How Mathematics Saved the World:
The Allies' decryption efforts during World War II
Written for Dr. David Beatty, History 3300
on January 25, 1998

by Andrew R.W. Sharpe

When Adolf Hitler approved the Enigma ciphering machine for use in his plan of world domination, he made a fatal mistake in assuming it was unbreakable. Overconfidence was perhaps the enemy's greatest fault; it ultimately led to their defeat. Military intelligence took on a whole new meaning in World War II. The enemy had made use of a new technology, encrypting their messages using electronic devices, making their communication almost air tight. Encrypting one's secret correspondence was not a recent invention. Julius Caesar was doing it as early as 50 BC. But the use of machines brought cryptography to a new level, since machines are much better at performing simple, monotonous tasks than we are. Hitler did not expect his foe to be able to read his orders. He underestimated the resourcefulness of desperate men, namely the Poles. Under threat of attack from the Nazis, they employed brilliant mathematical strategy to solve Hitler's Enigma. Only recently has the effect of cryptanalysis on WWII been brought to the fore. The Allies thought their intelligence victories so monumental, that they insisted on keeping the details secret for more than twenty-five years. It was only in the mid-seventies and eighties that the respective governments began to release information on how they were able to read the enemy's most secret transmissions. This paper will summarize the decryption efforts of the Allies, and show how important these efforts were to the cause. The Allies did not know it at the time, but the Poles had started them on the road to victory.

Cryptography is the art of encoding and decoding messages, or text. The original, unencoded text is called 'plaintext', which is readable by humans. The encoded text, usually unreadable by humans, is called 'ciphertext'. Encryption is the procedure that turns plaintext into ciphertext, while decryption turns ciphertext into plaintext. The 'cipher' or 'encryption algorithm', encrypts a series of plaintext. One method of encoding involves using a 'cipher key' (or just 'key'), which is usually just a short piece of text (1-10 letters will usually suffice). In this method, the same key is used to encrypt and decrypt the text. One cannot perform any encryption or decryption without both the key and the cipher (algorithm). In the case of the Enigma encoding machine, it was not enough to know how to solve the encrypted message; one also needed to know the key with which the message was encrypted.

In 1919, Dutchman Hugo Koch invented a machine capable of encrypting messages by typing onto a keyboard, which would produce encoded text out the other side. The difference between this and other coding machines is that the same letter would not necessarily encode to the same character every time. For example, suppose you typed the letter 'a', and 'g' came out the other side. The next time you typed 'a', a 'u' may come out the other side, rather than the 'g' that you might have expected. This made ciphertext very difficult to decrypt, since frequency analysis (seeing which character repeats most often, and then guessing that to be whatever character occurs most often in whatever language you are dealing with) solved nothing. Koch found little interest in his machine, and so he sold it to a German engineer named Dr. Arthur Scherbius. Scherbius improved the machine, and began shopping it around. He renamed it the Enigma, and sold it to the German government. At first the German military was reluctant to put the Enigma into use. However, after assurances by their team of

cryptologists that the machine was literally impossible to break (they claimed it would take a team of cryptologists over four billion years to find the cipher key for any given encryption), they began mass production of it. Like tanks and ammunition, manufacture of the Enigma was disguised in factories whose products were supposed to be non-military goods. (Kahn, "Seizing the Enigma," pp. 31-48) Hitler was putting his puzzle together and it was clear that he considered the Enigma a big piece.

Meanwhile, in Poland, the military saw the need to develop a cryptography unit. They were suspicious that the Germans were reading their Air Force messages, and felt this was an area that needed concentration. They organized a cryptography course for students of Poznan University. Three students of particular interest qualified for, and enrolled in the class: Marian Rejewski, Henryk Zygalski, and Jerzy Róycki. Rejewski graduated from Poznan with a Masters in Philosophy (essentially a mathematics degree at the time), and went to Göttingen University in Germany for training in the actuarial field. He stayed only a year, returning to Poznan in October of 1930. While in Germany, Rejewski had noticed a feeling of ill-will toward Poland, which escalated when Hitler came to power. When Rejewski returned, he found his former colleagues decrypting German ciphers for the Polish Cipher Bureau in the basement at Poznan University. He joined them in their attack on the messages. By 1931, they noticed a change in the German encryptions, and were unable to decrypt any further messages. The Enigma, for the time being, had them stumped. (Kozaczuk, pp. 1-6)

