CHAOCIPHER: ANALYSIS AND MODELS

ADDRESS: Lincoln, Nebraska 68521

ABSTRACT: Chaocipher, a method of encryption invented by John F. Byrne in 1918, was touted as being able to produce ciphertext having no statistical features that would distinguish it from a "jargon" of random characters. However, statistical analysis of Byrne's Exhibit 1 reveals that this claim is false when both plaintext and ciphertext are known. Further analysis reveals that the stepping mechanism of Byrne's 1937 cryptograph can be modeled as a simple, but revealing, Markov process. Cryptograph models based on this process are developed and then analyzed.

KEYWORDS: Chaocipher, John F. Byrne, cryptograph, time series, diffusion process, Markov process, Markov model, state transition matrix, statistical signature, cryptanalysis.

Introduction

Since the invention of Chaocipher in 1918, the method of encryption and the device used to implement this method have been a closely guarded secret known only to John F. Byrne, his family, and experts in the field of cryptanalysis who were consulted about its commercial value. The first Chaocipher cryptograph was constructed in a cigarbox and was, as patent attorney Marcellus Bailey described it, "scarcely more than a toy" [3, p. 266]. This toy, however, was given to Col. Parker Hitt and William F. Friedman for evaluation. Hitt informed Byrne in 1921 that he had found no way to break the cipher and advised him that he could proceed to market the device "with confidence in the practical indecipherability of the product" [3, p. 273]. The following year Hitt introduced Byrne to Friedman, who, as a civilian employee of the Army Signal Corps, examined the device and sent a report to Byrne describing the results of his investigation [8]. Unfortunately, in returning the cryptograph to Byrne, Friedman's clerk failed to package it securely and it was destroyed in shipping. After that incident, Byrne had no further contact with Friedman for many years.

Even as Byrne demonstrated the cigarbox model to Hitt and Friedman, he was planning to have a more substantial device built based on a blueprint which had been drawn up in 1919. According to Byrne, he was not able to obtain a firm bid for the construction of a prototype, but had received only vague estimates that it would cost between $5,000 and $20,000 to build [3, p. 267]. He has nothing else to say about this device, but even allowing for uncertainties stemming from the postwar inflation of 1919, it must have been considerably more complex than the original cigarbox model to warrant these estimates. Faced with the high cost of building another device and rebuffed when he sought to gain financial support from the State Department, he abandoned Chaocipher in 1922 and did not return to it for fifteen years.

Byrne constructed a second device in 1937 after learning that the Navy was seeking a new system of cryptography for fleet communications [3, p. 277]. A meeting with Naval officers was scheduled for May 3, 1938, at which time Byrne was to demonstrate his device and method of ciphering. However, when Byrne arrived for the demonstration it was "ended before it began" and he was advised to take his system to either the War Department or the State Department [3, p. 279]. The Navy, it seems, had already selected a cryptograph from among those demonstrated. The following day, May 4, 1938, a patent application for an electro-mechanical cipher machine was filed by inventors Bern Anderson and Donald Seiler listing as assignee the United States as represented by the Secretary of the Navy [16]. This device was an electric typewriter with a set of rotors interposed between the keyboard and the printing mechanism so that messages could be automatically enciphered or deciphered while being typed. Byrne's device had to match or exceed the sophistication of this device in order to hold the Navy's attention for more than a few minutes, but it failed to do so.

Whether the 1937 cryptograph was built from the 1919 blueprint or not is unclear. In 1954, Byrne offered to show the device to Henry Langen, editor of the American Cryptogram Association's magazine, *The Cryptogram*, but at the last minute he substituted the blueprint instead. His excuse was that the device was "too heavy and cumbersome" to bring to the meeting [5, p.194]. If the actual device closely resembled the one shown in the blueprint, then it had "two revolving disks with the alphabets arranged along the periphery in a complete disorder", according to Langen [Ibid.]. With "only two disks used", Langen did not understand how the device could be as effective as claimed. Also, further clouding the issue, Byrne described the device as being "made up somewhat like a typewriter" [Ibid.]. Given the high cost estimates for the 1919 prototype, the machine shown in the blueprint could easily have had a typewriter keyboard and a printing mechanism in addition to an electro-mechanical scrambling unit of some kind. However, if a machine shop could not build the prototype for less than $5,000 to $20,000 in 1919, it is hard to see how Byrne, working at home in the summer of 1937, could have built this same device. One possibility is that the 1937 cryptograph was in fact a much simpler device than the one shown in the blueprint and Byrne had not made this clear to Langen during their meeting.

Byrne intended for Chaocipher to be a direct refutation of a claim made by Poe that "human ingenuity cannot concoct a cipher which human ingenuity cannot resolve" [3, p. 265]. As Byrne well understood, Poe's cryptanalysis was based on the structure of language; that is, on the repetitions inherent in letter frequencies, word frequencies, and letter patterns within words. Byrne concluded that to insure the complete security of Chaocipher his system had only to produce ciphertext in which there were no exploitable repetitions. He states, "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, ... a cipher which could only be adequately described as a 'jargon of random characters'." [3, p. 270] This "jargon of random characters" would seem to be the inspiration for the name "Chaocipher", which was apparently derived by joining the words "chaos" and "cipher", using chaos as a metaphor for randomness. Confident that the ciphertext produced by Chaocipher met this test of randomness, Byrne states that, "possession of my device together with knowledge of the general principle involved, would not enable any person to decipher any messages whatever written by anyone else and not intended for him." [3, p. 266]

