"SILENT YEARS" – CHAPTER 21 (CHAOCIPHER) EXAMINED:
ANALYZING BYRNE'S ASSERTIONS

ADDRESS: Trabuco Canyon, CA; jcalof@yahoo.com

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

Throughout Chapter 21 of "Silent Years" [1], Byrne makes numerous claims, or "assertions", concerning the Chaocipher itself as well as his near 40-year journey between discovering the algorithm and publication of "Silent Years". This paper considers the veracity of these "assertions" and aims to conclusively answer questions as to whether Byrne was "asserting" from verified knowledge, speculation, hyperbole, or with intent to mislead or lie.

KEYWORDS: Chaocipher, John F. Byrne, J.F. Byrne, "Silent Years", Chapter 21, Assertions

FOREWARD

Readers of this paper are strongly encouraged to first read all of "Silent Years"– Chapter 21; while this paper liberally quotes from that Chapter, a complete read will put all such quotes into the full context Byrne intended. Readers are also encouraged to read the recently published papers "Chaocipher Revealed: The Algorithm" [2] and "Chaocipher Revealed: Deciphering Exhibit #1 in "Silent Years" " [3] by Moshe Rubin as this paper makes occasional references to each of them. Noted, but not yet published, is Rubin's "Chaocipher Revealed: Deciphering Exhibit #4 in "Silent Years" [4].

This paper owes a debt to the foundational research of Greg Mellen in his 1979 paper "J.F. Byrne and the Chaocipher: A Work in Progress" [5]. While this current paper does not delve into a study of Chaocipher's mathematical footprint or the algorithmic possibilities as did Mellen's, it does address several common topics of Chapter 21 analyzed in the earlier paper. With 31 years additional research and new source materials available, it is hoped that this new paper adds to Mellen's scholarship.

Note: There are two John Byrnes referenced in this paper: John F. Byrne, inventor of the Chaocipher, and his son, John Byrne, who carried forth the algorithm secret and privately disclosed it to editors of Cryptologia in 1989. The elder Byrne will consistently be referred to as John F. Byrne, or simply Byrne. When father and son are discussed together, for clarity the elder Byrne will be referenced as J.F. Byrne and the younger, always, as John Byrne.

INTRODUCTION

With the recent publication of the Chaocipher algorithm, as well as verified decryptions of Exhibit #1 & Exhibit #4, an analysis of the many "assertions" made by John F. Byrne in Chapter 21 of "Silent Years" offers an opportunity to confirm or refute his pronouncements in regards to the Chaocipher. A page-by-page review elicits at least nineteen distinct claims. It is the aim of this paper to consider each assertion in the context of Byrne's own time (with his privileged knowledge of the cipher), the present day given our newfound understanding of the algorithm, and with the newly afforded window into Byrne's own thoughts through many of his notes and letters, recently donated to the National Cryptologic Museum (NCM) by the Byrne estate.

Reading Chapter 21 of "Silent Years", one comes away with many impressions. Beyond the tantalizing and enigmatic description of the Chaocipher, there is a sense that the author is a man with something to prove. This is understandable. In the nearly 40 years since he discovered the Chaocipher algorithm in 1918, and the publication of "Silent Years" in 1954, Byrne seemed to experience nothing but frustration and heartbreak in his efforts to convince various government agencies and entities that he had created a fool-proof, unbreakable cipher. As Byrne himself later related in a1957 letter to William F. Friedman [6]:

"My main reason for writing the book was to be on record in the matter of my"Chaocipher." "

It is not surprising, then, that throughout Chapter 21 Byrne makes numerous pronouncements as regards his beliefs in his creation. Most must be taken at face-value, for Byrne does not often offer supporting empirical evidence. Consequently, what he perceives as a priori truths are, to a reader not privy to Byrne's own knowledge of Chaocipher, fascinating conjectures.

Now, 92 years after Byrne discovered the Chaocipher algorithm, and 56 years after "Silent Years" was published, we shall examine each assertion in detail. Does knowing the algorithm, and now understanding the relationship between Plaintext and Ciphertext in Exhibits #1 & #4, affect Byrne's pronouncements? For ease of reference, I have added a short notation regarding as to what page of "Silent Years" [SL] each assertion may be found.

THE ASSERTIONS

SL-264

"In a preceding chapter I have referred to Rutherford's achievement in 1919 of splitting an atom for the first time. In the preceding year, 1918, I had discovered a method of doing something to the written word, in any language, which affected that written word so as to result in its chaotic disruption. In two respects my method for achieving the complete annihilation of order and design in written language is more noteworthy than the method for the disruption of the atom. First, because my method for splitting the word is so simple that it could be performed by any normal ten-year-old school child, and second, because, unlike any other process of explosion or disruption, my method of disrupting the written words is identical and simultaneous with the complete restoration of order and design in the same written words."

Within this pronouncement are 5 distinct assertions (or sub-assertions within a primary assertion):

1. *"... my method for achieving the complete annihilation of order and design in written language is more noteworthy than the method for the disruption of the atom."*
2. *"... the complete annihilation of order and design in written language..."*
3. *"... my method for splitting the word is so simple that it could be performed by any normal ten-year-old school child..."*
4. *"... splitting the word..."*
5. *"... unlike any other process of explosion or disruption, my method of disrupting the written words is identical and simultaneous with the complete restoration of order and design in the same written words."*

1. "... my method for achieving the complete annihilation of order and design in written language is more noteworthy than the method for the disruption of the atom."

"Silent Years" was published in 1954, thirty-six years after Byrne discovered the Chaocipher algorithm and thirty-seven years after Ernest Rutherford first split the atom in 1917 [7]. Is one event "more noteworthy" than the other? Byrne's referential evidence favoring his own discovery is that 1) a normal ten-year-old school child could perform the algorithm, and 2) Chaocipher provides both an opportunity to disrupt the written word, and restore the written word, with the identical method, simultaneously.

Following Byrne's logic, if a normal ten-year-old school child could also split the atom, it would equate to the noteworthiness of Chaocipher. Since no ten-year-old school child (normal or otherwise) seems to be splitting atoms, either in 1954 or today, from Byrne's perspective "Evidence 1" would still hold true. Yet the opposite point of view might also be argued, that Chaocipher is a "simple" concept because a 10-year old could do it. Splitting the atom is a "greater', i.e. more "noteworthy", achievement because it takes far greater skill to do so. Whether Byrne considered both possible perspectives is unclear; if he did, that he chose to publish his assertion favoring Chaocipher over splitting the atom indicates his final thoughts on the matter.

Continuing on, if Rutherford's method of splitting the atom might also restore the atom by the same method (simultaneously), Byrne would equate this to the noteworthiness of Chaocipher. As no such method exists, historically or presently, from Byrne's perspective "Evidence 2" would also still hold true.

Yet the entire assertion is based on a subjective perspective. "Noteworthiness" is not a quantifiable state. While one may assign values to either achievement (e.g., Chaocipher rates "5" and Atom-splitting a "4" on a scale of 1-5, with 5 being best), those values would still be based on one's point of view [8]. Consequently, this assertion is not "proven" other than as the confident pronouncement of Byrne himself.

2. "… the complete annihilation of order and design in written language…"

Does Chaocipher achieve "the complete annihilation of order and design in written language"? One must ask what Byrne meant by "order and design". While he doesn't provide any such definition on SL-264, he does allude to it on SL-270:

"… a cipher which would, in actual fact, possess no order or design, a cipher which could only be adequately described as "a jargon of random characters."

To Byrne, then, "order and design" equates to the predictability and non-randomness of characters. Considered with his development of this theme on SL-265 and 268-269, where he references Edgar Allan Poe on the matter, it was the annihilation of letter frequency in the ciphertext that Byrne was after.

Though not published in "Silent Years", we also now have demonstrative evidence strongly supporting this conclusion. Recently donated by the Byrne estate to the National Cryptologic Museum Foundation is a 26 x 55 graph Byrne himself prepared [9] regarding Exhibit #1's letter frequency distribution (See Figure 1). This demonstrates Byrne was both highly aware of letter frequency distribution and was sophisticated enough to create the elaborate chart.

Does Chaocipher, then, achieve an annihilation of the language to prevent letter frequency analysis? Based on 56 years of failed cryptanalysis with full knowledge of matching plaintext and ciphertext for the majority of Exhibits #1 – #4, the answer is "Yes". With the recent publication of the algorithm, it can be seen that Chaocipher flattens letter frequency in the ciphertext extremely well, thoroughly hiding plaintext repetitions. Note the row near the bottom of the chart tallying the number of occurrences where a plaintext letter has zero enciphered representations by another letter (e.g., Column 5 "O" and Row "D" has zero examples; for Exhibit #1, the first "O" in "GOOD" is never enciphered by the letter "D").

