The Sting – Enabling Codebreaking in the Twentieth Century

Thomas R. Johnson

> ***. . . a successful Cryptographic Bureau should have its secret agents to ferret out scraps of information from foreign codes. — Herbert Yardley,* The American Black Chamber**
>
> ***You gotta keep his con even after you take his money— Henry Gondorf in* The Sting**

Cryptanalysts rarely admit to needing help. There is a fierce inbred independence that characterizes the trade. Yet they are not always successful through classical cryptanalysis. They have even been known to cheat. And they are not always honest about this – they have even been known to lie about their cheating.

Herbert Yardley, who headed the Black Chamber in the 1920s, understood the uses of human intelligence. He was not one to struggle over an intractable problem if help was available. Yardley apparently had few opportunities for outside help, but it probably was not for lack of trying. More likely he suffered from a surfeit of secrecy. Few knew about his code-breaking effort, and thus code thefts were not something that occupied the minds of those few who were engaged in intelligence work – at least, not in the U.S. Army. (The Navy, which did not have a code-breaking effort until later, did have a unit occupied with stealing codes – that is, acquiring a source of intelligence without a customer to give it to. This is a paradox that we shall soon discuss.)

This article is all about stealing codes – who did it, why, and to what effect? When did it make the difference? When was it unnecessary? What role did it play in cryptologic history? The subject is far larger than this short disquisition, which will deal with only a few examples. Our concentration is on the Americans, but of necessity we must begin with the British. It was in England that code acquisitions first made an impact.

The British in World War I

It was August 1914. While the guns roared on the Continent, in the Baltic the German cruiser *Magdeburg*, attempting to follow the lead of its comrades, had run up on a reef in the fog. Russian sailors from a torpedo boat soon swarmed aboard and, in the captain's cabin, discovered a naval codebook. On September 6 the Russian naval attaché in London informed Winston Churchill, First Lord of the Admiralty, of the capture. Within two weeks Churchill's codebreakers had it in their hands.

The Admiralty had had a code-breaking group for only a month. Formed at the outbreak of war, it was still in the process of getting organized – the expertise and experience approached zero, and the codebreakers needed help. Thus the *Magdeburg* acquisition could not have come at a better time.

Room 40 (as it became known) was so inexperienced that it could not break the German naval messages even with the codebook. A second codebook capture, from the German steamer *Hobart* in October, helped them out. It contained a merchantman codebook and, in addition, keys for a superencipherment system. The British cryptanalysts under Sir Alfred Ewing then understood how the Germans were using superencipherment, and that the German navy was probably using a system similar to that employed by the commercial vessels. With these clues they were soon reading the German naval messages.

Also in October Ewing's troops received a third find, another type of naval code taken from a German submarine that had been engaged and sunk by British forces. Thus by the end of autumn Room 40 had the three main German naval codebooks. British fortunes continued in that vein for the entire war – codebooks came from submarines, surface vessels, and even zeppelins shot down over the Continent. For their part the Germans did not seem to understand the significance of losing a vessel that carried a codebook, and they did not change their codes and enciphering tables often enough to stay ahead of the enterprising British.

Room 40 eventually came under the command of Admiral William Reginald "Blinker" Hall, and acquired a core group of cryptanalysts that served Britain well for over thirty years. But the effort was kick-started by acquisitions. Without them, it is anyone's guess how much time would have been required to penetrate German code systems.[1]

Sometimes the origins of a cryptanalytic triumph are murky. So it is with the Zimmermann Telegram. Room 40 obtained a plaintext version of a telegram from the German foreign minister, Zimmermann, to his ambassador to Mexico, von Eckhart, promising Mexico the lost territories of Texas, New Mexico and Arizona if it would join Germany in the war. Admiral Hall arranged to have the text communicated to President Wilson, who turned it over to the newspapers. This was a critical turning point in a chain of events that led to American entry into the war on the side of England.

How had Hall obtained the plaintext? Many conspiracy theories arose, all involving surreptitious acquisition. Hall himself attributed the acquisition to a German diplomat in the Middle East. The historical consensus was that it was probably an acquisition.

