A VERY PURPLE-XING CODE

Michael Cohen

Groups cannot work together without communication between them. In wartime, it is critical that correspondence between the groups, or nations in the case of World War II, be concealed from the eyes of the enemy. This necessity leads nations to develop codes to hide their messages' meanings from unwanted recipients. Among the many codes used in World War II, none has achieved a higher level of fame than Japan's Purple code, or rather the code that Japan's Purple machine produced. The breaking of this code helped the Allied forces to defeat their enemies in World War II in the Pacific by providing them with critical information.

The code was more intricate than any other coding system invented before modern computers. Using codebreaking strategy from previous war codes, the U.S. was able to crack the Purple code. Unfortunately, the U.S. could not use its newfound knowledge to prevent the attack at Pearl Harbor. It took a Herculean feat of American intellect to break Purple. It was dramatically introduced to Congress in the Congressional hearing into the Pearl Harbor disaster.[1] In the ensuing years, it was discovered that the deciphering of the Purple Code affected the course of the Pacific war in more ways than one. For instance, it turned out that before the Americans had dropped nuclear bombs on Japan, Purple

---

Michael Cohen is a Senior at the Commonwealth School in Boston, Massachusetts, where he wrote this paper for Tom Harsanyi's United States History course in the 2006/2007 academic year.

messages had revealed to the U.S. that Japan was almost ready to surrender. Naturally, the U.S., and Britain, for that matter, were very selective and secretive in releasing information about Purple to the public.[2]

The Japanese did not create such a powerful code from scratch. They had used other war codes before Purple. In fact, the U.S. had just broken Purple's predecessor, Red, when Japan switched to Purple. U.S. Navy Commander Joseph P. Rochefort had played a major role in the U.S. effort to crack the Red code. He had enlisted in the U.S. Navy in 1918,[3] and subsequently climbed up the ranks. At one point, he was working on the warship *U.S.S. Arizona.* Executive Officer Commander Chester C. Jersey liked crossword puzzles, and so did Rochefort. Jersey then moved to the Navy Department Headquarters. When the Navy needed someone for codebreaking in 1925, Jersey suggested Rochefort. Rochefort started this work in October of that year. At that time, the U.S. codebreaking team was made up of only one person, Lieutenant Laurance F. Safford. Safford's job was to create a U.S. Navy code, and he felt that he needed to look at foreign codes to do so. He trained Rochefort until February 1926, and then Rochefort took over, leading only a single cryptanalyst and an assistant "with no particular abilities." Rochefort's work made him sick from stress, which caused an ulcer to form in his stomach. He returned to his naval work at sea in 1927.[4]

During this two-year period, Rochefort made the first American breakthrough against the Japanese Navy. There was money remaining in a 1918 "secret naval intelligence slush fund." The amount was almost $100,000, an enormous sum of money at that time.[5] A Director of Naval Intelligence in the early 1920s used some of the money to pay for break-ins at the Japanese Consulate in New York City. The men who participated in these took pictures of the Red codebook there.[6] The Japanese would develop a machine a few years later to encipher this code, called the Red machine.[7] The Director used more of the fund to pay linguists to translate the codebook. However, Red also had a second layer of coding besides that which the codebook revealed. The encoder

used "additives," random numbers added to each group of encoded words, further concealing the message's meaning. These additives were taken from a separate book: the person receiving the message(s) would have a copy of the book, so he would know which numbers to delete from the code before decrypting the message. The additive book's page number used for a particular message was also hidden in the message. Rochefort had the incredibly challenging task of recreating the additive book with only the codebook and intercepted Japanese messages as reference![8]