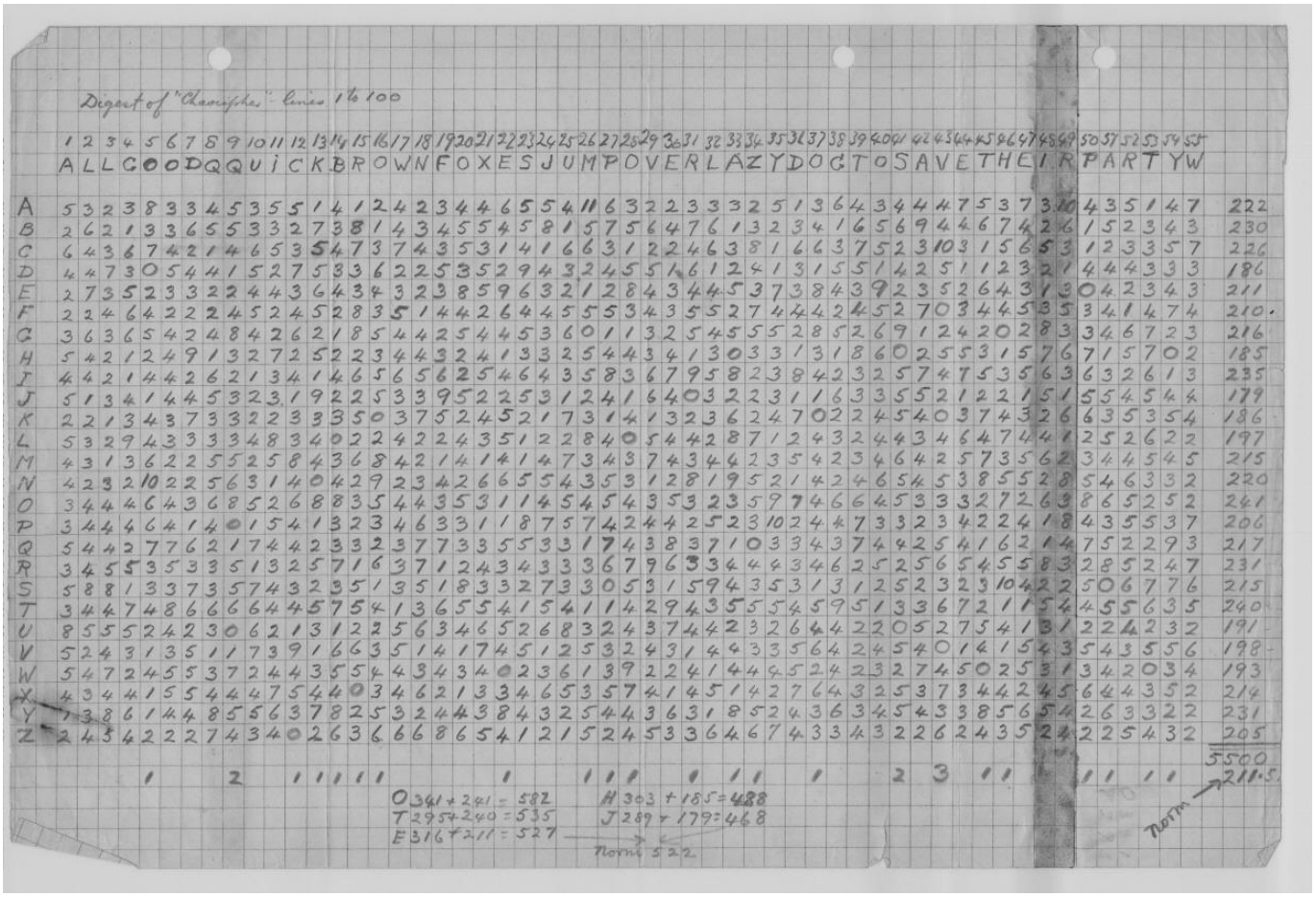


Figure 1 - Byrne-prepared graph demonstrating Exhibit #1 letter frequency
(courtesy of the National Cryptologic Museum Foundation)

Though Chaocipher reflects a flattened letter frequency count, studying only letter frequencies is not the strongest measure of proving a cipher's security. For example, prior to the 2010 publication of the Chaocipher algorithm, computer analysis [10] of Exhibit #1 revealed unique aspects such as:

- Strong tendencies towards a blocking factor of 13
- No plaintext/ciphertext identities with a distance of less than nine positions away; one result of this being that "XX" (plaintext) can never be "YY" (ciphertext)

Though not discernible from "Silent Years", Byrne was aware of the latter (as evidenced by his 1938 letter to Capt. John Irish, Assistant to Bureau of Engineering, Navy Department, proposing he review Byrne's blueprints and pamphlet "Chaocipher – The Ultimate Elusion" for consideration towards a Navy cipher) [11]. These features allow for cryptanalysis at a level Byrne may never have envisioned (and may one day lead to a specific or generic solution for decipherment).

3. "… my method for splitting the word is so simple that it could be performed by any normal ten-year-old school child…"

J.F. Byrne never defined "normal" for his phrase "any normal ten-year-old school child". We do have, however, conflicting evidence that it was Byrne's son, John Byrne, to whom he was referring. The conflict is not whether John Byrne understood or performed the Chaocipher method, but rather at what age he provided the assistance to his father. John Byrne related to Cryptologia's Louis Kruh and Professor Cipher Deavours in 1989 of his:

"… memories of tense and tedious hours striving for perfect accuracy while working with my father and his 'contraption' at the dining room table".

The Cryptologia Volume XIV Number 3, July 1990 edition includes their article "Chaocipher Enters the Computer Age when its method is disclosed to Cryptologia's Editors" [12]. While the article doesn't state at what age John Byrne assisted his father, this edition of the Cryptologia journal itself provides two precise references aligned to Assertion #3. First, on the edition's cover is a candid photo of father and son, below which reads the caption:

John F. Byrne and his ten year old son, John Byrne

It is likely the "ten year old" reference was provided by John Byrne, whether from a date on the photo or from memory (which we'll assume was accurate). Opening the journal, on the title page below the names of the five Cryptologia editors (David Kahn, Louis Kruh, Cipher Deavours, Brian Winkel, and Greg Mellen), we have the following quote from John Byrne:

"The cover photograph was taken at the time I really began to know my father and to work with him on his 'contraption'… simple enough for a ten-year old. If it hadn't been so serious, it could have been a wonderful puzzle. Sadly, for him it was Chaocipher – The Ultimate Elusion."[13]

With these two references to "ten-year-old", we encounter a minor discrepancy with the known Chaocipher timeline. In Chapter 21 [SL-277], Byrne writes:

"Working through the summer and fall of 1937, I made my model and prepared on and by it, a document which I intended for submission to the Navy Department… Chaocipher – The Ultimate Elusion."

With John Byrne's birth date of 6/6/1929, this would have made him just past 8 years old at the time. Consequently, several questions arise:

- If John Byrne assisted at this time, was he able to encipher Chaocipher at age 8? The 1990 Cryptologia edition seems to indicate he only began to encipher Chaocipher at age ten, which would be 1939, two years after Byrne enciphered his Exhibit #1
- Did he really work with his father on "Chaocipher - The Ultimate Elusion", or rather several years later when J.F Byrne enciphered Exhibits #2 - #4?
- If John Byrne didn't assist his father at age 8, why did J.F. Byrne choose the phrase "ten-year-old" for this assertion? Did he possibly demonstrate Chaocipher to another 10-year-old school child?

Presently, these answers are not known for certain. However, one of the recently donated materials to the NCM by the Byrne estate is a February, 1981 letter [14] from John Byrne to Greg Mellen (in reference to Mellen's own 1979 Cryptologia article). In this letter are two references confirming John Byrne's efforts in assisting his father at some point in time:

"The model may father, mother, and I worked on…" and *"I remember helping my mother and father check the galley proofs letter by damnable letter."*

J.F. Byrne's 1938 letter to Captain John Irish [11] contains several passages that Byrne himself later quotes in Chapter 21; others seem to be early paraphrases of what would later be written in "Silent Years". Concerning Assertion #3, Byrne provides a fascinating variant as he writes:

"A child could operate my model; and if the finished machine were to be developed as I envision, it could be operated by any child who had outgrown his infancy."

Byrne's choice of words here ("any child who had outgrown his infancy") is less specific than his claim in "Silent Years" written 16 years later. At the same time, outgrowing one's infancy would typically be considered to be an age far younger than 10 years. This lends credence to the idea that it was to John Byrne he may have been referring when he wrote the "Silent Years" passage.

As regards the Chapter 21 assertion, and seeking more direct evidence, I taught the algorithm to my 11-year old son and two of his friends (all just a few months past their 10th year). Over the course of 30 minutes, I demonstrated the rules for enciphering and deciphering using a hand-made Chaocipher machine (constructed from a tv-dinner tray, three wooden dowels, and Scrabble-tiles – see Figure 2). They were able to grasp the concept and execute the permutations quite readily (though it took several tries before being error-free). I then enciphered a short phrase and asked them to decipher it; again they were successful. I asked them to encipher their own short phrases and have each other decipher them; once again, success.

Figure 2 - Photo of home-made Chaocipher machine

Byrne's assertion, then, carries weight. At the same time, "normal" is a subjective term and, as John Byrne noted (and my son and friends discovered), "perfect accuracy" when enciphering by hand can be tedious and tense. It takes careful work so as not to make an error, and a ten-year-old's patience may be tested with longer passages.

4. "… splitting the word…"

Does Chaocipher "split the word"? Literally and figuratively, it does not. For example, in enciphering the word "explanation", the algorithm does not break the plaintext into smaller groupings such as "exp", "lana", "tion", nor is the resulting ciphertext broken into fragments. While the ciphertext does not reveal letter frequency, those ciphertext letters do reflect the sequential enciphering of "explanation". For successful deciphering, the same sequencing must be maintained in both ciphertext and plaintext. So, while Chaocipher creates a strong encryption, it does not "split the word" as Byrne asserts.

