A Feasible Mechanism for the 1937 Byrne Cryptograph

ADDRESS: Lincoln, Nebraska 68521

ABSTRACT: A study of electro-mechanical resources available to John F. Byrne for the construction of his 1937 Chaocipher Cryptograph.

KEYWORDS: Chaocipher, John F. Byrne, Electro-Mechanical Cryptograph

Introduction

In June, 1919, John F. Byrne gave a three-hour presentation to patent attorney Marcellus Bailey during which the principle of Chaocipher was demonstrated using a "cigar box device" that Byrne had constructed in 1918. He was advised by Bailey not to have that "toy" patented, but to proceed with plans to have professional blueprints drawn up for a "readily operable machine". The blueprints were completed by January 20, 1920, as noted in a letter from Bailey to Byrne. [2, pp. 266-267] Byrne then took the blueprints to several machine-makers and requested bids to determine the cost of constructing this machine, but, due to cost estimates of $5,000 to $20,000, the machine was never built. To put this into perspective, these costs estimates would range from $54,000 to $216,000 in 2009 dollars. [8]

In 1937, Byrne returned to the challenge of constructing a "readily operable machine", motivated by an item that had appeared in newspapers in the Spring of that year. According to the news item, the Navy Department was seeking congressional funding for a new system of cryptography which would be used to protect fleet communications. In a letter dated November 18, 1937, Byrne described his device and system to the Navy Department and enclosed his document, *Chaocipher—The Ultimate Elusion*, as an example of the ciphertext that this device could produce. [2, p. 277] The Navy initially found this material interesting and invited Byrne to demonstrate his system in Washington on May 3, 1938. That interest, however, did not last more than a few minutes once Byrne had arrived to give his demonstration. The meeting ended abruptly and Byrne was advised to take his device and system "either to the War Department or to the State Department". [2, p. 279] The following day, May 4, 1938, the Navy Department accepted an electro-mechanical cipher machine designed by inventors Anderson and Seiler. [11]

By 1937, electro-mechanical devices were commonplace technology and Byrne had witnessed the evolving state of this technology for eighteen years following his presentation to Marcellus Bailey. Therefore, the question naturally arises, did Byrne build an electro-mechanical cryptograph in 1937? If so, it could not have been very impressive to look at compared to the machine designed by inventors Anderson and Seiler, judging from the Navy's response to it. However, appearances aside, could such a device have been used to encipher Byrne's Exhibit 1? One purpose of the current study is to determine whether there were technological resources available in 1937 for the design and construction of an electro-mechanical cipher machine capable of producing the statistics observed in Exhibit 1. [6, p.4-5] A second purpose is to determine whether such a device could have been built by Byrne himself, working at home during the Summer and Fall of 1937.

Byrne's Law

As recounted in *Chaocipher: Analysis and Models*, William F. Friedman was contacted by Byrne in 1922 and again in 1942 about the indecipherability of Chaocipher with results that were both disappointing and frustrating for Byrne. [6, pp.1-3] In 1957, a further exchange of letters took place between Byrne and Friedman which, judging from the context, was initiated when Byrne wrote to express interest in a new book that was due to be published later that year by Friedman. However, in his letter of February 17, 1957, Byrne also seized the opportunity to once again challenge Friedman regarding Chaocipher: "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?". [3] On March 3, 1957, Friedman replied, "It may well be that your system is excellent - I won't say it is invincible**,** as you seem to think it is." [4] In the same letter, Friedman's final response to Byrne on the subject of Chaocipher is worth noting: "What makes you think you have done something that they [experienced and well-trained engineers] have not thought of or have over-looked?" If Byrne provided an answer to this question, it is not, unfortunately, among Friedman's papers at the George C. Marshall Research Library.

Given Byrne's relentless obsession with Chaocipher, one might reasonably ask, "What did Byrne know, or think that he knew, about indecipherability?" What, in other words, was the principle of Chaocipher that he so fervently believed in? In most contexts, "principle" simply means "method". The "principle of the machine" means the "method by which the machine operates". For example, Parker Hitt [7], in his August 3, 1921, letter to Byrne said, "As to *the principle of the machine* [emphasis added], it is undoubtedly a most ingenious and effective device." [2, p.273] Byrne dismissed this comment by saying, "it was clear to me that he [Hitt] had not at all fully apprehended the principle of my 'machine', as he called it." Clearly there was both a 'principle' and a 'machine', but in Byrne's mind the machine, no matter how it operated, was solely for the purpose of "demonstrating this principle". [2, p.266]

For Byrne the word "principle", when applied to Chaocipher, has the force of natural law. The following statement from *Silent Years* provides an expression of this law as Byrne understood it: "It should be obvious to anyone...that 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" [2, p. 270] Friedman's choice of the word "invincible" in his March 3, 1957, response to Byrne suggests the following concise expression of Byrne's fundamental belief:

> Byrne's Law: Cipher that is materially and mathematically indistinguishable from characters drawn at random is Invincible

This law is not true without qualification, as of course Friedman well understood. No matter how indistinguishable ciphertext might be from randomly drawn characters, there can still be hidden structure in the machine itself that can be exploited once the principle of the machine becomes known, Byrne's claim to the contrary not withstanding. [2, p.266]

