Aubrey

Dr. Bruff

Math 115F

2 November 2010

The Wheel Cipher

One of the most secure, yet simple enciphering devices in the history of cryptography is the Wheel Cipher, also known as the Jefferson disk or the Bazeries cylinder. This instrument was invented by Thomas Jefferson in the late 18th century, and was later independently reinvented by Commandant Etienne Bazeries one hundred years later. The Jefferson disk provided unrivaled security during the time of its birth and rebirth, thus making it effective for encrypting confidential military and diplomatic communication. In addition, the decryption of a message enciphered using the Jefferson disk is very difficult and relies on having certain information. The Jefferson disk cipher is remarkable, because of its high level of security, relative simplicity, and longevity.

Thomas Jefferson first designed the Jefferson disk cipher in 1795 (Reuvers and Simons). Jefferson's plans outline the construction and use of the device. The device is constructed by cutting wooden disks of equal diameter. The next step is to divide the edge of each disk into 26 equal sections and carve a different letter into each section in a random order. Each disk should be given a number, so that the different orders of the disks can be recorded. This process is repeated until the desired number of disks has been reached. The advantage of having more disks is that the number of possible combinations greatly increases with each additional disk. This makes the cipher less susceptible to brute force attacks. Jefferson's model used 36 disks.

Finally, a hole is carved through the center of each disk so that each is free to rotate along an axle. To encrypt, the sender must take note of the ordering of the disks by checking the assigned numbers of each one. The sender then spells out the message in a row across the device, using one letter from each disk. Then, the sender writes down the text from any one of the other 25 rows. This is the cipher text, which will have no apparent meaning or coherence to an unintended recipient. To decrypt the message, the recipient must have the same device with identical disks. The recipient arranges the disks on the axle in the same order as they were when the message was encrypted. The order of the disks should be agreed upon before the transmission of the cipher text, because this is key information to decrypting the message. If a third party were to intercept this information, it could make the cipher text vulnerable to decryption. Once the disks are in their proper order, the recipient spells out the cipher text in one of the horizontal rows. This will cause the plaintext to be spelled out on another row. The recipient then simply has to look at the other rows to find the spelled out plaintext. This process of encrypting and decrypting communication was quick, straightforward, reliable, and highly secure. Because this enciphering device had two, independent inventions, the alternate version is worth mentioning.

Commandant Etienne Bazeries was a cryptographer for the French military during the late 19th century and early 20th century. He gained recognition for his natural talent in the field of cryptography and eventually worked his way up to a position in the Bureau de Chiffre (Candela). Bazeries developed and designed his Bazeries cylinder in virtually the exact manner Jefferson did. He recognized the strength of the cipher, however it did not catch on until it was adopted by the U.S. Navy during World War I. Captain Parker Hitt of the U.S. Navy played with

designs for a Bazeries cylinder and eventually developed a new model. After some additional edits, the device, known as the M-94, was finalized. Other than the fact that it was made of aluminum, the M-94 was essentially the exact same device Jefferson had designed over 100 years earlier. The fact that the wheel cipher was redeveloped over a century later proves the cipher's strong security and longevity.

Though Jefferson's invention would have provided unmatched security during its time, little is known about its use during this time. There is no known record of Jefferson using his invention. However, this does not rule out the possibility that it was used but kept under wraps, given the secretive manner of the use of cryptography. There are a few potential explanations for why Jefferson never took advantage of his powerful enciphering system. Some assert that it would have been tedious to make exact replicas of the device, which would be needed for deciphering a message. Furthermore, it would have been difficult and risky to distribute the devices to the intended recipients. Others argue that Jefferson already used an encryption method for his communication that was sufficiently secure and more efficient for his needs (Mussulman). However, Bazeries reinvention and Captain Hill's subsequent development of the Jefferson disk sparked interest in the cipher and popularized its use. The idea was introduced to the Signal Corps Engineering and Research Division, until it eventually found its way to the U.S. Army, U.S. Navy, the U.S. Coast Guard, and the Radio Intelligence Division of the Federal Communications Commission (Kahn). The device was used effectively, frequently, and reliably throughout World War I, all the way up to the end of World War II to securely transmit military communication. As World War II drew to an end, holes in the security of the Bazeries cylinder were finally discovered and exploited by the Germans. In the proverbial encryption race, the

code breakers caught up to the code makers and eventually overtook them as they found flaws in the cipher and more reliable methods to decipher it.