Though the Poznan cipher group was soon disbanded, Rejewski, Zygalski, and Róycki all accepted full-time employment with the Polish Cipher Bureau, Biuro Szyfrów (BS-4), in Warsaw. The three mathematicians made progress, but were still unable to decrypt the intercepted messages. Meanwhile, the British and French were experiencing even more difficulties. They too had noticed a change in the German encrypted communications. A huge break into the mystery came when Captain Gustave Bertrand, chief of French radio intelligence, was approached by a German officer who claimed he had information for sale. The spy, Hans-Tilo Schmidt, was the younger brother of a high-ranking officer in the German military. He went by the codename "HE," which in French would be pronounced 'ashh-e'. The French simply referred to him as Asche, and this is how he is referred to in most texts. Once Asche was cleared by French intelligence, he supplied them with two key documents: an operating manual for the Enigma, and several encryption keys to Enigma ciphers. Betrand presented these to his cryptography unit, who shrugged their shoulders. So Betrand went to the British, but they too claimed that it was not enough to solve Enigma. Captain Bertrand had heard of the success of the Polish cryptanalysts, and so he passed the stolen information on to them.

Rejewski was ecstatic to receive this from the French, much to Betrand's surprise. French intelligence continued to correspond with Asche, and in turn continued to pass this information on to the Polish Cipher Bureau (BS-4). Bertrand could not understand why the Poles were so happy to receive the documents, since they reported no success. Rejewski and his crew were having an enormous amount of success; however, they did not report this to the British, since they were not yet convinced it was necessary. In December of 1932, Marian Rejewski solved the German military Enigma. His solution was mathematical in nature, but when combined with the stolen documents provided by the French, it was enough for him to construct a working model of the machine. By January of 1933, the Poles could read German military transmissions. (Kozaczuk, p. 21) Rejewski's method, however, was time-consuming. The most troublesome task was that of finding the cipher key for an individual message. In 1938, as the war drew near, Rejewski, Zygalski, and Róycki, constructed a machine capable of computing the

encryption key within two hours. They called this machine 'the bomb' (in some texts it is referred to as the bomby, or bombe). Thus, the Luftwaffe version of the German Enigma could be read regularly.

In September of 1938, Asche ceased contact with the French. He had been transferred to a different job in the military. (Kahn, "Seizing the Enigma," p. 78) The situation surrounding his death is somewhat cloudy. Kahn reports that a French intelligence agent, captured and tortured by the Germans, gave up Asche's identity. He was then arrested, convicted of treason, and shot in July 1943. (Kahn, "Seizing the Enigma," p. 115) Hawker claims that Asche was indeed convicted of treason by the German government, but claims that he committed suicide in his jail cell in 1942. (Hawker, "Breaking the Code.") In any case, Hans-Thilo Schmidt (Asche), though he was payed handsomely by the French government, is owed a debt of gratitude by the Allies.

On January 9, 1939, British, French, and Polish representatives of their respective intelligence agencies met in France to discuss their progress in decrypting Germany's transmissions. None of the three reported success, though they did share what they knew, and agreed to share the decryption load. The Poles still did not tell the French and British that they had solved Enigma. In the summer of 1939, Hitler declared the non-aggression pact of 1934 between Germany and Poland nullified. The scientists at BS-4 knew an attack was imminent, and that it was imperative that they pass the Enigma information on to the Allies. They had come to a stand-still in reading the messages, and felt they needed the Allies' help anyway. The Nazis had altered the Enigma, adding two more rotors to the choice, increasing the possible choices of encryption keys by a power of three. So on July 24, 1939, BS-4 invited Britain and France for a meeting in Warsaw. Here they divulged all that they knew about the German military Enigma, including a demonstration of the model Rejewski had built. The British in particular were amazed, and immediately sent for engineers. The Poles, however, informed them that this was not necessary since they had reconstructed two more Enigmas, one for the British and one for the French. Soon after the meeting, the two Polish-constructed Enigmas arrived in France, and the French sent one to Britain. Kahn remarks that, "Once again, as in World War I, Britain had obtained the means for solving her adversary's messages through a gift from a loyal ally." (Kahn, "Seizing the Enigma," p. 81) One month later, on September 1, Germany invaded Poland. Rejewski, Zygalski, and Róycki narrowly escaped to Romania, but not before they were forced to destroy all their equipment and files, for fear that the Nazis would find out what they had accomplished. From Romania, they contacted Bertrand, who immediately had them transported safely to France, so that they might continue the attack on German encoding. (Kozaczuk, pp. 70-72)

