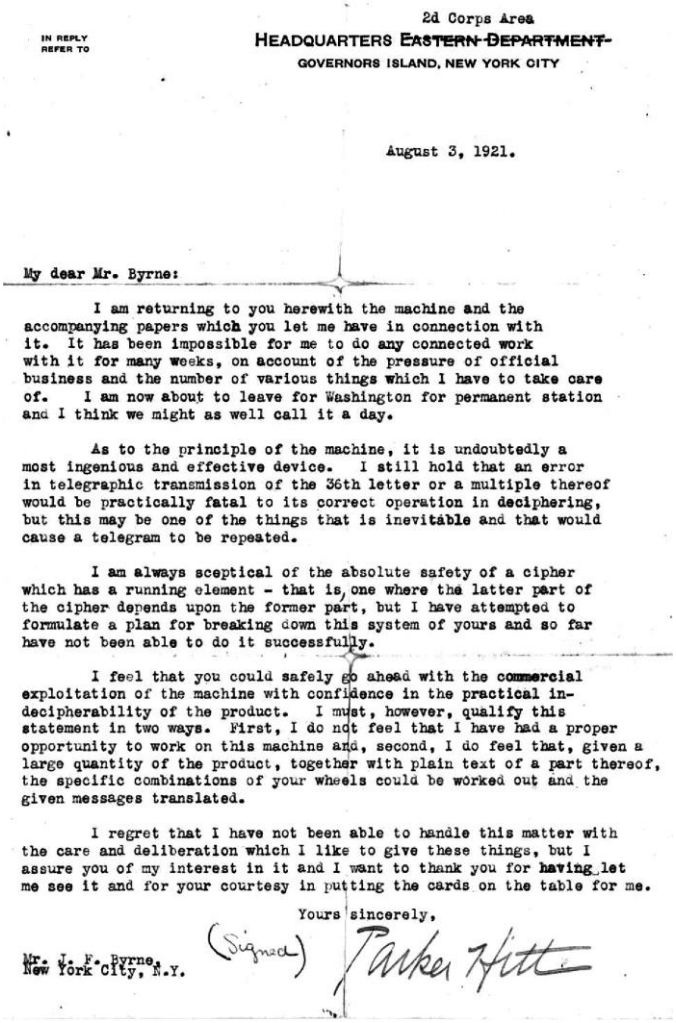
In the following year, 1921, encouraged by a new President in the White House and a new Secretary of State in the State Department, Byrne decided to contact Colonel Parker Hitt at the War College in Washington. Hitt, the author of the seminal treatise *Manual for the Solution of Military Ciphers*, was suitably impressed with the underlying principle of Chaocipher and wrote to Byrne on 3 August 1921:

> "*As to the principle of the machine, it is undoubtedly a most ingenious and effective device. I still hold that an error in telegraphic transmission of the 36th letter or of a multiple thereof would be practically fatal to its correct operation in deciphering, but this may be one of the things that is inevitable and that would cause a telegram to be repeated.*
>
> *I am always skeptical of the absolute safety of a cipher which has a running element – that is, one where the latter part of the cipher depends upon the former part, but I have attempted to formulate a plan for breaking down this system of yours and so far have not been able to do it successfully.*
>
> *I feel that you could safely go ahead with the commercial exploitation of the machine with confidence in the practical indecipherability of the product. I must, however, qualify this statement in two ways. First, I do not feel that I have had a proper opportunity to work on this machine and, second, I do feel that, given a large quantity of the product, together with plaintext of a part thereof, the specific combinations of your wheels could be worked out and the given messages translated.*" [42, see Figure 3]

It is educational to see how selective Byrne was when extracting out-of-context quotes from Hitt's letter. The underlined text above is what Byrne quoted in *Silent Years* [2, p. 273] – he consistently left out any portion of Hitt's letter that could point to a weakness or drawback in Chaocipher. Nonetheless, Hitt did acknowledge that Chaocipher had merit.

Buoyed by Hitt's glowing appraisal, Byrne once again sent a letter to the State Department in September 1921, only to be rudely disappointed by their unjustifiably smug reply that "*while the Department appreciates your courtesy in bringing this matter to its attention, the codes and ciphers now used are adequate to its needs*" [2, p. 274].

[4] Calculated using http://www.dollartimes.com/calculators/inflation.htm, assuming an annual inflation rate of 2.87%.



2d Corps Area
IN REPLY REFER TO
HEADQUARTERS ~~EASTERN DEPARTMENT~~
GOVERNORS ISLAND, NEW YORK CITY

August 3, 1921.

My dear Mr. Byrne:

I am returning to you herewith the machine and the accompanying papers which you let me have in connection with it. It has been impossible for me to do any connected work with it for many weeks, on account of the pressure of official business and the number of various things which I have to take care of. I am now about to leave for Washington for permanent station and I think we might as well call it a day.

As to the principle of the machine, it is undoubtedly a most ingenious and effective device. I still hold that an error in telegraphic transmission of the 36th letter or a multiple thereof would be practically fatal to its correct operation in deciphering, but this may be one of the things that is inevitable and that would cause a telegram to be repeated.

I am always sceptical of the absolute safety of a cipher which has a running element - that is, one where the latter part of the cipher depends upon the former part, but I have attempted to formulate a plan for breaking down this system of yours and so far have not been able to do it successfully.

I feel that you could safely go ahead with the commercial exploitation of the machine with confidence in the practical indecipherability of the product. I must, however, qualify this statement in two ways. First, I do not feel that I have had a proper opportunity to work on this machine and, second, I do feel that, given a large quantity of the product, together with plain text of a part thereof, the specific combinations of your wheels could be worked out and the given messages translated.

I regret that I have not been able to handle this matter with the care and deliberation which I like to give these things, but I assure you of my interest in it and I want to thank you for having let me see it and for your courtesy in putting the cards on the table for me.

Yours sincerely,

(Signed) Parker Hitt

Mr. J. F. Byrne,
New York City, N.Y.

Figure 3: Parker Hitt's original letter to John F. Byrne

1922: Major Moorman and William F. Friedman

Disappointed but undeterred, Byrne contacted Parker Hitt again in 1922 [2, p. 275]. Hitt, who in the interim had taken up a permanent station in Washington, was willing to introduce Byrne to Major Frank Moorman, a former cryptographic student of Hitt's connected with the Signal Corps. Byrne promptly traveled to Washington in March to meet Hitt who warmly introduced him to Major Moorman and William F. Friedman, then employed as a civilian cryptanalyst. Byrne demonstrated his Chaocipher to Moorman and Friedman, leaving his rudimentary model with them for analysis.

Not having heard from Moorman or Friedman by August, Byrne wrote them requesting that the device be returned to him. A few days later Byrne received his model, inadvertently damaged in transit. In a subsequent letter to Byrne on 7 September, in which Friedman profusely apologized for the damage, Friedman explained that he had waited for an improved model Byrne had promised to send (the original model "was very difficult to operate, giving doubtful letters and permitting errors to arise due to faulty operation of the model"). During this period Friedman analyzed the system and prepared a personal internal report based on his findings. He invited Byrne to resubmit a series of fifty messages of twenty-five words each, enciphered using the same original model [51]. Byrne apparently never took Friedman up on the offer.

1937 - 1938: The U.S. Navy

Disappointed, Byrne put Chaocipher aside for the next fifteen years. In 1937 he read a newspaper item that the U.S. Navy had requested a special congressional appropriation for developing an undecipherable cryptographic system. Byrne saw his opportunity and set about submitting Chaocipher as a candidate system. He commissioned a private printing of a pamphlet entitled *Chaocipher – The Ultimate Elusion* [40]. The pamphlet consisted of ten pages of ciphertext corresponding to a known 55-letter phrase enciphered 100 times, followed by the Declaration of Independence and the Gettysburg Address. Byrne prepared this text for a presentation to the US Navy Department and later printed 500 copies of the pamphlet as an informational flyer for potential "customers". Ready to submit Chaocipher for the Navy's perusal, Byrne sent a letter to Admiral Harold G. Bowen. In the ensuing correspondences, Byrne was invited to come to Washington to demonstrate his machine.

Byrne showed up in Washington on 3 May 1938 to give his demonstration which, according to Byrne, never took place [2, p. 279]. The panel of three Commanders included Samuel M. Tucker[5] as an expert in radio and electronics, and Joseph N. Wenger as cipher expert[6]. After a short meeting Tucker suggested he should take his device either to the War Department or the State Department[7].

1942: Friedman Reapproached

Four years were to pass before Byrne tried again. In March 1942 he demonstrated Chaocipher to Ralzemond D. Parker and others at Bell Telephone, this being the first time Byrne had ever demonstrated Chaocipher to a non-governmental agency. The reception was positive, with Parker suggesting that Byrne should reapproach William F. Friedman, who by now was Head Cryptanalyst in the US Signal Corps with the rank of Colonel.

On 3 June 1942 Byrne sent Friedman a letter reintroducing himself and reminding Friedman of their meeting twenty years earlier. Friedman obviously had no problem recalling his previous encounter; he delegated the task of replying to Byrne to Lieutenant Charles H. Hiser[8] [50], telling him "We are in for a bit of razzing here, I'm afraid. See what you can draw up by way of reply". [52]

The reply sent to Byrne on 6 June was courteous and professional. Besides a cover letter, it contained two enclosures sent standardly to anyone submitting a cipher system to the Signal Corps [59]. Enclosure A clearly

---

[5] Lieutenant Commanders Samuel M. Tucker and F.R. Furth coined the acronym 'radar' in November 1940, see http://www.meteor.iastate.edu/~jdduda/portfolio/571_write_up.pdf.

[6] Byrne refers to the two younger Commanders as Wagner and Tucker. I believe Byrne incorrectly refers to Lieutenant Commander Joseph N. Wenger. As a Communications Intelligence career officer and a cryptanalyst, Wenger headed OP-20-GY , the Navy cryptanalytic agency in Washington, during most of World War II. By 1937-1938 Wenger was a critical player in the field of machine processing and aided in the development and refinement of cipher devices which were adopted by the U.S. Navy. He would therefore have been supremely qualified to sit in on this meeting with Byrne. See Weller, Robert, 1984. Rear Admiral Joseph N. Wenger USN (Ret) and the Naval Cryptologic Museum. Cryptologia. 8(3): 208-234. This theory is upheld by David Kahn in *The Codebreakers* (page 768) who writes "negotiating apparently with Commander Joseph N. Wenger …".

[7] On 4 May 1938, the day following Byrne's aborted demonstration, the US Navy submitted a patent for a rotor machine known as the ECM Mark III (U. S. Patent 4,143,978). It is safe to assume that Tucker and Wenger had already decided on adopting the ECM Mark III. From Byrne's memorandum to G. M. Campbell [5] it would seem that Byrne at least began his demonstration to the Navy. See http://www.quadibloc.com/crypto/ro020703.htm for information about the ECM Mark III.

[8] Colonel Charles H. Hiser, 29 Dec 1915 - 28 Aug 1988.

explained the most important requirements which a cryptographic system for military use must fulfill (i.e., practicality and secrecy). Enclosure B was a form to be used when submitting a cipher system, and specified what type and quantity of enciphered material should be presented with the submission. Enclosure B clearly stated that a potential cipher inventor needed to provide the following material:

> "(aa) A detailed, complete statement of the basic cryptographic method.
>
> (bb) At least one example of a plain-text message of a minimum of 50 words in good English; all the keys employed in the encipherment of this message; and the final cryptogram. A step-by-step, detailed description of how the plain-text message is converted into the cipher message must be included.
>
> (cc) A minimum of three cryptograms, each being the enciphered version of the *same* plain-text message of at least 750 letters, in good English, the specific keys being *different* in each case. Neither the plain-text version of the cryptograms nor the keys pertaining thereto should be included.
>
> (dd) A minimum of 20 cryptograms, each being the encipherment of a *different* plain-text message of at least 100 letters, in good English, the specific key being exactly the same for these 20 messages. Neither the plain-text versions of these cryptograms nor the keys pertaining thereto should be included."

Byrne's reply to Friedman on 9 June was less courteous. Ignoring Friedman's justified request for standard material, Byrne wrote:

> "Now, keeping in mind this "Chaocipher" document alone: and prescinding from any other consideration of my cipher system, can you answer the following question? Do you deny my assertion that this cipher document as it stands is indecipherable?" [53].

Not understanding the science of cryptanalysis, Byrne could not comprehend why these sets of messages were necessary. Friedman's professional requests were probably seen by Byrne as bureaucracy at best and procrastination at worst[9].

Friedman's reply [54] was professional and to the point: the requirements in Enclosure B had long proved their usefulness. Unless Byrne would see his way to comply, the Chaocipher system could not be examined. Apparently there were no further correspondences at this time[10].

1953: Publication of Silent Years

In 1953 Byrne published his autobiography entitled *Silent Years: An Autobiography with Memoirs of James Joyce and Our Ireland* [2]. The book, published by Farrar, Straus & Young and containing 307 pages within its 21 chapters, paints a picture of Dublin as Byrne knew it at the beginning of the twentieth century. The book reveals many aspects of Byrne's life as a child in Ireland, his acquaintance with James Joyce, touching upon colorful personages along the way. It disclosed for the first time that Byrne was the real-life model of Cranly in Joyce's famous *A Portrait of the Artist as a Young Man* [63].

---

[9] This occurred almost two years after the Army Corps, led by Friedman and Rowlett, deduced the nature of the Japanese PURPLE machine. One can understand why Friedman was not enamored by a cipher system rising or falling on a single submitted message.

[10] A worksheet dated February 25, 1947 and found in the National Cryptologic Museum library, showing alphabets derived from the keyword "COMPREHENSIBLEX" using the disk pattern "LRRLLRRLRRRLLRL", adds the text "To encipher Friedman test stuff: …". This seems to indicate that Byrne was preparing material for Friedman as late as 1947. It is significant that Byrne does not recount any of this in *Silent Years*.

The book also presents some of Byrne's previously published material. As one who identified strongly with the Irish right to Home Rule from Britain, he dedicated Chapter 10 to his polemic entitled *The Irish Grievance* [2, pp. 102-122, 7]. Chapter 19 carried *A Parable in Gold*, an article Byrne was supremely proud of, which dealt with the gold standard and America's growing international debts and which was read by members of President Franklin D. Roosevelt's administration. Chapter 20 presented a science fiction story called *The Throne of Chaos*, a prophetic view of where the discovery of unlimited energy can lead [2, pp. 249-263].

Byrne's overriding purpose for writing *Silent Years* was, in his own words:

> I had three main reasons for writing "Silent Years" […] two of the lesser reasons were my story in the book, titled "The Throne of Chaos" and my chapters on "A Parable in Gold". But my main reason for writing the book was to be on record in the matter of my "Chaocipher". [56]

The book received a positive review in 1954 from reviewer Richard Ellmann (the renowned biographer of James Joyce) in the Saturday Review [21].

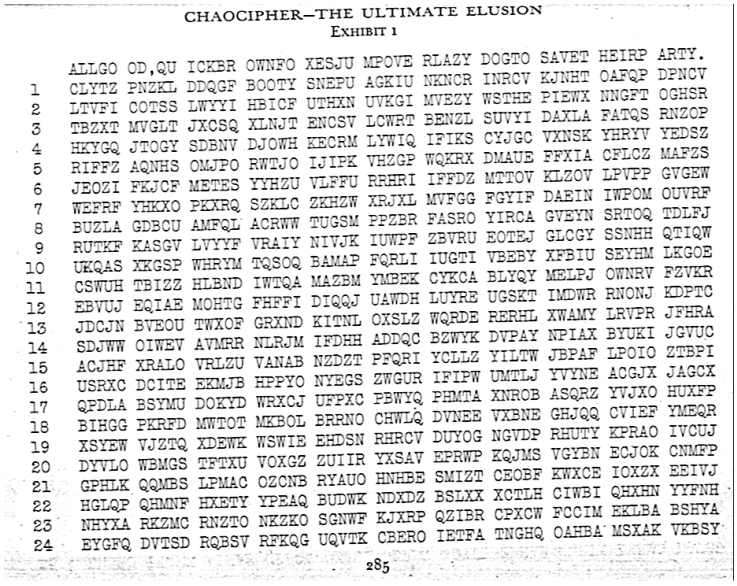
Chapter 21, entitled "Chaocipher", is dedicated in its entirety to Byrne's cipher brainchild. The chapter begins with 21 pages of prose detailing Byrne's inventing of Chaocipher in 1918 and his subsequent attempts over the next 35 years to interest others in it. Following this are four exhibits, spread over the next 23 pages.

Exhibit 1 is 13,615 characters long, with each line consisting of eleven 5-letter groups, amounting to 248 lines of text. The first one hundred lines consist of the encipherings of the 55-letter sequence:

ALLGO ODQQU ICKBR OWNFO XESJU MPOVE RLAZY DOGTO SAVET HEIRP ARTYW

with 'Q'and 'W' representing a comma and a period respectively. These one hundred lines are followed by the enciphered texts of the Declaration of Independence and the Gettysburg Address. The Declaration of Independence is preceded by 262 cipher characters for which no text is given (this was Byrne's challenge to would-be solvers).