But it probably wasn't. American cryptanalysts William Friedman and Charles Mendelsohn examined the reconstructed code (provided by the British after the war), and found evidence of incomplete recoveries and the painful process of reconstruction characteristic of straight-out cryptanalysis rather than a code pinch. They concluded that Hall's memory by 1926 had gone fuzzy. But perhaps, just perhaps, Hall made it all up, as he had done several times before to conceal the cryptanalytic talents of Room 40.[2]

In fact, two codes were involved. We know that Room 40 had partially decrypted 7500, the newer and more complex code used to transmit the telegram from Berlin to Washington. Partial decryptions are not characteristic of purloined codes. The second, 13040, used when the German ambassador in Washington re-encrypted and transmitted the message from Washington to Mexico City, was much simpler in construction, had been in use for many years, and was at the time almost completely recovered. It is hard to imagine Room 40 not being able to read it by 1917. Given their considerable expertise by then, they would not have needed a code pinch to get virtually the entire text from that version.

The Americans

During World War I the Americans struggled to learn what the British and French already knew about codebreaking. Herbert Yardley, the young lieutenant who was charged with providing the U.S. Army with cryptanalytic expertise, had little of it himself. His efforts to learn from his allies were unsuccessful. The Army benefited occasionally from battlefield acquisitions, but Yardley does provide us with one instance of an outright acquisition. The Spanish diplomatic codes had proved especially resistant, and Yardley resorted to thievery to acquire them. He benefited from an entry into the Spanish embassy in Panama, which provided him with one of the codebooks (there were, in all, nine families of Spanish diplomatic codes), and an agent man-

aged to obtain the indicator system from the Spanish code clerk in Washington. With the indicators he knew which family a message fell into, and with the cribs he was able to read some Spanish diplomatic messages through the end of the war.[3]

While Yardley deliberately employed agents to get the Spanish code, the Navy turned the procedure on its head. The Office of Naval Intelligence (ONI) obtained codes, then established a code-breaking organization to put the acquisitions to use. It seems that ONI had a secret slush fund left over from World War I. The money was deposited in the personal bank account of the Director of Naval Intelligence, a situation that could have become highly embarrassing had it ever come into public view. In the early 1920s (the dates from various sources are contradictory), the DNI decided to use the money to finance break-ins for intelligence purposes. One of the first such was into the Japanese consulate in New York, and it resulted in the acquisition of the main Japanese naval codebook, which they called Red. Two former missionaries were employed to translate the book, and in 1924 the Navy established the Research Desk in OP-20, which became known as OP-20-G, the cryptologic arm. Their first job was to exploit the Red code.[4]

ONI continued breaking into foreign diplomatic establishments throughout the 1920s and 1930s, and provided the results to OP-20-G. Ellis Zacharias, who served as point man for many of these exploits, discussed in his autobiography no fewer than six entries into Japanese diplomatic establishments alone from 1920 to 1935. Some entries succeeded; others did not.

His most notable exploit (and the best documented) was a pretextual entry into the Japanese naval attaché's apartment in the Alban Towers in Washington in 1935. Surveillance of the apartment complex had revealed clicking noises that sounded like a machine – perhaps a cipher machine! They came away empty-handed, not the last time that an entry team left without anything in its black bag.[5]

On the eve of American entry into World War II, the Twelfth Naval District in San Francisco had assembled a team of entry specialists under the leadership of a private detective, the eponymous Seaman Gaddis. In May of 1941 Gaddis and his team dressed up like customs inspectors and boarded a Japanese merchantman anchored in the Bay. Gaddis had a small stash of illegal drugs that he arranged to "find" in the captain's cabin and, in the chaos that surrounded the arrest of the startled crew, made off with their merchant codebook. The Army, which had already broken the system, protested that the Navy should do nothing further to alert the Japanese to the vulnerability of their codes.[6]

Entries were the most daring part of code breaking. Writer Steve Budiansky sums it up: "Breaking into foreign embassies was so outrageous a breach of diplomatic obligation that it made reading other gentlemen's mail look like kid's stuff by comparison. It was completely lacking in legal cover."[7]

There is no question that codebook acquisitions jump-started the Navy in the cryptanalytic business. While they would have come to it sooner or later, there is just nothing like a theft of crypto-material to prick the interest. But once the Navy got into the business, they assembled a team of remarkably skilled cryptanalysts, led by Agnes Driscoll. Driscoll and her protégés kept continuity on the Japanese navy's fleet code even after the Japanese changed it, and broke a good many Japanese naval systems for which they never received any help.[8] It is sometimes better to be lucky than good, but being both lucky and good is the very best one can hope for.