There is a lot of misinformation floating around about who solved the Enigma first. Authors and former intelligence officers such as Kenneth W.D. Strong and Frederick W. Winterbotham distort the truth, claiming that it was the British who solved Enigma, with a little help from the Poles. (Jedd, section 2 on "the Enigma") William Stevenson's biography of former head of British Intelligence Sir William Stephenson (the similarity in names is purely coincidence) also glorifies the achievements of the British. Stevenson claims that the Polish gift of Enigma to the British had been stolen from a German military truck, not mastered and then rebuilt. (Stevenson, p. 49) Kozaczuk, among others, criticizes Stevenson's account as biased and exaggerated, describing his remarks on Enigma as "most charitably characterized as history-fiction." (Kozaczuk, p. 327) The majority of historians seem to agree that Poland was responsible for the initial solution of the Enigma. Indeed, Britain was reading the commercial version well before the outbreak of war, but this version cannot compare to the military version in use by the Nazis. (Kahn, "Seizing the Enigma," p. 87) David Kahn is a well respected

author, who has published many books and articles on the subject of the Enigma. (See Jedd's commentary on "Seizing the Enigma") He writes, "The solution was Rejewski's own stunning achievement, one that elevates him to the pantheon of the greatest cryptanalysts of all time." (Kahn, "Seizing the Enigma," p. 66) James Rusbridger, another respected author on the subject, supports Kahn and Kozaczuk when he writes that the British and French were nowhere near solving the Enigma until the Poles helped them out in July of 1939. (Rusbridger, "Winds of Warning," p. 8) Glenn Zorpette and Józef Garliski also support Kozaczuk in his claim that "the solution of Enigma, in all its evolving manifestations during the years 1933-39, was a purely Polish achievement." (Kozaczuk, p. 95) Kozaczuk goes on to comment on the British's lack of acknowledgement for Polish contributions, "If the behaviour of the British can be explained by the imperatives of wartime secrecy, then certainly the passing over of the Poles' contributions until recently in contemporary publications is, to say the least, incomprehensible." (Kozaczuk, p. 208)

By the time of the invasion of Poland, Hitler was using roughly 40,000 Enigmas. (Kozaczuk, p. 61) The Nazis had, as mentioned, altered the machine by adding two rotors, making the total number five. This made decryption significantly more difficult, and for almost eight months the Allies were unable to decode radio intercepts. The three Poles mentioned earlier were now working for the French code and cipher agency, which was codenamed 'Bruno.' From here they corresponded with Britain's center for cryptography, the now famous Bletchley Park. The intelligence operation at Bletchley was codenamed *Ultra*. Ultra had benefited greatly from earlier assistance from the Poles, not to mention the Enigma it had received from them. Bletchley employed about 120 people, though this number would jump to nearly seven thousand in 1944. (Hinsley, p. 15) The British had followed the Poles' lead, hiring cryptologists with stronger mathematical backgrounds. These men and women (women cryptologists at Bletchley included Hilary Brett-Smith and Mavis Lever) had several decryption projects on the go by 1939. They were working to break the new 5-rotor Luftwaffe Enigma, as well as the naval version of the machine, which was wired differently. By May of 1940, they were once again reading the Luftwaffe's transmissions, but had still not been able to aid the Battle of the Atlantic by solving the naval Enigma. (Kahn, "Seizing the Enigma," p. 103)

In February of 1940 the British received a lucky break involving captured vital information from the German U-Boat *U-33*. It seems one of the captured German seamen, terrified and confused by the attack, had forgotten his captain's orders to throw the Enigma rotors into the sea. The boarding crew from the British vessel *Gleanor* confiscated the rotors, and shipped them to Bletchley immediately. This, combined with cipher keys captured from the German ship the *Krebs* in March of 1941, enabled the British to finally crack the Nazi naval Enigma. (Kahn, "Seizing the Enigma," pp. 136-137)

Though by late 1941 the Allies were capable of reading the German's naval messages, they did not have the manpower to do so with enough efficiency to contribute to the war effort. Churchill's visit to Bletchley Park on September 6, 1941, gave the cryptologists the break they needed to prove how important their contributions could be, if only the government could supply more resources. Churchill agreed, and provided them with more finance and man power. Correspondence with the United States in January, 1941 led to a strong intelligence alliance. The code-breaking efforts of these two nations, and France until its invasion in May of 1940, greatly influenced the outcome of the war, as will be discussed later. By 1943, the Allies could read German naval messages regularly. This monumental effort would change the tide of the Battle of the Atlantic. "This triumph, the result of hard work by brilliant people hidden in the

shadows and the daring of men at sea, was the greatest extended intelligence exploit of all time." (Kahn, "Seizing the Enigma," p. 242)