The complete plaintext follows the aforementioned ciphertext, save for the 262 enciphered challenge 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 4: Exhibit 1 in Silent Years

Exhibit 2 is 1263 characters long, consisting of Latin plaintext from Julius Caesar's *De Bello Gallico* (Commentaries on the Gallic War).

Exhibit 3 consists of the opening sentence of Parker Hitt's *Manual for the Solution of Military Ciphers* [26] repeated five times, resulting in a total of 910 plaintext/ciphertext pairs.

Exhibit 4 differs from the previous exhibits in that the plaintext, a speech of General Douglas MacArthur[11], is shorter than the ciphertext. This requires the would-be solver to determine how the plaintext and ciphertext map to each other. Byrne does mention that the ciphertext of Exhibit 4 contains "full and complete instructions to an initiate for its decipherment [2, p. 283]. He also adds that he reenciphered "a little over a dozen words, with punctuation marks" [2, p.283] in the last two lines of the cipher. This, supposedly, would be the way a would-be solver could prove his cryptanalytic success.

3 1953 to 2010: Post-Publication to Disclosure

From 1953 until his death in 1960, Byrne continued to champion the Chaocipher cause. Although Byrne no longer approached government institutions directly, he continued to contact individuals in the hope of furthering Chaocipher.

1954: Byrne Meets Henry E. Langen

Soon after publication of *Silent Years*, Byrne received a request from Henry E. Langen [13], editor of the American Cryptogram Association's periodical, *The Cryptogram*, to demonstrate Chaocipher. This request led to Byrne's visiting Langen in New Jersey on 25 May 1954. For two hours they discussed his book and Chaocipher, but Byrne did not bring the cipher machine "explaining that it was too heavy and cumbersome". Instead he brought the Chaocipher blueprints, but Langen failed to grasp the concept. Langen commented in his diary that "With only two disks used, I am a bit confused as to how this can result in such utter chaotification of the plaintext message." For a complete summary of Langen's dealings with Byrne and Chaocipher, see [31].

1954: Friedman's Lecture about Silent Years and Chaocipher

On 13 March 1954 William F. Friedman, two years away from retiring from NSA, delivered a speech at the American Association of University Women in Washington D.C. The evening featured Joycian experts, and Friedman was asked if he would comment on Byrne's *Silent Years*. Friedman delivered a speech in which he was highly critical of Byrne's claims, but did not reveal anything about the system "because our government has taken care, by means of a special law, that its cryptologic secrets will be kept". Notes scribbled by Friedman when preparing his speech give us a better insight into Friedman's thoughts about Chaocipher:

(a) Friedman disagreed with Poe's dictum that a holocryptic[12] cipher does not exist, an observation no doubt based on real-life experience.

(b) He noted that his 1922 letter to Byrne denied that Chaocipher was indecipherable.

(c) Friedman intimates that Chaocipher does not produce perfectly random ciphertext; rather, a consecutive plaintext repetition cannot result in a ciphertext repetition.

[11] Byrne used text from General Douglas MacArthur's address to the US Congress, 19 April 1951. There are differences between the different transcript of this speech; Byrne obviously used one of the many versions.

[12] The word 'holocryptic' is defined as 'wholly or completely concealing; incapable of being deciphered'. Thus, a holocryptic cipher is a cipher so constructed as to afford no clue to its meaning to one ignorant of the key.

(d) He took great umbrage to Byrne's insinuation that he broke the original crude model on purpose.

Beside these observations Friedman's speech did not add or disclose any details about Chaocipher.

1957: Friedman Reapproached II

The next time Byrne approached someone regarding Chaocipher, as far as the record discloses, was when he contacted Friedman on 29 January 1957. The purpose of Byrne's initial letter was, once again, to elicit a clear answer from Friedman: was Chaocipher indecipherable or not? Friedman answered on 6 February, saying:

> "I do remember you very well – and the remembrance was kindled by my reading The Silent Years. I never did figure out why you put in that book the completely extraneous matters of ciphers when you had so much of interest to tell about Joyce."[55]

This was certainly not what Byrne wanted to hear from Friedman. In his reply of 17 February Byrne put the question bluntly:

> "Now, to get to the point: it is my conviction that my Chaocipher system is universally available and is forever indecipherable. Have you any comment to make on this conviction of mine? Do you think I am right, or do you think I am wrong?" [56]

When Byrne did not receive a prompt reply he reissued his question in a letter on 28 February:

> "And may I ask you kindly to reply to my questions as propounded in my letter of February 17th? I am doing this because I do not think you are any longer officially connected with the U.S. Government as a Cryptanalyst. If I am wrong in this assumption, you will please tell me. But, otherwise, I would ask you to answer the questions that I have asked you at your earliest possible convenience". [57]

Friedman did reply on 3 March 1957, leaving no doubt as to what he felt about Chaocipher and Byrne's insistence on its indecipherability:

> "You appear to be so concerned about your "Chaocipher" system that I will answer your letters of 17 and 28 February, despite my rather precarious state of health.
>
> […] The days when "hand ciphers" were all that were available are gone – automation in cryptography began more than a dozen years ago and I don't think even the smaller or smallest nations today care a fig about them. […] Many, many experienced and well-trained engineers have been working for a score of years on this problem [ed. automated, secure systems], with the finest tools and facilities that our government could give them. What makes you think you have done something that they have not thought of or have overlooked? To repeat, solving or not solving your examples would prove absolutely nothing."[58]

This is the last record we have of Byrne corresponding with Friedman.

1958: Herbert O. Yardley

In June 1958 we encounter Byrne's final Chaocipher-related communication on record: a correspondence with Herbert O. Yardley, author of *The American Black Chamber*. Following the publication of Yardley's final book *The Education of a Poker Player* in 1957, Byrne wrote to Yardley on 1 June 1958 [27], raising the same issue against Yardley that Byrne had written about in *Silent Years*.

The core of the issue related to an episode told over in *The American Black Chamber* [65, pp. 85-86]. In the episode Yardley related how he was tasked by his superior, Col. Van Deman, to decipher a given message at

any cost. After spending a night working on it Yardley declared to Van Deman that, based on scientific analysis the message was a fraud, a collection of letters randomly typed on a typewriter.

As Byrne understood it, Yardley deduced the message was a fraud because its first-order letter frequency counts were totally "flat" (i.e., evenly distributed). This, in Byrne's mind, was the only way one could declare a message to be a "fraud". Since he believed Chaocipher to produce a perfectly random output and corresponding "flat" letter counts, and knowing that Chaocipher was not a "fraud", it therefore followed that Yardley's deduction was flawed[13].

Beginning his letter with a personal anecdote about Poker, Byrne soon got to the true purpose of the letter when he wrote about Chaocipher "In fact, the product is such as to yield to no process of analysis, and appears, on minute study, to be what might be described in your own book as a 'fraud and a fake, put together by someone who had picked out a jumble of letters on a typewriter"'. In essence, he demanded that Yardley admit that a cryptanalyst could never deduce that such a given message was a fraud, and that Chaocipher produced ciphers of this type.

Yardley responded on 8 June, addressing the story of the fraudulent message, adding:

> "I am no longer interested in codes and ciphers. Am Sorry."

Byrne responded on 24 June, demanding to know whether

> "a cipher system … which would forever produce such a product as would be totally inscrutable and indecipherable , do you or do you not, think that there would be a universal market for such a system, especially if the system I stipulate were to be produced electronically?"

To Byrne's dissatisfaction Yardley replied very briefly on 19 July, prompting Byrne to write once again to Yardley on 24 July, reiterating his question. Unfortunately Byrne was not to hear again from Yardley, who suffered a stroke a week later and passed away on 7 August 1958.

4 Previous Attempts at Solution

Byrne's Chaocipher made its first public appearance in his autobiography, *Silent Years*. It is unknown who attempted to solve the system when the book appeared. What is clear is that no one stepped forward to claim the prize offered by Byrne.

At the time of writing there is no evidence of government agencies like NSA or GCHQ trying to solve Chaocipher, and Freedom of Information Act (FOIA) requests have not unearthed any such evidence. The record of non-governmental persons attempting to solve Chaocipher, however, begins in the late 1970's and onwards. The following sections discuss the attempts made to solve Chaocipher, by whom and when.

[13] Although one theoretically cannot prove that a given message is not genuine ("proving a negative"), we can assume Yardley examined evidence other than first-order frequencies, enabling him to declare strongly that no known cipher system could display the same randomness in all observed aspects.

The 1960s: The Codebreakers

The first published description of Chaocipher and its history following the publication of *Silent Years* is in David Kahn's *The Codebreakers* [29, pp. 767-768]. Kahn presented an historical description of J. F. Byrne together with quotes from *Silent Years*. In Kahn's opinion Chaocipher was an autokey cipher[14].

The 1970s - 1980s: Members of the American Cryptogram Association (ACA)

The next published call to break Chaocipher was Gary Knight's *Cryptanalyst's Corner* in Cryptologia (April 1978). Knight gave a basic description of the history of Chaocipher, including excerpts from Exhibits 1 and 3 for the readers' perusal. Regarding his thoughts about Chaocipher Knight wrote "My own tentative conclusion, which should certainly not prejudice the reader's own analysis, is that Byrne probably developed a crude rotor or Vernam tape system that produced a polyalphabetic cipher with a fairly long period".

This was followed by Greg Mellen's landmark article, *J. F. Byrne and the Chaocipher: Work in Progress* [33]. The editor noted that the manuscript was received on 1 December 1978, and Mellen wrote "For the past two years, I have been examining the Chaocipher from a special point of view". We can therefore assume that Mellen began studying Chaocipher in 1976 or 1977.

Mellen's paper was a true *tour de force*: it afforded the first in-depth and complete description of Chaocipher in the open cryptologic literature, providing both the necessary historical context, pointing out significant patterns in the texts, and giving direction for further research. Mellen did not solve any part of Chaocipher; he did, however, provide a hypothetical cipher system that might match the observed patterns.

Behind the scenes, several American Cryptogram Association (ACA) members were working on Chaocipher. These included William G. Sutton (ACA *nom de plume* PHOENIX), Greg Mellen (CODEX), Jeff Hill (E. E. REMINGTON), Mike Barlow, Wesley Horton (DRIVE-IN), Jim Gillogly (SCRYER) and Rudy Lauer (ONYX, author of a popular cryptographic book [32]). Besides communicating between themselves, several of them made contact with Byrne's son John in the hope of convincing him to disclose the system or information about it.

Wesley Horton succeeded in interesting Abe Sinkov, one of Friedman's original cryptanalysts in the 30's, in Chaocipher in the early 1980's. No further record remains of what Sinkov did with it, but the fact that he hadn't heard of Chaocipher until then demonstrates that Friedman most likely never disclosed Chaocipher to his junior cryptanalysts, and to Sinkov for certain.

The 1990s: The Kruh and Deavours Article

The July 1990 issue of Cryptologia contained a turning-point paper for would-be Chaocipher researchers. The paper, entitled *Chaocipher Enters the Computer Age When its Method is Disclosed to Cryptologia Editors* [3] and authored by Lou Kruh and Cipher Deavours, fired the imagination of amateur cryptanalysts interested in Chaocipher. Lou Kruh had managed to find John F. Byrne's son, John Byrne, an architect living in Vermont. After resisting Kruh's attempts for many years, John finally agreed to disclose Chaocipher's inner workings to Kruh and Deavours[15].

---

[14] In a private email communication between David Kahn and this author on 21 November 2010, Kahn was unable to recall where he got the theory of an autokey as part of his research.

[15] The meeting took place at Deavours's home in New Jersey, with John, his wife Pat, Tony Bean (John's nephew), and his wife Brenda attending. John and Tony showed Kruh and Deavours the drawings and components of John's rudimentary model. As Tony relates "I remember both Cy and Lou getting very excited about this disclosure and after dinner Cy retired to his study and wrote a small [8080] assembly language program that replicated the Chaocipher

This disclosure led to Kruh and Deavours publishing their 1990 article in Cryptologia. While not revealing how Chaocipher worked, the article did present tantalizing hints about how it operated. It also added three more "in-depth" messages to work on (known as "Exhibit #5") [3]. The set consisted of :

> "... three messages of approximately 25 words each as an "in depth" specimen of Chaocipher (as opposed to the original exhibits in *Silent Years*, each of which was enciphered in a single continuous key). The plaintext, which is typical English prose, is taken from Stewart C. Easton's book, 'Rudolf Steiner: Herald of a New Epoch' [20]".

There was a general sense of disappointment that the article did not disclose the system, but Kruh and Deavours were not at liberty to do so. In a subsequent issue of Cryptologia Kruh and Deavours wrote [45]:

> "The article on Chaocipher (Cryptologia XIV(3): 193-198) disappointed several readers who expected it or a follow-up paper to disclose how it worked. Because no solutions were received, there was no need for another story. The article never suggested that the Chaocipher system would be revealed. In fact, it specifically pointed out that the reason for providing further information on Chaocipher was to determine if it had commercial value as a computer security algorithm. Presumably, if the messages were solved, permission would be given to describe Chaocipher's secret."

Kruh proposed a reveal-all disclosure article in 1996 for Cryptologia's 20th anniversary issue, but it never materialized in the end[16].

Figure 5: John F. Byrne and his ten year old son, John Byrne (with permission from the National Cryptologic Museum of the National Security Agency).

---

algorithm. […] I do not recall any agreement (other than non-disclosure) ever came although we knew articles would be written for Cryptologia." [1]

[16] Private communication from Jeffrey Hill to Wesley Horton, 23 July 1998. Hill tells how Kruh, at the 1997 American Cryptogram Association (ACA) conference, told him how he asked John Byrne "for a disclosure article to be published in the 20th anniversary issue of Cryptologia (January 1996). Byrne seemed to agree, but the deadline for the article came and went and no disclosure was forthcoming".

The 2000s: The Final Countdown

Chaocipher research seemingly languished from Kruh and Deavours's article until 2008. Searching for the term "chaocipher' on the Web invariably found the hundreds of copycat sites that echoed Elonka Dunin's famous page entitled *Famous Unsolved Codes and Ciphers* [19], while the Wikipedia page for "Chaocipher" was not helpful at all.

In July 2008 this author decided to attack the Chaocipher challenges. In February 2009 he created a web site called *The Chaocipher Clearing House* [8] for the purpose of publishing his own Chaocipher cryptanalytic findings. In parallel he tried to track down every person who had any connection with Chaocipher research over the years. A lead from members of the American Cryptogram Association's (ACA) staff led him to contact Jeffrey Hill, a retired software engineer living in Lincoln, Nebraska. Hill, who had collaborated with Mike Barlow and William Sutton starting in the 1980's, had continued to work on Chaocipher on and off over the years. Next to join over the next few months was Mike Cowan, an ACA member and co-editor of the Computer Column in ACA's publication, *The Cryptogram*. An online forum dedicated to Chaocipher was created [15], providing the platform for others to read, comment, and post about Chaocipher.

The Chaocipher Clearing House web site became the focal point of Chaocipher research, with periodic progress reports being published as research moved ahead.

In June 2009 Hill uploaded a monumental paper entitled *Chaocipher: Analysis & Models* [25]. Besides bringing chronological order to the Chaocipher timeline, Hill attempted to present a hypothetical cipher model that would explain certain significant patterns in Exhibit #1 in *Silent Years*.

The significant pattern observed by several researchers dealt with the frequency of identical pt/ct, or "hits". A hit is two identical pt/ct pairs found within a short distance of each other. Mellen was the first to document the phenomenon when he noted that doubled plaintext letters in Exhibit #1 never resulted in doubled ciphertext letters (i.e., no "hits" at an interval of one). The first few lines in Exhibit #1 in Figure 1 illustrate this, as can be seen in Figure 6:

```
Plaintext: A LL G OO D QQ UICKBROWNFOXES...

Line 1:    C LY T ZP N ZK LDDQGFBOOTYSNE...
Line 2:    L TV F IC O TS SLWYYIHBICFUTH...
Line 3:    T BZ X TM V GL TJXCSQXLNJTENC...
Line 4:    H KY G QJ T OG YSDBNVDJOWHKEC...
Line 5:    R IF F ZA Q NH SOMJPORWTJOIJI...
Line 6:    J EO Z IF K JC FMETESYYHZUVLF...
Line 7:    W EF R FY H KX OPKXRQSZKLCZKH...
Line 8:    B UZ L AG D BC UAMFQLACRWWTUG...
Line 9:    R UT K FK A SG VLVYYFVRAIYNIV...
Line10:    U KQ A SX K GS PWHRYMTQSOQBAM...
```

Figure 6: Mellen's observation of no pt/ct "hits" at distance one

Exhibit #1 in *Silent Years* begins with 100 encryptions of the 55-letter phrase "All good, quick brown foxes …" with the encryptions neatly lined up beneath the plaintext. Mellen noticed that doubled plaintext letters (e.g., "LL", "OO", "QQ") never resulted in doubled ciphertext letters (e.g., "BB" or "XX"), when probabilistically we would expect 20 to 25 such instances. From this observation Mellen hypothesized that "(1) The cipher component necessarily and causally changes from letter to letter, and (2) there is but one cipher component and not a plurality of different, mixed, cipher components."