The U.S. Army had an entirely different problem. After the closure of the Black Chamber in 1929, it was starting from scratch – a newly formed cryptologic organization, without experi-

ence or continuity. Moreover, they were confronted with new machine systems on Japanese diplomatic circuits. The first such system, which the Army called Red (not to be confused with the Japanese naval attaché code, a paper codebook also called Red), came on-line in 1935. It wasn't that hard to tackle, and several countries broke the machine. This was owing to the decision by the Japanese to encipher vowels for vowels and consonants for consonants.

The second, Purple, appeared a few years later. It was an entirely different proposition. The Japanese had designed a machine whose cycle length was almost beyond calculation, in theory the best available at the time. The Army had no clue what it looked like, and they got not even a peek at them until after World War II had ended. (Unsourced allegations by some writers that the Army had photographs of some parts of the Purple machine can be dismissed as totally lacking in proof, and are countered by vehement denials from all the analysts who worked on the problem.) The only help they got came from the Japanese themselves. They had taken their magnificent machine and had hard-wired its circuitry to reduce the cycle length from virtual infinity to a somewhat more manageable number.

Still, the total lack of any clues to the Japanese machines drove this cryptanalytic problem into the realm of the extremely unlikely. The U.S. Army's decryption of Purple was one of the most extraordinary of cryptanalytic accomplishments. It offered proof to the theorem that pure cryptanalysis is not a figment of someone's overwrought imagination. [9]

Enigma

At first blush the Poles appeared to be unlikely cryptanalytic geniuses. Yet in the 1920s Poland was producing some of the best mathematicians in the world. Their cryptologic organization was one of the first two (the United States Army was the other) to understand that cryptanalysis of a machine cipher required mathematicians. Moreover, they acted on their inspiration and assembled the best mathematicians from the graduating class of 1929 and taught them cryptanalysis. Only the very best of the best were retained. They were young, energetic, and had absorbed the most recent mathematical knowledge.

The Poles tried to attack Enigma through pure cryptanalysis. In October of 1932 they sequestered their finest crypto-mathematician, Marian Rejewski, in a room on the third floor of the general staff building. Working from all available knowledge about the commercial Enigma, he used advanced algebraic formulas to factor out knowns and attack unknowns through statistical probability. He already knew that the indicator system stemmed from the Enigma key sequences themselves, rather than from a separate system, and there were defects in the way the indicators were sent that permitted the cryptanalyst to extract strings of raw key. But through the end of the year he had been able to read no messages enciphered in the military Enigma.

Rejewski had one other advantage: an instruction manual on the Enigma and directions on how to set the daily keys. This told him for the first time that the Germans had added a plugboard to the machine. These materials had come to the Poles through the chief of the French cipher bureau, August Bertrand. Bertrand had a secret source deep inside the German cipher organization who had provided him with the instruction manuals. Bertrand's documents were rather general – they provided clues, but were not the daily key settings that the French cryptanalysts wanted. He also called on the British and the Poles. The British were in the same fix as the French – they could do nothing without the daily keys. But in Warsaw, the Polish attack was further along.

Bertrand went back again, and this time he returned with the daily key settings for several months. These he turned over to Guido Langer,

who headed the Polish cryptologic branch. But Langer held them back from Rejewski – presumably he wanted to be able to decrypt messages without relying on purloined crypto-materials from an ally who might not be there forever.

Rejewski still could not break the traffic. In December, his supervisor, Ciezki, seeing that they were at a standstill, nudged the process along. He gave Rejewski the keys for September and October. Early in 1933 Rejewski began to squeeze plain text out of the encrypted messages.

