Rob Rice

FYWS Cryptography

2 November 2010

The M-209 Cipher Machine

What does a person beg to have, but then immediately want to give away? The answer is a secret. In our daily lives, most of us only deal with minor, personal secrets that rarely have drastic consequences if leaked. But what about secrets concerning matters of national security? Even a small secret can be a powerful thing in the hands of the enemy, especially in times of war. In war, having a secure method of communication is invaluable. Knowing the enemy's next move is a nearly insurmountable advantage, while being unable to shield communications from the enemy could prove fatal. The quality of a nation's cryptography can be the difference between winning and losing a war. World War II provides some of the best examples of the monumental power of cryptography. The success of cryptanalysts at Bletchley Park in deciphering Enigma-enciphered messages prevented Germany from dominating naval combat on the Atlantic Ocean. American cryptanalysts gave U.S. forces the element of surprise at the Battle of Midway by deciphering a message enciphered using Purple, the Japanese cipher machine.[1] The Allies depended on deciphered German messages regarding troop positions along the French coast to form their invasion plans for D-Day.[2] The importance of ciphers in the Second World War is indisputable. However, to fully appreciate a good cipher, one must understand its history and the way it works. This is certainly the case for the M-209, a cipher machine used by the U.S. military in World War II. Despite the fact that over 140,000 of them were produced, the M-209 is one of the lesser-known cipher machines.[3] In fact, the origin, mechanics, field use, and decipherment of the M-209 make it a particularly interesting example of cryptographic technology in World War II.

There is a unique story behind the development of the M-209. The inventor of the machine was the Boris Hagelin, a Switzerland native. Hagelin, a mechanical engineer, started his cryptography career in 1925 as manager of a Swiss company called A.B. Cryptoteknik, which produced mechanical cipher machines.[4] In 1934, the French Cipher Bureau contacted the Swiss cryptographer with the request that he develop a small, compact cipher machine that could print messages.[5] In response to the French request, Hagelin developed several prototypes before coming up with his final product in 1938. He christened this cipher machine the C-38. The C-38 was originally adopted for use by the Swiss military, but the Swiss did not use it extensively. [6] Following the outbreak of World War II, Hagelin recognized the opportunity to market his product to other countries, including the United States. In 1940, he smuggled two of his C-38 machines to the United States. He did so with the help of the Swiss Foreign Office—the machines were concealed in a diplomatic pouch that was exempt from searches.[7] The U.S. Army Signal Corps purchased rights to the C-38. Army engineers made several mechanical and structural alterations to the C-38 and renamed it the M-209. The M-209 was mass produced in the U.S. by the manufacturing company Smith-Corona at a cost of approximately 64 dollars per machine. Thus, the M-209 was ready to be used in the field, and was first put to use during the African invasion of November 1942.[8]

The M-209 was favored by the army because it was compact, light, and easy to use. To encipher a message, an operator would first address the six wheels on top of the box. Each wheel displayed a letter of the alphabet, so the operator would adjust the wheels to create a six-letter key for encipherment. Encipherment keys were changed daily. Next, the operator set the "encipher-decipher" switch on the side of the box to "encipher". Then, he would rotate the indicator knob, which was labeled with the 26 letters of the alphabet, to the first letter he wished to encipher. Finally, the operator pushed down on a lever on the right side of the box, called the power handle. This printed out the enciphered letter on a strip of paper that spooled out of the top of the box. This process was repeated for the rest of the letters in the plaintext message. There was a convenient counter on top of the box that showed how many letters had been enciphered, so that the operator would not lose track of his place in the message. Once the entire message had been enciphered, the printout of the ciphertext could easily be read and transmitted to the intended recipient via Morse code. Decipherment of the message was similarly simple. The operator on the receiving end set the six wheels to the proper key for the day, turned the switch to "decipher", entered the ciphertext letter on the alphabet knob, and hit the power level to print the plaintext letter. The process of deciphering the message only took 2-4 seconds per letter, allowing for fairly quick transmittance even in battle situations.[9] As with the famous code used by the Navajo code talkers, messages could be transmitted in a short amount of time. This sense of urgency is a common theme in military cryptography, and the speed of the M-209 contributed to its popularity.

In contrast to its simplicity of use, the inner workings of the M-209 were highly complex. The basic method of encipherment was Caesar shift that depended on settings of the internal print wheel. The variation in which Caesar shift was used came from changes in the alignment of the print wheel. Shifting the print wheel was done by two primary mechanisms: six pin wheels and a lug cage. The six pin wheels were labeled with letters, and were the source of the visible letters of the key. During the setting of the key, each wheel could be rotated individually. However, during encipherment, each push of the power lever caused all the wheels to rotate one place. Each of the six wheels had multiple pins running through it, which could be pushed to the right to make them operational, or the left to disable them. Operational pins had an effect on the ciphertext, while disabled ones did not. The operator had to adjust the pins to a newly designated setting every day, week, or month, depending on the circumstances.[10] The key aspect of the wheels was that each wheel had a different number of pins. From left to right, the number of pins per wheel was: 26, 25, 23, 21, 19, and 17. The number of pins corresponded to the number of letters engraved on the wheel, as follows:

Pinwheel I: ABCDEFGHIJKLMNOPQRSTUVWXYZ
Pinwheel II: ABCDEFGHIJKLMNOPQRSTUVXYZ
Pinwheel III: ABCDEFGHIJKLMNOPQRSTUVX
Pinwheel IV: ABCDEFGHIJKLMNOPQRSTU
Pinwheel V: ABCDEFGHIJKLMNOPQRS
Pinwheel VI: ABCDEFGHIJKLMNOPQ