In his autobiography, *Silent Years*, Byrne is deliberately vague about the operation of his device. He describes the process of enciphering as being "identical and simultaneous" with the process of deciphering [3, p. 264]. He also states that "the ancient Egyptians and Babylonians could have been completely familiar with the principle [of Chaocipher], a fact which is readily deducible from a treatise on mathematics written by Hero [or Heron] of Alexandria." [3, p. 265] Heron of Alexandria is known not only for his mathematics, but also for several inventions, including an odometer which consisted of an arrangement of toothed wheels and endless screws with distance marked by means of a pointer [11, pp. 303, 309, 345]. Perhaps Byrne was simply alluding to the "toothed wheel" when he said of his system that "during the past two thousand years and more anyone could have had access to my method for the chaotification of language" [3, p. 265]. However, we find language strikingly similar to Byrne's in Boyer's *History of Mathematics*. "It was essentially the Babylonian type of mathematics that is found in Heron." [2, p. 172] "His name is attached also to 'Heron's algorithm' for finding square roots, but this method of *iteration* was in reality due to the *Babylonians* of 2000 years before his day [emphasis added]." [2, p. 174] Heron's method is defined by the following recursive formula [1, p. 403]:

$$X_{new} = \frac{1}{2} \cdot \left(X_{old} + \frac{A}{X_{old}} \right)$$

The mathematical relation expressed by this formula is unlikely to have any relevance to Chaocipher. What is significant is that the formula is iterative in the sense that the output of one step becomes the input of the next. Therefore, however important the "toothed wheel" may have been in providing "access" to Byrne's method, it is an iterative method known to the Babylonians that would have provided him with a basis for his claim that they and the Egyptians could have been "completely familiar" with his principle.

If Byrne had any inkling that cryptanalysis could be based on something other than the repetitions found in language, he gives no indication of it in *Silent Years*. For him the issue is whether Chaocipher conceals all repetitions in language and the issue is settled by noting that the ciphertext letter frequencies are very nearly equal and by noting also the complete lack of repeating letter patterns when the same short text is enciphered over and over, as, for example, in his Exhibit 1 [3, pp. 285-288]. If the ciphertext cannot be distinguished from a "jargon of random characters", then everyone ought to agree that Chaocipher is materially and mathematically indecipherable. Byrne, however, was baffled by the fact that "in all my efforts to locate backing for my idea and device, I have found it practically impossible to make people understand exactly the import of what I have just written" [3, p. 266].

Byrne claimed that complete knowledge of his device and his system would never be of the least help in cryptanalysis, but so far as can be determined from public sources, neither he nor his son ever allowed this idea to be seriously tested. He was informed by Friedman in 1922 that in addition to knowledge of the system, which had in this instance been provided, fifty messages representing one day's military traffic would be needed for an adequate test of Chaocipher [8]. Byrne never provided those messages. In 1942, when Byrne was again trying to interest Friedman in Chaocipher, he was sent a copy of what the Office of the Chief Signal Officer called "Enclosures A and B" [9]. These enclosures contained basic information about the requirements of military ciphers and provided forms to be used for submitting cipher systems to the War Department [7, p. 247]. Enclosure A discussed the two most important requirements for military ciphers, practicability and secrecy. Any system used by the Army must be simple and easy to use under battlefield conditions and the security of the system must depend only on the specific keys used and not at all on keeping the actual method secret [7, pp. 247-251]. Enclosure B requested full disclosure of the system and, in particular, submission of twenty cryptograms all enciphered with the same specific key [7, p. 255]. Instead of complying, Byrne responded to the receipt of these enclosures by insisting that Chaocipher be judged solely on the basis of the material in Exhibit 1. "Now, keeping in mind this 'Chaocipher' document alone; and prescinding from any other consideration of my cipher system, can you answer the following question? Do you deny my assertion that this cipher document as it stands is indecipherable?" [4] To which Friedman replied, "I can neither affirm or deny any assertion that you make concerning your system until we have more data. The purpose of the material sent you [Enclosures A and B] was to develop the facts along lines which have long ago proved their usefulness. Unless and until you can find your way clear to submitting the data called for, no examination can be made of your system in order to determine its merits for use in the military service." [10] For Byrne, however, the issue was very simple and did not require anything more to resolve it than the examination of a single cryptogram which he had already provided (Exhibit 1). That ended the matter until Byrne brought Chaocipher to public attention with the publication of his autobiography, *Silent Years*, in 1953.

For almost forty years, John F. Byrne attempted to enlist support from various corporate and government officials for the development of Chaocipher. In this he was completely disappointed, but as late as 1990 his son, John Byrne, was still hoping to develop a commercial application for his father's invention [5, p.195].

Cryptanalysis

In his autobiography, Byrne published four Chaocipher "exhibits", each containing ciphertext with all, or in some cases substantially all, of the corresponding plaintext [3, pp. 285-307]. Only Exhibits 1 and 4 contain a few rows of ciphertext for which the plaintext is unknown. The first challenge is to discover what sort of device was used to prepare the cryptograms and how the device was operated so that conventional cryptanalysis can begin. While we have a few vague statements by Byrne about the operation of the device and a few statements by Langen indicating that the device was equipped with two revolving disks, we must largely depend on statistical phenomena found in Byrne's exhibits for insight into the mechanism and its method of operation.

Greg Mellen noted two phenomena in Exhibit 1 which were easy to spot because the ciphertext in Exhibit 1 is arranged in flush depth [14, p. 144]. First, there is no isomorphism among the 100 encryptions of "ALLGOOD...PARTYW". Second, no doubled plaintext letter is enciphered by a doubled ciphertext letter (a combination which Mellen referred to as a "pt/ct identity") with one exception, which occurs in Exhibit 3 where plaintext TT is enciphered by YY [14, p. 146]. Further study revealed a third, less obvious, phenomenon. He discovered that when the Byrne exhibits are divided into blocks of thirteen letters, identical plaintext letters are rarely enciphered by identical ciphertext letters within those blocks. He called this the thirteen-letter block phenomenon. Two examples of this phenomenon, which were given by Mellen [14, pp. 146-147], are the following blocks from Rows 114 and 176 of Exhibit 1, where P/J and S/O each repeat in less than thirteen letters:

```
             =                       =
Row 114:  pt: P U R S U I T O F H A P P
          ct: J X M L S Q T V Z B Y J O

             =                       =
Row 176:  pt: S T E M O F E N G L I S H
          ct: O U Q F O Y U T E V V O D
```

In the analysis that follows, we refer to a plaintext letter and the ciphertext letter with which it is encrypted as a state of Byrne's machine. We can therefore say of Mellen's two examples that the initial machine state in each line repeats after eleven machine steps. However, Mellen's examples are misleading because of the way in which he divided the exhibits into thirteen-letter blocks. If we instead focus on machine states and the earliest repetition of such states, we find that no machine state repeats in less than nine steps in Exhibit 1, although exceptions to this rule occur in Byrne's other three exhibits.

