Tyler Merrill

Dr. Bruff

October 26, 2010

Chaocipher

Throughout history, humans have sought to keep information private. The need for confidentiality ranges from covering personal relationships to concealing military actions. As cryptanalysts became more adept at solving ciphers, those who needed secrecy were forced to innovate new methods. Thus, encryption became more complex as old methods were decrypted. Encryption evolved from manual methods such as Caesar Shifts to mechanical devices, such as the Enigma Machine. Messages encoded using John Byrne's cryptographic method, Chaocipher, published in his autobiography *Silent Years*, have yet to be solved. Byrne's system could have possibly ensured the privacy of all communication across the world.

In his essay, "Cryptography", Edgar Allan Poe wrote, "It may be roundly asserted that human ingenuity cannot concoct a cipher which human ingenuity cannot resolve." John Byrne refused to believe this and so began his struggle to design an indecipherable cryptographic system. To create such a cipher he realized that **"**…the only cipher which would be materially and mathematically indecipherable is one which would…be devoid of discernable order, or design"(Byrne 270). Byrne's implicit acknowledgment of the usefulness of patterns in cryptanalysis shows the potential for brilliance in his design. If he could successfully design a system lacking patterns, he would have an unbreakable cipher, barring human error in usage.

Because a model constructed by Byrne is not available today, a reconstruction of the device by Byrne's son, John, and the blueprints, which were not available until recently, must be used to gain insight into the Chaocipher. The Chaocipher device contained two discs with jumbled, moveable alphabets along the border. To encode, the right disc is used to find the plaintext, then the letter in the corresponding position is found on the left disc; this is the enciphered letter. After this, the left alphabet would be altered, then the right. Again, the plaintext letter would be found on the right disc and the letter in the corresponding location on the left disc is recorded as the ciphertext. These discs touched so that when one disc was rotated, the other rotated in the opposite direction with a one letter: one letter ratio (Rubin "Chaocipher Revealed" 2). For example, when the left disc rotates clockwise two letters, the right disc rotates counterclockwise two letters. The true cryptographic power lies in the permutations made after encryption of one letter. Each alphabet is altered in a slightly different way. The cipher essentially uses a different monoalphabetic substitution cipher for every letter.

The following directions follow Moshe Rubin's paper, "Chaocipher Revealed: The Algorithm. Typically, the left disc is rearranged first, but as long as sender and receiver both follow the same patter, left, right or any combination could be used (Rubin "Chaocipher Revealed" 3). First, shift the alphabet so that the letter that was just enciphered is at the zenith (first position). Next, remove the letter to the right of the zenith (zenith+1). There should be a gap where the letter was. Now the letters from zenith+2 to nadir (fourteenth position/zenith+13) are moved one to

the left. Now the gap is at the nadir. The extracted letter now fills the empty nadir position. Shown linearly without disc rotation, the process looks like this:

For this example, the letter “P” is enciphered for the plaintext “Q”

The ZENITH letter will be highlighted yellow; the NADIR letter will be highlighted purple. The plaintext being enciphered and corresponding ciphertext will be highlighted green. represents a gap.

The original alphabets are

Left: QWERTYUIOPLKJHGFDSAZXCVBNM
Right: POIUYTREWQASDFGHJKLMNBVCXZ

Step 1: Shift the left alphabet to get P at zenith.

PLKJHGFDSAZXCVBNMQWERTYUIO

Step 2: Remove zenith+1, L.

P★KJHGFDSAZXCVBNMQWERTYUIO

Step 3: Shift letters from zenith+2 to nadir one to the left.
This moves the gap to the nadir position.

PKJHGFDSAZXCV★BNMQWERTYUIO

Step 4: Put the extracted letter in at nadir.

PKJHGFDSAZXCVLBNMQWERTYUIO

The right disc is then enciphered, and the process repeats.

The right disc follows a similar pattern of encryption. The alphabet is shifted so that the letter just enciphered is at the zenith. The alphabet is then shifted one more position to the left. The letter at zenith+2 is removed and the alphabet from zenith+3 to nadir is shifted one letter to the left to fill the void. The letter

removed is now inserted at the nadir position. Again, the process will be demonstrated linearly without the effect of disc rotation.

For this example, use the same alphabets as above.

Left: QWERTYUIOPLKJHGFDSAZXCVBNM
Right: POIUYTREWQASDFGHJKLMNBVCXZ

Step 1: Shift cipher so Q is zenith.

QASDFGHJKLMNBVCXZPOIUYTREW

Step 2: Shift the alphabet one letter to the left. Q becomes zenith-1.

ASDFGHJKLMNBVCXZPOIUYTREWQ

Step 3: Remove the letter at zenith+2, D.

AS★FGHJKLMNBVCXZPOIUYTREWQ

Step 4: Shift the alphabet from zenith+3 to nadir one letter to the left. The gap is now at nadir.

ASFGHJKLMNBVC★XZPOIUYTREWQ

Step 5: Insert D at nadir.

ASFGHJKLMNBVCDXZPOIUYTREWQ

Now, the next letter is found on the right disc, and its corresponding ciphertext letter is found on the left disc. The message is encoded following this process.

The Chaocipher device, much like the Enigma Machine, is an ingenious attempt to integrate technology into cryptography. Both were invented around the same time and both created ciphers that were much more difficult to crack than previous manual ciphers. The Enigma and Chaocipher utilize multiple alphabets to encode messages. This is derived from the Vigenere cipher, but instead of static alphabets, the Enigma and Chaocipher utilize dynamic alphabets that change after

each letter is encoded. This helps to eliminate patterns and isomorphism, a mapping that shows a relationship between two objects (Wolfram Alpha). Though the Enigma and Chaocipher utilize different methods of altering the alphabet, both produce comparable results. The Chaocipher however, had little affect on history. It was never commercially produced or utilized by the government. It was never used in war and very few people tried to crack it. Though the Chaocipher is not universally recognized, it still produced a complex cipher.

