Marijus Balciunas March 18, 2004 CSC233

Japan's Purple Machine

Codes and ciphers have played many crucial roles in the past 3000 years, protecting the secrets of caesars and laymen. In World War II numerous nations used cryptographic systems to conceal their secret intentions and plans from the spying eyes of enemies everywhere. Cryptanalysts, however, undeterred by the complexity of the crypto-systems, worked diligently, trying to find any sort of weakness that would allow a break into the cipher and expose the secrets contained within. During the late 1930s two nations, Japan and the United States, were in a state of intense negotiations regarding various political conflicts. The US trying to indirectly help the Allies set numerous conditions for Japan that prevented her from receiving crucial resources and embarking on its agreed upon mission with its European friends. In the midst of this, a machine cipher, codenamed Purple was performing a vital role in the war making policies for both Japan and the United States. A rarely told story about a secret operation in the US involved in breaking Japan's most secure crypto-system reveals a truly remarkable set of events that not only shaped the outcome of WWII, but also spearheaded the launch of numerous intelligence agencies for protecting the citizens of its nations and preventing surprise attacks such as the one on Pearl Harbor.

— Japan's New Cipher Machine —

In the early 1930s, the Japanese Navy purchased a commercial version of the German Enigma and proceeded to modify it by adding features which enhanced its security (Kahn 6). The system that evolved was one of the most secure cryptographic machines in the world. The machine was codenamed "Red" by the US government and was used to encrypt the highest level of diplomatic communications between Japan and its subsidiary agencies around the world. After considerable effort, the American Army Signal Intelligence Service (SIS) using "statistical analysis techniques" created by William Friedman managed to break the system in 1936 and was able to read Japan's top level

classified communications. The flow of decrypted Japanese information did not last for long, however, since in early 1939, Japan's Foreign Ministry introduced a new cipher machine dubbed "Purple." This machine was considerably more sophisticated than the "Red" machine and no one, on the US side, knew whether it was even breakable.

The Purple machine was used by the Japanese in World War II to communicate with its most important embassies and consulates around the world, some of which were in Washington, Berlin and London. Purple was used to encrypt and thus conceal Japanese diplomatic information from the inquisitive eyes of foreign governments. The information that passed through the Purple machine was of paramount importance to both Japan and its enemies. Some examples of the type of messages that were sent through the system include daily diplomatic communications and also the ever important message which broke off negotiations between Japan and the United States, thus indirectly signaling a war between those two nations. Purple was also used to relay information from Europe to Japan regarding the state of German forces and other detailed data about various aspects of the war in Europe. The information that was transmitted through Purple undoubtedly would have been extremely valuable to the United States, if it only could break one of the most secure cipher machines the world had ever seen to date.

The Purple machine was a complicated piece of machinery not only in the 1930s, but even today. The machine was made up of three major components. One of them was an electric typewriter which was used for inputting information into the machine. The second part was a "cryptographic assembly" which consisted of a plugboard, four electric coding rings, and numerous wires and switches that acted in unison with the other parts (Kahn 2). The last part was an output unit that printed the encrypted message from the machine. Instead of using rotors like the German Enigma machine did, the Purple machine used "electro-mechanical 'stepping switches'" (Anon 1). This in effect was similar to a second generation four rotor Enigma machine. However, it was much heavier and bulkier than the Enigma machine and could not, therefore, be employed in the battlefield easily.

The typewriter for inputting plaintext was built in such a way that it could accept three types of alphabets, those being English, romaji, and roman (Kahn 18). The input typewriter was connected to a "six-level, twenty-five point" telephone exchange device which was additionally connected to a "commercial" grade plugboard (Clark 140). The heart of the machine was the combination of four stepping switches that were in between the input typewriter and the plugboard. These switches would constantly shift with respect to each other and produce complicated paths from plaintext letters to cipher letters (Kahn 19). The plugboard with the stepping switches, which diverted the path of a plaintext letter from the input typewriter to some other letter in the output typewriter, were the parts that gave the machine its large complexity degree and were the central mechanisms of the machine. The plugboard settings could of course be changed from message to message, thus delivering seemingly random combinations of plaintext to ciphertext letters.

The Purple machine could substitute a single letter with a series of letters hundreds of thousands in length before it would start repeating the same substitution of letters (Kahn 19). This in effect gave the purple machine an unprecedented capability of hiding its plaintext messages by going through a unique series of steps in the machine. The operator of the machine also had the ability to change the settings of the stepping switches, in addition to the plugboard settings, hence changing the basic method of the encryption mechanism for each day that the machine was in operation.