At another level, it is nevertheless clear that there is also a "method" of Chaocipher. Byrne describes his accomplishment by saying, "First, I formulated a principle for the development of a cipher which would be materially and mathematically indecipherable, and, second, I built the little model, of which I have spoken, for the purpose of demonstrating this principle." [2, pp.265-266] He provides a clue for the recovery of this method by placing it in the context of "Egyptian and Babylonians" who "could have been completely familiar with the principle". [2, p.265] Research suggests that the principle to which Byrne refers is in fact the general principle of iteration, where the output of one step becomes the input to the next. [6, p.2] If this is correct, then Chaocipher can be understood as a specific instance of the general principle of iteration, one with a defined method for generating output and then using this as input step after step. It is easy to see why Byrne might have considered a method of this type to be invincible. If Chaocipher uses a specific key to set the initial machine state and at each step the method uses the current plaintext letter, or some combination of plaintext and ciphertext letters, to generate the next machine state, then it might have seemed to Byrne that so long as the specific key remained a secret to everyone except an initiate, then none but that initiate could decipher the message. The final truth of this would depend, in Byrne's mind, on whether or not the cipher conformed to Byrne's Law by being indistinguishable from randomly drawn characters. Byrne, of course, would have compiled tables of letter frequencies to assure himself that Chaocipher met the test of mathematical indecipherability. Furthermore, the first 100 lines of Exhibit 1 were no doubt also a part of this test. These were likely intended to demonstrate that Chaocipher is materially indecipherable, first of all, by demonstrating that all repetitions in the plaintext have been concealed and, secondly, by demonstrating that no row of ciphertext repeats in the first 100 rows.

Design Challenges

The goal of an earlier study in 1989 [5] was to verify Byrne's claim that a cryptograph so small that it could be constructed in a cigar box could nevertheless produce cipher indistinguishable from randomly generated characters. That study described a cryptograph which was essentially a Wheatstone cryptograph equipped with segmented gears, similar to those used on the Kryha cryptograph in 1922. The Wheatstone component had a revolving key selector that made possible the use of either plaintext or ciphertext as a form of autokey cipher, while the segmented gears had an aperiodic component that insured that the same key did not always produce the same PT/CT encryption. While the cryptograph described in the 1989 study resolved a number of issues relating to Byrne's 1918 device, this all fell by the wayside after the discovery in 1994 that a statistical pattern was present in Exhibit 1 which could not be explained by the proposed model. [6, pp. 4-5] However, certain ideas were developed in the 1989 study that continue to have relevance today. As stated in the postscript to that study, "the device should first have a stepping mechanism that is mechanically driven by referencing either the plaintext or the ciphertext and, secondly, the stepping mechanism itself should have variable step sizes." [5, p. 4]

It has long been speculated that the ciphertext generated by the Byrne cryptograph depends in some way on a form of autokey in which either the plaintext or the ciphertext determines the next key. [5, p.3] That would mean that Chaocipher is an iterative method in the sense that the output of one step becomes the input of the next, a conjecture that finds support in the following statement by Byrne: "Let me make it explicit here that anyone who *really can* identify and decipher the dozen or so specified words [in lines 34 and 35 of Exhibit 4], must, *ipso facto*, be able to decipher the whole of this exhibit, because it is all of a piece." [2, p. 284] This suggests that to decipher Exhibit 4 (and presumably each of the Byrne Exhibits) an initiate must start at the beginning of the cipher and generate information after each decipherment that provides a key for the next decipherment.

In summary, the design challenges facing Byrne in 1937, if he did indeed build a simple electro-mechanical device to demonstrate his principle, were the following: (1) generate electrical signals using PT/CT disk alignment, (2) use these same electrical signals to generate variable step sizes and step frequencies, (3) develop a stepping mechanism, and (4) design a control circuit for the stepping mechanism that takes as input the electrical signals at each step and generates information as output that determines the key for the next step.

Design Challenge 1: Generating Electrical Signals using PT/CT Disk Alignment

Assuming that we have correctly deconstructed Byrne's statements, the first challenge for Byrne in designing an electro-mechanical cryptograph would have been to convert the signals designated by the plaintext and/or the ciphertext letters into electrical signals that would cause the cryptograph to move from one machine state to the next. This need not have been a difficult challenge, since it is safe to assume that Byrne would have known how to operate a conventional cipher disk and would have been equally familiar with the slightly more complex Wheatstone cryptograph. In either case, the alignment of one disk relative to another would naturally suggest that the alignment of the two disks could be used to signal the next key, provided that electrical contacts were attached to one or both disks.

Although cipher disks could be used as described, a more effective way to mount the electrical contacts is on a commutator, such as the one shown in Figure 1. The electrical current is routed to the commutator by a sliding contact on its inner ring. The current is then routed to a sliding contact on the outer ring, where only half of the contacts actually receive current. In other words, half of the contacts receive current and are there to complete the electrical circuit, while the other half do not receive current and are there to break the circuit. This produces a series of ON/OFF signals that are routed to the stepping mechanism. For security, the ON/OFF contacts should be randomly distributed on the commutator.