In 1931, the Japanese developed the machinery to encipher the Red code. They created two versions of the machine: Type No. 91 and Type No. 91-A. Type No. 91-A was nicknamed the Red machine and was distributed to the Japanese Foreign Office.[9] The machines were also known as *angoo-ki taipu A*. They were called Type No. 91 because they were created in 1931, or 2591 according to the Japanese calendar. The machines sent messages in "Romaji." This was "a Romanized spelling of the *kana* characters," which were "phonetic symbols" that the Japanese created to use when transmitting code (via radio). Each *kana* symbol corresponded to one of the 2,000+ Chinese-based characters in the Japanese language, since each of these characters has a meaning but no sound value, which poses a problem for creating a code system. The Red devices had two electric typewriters. One was used to input the plaintext message, and the other one would automatically type out the same message, but written in enciphered code. Some of the Red machine's mechanical workings were similar to those of the German Enigma machine, which was used by the Germans during the war.[10] Americans knew a decent amount about how the Enigma machine worked, but they had no idea how to decrypt the code it produced.[11]

After Red, Japanese code systems were affected by *The American Black Chamber*, a book written in 1931 by Herbert Yardley, an American cryptologist. In 1929, President Hoover chose Henry L. Stimson as Secretary of State. Yardley wanted Stimson (who was his boss) to approve of him, so he sent Stimson some deciphered

code detailing plans of the Japanese government. When Stimson didn't appreciate this gesture, Yardley published the findings in a best-selling book. The Japanese wanted to make sure their next code was more protected, so their vital information would not be released to the public in another such book.[12] Yardley's book, though it caused the Japanese to change their code, actually helped the Americans. The Japanese changed their code before WWII because of the book, so the U.S. codebreakers were able to decipher Japanese messages before the war started. If it had not been for the book, Japan might have changed its code just as the war was starting. The U.S. would then have had to crack the code during the war, and would therefore have been uninformed of Japan's secrets during this time.[13] After the fiasco with Yardley's book, Stimson shut down Yardley's codebreaking operations. It seemed that the U.S. was finished with codebreaking, but other federal agencies, such as the FBI, secretly continued the practice. Yardley's files were given to the U.S. Army Signal Corps, which, in turn, founded the Signal Intelligence Service (SIS). William Friedman was hired to lead SIS.[14]

According to Hervie Haufler, the author of *Codebreakers' Victory*, "many consider [Friedman] to be the greatest cryptologic genius of all time." In 1891, a very young Friedman moved from Russia (his birthplace) to Pittsburgh with his family. Friedman originally chose to follow a plant genetics career path when he was a graduate student at Cornell. This is where he met George Fabyan, described by Haufler as an "eccentric millionaire cotton researcher" who was looking for a geneticist to research ways to improve crop strains at his Riverbank Laboratory in the Chicago area. Fabyan made Friedman the leader of the Riverbank Lab's Department of Genetics.[15]

Fabyan was interested in one woman's studies. The studies led the woman to believe that Shakespeare's writings were actually the product of Francis Bacon and that Bacon had written messages in code in early copies of the plays which said "that [Bacon] was the illegitimate son of Queen Elizabeth I" and should be in line for the English throne. (The book did not provide the woman's name.)[16]

Fabyan had enough financial resources to have these claims investigated, so he recruited people, including Friedman, to do so. The code was supposed to be related to the fonts used in the Shakespearean folios that the woman mentioned. Friedman used his talent with cameras to produce larger copies of these fonts. He felt attracted to this work with code.[17]

Friedman married Elizebeth Smith (correct spelling), another one of Fabyan's decoders, in 1917. Both Friedmans felt that America needed to be skilled in "secret communications," since U.S. involvement in Europe's battles was becoming more and more probable. Fabyan shared this opinion and supported their research in this area. This was the start of a period of time in which Fabyan's lab was the only institute in America that was proficient in decrypting code. Fabyan was able to set the Friedmans up as teachers teaching Army officers how to crack code when the Army established its Cipher Bureau in 1917 (after the Friedmans were married). William Friedman wrote cryptography booklets to use to teach, which the Army liked. These works led to Friedman being offered the pay of a first lieutenant.[18]

After spending the final five months of WWI in France, working for General Pershing, trying to crack German codes, Friedman returned to Fabyan's lab and wrote a booklet entitled "The Index of Coincidence and Its Application to Cryptography." According to Daniel Kahn, author of *The Codebreakers*, the booklet "must be regarded as the most important single publication in cryptology." Prior to this paper's publication, codes were broken by a cryptologist examining the code until he/she had an epiphany. Friedman had come up with actual methods for codebreaking, which were presented in the booklet.[19] Friedman had discovered that if one arranges messages in code in multiple rows, two letters will occasionally repeat in the columns that the rows form.[20] This finding helped with the analysis of codes encrypted by machine. The Friedmans' government work in the 1920s was making them famous. William Friedman was appointed chief of SIS during the autumn of 1929. He selected four people (other than himself) for his team, and trained them, with great success.[21]