There is a class of "Fractionation" ciphers that in fact "split the word" through a combination of fractionating the plaintext and columnar transposition (of which Chaocipher does neither). Félix Marie Delastelle [15], like Byrne an amateur cryptographer, invented such examples as the bifid, trifid, and four-square ciphers. Later examples include the German ADFGVX and Russian VIC ciphers.

5. "… unlike any other process of explosion or disruption, my method of disrupting the written words is identical and simultaneous with the complete restoration of order and design in the same written words."

Byrne's argument by analogy is somewhat grandiose. Though not explicitly stated in this specific phrasing, his earlier reference to "splitting the atom" leads the reader here to think of just that though his literal phrasing (explosion or disruption) makes no such claim. On closer consideration, Byrne's intent seems to be comparing historical ciphering methods to that of the Chaocipher. Current scholarship of Byrne does not suggest he had any substantial professional or personal education in such methods; from what can be discerned from "Silent Years", his foundation for historical ciphers is based on the writings of Poe, and possibly some familiarity or research into the writings of Hero of Alexander [SL 265]. Greg Mellen, in his 1979 article [5], suggested Byrne's knowledge in this area increased in the years between his discovery of the algorithm and the publication of "Silent Years":

"I further surmise that Byrne, having had these many contacts, did not emerge totally naïve about cryptanalysis. There is evidence in Byrne's writings to support the view that he had tutoring." and, in the References, *"That the text of the Chaocipher is in five-letter groups is indicative of Byrne's awareness of operational practice. He also refers, to cite just one example, to "the third letter in the ninth group," [1, p. 282] rather than to the more natural and innocent "forty-third letter."*

Whether Mellen's assessment is true or not, from Byrne's limited knowledge of historical ciphers up to 1954 his pronouncement that Chaocipher's method was unique would be a true statement. To his credit, his method remained unique (at least in the non-governmental sector) both in 1918 up until 1990 when Terry Ritter patented and published his work on Dynamic Substitution [16]. The fact that Ritter independently discovered the concept does not lessen Byrne's achievement which was indeed unique in his time and remains the earliest documented instance of dynamic substitution.

SL-265

"When I discovered my method for the utter disruption of the written word, or, to express this differently, my method for writing a cipher which would, in fact, be absolutely indecipherable, I discovered something which was just as accessible to Poe as it was to me. The ancient Egyptians and Babylonians could have been completely familiar with the principle, a fact which is readily deducible from a treatise on mathematics written by Hero of Alexandria in the second century B.C. The point I am making is that during the past two thousand years and more anyone could have had access to my method for the chaotification of language."

Within this passage are 4 related assertions:

6. *"… I discovered something which was just as accessible to Poe as it was to me."*
7. *"The ancient Egyptians and Babylonians could have been completely familiar with the principle…"*
8. *"… a fact which is readily deducible from a treatise on mathematics written by Hero of Alexandria in the second century B.C."*
9. *"… during the past two thousand years and more anyone could have had access to my method for the chaotification of language."*

Let us examine each in detail.

6. "… I discovered something which was just as accessible to Poe as it was to me."

Could Edgar Allan Poe have discovered the Chaocipher algorithm? With intelligent thought, any individual could discern, perhaps even stumble upon, the concept behind the algorithm. Reading Chapter 21, Byrne's writing is more critical of Poe the cryptanalyst than in awe of his skills. He quotes two literary references from Poe: "The Gold Bug" [17] and "Cryptography" [18] [SL 265]. Though Byrne does not delve deeply into Poe's own cryptographic skills, Poe's strengths appear to have (mostly) been limited to mono-alphabetic substitution ciphers [19]. "The Gold Bug" addresses one such decipherment, and Poe's own writings promoting his cipher-cracking skills also reference ciphers of this nature. While it is possible Poe might have discovered the algorithm as did Byrne (for the algorithm is a mathematical truth, available to all), it is not likely that he would ever have done so.

7. "The ancient Egyptians and Babylonians could have been completely familiar with the principle…"

From the perspective that the Chaocipher algorithm (like any algorithm) is a mathematical truth, yes, it is possible the Egyptians and Babylonians could have been familiar with the principle. By the same token, other ancient civilizations such as the Greeks, Estruscans, or even our Cro-Magnon ancestors could have as well. The historical record, however, does not indicate evidence that any of them were familiar with the principle. Yet Byrne goes on to offer the following statement in support of his assertion:

8. "… a fact which is readily deducible from a treatise on mathematics written by Hero of Alexandria in the second century B.C."

Though Byrne notes Hero of Alexandria lived in "the second century B.C.", modern historians place his lifetime c. 10-70 AD, i.e. the first century AD [20]. Does this immediately negate Byrne's assertion, given this 200 year discrepancy? Was Byrne referring to a different "Hero of Alexandria"? It's possible in Byrne's time the years of Hero's life were not yet clarified and that "the second century B.C." was the accepted timeframe for reference. For purposes of this discussion, we'll assume Byrne was referring to the famous Greek mathematician, engineer, inventor, teacher, and author. More challenging, though, is that Byrne does not make clear to which "treatise on mathematics" he is referring. Hero wrote several such books [21] ("Metrica" being the most well-known example) – but these seem to pertain to the mathematics of geometry, such as calculating areas and volumes. None suggest any mathematical formulas or ideas from which one might infer or derive the Chaocipher algorithm. Hero is often credited with creating the "Babylonian Method" for finding a number's square-root, as well as "Heron's Formula" for finding the area of a triangle from its side lengths. Neither of these mathematical formulas appears related to the Chaocipher algorithm.

In the full passage noted above for SL-265, Byrne explicitly uses the terms "method" and "principle", collectively implying a theoretical process. If we focus on these, they perhaps could refer to a mechanical principle. Immediately following the passage above, Byrne goes on to write:

"The first device, or machine, which I constructed, solely for the purpose of demonstrating a principle…" and, in the next paragraph, *"…I formulated a principle for the development of a cipher… I built the little model… for the purpose of demonstrating this principle."*

Might Byrne have been referring, then, to one of Hero's treatise on "mechanics" rather than "mathematics"? While Byrne never built his Chaocipher machine for which he had blueprints professionally drafted, the recent donation of five of these blueprints to the Museum provides a window into his thoughts [22]. The drafts demonstrate two cipher wheels (one for plaintext, the other for ciphertext) that are geared to mesh and turn together (one clockwise, the other counter-clockwise) and, at the user's will, disengage to turn independently. Hero wrote of mechanical devices, including many that require similar gear-meshing systems. Most likely, Byrne was referring to the mechanical aspects of Hero's writings, specifically the intermeshing of two gear systems.

Many of Hero's writings are considered lost… whether they were available to Byrne as late as 1954 is not clear. Until such time as a "mathematical treatise" by Hero is found that provides a direct, or foundational, basis for the "principle" of the Chaocipher algorithm, we may assume that either 1) Byrne was mistaken in calling it a "mathematical" treatise, or 2) Byrne may have been misleading his readers with an intentional red herring.

Interestingly, in John Byrne's 1981 letter to Greg Mellen [14], he writes *"Forget about Euclid, Hero, Joyce, and all those others. Use your own head, you obviously have a damn good one."*. John Byrne may have been saying that the Hero track was, at best, a weak link and that it was actually irrelevant as a hint.

9. "… during the past two thousand years and more anyone could have had access to my method for the chaotification of language."

This is a true assertion. As a mathematical truth, the algorithm was there for anyone to discover. Is it possible others "during the past two thousand years" may have identified the algorithm but failed to recognize it for its virtues as a ciphering system? We can only speculate; what "Silent Years" demonstrates is Byrne was the first to recognize the algorithm as a method for ciphering - and then to take action upon his discovery by developing the Chaocipher principles, documenting his findings, and crafting a mechanism for the algorithm implementation.

As Byrne writes in the two following passages, his discovery was not happenstance:

On SL-268 and SL-276 respectively, he states:

"… let me make it clear that my discovery was not fortuitous".

"When I was devising my cipher system, I worked neither with model nor with diagram. I solved my problem in a short period of delicious mental concentration and exhilaration. In fact, I worked out the problem blindfold, as I would have worked out a chess problem…"

Byrne was himself an accomplished chess player [23]. Chapter 5 of "Silent Years" is entitled "Congress v. House of Commons at Chess" [24], where Byrne describes his own passion for the game and his rising improvement as a player. Lifelong friend James Joyce, in his "Portrait of the Artist as a Young Man", based the character Cranly on Byrne. The fictional Cranly was likewise a strong chess player. In the Chaocipher timeline, a reference to "blindfold chess" appears once again in the 1981 letter to Greg Mellen from John Byrne [14] who wrote [all spelling and punctuation transcribed verbatim]:

"Remember blindfold chess and all those other mental gymnastics? My father hardly ever used "pencil and paper" except for making rare notes for others to read. (More's the pity.) The "operations" could not have been performed with pencil and paper to any practical extent."

While J.F. Byrne admits he did not "create" the algorithm (rather, he "discovered" it), his accomplishment is not to be minimized. In known cryptographic history, he was indeed the "first" developer of a working dynamic substitution cipher.