Other researchers had independently found that "hits" did not occur for intervals less than nine. Based on this observation, it seemed clear that Chaocipher was not the "jargon of random characters" Byrne thought it was. Chaocipher seemed to have a potential Achilles heel.

Steps	Comparisons	Hits (Expected)	Hits (Observed)	Probability (Observed)
1	501	19	0	0
2	406	16	0	0
3	808	31	0	0
4	589	23	0	0
5	641	25	0	0
6	622	24	0	0
7	493	19	0	0
8	796	31	0	0
9	825	32	4	0.005
10	583	22	6	0.010
11	594	23	20	0.034
12	747	29	57	0.076
13	523	20	46	0.088
14	1026	39	81	0.079
15	726	28	38	0.052

Table 1: Frequency of Repeated Machine States, or "Hits", in Exhibit 1

In his important paper Hill presented a statistical graph that showed the observed hit probabilities that occurred at different intervals (the graph tracks the values found in Table 1). When shown, the graph displayed a wave-like form (see Figure 7).

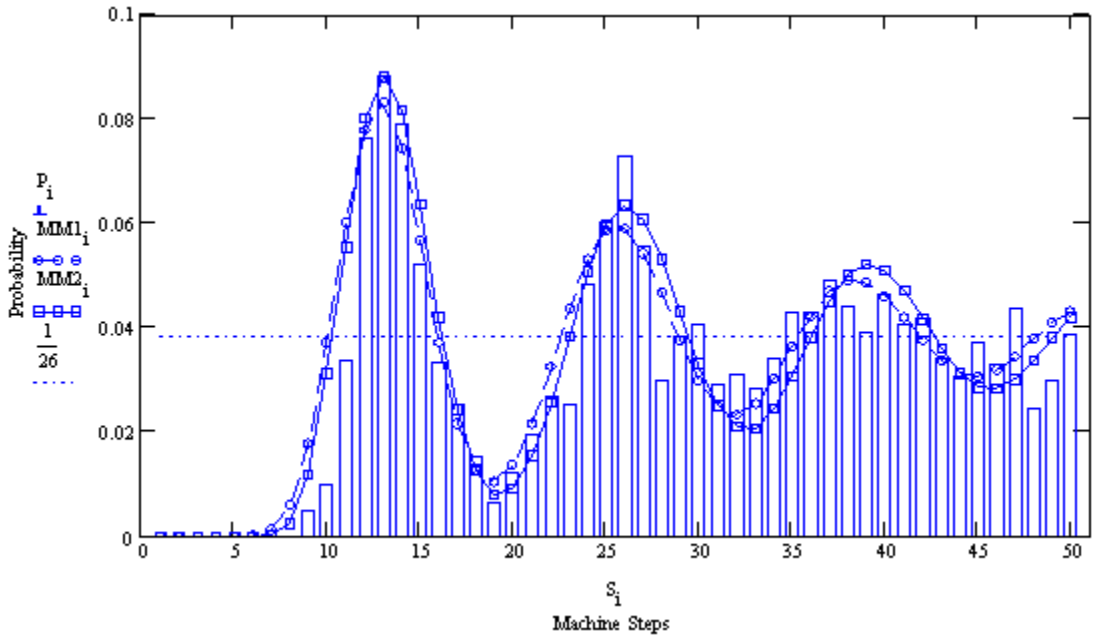


Figure 7: Markov Models fitted to the Probability of Repeated Machine States (courtesy of Jeffrey Hill)

The assumption was that any proposed model would need to exhibit a similar wave-like form. Hill attempted to discover the Chaocipher inner mechanism by presenting hypothetical models that also exhibited the "no hits < 9" phenomenon. In his paper he introduced three progressively more complex models called C98, C98A, and C98U, with the latter being a composite of the previous two models. The core of these models was advancing the keying element by 1, 2, or 4 positions after each encipherment. This keying sequence imparted a Markov-like characteristic to the ciphertext output, which matched the observed graph remarkably well.

The C98 and C98A models were disproven as the Chaocipher model in 2009. In April 2010 this author proved that Chaocipher could not be C98U [17], and a new model was needed.

It was with great interest that parallels were found between Chaocipher and William F. Friedman's summary of the PURPLE cipher solution. In a fascinating document entitled *Preliminary Historical Report on the Solution of the "B" Machine* written on October 14, 1940, Friedman described the history, analysis, and solution of the Japanese PURPLE cipher. Reading the paper showed that Friedman, Rowlett, and their team encountered phenomena and characteristics remarkably similar to what was seen in Chaocipher [10]. These phenomena, observed in Chaocipher, included:

- Jeff Hill had pointed out that John F. Byrne's overwhelming priority was to suppress repetitions. Hence Byrne was proud of the fact that 100 repetitions of the same sentence did not yield repeated sequences. The inventors of PURPLE seemed to have the same goal in mind. Suppression of repetitions, apparent in both PURPLE and Chaocipher, may have indicated deliberate 'tinkering' with the mechanism to bring that about.

- There is no readily discernible cyclic repetition, even for the 13,600+ letters in Exhibit 1.

- The PURPLE group experienced the same phenomenon of no successive pt/ct identities (i.e., at a distance of one). Chaocipher shows no pt/ct identities for all intervals from one to eight, while PURPLE showed no identities for intervals 1 and 26. Even with PURPLE pt/ct identities from two to five were rare.

- Like the PURPLE group, for whom this point "formed the subject of long and arduous study, fruitless experimentation and much discussion", so too Chaocipher researchers -- this exact point consumed much of their time.

- Different Chaocipher messages ("with different indicators") show no similarities or relations.

Freedom of Information Act (FOIA) Requests

In 1985 Wesley Horton submitted a declassification request to NSA based on the Freedom of Information Act (FOIA). In response he received a substantial amount of historical letters and material relating to Chaocipher which was later shared with other ACA researchers at that time.

With no knowledge of Horton's treasure trove, this author submitted an FOIA request in March 2009 for any Chaocipher-related material NSA might have. In response NSA sent a declassified photocopy of Byrne's *Chaocipher – The Ultimate Elusion*. It was only months later that Horton's material was shared with this author. When asked why they had not sent Horton's material, NSA replied that Horton's request had been processed prior to the existence of a FOIA database and was therefore unaware of Horton's previous request.

A request for Chaocipher-related material was made to GCHQ in the UK by Mike Cowan, one of the Chaocipher researchers. GCHQ responded "We have absolutely nothing in our archives about Chaocipher,

and nothing to suggest that anybody at GCHQ (or GC&CS, as we were called from 1919 to 1946) has ever spent time looking at it." [11]

Correspondences Uploaded to The Chaocipher Clearing House

As of May 2010 numerous correspondences between J. F. Byrne and other persons had been tracked down and uploaded to The Chaocipher Clearing House [12]. These included papers declassified by FOIA requests, quotes from *Silent Years*, letters of Byrne's from the James Joyce collection at the Harry Ransom Center at the University of Texas at Austin, William F. Friedman's papers at the George Marshall Library, and others. It was hoped that these letters would provide a clue on the arduous path of solving Chaocipher.

The Search for Chaocipher

The state of Chaocipher research as of August 2009 was that a handful of researchers was trying to determine the inner Chaocipher mechanism, while known correspondences and documents did not shed light on this goal. Kruh and Deavours's 1990 article in Cryptologia added the knowledge that, as of 1990, John F. Byrne's Chaocipher machine, papers, and artifacts were in the possession of John Byrne, J. F. Byrne's son, somewhere in the state of Vermont, USA. Since the article's publication, almost twenty years earlier, there had been no pronouncement, mention, or word from John Byrne or anyone else regarding the fate of the Chaocipher legacy.

In August 2009 this author began to be troubled by the possibility that, should John Byrne pass away, the Chaocipher legacy might be sold or discarded. In the best case the material would reside in someone's private collections for years; in the worst case, the Chaocipher secret would be lost forever.

Goaded by this unsettling thought, this author began calling all Byrnes residing in Vermont in the hope of finding John. After several "cold" telephone calls he had the good fortune to call Patricia Byrne[17], John F. Byrne's daughter-in-law and John's widow (John passed away in November 2008)[18].

For the next six months this author corresponded with Pat Byrne who, wanting to investigate marketing Chaocipher commercially, had entrusted the entire Chaocipher collection to an associate. During this time this author offered to help Pat patent the Chaocipher algorithm as a preliminary step to disclosing the system to test its commercial strength.

In a subsequent phone conversation Pat showed interest in finding a suitable home for the material. The most logical home for the material was the National Cryptologic Museum, so this author immediately sent an email to David Kahn. This led to an introduction to David D'Auria, the acquisition chairman of the National Cryptologic Museum, which enabled putting Pat and the NCM in direct contact. Although it took a few months, Pat magnanimously donated the entire Chaocipher collection to the NCM.

On 2 June 2010, after previewing several of Byrne's worksheets, this author uploaded a paper entitled *Chaocipher Revealed: The Algorithm* as the first public disclosure of the Chaocipher system [43].

---

[17] Patricia Byrne is the former Patricia Neway (born September 30, 1919, Brooklyn, New York). Patricia is an American operatic soprano and musical theatre actress who had an active international career during the mid-1940s through the 1970s. She is particularly remembered for creating roles in the world premieres of several contemporary American operas, most notably Magda Sorel in Gian Carlo Menotti's 'The Consul'. On Broadway she won a Tony Award for her portrayal of the Mother Abbess in the original production of Rodgers and Hammerstein's The Sound of Music [62].

[18] See http://www.mountainvistasoft.com/chaocipher/chaocipher-016.htm for description of how this author contacted Pat Byrne.

5 Description of System

Byrne's Mechanical Embodiment

In Byrne's embodiment of Chaocipher, the system consists of two disks, referred to as the *left* and *right* disks, each having 26 equal sized removable tabs around its periphery. These removable tabs contain the 26 letters of the alphabet (i.e., A through Z) in some order. On the circumference of each disk are studs that allow the two disks to 'engage' or interlock. When engaged, turning one disk in one direction (e.g., clockwise) will cause the other wheel to turn in the opposite direction (e.g., counterclockwise). The tabs are removable, meaning that a tab can be removed from the periphery, another block of tabs shifted, and the extracted tab inserted into an empty space in the periphery.

At any point in time the disks can be engaged to each other so that moving one moves the other. Similarly, engaged disks can be disengaged, at which point a disk can be turned without moving the other disk. Engagement and disengagement could conceivably be performed by moving a lever to or fro.

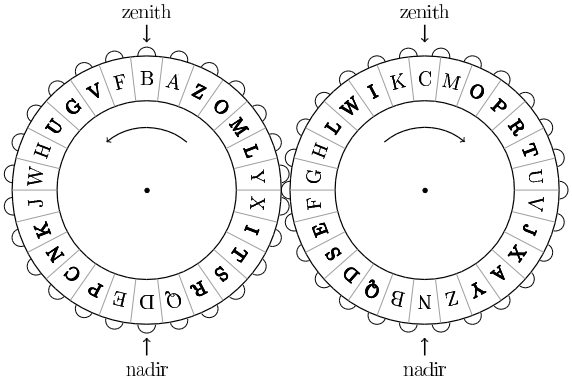


Figure 8: The Chaocipher disks in engaged mode

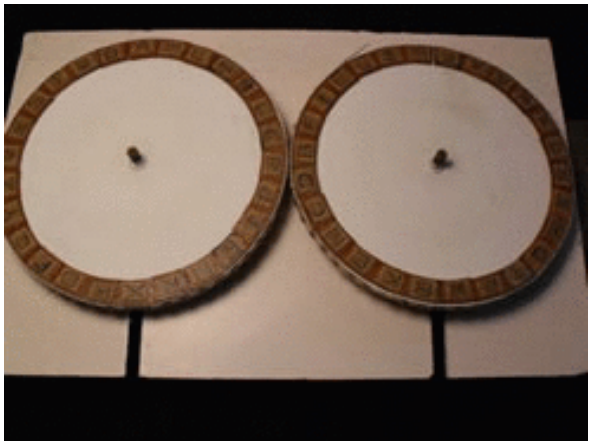


Figure 9: A Chaocipher mock-up built by John Byrne

The two disks mentioned above sit on a platform consisting of two spindles. Around each disk are two marks known as the 'zenith' and the 'nadir'. The zenith can be thought of 12 o'clock on an analog clock, while the nadir is 6 o'clock. Figure 8 shows what Chaocipher might look like when assembled.

It is important to note Byrne's convention that the right alphabet is used for finding the plaintext letter, while the left alphabet is used for finding the corresponding ciphertext letter[19].

[19] It is perfectly logical to alternate between locating the plaintext letter in the right or left alphabet based on some prearranged pattern. As will be shown in this paper, Byrne used this alternating alphabet method for deriving the starting alphabets.

The Chaocipher Algorithm Explained

Overview of Chaocipher Process

Given left and right disks, enciphering a plaintext character consists of five steps:

1. Verify the left and right disks are engaged.
2. Rotate the plain (right) disk, bringing the desired plaintext letter to the *zenith* position.
3. Read the corresponding ciphertext letter at the zenith position on the cipher (left) disk.
4. Permute the left disk.
5. Permute the right disk.

These five steps are performed continuously until the plaintext input is exhausted. To illustrate the process we will encipher the first few plaintext letters of Byrne's Exhibit #1 precisely the way he did, using the alphabets shown in Figure 8.

How to Encipher Plaintext

The first three plaintext letters of Exhibit #1 to encipher are "ALL", so the first letter to encipher is 'A'. Locate 'A' on the periphery of the plain (right) disk:

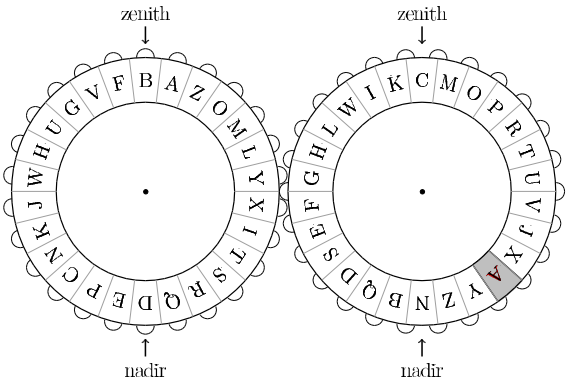


Figure 10: The plaintext letter 'A' is located on the plain (right) disk

While the disks are engaged, rotate the right disk to bring the plaintext letter 'A' to the *zenith*:

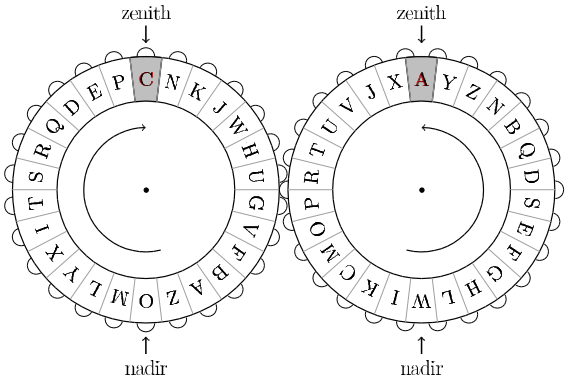


Figure 11: Aligning the plaintext 'A' reveals the ciphertext 'C'

The letter in the zenith position on the cipher (left) disk is our ciphertext letter.

Permuting the Alphabets

Now that the plaintext letter and its corresponding ciphertext letter are known, proceed to permute the alphabets on both disks in preparation for enciphering the next plaintext letter.

Permute the Left Disk

Permuting the left alphabet involves the following general steps:

1. Physically extract the letter tab found at position *zenith*-1 (i.e., one counter-clockwise position past the *zenith*) taking it out of the disk's alphabet, temporarily leaving an unfilled 'hole'.
2. Shift all letter tabs in positions *zenith*-2 (moving counter-clockwise) up to and including the *nadir* (*zenith*-13), moving them in unison one position clockwise. This will close the current 'hole', leaving a new 'hole' at the nadir position.
3. Insert the previously extracted letter tab into the empty *nadir* position.

Before performing the permuting the left disk should look like the diagram in Figure 12 (a).

Performing step (1), extract the letter at position *zenith*-1 (i.e., "P") leaving a momentary 'hole' at that position (see Figure 12 (b)).

