Jonathan O’Hara
Math 115F
Dr. Bruff
Due: November 2, 2010

The Purple Machine

Civilizations and countries have relied on codes and ciphers for thousands of years to keep information secret and safe. The interception and decipherment of codes and ciphers has dramatically shaped world history. From Mary Queen of Scots to World War II, the connotations of deciphering a code have been literally life and death. For example, JN-25 was Japan’s premier naval communications code during World War II. This code, used to encrypt Japanese military agendas and operational tactics, was broken by the United States in May 1942, enabling them to anticipate Japanese strategy and movements. Due to the breaking of JN-25, the United States had the chance to prepare for and ultimately emerge victorious from the decisive Battle of Midway (Kahn 625). However, the deciphering of a different Japanese code was just as, if not more important. The breaking of the Purple code in 1940 aided the United States in achieving Allied victory in World War II.

Prior to World War II, Japan’s “Type 91 Print Machine,” or “Red Machine” was constructed as a means of encrypting communications. The completion of the machine in 1931 was not without fault. The machine relied on a half-rotor switch that needed to be cleaned and maintained extremely regularly. Also, the vowels and consonants were enciphered separately, making the code easier to crack. These few flaws led to the cracking of the Red Machine in 1935 (Smith).

The Red Machine’s successor, 97-shiki O-bun In-ji-ki (Alphabetical Typwriter ‘97), was nicknamed the “Purple Machine” by the US government. It was made up of two separate typewriters connected to a box of four disks. Each of these disks was hooked up to a corresponding stepping switch. Twenty-six wires connected the typewriters to the disks through a series of sockets, otherwise known as the plugboard. To encipher plaintext, a daily key would be referenced in order to route the wires into the correct sockets of the plugboard (Kahn 19). If just a plugboard and two typewriters were utilized, the resulting cipher would be monoalphabetic and relatively easy to solve. Let's say an individual were enciphering the word "apples" using only two typewriters and a plugboard. The message would go from the first typewriter, though wires into the plugboard, and straight through to the second typewriter. Therefore, every time a letter appeared in the plaintext, the resulting ciphertext would be encrypted the exact same way each time. Both "p's" in "apples" would be enciphered with the same letter, a "q" for example, so the ciphertext could read, "fqqmlr," "pqqawb," and so on, depending on the way the cables were routed.

The disks and stepping switches complicated the decipherment process. In addition to the arrangement of wires in the plugboard, the disks needed to be arranged so the numbers on the disks corresponded with the numbers indicated by that day's key. Connected to each disk was a stepping switch, which linked a single input to twenty-five outputs. Every plaintext letter typed into the first typewriter resulted in an electrical impulse sent through the switch. With each electrical jolt, the switch would shift from one output to the next, thus rotating the disk, generating twenty-five possible cipher alphabets for *each disk*. Moreover, these disks could be set to "fast," "medium," or "slow" speeds, depending on the daily key to generate more possible cipher alphabets (Weiraud). The combination of the disks resulted in one monoalphabetic cipher alphabet per letter, however, due to the differing rotation of each disk, hundreds of thousands of cipher alphabets were possible for the enciphering of the entire plaintext, thus making it a polyalphabetic cipher. For example, since each letter would be enciphered using different cipher alphabet schemes, "apples" could be enciphered as "dfnqq," "bqlsne," "qabbwb," and so on, just a few of the myriad of ciphertext options that the rotating disks and stepping switches generate. The current would flow through the wires, switches, and rotating coding wheels to produce the ciphertext.

Distinct features of the Purple machine, such as the plugboard and coding disks, were also important elements of the German Enigma machine. These features, however, did not function in the exact same manner. For instance, the coding disks in the Purple machine shifted according to impulses sent from the stepping switches, whereas a disk in the Enigma machine only rotated after the disk before it had completed an entire revolution. The stepping switches, entirely unique to the Purple machine, added an extra level of complexity to the rotation of the disks that the German Enigma machine was lacking.

A weak point of the Purple machine was inherited from its forerunner, the Red machine. Both Purple and Red machines divided letters into two groups: the twenties and the sixes. The twenties were comprised of all of the consonants in the English language, whereas the sixes were made up of all of the vowels. Any plaintext letter that was connected to any one of the “sixes” on the plugboard would be enciphered as any one of the sixes, A, E, I, O, U, or Y. This separation limited the amount of possible cipher alphabets, but not by much; the number of possibilities was still astronomical (Weiraud).