SL-265

"The first device, or machine, which I constructed, solely for the purpose of demonstrating a principle, was a little model, constructed in an empty cigar box which, when full, had contained fifty small Havana cigars."

To paraphrase Byrne's passage above, we get the next assertion:

10. The first Chaocipher machine fit into an empty cigar box (which held 50 small Havana cigars)

As Byrne did not provide the specific dimensions of his cigar box, or the actual size of the fifty small Havana cigars, we are left to wonder about the box's exact height, width, & depth… and the length and thickness of the cigars. On SL-266, Byrne notes he brought his "cigar box device" to attorney Marcellus Bailey in 1919.

The National Cryptologic Museum Foundation published a photo [25] of the donated "wooden mock-up of the Chaocipher cipher wheels" for the original machine (see Figure 3). As the photo does not provide a scalable reference to ascertain the size of the wheels, I wrote to Rene Stein, Sr. Librarian of the NCM, inquiring as to the dimensions of the mock-up and received the following reply:

"The disks of the mock-up are 15 inches in diameter. The white background you see in the photo is heavy cardboard measuring 20x32 inches."

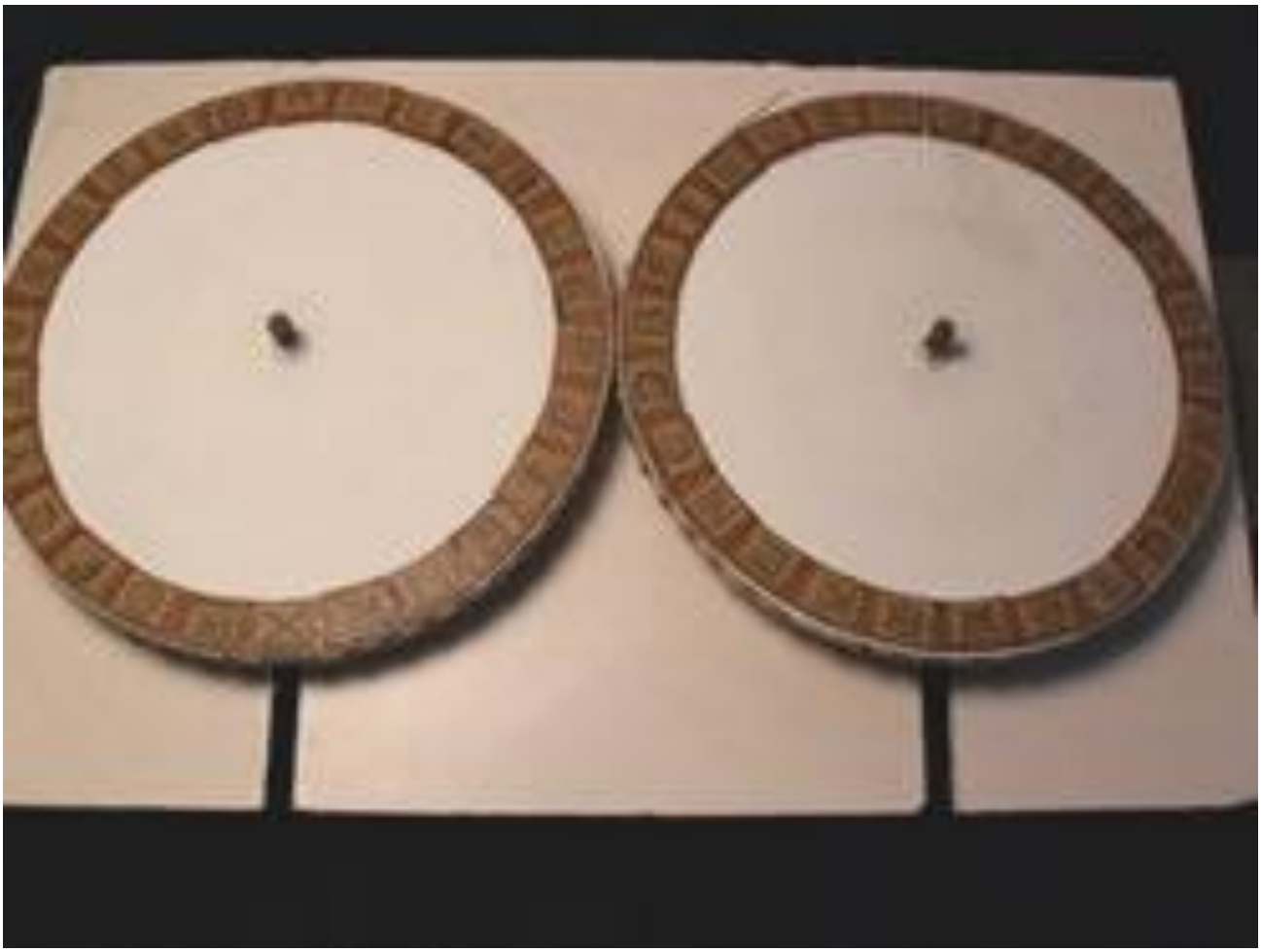


Figure 3 - Wooden Mock-up of Chaocipher cipher wheels
(courtesy of the National Cryptologic Museum Foundation)

Understanding that the "mock-up" is not the actual, original apparatus of Byrne's cigar box machine, can we determine if such a design would feasibly scale to within a box of the type Byrne describes? Consider the dimensions of the "cardboard" in the picture. 32 inches in length is nearly 3 feet; placing three 8 ½ by 11 inch pieces of paper end to end (landscape) equals 33 inches, and two pieces end to end (portrait) equals 17 inches. This surface area is far larger than a cigar box designed to hold "50 small Havana cigars".

How large, then, would such a cigar box likely have been if it held what Byrne stated? The only size reference Byrne provides is that the cigars were "small". Assuming cigar size comparisons in the early 1900s are similar to those of today, we can assume that a typical cigar was probably from 6" to 9" long and about ½" to 1" thick. If 6" was on the "small" side, and allowing for the 1" thickness, if laid out in a pattern to fill a flat cigar box the most efficient designs might be:

- 1 row, 10 cigars per row, 5 rows deep
- 2 rows for 2 levels / 1 row for top level, 10 cigars per row, 3 rows deep,

The latter option would provide for a larger surface area in which to place the Cipher wheels… but the inner dimensions of the box (assuming a snug fit for the cigars) would only be 20"x12"x3". Each cipher wheel would have to be just 9"-10" in diameter; the peripheral lettering on each would have to have been quite small in order to get all 26 letters around the circumference. Knowing that each letter also would need to be removable (to perform the plaintext/ciphertext alphabet permutations) suggests a functional-size challenge for the User.

With these considerations, can we determine if Byrne's original cipher machine was truly a scaled-down version of the mock-up inside a cigar box that previously held fifty small Havana cigars? Byrne tells us the original was demonstrated to Bailey in 1919 and then to William F. Friedman & Major Frank Moorman in 1922 where Byrne

noted, the machine was "*smashed to smithereens*" while in transit upon its return [SL-276]. A later "working model" was created in 1937 to prepare Byrne's pamphlet "Chaocipher – The Ultimate Elusion" for a presentation to the Navy Department [SL-277]; Byrne does not specify whether this too was in a cigar box. However, the 1981 letter from John Byrne to Greg Mellen (in response to Mellen's article "Chaocipher: A Work In Progress") provides us with the final whereabouts of the later model [all spelling and punctuation transcribed verbatim]:

"The infamous cigar box was "lost, stolen, or strayed" before my memory but it was NOT "non functional". The model my father, mother, and I worked on was destroyed by me shortly after my father's death.". Later, he writes *"It was not at all a less contrivance in terms of its capacity to perform the full function(s) of the envisioned final device."*

While it is clear some sort of box-type device existed, until demonstrative evidence surfaces, such as a photograph of the original machine, whether it was really in a *cigar box which held 50 small Havana cigars remains* open to some debate.

SL-265

"I formulated a principle for the development of a cipher which would be materially and mathematically indecipherable…"

Within this phrase is the next assertion:

11. "… a cipher which would be materially and mathematically indecipherable…"

Is the Chaocipher "materially and mathematically indecipherable"? For this assertion to be true, both aspects of it must be true (given Byrne chose to use the qualifier "and" versus "or"). Thus, we may consider this as two separate assertions – a) materially indecipherable, and b) mathematically indecipherable.

What did Byrne mean by "materially"? Oxford Dictionary Online [26] defines it as an adverb:

1. [often as submodifier] substantially; considerably:
   materially different circumstances
2. in terms of wealth or material possessions:
   a materially and culturally rich area

Of these two definitions, Byrne would almost certainly have been thinking of the former. Yet, by this definition, we are left with a non-quantifiable "submodifier" – how does one concretely define "substantially" or "considerably"? It's not necessarily 100%, but it's likely more than 50%. With Chaocipher, one would think Byrne might use the more exacting adverb "absolutely". By using "materially", did he subconsciously betray any doubts he might have had about its indecipherability? Given his choice of word, "materially indecipherable" is not a statement we can either prove or disprove. This leaves us with the phrase "mathematically indecipherable". Surprisingly, Byrne did, in fact, provide *his* definition for not only this, but the entire phrase "materially and mathematically indecipherable" a few pages later on SL-270:

"… the only cipher which would be materially and mathematically indecipherable is one which would present no feature other than that of having been drawn inconsequentially from a rotating drum, or pecked haphazardly on a typewriter – a cipher which would be devoid of discernible order, or design, a cipher which would, in actual fact, possess no order or design, a cipher which could only be adequately described as "a jargon of random characters."