In the early 1930s, Friedman's team cracked the Japanese code enciphered by the Typewriter-91 machine, to which they assigned the code name "Red."[22] They did this partly by using "cryptanalytical techniques," and partly by the information gleaned from the Japanese Embassy break-ins discussed earlier. [23] However, between the end of 1938 and the beginning of 1939, deciphered Red messages revealed that Red would be replaced by *angoo-ki taipu B* ("cipher machine Type B"). Friedman and his team designated this machine with the code name "Purple."[24]

Purple was "the diplomatic Japanese cipher-system used by the Foreign Office in Tokyo for the most secret communications with its ambassadors abroad."[25] It was developed by the Special Signals Unit of the Japanese Navy, led by Captain Ito. The machine was also called the Alphabetical Typewriter, Type 97, the J Machine, and *97-shiki O-bun In-ji-Ki* ("97" because it was created in 1937, or 2597, according to the Japanese calendar).[26]

In 1937, Friedman and his colleagues received their first intercepted Purple message to analyze.[27] After gathering enough messages to begin fruitful analysis, the American codebreakers realized that the Japanese had made many alterations to their machine so that it was much harder to crack their code than that of the Germans' Enigma machine. The Japanese Navy had given their slightly modified Enigma machine to the Japanese Foreign Office, which had made the critical changes to it. Some other such advances had given the U.S. trouble in figuring out how to decipher Red. When the U.S. had finally figured out Red, the Japanese switched to Purple.[28]

The Purple machine was not just a "modification of Red," as the Americans had wished.[29] It used multiple "rotating switches to encipher every letter of a message in a different key from the last or the next."[30] The machine physically consisted of a group of "standard six-level, 25-point [commercially available] stepping switches plus a standard commercial plugboard" and a complex wiring network.[31] One aspect of the machine that was similar to the Red machine was the two typewriters that were involved. One was for plaintext input and the other was for code output.[32]

To send a message from a Purple machine, the machine operator would first calibrate the machine's plugboard and rotors for that day's code keys, as determined by a book. Later, a second, ultra-secret, code was added for each day of the month for use with messages of the utmost secrecy. Next, the operator would type the plaintext message that he wanted to send into the input typewriter, using designated three-letter codes for any numbers in the message. As he did so, the encoded message was automatically typed by the output typewriter.[33]

The first task of the Americans in cracking the code was to collect a certain number of encoded messages that were encrypted in the same key. At first the same keys were used every day, but soon it depended on what day of the month it was. The next job was to determine how the Purple machine's wiring was arranged for each key. At first, the Americans would figure these keys out by trial and error. A successful choice would enable the U.S. decoders to decipher all messages using one key (those messages from one day of the month), but the U.S. did not guess successfully for months. A discovery led them to perfect their methods, as will be explained later. Finally, to crack the code itself, Friedman and his team basically had to look for patterns in the encoded text, which would eventually show them the rules governing the code.[34]

The U.S. Navy decoders helped Friedman and his team. They gave them all their intercepted Purple messages for analysis, as well as their knowledge about the Red machine and code, which were close enough to Purple for this information to help.[35] This assistance was virtually the only outside help that Friedman and his team received.[36] Friedman and his workers also used Japanese errors and customs to help them crack Purple. Certain customary Japanese "diplomatic forms of address such as 'I have the honor to inform your Excellency,'" were always written at the beginning of certain messages. The U.S. knew some of them and could guess others, so they were able to find these headings in encrypted messages, and would then know which code words corresponded to them. The U.S. would then be able to identify individual words of the headings in other parts of the message, and the headings

also gave them clues about the keys used. The Japanese had to resend some Purple code messages in Red code to embassies which only had the Red machine. The U.S., which had already decrypted Red, would not only know what the messages said but also how to write them in Purple. Every so often, the sender of a Purple message would set his machine to the wrong setting, and then would have to resend the message with the machine set correctly. This gave the U.S. some insight into how the machine worked and which keys were used on which days.[37] Sometimes (not very often), the State Department would have an unencoded copy of a message that the U.S. also had in code, hinting at which keys the Japanese were using that day. Such leads led to new theories, and even if these theories ended up being wrong, they had still been eliminated as possibilities.[38]