For step (2) shift all letters in the counter-clockwise sequence beginning with *zenith*-2 ("E") up to and including the *nadir* ("O"), moving the sequence ("EDQRSTIXYLMO") as a complete block one position clockwise (see Figure 12 (c)).

In the final step (3), insert the extracted letter ("P") back into the alphabet at the *nadir* position. The left is now permuted and should now look like Figure 12 (d).

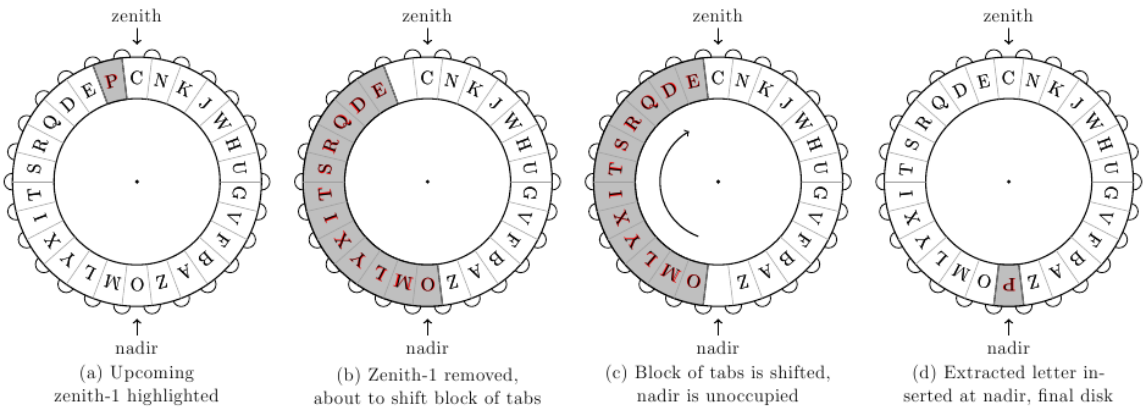


Figure 12: Step-by-step diagrams of left disk permuting

Permute the Right Disk

Permuting the right disk is similar to that of the left disk, with small but significant differences. It consists of the following general steps:

1. Disengage the two disks, rotate the right disk one position counter-clockwise (i.e., the current letter at the zenith should rotate to position *zenith-1*), and reengage the two disks.

2. Physically extract the letter tab now found at position *zenith*+2 (i.e., two clockwise positions past the *zenith*) taking it out of the disk's alphabet, leaving a temporarily unfilled 'hole'.
3. Shift all letter tabs in positions *zenith*+3 up to and including the *nadir* (*zenith*+13), sliding them in unison one position counter-clockwise. This will close the current 'hole', leaving a new 'hole' at the nadir position.
4. Insert the previously extracted letter tab into the empty *nadir* position.

Let's perform the above steps on the right disk using our example. The right disk should look like the diagram in Figure 13 (a). In this configuration the letter at the *zenith* is 'A'.

In step (1) first disengage the two disks. This allows rotating the right disk (see next step) without moving the left disk. Next, rotate the disk one position counter-clockwise, moving the letter 'Y' to the *zenith* position (see Figure 13 (b)). Lastly, reengage the two disks.

In step (2) extract the letter tab at position zenith+2 ('N') from the disk, temporarily leaving a 'hole' (see Figure 13 (c)).

In step (3) slide the eleven letter tabs from zenith+3 until zenith+13 (i.e., 'BQDSEFGHLWI') one position counter-clockwise. This closes up the 'hole' at *zenith-2* while opening a new 'hole' at the *nadir* (see Figure 13 (d)).

For the final step (4) insert the previously extracted letter tab ("N") back into the disk at the *nadir* position. This completes permuting the right disk, which should now look like Figure 13 (e).

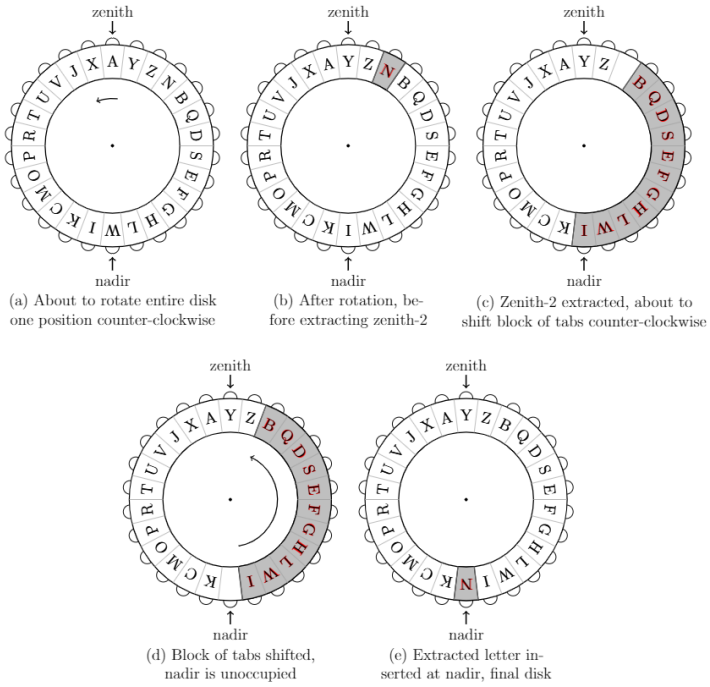


Figure 13: Step-by-step diagrams of right disk permuting

Reengaging the disks prepares the system for enciphering the next plaintext letter:

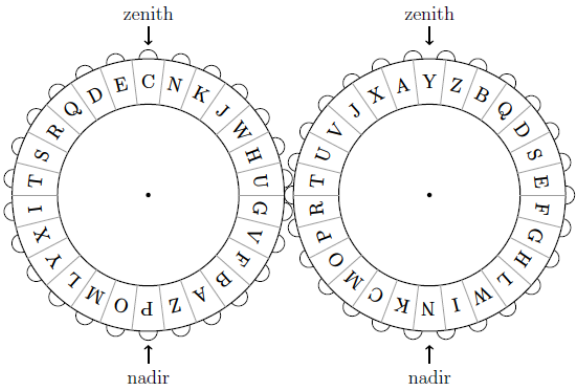


Figure 14: The permuted disks reengaged, ready to encipher the next plaintext letter

How to Decipher Ciphertext

Deciphering a Chaocipher-encrypted message is identical to the steps used for enciphering. The sole difference is that the decipherer locates the known ciphertext letter in the left (ct) disk, reading off the plaintext letter from the right (pt) disk. Left/right disk permuting is identical in enciphering and deciphering.

A Simpler Equivalent Chaocipher Model

In the description above we presented John F. Byrne's view of Chaocipher in mechanical terms, such as "engaging" and "disengaging" the disks to prevent simultaneous rotation of the disks at certain points in the enciphering/deciphering process. The reader will find that using this model to encipher / decipher messages is tedious and error prone. For cryptanalytic purposes it is, therefore, preferable to use a simplified model of *alphabet strips* or *rods* which is not constrained by mechanical concerns and does not require the use of disks [47, p. 2ff]. An added bonus when using the simpler model is that the left and right alphabets are handled in the same way, without having to differentiate between clockwise and counter-clockwise movements.

This simpler method will be used for the remainder of the paper so a short description is in order. To begin with, the disks in Figure 8 can be represented as two, flat alphabet strips:

```
              +              *
Left  (ct):   BFVGUHWJKNCPEDQRSTIXYLMOZA
Right (pt):   CMOPRTUVJXAYZNBQDSEFGHLWIK
```

Figure 15: Starting alphabets as two flat strips

Note the two symbols '+' and '*' positioned above the alphabets in Figure 15. These are the *zenith* and *nadir*, corresponding to the 1st and 14th positions of each alphabet, respectively. These positions play a major role when permuting each alphabet following each enciphering/deciphering step, as seen when using Byrne's disks.

The process of enciphering is similar to using disks, with minor differences. Let's illustrate them by enciphering the plaintext letter 'A', as done with the disks.

To encipher a plaintext letter, locate it in the right (pt) alphabet. The letter in the left (ct) alphabet directly above the plaintext letter is the ciphertext letter.

```
              +             *
Left  (ct):   BFVGUHWJKNCPEDQRSTIXYLMOZA
Right (pt):   CMOPRTUVJXAYZNBQDSEFGHLWIK
                          ↑
```

Now that the plaintext letter and its corresponding ciphertext letter are known, proceed to permute the alphabets in preparation for enciphering the next plaintext letter.

To permute the left alphabet:

1. Shift the entire left alphabet cyclically so the ciphertext letter just enciphered is positioned at the *zenith* (i.e., position 1).
2. Extract the letter found at position *zenith*+1 (i.e., the letter to the right of the *zenith*), taking it out of the alphabet, temporarily leaving an unfilled 'hole'.
3. Shift all letters in positions *zenith*+2 up to, and including, the *nadir* (*zenith*+13), moving them one position to the left.
4. Insert the just-extracted letter into the *nadir* position (i.e., *zenith*+13).

Let's perform the above steps on the left (ct) alphabet using our example. Performing step (1) shift the entire alphabet to bring the ciphertext letter "C" to the zenith position:

```
              +             *
Left  (ct):   CPEDQRSTIXYLMOZABFVGUHWJKN
```

Performing step (2), extract the letter at position *zenith*+1 (i.e., "P") leaving a momentary 'hole'. This leaves the left alphabet looking like this:

```
              +             *
Left  (ct):   C.EDQRSTIXYLMOZABFVGUHWJKN
```

For step (3) shift all letters beginning with *zenith*+2 ("E") up to and including the *nadir* ("O"), moving the sequence ("EDQRSTIXYLMO") as a complete block one position to the left. The left alphabet now looks like this:

```
              +             *
Left  (ct):   CEDQRSTIXYLMO.ZABFVGUHWJKN
```

In the final step (4), insert the extracted letter ("P") back into the alphabet at the *nadir* position:

```
              +             *
Left  (ct):   CEDQRSTIXYLMOPZABFVGUHWJKN
```

This is the new permuted left alphabet.

Permuting the right alphabet is similar to that of the left alphabet, with small but significant differences. It consists of the following steps:

1. Shift the entire right alphabet cyclically so the plaintext letter just enciphered is positioned at the *zenith*.
2. **Now shift the entire alphabet one more position to the left** (i.e., the leftmost letter moves cyclically to the far right), moving a new letter into the *zenith* position.

3. Extract the letter at position *zenith*+2, taking it out of the alphabet, temporarily leaving an unfilled 'hole'.
4. Shift all letters beginning with *zenith*+3 up to, and including, the *nadir* (*zenith*+13), moving them one position to the left.
5. Insert the just-extracted letter into the *nadir* position (*zenith*+13).

Let's perform the above steps on the right (pt) alphabet using our example. For step (1) shift the entire alphabet cyclically to bring the plaintext letter "A" to the *zenith* position:

```
                +             *
Right (pt): AYZNBQDSEFGHLWIKCMOPRTUVJX
```

In step (2) shift the alphabet one more position to the left, sending the letter 'A' to the end of the alphabet and bringing the letter "Y" to the *zenith* (don't forget to always do this step for the right-hand alphabet!):

```
                +             *
Right (pt): YZNBQDSEFGHLWIKCMOPRTUVJXA
```

Next, in step (3), select the letter located two positions to the right of the *zenith* (i.e., "N") and extract it momentarily. This leaves the right-hand (pt) alphabet looking like this:

```
                +             *
Right (pt): YZ.BQDSEFGHLWIKCMOPRTUVJXA
```

For step (4) shift all the remaining letters following the 'hole' up to, and including, the *nadir* ("BQDSEFGHLWI") one position to the left:

```
                +             *
Right (pt): YZBQDSEFGHLWI.KCMOPRTUVJXA
```

For the last step, step (5), insert the just-extracted letter ("N") back into the alphabet at the *nadir* position:

```
                +             *
Right (pt): YZBQDSEFGHLWINKCMOPRTUVJXA
```

At this point there are two newly permuted left and right alphabets:

```
                +             *
Left (ct):  CEDQRSTIXYLMOPZABFVGUHWJKN
Right (pt): YZBQDSEFGHLWINKCMOPRTUVJXA
```

Byrne's Chaocipher Priming Method

As mentioned above, the Chaocipher machine must be set up before encryption / decryption can take place. To this end both the sender and the recipient must prime the machine with the left and right alphabets and the zenith positions for both disks. Byrne devised a keyword-based method for producing initial mixed alphabets, bundling the keyword and the initial zenith positions into a system indicator embedded within the transmitted ciphertext message [37]. We'll illustrate the method by showing how Byrne embedded the key settings needed to decipher Exhibit #4 within its ciphertext.

To generate the starting alphabets for Exhibit #4 Byrne chose the key phrase "CHAOCIPHER". A simple method of generating the starting alphabets (not the one used by Byrne) is the following:

1. Set both Chaocipher disks to the straight, standard alphabet ("ABC…XYZ")
2. Position both disks so the letter "A" is at the zeniths
3. Encipher the key phrase (i.e., "CHAOCIPHER"), finding all ciphertext letters in the right alphabet

When finished the semi-mixed left and right alphabets should look like this:

```
L: ABCDEFGHIJKLMNOPQRSTUVWXYZ   R: ABCDEFGHIJKLMNOPQRSTUVWXYZ   (C,C)
L: CEFGHIJKLMNOPDQRSTUVWXYZAB   R: DEGHIJKLMNOPQFRSTUVWXYZABC   (H,G)
L: GIJKLMNOPDQRSHTUVWXYZABCEF   R: IJLMNOPQFRSTUKVWXYZABCDEGH   (A,Y)
L: YABCEFGIJKLMNZOPDQRSHTUVWX   R: BCEGHIJLMNOPQDFRSTUKVWXYZA   (O,L)
L: LNZOPDQRSHTUVMWXYABCEFGIJK   R: PQFRSTUKVWXYZDABCEGHIJLMNO   (C,Y)
L: YBCEFGIJKLNZOAPDQRSHTUVMWX   R: EGIJLMNOPQFRSHTUKVWXYZDABC   (I,C)
L: CFGIJKLNZOAPDEQRSHTUVMWXYB   R: JLNOPQFRSHTUKMVWXYZDABCEGI   (P,J)
L: JLNZOAPDEQRSHKTUVMWXYBCFGI   R: QFSHTUKMVWXYZRDABCEGIJLNOP   (H,Z)
L: ZAPDEQRSHKTUVOMWXYBCFGIJLN   R: TUMVWXYZRDABCKEGIJLNOPQFSH   (E,M)
L: MXYBCFGIJLNZAWPDEQRSHKTUVO   R: GILNOPQFSHTUMJVWXYZRDABCKE   (R,S)
L: SKTUVOMXYBCFGHIJLNZAWPDEQR   R: DACKEGILNOPQFBSHTUMJVWXYZR

Pattern:    RRRRRRRRRR
Plaintext:  CHAOCIPHER
Ciphertext: CGYLYCJZMS
```

Figure 16: Resultant alphabets when generating the starting alphabets for Exhibit #4

Byrne's method differs in that the plaintext letters are sometimes found on the right alphabet *and sometimes on the left one*. The sender must determine the disk sequence for finding the plaintext letter. In Exhibit #4 Byrne chose the sequence "RRLLRRLRLR", where 'R' and 'L' denote the right and left disks, respectively. The disks on which to locate the plaintext letters are therefore:

```
Plaintext: CHAOCIPHER
Disk:      RRLLRRLRLR
```

One more detail is required before Byrne's alphabet generation process can be duplicated. Before enciphering the key phrase "CHAOCIPHER" Byrne set the left disk to bring the letter 'T' to the zenith, while leaving the right disk's zenith as 'A'.

