A FEASIBLE MECHANISM FOR THE 1918 BYRNE CRYPTOGRAPH

INTRODUCTION

The cryptograph illustrated in FIGURE 1 is a three disk system that combines the essential features of a Wheatstone and a Kryha cryptograph into a single mechanism. The rotating components are the two alphabet disks, Pt and Ct, and the Key Selector, A, which points to a stationary Key alphabet. The Key Selector drives the other disks as it is moved from one Key letter to another. Gears B and D, which can have a ratio of 27 to 26 as in the Wheatstone, introduce an aperiodic component into the key stream, while gears E and F have sectors with a variable number of teeth, as in the Kryha cryptograph, to provide a key stream with a very long period. It was hoped that this device would prove to be similar to the actual cryptograph used by J.F.Byrne to create the cipher exhibits which were published in his autobiography, Silent Years. Extensive testing has so far failed to establish the truth of this conjecture. However, the design suggests that a small, multi-disk system could be built that would generate a much more effective key stream than either the Wheatstone or the Kryha. Thus the design presented here provides the first evidence that Byrne's "cigar box" cryptograph was a multi-disk system, perhaps very similar to the device in FIGURE 1.

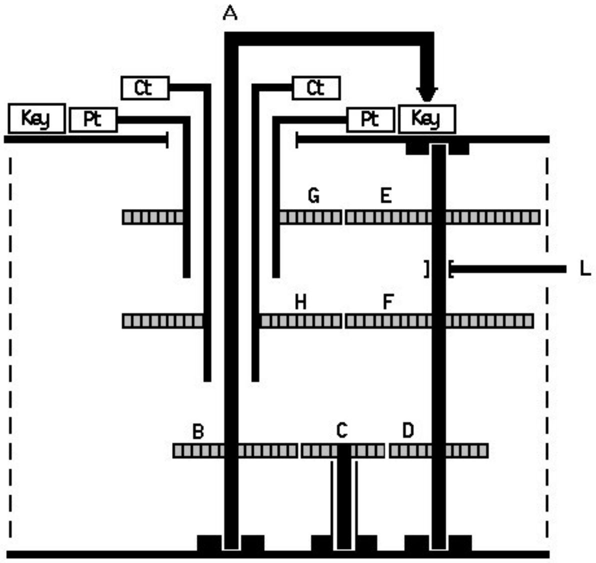

Figure 1. Hypothetical Byrne Cryptograph

MECHANICAL DESCRIPTION

The Key Selector, A, points to a stationary mixed alphabet, called the Key Alphabet, that is arranged in a circle with the shaft of the Key Selector at its center. The shaft of the Key Selector passes through the hollow, concentric shafts of two rotating disks, each of which has a mixed alphabet inscribed along its circumference. A key text, such as A GLIMPSE OF CHAOS, determines the sequence of key letters selected when enciphering and deciphering with the device. As the Key Selector is moved from one key letter to the next, the two rotating alphabet disks are realigned to produce a new alphabet tableau. The Key Alphabet contains at least one null character in addition to the twenty-six letters of the English alphabet so that it will have a longer cycle than either the Plain or Cipher alphabets.

As the Key Selector turns, it transmits motion to the rotating disks through the Gears B, C, D, E, F, G, and H. C is an idle gear which compensates for differences in the diameters of the other gears. Gears B and D are the Wheatstone components of the design, with D completing 1 and 1/(26+M) revolutions for each revolution of B, where M is the number of null characters in the Key Alphabet. Gears E and F are the Kryha components, each having a variable number of sectors and each sector having a variable number of teeth, as outlined in TABLE 1.

Gear	Number of Sectors	Number of Teeth per Sector	Number of Teeth per Gear
B Key	26 + M	N	(26 + M)*N
C Idler	26	N	26N
D	26	N	26N
E Pt	S	Ai	A1+A2+...+As
F Ct	T	Bj	B1+B2+...+Bt
G Pt	26	N	26N
H Ct	26	N	26N

TABLE 1. GEAR SPECIFICATIONS. M,N >= 1. Ai,Bj > N.

A lever, L, is used to lift the shaft of gears E, F, and D, thereby disengaging them from gears G, H, and C, so that the two rotating alphabet disks can be set to an initial tableau, perhaps determined by the first two letters of a key text. For example, if the key text is A GLIMPSE OF CHAOS, the initial tableau could be the one in which $A_p = G_C$. It should also be noted that after the initial tableau is specified the encipherment could be autokey, with either the plaintext or the ciphertext from one tableau becoming the key letter which determines the next tableau.

DISCUSSION

The hypothetical Byrne cryptograph described above is a logical extension of the Kryha cryptograph just as the Kryha is a logical extension of the Simple Progressive. The Simple Progressive consists of a fixed outer disk inscribed with the plain alphabet and a movable inner disk inscribed with the cipher alphabet. As each letter of the plaintext is replaced by a cipher letter, the inner disk is shifted one letter position so that a new tableau is displayed for the next substitution. Assuming that the cipher alphabet is normal (although it would usually be mixed) and that the "A" Key (that is, the tableau in which $A_p = A_c$) has been selected as the starting key, then the progression of the Keys during a typical encipherment is illustrated in FIGURE 2.

Key Shift:	-	+1	+1	+1	+1	+1	+1	+1	+1	+1	+1	+1	+1
Key:	A	B	C	D	E	F	G	H	I	J	K	L	M ...
Pt:	A	L	L	G	O	O	D	Q	Q	U	I	C	K ...
Ct:	A	M	N	J	S	T	J	X	Y	D	S	N	W ...

FIGURE 2. SIMPLE PROGRESSIVE ENCIPHERMENT.