This harkens back to Assertion #2's challenge of statistical analysis by letter frequency in the ciphertext. Was his confidence also based on the expectation it would be only classic "pencil and paper" attacks on Chaocipher? Chapter 21 does not suggest Byrne had any other mathematical technique in mind, though on SL-284, his last page of prose prior to Exhibit #1, he makes the following prescient challenge:

"And finally, I issue to the believers in the wonderful capabilities of electronic calculating machines, a warm invitation to take up my challenge. Perhaps the genial-looking Professor Norbert Wiener [27] of the Massachusetts Institute of Technology would like to embark on these waters of chaos in the hope that his cybernetical pilot might, by the exercise of super-human navigatory prowess, be able to steer him to some port".

With electronic computing still in its infancy in 1954, one can only ponder if Byrne envisioned its growth in both power and speed in the coming years; to what degree Byrne was aware of his era's computing limitations/capacities is speculative. John Byrne, in his 1981 letter to Greg Mellen, offered some additional insight on this matter:

"Dad saw the advent of a computer technology and predicted that one day the use of his system would be as "simple as using a typewriter." "

What is clear is that from 1954 to 1990, no non-governmental computers were able to solve Byrne's Chaocipher challenge, or determine the algorithm used to derive its ciphertext. It is not known whether any government agency was able to accomplish the task. In 1989, John Byrne revealed the algorithm to Louis Kruh and Professor Cipher Deavours. They proceeded to write in their 1990 Cryptologia article "Chaocipher Enters the Computer Age when its method is disclosed to Cryptologia's Editors":

"Attempts to cryptanalyze the cipher appear to substantiate the elder Byrne's claim that ". . . any person on earth using a device similar to my own home-made contraption, could produce a cipher message which would be indecipherable by any other person except the one to whom the message is directed." Certainly, Chaocipher was a very secure cryptographic system for its time and even the original system would not be easy to solve today using a computer."

Over the next 20 years, continued unsuccessful efforts to solve Byrne's challenge have proven Kruh and Deavour's pronouncement to be true. It was not until the Chaocipher algorithm became publicly known in 2010 that – when combined with the known plaintext – Exhibits #1 & #4 were "solved" in the sense that both the starting left and starting right alphabet sequences were derived. As of this paper's writing, Byrne's Exhibits #2 & #3, and Kruh & Deavour's own Challenge Exhibit #5, remain unsolved.

Is Chaocipher, then, "materially and mathematically indecipherable"? Though often speculated that most any classic (pre-computer) cipher can be deciphered with today's computing resources, at this time a true singular ciphertext-only Chaocipher message (where the underlying plaintext, or plaintext source, is unknown), or a set of in-depth Chaocipher ciphertext-only messages (where both messages begin with the same left/right alphabets but have different underlying plaintexts, a possible real-life scenario), have yet to be solved – either by "pencil and paper", or through computational programming. Solving either would disprove Byrne. Time will tell if a solution can be discovered (either generic or case-specific).

SL-266

"With these two things, my device and my principle, any person, anywhere, writing in any language, could by applying my principle and using my device transcribe his written words into a script which would be absolutely indecipherable by anyone except the persons for whom the message is intended; and be it remembered that while possession of my device together with knowledge of my principle, would enable any person to write a script which be absolutely indecipherable by anyone except the person or persons for and to whom the script was written and addressed, yet possession of my device together with knowledge of the general principle involved, would not enable any person to decipher any message whatever written by anyone else and not intended for him."

Within this paragraph are two distinct assertions. First:

12. "… any person, anywhere, writing in any language, could by applying my principle and using my device transcribe his written words into a script which would be absolutely indecipherable by anyone except the persons for whom the message is intended…"

Assertion #12 revisits much of the same territory as previously examined in Assertion #11. What is unique about the later assertion is its claim as regards to "writing in any language". As evidence for his claim, Byrne's Exhibit #2 provides an example of a Latin plaintext (from Caesar's "De Bello Gallico") transcribed by the Chaocipher algorithm into a ciphertext that masks the Latin language letter frequency. Byrne writes on SL-282 to SL-283:

"… the reader will note the frequency of the recurrence in the cipher script of both the letters W and K, notwithstanding that the letter W does not occur at all in Latin, and the letter K is extremely rare in that language."

As Exhibits #1, #3, & #4 all transcribe English text, Byrne's "any language" assertion is thus directly supported by two distinct examples (Latin and English). Yet all four of his Exhibits cite the use of a Latin letter-based alphabet (26 letters A to Z) in both his plaintext and ciphertext permutation alphabets. His assertion is bolder than this -- would the algorithm be applicable in a foreign language's non-Latin character alphabet? Would Chaocipher work for Russia's Cyrillic script, an Asian script such as Chinese, or a symbolic script such as Hieroglyphics?

For permutation purposes, Byrne's algorithm contains a "zenith" at position 1 and "nadir" at position 14 (based on a 26-character alphabet). Conveniently, the English Latin-character alphabet splits evenly into 2 groups of 13 letters. It is conceivable that alphabets with greater or lesser total characters might adapt the zenith/nadir positions (and the algorithm permutations) relative to their own length. While Byrne chose to set his zenith and nadir at the initial positions of each equal-size 13-letter block, the algorithm might be adapted to unequal block-sizes. For example, Russia's Cyrillic script uses 33 distinct characters [28]; while this does not divide into 2 equal groupings of letters, the Chaocipher algorithm will still work if a nadir is defined accordingly.

A language based on glyphs offers an interesting consideration. Rather than each character representing a single letter (as in Latin-based English), glyphs may often represent a single word, or even a group of words. Yet Byrne's assertion is not negated by this challenge, for the algorithm's function is predicated solely on having a singular character in each available position. What that character might represent is not a consideration towards the algorithm's successful function. All that needs to be maintained for successful enciphering and deciphering is the consistency of characters represented in the chosen ciphertext and plaintext alphabets.

Byrne correctly refers to his "principal" as opposed to his "device". The Chaocipher principle can be defined in a generic fashion: for an alphabet of N letters, the nadir may be any number between 1 and N. The method of permuting the left and right alphabets can also be made more generic. Byrne uses one specific manifestation of his principle, but one can make it much more generic. Consequently, Chaocipher can be adapted easily into software for most any language. Using a physical device, rather than software, makes that somewhat more difficult for exotic languages.

The recently donated Byrne archives to the NCM provide a data sheet prepared for John Byrne (by his nephew) describing how Chaocipher was implemented in software for binary data [29]. This is a generic implementation that will work for any script (e.g., Chinese, Korean, Hieroglyphics, etc) that can be encoded in an 8-bit binary form. An implementation for Unicode (e.g., 16 or 32-bit) could easily be designed. An implementation of Chaocipher that supports the full 256-character ASCII page has already been created by Paul Makowski. [30]

Assertion #12, then, appears to be correct concerning "any language" as it pertains to *known* languages. Yet taking Byrne at his own words of '*any person, anywhere, writing in any language",* is it still possible there exists a language which will not adapt into the Chaocipher algorithm? The generic Chaocipher principle noted above suggests an answer of "no". Yet from a mathematical perspective, we have not proven this to be so. It is theoretically possible that a language may exist (or may be created) whose rules preclude adaption into the principle (or even into binary). As such, while Byrne's assertion is probable in a real-world sense, it has not yet been mathematically proven to be "true" for all possible instances.

The second distinct assertion is:

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

This assertion is the closest evidence we have regarding Chaocipher as it relates to Kerckhoff's principle [31] that a cryptosystem should be secure even if everything about the system, except the key, is public knowledge. Whether Byrne actually knew of Kerckhoff's principle is unclear; there is no mention of Kerckhoff or his principle in "Silent Years", nor in any Byrne-related letters or personal documents that (to date) have been publicly reviewed. One of the primary complaints made by researchers against Byrne, and his claim of Chaocipher's indecipherability, is that he did not "play by the rules" in making the "system" known to the cryptographic community, thereby providing for a fair testing of its merits and strengths. Now, with the recent publication of the algorithm, such scrutiny is underway. As of this paper's writing, a ciphertext-only message has yet to be successfully deciphered.

One fascinating consideration of this assertion is that within Chapter 21, Byrne writes that he *did* demonstrate both his principle and device to several persons well-versed in cryptographic methods:

SL-272
"I got in touch with Colonel Parker Hitt, who had authored a little booklet… bearing the title, Manual for the Solution of Military Ciphers. …It was not until August 3, 1921 that he wrote me a definitive and formal letter about my system."

SL-273; Byrne quotes from Hitt's letter
"I am returning to you herewith the machine and the accompanying papers… As to the principle of the machine, it is undoubtedly a most ingenious and effective device… 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."