Now the Exhibit #4 starting alphabets can be generated. The machine begins with two straight alphabets, with the zeniths for the left and right disks beginning 'T' and 'A', respectively:

```
        +             *
Left:   TUVWXYZABCDEFGHIJKLMNOPQRS
Right:  ABCDEFGHIJKLMNOPQRSTUVWXYZ
          ↑
```

Enciphering the first plaintext letter 'C', finding it on disk 'R', gives ciphertext 'V' and the following permuted alphabets:

```
        +             *
Left:   VXYZABCDEFGHIWJKLMNOPQRSTU
Right:  DEGHIJKLMNOPQFRSTUVWXYZABC
           ↑
```

Enciphering the next plaintext letter 'H', finding it on disk 'R', gives ciphertext 'Z' and the following permuted alphabets:

```
        +           ↓*
Left:   ZBCDEFGHIWJKLAMNOPQRSTUVXY
Right:  IJLMNOPQFRSTUKVWXYZABCDEGH
```

Encipher the next plaintext letter 'A', this time finding it on disk 'L', giving ciphertext 'K' and the permuted alphabets:

```
        +            *
Left:   ANOPQRSTUVXYZMBCDEFGHIWJKL
Right:  VWYZABCDEGHIJXLMNOPQFRSTUK
```

The following table details the output of all steps encountered while enciphering the key phrase:

Plaintext Letter	Plaintext Alphabet Used	Ciphertext Letter	Permuted Alphabets	
			Left	Right
---	---	---	TUVWXYZABCDEFGHIJKLMNOPQRS	ABCDEFGHIJKLMNOPQRSTUVWXYZ
C	R	V	VXYZABCDEFGHIWJKLMNOPQRSTU	DEGHIJKLMNOPQFRSTUVWXYZABC
H	R	Z	ZBCDEFGHIWJKLAMNOPQRSTUVXY	IJLMNOPQFRSTUKVWXYZABCDEGH
A	L	K	ANOPQRSTUVXYZMBCDEFGHIWJKL	VWYZABCDEGHIJXLMNOPQFRSTUK
O	L	Y	OQRSTUVXYZMBCPDEFGHIWJKLAN	ZACDEGHIJXLMNBOPQFRSTUKVWY
C	R	R	RTUVXYZMBCPDESFGHIWJKLANOQ	DEHIJXLMNBOPQGFRSTUKVWYZAC
I	R	V	VYZMBCPDESFGHXIWJKLANOQRTU	JXMNBOPQGFRSTLUKVWYZACDEHI
P	L	P	PESFGHXIWJKLADNOQRTUVYZMBC	QGRSTLUKVWYZAFCDEHIJXMNBOP
H	R	R	RUVYZMBCPESFGTHXIWJKLADNOQ	IJMNBOPQGRSTLXUKVWYZAFCDEH
E	L	R	EFGTHXIWJKLADSNOQRUVYZMBCP	STXUKVWYZAFCDLEHIJMNBOPQGR
R	R	P	PFGTHXIWJKLADESNOQRUVYZMBC	STUKVWYZAFCDLXEHIJMNBOPQGR

Table 2: Step-by-step enciphering of key phrase "CHAOCIPHER"

Armed with the left and right starting alphabets ("PFG…MBC" and "STU…QGR") encipher the plaintext beginning with "BEYONDPOINTINGOUT…", giving the ciphertext beginning with "VEHRNWQSJLDIWLUKK…".

Now everything can be packaged for transmittal to the recipient. The following information needs to be transmitted:

- The starting zenith for the left alphabet for generating the starting alphabets
- The key phrase for generating the starting alphabets (i.e., "CHAOCIPHER")
- The sequence of alphabets for locating the plaintext letters (i.e., "RRLLRRLRLR")
- The 'plaintext' letter 'Z' to indicate "end of keying indicator".

This information is encoded as the 20-letter sequence:

```
TLCHRAOLCIRPLHRELRRZ
```

This should be parsed in the following fashion:

```
T L / C H R / A O L / C I R / P L / H R / E L / R R / Z
```

This should be understood as follows:

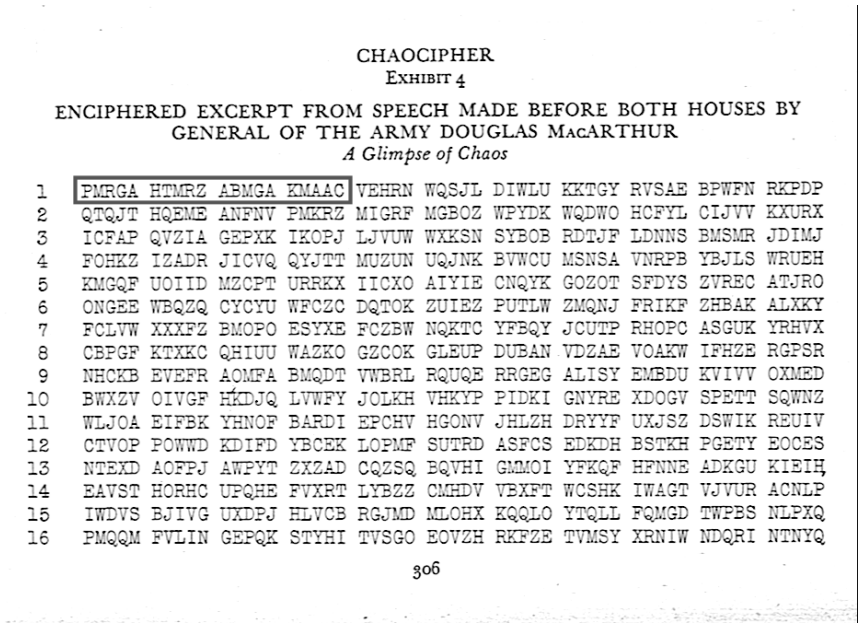
Sequence	Means
TL	T is the zenith for the Left alphabet before generating the starting alphabets (A is the default zenith for the right alphabet)
CHR	Find the plaintext letters "C" and "H" in the Right alphabet
AOL	" " " " "A" and "O" in the Left alphabet
CIR	" " " " "C" and "I" in the Right alphabet
PL	" " " " "P" in the Left alphabet
HR	" " " " "H" in the Right alphabet
EL	" " " " "E" in the Left alphabet
RR	" " " " "R" in the Right alphabet
Z	"End of embedded key" indicator

Table 3: Understanding the Exhibit #4 key indicator

The entire key indicator is now monoalphabetically enciphered with substitution alphabets known to the sender and recipient. In Byrne's case he used the alphabets:

```
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
H L R Q K J O G Z S F M D W T B X A Y P V E I N U C
```

Enciphering the keying indicator gives "PMRGAHTMRZABMGAKMAAC". Prepending the keying indicator to the cipher text "VEHRNWQSJLDIWLUKK" gives the precise text found in Exhibit #4 (see Figure 17).



CHAOCIPHER
EXHIBIT 4

ENCIPHERED EXCERPT FROM SPEECH MADE BEFORE BOTH HOUSES BY GENERAL OF THE ARMY DOUGLAS MACARTHUR
A Glimpse of Chaos

```
 1  PMRGA HTMRZ ABMGA KMAAC VEHRN WQSJL DIWLU KKTGY RVSAE BPWFN RKPDP
 2  QTQJT HQEME ANFNV PMKRZ MIGRF MGBOZ WPYDK WQDWO HCFYL CIJVV KXURX
 3  ICFAP QVZIA GEPXK IKOPJ LJVUW WXKSN SYBOB RDTJF LDNNS BMSMR JDIMJ
 4  FOHKZ IZADR JICVQ QYJTT MUZUN UQJNK BVWCU MSNSA VNRPB YBJLS WRUEH
 5  KMGQF UOIID MZCPT URRKX IICXO AIYIE CNQYK GOZOT SFDYS ZVREC ATJRO
 6  ONGEE WBQZQ CYCYU WFCZC DQTOK ZUIEZ PUTLW ZMQNJ FRIKF ZHBAK ALXKY
 7  FCLVW XXXFZ BMOPO ESYXE FCZBW NQKTC YFBQY JCUTP RHOPC ASGUK YRHVX
 8  CBPGF KTXKC QHIUU WAZKO GZCOK GLEUP DUBAN VDZAE VOAKW IFHZE RGPSR
 9  NHCKB EVEFR AOMFA BMQDT VWBRL RQUQE RRGEG ALISY EMBDU KVIVV OXMED
10  BWXZV OIVGF HKDJQ LVWFY JOLKH VHKYP PIDKI GNYRE XDOGV SPETT SQWNZ
11  WLJOA EIFBK YHNOF BARDI EPCHV HGONV JHLZH DRYYF UXJSZ DSWIK REUIV
12  CTVOP POWWD KDIFD YBCEK LOPMF SUTRD ASFCS EDKDH BSTKH PGETY EOCES
13  NTEXD AOFPJ AWPYT ZXZAD CQZSQ BQVHI GMMOI YFKQF HFNNE ADKGU KIEIH
14  EAVST HORHC UPQHE FVXRT LYBZZ CMHDV VBXFT WCSHK IWAGT VJVUR ACNLP
15  IWDVS BJIVG UXDPJ HLVCB RGJMD MLOHX KQQLO YTQLL FQMGD TWPBS NLPXQ
16  PMQQM FVLIN GEPQK STYHI TVSGO EOVZH RKFZE TVMSY XRNIW NDQRI NTNYQ
```

306

Figure 17: Exhibit #4 as transmitted, showing the keying indicator and the ciphertext message

The recipient, upon receiving the transmission, scans the message for the first occurrence of plaintext letter 'Z', which will show up as ciphertext letter 'C'. All that remains is to strip off the header, decrypt it using the monoalphabetic keying alphabets, and parse the decrypted indicator to derive the keying setup parameters.

Although Exhibit #1's starting alphabets are generated from a key phrase (i.e., phrase "THINKTHINK" and alphabet order "RLLRLLRRLR") , the exhibit does not contain an encoded key indicator.

Practical problems with Byrne's Indicator Method

Byrne's indicator method, however, has operational flaws. Ideally, the key phrase should not contain the letters 'L', 'R', or 'Z' (or whatever the end-of-header character is) as these have special meaning. That would preclude any key phrases containing these letters. Byrne's key phrase, "CHAOCIPHER" does have an 'R', but it is the last letter of the phrase, thus avoiding ambiguity. Here's a contrived example that illustrates the point.

> What is the key phrase, and what is the wheel order, for the decrypted key indicator "TRRALILRELRR"? The key phrase is "TRAILER" and the intended division is "TRR/AL/ILR/EL/RR". Unfortunately the parsing is ambiguous because both 'L' and 'R' are used as key letters, so there are other possible divisions. How is the recipient to know which is the correct one?

The other interesting point of Byrne's key indicator system is that it opens up a host of solving techniques for a cryptanalyst. These include:

- The sender has an unlimited number of key phrases to choose from, which the recipient does not need to know 'a priori'.
- Given a moderate number of messages, the cryptanalyst can deduce the key termination ciphertext character (e.g., 'C' in Exhibit #4). This enables him to strip off the key indicator characters.
- Based on frequency analysis alone, a cryptanalyst should be able to determine the two ciphertext letters for 'L' and 'R'.
- Assuming the key phrases are English (not necessarily, but possibly) then the indicators can be solved as simple substitution ciphers. Once done, the key indicators are the Achilles heel, giving the key settings without having to solve the actual messages!
- Two messages with the identical key indicator are "in-depth", i.e., they both begin with the identical components and settings (similar to Kruh and Deavour's Exhibit #5). Although no technique as of yet has been found to leverage this knowledge (consider this an open challenge to you cryptanalysts out there!), one's gut feeling is that knowing two messages are in-depth will greatly reduce the key space to search.
- One or more similar message indicators may yield other cryptanalytic weaknesses.

In summary, Byrne's attempt to devise a key management system [64] has problems and falls short of a robust method.

Deciphering the Other Exhibits

With the Chaocipher algorithm revealed, and having access to Byrne's worksheets, it is now possible to decipher several of the original exhibits in *Silent Years*. The underlying plaintexts and keys for exhibits #1 and #4 have been documented in the open literature [48, 16, 14], while exhibits #2 and #3 have eluded researchers to date. At the time of writing, Exhibit #5 [3] is still unsolved.

The following table summarizes what is known about each exhibit.

Exhibit	Solved?	Keying Information	Comments

1	✓	`Left (ct): BFVGUHWJKNCPEDQRSTIXYLMOZA`
		`Right (pt): CMOPRTUVJXAYZNBQDSEFGHLWIK`
		`Key phrase: THINKTHINK`
		`Left/right pattern: RLLRLLRRLR`
			No keying information embedded in exhibit

2	✘	Unknown but probably based on the phrase "SI VALES BENE EST W".	Apparently enciphered differently than Exhibits #1 and #4. Byrne may inadvertently have introduced errors when enciphering. See [39] for Byrne's own notes written when enciphering this exhibit.
3	✘		No research done to date on this exhibit. Plaintext/ciphertext "hits" at distances 1, 6, and 7 seem to indicate that Byrne enciphered differently than Exhibits #1 and #4.

4	✓	`Left (ct): PFGTHXIWJKLADESNOQRUVYZMBC`
		`Right (pt): STUKVWYZAFCDLXEHIJMNBOPQGR`
		`Key phrase: CHAOCIPHER`
		`Left zenith: T`
		`Left/right pattern: RRLLRRLRLR`
			Keying information embedded in first twenty characters of exhibit

5(a)	✘		All three messages are in-depth. Message (c) has five-letter repetition "BBNKF" at distance of 31.
5(b)	✘		
5(c)	✘		

Table 4: Current research status of Chaocipher Exhibits: A Summary

The 1918 vs. 1937 Models

The Chaocipher literature intimates that there were one or more embodiments of Chaocipher used by Byrne to demonstrate the concept.

- Byrne apparently built his famous cigar box model in 1918 after conceiving of the idea.
- Byrne used his cigar box model to demonstrate Chaocipher to Hitt in 1921, and Moorman and Friedman in 1922. This model was damaged in transit in 1922 following the Moorman/Friedman demonstration.
- One cannot say with certainty that the Chaocipher models of 1922 and 1937 were identical (the earliest worksheet showing the enciphering process dates to 1937, see Figure 18).
- It may be assumed that Byrne constructed a new model to show the US Navy in Washington in 1937.
- When visiting Henry E. Langen in 1954 Byrne apologized for not bringing the cipher machine itself, "explaining that it was too heavy and cumbersome." Unless Byrne was bluffing, this would indicate that he had a model at the time[20].

[20] Tony Bean relates [1] that he had many conversations about 'the model' with his uncle John (the son of John Francis Byrne). He writes "… to the best of my knowledge, my grandfather never constructed any device that was "too heavy

- In a letter to Greg Mellen on 8 February 1981, Byrne's son John wrote "The model my father, mother, and I worked on was destroyed by me shortly after my father's death". [36]

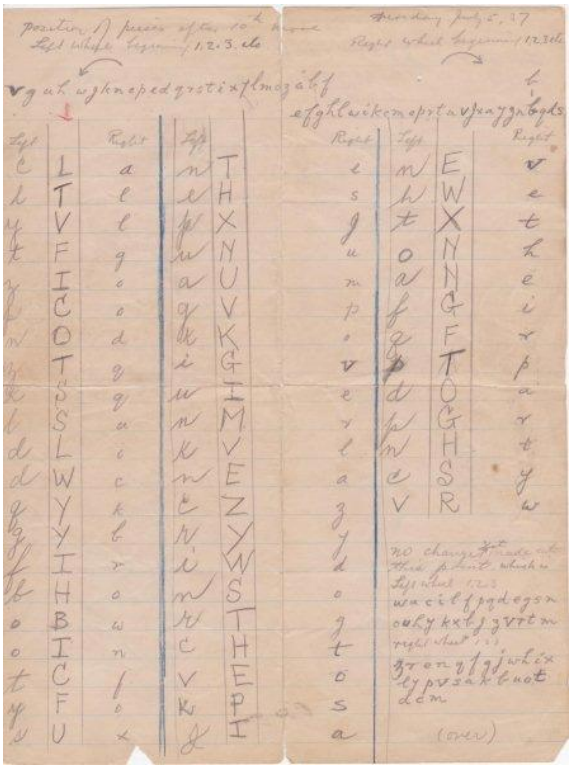


Figure 18: Worksheet dated Monday, July 5, 1937 enciphering the first line of Exhibit #1

Chaocipher as a Forerunner of Dynamic Substitution or CBC Mode

The Chaocipher concept is unique for a cipher system of its time in that it modifies its alphabets after each encipherment. The vast majority of cryptographic substitution systems preserve the enciphering alphabets throughout the enciphering process, with the order of the alphabets being determined by the starting key. So, for instance, a Vigenere-like polyalphabetic system consists of 26 mixed but unchanging alphabets, with the alphabet order determined by a keyword. Similarly, with the Enigma machine, the wire connections within the rotors remain unchanged, with the key determining how the myriad number of alphabets are generated. In the case of Chaocipher, the two underlying alphabets are modified after each encipherment. Although the changes are small, the overall effect is a sequence of highly nonlinear and diffused alphabets .

The first official mention in the open literature of modifying the underlying components during enciphering is Terry Ritter's patent for *Dynamic Substitution* [46][21]. In Ritter's scheme a stream of pseudo-random data is used to modify the substitution table after each encipherment. In Chaocipher, the left and right alphabets are modified as a function of the previous plaintext and ciphertext letters. In both cases, the alphabets are modified based on a stream of data, resulting over time in a progression of seemingly chaotic alphabets.

---

and cumbersome". The only models I ever heard of were the "cigar box" one and the two disk model depicted in [Figure 9]".

[21] In actuality, Greg Mellen's hypothetical system [33, pp. 149-152], included in his 1979 paper, may be the first recorded example of a dynamic substitution cipher (thanks to Jeff Hill for pointing this out).