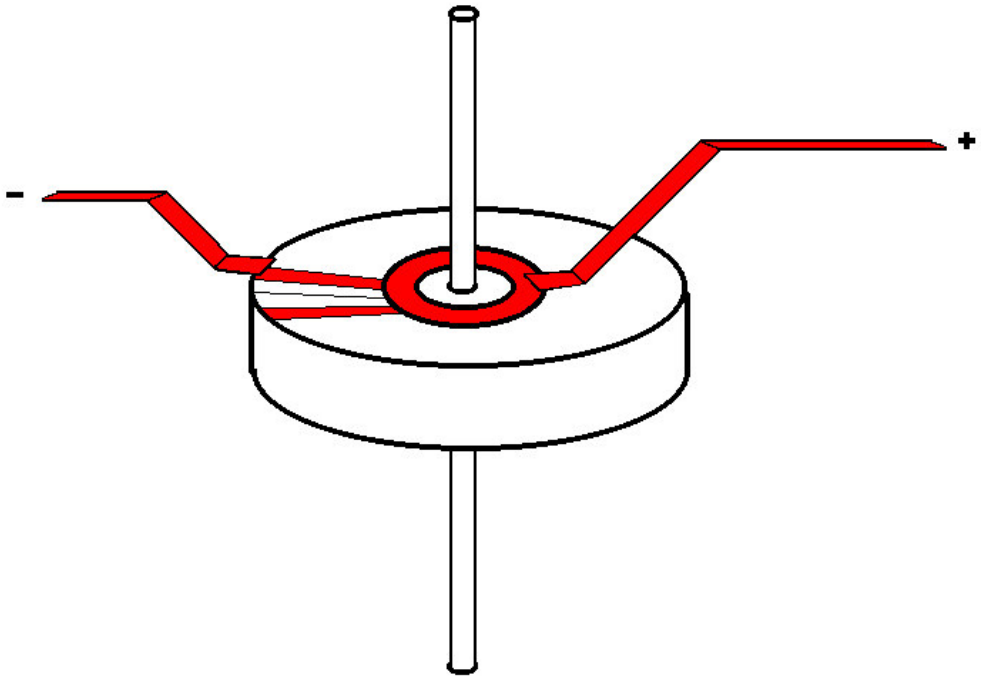

Figure 1. Commutator

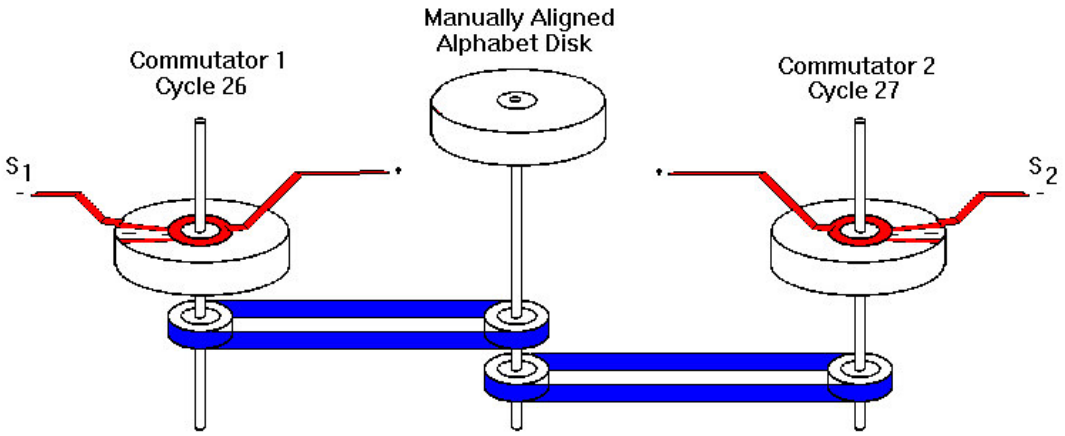

Figure 2. Commutator Drive Mechanism

Two commutator disks would be more effective than one. If there are two commutators, one with 26 contacts and the other with 27 contacts as in Figure 2, this arrangement will have a composite cycle that is 702 steps in length. If the commutators are initially aligned at specified positions, A and B, then the commutators will not return to the same positions in less than 702 steps. This is due to the fact that in order to return to the same positions, one commutator must complete N rotations of 26 steps each and the other must complete M rotations of 27 steps each, and for a repeat to occur 26N must be equal to 27M. In other words:

$$N = (27/26)M$$

The smallest value for M which results in the value of N being a whole number is 26, in which case N equals 27. Consequently, 26N = 26*27 = 27M = 27*26 = 702 steps. As a general rule, if two cycles, C_1 and C_2, are relatively prime, then both cycles will return to the same initial position in $C_1 \times C_2$ steps. This can be extended to any number of cycles, $C_0..C_n$, provided that the factors of each cycle are relatively prime to the factors of all of the other cycles. This has implications for Exhibit 1, where the first line of plaintext repeats 100 times. That first line represents a cycle of 55 steps with factors of 5 and 11. Combined with commutator cycles of 26 and 27 steps, the first row of ciphertext would not repeat in less than 26 x 27 x 5 x 11, or 38,610 steps. Since this is equivalent to 702 rows of repeating plaintext, it is clear that even if there were no other mechanical complexities, two short commutator cycles, one of 26 steps and the other of 27 steps, are sufficient to guarantee that no row of ciphertext in Exhibit 1 repeats in the first 100 rows.

Design Challenge 2: Control of Variable Step Size and Frequency

Using two commutators insures that two independent electrical signals, S_1 and S_2, are available to control the stepping mechanism of our hypothetical Byrne cryptograph. As stated in *Chaocipher: Analysis and Models*, "If we take seriously the possibility that Byrne's cryptograph was electro-mechanical in design, then a logic gate with the required properties is the Half Adder ... A pseudo-random sequence of inputs ... would, by hypothesis, be provided by another component of the device." [6, p. 8] The component of the device that would generate the pseudo-random sequence of inputs would thus consist of the two commutators just described. Commutators 1 and 2 generate signals S_1 and S_2, respectively, where each signal simply specifies whether current is flowing through a particular commutator, or not. Each signal, S_i, controls a relay switch SW_i, as shown in Figure 3. If current is flowing, the signal sent from the commutator is SWITCH ON, otherwise the signal sent is SWITCH OFF.