Sl-269
"… I had given a demonstration to the War Department in Washington of my first crude cipher machine. The persons to whom I demonstrated my "machine" were Major Frank Moorman, of the General Staff… and Mr. W.F. Friedman, cryptanalyst; and this demonstration was given by me in July 1922…"

SL-283
"A formal demonstration of my Chaocipher system, together with a decipherment of this exhibit [Exhibit #1]*, were given by me to the American Tel. & Tel. Company through some top official of the Bell Laboratories, these including Mr. Ralzemond D. Parker, a former Telegraph Development director for that organization."*

Of all these named individuals, it is that of William F. Friedman [32] which is most intriguing. Byrne corresponded with Friedman for decades regarding Chaocipher [33], pointedly asking Friedman if he could decipher his challenge messages and, if he couldn't, Friedman would have to admit to the cipher's strength of security. Friedman was firm in replying that he couldn't answer Byrne's question until Byrne provided requested materials and additional information about Chaocipher to Friedman, something Byrne (as demonstrated by his actions) refused to do.

Yet Byrne did, in fact, demonstrate the original Chaocipher machine, including the underlying system, to Friedman in 1922. Friedman himself mentioned, in a 1954 after-dinner speech [34], that:

"Mr. Byrne… thought he had invented what is sometimes called a holocryptic cipher, that is, one that cannot be solved by pure analysis. Maybe Mr. Byrne did invent a holocryptic cipher, but I doubt it. I doubt it not because I think it is impossible to devise such a cipher but because the record which remains as to what Mr. Byrne presented to me about 32 years ago shows that I then believed his cipher system susceptible of solution if employed for practical purposes. I still believe this to be true of Mr. Byrne's invention but I am in no position to prove my contention, nor do I wish to, even with the $5,000 bait hung in front of my eyes."

One might suspect that Friedman knew more than he was telling here, i.e. that he already foresaw a method to successfully cryptanalyze a Chaociphered message. It is reasonable to believe that Friedman, based upon Byrne's presentation, knowledge of the algorithm, and the time he had the Chaocipher "machine" at his personal disposal, created his own series of enciphered, in-depth challenge messages to test the system's security. Considered with his repeated and ultimately futile efforts to have Byrne submit the requisite material samples for study (in line with any cipher-review requests made to the military), this suggests he had not yet found a solution.

We also have, in the above passage, Friedman's passing reference to "*the record which remains as to what Mr. Byrne presented to me…*". It would be surprising if Friedman had *not* written a report on Chaocipher following his meeting with Byrne. Recent requests under the Freedom of Information Act to release all Chaocipher-related materials in the possession of the government and its affiliated organizations, however, have not brought forth any such report [35]. Assuming it exists, might it still remain classified?

Given Byrne's persistence through the years, Friedman would surely have informed Byrne if any solution had been found -- unless the Chaocipher was found to be so secure that the government adopted it in secret. As no such revelation has come to light (or been declassified), it is reasonable to conclude that, in Friedman's time, the Chaocipher remained unbroken.

14. "… if every person on earth were to encipher the same message, say for instance, this paragraph of which this sentence is a part, no two of the resultant encipherments would be alike."

The recent revelation of the Chaocipher algorithm provides the opportunity to verify this assertion. When we hold Byrne to his exact words, this assertion is false. If two persons, using the same starting plaintext and ciphertext alphabets, began enciphering the same plaintext message, they would indeed arrive at the identical ciphertext. Byrne's assertion, though, makes clear he understood that the probability of this ever occurring would be extremely remote. The number of *single* alphabet permutations is 26! (26x25… x2x1), which equals:

403,291,461,126,605,635,584,000,000

That's over 403 septillion alphabet permutations [36]. As Byrne knew, this is a total that far exceeds the number of living persons on earth. Considering Chaocipher requires 2 distinct alphabets (one each for plaintext and ciphertext), this equates to 26! ^ 2 possible starting enciphering permutations, equaling:

162,644,002,617,632,464,507,038,883,409,628,607,021,056,000,000,000,000.

Time will tell whether two isologs (i.e., two enciphered messages with identical underlying plaintexts but created with different keys) can be leveraged to successfully decipher the messages.

SL-277

"When I constructed my cigar-box model in 1918, I had in mind only the construction of a model on which I could demonstrate a principle. My cousin Mary Fleming was charmed with the resultant "toy" – it looked so simple and colorful; and when I told her the purpose for which it was intended and explained its operation, she was entranced with the idea which she grasped quickly and clearly. And very earnestly she said to me, "That will surely bring you a Nobel Prize." At the time all I replied was, "Well it certainly is a strange that thing that, being so simple as it is, no one ever thought of it before."

Within this paragraph is Byrne's next assertion:

15. "… it certainly is a strange thing that, being so simple as it is, no one ever thought of it before."

This is a speculative assertion, one that cannot be quantified. Consequently, a conclusion regarding its veracity cannot be made. On the surface, it reads innocuously enough, and Byrne must have thought it self-evident. Previous analysis in this paper has touched upon the "so simple" aspect (see Assertion #3) as well as the "no one ever thought of it before" angle (see Assertions #6–#9). What's new, then, is Byrne's labeling of "strange", and we may ponder if Byrne's assertion carries any validity. In 1989, when John Byrne revealed the algorithm to Louis Kruh and Professor Cipher Deavours, they commented in their 1990 Cryptologia article:

"They [Kruh and Deavours] were quickly impressed with its simplicity, ease of operation and security."

Considering the concerted efforts of many researchers and programmers between 1990 and the 2010 publication of the algorithm (many of which are documented at the Chaocipher Clearing House [37]) , as well as the speculation derived from those efforts of how Chaocipher might work, the actual algorithm does appear to be a far less complex system than that envisioned by the cryptographic community. But is it "strange" that it was not until Byrne that anyone thought of it?

The gains in human knowledge and discovery, when perceived over the long term, have progressed in an exponential upward curve. Foundational learnings provide the basis for incremental growth, after which it in turn becomes the new foundation. At times, there are "great leaps forward", the result of inspiration, in-depth research, or perhaps an epiphany. In the cryptographic history of substitution ciphers, its foundation begins with "simple" encipherment models such as the Caesar shift. Centuries later, polyalphabetic substitution methods such as the Vigenere cipher were discovered, a great leap forward relative to Caesar. Byrne's discovery of the Chaocipher algorithm, a method of "dynamic substitution", would seem a logical progression in the development of substitution ciphers [38]. While it's a "simple" system by way of operation, conceptually it is another "great leap forward" and does not necessarily mean someone should have "thought of it before". Byrne was simply the right person, at the right time, who had both the inspiration (he sought to find such an unbreakable cipher) and flash of genius (he recognized and developed the algorithm for its enciphering strength) to bring the Chaocipher to light.

SL-282

16. "I assert and claim that the publication of the plain text of a trillion documents enciphered by my cipher system would not be of the least use or assistance to anyone attempting to cryptanalyze the cipher product of my system."

We noted in the analysis of Assertion #14 that each of the two Algorithm alphabets (left and right/plaintext and ciphertext) had a possible letter mixing of 26!, a number far greater than one trillion. Yet in Assertion #16, Byrne's concern pertains to "documents", not specific words or letters, i.e. the "trillion documents' would contain countless more encipherment examples for a cryptanalyst to reference. Byrne certainly had no direct, empirical evidence to support his claim; the "Silent Years" challenge only contains four distinct "Exhibits" running 22 pages (SL-285 to 307). Consequently, his claim is not just confident speculation, but may even be considered the hyperbole of someone unfamiliar with the art of cryptanalysis.

Over a period of more than 30 years, Byrne made repeated entreaties to William Friedman to solve his Chaocipher challenge. Friedman, perhaps the most accomplished cryptanalyst of his time, provided Byrne the opportunity to submit a series of encryption examples (no different a request than what any other cipher inventor would have been asked); Byrne never did so. As it relates to Assertion #16, Byrne betrayed his own confidence in Chaocipher – was he concerned providing additional "documents" to a learned cryptanalyst would reveal a weakness in Chaocipher? Further research into Byrne's papers donated to the NCM may one day help elucidate an answer.

SL-283

17. "I call the fourth exhibit reproduced "A Glimpse of Chaos"… this encipherment is distinguished from the other three in that it bears within itself full and complete instructions to an initiate for its decipherment."

With the recent donation of the Byrne archives to the NCM, this assertion can at last be verified as true. Byrne indeed had a method for hiding such instructions in the preamble of his ciphertext. For Exhibit #4, his method may be read – as documented by Byrne himself – in the article linked to here:

http://www.nsa.gov/about/_files/cryptologic_heritage/museum/library/macarthur_speech.pdf

A forthcoming paper by Moshe Rubin, "Chaocipher Revealed: Deciphering Exhibit #4 in "Silent Years" ", will also discuss this method in greater detail and will be found at The Chaocipher Clearing House.

SL-284

"One final plea I make to all my readers in regard to these dozen or so re-enciphered words in exhibit four: Please do not send me guesses – they will do you no good. Chaociphering is not guesswork. There never was – and there never will be – anything requiring a higher degree of exactitude and truth."

18. "Chaociphering is not guesswork."

As can be seen from its contextual paragraph, Byrne's intent was to state that deciphering a Chaociphered message could not be done through random, or haphazard, guesses. The historical record since publication of "Silent Years" Exhibit #4 supports his claim, i.e. nobody was able to successfully decipher the twelve re-enciphered words until Byrne's private notes on his encipherment key & method became public (see Assertion #17 link above).