Bertrand met his source many times and continued to provide keys to Langer. Langer, however, held them back from his cryptanalysts. They no longer needed the help. But in 1938 the Germans introduced two new rotors, and Rejewski and his compatriots lost the ability to read the messages. At this very moment, Bertrand's source was transferred, and that ended the supply of materials. Poland had stopped reading German Enigma ciphers, and now there were no keys to help them.

Hoping for aid from the allies, Langer called a conference with the British and French in early 1939. It was evident to him that the allies had made far less progress than his own people, and he decided not to reveal what he knew. The conference adjourned without result.

By June the situation had changed dramatically. Poland was on Hitler's short list for invasion. Langer called another conference, this time to pass on to the British and French what the Poles had been able to do with Enigma. He also arranged to have two Enigma analog machines shipped to London and Paris.

This revolutionized the British effort. They were moving their cryptologic effort to Bletchley Park, and began augmenting their existing effort with mathematicians from Oxford and Cambridge. Within a year they were reading German army and Luftwaffe messages.[10]

How much did the French human source help? In the case of the Poles, it clearly gave Rejewski that final boost that he needed. He himself testified to the importance of the human source material: "... the intelligence material furnished to us should be regarded as having been decisive to the solution of the machine."[11]

As for the British, they had gotten the same material in 1931, but were not far enough along on their Enigma attack for it to make the difference. The Poles had assembled the mathematical talent to use the clues – the British had not. Eight years later, they had. Such information was valuable only to those who were ready for it.

In Paris, not even the daily keys made a difference during the 1930s. Once they got the analog from the Poles in 1939, they set up a substantial effort, which included some of the Polish cryptanalysts, refugees from their captured homeland. And there is information (all of it rather vague) that they were reading some messages, although probably not consistently.

To be fair, they didn't have the British advantages. Once their country was occupied, their cipher bureau was constantly on the run. For them, no cloistered Bletchley, no unbothered time, no Oxford and Cambridge. But it is instructive to reflect that in 1940 there were three first-rate scientific powers: Germany, England, and the United States. France no longer belonged to that club.

The history of the attack on Enigma recalls the famous axiom by Louis Pasteur: "Chance favors only the prepared mind."

World War II

Theoretically, Enigma's cycle length ensured it against attack. British success against Enigma came not by "breaking" the machine, but by exploiting weaknesses in German operational procedures. This worked well against the German army, air force and several paramilitary forces like the Gestapo.

It was otherwise, however, with the German navy. The difference, initially, was in the use of indicators. Other services encrypted their indicators by the Enigma itself – break an indicator and the cryptanalyst could recover the starting positions for the rotors and plugboard. But the navy used a bigram substitution table, completely unrelated to Enigma settings, that changed monthly. Recovering the rotor order, plugboard and rotor starting positions took much longer, and often Hut 8 (which worked Germany navy) would be working several days behind real time.[12] In this situation, Hut 8 desperately needed a little help from its friends. Fortunately for them, World War II was almost a replay of the Great War.

The first acquisition came from a German submarine in February 1940. Like the others, it resulted from a dramatic encounter on the high seas, and produced for Hut 8 two unknown rotors, VI and VII. Rotor 8, the final rotor of the naval set, came in August from British divers combing through the detritus of a German submarine sunk off the British coast. Each new rotor acquisition reduced the number of unknowns that Bletchley had to work with, and thus speeded the process of key recovery.[13]

In April a British destroyer captured a German patrol boat disguised as a Dutch fishing vessel. This yielded keys for a few days in April, but once those were exhausted Bletchley again bogged down. For the next major acquisition Bletchley had to wait until February of the following year. The *Krebs*, a German patrol ship, carried the home waters keys for February 1943. This knowledge allowed Bletchley to read the back traffic for that month, and from that they learned more about German procedures. As a result, they also read traffic from April and May.[14]

In 1941 Harry Hinsley, a young Cambridge undergraduate working in the Naval Section at Bletchley, devised a method for actively acquiring crypto-material. Hinsley targeted lone German ships in remote areas communicating through Enigma. The best candidates were weather ships that sat, storm-tossed and isolated, in the North Atlantic for weeks on end. Acting on Hinsley's idea, the Admiralty on May 7 captured the weather ship *Munchen*. This capture yielded a copy of the German weather cipher book (the code that underlay the Enigma encipherment) and the home water keys for June. A second weather ship capture in June provided the July keys.[15]

A few days after the capture of the *Munchen*, a British escort group forced the submarine U-110 to surface. It was carrying key tables for Enigma messages for June, various procedure books, and the bigram indicator book.[16] These various acquisitions reduced processing time on naval Enigma traffic, sometimes to as little as a few hours. The situation was not as favorable as for other Enigma traffic, but it wasn't bad.