While the Polish, French, and British were primarily working on Germany's ciphers, the US Signals Intelligence Service (SIS) was hard at work on the Japanese version of the Enigma. Codenamed 'Purple' by the Americans, this machine cipher was a modified version of the Enigma which the Japanese called '97-shiki-O-bun In-ji-ki.' The SIS, headed by William Friedman (1891-1969), broke this cipher in September of 1940. Although Friedman himself is often given credit as being the man who broke Purple, it was actually a team effort; one should not leave out Frank B. Rowlett's name, who was the head cryptologist. (Prados, p. 164) The SIS had already broken a previous version of Purple, which they had codenamed 'Red.'

Author John Prados believes that the solution of Purple was even more impressive than that of Enigma: (note that 'machine A' refers to Red, while 'machine B' refers to Purple) "The break into Purple is especially remarkable both because the B machine was highly sophisticated - much more sophisticated than the German's Enigma - and because the code was solved entirely by mathematical analysis." (Prados, p. 164) Prados's comments are incorrect for two reasons. Firstly, Enigma **was** solved by pure mathematical analysis, Rejewski had done it in 1932 (see earlier discussion on who cracked the enigma). Secondly, solving a problem mathematically is no more impressive than if one were to build a machine to solve the same problem. Either way, Enigma was broken, whether or not it was solved by mathematics does not make it any more or less impressive. Prados also believes that the solution of Purple is more remarkable because the "Americans solved Purple all by themselves." (Prados, p. 164) Prados is wrong again. Kozaczuk's comment on the solution of Enigma being purely a Polish achievement has already been backed up in an earlier paragraph. It is possible that Prados is referring to the British's continuing efforts to keep reading the ever-changing Enigma. Even if this is so, is the reading of Enigma less impressive because a country employs an alert foreign policy?

While the US Army was solving the Japanese Purple machine, the Navy was working hard on the Japanese naval version of the Enigma, which was codenamed 'JN-25.' The solution to this machine came just after that of Purple in the fall of 1940. Also, right around this time, the US Army and Navy agreed to share all cipher information on their respective projects; the US version of Ultra was codenamed project 'Magic'. The communication between Magic and Ultra prior to 1941 had been sporadic at best, with neither side revealing any information of great importance. This changed in January of 1941, when the two sides started an intelligence alliance that would change the tide of the war. The British traded the solution of the Enigma for the American solution of Purple. (Kahn, "Seizing the Enigma," p. 80) They also agreed to share all further intelligence on the enemy's ciphers. The British agreed to train Americans in the art of code-breaking, since the US was in short supply of cryptanalysts.

More important than the solutions of Enigma and Purple is the solution of Tunny. (Zorpette, p. 49) This German machine has received much less attention than the other two because of the intense security which has shrouded the details in secrecy until only recently. Tunny was the codename given to the machine the Germans called 'Schlussel-zusatz 40.' It was manufactured by a German company called Lorenz, and it therefore sometimes referred to as the Lorenz-machine. This electronic cipher was used to encrypt top secret messages from German high command, many of which came directly from Der Fuhrer himself. On August 30, 1941, a German radio operator made a crucial mistake which allowed the Allies to solve Tunny. Upon sending a four-thousand character message, he received a

request from the receiving station to please re-send due to an error. He then made the mistake of resending the message using the same start settings for Tunny, which was against Nazi procedure. Bletchley, who had intercepted both messages, simply compared the two for subtle differences, which allowed them to decrypt the message. (Fox and Webb, p. 40) Professor Max Newman and Tommy H. Flowers designed an electronic device, based on the theoretic work by Alan Turing, which would mechanize the solution of Tunny. They named the machine Colossus, and since its invention in 1943 predates that of the ENIAC, it has been argued as the world's first electronic computer. (Zorpette, p. 48) Colossus and its successor Mark II, were incredibly efficient at performing the tasks they had been designed for. For example, even today's Pentium computer cannot compete with the tasks that Colossus and Mark II were programmed to do. (Fox and Webb, p. 43) The reason so little information about Colossus is known is because Prime Minister Churchill had it destroyed and its blueprints burned, for fear that the enemy would discover it. (Fox and Webb, p. 39) The existence of Colossus was not even confirmed until 1976. Today, Tony Sale, an ex M15 intelligence agent, is attempting to rebuild what he feels was the world's first electronic computer. There is also a science-fiction movie and play based on Colossus.