The chief of the U.S. Army Signal Corps, General Joseph O. Mauborgne, realized that American progress on cracking Purple was too slow to be effective.[39] One cause of this was that instead of fully concentrating on Purple, Friedman was largely focused on solving the preliminary problems that needed to be eliminated if Sigaba (an American code that was being developed concurrently with Purple) would be able to be put to use soon and be effective.[40] Mauborgne decided that Purple was more important than Sigaba and Friedman's other duties, so, in February of 1939, he ordered Friedman to devote his undivided attention to Purple and to not work on any other projects.[41]

Purple codebreaking went on through the summer of 1939 with no huge successes.[42] The first major success occurred in August of 1940.[43] Americans had determined that Purple's encoding mechanism used a "subsequence of six" letters that were encoded independently of the other 20. This group was the letter "v" and five other letters. Frank Rowlett (one of the SIS staff) had created preliminary plans for a machine that would encode and decode the six letters for Americans as the real machine did for the Japanese. SIS had then hired Leo Rosen, a member of the Reserve Officer Training Corps at MIT, as well as an electrical engineering student there. Rosen had built the "'Six Buster"' machine from

Rowlett's blueprints and discovered that "telephone switchboard stepping switches" could be used to construct the machine. In August 1940, Harry L. Clark brought up the matter of whether or not the Purple machine used an unprecedented "enciphering mechanism," possibly relating to the telephone switches in Rosen's machine.[44] Friedman was intrigued by this hypothesis.[45]

To determine if the claim was correct, the Americans needed more information and plaintext versions of the groups of the 20 remaining letters.[46] Every day, the SIS workers wrote down the most likely correspondences and matches of the 20 letters when they were encoded with the 20 letters in plaintext. Genevieve "Gene" Grotjan, who had been collecting the results of this work, discovered that some coded letters and words matched with plaintext letters and words, and that these same matches occurred in multiple instances. This meant that a certain string of code would always correspond to the same word, provided that the same key was used. This discovery was the first step in the process of SIS creating a Purple machine from scratch.[47] It also led to the discovery that stepping switches were the component of the Purple machine that enabled it to "advance at regular intervals from one encipherment stage to another."[48]

The first U.S. decryption of a message encoded in Purple that resulted in a clear English translation occurred on September 25, 1940. Two days later, Italy, Germany, and Japan signed the Tripartite Pact, which forged the Axis alliance among them. It also provided the U.S. with a large flow of Purple messages. From there, the U.S. proceeded to create a Purple machine from scratch. This construction process is shrouded in myth. In reality, it was built "from electrical equipment in short supply."[49]

Though the U.S. created an almost perfect copy of the machine—only two of the hundreds of connections in the SIS's version of the Purple machine did not match those in the actual device—their work was not finished.[50] They still needed to figure out which keys were used for many days of the month.[51] Lieutenant Francis A. Raven, a young U.S. Naval officer, figured out that the Japanese had divided each month into thirds, or 10-day sections

(each day of a month used the same keys as did that day of the other months; for instance, the same keys were used on January 1, February 1, March 1, etc.). Raven discovered that the keys used on the final nine out of the 10 days in each section were anagrams of those used on the first day of the section. This meant that determining the keys used on the 1st, 11th, and 21st of the month led to a much simpler solution to the keys of the other days. This breakthrough led to the American cryptologists' ability to guess many of the keys before they were used, which helped them decode more messages.[52] However, figuring out a key could take anywhere from 15 minutes to a month, slowing the codebreaking process.[53]