So, the arrangement of wheels repeated itself only after (26 * 25 * 23 * 21 * 19 *17 =) 101,405,850 letters have been enciphered.[11] The second part, the lug cage, sat behind the pin wheels. The lug cage consisted of 27 horizontal bars held between two disks. On each of the 27 bars there were 2 lugs, which could be set in 2 of 8 available positions. Lug positions 1 through 6 lined up with the 6 pin wheels, so that the rotation of the pin wheel caused the pin to hit the lug, shifting that bar of the cage to the left. The other 2 lug positions were both marked “0”. The first 0 was located between positions 1 and 2, and the other was between positions 5 and 6. Because they were not lined up with a wheel, these “neutral lugs” did not interact with the pins, so they had no effect on the rotation of the lug cage.[12] The position of the lug cage bars ultimately determined the key for the shift of the print wheel, which in turn printed the enciphered letter on the paper. The math behind this process was as follows:

Ciphertext letter value = (key value -1) - (plaintext letter value)

In this equation, the cipher letter and plain text letter were represented by a number mod 26, so that letter values ranged from 0 to 25. The key value was a product of the variable settings and effects of the pins and lugs. Because the pin wheels rotated after each press of the power lever, the key value changed for each letter. The following is a demonstration of the math used to encipher the seven-letter plaintext word HAGELIN using a possible set of generated key values:

Plaintext Letter	Plaintext Letter Value	Key Value	Ciphertext Letter Value = (key value -1) - (plaintext letter value)	Ciphertext Letter Value mod 26	Ciphertext Letter
H	7	12	4	4	E
A	0	18	17	17	R
G	6	23	16	16	Q
E	4	18	13	13	N
L	11	9	-3	24	Y
I	8	18	9	9	J
N	13	11	-3	24	Y

So, the plaintext HAGELIN would be enciphered and printed as ERQNYJY.

The M-209 worked in the same way to decipher an enciphered message. The original equation can be rewritten as:

Plaintext letter value = (key value -1) - (ciphertext letter value)

To work in this direction, the “encipher/decipher” switch was set to “decipher”. Doing so reversed the direction of the print wheel offset, which had the effect of translating the ciphertext letter back to the original plaintext letter.[13] It is interesting to note that this entire mechanical system operated without electricity—it used only the energy provided by the work done in pressing the power lever. The machine was also very light. These two factors made the M-209 fully portable, unlike other, bulkier, electric cipher machines such as Enigma. This connects to another common theme in cryptography: often, cryptographers must adapt their creations to fit particular conditions. In this case, the M-209 was engineered specifically for use on the battlefield, where there was no electricity and the machine had to be constantly carried. The light weight and electricity-free operation of the M-209 made it well suited to this environment.

Unfortunately, though it was a popular choice for use in the field, the M-209 system of encryption was not perfect. Unlike messages encoded using the formidable SIGABA, its messages could be decrypted by hand with relative ease once the enemy gained knowledge of the physical mechanisms of the machine. The Germans managed to procure several M-209s, thereby giving them a chance to become familiar with the way it worked. With this knowledge, the Germans eventually discovered that certain settings of the M-209, especially sections of text greater than 150 characters, yielded patterns that could be analyzed to deduce the positions of the pins and lugs, and subsequently enable them to decode the message using one of their M-209s. [14] This process, however, was far from instantaneous. It still took the Germans a fair amount of time to decipher an intercepted message that had been encoded by an M-209 machine. For this reason, the M-209 was mostly limited to use in tactical situations in which the messages transmitted would be acted on immediately by the receiver. In this way, the U.S. ensured that even if a message were to be deciphered, it would be too late to be of any benefit to the enemy. For these purposes, it remained quite useful. In fact, the M-209 continued to be used through the Korean War, by the United States as well as other nations using different variants of Hagelin's original C-38 design.[15]

Overall, the unique origin, clever design, ease of use, and longevity of the M-209 make it worthy of recognition alongside such cryptographic marvels as Enigma and SIGABA. This machine was a valuable part of the Allies' cryptographic victory in World War II. Today, it serves as an inspiring blend of complex mathematics, intricate engineering, and practical design. Boris Hagelin would undoubtedly be proud to see the place in history that his creation has earned.

Endnotes

[1] Singh, Simon. *The Code Book*. New York: Anchor, 2000. 191. Print.

[2] Singh, 185-186.

[3] Goebel, Greg. "Boris Hagelin & The M-209." *Codes, Ciphers, & Codebreaking*. 1 Jan. 2009. Web. 27 Oct. 2010. <http://www.vectorsite.net/ttcode_09.html#m4>.

[4]Rijmenants, Dirk. "History of the Hagelin Cipher Machines." *Cipher Machines and Cryptology*. Web. 27 Oct. 2010. <http://users.telenet.be/d.rijmenants/en/hagelin.htm>.

[5] Goebel.

[6] Andersson, Torbjörn. "The C-38 / M-209 Cipher Machine." *Passagen*. Web. 27 Oct. 2010. <http://hem.passagen.se/tan01/c38.html>.

[7] Torbjörn.

[8] Proc, Jerry. "M-209." *Crypto Machines*. Web. 27 Oct. 2010. <http://www.jproc.ca/crypto/m209.html>.

[9] Goebel.

[10] Churchhouse, R. F. "The M209 Cipher Machine: a War of Words." *IEE Review* 39.4 (1993): 173-75. *IEEE Xplore*. Web. 27 Oct. 2010. <http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=00229385&tag=1>.

[11] Goebel.

[12] Churchhouse.

[13] Goebel.

[14] Schmeh, Klaus. "Als Deutscher Code-Knacker Im Zweiten Weltkrieg." *Telepolis*. 23 Sept. 2004. Web. 28 Oct. 2010. <http://www.heise.de/tp/r4/artikel/18/18371/1.html>. (Translated from German to English by Google Translate)

[15] Goebel.