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

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

In February, 1994, William G. Sutton, then editor and publisher of the ACA's periodical, *The Cryptogram* sent a letter to several ACA members who were analyzing Chaocipher. He called our attention to the data in Table 1, where matching pt/ct pairs have been counted by taking each encipherment in Exhibit 1 and checking to see whether or not a matching pt letter occurs within 15 steps [15]. If a pt match is found, we count this as a "comparison" and then check to see if the ct letters also match. If there is a ct match, we count this as a "hit". As can be seen from the table, there are significant differences at almost every stepping interval between the actual number of hits and the expected number for random text.

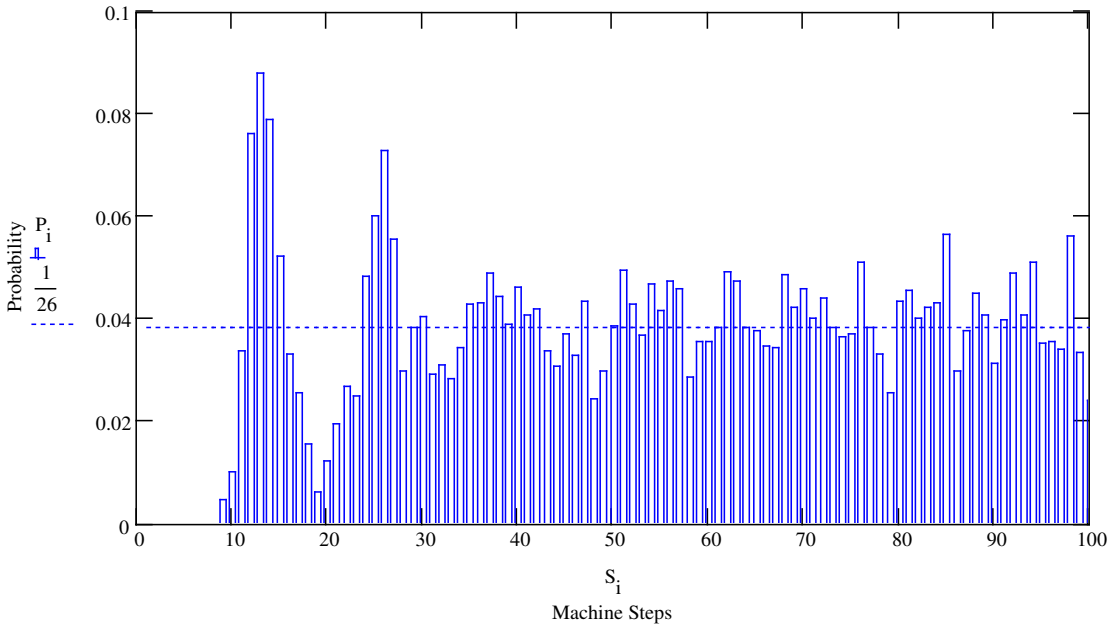

Figure 1. Probability of Repeated Machine States in Exhibit 1

Table 1 opens the door to further analysis. When hit/comparison ratios are converted to probabilities and the stepping intervals are plotted as a time series extending well beyond Step 15, a very distinct pattern emerges from Byrne's "chaos", as can be seen in Figure 1. The graph is wave-like in appearance, with two distinct peaks at steps 13 and 26 and with less obvious peaks at steps 39 and 52. Beyond step 50, however, the "wave" is all but damped out and the probabilities differ little from chance. As will be seen in the analysis which follows, the observed time series can be interpreted in terms of particle diffusion.

We begin by considering a particle constrained to move on a circular path that is lined with 26 cells, C_0 through C_{25}. The particle is initially in cell C_0. After a fixed time period, t, the particle jumps in a clockwise direction to a new cell a short distance away. To put the nature of the problem that is being analyzed into perspective, we place in C_0 an observer who can only observe the contents of that particular cell. He initially observes that the particle is in C_0 and then counts the number of fixed time periods, or steps, until the particle returns to C_0. He finds that the particle never returns in less than nine steps. He also finds that the highest probability that the particle will return is at step 13 and this probability is more than twice that which would be expected on the basis of chance. He finds, in fact, that the graph of all observed probabilities matches that of Figure 1.

This diffusion process has a natural interpretation in terms of the relative motion of two disks, each of which is inscribed with a mixed alphabet of 26 letters. Let A be a letter on the outer, stationary disk, and let C be a letter on the inner, rotating disk. Let A and C be initially aligned. With each step of the mechanism, the rotating disk moves clockwise in short jumps until C is again aligned with A. As our analysis will show, C is constrained to move a distance of about 1 to 5 letters on each step, with an average move being very nearly, if not exactly, a distance of two letters, so that on average C does not align again with A for 13 steps. We are not so fortunate as to have an observer in place on the stationary disk whenever C aligns with A, since we can only make observations when a particular plaintext letter occurs in the text of Exhibit 1. Therefore, even though we may not observe the alignment of A and C in Exhibit 1 at a particular step, that does not mean that the corresponding disk alignment did not occur.

Markov Models

Let S be a dynamic system, or Markov process, which at time t can be in one of 26 states, S_0 through S_{25}. We represent the system as a state vector, $\mathbf{S}_t = (q_0, q_1, q_2, \ldots q_i, \ldots q_{24}, q_{25})$, where q_i is the probability that the system is in state S_i at time t. The sum of all q_i in $\mathbf{S}_t$ is 1.