One distinction must be drawn between the Enigma machine and the Chaocipher device. The Chaocipher device uses an autokey system, but the Enigma does not. This means that the message plays a part in the key used. Because the key is changed after each letter is encrypted, and is changed in relation to the letter encrypted, the new key will be different depending on the letter previously encoded. When deciphering, this means that even if the initial alphabet is known, the whole message must be decoded flawlessly, letter by letter. One incorrect move will render the message useless. The Enigma machine does not posses this protection. Once the initial key is set on an Enigma Machine, the key of any letter at any position enciphered can be determined. This added complexity might have been an advantage of the Chaocipher. However, this could have also hindered the efficiency of the machine. The permutations after every letter are much more complex than a simple rotation of a rotor of the Enigma machine. Byrne's device may have sacrificed some speed for enhanced security.

While Byrne valued secrecy, he also valued ease of use. He aimed to create a device that anyone could use and use effectively. Commercial, not

militaristic, motives inspired Byrne. He explains his intentions in his autobiography, "I aimed at supplying for one and all a method and a means for conveying his or her thoughts in such a way that he or she could be absolutely assured that only the recipient would be able to read them"(Byrne 270-271). He sought to ensure the confidentiality of communications worldwide. In an attempt to bring his device to the global market, he consulted with attorney, Marcellus Bailey. Bailey recognized the cryptographic strength of the machine, but said, "…it is scarcely more than a toy"(Byrne 266). Byrne then collaborated with a draftsman to design blueprints for potential patent approval. He asked for estimates of the cost of production of the machine; they ranged from five thousand to twenty thousand dollars per machine. Byrne was unable to start production because of this cost.

After realizing that he would need a partner in this venture, he began to explore other markets. He met with the Secretary of State in 1920 to demonstrate the machine, but the State department turned him down. In 1921 a new Secretary of State was appointed, however, Byrne was not allowed the opportunity to demonstrate his machine. Around this time, Byrne also explored militaristic implementations of the Chaochipher. He contacted Colonel Parker Hitt, author of the booklet, "Manual for the Solution of Military Ciphers." Hitt acknowledged the effectiveness of the device, but said he did not have the time to continue looking into this machine. In 1922, Hitt arranged a meeting between Major Frank Moorman, W.M. Freidman, and Byrne. Moorman was a pupil of Hitt and Friedman was a cryptanalyst. This encounter also proved fruitless. These unproductive meetings kept Byrne dormant for fifteen years. When the US Navy published an

advertisement in the newspaper requesting, "…congressional appropriation 'for the development of a system of Cryptography by which warships can transmit signals to another vessel in the fleet which cannot be deciphered by an enemy vessel'"(Byrne 277), he constructed a model of his machine to show the Naval Department. However, his model fell short of a design that included a keyboard and printing device (Hill 1). The first record of Byrne's machine comes from Henry Langen, editor of the American Cryptogram Association's magazine, "The Cryptogram"(Hill 2). Byrne showed the blueprints to Langen, who questioned how the device could be successful with only two rotors (Hill 2). Byrne described this design as "made up somewhat like a typewriter"(Hill 2). This means one of two things: either Byrne modified his design after the rejection of the Naval Department, or he did not fully construct his design for the Naval Department. His new device could have been designed to expedite encryption and decryption. A keyboard and output device could have been integrated into an initial design in response to the Naval Department's decision. On the other hand, because his model would have cost between five thousand and twenty thousand dollars to construct in 1919-1920, it is plausible that he built a less complex model to demonstrate his cipher to the Naval Department. This could also be a component of their decision. They may not have believed that Byrne's device could efficiently encipher and decipher data because he presented an abbreviated machine. Byrne again went inactive in the propagation of his device. In 1953, Byrne dedicated the final chapter of his autobiography to the Chaocipher. He issued a challenge in the final pages offering five thousand dollars to anyone who could solve a message at the end of his book that was enciphered with

the Chaocipher. That message remains unsolved (Byrne, Deavours, Kruh 196 and Rubin “What is Chaocipher”).

The fact that the Chaocipher has not been broken could be attributed to the superiority of the device, or perhaps to the lack of use. Byrne’s ingenuity could have potentially proved useful either to replace cracked systems or as the initial cipher utilized by the US Government. Byrne could never find a niche for his invention, but nonetheless it is a noteworthy advancement in cryptography.

Works Cited

Byrne, J. F. *Silent Years; an Autobiography with Memoirs of James Joyce and Our Ireland.* New York: Farrar, Straus and Young, 1953. Print.

Byrne, John, Cipher Deavours, and Louis Kruh. "Chaocipher Enters The Computer Age When Its Method Is Disclosed To Cryptologia Editors." *Cryptologia* 14.3 (1990): 193-98. Print.

Hill, Jeff. *Chaocipher: Analysis and Models*. Rep. 2010. Print.

"Isomorphism -- from Wolfram MathWorld." *Wolfram MathWorld: The Web's Most Extensive Mathematics Resource*. Web. 02 Nov. 2010. <http://mathworld.wolfram.com/Isomorphism.html>.

Rubin, Moshe. *Chaocipher Revealed: The Algorithm*. Rep. 2010. Print.

Rubin, Moshe. *What Is Chaocipher?* Rep. 2010. Print.