Tanner Strickland

Dr. Bruff

Math 115F

2 November 2010

Unveiling the Chaocipher

Born in Dublin, Ireland on February 11, 1880, John F. Byrne created a cipher called the Chaocipher that has long been categorized with the likes of the Beale ciphers and the Zodiac ciphers because of how difficult it was to break. This cipher, which he created in 1918, remained unbroken until 2010, when Byrne's daughter-in-law was convinced to donate all of his remaining records and notes about the Chaocipher to the National Cryptological Museum. The tool he used to encipher plain text into his Chaocipher involved only a cigar box, string, and several small wheels. According to Byrne, this cipher was unbreakable, and when he made it available to the public, it would prove to be invaluable for communication between government officials, religious institutions, and businesses. Byrne's purpose was to create a cipher that would help everyone, which he states in his autobiography, saying, "What I had in mind .... was a system available for everybody; and I fully believed .... that the really big market for my system would be in the commercial, general correspondence, and literary fields" (Byrne 270). Byrne foresaw his Chaocipher having a huge impact on communication, and he hoped to patent his device so that he could profit from his idea.

In 1919, Byrne approached an attorney named Marcellus Bailey with his design in an attempt to patent it, but Bailey called it little more than a toy and recommended that he have blueprints professionally made.[1] The next year Byrne approached Bailey with these blueprints, but Bailey had little interest in them because they were estimated to cost between $5000 and $20000 to build. Byrne's next attempt was with the Secretary of State, who also expressed his lack of interest in the Chaocipher system. Then, in 1921, Byrne decided to get professional advice on his Chaocipher before marketing it any further, so he sent a sample machine and papers to Colonel Parker Hitt, who was renowned for his

[1] The following history comes from Byrne (264-284).

prowess involving military ciphers. Colonel Hitt was very impressed with Byrne's work and recognized its possible value in the marketplace, but Hitt had no time to look any further into the subject for reasons he did not explain.

Encouraged by Hitt's compliments, Byrne contacted the new Secretary of State about his Chaocipher system. To his surprise, the Secretary of State promptly replied, saying, "The codes and ciphers now used are adequate to [the Department's] needs" (Byrne 274). Undaunted, Byrne wrote another letter to Colonel Hitt, who wrote back, giving Byrne the contact information of a man who might be interested in the Chaocipher. After speaking with this man in person, Byrne waited to hear back from him. When he finally did, all he received was a package with his Chaocipher machine "smashed into smithereens" (Byrne 276). Stung by this last insult, Byrne waited fifteen years before he tried to sell the government his Chaocipher machine again. When he did try again, it was with the Navy, and their suggestion was to check with the Secretary of State to see if he was interested.

With unwavering determination, Byrne published a pamphlet with sections of text in Chaocipher that he challenged the public to decipher. In 1954, when nobody had been able to crack the cipher, he wrote a book called *Silent Years: An Autobiography with Memoirs of James Joyce and Our Ireland* that detailed many of his experiences with famous author James Joyce. However, according to David Kahn, author of *Codebreakers*, "his real reason for writing it was not to shed light on early Joyce, but to get his Chaocipher before a larger audiences" (Kahn 768). The last chapter of Byrne's novel is devoted completely to the Chaocipher and wagers $5000 that in the first three months after publication nobody will be able to decipher the Chaocipher text that is included on the last pages. In addition to the ciphertext, Byrne tells the readers the plaintext, which includes passages from the Gettysburg Address, the Declaration of Independence, and Caesar's *De Bello Gallico*. After Byrne's death a few years later, the Chaocipher slowly developed notoriety for being unbreakable, like the Beale ciphers. It never quite achieved the same level of fame, though, because the acclamation associated with cracking the Chaocipher paled in comparison to the treasure associated with cracking the Beale ciphers.

On May 10, 2010, Byrne’s daughter-in-law discussed donating Byrne’s notes, blueprints of the Chaocipher machine, and a wooden wheel that served as an example of the original machine with the Acquisition Committee of the National Cryptological Museum.[2] Once these things were given to the museum and made public, cryptanalysts quickly uncovered the algorithm that is used to encipher and decipher the Chaocipher. This decipherment of the Chaocipher is important in the modern field of cryptology because it represents an example of a system that is very rudimentary compared to modern encryption systems, but it proved to be indecipherable for close to a century.