Let **P** be a 26x26 transition matrix specifying the probabilities with which the system S changes from one state to another during each transition. The first row of **P** specifies that when the system is in state S_0, it changes to states $S_0, S_1, S_2, \ldots, S_n$ with the corresponding probabilities, $p_0, p_1, p_2, \ldots, p_n$ in that row. To generalize, row i of **P** specifies that when the system is in state S_i, it changes to state S_j with probability p_j during any transition. We define the transition from one state vector to the next by the following equation, using matrix multiplication:

$$\mathbf{S}_{t+1} = \mathbf{S}_t\mathbf{P}$$

By this rule, $\mathbf{S}_1 = \mathbf{S}_0\mathbf{P}$, $\mathbf{S}_2 = \mathbf{S}_1\mathbf{P}$, and so on, where $\mathbf{S}_0$ is the initial state vector. To generalize, the state vector $\mathbf{S}_t$ can be computed for any time interval t from the following equation:

$$\mathbf{S}_t = \mathbf{S}_0\mathbf{P}^t$$

The meaning of this equation is that at time t the state vector $\mathbf{S}_t$ depends only on the initial state vector $\mathbf{S}_0$ and the state transition matrix **P**. For our diffusion model, $\mathbf{S}_0 = (1, 0, 0, 0, \ldots., 0, 0, 0)$, which means that the system is certainly in state S_0 initially and certainly not in any other state. Once **P** is known, we can calculate the probability that the system is in state S_0 at any time t, which is to say that we can calculate the probability that S_0 repeats at any step.

Due to Langen's observation that Byrne's cryptograph is equipped with two rotating disks, each inscribed with a mixed alphabet, it is natural to consider first a conventional cipher disk with a fixed plain alphabet surrounding a rotating cipher alphabet, even though this would be one rotating disk instead of two. Our justification is that even if both disks are rotating, we can assume that one is stationary with respect to the other since motion is relative. To supply a key stream, the rotating disk is assumed to be driven by an arbitrarily long belt that is divided into sectors, with each sector containing one or more gear teeth much like the sectored drive gear of the Kryha cryptograph [6, p. 151]. Each time that the drive mechanism steps, it advances the belt by one sector which in turn advances the cipher alphabet by as many teeth as there are in that sector. Since no state repeats after one step, as is evident from the fact that doubled pt are never enciphered by doubled ct in Exhibit 1, we conclude that every sector has at least one tooth. The average stepping distance will be determined by the expected number of teeth per sector, E(N). Let the number of teeth per sector vary from 1 to n and let p_i be the probability that a sector has i teeth. Then the expected number of teeth per sector is calculated from the formula:

$$E(N) = \sum_{i=1}^{n} i \cdot p_i \quad \text{provided that} \quad \sum_{i=1}^{n} p_i = 1.0$$

Guided by this hypothetical model, we are able, by trial and error, to fit a Markov process to the graph in Figure 1 [12, p. 1]. We begin by assuming that the rotating disk advances about two letters per step, on average, relative to the stationary disk, or in other words, that the value of E(N) is approximately two teeth per sector. This follows from the observation that the system advances 13 steps before it has the greatest probability of returning to its initial state, at which point it will have traveled a distance of 26 letters. It is further assumed that whatever the physical reality of the driving mechanism, each "sector" would have only a few teeth. Thus the possibility that each sector contained 1 to 3 teeth is considered first and when this does not yield a convincing fit to the graph of Figure 1, the value of n, the maximum number of teeth per sector, is increased to 4 and then later to 5. While it is possible to include probabilities for 6, 7, and 8 teeth per sector, these probabilities have to be very small in order for the value of E(N) to remain

close to 2. They will be so small, in fact, that for graph fitting purposes they can be neglected. Based on these considerations, our task is to choose probabilities p_1 through p_5 so that the following equation is true:

$$E(N) = p_1 + 2p_2 + 3p_3 + 4p_4 + 5p_5 = 2 \text{ (approximately)}$$

As soon as this equation has been satisfied, the probabilities can be substituted into the corresponding variables of transition matrix, **P**, as specified in Table 2. The state vector, $\mathbf{S}_t$, is then calculated for each value of t from 1 to 100 and at each step the probability that the system is in state S_0 is plotted on a graph that is superimposed on Figure 1. If the new graph has peaks and troughs that closely match those of Figure 1, then we have a model with which to explain the operation of Byrne's cryptograph.

P	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**...**	**25**
0	0	p_1	p_2	p_3	p_4	p_5	0	0	0	0	0	...	0
1	0	0	p_1	p_2	p_3	p_4	p_5	0	0	0	0	...	0
2	0	0	0	p_1	p_2	p_3	p_4	p_5	0	0	0	...	0
...													...
25	p_1	p_2	p_3	p_4	p_5	0	0	0	0	0	0	...	0

Table 2. Markov Process State Transition Matrix

Fitting a Markov model to a graph in the way just described is art rather than science. Nevertheless, Markov Model 1 (MM1), derived from the values in Table 3, generates a good fit to the state repetition probabilities, as can be seen in Figure 2. The value of E(N) derived from the percentages in Table 3 is very close to 2:

$$E(N) = 0.485 + 2(0.248) + 3(0.099) + 4(0.069) + 5(0.099) = 2.049$$

Teeth per Sector, N	Percentage of Sectors having N teeth
1	48.5
2	24.8
3	9.9
4	6.9
5	9.9

Table 3. Sector Specifications for a Hypothetical Drive Belt (MM1)

Further analysis reveals the set of probabilities in Table 4, which define Markov Model 2 (MM2), for which the value of E(N) is exactly 2.

$$E(N) = 1/2 + 2(1/4) + 4(1/4) = 2$$

Teeth per Sector, N	Percentage of Sectors having N teeth
1	50
2	25
4	25

Table 4. Sector Specifications for a Hypothetical Drive Belt (MM2)