SW_1 is a Single-Pole, Single-Throw (SPST) switch that is normally aligned with branch A. When S_1 is ON, the electromagnet that controls SW_1 is activated and redirects the circuit to branch B. SW_2 is a Double-Pole, Single-Throw (DPST) switch which is equivalent to two SPDT switches controlled simultaneously by a single electromagnet, thus redirecting the current through one of four possible branches, depending on the alignment of SW_1 and SW_2. As explained in *Chaocipher: Analysis and Models*:

> The simple probabilities derived from [statistical data derived from Exhibit 1], that is ½, ¼, and ¼, suggest other ways to interpret Byrne's stepping method . . . These probabilities arise when a trial has two outcomes, A and B, each having probability ½, and two trials are made simultaneously or in sequence, so that the possible outcomes are AA, AB, BA, or BB. In the context of Chaocipher, this would mean that if AA occurs, then the rotating disk is moved ahead two letters. If either AB or BA occurs, the disk is moved ahead one letter. Finally, if BB occurs, the disk is moved four letters. [6, p. 8]

We are now able to identify outcomes A and B with the signals SWITCH OFF and SWITCH ON, respectively, as shown in Figure 3 and Table 1, with each signal having probability ½.

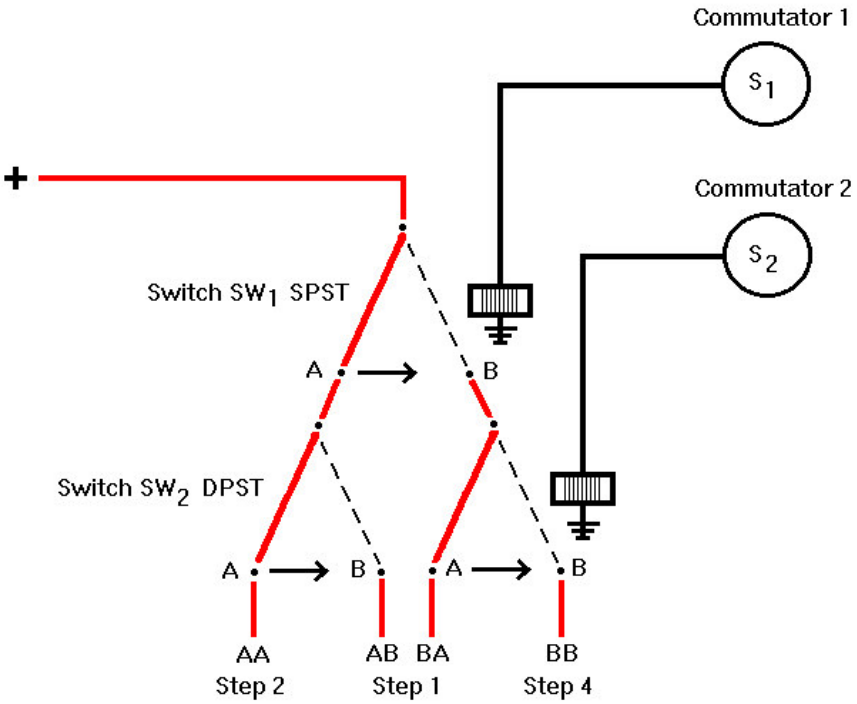

Figure 3. Logic Gate for Step Control Circuit

The Logic Gate in Figure 3 need not be restricted to the specific step sizes given in Table 1, where the signals generated are for steps sizes of 1, 2, and 4 letters. However, one factor that does influence the choice of step sizes is the time required for the machine to move ahead N steps. The greater the value of N, the longer it takes to encipher or decipher a document, so small steps reduce the time required for the process. In that respect, steps sizes of 1, 2, and 3 would have required less processing time than the step sizes that research suggests were actually chosen, that is, step sizes 1, 2, and 4. However, Byrne's choice of steps sizes might have been made for reasons other than efficiency. In *Silent Years*, Byrne takes a great deal of interest in the mystic properties of the number 7, which he identifies with No. 7 Eccles Street, Dublin, where he lived for several years before moving to the Untied States. [2, p.36, pp. 153-54] So, with Byrne as our guide in these matters, it is possible that he chose step sizes of 1, 2, and 4 simply because the sum of these numbers is the mystic number 7.

S_1	S_2	SW_1	SW_2	Signal
0	0	A	A	Step 2
0	1	A	B	Step 1
1	0	B	A	Step 1
1	1	B	B	Step 4