Other means of modifying the underlying components are the block cipher encryption modes [60] recommended for strengthening block ciphers (e.g., the Data Encryption Standard). The recommended practice is to bolster existing block cipher security by modifying the key stream using previous key, plain, or cipher blocks. These modes include Cipher-Block Chaining (CBC), Propagating Cipher-Block Chaining (PCBC), Cipher Feedback (CFB), and Output Feedback (OFB). These, in effect, add a running-key element to the encryption process and makes cryptanalysis significantly more difficult. In the case of Chaocipher, the underlying components (i.e., the right (pt) and left (ct) alphabets) are cross-modified and highly coupled to the plaintext and ciphertext stream.

It is this author's opinion that Byrne may possibly be considered the discoverer of dynamic substitution.[22]

6 Cryptanalysis of Chaocipher

The cryptanalysis of Chaocipher can refer to several progressively difficult sub-problems. Here are some of the more evident sub-problems that need to be solved to allow us to claim that there is a general solution to Chaocipher.

- Known Plaintext
- In-Depth Messages
- Ciphertext-Only

Known plaintext

Assuming the Chaocipher algorithm is known, the question becomes: given a Chaocipher ciphertext message of sufficient length and given its corresponding plaintext, can the underlying keys be deduced? Once the Chaocipher method was disclosed one of the initial challenges was to deduce Exhibit #1's underlying alphabets and starting positions (an added bonus was to discover the keyword or phrase used to generate the starting alphabets).

Within days of the disclosure several researchers had implemented software programs for finding the starting alphabets to Exhibit #1 (for a particularly clear explanation see Carl Scheffler's webpage [49]). A limited but detailed explanation how to do so will now be presented.

The general principle for deducing the starting alphabets is to take a sequence of N Chaocipher plaintext letters and their corresponding ciphertext. It is highly recommended to find sequences with a maximum number of plaintext and ciphertext repetitions that allow *chaining* of pt/ct pairs. In Scheffler's solution he used the following plaintext and ciphertext sequences from Exhibit #1 beginning at offset 7187. As will be seen, these sequences afford the optimal amount of pt/ct pair chaining which greatly facilitates solution.

```
                                    ↓↓
...RANCEOFTHESECOLONIESUANDSUCHISNOWTHENECESSITYWHICHCONSTRAINSTHEMTOALTERTHEIRFORM...
...SREXYRUWMBTXTHYVNGZLXELVTZDCQMVFLCBBYKBMESGHSOEPSKPKEWMEQWCOQNBURIIQBNQOGAAXPEIT...
```

The game plan is as follows:

1. Start with empty left and right alphabets

[22] In an email thread this author had with Terry Ritter, Ritter could not think of a pre-90's example of Dynamic Substitution. In a later conversation Ritter wrote "it seems to me that it [ed. Chaocipher] could well be related to DynSub. The idea of combining RNG [ed. random number generator] and combiner would be an interesting approach for a system not based on computing."

2. Insert S/E anywhere in the left/right alphabets
3. Plaintext 'S' is already placed so we can insert pair S/S
4. The pair I/G has nothing in common with the previously inserted pairs, so we will try to insert the pair in the 24 remaining empty slots, discarding the placement if we end up in an eventual contradiction. This is known in computer programming as *backtracking*. We will call this situation 'traversing the gap'.
5. Handling the next pair, T/H, requires traversing a gap. For each placement of I/G, insert T/H in each of the remaining empty slots, backtracking if necessary.
6. We now arrive at the pair Y/S. Since we previously inserted a ciphertext 'S' in the alphabets, this one can be placed immediately.
7. Pair W/O requires traversing the gap
8. Here we have a clear sailing, without requiring traversing, until we hit the pair A/Q at offset 7203. In this case we have neither encountered a plaintext 'A' nor a ciphertext 'Q'. At this point we begin extending our chaining from the pair E/M at offset 7186 going left. Starting with E/M, we encounter no gaps until pair U/Z at offset 7172.
9. Hitting the gap at offset 7172, we now return to where we left of on the right side (i.e., A/Q at 7203). Because of our work on the left side we now have enough letters to 'chain' until pair M/U at offset 7210. This is the last gap that needs traversing.
10. From this point onwards we encounter no problems, quickly completing the ciphertext alphabet, which enables us to eventually complete the plaintext alphabet, too.

```
                      32222222222111         11111113333333334444444444555555
                  <--0987654321098712345678901234561234567890123456789012345678901234-->
pt:  ...COLONIESUANDSUCHISNOWTHENECESSITYWHICHCONSTRAINSTHEMTOALTERTHEIRFORM...
ct:  ...THYVNGZLXELVTZDCQMVFLCBBYKBMESGHSOEPSKPKEWMEQWCOQNBURIIQBNQOGAAXPEIT...
```

Figure 19: The order in which pt/ct pairs are processed to determine the starting alphabets

Let us demonstrate the technique using the game plan listed above. Initially we know nothing so far about the left and right alphabets, so we begin with empty alphabets:

```
                 +            *
  LEFT (ct): ..........................
 RIGHT (pt): ..........................
             --------------------------
   Position: 12345678911111111112222222
                      01234567890123456
```

We can insert the pt/ct pair S/E (order #1) into the alphabets by inserting them at the zenith positions (remember, plaintext in the right alphabet, ciphertext in the left):

```
            +           *
 LEFT (ct): E.......................
RIGHT (pt): S.......................
            -------------------------
  Position: 12345678911111111112222222
                      01234567890123456
```

To incorporate the following pair S/S (order #2) we need to permute the previous alphabets the way the sender did when enciphering the text. Using the permuting instructions explained above (and ignoring any alphabet position that is empty) we get:

```
            +           *
 LEFT (ct): E.......................
RIGHT (pt): .......................S
            -------------------------
  Position: 12345678911111111112222222
                      01234567890123456
```

Figure 20: The permuted alphabets after inserting the first plaintext/ciphertext pair S/E

We now insert the pair S/S at the zenith to get:

```
            +           *
 LEFT (ct): SE......................
RIGHT (pt): S.......................
            -------------------------
  Position: 12345678911111111112222222
                      01234567890123456
```

To work with the pair I/G (order #3) we need to first permute the alphabets:

```
            +           *
 LEFT (ct): S...........E...........
RIGHT (pt): .......................S
```

Neither I nor G exists in the respective alphabets so this requires 'traversing the gap'. There are 23 candidate positions in the alphabet, so we'll iterate over all of them, rejecting any that lead to a contradiction down the line. In all probability there will be one and only one positioning of I/G that will be consistent to the end.

The pair I/G can be tentatively inserted at the first available slot:

```
            +           *
 LEFT (ct): SG..........E...........
RIGHT (pt): .I......................S
```

Note that this is an iteration point. Should a contradiction be encountered before the next iteration point we will return here to iterate to the next candidate.

The pair T/H (order #4) again requires traversing the gap. As before, first permute the alphabets:

```
            +           *
 LEFT (ct): G.........E.............S
RIGHT (pt): ......................S.I
```

Now tentatively insert T/H at the first available slot:

```
             +             *
 LEFT (ct): GH.........E.............S
RIGHT (pt): .T.....................S.I
```

The pair Y/S (order #5) can be mapped to the existing ciphertext 'S' without the need for traversal. As before, permute the alphabets and insert Y/S using the existing ciphertext 'S':

```
             +             *
 LEFT (ct): H........E..............SG
RIGHT (pt): ......................S.IYT
```

W/O (order #6) requires a traversal, so permute and insert in the first available slot:

```
             +             *
 LEFT (ct): SHO.......E.G............S
RIGHT (pt): T.W...................S.IY
```

Figure 21: Permuted alphabet with inserted W/O pair

We can easily continue onwards with orders #7 through #10. The first contradiction is encountered at C/P (order #11). Permuting the alphabets before placing the pair gives:

```
             +             *   ↓
 LEFT (ct): K..E.G.H.........P...SO...
RIGHT (pt): .T.........S..I.Y.WC.....H
                                 ↑
```

The problem is that plaintext (P) and ciphertext (C) are already placed in the alphabets but are not in vertical alignment. This is an inconsistency which means that the last traversal (i.e., W/O at order #6) is incorrect and needs to be backtracked. Returning to the alphabets in Figure 21, undoing the insertion of W/O in the first candidate slot, and reinserting the pair in the next available slot gives:

```
             + ↓           *
 LEFT (ct): SH.O......E.G............S
RIGHT (pt): T..W..................S.IY
```

Throughout this process we have been storing a pair of left/right alphabets corresponded to offset 7187 (see Figure 20). Whenever we extend the alphabets to the right we should update these leftmost alphabets with our tentative insertions. When the algorithm hits a gap on the right-hand side, it checks if there is a simple, non-gap extension on the left side. If there is, it will use the leftmost alphabets to extend leftwards, 'mirroring' any insertions in the rightmost alphabets, and so forth until it finds the starting alphabets. This is the core of the algorithm, with an added complication that the alphabets need to be permuted backwards when extending the alphabets on the left.

Running the algorithm on the plaintext 'crib' in Exhibit #1, then unwinding the alphabets backwards to offset 0, yields the original starting alphabets for Exhibit #1:

```
left:  CPEDQRSTIXYLMOZABFVGUHWJKN
right: AYZNBQDSEFGHLWIKCMOPRTUVJX
```

As just shown, the starting alphabets of a message can be reconstructed with 50-60 plaintext characters, in the good case. This opens the door to cribbing techniques used by the British and Americans to solve the German Enigma machine during World War II. Further research should be done in this area.

In-Depth Messages

The next step up the cryptanalytic ladder is solving a set of N 'in-depth' Chaocipher messages. By in-depth we mean that there is a point in each of the N messages where the machine settings (e.g., alphabets, zenith alignment) are identical. The challenge here is to leverage this knowledge to solve for the starting alphabets.

The best known example of in-depth Chaocipher messages is the set of three messages offered by Kruh and Deavours [3]. Although Kruh and Deavours never clarified the issue, it was assumed that the three messages all began with the identical machine settings. In addition to this information, the authors also revealed that the three messages were taken from a publically available book. At the time of writing these messages have not been solved.

The general feeling is that three in-depth messages are insufficient to solve the alphabets. As mentioned above, William F. Friedman asked John F. Byrne for twenty-five (25) in-depth messages. In the future we hope to prepare a set of messages to conform with Friedman's Enclosure B request. This will allow the Chaocipher researcher to try his hand at tackling the crypto-system in the same circumstances as Friedman back in 1922.

Ciphertext-only

The case of having to find the underlying plaintext and starting alphabets given only the ciphertext represents the ultimate challenge for a cryptanalyst, and would rate the security of the Chaocipher system. At the time of writing there is no obvious method for doing so other than brute force analysis.

What makes this challenge so difficult is the fact that there is a running key-like element in Chaocipher, with the plaintext affecting the cipher outcome and vice versa. Without knowledge of the plaintext (as in the known-plaintext case) the cryptanalyst is chasing a moving target.

Fortunately, real-life messages do not exist in a void. There is always a wealth of collateral information and probable text provided by sources such as traffic analysis. We may find ourselves in the company of historical cipher system such as Enigma and Purple that often required probable plaintext and cribs to break into a key period.

General Comments

Research should be done on attempting to solve Chaocipher messages given special cases, including:

- Isologs: the underlying plaintexts of all messages are identical while the outer machine settings are different.
- Missing character: two in-depth messages (beginning with the same machine settings) have identical underlying plaintexts, except for the fact that a single plaintext character is inadvertently skipped while enciphering. This case can often leads to elegantly cracking a cipher message [30]
- Due to the somewhat chaotic effects of alphabet permutation in Chaocipher, it is not clear whether hill-climbing or genetic algorithms will be of value when solving a message.

7 Technical appraisal

It may be too early yet to provide an accurate appraisal of the Chaocipher crypto-system. We can, however, present several issues and views as jumping-off points for future research.

Similarities to Dynamic Substitution and Block Cipher Encryption Modes

Although invented in 1918, Chaocipher actually incorporates concepts that only arose due to the advent of the computer, specifically *dynamic substitution* [46] and *block cipher encryption modes* [60]. Both concepts involve modifying the plain and cipher elements of a cipher based on previous streams (i.e., a keying stream in the case of dynamic substitution, or the plain or cipher stream in Cipher Block Chaining (CBC) or Output Feed Back (OFB)). Chaocipher seems to couple the plaintext and ciphertext together so that a transmission error creates a high rate of error propagation. In a computerized environment this may be less of a problem than it was in the past.

As mentioned above, it is this author's opinion that John F. Byrne's Chaocipher is the first recorded example of what can essentially be considered Dynamic Substitution.

Modifiable Parameters in Chaocipher

As has been described above, the "classic" Chaocipher algorithm permutes the left and right disks according to specific parameters. These parameters include:

- using the right disk for plaintext and the left disk for ciphertext
- the zenith is at 12 o'clock while the nadir is at 6 o'clock
- specific instructions and offsets for permuting the disks

There is no reason why the sender and receiver cannot modify these parameters according to their wishes. For example, the nadir can be specified as a different position relative to the zenith. Modifying the parameters would make the cryptanalyst's task that much harder.

An encipherer could conceivably switch the functionality of the disks during the enciphering process according to an agreed upon schedule. Indeed, it is currently believed that Exhibit #2 does just this while enciphering its text.

It is also conceivable that the Chaocipher 'disk' may encompass ranges larger than the 26 letters and/or the 10 digits. In an attempt to commercialize Chaocipher, a version supporting all ASCII characters and outputting binary values 0 to 255 (i.e., 8-bit bytes) was developed [41]. Once the system handles 8-bit binary bytes, it can handle Unicode and multi-byte encodings with ease.

Highly Prone to Transmission Errors

As mentioned above, Chaocipher introduces a running key-like element into the algorithm which greatly increases the error propagation rate when a transmission error is encountered. Indeed, early on this author had to contend with transmission errors introduced in the exhibits in *Silent Years*. When decrypting Exhibit #1 with Byrne's starting alphabets a single incorrect ciphertext character would completely stymie this author; no amount of guessing the correct plaintext would solve the problem. The problems were only cleared up when the Silent Years texts were carefully compared with Byrne's 1939 pamphlet, *Chaocipher: The Ultimate Elusion*.

According to Friedman's Enclosure A, a system with such a high rate of error propagation was simply impractical for real-life military use.

Blueprints

As mentioned above, Byrne constructed a set of blueprints detailing a theoretical mechanical embodiment of his Chaocipher concept [38]. It is not evident that Byrne actually constructed a machine based on the

blueprints, nor is it clear whether such a machine would even work. It is known that Byrne brought along the blueprints to his May 1954 meeting with Henry E. Langen [31].

8 Post-Disclosure

At this point, having described the historical and technical background of John F. Byrne's Chaocipher, one can take a broad historical look at Chaocipher and its place in the family of crypto-systems. With the technical parts of it revealed, it is time to raise other important issues.

Byrne's Non-Conformance with Kerckhoffs's Principle and Friedman's Requests

One of the most evident sour notes in the entire Chaocipher saga is the fact that Byrne was so set in his conviction that his system was unbreakable. His belief in its infallibility was so strong that he would not provide William F. Friedman (or anyone else, for that matter) with more messages on demand, nor would he reveal his algorithm to the public. This was in direct opposition to Kerckhoffs's axiomatic principle that a cryptosystem should be secure even if everything about the system, except the key, is public knowledge [61]. What is clear is that Byrne was not a cryptanalyst and had only the most rudimentary concepts of breaking a cipher.

Indeed, it is evident today from his correspondences with others that he equated a perfectly first-order frequency count with total unbreakability (see Figure 22). His constant question to Friedman and Yardley was whether they would agree that a system could be constructed whose ciphertext was totally random and hence unbreakable, and if so, was Chaocipher that system? He could not fathom how someone could make a break into a system whose frequency count showed no order. Today, amateur cryptanalysts know that there are latent patterns within ciphertext that are independent of a first-order frequency count.

One can speculate what would have happened had Byrne conformed to Friedman's requests to send other types of messages (e.g., in-depth). Imagine what would have happened had Friedman broken the set of test messages: would Byrne have continued to champion its infallibility? Would he have published *Silent Years* with its Chapter 21 detailing Chaocipher?

This author feels that Byrne did not conform to Friedman's request for more material for several reasons:

- Enciphering material using Byrne's crude Chaocipher model was error-prone and laborious. Byrne may have wanted to avoid the hard work it entailed.

- Byrne may have thought that Friedman was "beating around the bush" and stalling for time, when it was plain to all (i.e., to Byrne) that Chaocipher fulfilled the only qualification he knew of for an unbreakable cipher, that is, a near-perfectly flat frequency distribution.

- As with many other creators of "unbreakable" cryptographic systems, Byrne was trapped in his misconception vis-à-vis cryptanalysis and could not see the bigger picture.

Byrne himself had supreme confidence that his cipher was unbreakable. This is abundantly clear from a handwritten postscript Byrne wrote in his memorandum to G. M. Campbell of Bell Labs [5]:

> "P.S. I want to emphasize the point that possession of my machine – with full knowledge of its principle and method of operation – would not be of the slightest help in any attempt at decipherment."