Another inhibitor of decoding was the slow speed with which the messages were transported to the codebreakers. Only special messages (a small percentage of the messages) were radioed to the cryptographers. Other messages were delivered by far less rapid means.[54] Also, there were not many men sorting through the messages (dividing them by priority, with Purple messages being most important) relative to the large number of messages being transported to Washington.[55] Another issue was that it was not simple to find cryptanalysts, nor was it easy to find trustworthy Americans who could translate messages from Japanese into English (there were very strict security measures for recruitment to this position, because many applicants were Japanese-American). Only after translation could the Purple messages themselves be sorted by priority.[56]

Friedman and his team's work gave the U.S. State Department access to Japan's highly classified military plans, tactics, and other valuable wartime information, from the autumn of 1940 until the end of the war. Friedman did not have any say in how the U.S. chose to use the information that he and his team provided, and though he did not complain in public, papers he wrote in the years following the cracking of Purple seem to show that he was upset at how certain politicians and the military made use of his work.[57]

Purple became indispensable to the war effort, even in Europe, because of the Japanese Ambassador to Germany, Hiroshi Oshima. Also a baron and a general, Oshima's extreme Nazi beliefs caused Hitler and other high-ranking Nazis to support him. Oshima would interview Hitler for hours, during which time Hitler would disclose his most highly confidential secrets. Then, Oshima would summarize these interviews and have his workers encode them in Purple and send them to Tokyo. The U.S. and Britain intercepted them, decoded them, and gained knowledge of their top-secret contents in this way.[58] In addition, the Japanese Ambassador in Moscow sent information to other embassies about Soviet Russia, the Japanese Ambassador in Rome sent information about Mussolini and other Italians, and the Japanese Ambassadors and military attachés in neutral countries transmitted anything they discovered. All of these transmissions were sent in Purple, and the Allies intercepted many, if not all, of these messages.[59] Ironically, Oshima's Purple code transmissions "were of far greater value to the Allies than they were to" the Japanese.[60] Sadly, Oshima never mentioned plans to attack Pearl Harbor in his Purple transmissions. He was most likely not told about the Pearl Harbor plans because, although he was a general, he was also a diplomat, and Japanese admirals and generals were reluctant to divulge details of war plans to diplomats.[61]

People today still debate about how the Japanese were successfully able to attack Pearl Harbor given the high level of U.S. attention to Japanese codes at the time and the Americans' ability to decipher Purple. According to Friedman, "There were no messages which can be said to have disclosed exactly where and when the attack would be made." However, this only refers to messages that the U.S. had intercepted and decoded. FDR has been accused of knowing about the plans for the Pearl Harbor attack before it occurred, but of waiting until the plans were carried out before responding to them.[62] However, many historians refute these claims.[63] Since WWII, many things have been found which should have caught the U.S.'s attention but didn't, because America was enjoying a time of peace prior to the Pearl

Harbor attack.[64] Pearl Harbor brought to light the faults in the American methods of decoding at the time. Mainly, as has been mentioned, all steps of the process were painfully slow. On a more minor note, Hawaii had no Purple machine.[65]

Throughout 1941, decoded Purple messages revealed to the U.S. the exchanges between the Japanese Foreign Office and the Japanese Embassy in Washington. The embassy was pressured by the Foreign Office to make the U.S. agree to the terms the Foreign Office set. During this time, Japan's politically moderate Prime Minister Prince Konoe died, and his successor was the extreme nationalist General Tojo and his cabinet. On November 26, 1941, the U.S. State Department laid out its conditions to Japan in order to bring the negotiations between them to a successful conclusion. Tojo did not approve, just as the Japanese diplomat negotiators had predicted. The Japanese response to the U.S. was sent on December 7th, first to the Japanese Embassy in Washington and then to the U.S., but was intercepted by the U.S. when it was sent to the embassy. The response closed by saying that, "'it was impossible to reach an agreement through further negotiations,'" meaning that the Japanese were about to take military action against the U.S. (intercepted at 3:00 AM Eastern time).[66] The Foreign Office told the embassy to give the U.S. the response at 1:00 PM EST (intercepted at 4:30 AM EST).[67] The Foreign Office then told the embassy to "destroy its code materials" (intercepted at 5:00 AM EST).[68]