Table 1. Logic Gate with two Inputs, S_1 and S_2, and two Outputs, SW_1 and SW_2

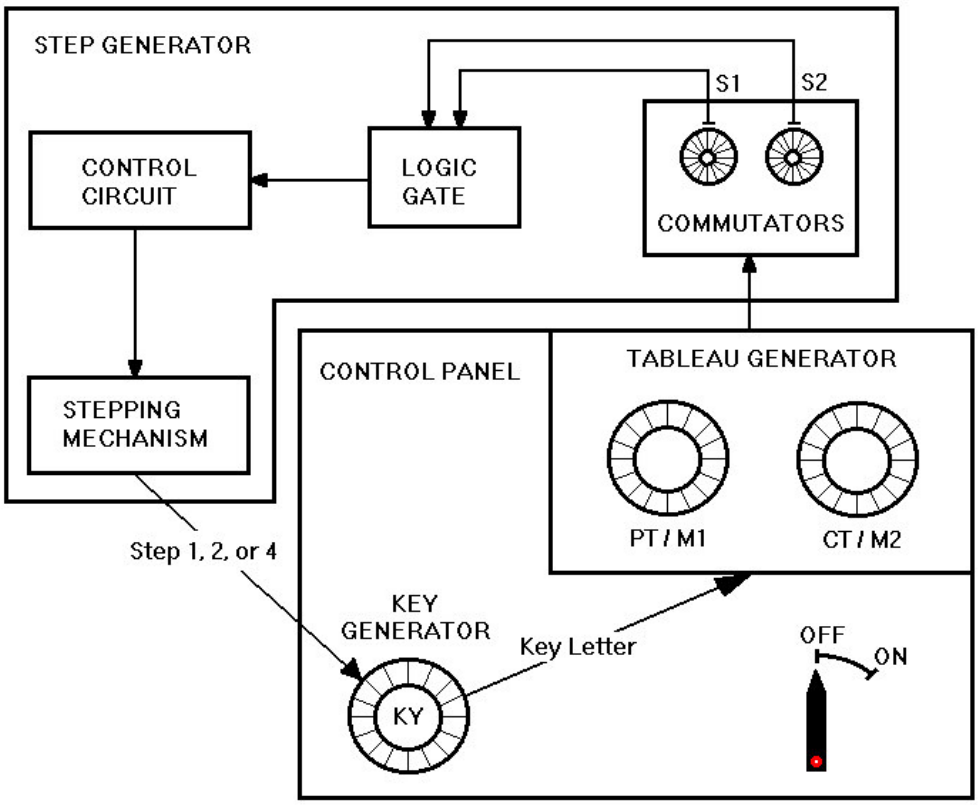

Figure 4. Cryptograph Control System Schematic

In *Chaocipher: Analysis and Models*, it was convenient to break the series of hypothetical C98 cryptographs down into abstract components as an aid to explaining the operation of Byrne's cryptograph:

> The essential components that have so far been developed to explain the operation of Byrne's cryptograph are a step generator, a key generator, and a tableau generator. The step generator has simply been treated as a black box which outputs step requirements of one, two, or four letters with the probabilities derived from analysis of Exhibit 1. The step requirements are transmitted to a key generator which then steps the specified distance to produce the next key. The key letter is transmitted to a tableau generator where it serves to align a CT alphabet with a PT alphabet, either directly as in a conventional cipher disk or indirectly through a pair of revolving half-rotors. [6, p.11]

As shown in the schematic in Figure 4, the Step Generator can now be represented as a pair of Commutators, a Logic Gate which receives electrical signals from the Commutators, and a Control Circuit that activates a Stepping Mechanism which mechanically advances the key generator, KY, by 1, 2, or 4 letters. The key letter is read from the KY disk and then the M1 disk is aligned manually.

The ON/OFF Control Switch on the Control Panel switch is used to turn off current to the Commutators while the M1 disk is being manually realigned. If this is not done, the Commutators will continue to send signals to the Logic Gate as the M1 disk is being turned to a new alignment with the PT disk, resulting in unwanted activation of the Stepping Mechanism.

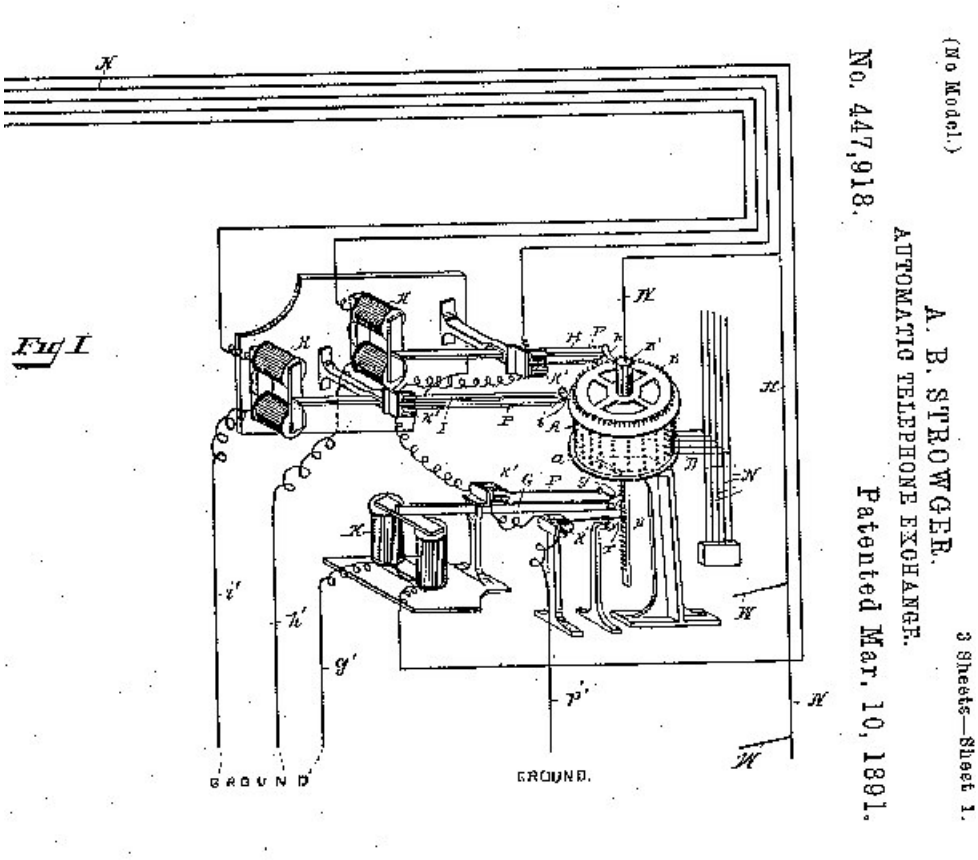

Figure 5. Automatic Telephone Exchange, (Strowger, 1891). US Patent 447,918.