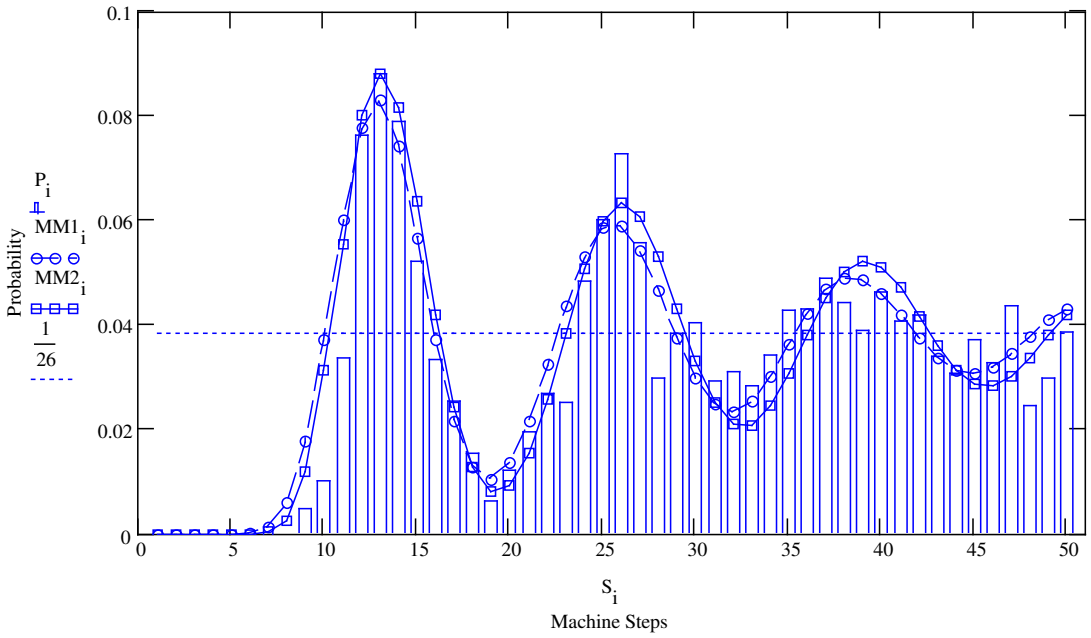

Figure 2. Markov Models fitted to the Probability of Repeated Machine States

Table 5 compares the probabilities actually observed at steps 13 and 19, which correspond to the first peak and the second trough of the graph, with those predicted by MM1 and MM2. The fit to the step 13 peak by MM2 is exceptionally good.

Step	Observed Probability	Predicted Probability (MM1)	Predicted Probability (MM2)
13	0.08795	0.08295	0.08801
19	0.00619	0.01039	0.00798

Table 5. Comparison of Data to Markov Model Predictions

The simple probabilities derived from Table 4, that is 1/2, 1/4, and 1/4, suggest other ways to interpret Byrne's stepping method that go beyond the hypothetical drive belt which has so far been assumed. These probabilities arise when a trial has two outcomes, A and B, each having probability 1/2, 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. 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. This logic gate, which can be built from four relays by combining an AND gate with an XOR gate, has the properties listed in Table 6. A pseudo-random sequence of inputs, A and B, would, by hypothesis, be provided by another component of the device.

A	B	Q1	Q2	Signal
0	0	0	0	Forward 2
0	1	1	0	Forward 1
1	0	1	0	Forward 1
1	1	0	1	Forward 4

Table 6. Logic Gate with two Inputs, A and B, and two Outputs, Q1 and Q2

To summarize our results so far, Mellen's observations with which we began our analysis have been extended beyond step 13 and interpreted as a time series. This time series has been replicated by a mathematical model. The model demonstrates that Byrne failed to eliminate all order and regularity in Chaocipher, even though this regularity is only discernible when both plaintext and corresponding ciphertext are available to the analyst. The phenomena described by Mellen and quantified in Table 1 may be taken as a statistical signature, or characteristic data set, of the Byrne cryptograph in Exhibit 1. Any model of Byrne's device must replicate this signature.

Cryptograph Models

The conventional cipher disk which served as a model during our analysis of the Markov stepping process, cannot, as it stands, be a model of Byrne's device. Suppose pt EE is to be enciphered using this device, then from Figure 3 the first encipherment is E/D.

```
PT: ABCDEFGHIJKLMNOPQRSTUVWXYZ
CT: ACOWDMUEGQYIJTKFPXLBNVSHRZ ==> Markov Step
```

Figure 3. Cryptograph C94, Conventional Cipher Disk.

The CT disk then steps one, two, or four letters (assuming that MM2 is the best model) bringing either W, O, or A into alignment with E for the second encipherment. This means that if we locate every occurrence of pt EE in Exhibit 1, we should find at most three encipherments, EE/DW, EE/DO, or EE/DA, in which the first ct letter is D, with EE/DW comprising about 50% of the observed cases. The same analysis applies to any doubled pt letters in which the first letter is enciphered with D. The second pt letter will necessarily be enciphered by one of the three ct letters W, O, or A, if the cryptograph is C94. What we find in Exhibit 1, however, is that for all doubled pt letters, $\alpha\alpha$, taken as a group, when the first encipherment is α/D, the second pt letter can be enciphered by any one of twenty ct letters. This greater than expected variety of contact must be explained by any model of Byrne's device, but it cannot be explained by Cryptograph C94.

```
PT:  ACOWDMUEGQYIJTKFPXLBNVSHRZ
R1: [ABCDEFGHIJKLMNOPQRSTUVWXYZ] ==>
R2: [ACJPVDEKQWIFLSXOGMTYRBHNUZ] ==>
CT:  ABCDEFGHIJKLMNOPQRSTUVWXYZ
```

Figure 4. Kullback Single-Rotor Cryptograph.