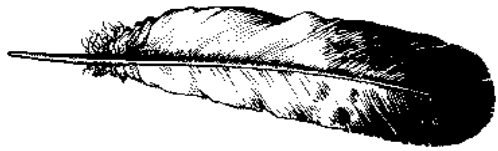
The Americans who saw these messages figured out their meaning, but did not warn Hawaii because of misunderstandings. FDR thought that somewhere in Southeast Asia would be attacked, since he forgot that 1:00 PM EST was slightly after daybreak in Hawaii. The U.S. Chief of Naval Operations, Admiral Harold Stark, didn't realize that the U.S. didn't send decoded Purple messages to Hawaii any more, so he thought that the U.S. Army personnel on the islands already knew about the messages and their contents. U.S. Chief of Staff General Marshall did not want to notify his commander in Hawaii, General Walter Short, by scrambler phone because he thought it wasn't secure enough. He

wanted his message sent by radio, but bad radio interference caused him to send it instead by commercial telegraph to San Francisco, from which it was sent to Hawaii seven hours later. It was then given to Short by a messenger on a bicycle after the Japanese planes had finished their first pass over Hawaii. Two privates in Hawaii noticed the Japanese aircraft and notified the lieutenant on duty, but he assumed that the planes were just the scheduled arrivals from the U.S. mainland that he knew were arriving that day.[69]

OP-20-G, a U.S. Naval agency, found out that Japan was planning to send to its outposts what became known as the "winds execute" message if there was an emergency—ending diplomatic relations with another country, for instance.[70] The name "OP-20-G" meant that it "was the G section of the 20th division of OPNAV, the Office of the Chief of Naval Operations, [which was] the Navy's headquarters establishment."[71] The "winds execute" message would be a short message inserted into Japanese weather forecast broadcasts.[72] *Higashi no kase ame*, meaning "east rain wind," was the code message for the Japanese outposts in the U.S. to end diplomatic relations with the U.S. and to destroy their machines and materials for codes. In Washington at the time, young Navy communications intelligence technician Ralph T. Briggs had insisted that he saw *higashi no kase ame* embedded in a Tokyo weather broadcast on the morning of December 4. He said that he realized the significance of this message, and that he then told officials of higher rank about it. However, after this point, the story of Briggs' discovery becomes shrouded in mystery, and some of this confusion seems to have been purposely caused to hide some of the facts of the story.[73]

Almost until the war's close, "Purple continued to give the Allied commanders advance notice of enemy intentions in Europe."[74] When Truman was being informed of the success of tests of the atomic bomb, Purple exchanges between Tokyo and Moscow revealed that Japan was on the verge of surrender. Later, though historians today still dispute this, Friedman often said that, "If only [he] had had a channel of communication to the President [he] would have recommended that [the President] not drop the bomb—since the war would be over within a week."[75]

Friedman did not have such a communication channel, however, and his codebreaking attempts were plagued with a number of problems from the start. The lack of intercepted materials to decode, and especially the U.S. decoders' limited initial knowledge of Purple, greatly slowed the pace of Friedman's mission. Although deciphering the Purple code did not prevent the bombings of Pearl Harbor, it was responsible for U.S. knowledge of other critical enemy plans. Cracking Purple was a key breakthrough for the Allies in World War II, showing that decrypting enemy code is vital to a nation's wartime success.



[1] Ronald Clark, The Man Who Broke Purple: The Life of Colonel William F. Friedman, Who Deciphered the Japanese War Code in World War II (Boston: Little, Brown, 1977) p. 139

[2] Ibid., pp. 138-139

[3] Stephen Budiansky, Battle of Wits: The Complete Story of Codebreaking in World War II (New York: Free Press, 2000) p. 3

[4] Ibid., p. 4

[5] Ibid., p. 4

[6] Ibid., p .5

[7] Ronald Lewin, American Magic: Codes, Ciphers, and the Defeat of Japan (New York: Farrar Straus Giroux, 1982) p. 36

[8] Budiansky, p. 5

[9] Lewin, pp. 35-36

[10] Hervie Haufler, Codebreakers Victory: How the Allied Cryptographers Won World War II (New York: New American Library, 2003)