Allied solutions of both German and Japanese cipher machines were ingenious, innovative, and highly technical, but did they affect the outcome of World War II? Sufficient evidence exists to answer with a resounding 'Yes.' While there are a few authors who claim the battles were won by guns and bombs alone, most claim that military intelligence was every bit as important, if not more. Chief of British Security Coordination (BSC), Sir William Stephenson, put it well when he told Churchill, "If we can read their signals, we can anticipate their actions." (Sir William Stephenson in Stevenson, p. 30) In fact, Allied decryption efforts were responsible for several key victories against the enemy.

The naval forces involved in battles in the Atlantic and Pacific ocean were particularly reliant on transmissions from headquarters to dictate their actions. Subsequently, any insight into an enemy's transmissions would provide a great weapon, both for offensive and defensive confrontations. The German U-Boats communicated with Nazi high command using Enigma-encoded radio messages; the Japanese used JN-25 to do the same with their military leaders. The ability to read these ciphers allowed the Allies to predict an Italian naval strike on March 27, 1941, and so they were ready for the Battle of Matapan. This key Allied victory drove the Italians from the Mediterranean. (Kozaczuk, p. 168) Garlinski supports the claim that Ultra had a substantial impact on the results at Matapan (Garlinski, p. 129), as does Hinsley. (Hinsley, p. 17) David Kahn adds the Battle of Midway (June 4, 1942) to the list of key naval victories influenced by allied code-breakers. (Kahn, "The Intelligence Failure...", p. 151)

Controversy arises when authors such as Hinsley and Zorpette claim Ultra aided in the sinking of the great German warship Bismark on May 27, 1941. Hinsley argues that Allies' decryption efforts played a large part in the Bismark's defeat. (Hinsley, p. 17) Zorpette agrees. He claims that Ultra had deciphered Luftwaffe Enigma messages detailing an unspecified mission over Brest, which the allies guessed to be the protection of the Bismark. (Zorpette, p. 47) Although the ship **was** sunk only 800 miles off Brest, Kozaczuk claims that Ultra had nothing to do with the victory, since the British could not read naval ciphers at that time. (Kozaczuk, p. 195) Since it is not exactly clear when in 1941 the Allies cracked the German naval Enigma, the controversy remains unsolved.

In April of 1943, US code-breakers intercepted a Japanese message which described the location of an inspection by Admiral Isoroku Yamamoto. Yamamoto was loved by the Japanese navy, and was responsible for many Allied defeats.

The decrypted message revealed that he would be landing in the Solomon Islands on April 18. American fighters took off from Guadalcanal's Henderson Field, intercepted, and destroyed the plane carrying Yamamoto. This assassination struck a tremendous blow to Japanese morale. The loss of Yamamoto, a brilliant leader and strategist, significantly aided the Allies' struggle in the Pacific Ocean. (Rusbridger, "The Sinking...," p. 9) Both Rusbridger and Kahn (Kahn, "The Intelligence Failure ...", p. 151) list the assassination of Admiral Yamamoto as one Magic's greatest accomplishments.

July of 1943 saw the invasion, and subsequent conquering of Sicily, Italy by the Allies. Codenamed 'Husky,' this invasion was largely based on Enigma decrypts. (Kozaczuk, p. 175) Included in this invasion was a planned assassination of German Field Marshal Albert Kesselring, whose location was revealed by Enigma decrypts to be the San Dominico Hotel in Laormina. The British bombed this hotel, but Kesselring was in Rome at the time (though he was staying at the San Dominico while in Sicily). In any case, the conquest of Sicily triggered the collapse of Benito Mussolini's Fascist government. It struck a huge blow to the Nazi war effort, and was mostly due to projects Ultra and Magic. (Kozaczuk, p. 175)

Hitler's V-1 rocket was a weapon he planned to use as an aid in his destruction of Britain. Nicknamed the Vengeance Weapon by Nazi propagandists, it threatened the safety of Britain's citizens, as well as its military. The Allies were aware that Hitler was building the V-1, and they longed to destroy it before Hitler could do any damage. Enigma decrypts revealed Peenemünde, Germany, as the launch sight. In August of 1943, the Allies bombed Peenemünde and set the production of the V-1 back six months. (Kozaczuk, p. 186) Had the Nazis been able to launch the V-1 as planned, the Allies may not have been able to launch Operation Overlord, the invasion of France. Hitler himself said of V-2 (V-1's successor), "If I had had this weapon in 1939 we would not be at war now." (Adolf Hitler in Jedd, paragraph 6) Although Hitler did eventually build and use both the V-1 and V-2, one can easily see how Enigma decrypts aided the war effort in this situation.