To encipher a message, the operator of the machine would first need to look up the key of the plugboard settings and the initial settings of the four stepping switches, and set up the machine accordingly. Once it was ready for operation, the operator would only need to type in the plaintext message into the typewriter and the machine would do the rest. The plaintext message would go through a complicated path of the stepping switches and the plugboard settings and come out through the second typewriter as enciphered text. The brilliance of this machine was in the fact that each letter encryption would cause the stepping switches to advance *varying* degrees and consequently produce seemingly random encryptions of the same letter for even extremely long portions of text.

One limitation of the Purple machine was that it did not have a direct ability to encipher punctuation or numbers (Kahn 18). Therefore, the operator had to look up punctuation marks or numbers in a book and input their corresponding codes into the machine, which would be enciphered along with the rest of the message. To decrypt a message the operator would need to set up the Purple machine in exactly the same manner as it was used to encrypt the message. Then the operator would type the ciphertext into the machine and plaintext would come out from the second typewriter. All numbers and punctuation which were represented as code-words in the message would have to be manually placed into the message after looking up their appropriate values in the code book.

— The Machine Breaks --- Not Without Dividends —

In 1929, the US Army hired William F. Friedman, one of the leading figures in the field of cryptanalysis, to create and lead the Signal Intelligence Service or SIS. He led a team of individuals from various areas of study who would soon face their greatest challenge yet, breaking the Purple cipher. Friedman, who had a great understanding of the fundamentals of codes and ciphers, aided his team at SIS to create a mathematical understanding of how the Purple machine worked (Gresham 30). Frank B. Rowlett, who was the head cryptologist at SIS, also played a crucial role in the process of breaking the Purple cipher. They were faced with the daunting task of trying to discern a pattern, or some structure, from the myriad of five letter groups in the intercepted Purple code. It was definitely not easy. Friedman, after 18 months of excruciating work suffered a mental breakdown and had to temporarily withdraw to a psychiatric ward to deal with his sudden illness. Nevertheless, before that he provided his team with vital help in breaking the Purple cipher.

The first step in breaking any cipher system is the collection of “raw” code, which is not always as trivial as it may sound. Communications between Japan and its various offices around the world did not occur through a single cipher system. Japan as many other countries had a hierarchy of encryption systems, where specific agencies used one

or many systems depending on the sensitivity of the material being transmitted (Kahn 14). The Purple encryption system was used for the most confidential communications, thus at first Purple messages were rare, while other ciphers were used to carry the main load of Japan's diplomatic communications. Purple messages first began appearing in 1937 and not too long afterwards Purple material started to be intercepted more frequently by the day. Radio stations around the Pacific continuously monitored and collected radio telegraph transmissions (Anon. 1). As a result, Purple interceptions began amounting to enough material for American cryptanalysts to attempt breaking it.

After enough Purple code had been collected, the next step in the decryption process was determining the combination of wiring that could have produced the enciphered messages. This undoubtedly was not a trivial task as the number of possible combinations of the stepping switches and switchboard settings was extremely large. Luckily for the American cryptanalysts the Red crypto system had been broken a number of years earlier, which provided many clues into how Purple worked and could potentially be broken. In addition, the cryptanalysts had in their possession Tokyo's naval conference codes which had been obtained by some covert means. Using these conference codes the cryptanalysts became familiar with specific salutations and closings of letters and telegrams that were being transmitted (Kurzeja 1). Having broken the Red crypto-system, the American codebreakers had gained invaluable information as to how messages were structured and what form of address was used for what types of letters. For example, the Japanese often started their messages with "I have the honor to inform Your Excellency …" (Momsen). This in effect provided the cryptanalysts with numerous "cribs" that could be applied to their Purple ciphertexts for analyziation. As events unfolded these seemingly innocuous cribs turned out to be precious means into breaking the Purple cipher.

Sometimes the cryptanalysts would obtain information about the contents of a particular letter from outside sources and could guess the likely keywords in the letter. They would then use various techniques to try to deduce the possible locations of those words or the possible combinations of switchboard and stepping switch settings that were

used for that particular letter. At other times, the State Department would obtain plaintext letters that were also sent encrypted through the Purple machine (Clark 143). This allowed the cryptanalysts to look for loops or cycles between the cipher text and the plaintext of the messages. Once loops were determined the codebreakers could then try to work out the possible settings of the stepping switches. This was another crucial step in the process of breaking the Purple cipher and it interestingly paralleled the way the Enigma machine was broken in Europe.

There were also numerous occasions during a transitional phase when the Red cipher system was being replaced by the Purple cipher system, at which time identical messages were sent using both systems (Anon 2). Since, the Red system was already broken, it provided the cryptanalysts with even more plaintext and ciphertext combinations to analyze. On other occasions, Japanese operators after making a mistake encoding a letter would repeat the transmission of the same plaintext, enciphered with a different key (Kahn 20). Of course, the more plaintext and ciphertext combinations the American cryptanalysts had at their disposal, the more they could understand the way the Purple machine worked and how, in particular, it was used by the Japanese.