[11] Lewin, p. 35

[12] Haufler, p. 19

[13] Clark, p. 139

[14] Haufler, p. 110

[15] Ibid., p. 110

[16] Ibid., pp. 110-111

[17] Ibid., p. 111

[18] Ibid., p. 111

[19] Ibid., p. 111

[20] Ibid., pp. 111-112

[21] Ibid., p. 112

[22] Ibid., p. 113

[23] Lewin, p. 22

[24] Haufler, p. 114

[25] Clark, p. 138

[26] Ibid., p. 139

[27] Ibid., p. 139

[28] Ibid., p. 140

[29] Haufler, p. 114

[30] Budiansky, p. 6

[31] Clark, p. 140

[32] Ibid., pp. 140-141

[33] Ibid., p. 141

[34] Ibid., p. 141

[35] Ibid., p. 141

[36] Ibid., p. 143

[37] Haufler, p. 115
[38] Clark, p. 143
[39] Ibid., p. 142; and Haufler, pp. 114-115
[40] Clark, p. 36
[41] Ibid., p. 142, and Haufler, pp. 114-115
[42] Clark, p. 143
[43] Ibid., p. 144
[44] Haufler, p. 115
[45] Clark, p. 144
[46] Haufler, pp. 115-116
[47] Ibid., p. 116
[48] Ibid., p. 117
[49] Clark, p. 144
[50] Ibid., p. 144, and Haufler, p. 117
[51] Clark, p. 144
[52] Ibid., p. 145
[53] Ibid., p. 146
[54] Ibid., p. 145
[55] Ibid., pp. 145-146
[56] Ibid., p. 146
[57] Ibid., p. 146
[58] Haufler, p. 128
[59] Ibid., pp. 128-129
[60] Ibid., p. 130
[61] Ibid., p. 129
[62] Ibid., p. 122
[63] Ibid., pp. 122-123
[64] Ibid., p. 122
[65] Ibid., p. 127
[66] Ibid., p. 123
[67] Ibid., pp. 123-124
[68] Ibid., p. 124
[69] Ibid., p. 124
[70] Ibid., p. 124
[71] David Kahn, The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet (New York: Scribner, 1996) pp. 9-10
[72] Haufler, pp. 124-125
[73] Ibid., p. 125
[74] Clark, p. 199
[75] Ibid., p. 201

Bibliography

Budiansky, Stephen Battle of Wits: The Complete Story of Codebreaking in World War II New York: Free Press, 2000

Clark, Ronald The Man Who Broke Purple: The Life of Colonel William F. Friedman, Who Deciphered the Japanese War Code in World War II Boston: Little, Brown, 1977

Haufler, Hervie Codebreakers Victory: How the Allied Cryptographers Won World War II New York: New American Library, 2003

Kahn, David The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet New York: Scribner, 1996

Lewin, Ronald American Magic: Codes, Ciphers, and the Defeat of Japan New York: Farrar Straus Giroux, 1982

Consortium *for* Varsity Academics®

Member Schools include: Williston Northampton School of Easthampton, Massachusetts, Menlo School of Atherton, California, Poly Prep Country Day School of Brooklyn, New York, Albuquerque Academy of Albuquerque, New Mexico, Phillips Academy of Andover, Massachusetts, and Deerfield Academy of Deerfield, Massachusetts.

Partners include: the American Council of Trustees and Alumni, the Boston University School of Education, Anonymous, Ann Mactier, the Leadership and Learning Center, the Lagemann Foundation, the History Channel, Carter S. Bacon, Jr., John Herbert, the National Center on Education and the Economy, and the Gilder-Lehrman Institute.

"Teach by Example"
Will Fitzhugh [founder]
Consortium *for* Varsity Academics® [2007]
The Concord Review [1987]
Ralph Waldo Emerson Prizes [1995]
National Writing Board [1998]
TCR Institute [2002]
730 Boston Post Road, Suite 24
Sudbury, Massachusetts 01776 USA
978-443-0022; 800-331-5007
www.tcr.org; fitzhugh@tcr.org
Varsity Academics®