Statistically, like winning the lottery, there is in fact a single "guess" that one could make about any enciphered message that would be the correct plaintext translation. The twelve re-enciphered words in Exhibit #4 total 93 characters. If the odds of correctly guessing each individual character is 26 to 1, the odds of correctly guessing all 93 characters is 26 ^ 93 (26x26…x26) which equates to the astronomical odds of:

391,310,373,715,552,665,742,477,550,866,564,009,204,326,841,496,617,966,930,170,284,865,930,067,072,853,095,210,579,911,876,356,362,898,555,145,718,823,786,006,497,854,488,576 to 1.

One might argue that if a decipherer were confident of certain "beginning of words or phrases", random chance would not be at work for later letters in the words or phrases, hence greatly lessening the stated odds. Yet with Byrne's method, a decipherer might never know for certain if his "guess" as regards a Chaociphered word or phrase would be correct unless verified by either the encipherer or intended recipient of the message.

19. "There never was – and there never will be -- anything requiring a higher degree of exactitude and truth."

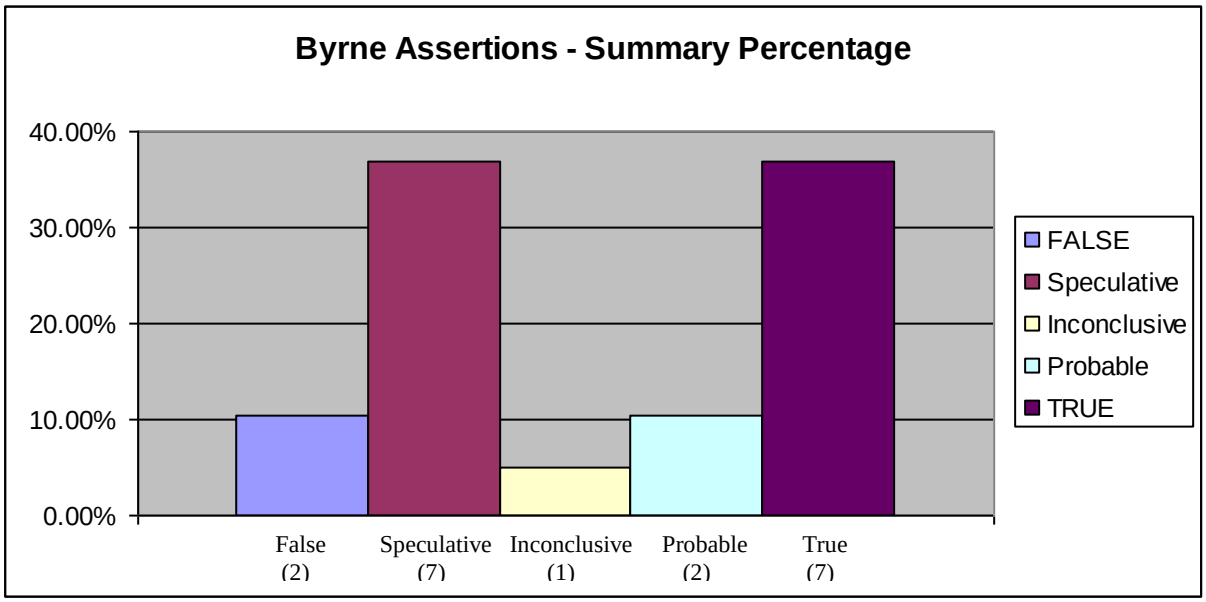
Considering this sentence in the context of its paragraph, it (like Assertion #18) pertains to the act of deciphering a Chaociphered message. It may also refer to the act of enciphering the plaintext. As a flourish to Chapter 21 it's a fitting ending but, as a verifiable statement of truth, it falls short of its claim. Brain surgery, rocket science, and countless other endeavors have extremely high degrees of exactitude and truth; some might argue there is no room for error in these either (as Byrne suggests is the case with Chaocipher). Whether these are equal, or higher, endeavors when compared to Chaocipher is speculative. For Byrne to state "there never will be" anything higher is presumptive and, like many other assertions in Chapter 21, without empirical evidence.

SUMMARY

This paper has examined 19 of Byrne's assertions made throughout Chapter 21 of "Silent Years". Analysis and direct evidence have been used to assign one or more of the following conclusions to each: True, Probable, Inconclusive, Speculative, and False.

	ASSERTION	**CONCLUSION**
1	*"... my method for achieving the complete annihilation of order and design in written language is more noteworthy than the method for the disruption of the atom..."*	**Speculative**
2	*"... the complete annihilation of order and design in written language..."*	**True**
3	*"... my method for splitting the word is so simple that it could be performed by any normal ten-year-old school child..."*	**Probable**
4	*"... splitting the word..."*	**False**
5	*"... unlike any other process of explosion or disruption, my method of disrupting the written words is identical and simultaneous with the complete restoration of order and design in the same written words."*	**True – for its time**
6	*"... I discovered something which was just as accessible to Poe as it was to me."*	**True**
7	*"The ancient Egyptians and Babylonians could have been completely familiar with the principle..."*	**True**
8	*"... a fact which is readily deducible from a treatise on mathematics written by Hero of Alexandria in the second century B.C."*	**Inconclusive**
9	*"... during the past two thousand years and more anyone could have had access to my method for the chaotification of language."*	**True**
10	*The first Chaocipher machine fit into an empty cigar box (which held 50 small Havana cigars)*	**Probable**
11	*"... a cipher which would be materially and mathematically indecipherable..."*	**Speculative; True as of this paper's writing**
12	*"... any person, anywhere, writing in any language, could by applying my principle and using my device transcribe his written words into a script which would be absolutely indecipherable by anyone except the persons for whom the message is intended..."*	**Speculative, though functionally True**
13	*"... possession of my device together with knowledge of the general principle involved, would not enable any person to decipher any message whatever written by anyone else and not intended for him."*	**Speculative; True as of this paper's writing**
14	*"... if every person on earth were to encipher the same message, say for instance, this paragraph of which this sentence is a part, no two of the resultant encipherments would be alike."*	**False, though Probable in real world scenario**
15	*... it certainly is a strange thing that, being so simple as it is, no one ever thought of it before."*	**Speculative**
16	*"I assert and claim that the publication of the plain text of a trillion documents enciphered by my cipher system would not be of the least use or assistance to anyone attempting to cryptanalyze the cipher product of my system"*	**Speculative (and Hyperbole)**
17	*"I call the fourth exhibit reproduced "A Glimpse of Chaos"... this encipherment is distinguished from the other three in that it bears within itself full and complete instructions to an initiate for its decipherment."*	**True**
18	*"Chaociphering is not guesswork."*	**True**
19	*"There never was – and there never will be anything requiring a higher degree of exactitude and truth."*	**Speculative**

The final tally (percentages rounded = 99.6%):



Byrne's "True" batting average would be considerably higher if those "Speculative" assertions could be proven. Whether by choice, lack of knowledge, or lack of research capacity, he did not provide evidence in "Silent Years" to support the "Speculative" assertions, rather basing them on intangible sources such as instinct, confidence, and pride – or on information he calculated but chose to keep private (like the algorithm itself). Future research may well prove them to be true -- or not.

Based on the newfound knowledge of the algorithm, the two "False" assertions are of interest as each seems "obviously" so. Given the exactitude Byrne exhibits in most all-things Chaocipher, it is surprising he'd choose explicit phrases such as "splitting the word" and "no two would be alike" which leave no wiggle room for interpretation or exception. When Byrne held his privileged knowledge of Chaocipher, his readers and cryptanalysts could not prove (or disprove) him due to lacking the knowledge of the algorithm. We may wonder if he intended to mislead his readers, or he simply never thought to double-check himself on these assertions.

The two "Probable" assertions may in fact be "True"; while one cannot be proven (Assertion #3), the other (Assertion #10) lacks only reliable source verification.

CONCLUSION

Of the 19 examined assertions, just 2 proved to be false, and then only due to linguistic or mathematical technicalities. Based on this, it is highly doubtful Byrne set out to intentionally mislead his readers when writing "Silent Years"- Chapter 21. The "speculative" assertions remain most tantalizing, as they provide fodder for both what is most remarkable about Byrne, as well as what's most frustrating. Remarkable, as his personal belief in his discovery remained unshaken until the end of his life. With the recent publication of the algorithm, the cryptographic community can fully appreciate the amazing accomplishments of this true dilettante. Frustrating, in that Byrne proved to be his own worst enemy in attaining the recognition and serious consideration he so desperately sought for nearly 40 years. With new information about the algorithm and Byrne's methods now available, a re-evaluation of his discovery and intentions may elevate, or diminish, his rightful place in the pantheon of cipher-makers.

Acknowledgements

I would like to thank Moshe Rubin for inspiring the idea for this paper, his consistent input throughout its creation, and his insightful feedback while helping it to take shape into a publishable document.

Thanks also to National Cryptologic Museum, and Senior Librarian Rene Stein, for their generous assistance in providing both permission to publish, and link to, Byrne-archived photographic & documented content, and in graciously responding to questions regarding the donated Byrne materials.

As noted in the opening of this paper, a great debt is acknowledged to the late Greg Mellen for his seminal research and published findings in "J.F. Byrne and the Chaocipher: A Work in Progress".

References

[1] Chapter 21 of "Silent Years" can be seen at: http://www.mountainvistasoft.com/chaocipher/Silent-Years-Chapter-21-Chaocipher.pdf. Retrieved 10/12/2010.