Operation Overlord was the codename given to the planned invasion of France by the Allies in August of 1944. This invasion was highly influenced by decrypted Enigma messages from Field Marshal Gunther von Kluge to German high command. During the summer of 1944, Kluge sent several messages to OKW (Oberkommando der Wehrmacht), the Supreme Command of Armed Forces, and OKH (Oberkommando des Heeres), German Army High Command. These messages consisted of a careful inventory of the troops and equipment under his command. Kluge sent these messages because he had heard a rumour that Hitler, refusing to admit defeat, was commanding non-existent armies. Kluge therefore wanted to make sure that German High Command was sure of what they had available. The fact that the Allies had in their possession the locations and descriptions of all German armoured divisions under Kluge's command allowed them to plan a careful attack, and be able to predict the speed and strength of counter-attacks. (Hinsley, p. 20, also Kozaczuk, p. 182) The information from von Kluge's reports led to the Allied victory at the Battle of Falaise, the key Western battle of Overlord. Frederick W. Winterbotham calls this victory "Ultra's greatest triumph." (Winterbotham in Kozaczuk, p. 185)

Although Allies' decryption efforts affected many other events of the war, only the key battles which they influenced have been discussed. One should consult the works of Kozaczuk and Kahn for detailed descriptions of these and other battles which may or may not have been determined by Allied interception of enemy communications. Still, considering the importance of the battles discussed, it

should be enough for one to conclude that the work of projects Ultra and Magic greatly influenced, and perhaps even determined, the outcome of World War II.

The extent to which code-breaking affected the Allied victory has been discussed at length by historians. Hinsley emphasizes the effect Ultra had on Operation Overlord. He goes on to claim that the ability to predict U-Boat locations saved 1.5 million tons of Allied shipping. (Hinsley, p. 19) General Dwight Eisenhower, future president of the United States, once remarked to the British Intelligence Agency, "The intelligence which has emanated from you before and during this campaign has been of priceless value to me. It has simplified my task as a commander enormously. It has saved thousands of British and American lives and, in no small way, contributed to the speed with which the enemy was routed and eventually forced to surrender." (Eisenhower in Coghlan, p. 45) Still, it would be an overstatement to claim that Allied cryptanalysts won World War II. Even though Kahn describes the decryption of German coded radio messages as "the chief hidden factor that helped the Allies win," (Kahn, "Seizing the Enigma," p. ix) he also admits that neither Ultra, nor Magic, nor the combination of the two, won the war. (Kahn, "Seizing the Enigma," p. 277) He instead reports that "Enigma solutions saved between 1.5 and 2 million tons of shipping in the last half of 1941 and more than 650,000 tons in the first five months of 1943." (Kahn, "Seizing the Enigma," p. 277) He also claims that "Ultra saved the world two years of war, billions of dollars, and millions of lives." (Kahn, "Seizing the Enigma," p. 278) Jedd does not agree, claiming that if the Allies, by 1945, had not been close to victory, they would have ended the war by dropping a nuclear bomb over Berlin rather than Hiroshima. (Jedd, 2nd last paragraph) Even if this is true, one can still conclude that Allied code-breaking saved millions of Allied lives, and cost the enemy millions as well.

The necessity of secrecy in military intelligence operations sometimes backfires on a nation. Inadequate or modified records, spies who betray their nations, and even political leaders initiating cover-ups, are all products of this necessary secrecy. But did such things affect the Allies during World War II? Perhaps this question is best answered by evaluating several situations which have been deemed by some as 'scandals', or cover-ups. There exist credible references who claim that the truth has not been revealed about World War II, or some part of it. It is crucial to evaluate why certain things happened during the time of war, so that they do not happen again.