Design Challenge 3: Stepping Mechanism

Various stepping mechanisms were available in 1937, including stepping motors and telephone stepping switches, but a survey of the technology led to an earlier stepping mechanism that was used in the 1891 Strowger Telephone Exchange, a mechanism that provides a simple way to control our hypothetical Byrne cryptograph. The Strowger patent drawing, Figure 5, shows three electro-mechanical pawls that were used to rotate and elevate a canister containing the electrical contacts that provided access to all telephones linked to the exchange. [9]

An electro-mechanical pawl from the Strowger patent is shown in greater detail in Figure 6. When electricity was turned on, an electromagnet pulled the left end of the pawl's arm up, which simultaneously forced the right end of the arm down to advance a notched wheel. To accomplish anything of practical value, electricity had to reach the electromagnet in pulses, with each pulse advancing the wheel by one notch. To implement this, phone service subscribers were issued three digit phone numbers, such as, for example, 837. Phone numbers were "dialed" by pressing each of three push buttons in succession, one for each digit of the destination phone number. For example, 837 would be "dialed" by pressing the first button eight times, the second button three times, and the third button seven times. This sent a series of electrical pulses corresponding to each of the three electrically activated pawls to rotate and/or elevate the canister and make the connection.

At first the Strowger electro-mechanical pawl seems to create more problems than it solves. On the one hand, it provides a simple stepping mechanism that can be used to advance the KY disk of our

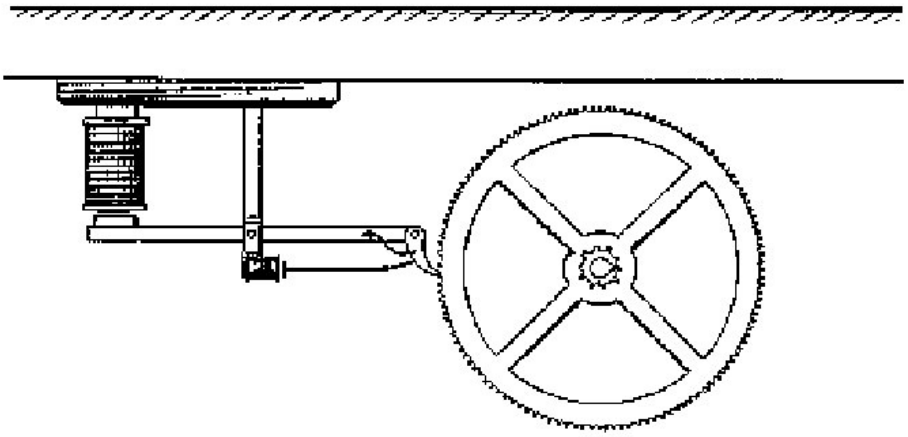

Figure 6. Electro-Mechanical Pawl Stepping Mechanism (Strowger, 1891)

hypothetical cryptograph. On the other hand, it requires that electricity be delivered in pulses to the electromagnet that controls the pawl. The means to achieve this using something other than push buttons was not immediately clear. However, as the survey of 1937 technology continued, a device referred to as a slow-acting relay was discovered in various old patents drawings from the 1920's and 1930's. The device shown in Figure 7, for example, was an improved version that was patented in 1930. [10] The schematic in Figure 8 shows a relay switch in parallel with a capacitor which is described in a 1935 patent application as "the circuit normally used for obtaining time-delay by the slow operation of a relay". [1] The "circuit normally used", or in other words, what is called "prior art", worked in the following way: "When contacts *a* [in Fig. 3 of Figure 8] are closed, condenser CR charges up to the operating voltage for relay B, which then operates." [1] The patent went on to describe an improved version of this device which was the real purpose of the application, but for our hypothetical cryptograph, we rely on the "circuit normally used", which was pre-1935 technology and more likely to have been used by Byrne.

The importance of a slow-acting relay for our analysis is that after a time-delay, the relay can open or close a switch in another circuit. For example, if current begins to flow in two circuits, A and B, at time t_0, and after a time-delay of t seconds, a slow-acting relay in circuit A opens a switch that breaks the current in circuit B, then a short pulse of electricity has been created in circuit B that has a duration of t seconds. This is exactly what is required to control the stepping mechanism of our hypothetical cryptograph.

Design Challenge 4: Stepping Mechanism Control Circuit

To summarize our results so far, a device has been described in which two Commutators deliver electrical signals, S_1 and S_2, to a Logic Gate where these signals determine which of four electrical circuits, AA, AB, BA, or BB will receive current. The circuit that receives current then activates a Control Circuit that transmits one or more electrical pulses to a Stepping Mechanism, which in turn advances the KY disk. What remains to be presented is a detailed description of Control Circuit operation.

The Step 1 Signal, which can be delivered through either circuit AB or circuit BA, as shown in Figure 9, energizes the coil for switch SW_1, which closes that switch. Current then flows through switch SW_2 to the coil that energizes the Pawl arm, thereby causing the KY disk to advance one step. Simultaneously, voltage charges the capacitor in slow relay A. When this capacitor is fully charged, current then flows through the coil for switch SW_2, causing that switch to open, which ends the pulse of electricity to the Pawl coil. The Pawl then returns to its initial position, ready for the next pulse.