But on February 1, 1942, the Germans introduced the second difficulty: they added a fourth rotor to their Enigmas. Since each rotor had twenty-six points, this increased the work factor by 26, and sent naval Enigma processing time through the roof. Bletchley had no four-rotor bombes, and processing four-rotor traffic on a three-rotor bombe, though technically possible, was difficult and time-consuming.[17]

Through a wartime agreement Bletchley got the Americans to design and build four-rotor bombes, but no bombes rolled off the assembly line in Dayton, Ohio, until 1943. Meanwhile, the British limped along, hoping for assistance. On October 30, 1942, they finally got it – another

code capture on the high seas. The unlucky ship was U-559, which was captured in the Mediterranean with the complete indicator list and code tables for the new weather short signals. This was the critical break. It took over a month to begin solving four-rotor Enigma messages, but once they did, the Bletchleyites were never again working in the dark on German naval Enigma messages.[18]

Crypto captures were determinant in breaking the naval Enigma traffic. Bletchley still struggled to recover the keys each day, but without acquisitions their struggle would have been without consequence. In the Pacific, the U.S. Army was confronted with large volumes of Japanese military traffic. Each message was encoded, and the code was in turn enciphered with an additive table. There were as many different additive tables as there were Japanese army area commands, and Army cryptanalysts, who had broken the Japanese machine cipher system used on the diplomatic circuits, could not break the paper codes.

There was one major exception. The water transport code, like the German army Enigma, employed an indicator system that was embedded in the additive book itself. In March of 1943 the Army broke the indicator system, and this allowed them to place some messages in depth. They were helped by the highly stereotypical formatting of the water transport messages, which sent logistics information like sailing dates and time, cargo types, and hold capacities. By June the Army was reading this code system.[19]

Success was not contagious, and in January of 1944, with the war only a year and a half from the end, the main army codes were still unbroken. Then they got lucky. An Australian engineering unit near Sio in northern New Guinea, looking for land mines, found a large metal chest buried beneath a river by the retreating Japanese 20th Army. The chest contained the organization's entire cryptologic library. The code pages, sopping wet, were flown to Brisbane, where the U.S. Army maintained a code-breaking unit. The Army immediately began breaking Japanese army messages, and continued to do so through the end of the war.[20]

Battlefield captures, like naval acquisitions, provided a substantial assist to codebreakers in all theaters. Cryptographic recoveries were more important early in the campaign, and the Japanese air force codes were first broken through codebook recoveries. Later on, Army codebreakers often found that their code recoveries were on target and virtually complete by the time a raw code made its appearance.[21]

During the war American intelligence organizations maintained a vibrant, almost hyperactive, surreptitious entry program. Everyone was doing it: FBI, OSS, Army, and ONI were all out stealing codes. Some of the activities were startling in their scope and audacity. The FBI stole Spanish, Vichy French, Finnish, Brazilian, and Chilean diplomatic codes. The Spanish embassy in Washington was so thoroughly penetrated that FBI and OSS entry teams showed up at the same embassy at virtually the same time, leading to recriminations and accusatorial finger-pointing. OSS was forced to cancel entry operations against Portugal and Turkey because of conflicts with the Bureau.[22]

Although these break-ins were all done against "neutral" nations, they were of interest to American cryptologists. The Army, in particular, had broadened its perspective far beyond the Axis powers, and codebreakers targeted almost any country that sent enciphered messages. Acquisitions lessened their workload and permitted the Army to devote scarce cryptanalytic talent to the major targets.