After twenty-six Key shifts, the Key cycle repeats, rendering the Simple Progressive very insecure. The Kryha improves on this by using a shifting wheel divided into sectors with each sector having a variable number of gear teeth. The regularity of the Key cycle is disrupted, as in FIGURE 3, but the Kyrha remains insecure due to the fact that progression from one sector to the next remains regular and the key alphabets will therefore repeat at regular (although fairly long) intervals.

```
Sector Shift:  - +1 +1 +1 +1 +1 +1 +1 +1 +1 +1 +1 +1
Sector:       S1 S2 S3 S4 S5 S6 S1 S2 S3 S4 S5 S6 S1
Key Shift:     - +3 +1 +2 +2 +3 +1 +3 +1 +2 +2 +3 +1
Key:           A  D  E  G  I  L  M  P  Q  S  U  X  Y  ...
Pt:            A  L  L  G  O  O  D  Q  Q  U  I  C  K  ...
Ct:            A  O  P  M  W  Z  P  F  G  M  C  Z  I  ...
```

FIGURE 3. KRYHA ENCIPHERMENT (SIX SECTOR SHIFT WHEEL).

The Kryha can produce key cycles one thousand or more characters in length (compared to the Simple Progressive key cycle of twenty-six characters), but given enough cipher text it will yield to index of coincidence analysis. The cryptograph of FIGURE 1 improves on the Kryha by disrupting the regularity of the Sector shift, as illustrated in FIGURE 4 (which assumes a normal Key Alphabet with one null character between Z and A, or twenty-seven characters in all). The length of the Sector cycle is limited only by the length of the Key text, which could just as easily be the entire plaintext message itself (plaintext autokey) or the ciphertext (ciphertext autokey).

```
Key Text:  A  G  L   I  M  P  S   E   O   F   C  H   A   O  S  A
Ordinal:   1  7 12   9 13 16 19   5  15   6   3  8   1  15 19  1

Sector
Shift:     - +6 +5 +24 +4 +3 +3 +13 +10 +18 +24 +5 +20 +14 +4 +9

E Sector: S1 S1 S6  ...  (Six Sectors)
F Sector: T1 T7 T5  ...  (Seven Sectors)
Key:      A1 A7 A12 ...
Pt:       A  L  L   ...
Ct:       A  Q  Z   ...
```

FIGURE 4. SECTOR SHIFTS OF THE HYPOTHETICAL BYRNE CRYPTOGRAPH.

From another point of view, what the device is doing is sampling the key stream at irregular intervals, as illustrated in FIGURE 5.

```
             ----------- +6 ---------> ------- +5 ------->

Key:        [A]  B   C   D   E   F  [G]  H   I   J   K  [L]  M  ...

E Sector:   S1  S2  S3  S4  S5  S6  S1  S2  S3  S4  S5  S6  S1 ...
F Sector:   T1  T2  T3  T4  T5  T6  T7  T1  T2  T3  T4  T5  T6 ...

Key
Stream:     A1  A2  A3  A4  A5  A6  A7  A8  A9 A10 A11 A12 A13 ...

Pt:         A                       L                   L      ...
Ct:         A                       Q                   Z      ...
```

FIGURE 5. BYRNE ENCIPHERMENT (HYPOTHETICAL CRYPTOGRAPH).

Each letter of the Key Alphabet corresponds to one sector of gear E and one of gear F. Moving the Key Selector from A to G produces a continuous stream of Shift Sectors, with each pair of sectors, S_i and T_j, producing one alphabet tableau, A_k. However, this continuous stream of alphabets is only "sampled" at the points that correspond to a key letter from the key text. Since these are spaced at irregular intervals on the Key Alphabet, there is no regular relationship between any two columns of ciphertext, such as those of Exhibit 1.

REFERENCES

Byrne, J. F., Silent Years: An Autobiography with Memoirs of James Joyce and our Ireland, New York: Farrar, Straus and Young, 1953.

POSTSCRIPT

The above article was presented at the American Cryptogram Association's Montreal Conference in August, 1990. Byrne, Deavours, and Kruh had published the article, *Chaocipher Enters the Computer Age,* [Cryptologia, July 1990] just a few weeks before the conference and Kruh himself was present at the conference. My first meeting with him took place when he attended my Chaocipher presentation. During the discussion period that followed, he was asked by ACA President, Bill Sutton, to comment on my analysis. Kruh, of course, could not comment directly and instead gave us a review of his fifteen-year quest for a meeting with Byrne, Jr., and the subsequent publication of the Exhibit 5 Challenge.

My preparations for the Montreal Conference had been completed months before the publication of *Chaocipher Enters the Computer Age* and there was no time to revise my article in light of new information. It was, however, very encouraging to read that the Byrne device had "two revolving disks with the alphabets arranged along the periphery in a complete disorder" and this seemed to be a confirmation of my own analysis. Nineteen years later, after far more extensive analysis, I find that the situation is not quite what I had imagined at the time.

My article attempted to answer the question, "How could a cigarbox cryptograph produce relatively secure ciphertext, such as that found in the four Byrne Exhibits?" The answer that is suggested by the article is that 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. That answer remains valid even today and will be explored in a future article.

I have made a few minor editing changes to the original article for the sake of clarity and to improve the writing style. The article had originally contained several pages of analysis that attempted to deconstruct a number of statements made by Byrne, but I have omitted those pages since I no longer believe that the analysis presented there is relevant today.

FIGURE 1, as it appears above in my original 1989 article, shows gears E and F attached to the same drive shaft. However, for best results gears E and F should be mounted on separate drive shafts on opposite sides of the main drive shaft, A. I presented a more detailed set of drawings at the ACA's 1990 Conference that clarified the cryptograph's actual design. One change made in the drawings was that the Idle gears were replaced with drive belts. These drawings can be found at The Chaocipher Clearing House.

Jeffrey Hill
April 5, 2009