This is echoed later in [2, p. 266]:

> "… yet possession of my device together with knowledge of the general principle involved, would not enable any person to decipher any messages whatever written by anyone else and not intended for him."

At the current time no method has been devised for deciphering a ciphertext-only message. Future research will be more capable of either strengthening or negating Byrne opinion of Chaocipher's indecipherability.

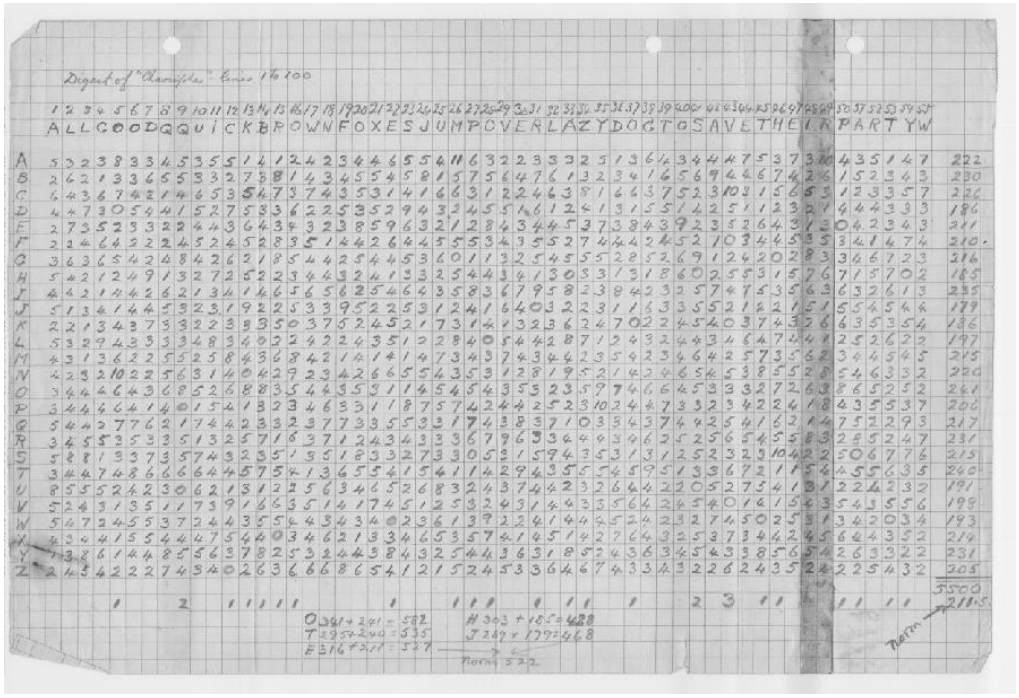


Figure 22: Byrne's first-order frequency table for first 100 lines of Exhibit #1

Correspondences

During the period leading up to the Chaocipher revelation, numerous correspondences between Byrne and other persons surfaced [12]. These include correspondences quoted in Chapter 21 of *Silent Years* and personal correspondences with, among others, William F. Friedman and Herbert O. Yardley. The correspondences were found in numerous libraries in the United States, with more correspondences waiting to be found in other personal collections.

Future Chaocipher researchers are encouraged to seek additional correspondences and information in private, academic, and governmental libraries in the hope that new information will add to the unrolling history and understanding of Chaocipher.

Parker Hitt's Reference to Multiples of 36

In Parker Hitt's letter to Byrne dated 3 August 1921 (see Figure 3), Hitt refers to a potential Chaocipher weakness:

> "I still hold that an error in telegraphic transmission of the 36th letter or of a multiple thereof would be practically fatal to its correct operation in deciphering …"

In [2, p. 273] Byrne writes:

> "When I read Colonel Hitt's letter, it was clear to me that he had not at all fully apprehended the principle of my "machine," as he called it."

Byrne may have been correct about Hitt. Given our knowledge today of the Chaocipher algorithm, it is not clear what the significance of a multiple of thirty-six (36) would have had for Hitt. The 36 positions on the Byrne blueprint were probably reserved for the 26 letters of the alphabets and the digits 0 through 9, as evidenced by the 36 keys on the typewriter keyboard. Byrne's criticism that Hitt had not grasped the principle begins to make sense if Hitt, in Byrne's view, had not understood that the alphabets would be continuously permuted and would not simply begin to repeat at step 36.[23].

Did Friedman Consider Chaocipher when Analyzing PURPLE?

From the corpus of Chaocipher material we may deduce the following facts:

- Friedman understood the internal Chaocipher algorithm, having been explained it by Byrne himself in 1922.
- Friedman did not appear to speak about Chaocipher to his junior cryptanalysts. This is indicated by the fact that Abraham Sinkov, one of Friedman's three original junior cryptanalysts, was introduced to Chaocipher by Wesley Horton in the 1980's. It can be assumed that Sinkov would have remembered the system had Friedman assigned them to work on it.
- Chaocipher is not mentioned or alluded to in Friedman's October 14, 1940 document *Preliminary Historical Report on the Solution of the "B" Machine*.
- There seems to be no allusions to Chaocipher in Friedman's declassified technical works.

One can assume that Friedman did not think highly of the system, and therefore ignored it without documenting it and passing it on to his students. This is forgivable, but it may have somewhat boomeranged when Friedman and his team investigated the Japanese Purple cipher in the late 1930's. As mentioned above, Purple and Chaocipher share observable characteristics in common. Although we know today that the underlying systems are starkly different, Friedman did not know that at the time. Had Chaocipher been documented and taught internally within the Signal Corps, it might have provided a mental leverage when analyzing Purple.

Although a moot point today, had Friedman observed similarities between Chaocipher and Purple, he might have entertained the possibility that Byrne had sold his idea to the Japanese. Regardless of what we know today, documenting and studying Byrne's Chaocipher within the organization would have been a correct thing to do, notwithstanding the heavy load on Friedman and his team.

Why Didn't the US Army Adopt Chaocipher?

As innovative as Chaocipher was at the time (in a way it was far ahead of many other cipher schemes of the era) we know that no organization adopted the cipher system for military or diplomatic use. While the US State Department may have refused to consider Chaocipher out of an unjustified sense of security, one must take a more balanced look when assessing why William F. Friedman did not consider the system for military use. This is all the more curious, as in the 1940's the US Army adopted the Hagelin M-209, which Friedman recognized as being weak, especially in practice.

[23] I am indebted to Jeff Hill for this interesting insight.

In a similar fashion the British needed a good cipher badly at the level below TYPEX, especially as a field cipher. Brigadier John H. Tiltman of the British GC&CS ended up creating the stencil subtractor cipher [22]. There is no mention of Chaocipher in Tiltman's wartime papers [34] or GCCS's World War II papers [35], but one wonders what he might have done with a concept like Chaocipher.

In the final analysis, the reason the US Army did not adopt Chaocipher as a military cipher (either field or diplomatic) may have been related to one or more of the following reasons:

- The system's high rate of transmission error propagation
- The lack of a proven mechanism embodiment
- Byrne's steadfast refusal to submit the necessary material to enable a full evaluation (if true, Friedman, who knew the underlying algorithm, should have overlooked this and investigated the system regardless of Byrne's obstinacy)

"MAPHJAGEFR": Who was Byrne Referring to?

The secret section of Exhibit #1, once deciphered, reads:

> *"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 meaning of the phrase "MAPHJAGEFR" has eluded researchers until now. An important clue to its meaning, however, has surfaced within Byrne's writings, currently housed at the National Cryptographic Museum.

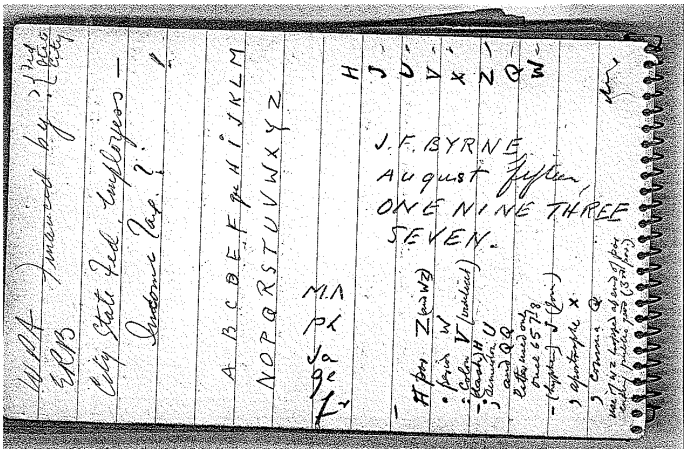


Figure 23: Byrne's worksheet mentioning MAPHJAGEFR

The clue is a notepad sheet found in Byrne's archival papers. Halfway down the page you can clearly see that Byrne wrote the letter pairs "MA", "Ph", "Ja", "Ge", "Fr" one under the other. Interestingly, each pair is a pronounceable pair of letters. A plausible theory is that the pairs represent the first two letters of the names of five friends or relatives of Byrne's that he wished to acknowledge. A check into Byrne's acquaintances leads to several candidates:

Initials	Possible Meaning
MA	"M"ary "A"lice Headen Byrne[24] (John F. Byrne's wife [4]); Mary Fleming (Byrne's cousin, see *Silent Years*, Chapter 21, page 276), or maybe Marcellus Bailey (his patent attorney)
Ph	Phila, Byrne's oldest child and daughter from Alice Headen; "P"arker "H"itt?
Ja	Possibly James Joyce?[25]
Ge	Gertrude Rodman (Byrne's paramour)
Fr	Francis, maybe referring to his son?

Table 5: Possible explanations for MAPHJAGEFR bigrams

All of this is conjectural, but the notepad page seems to indicate that the phrase consists of five bigrams, possibly representing five persons.

Byrne's Wording in Silent Years: Accurate or Hyperbole?

It is evident when reading *Silent Years* that John F. Byrne was a man who understood the English language and selected his words very carefully. In the light of the algorithmic disclosure, we are in the position to assess his writings. For a complete and definitive analysis of Byrne's pronouncements, the reader is directed to Jeff Calof's paper *'Silent Years' - Chapter 21 (Chaocipher) Examined: Analyzing Byrne's Assertions* [6].

Was Kruh and Devours's "Exhibit #5" a Fair Challenge?

In their 1990 article in Cryptologia, authors Lou Kruh and Cipher Deavours provided the reader with a set of three in-depth messages [9]. The authors reasoned that "… Friedman asked for more messages, but in the computer age three should be enough …". This assumption might not have been justified: while Friedman had full knowledge of the underlying Chaocipher algorithm, readers of the Cryptologia article did not. Expecting Cryptologia readers to suffice with three short messages when the algorithm was unknown might be considered unfair. The authors never clarified anything beyond their article, thus leaving this Exhibit shorn of any helping value it could have had.

It is conceivable that the authors did not intend for the messages to be solved. Rather, they may have wished to placate the junior John Byrne for allowing them to see how Chaocipher worked. In return for this favor they may have bolstered his belief that marketing the system was commercially feasible.

Implementing Chaocipher in Software

The Chaocipher encryption/decryption algorithm has been implemented in a host of programming languages including BASIC, C++, C, C#, Haskell, Java, PowerShell, Python, Perl, Ruby, and Scheme. Searching the Web will find many examples which one can copy and experiment.

9 Post-mortem

With thousands of man-hours invested in working on Chaocipher over the years with no apparent success, a brief post-mortem analysis may yield valuable tips for the future. This section attempts to highlight both the positive and negative aspects of the analysis with an eye to learning from one's mistakes.

[24] This may explain why "MA" consists of all capitals while the others consist of a capital latter followed by a small letter, i.e., Byrne retained the upper/lower case when borrowing the letters.

[25] I am indebted to Jeff Calof for raising this possibility.

Once researchers latched onto a possible model it was hard to free oneself from it to consider other out-of-the-box possibilities. Here are some examples:

- With nothing else to go on besides the writings of Kruh and Deavours, analytical thought was guided by Jeffrey Hill's important document *Chaocipher: Analysis and Models*. Analysis was focused on three related models that considered two disks which rotated independently of each other.

- Much thought was given to the "no hits < distance of 9" and the visual features of the resulting graph phenomena. Since the Hill models simulated these aspects well, researchers were reticent to abandon such a valuable model.

- It is interesting that Chaocipher researchers actually touched upon the possibility of Chaocipher being a Dynamic Substitution system [18]. This was abandoned when different schemes did not produce the visual graph features expected by the Chaocipher system. It is speculative to wonder whether researchers going down the Dynamic Substitution path would have hit upon the actual Chaocipher algorithm. With no other hints and so few collateral messages, there are simply too many parameters to choose from to find the actual algorithm used. One can comfort oneself by realizing that the US team working on Purple also required hundreds of related plaintext / ciphertext messages before they could begin their analysis.

Until the establishment of the Chaocipher Clearing House web site, most Chaocipher research was done in isolation, with a small core of researchers sharing selective information with others. A researcher with no connection would have had to begin everything from scratch: transcribe the exhibits to text files, write his own software analysis programs, and duplicate what other researchers had done before him. Although an apparent truism, the key to successful research lies in open collaboration and sharing between researchers.

Suggested Future Work

This paper by no means signals the end of Chaocipher research. Rather, it only scratches the surface of what can and should be done. Here is a partial list of topics waiting to be tackled by future researchers:

- In Friedman's letter to Byrne, dated 7 September 1922 [51] Friedman writes "Hence, when you requested your device be returned to you, I made a personal report based upon my findings reached 'long ago' …". A high priority task is to track down Friedman's personal report on Chaocipher, possibly submitting FOIA requests until it is found
- Devise general solutions for cryptanalytic sub-problems (e.g., in-depth, ciphertext only)
- Track down other Chaocipher-related correspondences in academic and private libraries
- Solve *Silent Years* exhibits 2, 3, and "5"

10 Conclusion

John Francis Byrne was undoubtedly an original and creative thinker who was fortunate enough to figure in the life of a famous literary figure, James Joyce. It is in a complete non-Joycean context that we have examined and evaluated Byrne: as the inventor of the Chaocipher crypto-system. Byrne had no formal training in the art of cryptanalysis, which clouded his judgment regarding the strength of his invention. Nonetheless, the Chaocipher crypto-system embodied a principle ahead of its time. It may well be that the time has come to recognize the original cryptographic contribution discovered by John Francis Byrne.

11 Acknowledgments

This author would like to acknowledge and thank the following people who were instrumental and helpful in the writing of this article:

Tony Bean (John Byrne's nephew) for generously sharing genealogical information about the Byrne family and for proof-reading from a unique vantage point; David Kahn for inspiring my life-long interest in cryptanalysis in general and Chaocipher in particular, and for facilitating the successful connection to NCM; David D'Auria for negotiating the donating of the Chaocipher material with Pat Byrne; Jeff Hill for the hundreds of absorbing Chaocipher-related hours and emails traded with this author, and for proof-reading this paper; Jeff Calof for providing the highest level of proof-reading of this and other Chaocipher papers written by this author, and for valuable leads and ideas; Mike Cowan for coming aboard and contributing to the ongoing attack on Chaocipher; and my wife Rochelle, for her excellent proof-reading of this paper and constant support.

This author has a special debt to repay to three women without whose help this paper, and the story of Chaocipher, could not have been written:

Pat Byrne, for magnanimously heeding the call of history and donating her father-in-law's entire collection of Chaocipher-related artifacts to the National Cryptologic Museum (NCM). Chaocipher researchers and historians will owe her a debt for generations to come.

Cheryl Needle who, as Pat Byrne's associate in parallel with her own illustrious career as a book antiquarian, was highly instrumental in making the Chaocipher donation to NCM a reality.

Rene Stein, NCM Librarian, who responded to every request I had from NCM with exactly the material I needed, providing it promptly, efficiently, and always with a smile.

Special thanks are due to the National Cryptologic Museum of the NSA, Ft. Meade, MD, USA, for permission to reproduce pictures and photographs from the Chaocipher archives currently residing in the library.

Thanks are also due to the Curran Collection for permission to reproduce photographs of John F. Byrne. The Curran Collection – Photographs. Reproduced with kind permission of Helen Curran Solterer, from the originals held in UCD Library Special Collections. Digital image is copyright of UCD Irish Virtual Research Library and Archive.

12 About the Author

Moshe Rubin is a software engineer residing in Jerusalem, Israel. He received his B.Sc. in Computer Science from the Jerusalem College of Technology in 1979. His interest in cryptanalysis began at age fifteen after reading David Kahn's *The Codebreakers* from cover to cover multiple times, and it was Kahn's description of Chaocipher which led to a life-long fascination with this cipher.

13 References

Note: Due to the dynamic nature of the Internet, links to reference entries may 'break' over time. The most up-to-date list of reference links can be found at http://www.mountainvistasoft.com/chaocipher/chaocipher-revealed-reference-list.html.