A study was made of the single-rotor cryptograph described by Kullback [13, pp. 198-199], but this model does not replicate the Markov transition probabilities as required. The problem is that even when the rotor is stepping one, two, or four letters with the correct transition probabilities, it mixes the CT letters to such an extent that the Markov process cannot be detected in statistics collected from Exhibit 1. However, the rotor diagram in Figure 4 suggests a way to increase variety of contact while preserving the discernibility of the Markov process in the statistics. This is accomplished by splitting Kullback's single rotor into two half-rotors, M1 and M2, each of which is mounted on a separate, rotating disk, as in Figure 5. This device, Cryptograph C98, can also be described as two conventional cipher disks mounted side by side and used in an unconventional way, in agreement with Langen's statement that "only two disks" were used.

```
PT: ABCDEFGHIJKLMNOPQRSTUVWXYZ
M1: ACOWDMUEGQYIJTKFPXLBNVSHRZ ==> Markov Step

CT: ABCDEFGHIJKLMNOPQRSTUVWXYZ
M2: ACJPVDEKQWIFLSXOGMTYRBHNUZ ==> Periodic Step
```

Figure 5. Cryptograph C98, Two Half-Rotors.

Enciphering with C98 begins by locating plaintext letter E in alphabet PT and noting enciphering mark D on half-rotor M1 directly below E. Mark D is then located on half-rotor M2 and cipher letter F is read directly above it in alphabet CT, completing the encipherment, E/F. Half-rotor M1 is a "fast" disk, stepping one, two, or four letters after each encipherment in accordance with the Markov model already described. Half-rotor M2 is a "slow" disk, stepping only periodically, perhaps at the end of each row in Exhibit 1, or every 55 letters. For each M2 position there is an implicit CT disk which can be obtained by reducing M1, M2, and CT to a single rotating disk (see Complexity Reduction in the next section). This makes C98 the equivalent of C94 within each M2 period. Contact variety is assured, because as M2 rotates through each of 26 positions, the system in effect uses 26 different C94 devices instead of just one. Every C94 has the same PT alphabet, but each has implicitly a different CT alphabet.

```
MK: +
KY: QWERTYUIOPASDFGHJKLZXCVBNM ==> Markov Step

PT: ABCDEFGHIJKLMNOPQRSTUVWXYZ
CT: QYIJTKFPXLBNVSHRZACOWDMUEG ==> Manual Alignment
```

Figure 6. Cryptograph C98A, Key Disk and Conventional Cipher Disk.

Another possible Chaocipher design is that of Cryptograph C98A in Figure 6. C98A has a fixed alignment mark, MK, indicated by a plus sign fixed just outside the arc of a revolving disk, KY, making this a distinct departure from the C94 design. Instead of a rotating disk moving relative to a stationary disk to generate the characteristic statistics of the Markov process, we now have a rotating disk moving relative to a fixed mark to accomplish the same thing. The second disk of the system is a conventional cipher disk that is operated manually. For each encipherment, the KY disk steps one, two, or four letters in accordance with the Markov transition probabilities and the letter that comes to rest under the alignment mark is used as a key to align the CT alphabet with the PT alphabet. For example, if the key letter is Q, then the CT disk is manually "dialed" to place Q under the A of the PT alphabet. Cipher letter T is then located under plain letter E to complete the encipherment, E/T.

```
PT: ABCDEFGHIJKLMNOPQRSTUVWXYZ   PT: ABCDEFGHIJKLMNOPQRSTUVWXYZ
CT: ACOWDMUEGQYIJTKFPXLBNVSHRZ   CT: NVSHRZACOWDMUEGQYIJTKFPXLB
CT: PXLBNVSHRZACOWDMUEGQYIJTKF   CT: BNVSHRZACOWDMUEGQYIJTKFPXL
CT: OWDMUEGQYIJTKFPXLBNVSHRZAC   CT: VSHRZACOWDMUEGQYIJTKFPXLBN
CT: UEGQYIJTKFPXLBNVSHRZACOWDM   CT: XLBNVSHRZACOWDMUEGQYIJTKFP
```

Figure 7. Cryptograph C98A, Comparison of Contact Variety

We saw in the case of C94 that only the letters W, O, and A, are possible values of γ in the encipherment $\alpha\alpha/D\gamma$. This is because the contacts of D can only come from the letters one, two, and four places from D on CT (see Figure 3). With C98A, however, encipherments are determined by sequences of key letters instead of sequences of cipher letters. As shown in Figure 7, the key A and its three possible successors, P, O, and U, on KY will produce the encipherments EE/DN, EE/DU, and EE/DY, while the key N and its possible successors, B, V, and X, will produce a completely different set of ct contacts in the encipherments KK/DW, KK/DM, and KK/DC. Therefore when the encipherment $\alpha\alpha/D\gamma$ is produced by C98A, the letter γ will have 26 possible values instead of three, which gives this cryptograph a contact variety similar to that produced by Byrne's device.

The C98 design finds final expression in Cryptograph C98U, which embodies every useful feature so far discussed. First, as shown in Figure 8, there are two half-rotors to increase contact variety. Next there is a separate key disk driven by a Markov process to replicate the statistical signature of Byrne's device and to further insure variety of contact. It could be argued that C98U is clearly not consistent with Langen's description of Byrne's device, i.e. "only two disks used". In that case, all that can be said in defense of the C98U design is that Langen did not see Byrne's actual cryptograph, but only a much older blueprint of what must have been, judging from the cost estimates, a rather complex design. One can argue

that Byrne was unlikely to have built the device shown in the blueprint and consequently what Langen saw did not necessarily resemble the actual cryptograph to a high degree.

```
MK: +
KY: QWERTYUIOPASDFGHJKLZXCVBNM ==> Markov Step

PT: ABCDEFGHIJKLMNOPQRSTUVWXYZ
M1: QYIJTKFPXLBNVSHRZACOWDMUEG ==> Manual Alignment

CT: ABCDEFGHIJKLMNOPQRSTUVWXYZ
M2: ACJPVDEKQWIFLSXOGMTYRBHNUZ ==> Periodic Step
```

Figure 8. Cryptograph C98U, Key Disk and two Half-Rotors.

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. These generators are not always separate components. In C94, the CT disk of the tableau generator also serves as the key generator, as does the M1 disk of C98. However, in every model of the C98 series, it is a key generator in the form of a rotating disk that replicates the characteristic signature of Chaocipher by stepping relative to a fixed mark, or key indicator. It is difficult to imagine a different design consisting chiefly of two revolving disks with mixed alphabets that could generate this same statistical signature.