To encipher a message into Chaocipher, a tool consisting of two wheels sitting side by side is used (Figure 1). Around the border of each wheel is every letter of the alphabet in a random order. Where they touch, the wheels interlock so that rotating one wheel rotates the other with a ratio of one letter to one letter. The letters on the rim of each wheel are removable, so each alphabet can easily be permuted, which simply means that the order of the letters around the wheels can be changed. Because the process of enciphering the plaintext involves many permutations of the alphabets on each wheel, the cipher text contains such a paucity of noticeable patterns and such an even frequency of ciphertext letters that it withstood the efforts of cryptanalysts throughout the twentieth century.

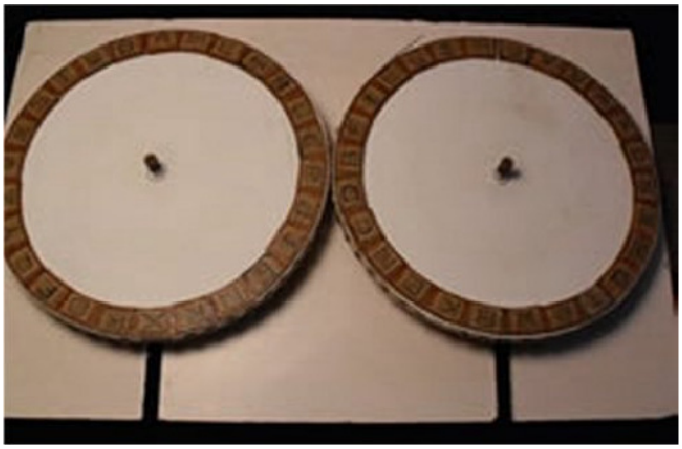

Figure 1. (Ruben 2)

Because these disks are rotated and the alphabets around them are permuted, the Chaocipher is an autokey cipher, which means that the key to encipher the plaintext changes throughout the message.

[2] All current information and updates on the status of the Chaocipher can be found on the National Cryptological Museum’s website.

More specifically, it is known as a text autokey cipher because the permutations of the alphabets depend on the plaintext letter being enciphered and on this letter's position in the alphabet on the rim of the right wheel. It is also a polyalphabetic substitution cipher because the permutations of the alphabets around each disk mean that new alphabets are used to encipher each plaintext letter. Disks are not necessary to perform the algorithm of the Chaocipher, however. It can also be done using a linear model, which represents what is happening on the wheels. First, two alphabets, with letters in a random order, are written linearly and labeled left and right to indicate whether they are located on the left or right wheel when one is facing the two wheels.

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

Two important details to make note of are that the right alphabet is used to show the plaintext letter, and the left alphabet shows the ciphertext letter. The '+' and '*' that are symbols that Byrne referred to as *zenith* and *nadir*, respectively. *Zenith* (+) represents the first letter in the alphabet, and *nadir* (*) represents the fourteenth. To create a Chaocipher, there are three basic steps: match the correct cipher letter to that in the plaintext, permute the left alphabet, and finally, permute the right alphabet.

To match the cipher letter to its plaintext component, one must find the plaintext letter in the right alphabet and then correlate this letter to its partner in the left alphabet. For example, to encipher the letter D, one must find the letter D in the right alphabet and find its partner in the left alphabet, T, which will serve as the cipher letter. This process is shown below.[3]

	+												↓	*												
Left:	Q	A	Z	W	S	X	E	D	C	R	F	V	**T**	G	B	Y	H	N	U	J	M	I	K	O	L	P
Right:	M	Z	N	X	B	C	V	L	A	K	S	J	**D**	H	F	G	P	Q	O	W	I	E	U	R	Y	T

The next step is to permute the left alphabet. To do so, the alphabet is shifted cyclically so that the ciphertext letter that has been chosen is moved to the *zenith* position.

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

[3] This example is adapted from Rubin (2-5).

After this shift is performed, the letter in the *zenith+1* position (G) is removed. This leaves the alphabet with a gap.