Spain was the best example. Franco's Spain was of more than passing interest to U.S. diplomatic and military customers. In 1942 Spain switched from code systems the Army could read

to one-time tape systems, which they couldn't. To be readable, a one-time system must be stolen. The FBI, after having waved OSS out of its domestic turf, stole the tapes regularly, and the Army codebreakers came to count on new supplies of tape at regular intervals to keep its customers happy.[23]

Though none of the entry teams was ever discovered (at least, there is no evidence that they were), the military always feared that someone would get caught, and that the target country would change its codes. This fear was behind the infamous Lisbon Incident of 1943. OSS was the unlucky agency.

OSS agents had recruited a Portuguese stenographer at the Japanese embassy in Lisbon, and that agent provided leavings from the trash basket. One such haul included a copy of a classified cable that had been sent in a Purple-encrypted message a few days before. OSS triumphantly circulated a copy of the cable in intelligence channels. Unfortunately for them, Italian intelligence warned Tokyo that cryptographic materials in Lisbon had been compromised. Tokyo dispatched a team to investigate. This did not, in the long run, result in any sort of tightening of the cryptographic belt by the Japanese, but it did alarm the Army, which seized upon the incident to obtain a prohibition on OSS obtaining any more material of a cryptographic nature.[24]

Venona

Venona, now part of the language of intelligence, was one of the most significant of cryptanalytic achievements. In total it consisted of some 2,000 decrypts of KGB and GRU communications relating to Soviet wartime espionage in the United States. The encryption method was one-time pad. Now one-time pads are generally considered to be unbreakable if properly constructed and used. In the case of Venona, a few of the pads were reused. If one discovered reuse, theoretically one could read the messages that were in depth. A depth of one under those conditions is very difficult. Venona was a depth of one.

It was in fact so difficult that many have long assumed that it occurred through an acquisition. And indeed Russian diplomatic crypto materials did make their way to the West, through the now-famous Stella Polaris project. The crypto materials began showing up in Sweden, England, Germany, and finally in the U.S., courtesy originally of the Finnish cryptologic service.

But the timing doesn't work. The materials did not arrive at Arlington Hall (headquarters of the Army's cryptologic service, SSA) until after the initial breaks into the system had been made. Cryptanalysts who worked the project do not remember ever receiving such materials while they were making their recoveries. Like Purple, it was pure cryptanalysis.[25]

There is such a thing as cryptanalysis, and there is such a thing as crypto acquisitions. Sometimes they work together, sometimes in parallel, and sometimes they work at cross-purposes. This is a paper without a bright line. It is impossible to generalize.

There are times when the cryptanalyst needs no help, when help can become harm. Purple is a good example, although hardly the only one. There are other times when the cryptanalyst is stumped and absolutely requires help in order to succeed. Spanish one-time tapes in World War II offer proof And there are the in-between cases, where a system might be readable given a certain expenditure of effort and that critical flash of intuition, but the resources are insufficient. In those cases acquisitions can make the difference.

Sometimes the entry people walk into the room with the entire solution. "Here are the key pads you will need to read every single message." But often they will have only clues, and the cryptanalyst will have to work through the night to use the clues.

There are times when an organization is not ready to use the clues, and the seeds fall on parched ground. This happened in France and England in 1931 with the initial acquisitions for the Enigma.

Above all, a code acquisition must be undetected. Once known, it can result in the enemy changing its codes, and all the effort goes for naught. Remember the words of Henry Gondorf: "You gotta keep his con even after you take his money." It could be chiseled on the headstone of every agent that ever carried a black bag.

(U) Notes

1 On World War I codebook acquisitions, see David Kahn, *Seizing the Enigma: The Race to Break the German U-Boat Codes, 1939-1943* (Boston: Houghton Miffiin Company, 1991), 15-30. Also useful is Nigel West's *GCHQ: The Secret Wireless War*, 1900-1986 (London: Weidenfeld and Nicolson, 1986), 38.

2 There are many sources on the Zimmermann telegram, but few of them possess the discerning analysis of the true cryptanalyst. Rather than Barbara Tuchman's popular *The Zimmermann Telegram* (New York: The Macmillan Company, 1958), read Henry Schorreck's "The Telegram That Changed History," *Cryptologic Spectrum* Vol 1, # 2 (Summer, 1970). 22-31. A retired NSA historian, Mr. Schorreck also received training in cryptanalysis.