Complexity Reduction

In the analysis that follows, we assume that Byrne's device is one of the cryptographs in the C98 series of designs. Since we lack complete knowledge of Byrne's device and system, the most accessible component to attack is the tableau generator, since it produces the alignment of plain letters and cipher letters found in Exhibit 1. If the alphabets of the tableau generator can be recovered, then the KY alphabet (if there is one) and the underlying stepping sequence can be recovered for further analysis.

To reduce the complexity of the alphabet recovery problem, we note that the M1 and M2 disks contain arbitrary symbols used as enciphering and deciphering marks that can be replaced by any symbols that we choose, so long as the new marks consistently reference the same disk positions as the old marks. Consequently, we can replace the mixed M2 alphabet of C98 (Figure 5) with a standard alphabet and then relabel the mixed M1 alphabet to be consistent with that of M2, as shown in Figure 9. For example, the letter E in the original M2 alphabet is replaced with G during relabeling, so the letter E in the original M1 alphabet must also be relabeled as G.

```
Original  M2: ACJPVDEKQWIFLSXOGMTYRBHNUZ
Relabeled M2: ABCDEFGHIJKLMNOPQRSTUVWXYZ

Original  M1: ACOWDMUEGQYIJTKFPXLBNVSHRZ
Relabeled M1: ABPJFRYGQITKCSHLDOMVXENWUZ
```

Figure 9. Relabeling of Enciphering/Deciphering Marks

As a result of relabeling, the original C98 is transformed into the equivalent machine shown in Figure 10. The equivalent machine will produce exactly the same ciphertext as the original C98, but it has one less alphabet to recover during analysis, since M2 is now known. In order to obtain an equivalent

machine for C98U, the original key letters on KY must also be replaced with new symbols that correctly reference the new enciphering/deciphering marks on M1.

```
PT: ABCDEFGHIJKLMNOPQRSTUVWXYZ
M1: ABPJFRYGQITKCSHLDOMVXENWUZ ==> Markov Step

CT: ABCDEFGHIJKLMNOPQRSTUVWXYZ
M2: ABCDEFGHIJKLMNOPQRSTUVWXYZ ==> Periodic Step
```

Figure 10. Cryptograph C98, Equivalent Machine

The alphabet recovery problem can be further reduced in complexity if we know that the position of the M2 disk is fixed, or unchanged, relative to the CT disk over a given text interval. In that case, disks M1, M2, and CT can be replaced by an implicit CT disk to obtain an equivalent machine for that text interval.

```
PT: ABCDEFGHIJKLMNOPQRSTUVWXYZ
M1: ABPJFRYGQITKCSHLDOMVXENWUZ ==> Markov Step

CT: ANWCJGZEIBQPXHUSKMDTFYLRVO
M2: ABCDEFGHIJKLMNOPQRSTUVWXYZ ==> Periodic Step
```

Figure 11. Cryptograph C98, Variant with Mixed CT Alphabet

To illustrate this reduction, we start with the variant C98 device in Figure 11, where the standard CT alphabet shown in Figure 10 has been replaced with a mixed alphabet for greater clarity. Since the CT and M2 disks are fixed in relation to each other over a given text interval, an enciphering mark, φ, on M2 will be aligned with a particular CT letter, γ, over the entire interval. That means that φ on M1 will always point to γ and can simply be replaced by it, thereby demonstrating that M1 is an implicit CT disk for this text interval. For example, F on M1 is linked by enciphering rule to F on M2 which in turn is always aligned with G on CT. Therefore F can be replaced by G on M1. This procedure will convert the four-alphabet C98 variant in Figure 11 to an equivalent two-alphabet C94 machine, as shown in Figure 12. This procedure will also convert the five-alphabet C98U to an equivalent C98A machine with three alphabets KY, PT, and CT, provided that the KY alphabet is relabeled to be consistent with the implicit CT alphabet.

```
          PT: ABCDEFGHIJKLMNOPQRSTUVWXYZ
Implicit CT: ANSBGMVZKITQWDEPCUXYRJHLFO ==> Markov Step
```

Figure 12. Cryptograph C98, Equivalent Variant for Fixed M2 Period

Monoperiod Text

It is difficult to determine an M2 stepping interval, or period, in Exhibit 1, since we lack complete knowledge of Byrne's device and system. However, a possible clue may be found in Exhibit 3 where TT is enciphered by YY, which, as Mellen noted, is the only instance of doubled pt letters enciphered by doubled ct letters in the four exhibits. The first T/Y encipherment occurs at the end of Row 31 with the second following in Row 32, as shown in Figure 13.

```
                                                                      =
Row 31 pt: N O F D I S P A T C H E S A N D O R D E R S W R I T
       ct: E P N Q O W R Q F B S K K Y C J O Y F C P R V J B Y

           =
Row 32 pt: T E N I N P L A I N L A N G U A G E H A S R E S U L
       ct: Y G F S B Q E U K I Y J E L J Z K P H H L S X K N H
```

Figure 13. Location of the encipherment TT/YY in Exhibit 3.

Exhibit 3 differs from Exhibit 1 in that it is arrayed in lines of 26 letters instead of in eleven blocks of five letters each. The significance of this is that the only place where either C98 or C98U could encipher doubled pt with doubled ct is at the boundary between two M2 periods. This is due to the fact that within any M2 period these cryptographs reduce to the equivalent of C94 or C98A, respectively, neither of which can encipher doubled pt with doubled ct. However, at the end of a period, C98 and C98U become the equivalent, respectively, of a new C94 or C98A machine. What one machine acting alone cannot do, two acting in succession can do by chance at the boundary between two periods. In view of this, it is perhaps no accident that Exhibit 3 is arrayed in rows of 26 letters. One can speculate that when Byrne was testing Chaocipher, he found it convenient to have the boundaries of M2 periods plainly delimited by placing the text of each M2 period on a single row. One might further speculate that this was also his practice in Exhibit 1 which is arrayed in rows of 55 letters, especially since each of the first 100 rows encrypts the same plaintext, "ALLGOOD...PARTYW". To test this hypothesis, the first 100 rows of Exhibit 1 were checked for anomalies by comparing every combination of two rows to find matching cipher letters. The results are summarized in Table 7, where the probability of N matches per combination has been derived by modeling the experiment as a Poisson distribution (p = 1/26, n = 55). The expected frequency distribution is based on the total number of experiments, or combinations, i.e. C(100, 2) = 4950.