The notion that a given cipher text could possibly be deciphered by using trial and error in a timely manner can easily be dispelled by examining the number of possible configurations of the disks. The number of possibilities depends on the number of disks used. If 10 disks are used, the number of possibilities of different disks to be used as the first is 10. The number of possibilities of different disks to be used as the second is then 9, because one disk is already in use. The number of possibilities decreases by one each time an additional disk is added until all 10 disks have been added. This number can be represented by:

10 x 9 x 8 . . . 2 x 1, or 10! = 3,628,800

In this case, using 10 disks creates 3,628,800 different combinations of disk orderings. Using 25 disks, as Bazeries proposed, yields 25!, or15,511,210,043,330,985,984,000,000 possibilities. If every German in 1946 were to compute a different possibility at a rate of one combination per second, it would take

$$\frac{25!}{60 \text{ sec.x } 60 \text{ sec.x } 24 \text{ hrs.x } 365 \text{ days x } 64{,}500{,}000 \text{ ppl}} = 7{,}625{,}693{,}704 \text{ years}$$

to try every possibility. Clearly, the cipher is unsolvable using trial and error. The first and main attack against the Bazeries cylinder is known as the de Viaris method. This method decryption relies on letter orderings on a disk that are not random. If a third party intercepts the message and has a copy of the disks used to encode a message, it may be possible to determine the

displacement from the cipher text letter to the plaintext letter. This could then be used to facilitate the process of determining the order of the disks (Savard). The de Viaris method requires that there be a fault in the disks and therefore, is unreliable. Another method that can be used to crack the Bazeries cylinder is the kappa test. The kappa test relies on the fact that "two unrelated plaintexts will have more identical characters in corresponding positions than two sequences of random letters, which will have one coincidence for every 26 letters" (Savard). This information can then be used to determine the displacement of the plaintext letter from the cipher text letter. However, the code breaker would have to have several hundred messages for the kappa test to be effective. This requirement also makes the kappa test unreliable. Yet, the Bazeries cylinder's vulnerabilities could not be ignored due to the high importance of the messages it encoded. Because of this, the Bazeries cylinder went out of fashion at the end of World War II as other forms of cryptography took over.

The wheel cipher made a significant contribution to the history of cryptography. It was the last major cipher to be simple to construct and use, but remain secure. Because of these attractive traits, the wheel cipher played an important role in both World War I and World War II. The decryption of wheel cipher codes would have been a daunting task for a code breaker in the first half of the 20th century. The wheel cipher's user friendliness and security during a time of great technological advancement merit it recognition as one of the most efficient ciphers in the history of cryptography.

Works Cited

Candela, Rosario. *The Military Cipher of Commandant Bazeries.* New York: Cardanus Press, 1938.

Kahn, David. *The Code Breakers: the Story of Secret Writing*. New York, NY: Signet Book, 1973.

Mussulman, Joseph. "Jefferson's Wheel Cipher." *Discovering Lewis & Clark*. Jan. 2009. Web. 31 Oct. 2010. <http://lewis-clark.org/content/content-article.asp?ArticleID=2224>.

Reuvers, Paul, and Marc Simons. "Jefferson Disk." *Crypto Museum*. 2009. Web. 01 Nov. 2010. <http://www.cryptomuseum.com/crypto/usa/jefferson/index.htm>.

Savard, John. "The Bazeries Cylinder." *A Cryptographic Compendium*. 1998. Web. 31 Oct. 2010. <http://www.quadibloc.com/crypto/jscrypt.htm>.