	+													*												
Left:	T	.	B	Y	H	N	U	J	M	I	K	O	L	P	Q	A	Z	W	S	X	E	D	C	R	F	V

Next, the letters in the *zenith+2* position (B) all the way through, and including, the *nadir* position (P), are shifted left to fill this gap. This leaves a gap in the *nadir* position.

	+													*												
Left:	T	B	Y	H	N	U	J	M	I	K	O	L	P	.	Q	A	Z	W	S	X	E	D	C	R	F	V

Finally, the letter that was removed earlier (G) is put in the *nadir* position to fill the gap. This completes the permutation of the left alphabet.

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

Once the left alphabet has been permuted, all that remains to do is permute the right alphabet. The first step in this process is the same as the first step in permuting the left alphabet. The right alphabet is shifted left cyclically until the plaintext letter (D) is in the *zenith* position.

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

The next step in permuting the right alphabet differs from the left. Instead of removing a letter, the right alphabet is shifted to the left one more position, putting H in the *zenith* position.

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

Then, the letter two positions to the right of the *zenith*, or in the *zenith+2* position, is removed.

	+													*												
Right:	H	F	.	P	Q	O	W	I	E	U	R	Y	T	M	Z	N	X	B	C	V	L	A	K	S	J	D

After removing the *zenith +2* position, shift everything after the *zenith +2* position and up to the *nadir*, including the *nadir*, left to fill the gap. This should leave a gap in the *nadir* position.

	+													*												
Right:	H	F	P	Q	O	W	I	E	U	R	Y	T	M	.	Z	N	X	B	C	V	L	A	K	S	J	D

Finally, put the letter that was removed in the third step of the permutation (G) into the gap in the *nadir* position.

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

Now, both the left and right alphabets have been permuted and are ready to encipher the next letter of the plaintext. The two alphabets are shown below.

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

To decipher a message that has been written in the Chaocipher, the only step that must be taken differently is the very first step in the process. Instead of locating the plaintext letter in the right alphabet and its corresponding ciphertext letter in the left alphabet, the decipherer locates the ciphertext letter in the left alphabet and matches it with its plaintext correlation. Both alphabets are permutated exactly the same way in deciphering the Chaocipher. The decipherer must know the starting right and left alphabets, however, in order to start deciphering the Chaocipher.

Like the Enigma code in World War II, decipherers had cribs to the Chaocipher, but unlike the Enigma code, nobody was ever able to crack the Chaocipher. Although the enciphering mechanism was much simpler for the Chaocipher, it was able to withstand cryptanalysis for almost a century, and its cribs were much clearer than those that the Allies had during WWII for the Enigma code. Although Byrne, like Vigenere, never received credit during his lifetime for his work, he did make his own impact on the field of cryptology. The Chaocipher proves that complex computers are not necessary to create secure ciphers. All that is needed is creativity to make a system of enciphering plaintext that is secure against frequency analysis, even if it is rudimentary compared to the ciphers created by modern computers. Today, the main use of the Chaocipher is in personal correspondence because the algorithm can be run as a software program, making it a quick way to encipher plaintext in a secure fashion for those who lack the supercomputers necessary for more complex, modern ciphers[4]. While there was not the same level of pressure to crack the Chaocipher as there was to crack the Enigma code, the Chaocipher has still earned its place among famous codes and ciphers because it illustrates the efficiency and value of simple creativity in the field of cryptology.

[4] Rubin (6)

References

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

National Cryptologic Museum Foundation. "Chaocipher Machine and Papers." *National Cryptologic Museum Foundation Website*. 27 May 2010. Web. 01 Nov. 2010. <http://www.cryptologicfoundation.org/content/Direct-Museum-Support/recentacquisitions.shtml#Chaocipher>.

Kahn, David. *The Codebreakers*. New York: Sphere, 1967.

Rubin, Moshe. "Chaocipher Revealed: The Algorithm." *Mountain Vista Soft*. 2 July 2010. Web. 20 Oct. 2010. <http://www.mountainvistasoft.com/chaocipher/ActualChaocipher/ Chaocipher-Revealed-Algorithm.pdf>.