The decipherment process of the Purple machine was a long and laborious one, beginning in the late 1930’s and not completed until August of 1940. The man behind the “greatest feat of cryptanalysis the world had yet known” was William Friedman, touted as the world’s greatest cryptologist. Friedman and his team were correct in believing that the Purple machine was just an upgraded, more intricate form of the red machine. They began the process with trial and error, stumbling on some useful information, but not much. They gained insight through the frequency of appearance, absence, and repetition of letters from the ciphertext. They ultimately, however, made the most progress by grouping the ciphertext letters based on the way the disks spun and were able to eventually construct a crude replica of the machine, which functioned perfectly (Kahn 20). With Friedman at the helm, Signals Intellegence Service, the Army’s codebreaking division, was the first and only group to crack the Purple cipher. This milestone was not Friedman’s solo endeavor; on the contrary, it was a giant group effort. Lieutenant Francis A. Raven determined the pattern within the daily keys that allowed SIS to essentially anticipate the keys for each day (Kahn 23). Until 1942, the army and the navy shared codebreaking duties, intercepting and deciphering messages daily. The navy eventually gave up their resources to the army in order to consolidate American cryptographic efforts in regards to the Purple code. The navy had reorganized their cryptography department to focus on codes and ciphers other than Purple. This is an example of how the United States’ success in World War II cryptography stemmed from their cohesive, organized internal efforts. Similar to this was Bletchley Park, Britain’s cryptography department whose organization, centralization of resources, and clandestine nature put Britain at a militaristic advantage in World War II.

Just as the knowledge gained by the British through deciphering German Enigma codes was nicknamed *Ultra*, this information gained by the US is known as *Magic* (Rohwer 940). A large amount of this magic was obtained by the United States before and in the relatively early stages of World War II, giving them a distinct advantage in being able to understand and anticipate Japanese tactics in the Pacific theater. The US shipped a replica of a Purple machine to England, in return receiving access to English intelligence from Bletchley Park. SIS was also able to intercept Japanese communication with the Germans. This gave the US an advantage not only in the Pacific theater, but in the European theater as well, allowing them to predict the German forces’ positions. Ultimately, this intelligence proved to be crucial in battle, most notably on D-day. Baron Hiroshi Oshima, the Japanese ambassador to Germany, reported to Japan in great detail the position and details of the German army readying themselves for an invasion from the west. General Eisenhower used this information to his advantage, setting up a fake launch point for the invasion of Europe and took the Germans by surprise. The interception of that message proved to be instrumental in the United States’ success at Normandy (Kahn 508-9).

Until 1941, the Japanese had little knowledge of the American ability to intercept and decode their messages. They also had no idea that SIS cryptanalysts had broken the red code three years prior to the creation of the purple machine. In April 1941, a counselor of the German embassy in the United States discovered that the United States had the ability to read and decipher encoded Japanese communication. He secretly sent a cablegram to his Foreign Ministry explaining what he had learned and said that his source of information was completely dependable. The American government became anxious because their major source of Japanese intelligence could have been destroyed at any moment. Furthering the United States' apprehension, Japan acknowledged that "the United States is reading some of our [Japanese] codes" and would "exercise the utmost caution in accomplishing this mission"(Kahn 27). However, due to their confidence in the security of purple Japan continued to use the unchanged purple code week after week, allowing the US continual access to Japanese intelligence.

There had been some debate over whether or not the government had any advanced knowledge of the bombing of Pearl Harbor and whether or not it could have been prevented. It is true that a message was intercepted in the few hours before Pearl Harbor stating Japan's intentions to withdraw from diplomatic discussions with the United States. Essentially, this was a declaration of war; however, there was no explicit reference to an attack on Pearl Harbor. Even though there had been mention of Japanese interest in the action of American warships in Pearl Harbor, there had also been interest in the action of ships in other American ports. There were no overt threats against America nor was there any reason to believe that Pearl Harbor was going to be bombed. There was no blame to be placed on cryptographers or governmental agencies for alleged concealment of information. It was actually quite the opposite; Congress applauded Signals Intelligence Service for carrying out their job at the highest level (Kahn 4).

The Purple machine ended up being more of a curse than a boon for the Japanese. Although—to the Japanese—it seemed that Purple code was protecting diplomatic and military information, it was truly giving the United States valuable information essential in facilitating Allied victory.

Jonathan O’Hara
Math 115F
Dr. Bruff
Due: November 2, 2010

Works Cited

Kahn, David. "Codebreaking in World Wars I and II: The Major Successes and Failures, Their Causes and Their Effects." *The Historical Journal* 23.3 (1980): 625-33. *Jstor.org*. JSTOR. Web. 25 Oct. 2010. <http://www.jstor.org/stable/2638994>.

Kahn, David. *The Codebreakers: the Comprehensive History of Secret Communication from Ancient times to the Internet.* New York: Scribner's and Sons, 1997.

Rohwer, Jurgen. "Signal Intelligence and World War II: The Unfolding Story." *The Journal of Military History* 63.4 (1999): 940-51. *Jstor.org*. JSTOR. Web. 25 Oct. 2010. <http://www.jstor.org/stable/120557>.

Smith, Michael. *The Emperor's Codes: the Breaking of Japan's Secret Ciphers*. New York: Arcade Pub, 2001.

Weiraud, Frode. "How Purple Works." 8 Feb. 2003. Web. 27 Oct. 2010. <http://cryptocellar.web.cern.ch/cryptocellar/simula/purple/operation.html>.