One such incident is the famous Japanese attack on Pearl Harbor, which killed 2,403 Americans, and entered the United States into World War II. The 1945 Congressional Investigation into the Pearl Harbor attack investigated the claim that the Allies had prior knowledge of the attack. The official investigation concluded that they did not, but historians still argue whether or not this is true. The main problem historians and conspiracy-theorists have is this: How did the Japanese achieve complete and utter surprise on the morning of Sunday, December 7, 1941? How, with all the success American cryptanalysts were having, could the US not have been able to predict such a large-scale attack? The answer is not simple, and much has been published on the subject. 1971 Pulitzer Prize winner John Toland wrote a book entitled, "Infamy: Pearl Harbor and Its Aftermath," which is perhaps the leading source arguing the United States government had prior knowledge of the Pearl Harbor attack. (Prados, pp. 172-173) Most authors tend to argue that this is an exaggeration, and that there was no way for the Allies to predict the attack.

The main source of controversy revolves around the now famous "Winds" messages. Transmitted November 19, 1941, these signals supposedly gave an indication of war by including the keywords "East Wind, Rain." It was known to

the Allies at the time that this phrase indicated that Japanese-American relations were in danger, and that Japanese embassies in the USA were to destroy all code papers and encrypting devices. The "Winds" messages also contained an "execute command," though it is not clear just what the Japanese government is ordering execution of. In the 1945 investigation, it was alleged that the "Winds execute" had been intentionally suppressed from the military records. True enough, the file containing the "Winds execute," serial number JD-1:7001, is missing, but the Navy claims that this is not uncommon, and that serial numbers were often cancelled for legitimate reasons. (Kahn, "The Intelligence Failure...," p. 149) Captain Laurence Safford, the head of the Navy code-breaking unit at the time, insists that this record was deliberately removed because knowledge of the Winds execute would prove that the military knew of the attack. Kahn disputes Safford's claim, saying that possession of the Winds execute would still not have been enough to predict the attack. (Kahn, "The Intelligence Failure...," p. 149)

Rusbridger points out that the Winds intercepts were not even decoded until January 28, almost two months after the Pearl Harbor attack. He claims that American cryptanalysts were too busy working on Purple decrypts rather than J-19, which was the device used to encrypt the Winds transmissions. (Rusbridger, "Winds of Warning," p. 11) So even if the Winds messages did contain incriminating information, they were not decrypted in time to prevent the attack on Pearl Harbor.

There are also indications that the US government may have known the location of the Japanese Navy at the time. Indeed, instructions for the Japanese Navy to sail for Hawaii were intercepted, but the military maintains that it did not decrypt these until after the war. The Dutch had provided details that the Japanese fleet were sailing in a southerly direction, but there was no specific mention of Pearl Harbor. Rusbridger concludes that the military did know that some sort of action was to take place on December 7, 1941, but did not know what or where. (Rusbridger, "Winds of Warning...," p. 12) He seems to believe that had one person been in charge of all military intelligence, navy and army combined, and had that one person been given all decoded transmissions, including the Winds execute command, then perhaps Pearl Harbor could have been predicted. However he does not believe that there was any deliberate conspiracy attempt. "Despite some exotic theories propounding the "smoking gun" thesis, all available evidence on the attack on Pearl Harbor points to it being a combination of audacity and security on the part of a calculating enemy, and administrative lethargy largely resulting from years of peacetime penny-pinching that reduced America's ability to react swiftly to what should have been an obvious threat." (Rusbridger, "Winds of Warning," p. 13)

There is also the question of why. Why would a nation's own government allow the slaughter of thousands of its citizens? Originators of the Pearl Harbor conspiracy contend that President Roosevelt suppressed knowledge of the attack in order to force his otherwise reluctant nation into the war. Indeed, if this was Roosevelt's intention, it worked. Immediately following Pearl Harbor, the United States government declared war on Japan. It is has also been contended that it was British Prime Minister Churchill that suppressed knowledge of the attack, due to his desire to have the US as an ally in the war. However, Churchill wanted the US in the war against Germany, not Japan. Kahn argues against these conspiracy-theorists, "The concocters of these theories are unable to accept that humans sometimes do things wrong or do not do them at all, that accidents happen, that in the complex system that is the world improbable events occur." (Kahn, "The Intelligence Failure...," p. 150) Is Kahn suggesting that Pearl Harbor was an 'accident'? Did the US scientists in charge of decrypting JN-25 'do things

wrong'? Could Pearl Harbor have been prevented? Perhaps we'll never know for sure. Perhaps the answer has been 'encrypted' by a higher power.