1,922,089

SLOW ACTING RELAY

Filed Sept. 6, 1930

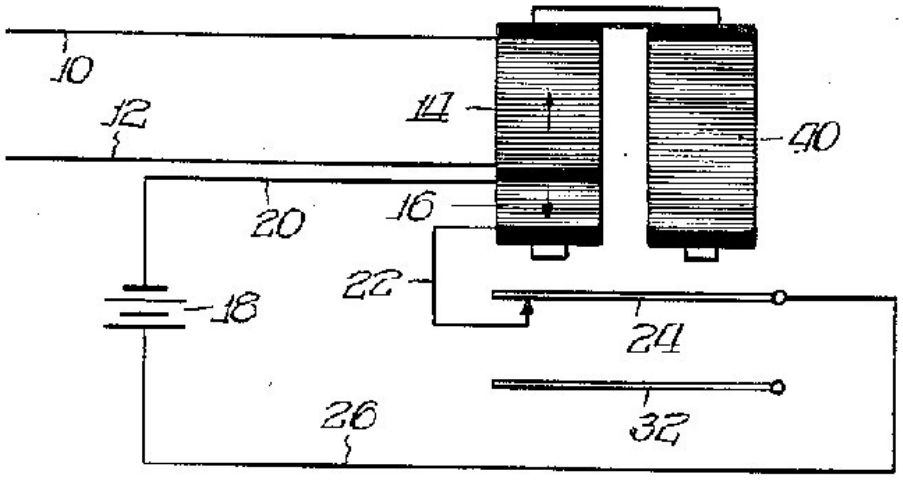

Figure 7. Slow-Acting Relay, 1930. US Patent 1,922,089.

468,222

Application Date: Dec. 31, 1935.

Complete Specification Accepted: June 30, 1937.

Fig. 3.

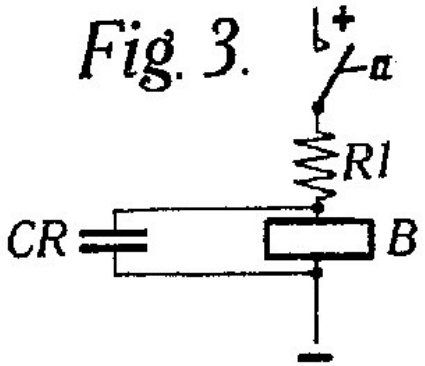

Fig. 3 shows the circuit normally used for obtaining time-delay by the slow operation of a relay. When contacts a are closed condenser CR charges up to the operating voltage for relay B which then operates. The time constant for the charging of condenser CR is: $c\frac{R_1 \times R_2}{R_1 + R_2}$ where c is capacity of condenser CR. R_1 is a resistance in series with the supply circuit, and R_2 is the resistance of relay B. To get maximum delay, R_1 is made equal to R_2 so that the time constant equals $c\frac{R_1}{2}$. If the relay operates at V_o volts and V volts are applied, the delay is t secs. $= c\frac{R_1}{2} \times 2.3 \log 10 \frac{\frac{V}{2}}{\frac{V}{2} - V_o}$.

Figure 8. Slow-Acting Relay, 1935 and Earlier. US Patent 468,222.