Number of ct Matches, N	Probability of N Matches	Expected Distribution	Chaocipher Distribution	C98U Distribution
0	0.12058690	597	556	628
1	0.25508768	1263	1280	1234
2	0.26980427	1336	1313	1375
3	0.19024660	942	985	946
4	0.10061118	498	497	482
5	0.04256627	211	227	175
6	0.01500734	74	66	75
7	0.00453518	22	18	20
8	0.00119921	6	5	7
9	0.00028187	1	2	5
10	0.00005963			1
11	0.00001147		1	
12	0.00000202			
13	0.00000033			
14	0.00000005			2
Totals	1.00000000	4950	4950	4950

Table 7. Number of Ciphertext Matches for Combinations of Two Rows in Exhibit 1.

Byrne very likely intended the repeated encryptions in Exhibit 1 as a demonstration that Chaocipher does not produce isomorphism. While it is true that no isomorphism is present, there are nevertheless some anomalies. One combination with eleven matches, Rows 22-34, stands out in Table 7 as having an exceptionally large number of matches, while another combination, Rows 43-55, bears some resemblance to the first in that there is a difference of twelve rows between the first and second row of each

combination and also the letter matches in the latter combination occur in the same columns as matches in the former, as shown in Figure 14.

```
   ALLGO ODQQU ICKBR OWNFO XESJU MPOVE RLAZY DOGTO SAVET HEIRP ARTYW

       = ====    =       =   =           =         =             =
22 HGLQP QHMNF HXETY YPEAQ BUDWK NDXDZ BSLXX XCTLH CIWBI QHXHN YYFNH
34 VFYNP QHMNM IDEIH ISTYQ QVDRN ZIBXA IKSXO KESPN XIMTE KILQX OPONS

         ====           =               =
43 FDEVG HWYWX LIKKF IHIIZ AXOPI DHUWQ XNWLM YVDDH GOIAZ SCCQF ZULJA
55 KRNXC HWYWL EYFHB TUZXZ JKVSC VOYKJ NRCLO OZARV LBSZG TYHGU JZHZV
```

Figure 14. Matched Cipher Letters in Selected Rows of Exhibit 1.

From Table 7, two rows are expected to have eleven or more matches in common by chance only once in 100,000 combinations. When this phenomenon occurs during C98U simulations, it can be verified that the rows involved correspond to machine states having identical M2 periods. If Byrne's device is similar to C98U, as we have so far assumed, then the matches in Rows 22-34 are consistent with the hypothesis that the rows of Exhibit 1 correspond to M2 periods. This places severe constraints on analysis, since instead of a single period of 13,615 characters (the length of Exhibit 1), there are, in the absence of any way to identify such periods with certainty, only monoperiod text intervals of 55 and 110 characters readily available. It is only for monoperiod text intervals that certain of the complexity reduction techniques of the last section apply.

Conclusions

Byrne's claim that Chaocipher is indecipherable is based on the principle 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" [3, p. 270]. However, the Markov process which was derived from the transition statistics of Exhibit 1 proves that Chaocipher is far from having cipher "drawn inconsequentially from a rotating drum", so if Byrne's principle is accepted, it follows that Chaocipher is not "materially and mathematically indecipherable". If either the C98 or C98U design provides an accurate description of Byrne's device, then analysis may yet recover the disk alphabets, after which a complete break of Exhibit 1 seems certain.

References

1. Borowski, E. J., and Borwein, J. M. 1991. *The Harper Collins Dictionary of Mathematics*. New York: Harper Collins.

2. Boyer, Carl B. 1991. *A History of Mathematics, 2nd Ed*. New York: John Wiley & Sons.

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

4. Byrne, John F. June 9, 1942. Letter to Col. W. F. Friedman. Friedman Collection. George C. Marshall Research Library. Lexington VA.

5. Byrne, John, Deavours, Cipher A., Kruh, Louis. 1990. Chaocipher Enters the Computer Age when its Method is Disclosed to Cryptologia Editors. *Cryptologia*. 14(3):193-198.

6. Deavours, Cipher A., and Kruh, Louis. 1985. *Machine Cryptography and Modern Cryptanalysis*. Norwood MA: Artech House, Inc.

7. Friedman, William F. 1991. Information Regarding Cryptographic Systems Submitted for Use by the Military Service and Forms to be Used. *Cryptologia*. 15(3):247-257.

8. Friedman, William F. Sept. 7, 1922. Letter to John F. Byrne. Friedman Collection. George C. Marshall Research Library. Lexington VA.

9. Friedman, William F. June 6, 1942. Letter to John F. Byrne. Friedman Collection. George C. Marshall Research Library. Lexington VA.

10. Friedman, William F. June 16, 1942. Letter to John F. Byrne. Friedman Collection. George C. Marshall Research Library. Lexington VA.

11. Heath, Sir Thomas. 1981. *A History of Greek Mathematics, Vol. II*. New York: Dover Publications, Inc.

12. Hill, Jeffrey A. April 22, 1994. *Chaocipher Update: Study No. 1 - A Stochastic Model of the Exhibit 1 Tableau Repeats*. Unpublished manuscript.

13. Kullback, Solomon. 1976. *Statistical Methods in Cryptanalysis*. Laguna Hills CA: Aegean Park Press.

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

15. Sutton, William G. February 2, 1994. Letter to Jeffrey Hill.

16. U. S. Patent Office. Patent No. 4,143,978. Electro-Mechanical Cipher Machine. Issued to Bern Anderson et. al. March 13, 1979. (Original application dated May 4, 1938.)