After many months of excruciating work, the cryptanalysts figured out how the Japanese Purple machine worked in transforming its input, the plaintext, into ciphertext. Once they had a rough, but mathematically precise idea of how the machine worked, they devised a replica machine that would enable them to automatically decrypt Purple messages. By August of 1940, eight replica Purple machines had been built by the SIS (Young). At this point, if the SIS had the key and other setting information for the machine they could decode any Purple encrypted message that came through their offices. However, obtaining the key was not a simple task and the codebreakers at SIS spent many agonizing months trying to determine the method by which the keys were made by.

A major discovery was made by Lieutenant Francis A. Raven regarding the keys that the Japanese used to send messages through Purple. First he noticed that the keys for a certain month were divided into three groups. In other words, the month was divided into three 10-day periods, each having some kind of pattern that could be discerned (Clark

145). Next, he found that the first day's key of a single 10-day period was uniquely related to the keys of the next 9 days (Kahn 23). More particularly, the first day's key reappeared in the next 9 days just in shuffled form. The shuffled form that was used for the first 10-day period was also the same for the next 10-day period as well. Therefore, with the knowledge of one day's key they were able to find out the keys of the next 9 days. However, the cryptanalysts were still faced with the uneasy task of finding the first day's key using "traditional" analysis (Kahn 23). Nevertheless, as a result of this discovery the cryptanalysts had obtained a means of gaining access to all Purple material during a 10 day period if only one key was broken. This was a crucial discovery that aided greatly the effort in breaking the Purple machine.

Decoded messages of the Purple cipher were code-named Magic by the US government, similarly as the British called Enigma decryptions "Ultra" (Anon 3). The SIS team of cryptanalysts, led by Friedman, had created an invaluable source of information regarding Japan to the US government. The material uncovered by Magic was so sensitive in nature that only the top government officials in the "American power structure" were aware of it. Among the receivers were the President, the War, State, and Navy secretaries, and the Chief of Staff (Kahn 24). Magic supplied the best intelligence that was available on Japanese plans in the year leading to Pearl Harbor. US policy makers were continuously aware of Japan's most secret communications. This insight into the activities and thinking of Japanese officials was an immeasurable benefit to the Americans. One must not forget that the US was in an aggressive mode of negotiations with Japan during this time in history and any insight into the plans and tactics of the Japanese was a "priceless asset" to have (Kahn 31). The breaking of Purple gave them this asset.

In addition to gaining valuable insight into Japanese plans, the Americans, through Magic, were able to obtain important information regarding the war in Europe. Japanese ambassadors from Germany and elsewhere in Europe sent detailed information to Tokyo regarding Hitler's capabilities and plans. Moreover, Magic revealed Germany's plans regarding United States and what possible actions they were to take as the numerous

battles in Europe unfolded. The US passed this information to Great Britain so they could take advantage of it immediately.

But the distribution process of Magic was not flawless. Since only a handful of people in the top echelon of the US government received the decrypted material, all the possible benefits of it were not reaped. Many people in policy making positions never saw nor were even aware of Magic and the valuable information it contained (Perloff 5). Therefore, many of them could not make decisions on foreign policy that current historians argue they should have made, plainly because they did not have that information.

There was a good reason why Magic was not distributed more freely. Any leak of information regarding the US success in the breaking of Purple would have resulted in an immediate change of the cryptosystem that the Japanese used and all information that was gained from Magic would have been lost. For this reason, it was decided that in the interest of sustaining the flow of information that Magic provided, it was best to keep the recipients of that information to as few as possible. Even those who did receive Purple decrypts were under the tightest restrictions regarding the viewing of Magic. In fact, carriers would bring Purple decrypts to those who were authorized to view them and would take them back as soon as they were finished reading them. No copies, whatsoever, were allowed to be made. Even under these tight precautions there were numerous cases when Japan had gotten tips from spies around the world that Purple had been broken by the US (Momsen 4). But the Japanese were so "blindingly" assured by the security of their Purple machine that they did not take those tips to be credible.

— The Missed Clues of Pearl Harbor —

Numerous historians and researchers have posed the question of why the catastrophe of Pearl Harbor was not prevented in light of the Americans having access to the most secret Japanese communications. The answer to this question is multi-faceted. First and foremost, it has to do with the inherent secrecy of the Japanese Military. In the pre-war era Japanese policy was controlled in part by the Japanese Military and they were

extremely secretive about their operations (Hatch 4). Information about the assault on Pearl Harbor was so secretly held that even the Japanese Foreign Office, for security reasons, was not aware of the impending attack. Some authors argue that if Japan's own diplomats did now know about the attack then how could the United States have possibly known about it? This line of argument has been rebuked by many, saying that although the Japanese never sent a message saying "…attack Pearl Harbor on December 7…." there were in fact many clues suggesting some sort of attack on the United States. One example of this occurring was in the weeks before the infamous day in Pearl Harbor, when Japan's foreign offices around the world received specific instructions to destroy their Purple machines and any secret documents that should not be seen by any foreign nation (Kahn 44). This sort of urgent call to action strongly implied that the Japanese were planning on breaking off negotiations and inevitably declaring war. Why did it imply a surprise attack on the US? Because Japan knew that if it wanted to have a chance of victory against the US, it had to, with all its might, cast a blow to the United States that would allow Japan to gain the upper hand in the war quickly, instead of not attacking immediately and letting the US prepare its defenses.