[2] The Chaocipher Clearing House, 2010. "Chaocipher Revealed: The Algorithm" by Moshe Rubin can be seen at: http://www.mountainvistasoft.com/chaocipher/ActualChaocipher/Chaocipher-Revealed-Algorithm.pdf. Retrieved 10/12/2010.

[3] The Chaocipher Clearing House, 2010. "Chaocipher Revealed: Deciphering Exhibit #1 in "Silent Years" " by Moshe Rubin can be seen at: http://www.mountainvistasoft.com/chaocipher/ActualChaocipher/Chaocipher-Revealed-Deciphering-Exhibit-1.pdf. Retrieved 10/12/2010.

[4] The Chaocipher Clearing House, 2010. "Chaocipher Revealed: Deciphering Exhibit #4 in "Silent Years" ", will eventually be published at The Chaocipher Clearing House: http://www.mountainvistasoft.com/chaocipher/

[5] Greg Mellen's article "J.F. Byrne and the Chaocipher: A Work in Progress" was published in Cryptologia 1979 Volume 3, Issue 3. Copies may be ordered at http://www.informaworld.com/smpp/title~content=g741902804~db=all

[6] Byrne's February 17th, 1957 letter to William F. Friedman may be read at: http://www.mountainvistasoft.com/chaocipher/byrne-correspondences/GCMRF-1957-02-17.html. Retrieved 10/12/2010.

[7] Wikipedia article about Ernest Rutherford may be found at: http://en.wikipedia.org/wiki/Ernest_Rutherford. Retrieved 10/12/2010.

[8] Readers of this paper may also wish to consider that the scanned copy of Chapter 21 of "Silent Years" (See Reference [1] above) was Albert Einstein's personal copy. While he marked/highlighted many paragraphs in this Chapter he found of interest, it is clear that Byrne's assertions of Chaocipher vis-à-vis the splitting of the atom did not merit any such markings.

[9] This scanned photo, of a document donated in May, 2010 by the Byrne family, is kindly provided with permission by the National Cryptologic Museum Foundation.

[10] See "Progress Report #1" and "Progress Report #3", authored by Moshe Rubin, 2009 at The Chaocipher Clearinghouse: http://www.mountainvistasoft.com/chaocipher/. Retrieved 10/12/2010. See also the Greg Mellen article noted in Reference [5].

[11] Letter from Byrne to Capt. John Irish – posting on NCM website forthcoming. A link in this reference section will be updated at that time.

[12] John Byrne, Cipher A. Deavours and Louis Kruh. "Chaocipher enters the computer age when its method is disclosed to Cryptologia editors". Cryptologia, 14(3): 193-197. Can be ordered at http://www.informaworld.com/smpp/content~db=jour~content=a741902642. Retrieved 10/12/2010.

[13] The National Cryptographic Museum has kindly provided a direct link to a scanned copy of Byrne's original pamphlet "Chaocipher – The Ultimate Elusion": http://www.nsa.gov/about/_files/cryptologic_heritage/museum/library/chaocipher.pdf

[14] Letter to Greg Mellen from John Byrne – posting on NCM website forthcoming. A link in this reference section will be updated at that time.

[15] Wikipedia article regarding Delastelle may be found at: http://en.wikipedia.org/wiki/Delastelle. Further links to bifid, trifid, and four-square ciphers may be found here as well. Retrieved 10/12/2010.

[16] Ritter's article "Substitution Cipher with Pseudo-Random Shuffling: The Dynamic Substitution Combiner" may be read at: http://www.ciphersbyritter.com/ARTS/DYNSUB2.HTM. Retrieved 10/12/2010.

[17] Poe's short story "The Gold Bug" is published in many different books, including http://www.amazon.com/Gold-Bug-Other-Tales-Thrift-Editions/dp/0486268756/ref=sr_1_1?ie=UTF8&s=books&qid=1283382541&sr=8-1

[18] Try as I might, I could not find a current reference to an essay, article, or book by Poe titled "Cryptography". In a 1937 article by William Friedman, entitled "Edgar Allan Poe, Cryptographer", he writes that the only known cryptographic writings of Poe are "Gold Bug" and four articles in "The Graham's Magazine" entitled "A Few Words on Secret Writing". It is possible it is to one of these articles Byrne was referring, but I am unable to confirm. The Friedman article may be seen here): http://www.mountainvistasoft.com/chaocipher/ActualChaocipher/Edgar-Allan-Poe-Cryptographer.pdf Retrieved 11/15/10.

[19] There are many references relating Poe's limited cryptanalyst skills. See David Kahn's "The Code Breakers" Pages 783-793 for one http://www.amazon.com/Codebreakers-Comprehensive-History-Communication-Internet/dp/0684831309/ref=sr_1_1?s=books&ie=UTF8&qid=1287555186&sr=1-1 , or "Edgar Allan Poe and Cryptography" by R. Morelli which may be seen at: http://www.cs.trincoll.edu/~crypto/historical/poe.html. Retrieved 10/12/2010.

[20] Wikipedia article on "Hero of Alexandria" may be seen at: http://en.wikipedia.org/wiki/Hero_of_alexandria. Retrieved 10/12/2010.

[21] An overview of Hero's works may be seen at: http://www.bookrags.com/biography/hero-of-alexandria-wom/. Retrieved 10/12/2010.

[22] The Blueprint photos are courtesy of the National Cryptographic Museum. While one photo was originally published at http://www.cryptologicfoundation.org/content/Direct-Museum-Support/images/charo3.jpg, Sr. Librarian Rene Stein has made the series of 5 photos available for this article: http://www.nsa.gov/about/_files/cryptologic_heritage/museum/library/chaocipher_blueprints.pdf

[23] See Tim Harding's article "Masters and patzers in the biographical dictionaries" for an interesting overview of the Byrne/Cranly chess connection, http://www.chesscafe.com/text/kibitz165.pdf (Page 6). Retrieved 10/12/2010.

[24] Chapter 5 of "Silent Years" can be seen at: http://www.mountainvistasoft.com/chaocipher/Silent-Years-Chapter-5-Chaocipher.pdf. Retrieved 11/14/10.

[25] The National Cryptographic Museum's article regarding the Byrne material donation, including the published photograph of the Chaocipher cipher wheels mock-up, may be found at: http://www.cryptologicfoundation.org/content/Direct-Museum-Support/recentacquisitions.shtml#Chaocipher. Retrieved 10/12/2010.

[26] Oxford Dictionary Online's definition of "materially" may be found at: http://oxforddictionaries.com/view/entry/m_en_us1266483#m_en_us1266483. Retrieved 10/12/2010.

[27] Wikipedia article regarding Norbert Wiener may be found at: http://en.wikipedia.org/wiki/Norbert_Wiener. Retrieved 10/12/2010.

[28] Answers.com article regarding Cyrillic script may be found at: http://www.answers.com/topic/cyrillic-alphabet. Retrieved 10/12/2010.

[29] The National Cryptographic Museum has kindly provided a direct link to a scanned copy of the document titled "Preliminary Instructions for Chaocipher II" by John Byrne's nephew at: http://www.nsa.gov/about/_files/cryptologic_heritage/museum/library/instructions_for_chaocipher.pdf. Presently, I have not been able to confirm this gentleman's name. If done so at a future date, this reference will be updated accordingly to give proper credit.

[30] This implementation may be seen at: http://paulmakowski.wordpress.com/2010/07/07/chaocipher-now-with-ascii-support/. Retrieved 10/12/2010.

[31] Wikipedia article on Kerckhoff may be seen at: http://en.wikipedia.org/wiki/Kerckhoffs%27_principle. Retrieved 10/12/2010.

[32] Wikipedia article on William F. Friedman may be seen at: http://en.wikipedia.org/wiki/William_F._Friedman. Retrieved 10/12/2010.

[33] Beyond the letter excerpts Byrne himself provides in "Silent Years", additional correspondence between Byrne and Friedman, from 1942 to 1957, may be read at The Chaocipher Clearing House at: http://www.mountainvistasoft.com/chaocipher/byrne-correspondences/index.html. Retrieved 10/12/2010.

[34] A copy of Friedman's 1954 prepared speech may be found at The Chaocipher Clearing House at: http://www.mountainvistasoft.com/chaocipher/byrne-correspondences/GCMRF-1954-03-13.html. Retrieved 10/12/2010.

[35] See Progress Report #10 at The Chaocipher Clearing House for the result of a FOIA request for Chaocipher information: http://www.mountainvistasoft.com/chaocipher/chaocipher-010.htm. Retrieved 10/12/2010.

[36] There are many Big Number Calculators available online; for this paper, I used the one found at: http://world.std.com/~reinhold/BigNumCalc.html. Retrieved 10/12/2010.

[37] See the many Progress Reports and article links under the heading "Ongoing Research and Updates". The major contributors include Moshe Rubin, Jeff Hill, and Mike Cowan. http://www.mountainvistasoft.com/chaocipher/. Retrieved 10/12/2010.

[38] A thorough summary of the Caesar substitution and Vigenere ciphers may be found in numerous books on ciphers including Kahn's "The Code Breakers" (See reference [19]) and Simon Singh's "The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography": http://www.amazon.com/Code-Book-Science-Secrecy-Cryptography/dp/0385495323/ref=sr_1_1?ie=UTF8&s=books&qid=1283387136&sr=8-1