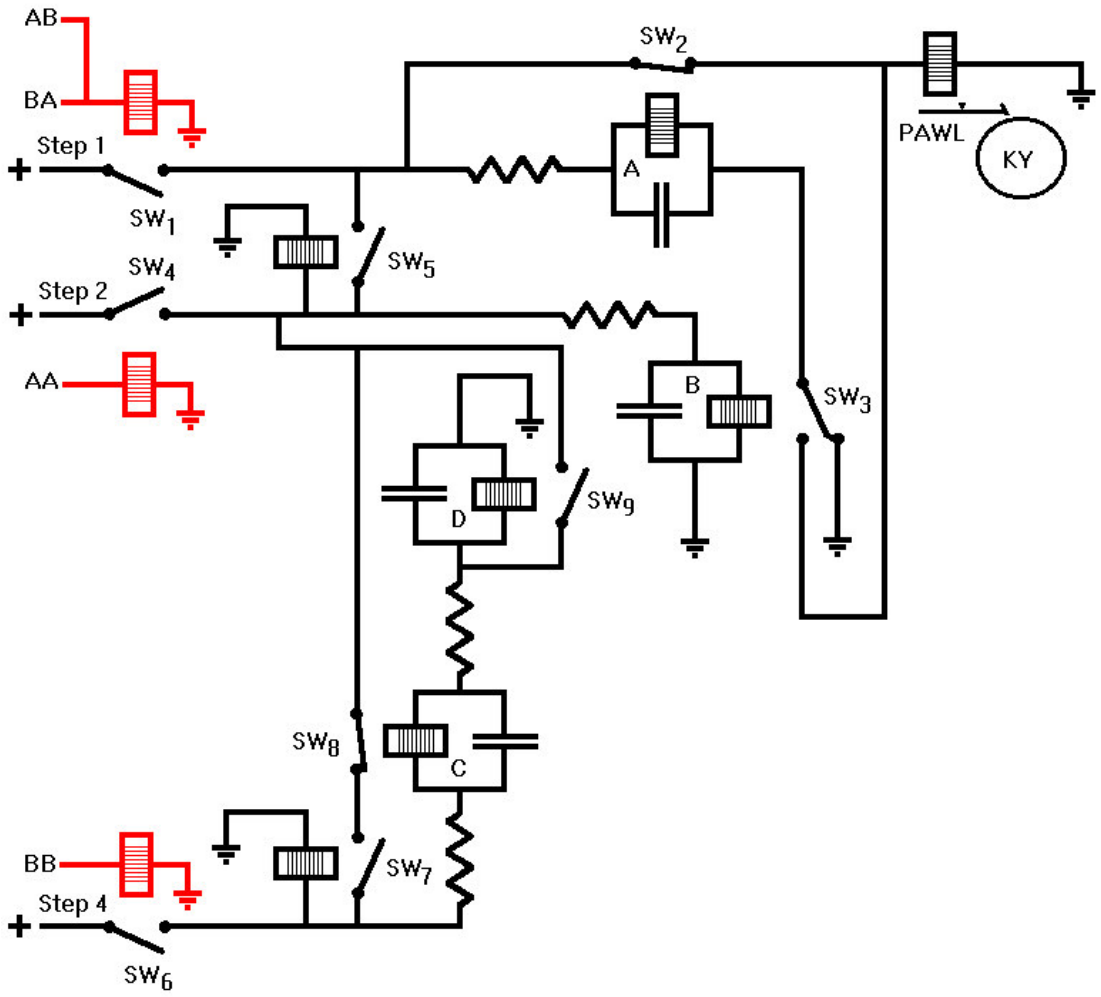

Figure 9. Control Circuit Schematic

The Step 2 Signal, which is delivered through circuit AA, energizes the coil for switch SW_4, closing that switch and allowing current to energize the coil for switch SW_5, which in turn allows the Step 1 sequence to be executed to produce one pulse. Simultaneously, voltage charges the capacitor in slow relay B. When this capacitor is fully charged, the coil for switch SW_3 is energized, closing that switch and allowing current to flow once again to the Pawl coil, producing a second pulse. The time delay for relay B is longer than for relay A in order to allow time for the Step 1 sequence to be completed before the second pulse is allowed through to the Pawl coil.

The Step 4 Signal, which is delivered through circuit BB, energizes the coil for switch SW_6, closing that switch and allowing current to energize the coil for switch SW_7, which in turn allows the Step 2 sequence to be executed to produce two pulses. Simultaneously, voltage charges the capacitor for slow relay C. After a delay, which must be significantly longer than the delays for relays A and B, the coil for switch SW_8 is activated, which opens that switch and ends the second pulse. Voltage then charges the capacitor for slow relay D and after a delay, which is required to allow capacitors A and B to discharge, the coil for switch SW_9 is energized, which closes that switch and allows the Step 2 sequence to be executed a second time, producing a third and fourth pulse.

As explained in the section on the Cryptograph Control System Schematic, the ON/OFF Control Switch on the Control Panel is used to turn off current to the Commutators, so that the M1 disk can be manually realigned with the PT disk without triggering a series of unwanted signals to the Stepping Mechanism in the process. This same switch also turns off current to the Control Circuit. This is done in order to provide time for the capacitors in the Control Circuit to discharge. The stepping sequences cannot be repeated until every capacitor has returned to its initial state.

Summary

This paper makes no claim that the actual design of Byrne's cryptograph has been recovered by analysis nor does it claim that the design presented in this paper is a complete blueprint for engineering purposes. What it does claim is that an electro-mechanical cryptograph can be built, using 1937 technology, that would replicate the statistical signature of Byrne's machine, as was derived from analysis of Byrne's Exhibit 1. This makes the device functionally equivalent to Byrne's device, without necessarily making it an exact duplicate, thereby solving the challenges that Byrne would have faced in 1937 and demonstrating both the iterative nature of enciphering and deciphering as well as the PT/CT dependency of the output Key. It also demonstrates that the complexity of the machine was not beyond the talents of a novice familiar with the basics of physics and mathematics.

References

1. British Patent Office, Patent No. 468,222, Improvements in or relating to Electromagnetic-relay Time-delay Circuits. Issued to Bent B. Jacobsen et. al., June 30, 1937. Application dated December 31, 1935.

2. Byrne, John F. 1953. *Silent Years*. New York: Farrar, Straus, and Young.

3. Byrne, John F. February 17, 1957. Letter to Col. W. F. Friedman. Friedman Collection. George C. Marshall Research Library. Lexington VA.

4. Friedman, William F. March 3, 1957. Letter to John F. Byrne. Friedman Collection. George C. Marshall Research Library. Lexington VA.

5. Hill, Jeffrey A. November 12, 1989. *A Feasible Mechanism for the 1918 Byrne Cryptograph*. Available as Progress Report #8, The Chaocipher Clearing House, www.mountainvistasoft.com/chaocipher.

6. Hill, Jeffrey A. February 28, 2003. *Chaocipher: Analysis and Models*. Available as Progress Report #9, The Chaocipher Clearing House, www.mountainvistasoft.com/chaocipher.

7. Hitt, Parker. 1976. *Manual for the Solution of Military Ciphers*. Laguna Hills CA: Aegean Park Press. Originally published in 1916.

8. U.S. Bureau of Labor Statistics, Inflation Calculator, http://www.bls.gov/data/inflation_calculator.htm

9. U.S. Patent Office. Patent No. 447, 918, Automatic Telephone-Exchange. Issued to Almon B. Strowger, March 10, 1891. Application dated March 12, 1889.

10. U.S. Patent Office. Patent No. 1,922,089, Slow Acting Relay. Issued to Mark H. Hovey, assignor to The Union Switch & Signal Company, August 15, 1933. Application dated September 6, 1930.

11. U. S. Patent Office. Patent No. 4,143,978. Electro-Mechanical Cipher Machine. Issued to Bern Anderson and Donald Seiler. March 13, 1979. Original application dated May 4, 1938.