[1] E-mail from Tony Bean to Moshe Rubin, 8 April 2011. Bean, a software engineer, also recalls contacting the Digital Equipment Corporation (DEC) office involved with computer security about Chaocipher, only to be informed that the company was not interested.

[2] Byrne, John Francis, *Silent Years: An Autobiography with Memoirs of James Joyce and Our Ireland* (New York: Farrar, Straus, and Young, 1953.) Reprinted in 1975 by Octagon Books, a division of Farrar, Straus, and Giroux.

[3] Byrne, John, Deavours, Cipher and Kruh, Louis. *Chaocipher Enters the Computer Age when its Method is Disclosed to Cryptologia Editors.* (Cryptologia, July 1990, 14(3):193-198, Volume 14, Number 3, July 1990). The three messages comprising Exhibit #5 can be found at http://www.mountainvistasoft.com/chaocipher/Chaocipher-ASCII-versions.htm (accessed 31 March 2011).

[4] Byrne, Mary Alice (nee Headen). John F. Byrne and Alice were never divorced and he never married Gertrude [1]. Alice's tombstone epitaph can be seen at http://www.findagrave.com/cgi-bin/fg.cgi?page=gr&GRid=12254369 (accessed 4 April 2011).

[5] Byrne, John Francis. Letter from Byrne to G. M. Campbell (a senior engineer in Bell Labs), dated March 1942. http://www.mountainvistasoft.com/chaocipher/byrne-correspondences/GCMRF-1942-03.html (accessed 7 April 2011).

[6] Calof, Jeff. *'Silent Years' - Chapter 21 (Chaocipher) Examined: Analyzing Byrne's Assertions*, 2010. http://www.mountainvistasoft.com/chaocipher/chaocipher-019.htm (accessed 31 March 2011).

[7] The Century Magazine, *The Irish Grievance: The Case for the Anti-Irish Party*, Vol. XCIII New Series: Vol. LXXI November, 1916, to April, 1917, pp. 465-473.

[8] The Chaocipher Clearing House, http://www.mountainvistasoft.com/chaocipher/ (accessed 31 March 2011).

[9] The Chaocipher Clearing House, *Progress Report #5*, http://www.mountainvistasoft.com/chaocipher/chaocipher-005.htm (accessed 31 March 2011).

[10] The Chaocipher Cleaning House, *Progress Report #12* (13 July 2010) ,http://www.mountainvistasoft.com/chaocipher/chaocipher-012.htm.

[11] The Chaocipher Clearing House, *Progress Report #14* (30 October 2009), http://www.mountainvistasoft.com/chaocipher/chaocipher-014.htm . With hindsight, it is most improbable that Byrne, a staunch Irish patriot who strongly opposed the British presence in Ireland, would ever have offered the "apple of his eye" to the British government.

[12] The Chaocipher Clearing House, *Historical Correspondences Related to Chaocipher*, http://www.mountainvistasoft.com/chaocipher/byrne-correspondences/index.html (access 31 March 2011).

[13] The Chaocipher Clearing House, *Information about Henry E. Langen*, http://www.mountainvistasoft.com/chaocipher/general/henry_e_langen_info.html (accessed 31 March 2011).

[14] Cowan, Michael J. *Chaocipher: Solving Exhibits 1 And 4*, 2010. http://www.mountainvistasoft.com/chaocipher/CowanDocs/MJC-paper-12.10.pdf (accessed 2 April 2011).

[15] The Crypto Forum, Chaocipher, http://s13.zetaboards.com/Crypto/forum/3003636/ (accessed 31 March 2010).

[16] Crypto Forum, a discussion about Exhibit #4. http://s13.zetaboards.com/Crypto/topic/6744990/1/ (accessed 31 March 2011).

[17] The Crypto Forum, *Paper describing algorithm to determine inconsistent C98U turnover periods*, 23 April 2010, http://s13.zetaboards.com/Crypto/topic/6693883/1/ (accessed 1 April 2011). This author had thereby disproven the possibility that C98U, or any other C98 model was the model used by Chaocipher. After this point there was no other candidate model.

[18] Crypto Forum, *Chaocipher as Dynamic Substitution?*. http://s13.zetaboards.com/Crypto/topic/6650602/1/ (accessed 11 April 2011).

[19] Dunin, Elonka. *Famous Unsolved Codes and Ciphers*, http://elonka.com/UnsolvedCodes.html (accessed 31 March 2011).

[20] Easton, Stewart C. *Rudolf Steiner: Herald of a New Epoch*. Anthroposophic Press. 1980.

[21] Ellmann, Richard. *Cranly's Memoirs*, Saturday Review, 13 Match 1954, page 18ff. Ellmann summarizes his review as follows: "Mr. Byrne is a chess player, and his book, which often appears circuitous and disconnected, has something of the character of a fine but unconventional approach in which the game is won by an unexpected mixture of heavy battling and finesse. His attitude of asking for neither admiration nor indulgence seems at first a bit stand-offish, but in the end his strength comes to include warmth, and the two combine to form a very attractive picture of an uncommon life".

[22] Erskine, Ralph and Freeman, Peter. *Brigadier John Tiltman: One of Britain's Finest Cryptologists*. Cryptologia, July 1990, 14(3):193-198. See pp. 310-313 for background of the stencil subtractor frame. I'm indebted to Ralph Erskine for raising the issue of US and British needs for a more secure field cipher.

[23] Fargnoli, A. Nicholas and Gillespie, Michael Patrick. *Critical companion to James Joyce: a literary reference to his life and work*. Infobase Publishing, 2006.

[24] Harding, Tim. *The Kibitzer #165: Masters and Patzers in the Biographical Dictionaries*. http://www.chesscafe.com/Tim/kibb165.htm (accessed 30 March 2011). In this column Harding mentions Byrne's supposed strength as a chess player. In a subsequent email Harding produced numerous clippings from The Irish Times over the period of 1904-1909 showing that Byrne was a member of the Sackville Club, participating both as a league and tournament player. Among his results were April 1905, Sackville Club class tourney, Gold Medal for the First Class; November 1905, Sackville Club wins every game in match against Dublin University on 14 Nov, Byrne on top board v T. W. Fitzgerald; 1 Feb 1906, Sackville Club return match against Clontarf, Byrne wins on top board v E. A. Ingram.Dec 1909, Byrne won on board 1 for Sackville versus J. G. Oulton (Dublin University). See [2, pp. 179-180] for Byrne's story of how he unknowingly beat the German chess master, Richard Teichmann. [2, pp. 43-44] explains that Joyce called Byrne 'Cranly' after Archbishop Cranly, who had come to Dublin in 1398, was known as the 'white bishop'.

[25] Hill, Jeffrey A., *Chaocipher: Analysis and Models*, (2003, revised 2009), located on The Chaocipher Clearing House web site, http://www.mountainvistasoft.com/chaocipher/chaocipher-009.htm (accessed 31 March 2011).

[26] Hitt, Parker. *Manual for the Solution of Military Ciphers*. Aegean Park Press, 1976.

[27] The Harry Ransom Center, The University of Texas at Austin, James Joyce Collection, Folder 5, boxes 1-3.

[28] Irish Virtual Research and Archive. Two pictures of John F. Byrne from the Curran Collection. http://hdl.handle.net/10151/OB_1000535_SC and http://hdl.handle.net/10151/OB_1000536_SC (accessed 4 April 2011).

[29] Kahn, David. 1967. *The Codebreakers*. New York: MacMillan.

[30] Kelley, Stephen J., October 1997, *The SIGCUM Story: Cryptographic Failure, Cryptologic Success* Cryptologia 21(4):280-316. Tells the story how Frank Rowlett leveraged two back-to-back messages sent using the SIGCUM (or M-228), enabling him to determine the complete rotor wirings. With Chaocipher, plaintext and ciphertext are so closely intertwined that the difference of a single character between two messages results in highly diffused and nonlinear outputs. One would like to believe that it is possible to solve Chaocipher given this scenario. This may give Chaocipher a cryptographic advantage over other rotor systems.

[31] Langen, Henry E., *Cryptography – Confidential*, located on The Chaocipher Clearing House web site, http://www.mountainvistasoft.com/chaocipher/general/Langen_Byrne.pdf (accessed 7 April 2011). Donated by David Kahn to the National Cryptologic Museum, this manuscript is a collection of notes and letters from people who believed they had devised unsolvable ciphers or cipher devices.

[32] Lauer, Rudolph F., *Computer Simulation of Classical Substitution Cryptographic Systems* Aegean Park Press, 1981.

[33] Mellen, Greg. 1979. *J. F. Byrne and the Chaocipher, Work in Progress*. Cryptologia. 3(3): 136-154.

[34] The National Archives, HW 25/33, *Chief Cryptographer [Brigadier Tiltman]. Miscellaneous cryptological papers*. http://www.nationalarchives.gov.uk/catalogue/displaycataloguedetails.asp?CATLN=6&CATID=8438300&j=1 (accessed 2 April 2011).

[35] The National Archives, PRO HW 14, Government Code and Cypher School: Directorate: Second World War Policy Papers. http://www.nationalarchives.gov.uk/catalogue/displaycataloguedetails.asp?CATID=7984&CATLN=3&FullDetails=False&j=1 (accessed 2 April 2011).

[36] National Cryptologic Museum Library, Ft. Meade, MD. Chaocipher Archives, Letter from John Byrne to Greg Mellen, catalogued as JF110-1, 8 February 1981. http://www.nsa.gov/about/_files/cryptologic_heritage/museum/library/irish_and_mellen_letters.pdf (accessed 4 April 2011).

[37] National Cryptologic Museum Library, Ft. Meade, MD. Chaocipher Archives, http://www.nsa.gov/about/_files/cryptologic_heritage/museum/library/macarthur_speech.pdf (accessed 31 March 2011).

[38] National Cryptologic Museum Library, Ft. Meade, MD. Chaocipher Archives, http://www.nsa.gov/about/_files/cryptologic_heritage/museum/library/chaocipher_blueprints.pdf (accessed 31 March 2011). The full set of five (5) blueprints, drawn up in November 1920.

[39] National Cryptologic Museum Library, Ft. Meade, MD. Chaocipher Archives, http://www.nsa.gov/about/_files/cryptologic_heritage/museum/library/chaocipher_2_and_si_vales.pdf (accessed 4 April 2011).

[40] National Cryptologic Museum. 1937 pamphlet entitled *Chaocipher: The Ultimate Elusion*. http://www.nsa.gov/about/_files/cryptologic_heritage/museum/library/chaocipher.pdf (accessed 31 March 2011).

[41] National Cryptologic Museum Library, Ft. Meade, MD. Chaocipher Archives, *Preliminary Instructions for Chaocipher II,*

http://www.nsa.gov/about/_files/cryptologic_heritage/museum/library/instructions_for_chaocipher.pdf (accessed 10 April 2011). This document describes a general purpose file encryption utility based on the original Chaocipher, with the added feature that it enciphers and deciphers any 8-bit binary byte value.

[42] National Cryptologic Museum. Letter from Parker Hitt to John F. Byrne, dated 3 August 1921. http://www.mountainvistasoft.com/chaocipher/byrne-correspondences/NCM-1921-08-03-Hitt-to-Byrne.gif (accessed 1 April 2011).

[43] Pelling, Nick. Cipher Mysteries web site, *The Chaocipher revealed!* (3 July 2010), http://www.ciphermysteries.com/2010/07/03/the-chaocipher-revealed (accessed 31 March 2011).

[44] Renby, J. F. (pseudonym for John F. Byrne). For an on-line example of his writing, see *The Possibility of Invading Germany; Plans Elaborated for an Attack on Her Western Coast by Means of Huge Guns Mounted on Armored Floats*, New York Times, 14 October 1915. http://query.nytimes.com/gst/abstract.html?res=F60F17FD395D16738DDDAD0994D8415B858DF1D3 (accessed 30 March 2011).

[45] Reviews and Things Cryptologic, Cryptologia, April 1991, XV(2): 176.

[46] Ritter, Terry. *Dynamic Substitution*. http://www.ciphersbyritter.com/index.html#DynSubTech (access 31 March 2011). Ritter was awarded U.S. Patent 4,979,832 in 1990. Dynamic Substitution is essentially a substitution table in which the arrangement of the entries changes during operation. Chaocipher can be considered a system whose alphabets (i.e., the left and right) change during operation.

[47] Rubin, Moshe. *Chaocipher Revealed: The Algorithm* (2 July 2010), http://www.mountainvistasoft.com/chaocipher/ActualChaocipher/Chaocipher-Revealed-Algorithm.pdf (accessed 31 March 2011).

[48] Rubin, Moshe. *Chaocipher Revealed: Deciphering Exhibit #1 in "Silent Years"* (8 August 2010), http://www.mountainvistasoft.com/chaocipher/ActualChaocipher/Chaocipher-Revealed-Deciphering-Exhibit-1.pdf (accessed 11 April 2011).

[49] Scheffler, Carl, *Chaocipher* 2010. http://www.inference.phy.cam.ac.uk/cs482/projects/chaocipher/ (accessed 31 March 2011).

[50] United States Cryptologic Series, Series IV, World War II, Volume 1, *American Signal Intelligence in Northwest Africa and Western Europe*, page 123, reference 12, which states that Hiser became Chief, Intelligence Branch, SID in 1944). http://www.nsa.gov/about/_files/cryptologic_heritage/publications/wwii/asi_in_northwest_africa.pdf (accessed 21 March 2011).

[51] George C. Marshall Research Foundation, William F. Friedman Collection. Letter from William F. Friedman to John F. Byrne, dated 7 September 1922. http://www.mountainvistasoft.com/chaocipher/byrne-correspondences/GCMRF-1922-09-07.html (accessed 31 March 2011).

[52] George C. Marshall Research Foundation, William F. Friedman Collection. Memo from William F. Friedman to Charles H. Hiser, dated 5-6 June 1942. Also received in response to Freedom of Information Act (FOIA) case 60070, 13 November 2009. http://www.mountainvistasoft.com/chaocipher/byrne-correspondences/GCMRF-1942-06-03-b.html

[53] George C. Marshall Research Foundation, William F. Friedman Collection. Letter from John F. Byrne to William F. Friedman, dated 9 June 1942. Also received in response to Freedom of Information Act (FOIA)

case 60070, 13 November 2009.
http://www.mountainvistasoft.com/chaocipher/byrne-correspondences/GCMRF-1942-06-09.html

[54] George C. Marshall Research Foundation, William F. Friedman Collection. Letter from William F. Friedman to John F. Byrne, dated 16 June 1942. Also received in response to Freedom of Information Act (FOIA) case 60070, 13 November 2009.
http://www.mountainvistasoft.com/chaocipher/byrne-correspondences/GCMRF-1942-06-16.html

[55] George C. Marshall Research Foundation, William F. Friedman Collection. Letter from William F. Friedman to John F. Byrne, dated 6 February 1957. http://www.mountainvistasoft.com/chaocipher/byrne-correspondences/GCMRF-1957-02-06.html (accessed 31 March 2011).

[56] George C. Marshall Research Foundation, William F. Friedman Collection. Letter from John F. Byrne to William F. Friedman, dated 17 February 1957. http://www.mountainvistasoft.com/chaocipher/byrne-correspondences/GCMRF-1957-02-17.html (accessed 30 March 2011).

[57] George C. Marshall Research Foundation, William F. Friedman Collection. Letter from John F. Byrne to William F. Friedman, dated 28 February 1957. http://www.mountainvistasoft.com/chaocipher/byrne-correspondences/GCMRF-1957-02-28.html (accessed 31 March 2011).

[58] George C. Marshall Research Foundation, William F. Friedman Collection. Letter from William F. Friedman to John F. Byrne, dated 3 March 1957. http://www.mountainvistasoft.com/chaocipher/byrne-correspondences/GCMRF-1957-03-03.html (accessed 31 March 2011).

[59] Friedman, William F. *Information regarding cryptographic systems submitted for use by the military service and forms to be used.* Cryptologia, Volume 15, Number 3, July 1991.

[60] Wikipedia, *Block cipher modes of operation*, http://en.wikipedia.org/wiki/Block_cipher_modes_of_operation (accessed 31 March 2011).

[61] Wikipedia, *Kerckhoffs's Principle*, http://en.wikipedia.org/wiki/Kerckhoffs's_Principle (accessed 8 April 2011).

[62] Wikipedia, entry on Patricia Neway, http://en.wikipedia.org/wiki/Patricia_Neway (accessed 4 April 2011)

[63] Wikipedia, *James Joyce's A Portrait of the Artist as a Young Man.*
http://en.wikipedia.org/wiki/A_Portrait_of_the_Artist_as_a_Young_Man (accessed 31 March 2011).

[64] Wikipedia, *Symmetric key management*, http://en.wikipedia.org/wiki/Symmetric_key_management (accessed 31 March 2011).

[65] Yardley, Herbert O., *The American Black Chamber.* 1931. Reprinted by Ballantine Books, New York, 1981.