3 Herbert O. Yardley, *The American Black Chamber* (Indianapolis: Bobbs-Merrill Company, 1931), 172-196.

4 Stephen Budiansky, *Battle of Wits: The Complete Story of Codebreaking in World War II* (New York: The Free Press, 2000), 4-5. See also Frederick Parker, *Pearl Harbor Revisited: United States Navy Communications Intelligence, 1924-1944*, United States Cryptologic History, Series IV, Vol. 6 (Fort Meade, MD: NSA, 1994).

5 Ellis Zacharias, *Secret Missions: The Story of an Intelligence Officer* (New York: G. P. Putnam's Sons, 1946),178-82; Budiansky, 83-84.

6 Budiansky, 84; Rear Admiral Edwin T. Layton with Captain Roger Pineau and John Costello, *And I Was There: Pearl Harbor and Midway - Breaking the Secrets* (New York: William Morrow and Company, Inc., 1985), 109-110.

7 Budiansky, 83.

8 For examples, see Budiansky, 83, and G.J.A O'Toole, *Honorable Treachery: A History of U.S. Intelligence, Espionage, and Covert Action from the American Revolution to the CIA* (New York: Atlantic Monthly Press, 1991), 334 and 342.

9 For a description of the process by which the Army attacked Red and Purple, see Frank B. Rowlett, *The Story of Magic: Memoirs of an American Cryptologic Pioneer* (Laguna Hills, CA: Aegean Park Press, 1998). The best discussion of the Purple machine itself is Steve Kelley's *Big Machines* (Laguna Hills: Aegean Park Press). For a sample of the "unsourced allegations," see Nigel West, *GCHQ: The Secret Wireless War, 1900-1986* (London: Weidenfeld and Nicolson, 1986), 172.

10 A good discussion of the interplay between human sources and cryptanalysis is Kahn's *Seizing the Enigma*, 55-84. See also Josef Garlinski, *The Enigma War: The Inside Story of the German Enigma Codes and How the Allies Broke Them* (New York: Charles Scribner's Sons, 1979).

11 Marian Rejewski. "How Polish Mathematicians Deciphered the Enigma." *Annuals of the History of Computing* (July 1981)3: 221, quoted from Kahn, *Seizing the Enigma*. 66.

12 Budiansky, 151-52.

13 Kahn, 104-111, 129-36; Budiansky, 191.

14 Budiansky, 156.

15 Kahn, 170-73.

16 Kahn, 161-69.

17 Kahn, 214-17.

18 Kahn, 218-27; Budiansky, 283-84.

19 Budiansky, 320-23.

20 Sharon Maneki, *The Quiet Heroes of the Southwest Pacific Theater: An Oral History of the Men and Woman of CBB and FRUMEL*, United States Cryptologic History, Series VI, Vol 7 (Ft. Meade: NSA,1996), 17,25,40-41.

21 Maneki's book offers many examples for the Southwest Pacific Theater.

22 Matthew Aid, draft of an unpublished book, furnished by the author; David Alvarez, *Secret Messages: Codebreaking and American Diplomacy, 1930-1945* (Lawrence: University of Kansas, 2000),171; Donald Downes, *The Scarlet Thread: Adventures in Wartime Espionage* (London: Derek Verschoyle, 1953), 93-9.

23 Alvarez, 171.

24 The Lisbon Incident is described by many sources. See, for instance, Alvarez, 162-63, and Budiansky, 259-60.

25 Alvarez, 215-17.

(U) Dr. Tom Johnson is a retired NSA employee now working on contract to CIA. He worked in the U.S. SIGINT System from 1964 to 1992 in a variety of operational jobs both at Fort Meade and in the field. In 1992 he joined the staff of the Center for Cryptologic History, where he completed a four-volume history entitled American Cryptology during the Cold War, 1945-1989. He is the author of other books and articles, mostly on historical cryptologic topics, and has been a long-time contributor to Cryptologic Quarterly. He lives in Front Royal, Virginia.