Another reason for the failed prevention of the Pearl Harbor incident was the fact that the SIS was underfunded and thus understaffed to do the job it was supposed to do effectively (Gresham 33). The number of messages that were coming through the SIS offices before the outbreak of war was astonishing, and it was impossible for all of it to get processed because there were not enough resources available for the agency. A third reason for why the US was unable to prevent the event at Pearl Harbor is because there was no single agency that was responsible for "real" analysis of the decoded material (Gresham 33). A decoded Japanese letter, taken out of context, may lead to many wrong interpretations if it is not accompanied by a required set of supporting material. It is true that most of the important messages were delivered to top leaders of the US government and military, but this method of distribution was flawed since all they were getting were small snippets of communication from a pool of thousands of letters of communication. Therefore, it was impossible for the receivers of Magic to get a true sense of the

intentions of Japan, because not only were the methods of communications different, but also the Japanese "language and culture" played a role in the ineffective understanding of the meaning of those letters (Gresham 33).

As one can see the reason the attack on Pearl Harbor was in a way inevitable, was because of numerous causes that when put together were the factor that prevented the US to raise its shields for the impending attack. There was no effective "infrastructure" for the collection, decryption, analyzation and distribution of foreign intelligence information for the US to have successfully prevented such a calamity (Gresham 33). As a result, not too long afterwards two agencies, the CIA and the NSA, were established to effectively manage security and intelligence for the United States.

All in all, it was an amazing feat that the cryptanalysts at SIS accomplished during their 20 months of painstaking work. In that period they were able to deduce the setup and the numerous mechanisms of the Purple machine. Not only that, but they were able to build replica machines, which could decrypt Purple messages as fast as those operated by the Japanese. According to Kahn, a respected cryptography expert, the break of the Purple machine was "the greatest feat of cryptanalysis the world had yet known" (18). This feat allowed the Allies to win many battles that were primarily based on information gathered from Purple traffic. Although the break of the Purple machine did not prevent the Pearl Harbor incident, it did provide numerous clues and hints about impending attacks after the Pearl Harbor episode and undoubtedly saved countless lives. Even though the names responsible for this extraordinary cryptanalysis feat are not widely recognized, they were truly central figures in the war and aided the Allies with truly magical information.

Works Cited

Anonymous 1. Purple. March 07, 2004.
http://webhome.idirect.com/~jproc/crypto/purple.html

Anonymous 2. (Excerpted from *Codes and Ciphers: An A to Z of Covert Communication from the Clay Tablet to the Microdot*, Fred B. Wrixon, Prentice Hall, 1992)
http://jya.com/nsa-rowlett.htm

Anonymous 3. Osprey Essential Pearl Harbor: Purple. March 01, 2004
http://216.168.37.48/FMPro?-DB=osehph.FP3&-FORMAT=/scribe/osehph/osehphformat.html&ReferenceNumber=OSEHPH231&-Max=1&-Find

Clark, Ronald. The Man Who Broke Purple. Little Brown & Company, 1997.

Gresham, D. John. Codebreaking. March 01, 2004.
http://www.faircount.com/web04/pearlharbor/pdfs/codebreakers.pdf

Hatch, A. David. Enigma and Purple: How the Allies Broke German and Japanese Codes During the War. March 06, 2004.
http://cadigweb.ew.usna.edu/~wdj/papers/cryptoday/hatch_purple.ps

Kahn, David. The Codebreakers. New York: Scribner, 1996.

Kurzeja, Karen. Pearl Harbor & Ciphering Methods. March 1, 2004.
http://raphael.math.uic.edu/~jeremy/crypt/contrib/kurzeja.html

Momsen, Bill. Codebreaking and Secret Weapons in World War II. March 07, 2004.
http://home.earthlink.net/~nbrass1/3enigma.htm

Perloff, James. Pearl Harbor. The New American. December 8, 1986.
http://www.thenewamerican.com/departments/feature/1999/070499.htm

Young, Frank Pierce. Flame & Blame at Pearl Harbor. The Responsibility Question. March 01, 2004. http://www.microworks.net/pacific/special/flame1.htm

Note: More sources were used to write the paper, but direct quotes were not taken from them therefore I am not including them in this list. However, if there is a need I can provide the rest of the sources used to write this paper.