The bombing of Coventry, England, by the Nazis on November 14, 1940, is another source of controversy caused by decrypts of enemy messages. William Stevenson claims that British Prime Minister Churchill knew of the Germans' plans to bomb the city of Coventry, and allowed the bombing to take place rather than allow the Germans to know that the British could read Enigma. He reports that the British had decoded the order to destroy Coventry, and that the plaintext actually had the city directly named in it, rather than the use of a codeword, which was standard Nazi practice. (Stevenson, p. 153) Lewin disputes this, saying that the decoded message had only the word "Korn," which was the German word for Coventry. He contends that the British did not know that Korn referred to Coventry, and therefore was not aware of the attack beforehand. (Lewin in Momsen, http://members.aol.com/nbrass/2enigma.htm)

It seems possible that Churchill did indeed sacrifice Coventry. If he had evacuated the city, the Germans would have been alerted to the fact that the British could read Enigma. They would have almost certainly changed the cipher, and a key source of military intelligence would have been lost. As head of British Security Coordination William Stephenson once said, "Better lose a battle than lose a source of intelligence." (Stephenson in Stevenson, p. 63) In other words, had Churchill evacuated Coventry, it would indeed have saved many lives, but would have consequently cost many more in the long run. In Churchill's defence, he did alert fire-fighting and ambulance services ahead of time. There would be many more sacrifices made to preserve the secrecy of Ultra and Magic; they were probably all worth it.

Perhaps the most controversial is the recent claim that the Allies knew of Germans conducting mass executions of Jews as early as 1941. The British government has only recently released documents decrypted at Bletchley Park which may have indicated this. Some contend that something should have been done to stop this, that the Allies should have concentrated all efforts to save the Jews from the holocaust. John Keegan's arguement is that by battling Hitler's armies, they were fighting for the Jews. "It is understandable to deplore anything that was not done to halt or check the Holocaust. But the overriding necessity throughout World War II was to defeat Hitler. Ultra was not the sole cause of Hitler's failure, but it was one of the mightiest weapons on the Allied side. Anything that compromised it would in the long run have served not the cause of freedom but that of tyranny itself." (Keegan, 2nd last paragraph) In essence, it was more important to maintain the secrecy of Ultra and Magic. Had the Allies announced publically what the Nazis were doing to the Jews, it would have comprimised one of their most powerful weapons. Without Ultra and Magic, the Allies knew it may not be long before they too were in concentration camps. By concentrating all efforts on defeating Hitler, they were fighting for the Jews' freedom as well as their own.

While we have so far only examined the role that Allied code-breaking played on the war, it is perhaps worthwhile to mention a few things about the enemy's efforts as well. The Germans had at least as much success reading the Allies' encoded messages as the British and Americans did. Especially during the earlier stages of the war, the German counterpart of Ultra, 'B-Dienst', actually read the allied ciphers quite regularly. Britain and the others did not use machine ciphering until the mid-stages of the war, which made decryption much easier for the Germans. Kahn describes the American encryption techniques as "transparent as a fish tank for any competent cryptanalyst." (Kahn, "Seizing the Enigma," p. 49) In fact, so superior was the Enigma to any other cipher that once the Allies had

re-built it, the British and Americans even used it to encode top-secret intelligence messages to each other!

With the strong effect that cryptography had on the Allied war effort, as has been shown, it seems reasonable to ask the question, why did not the Germans and Japanese simply use new cipher machines? The answer is a combination of two factors. Firstly, they simply did not know the extent that the Allies were reading their transmissions. Secondly, those that did know, or at least had an idea, could not convince higher authorities that it was so. Perhaps the biggest Nazi weakness was their overconfidence; the Enigma was no exception. Hitler simply could not accept the fact that the inferior British or American, let alone the Polish, nations could solve his machine. The extent to which the enemy did know has been debated among authors. Hinsley claims that throughout the war, the enemy simply did not know. (Hinsley, p. 16) Hawker argues that they did know, but were reluctant to change the system they had come to be so dependent on. (Hawker, "Breaking the Code.") Kahn agrees that overconfidence did not allow Hitler and his confidants to accept the fact that the Allies had solved their ciphering machines. (Kahn, "Seizing the Enigma," pp. 200-208) Indeed, Hitler's confidence in the Enigma was not unrealistic; there were 10.5 quadrillion possible keys so it is conceivable that no existing person or machine could ever try all of them. He simply did not have any faith in the Allies' abilities as code-breakers.

Another reason the enemy did not abandon their cipher machines is the extreme secrecy Ultra and Magic insisted upon. "Churchill's anxiety about the secrecy of Ultra was constant; rules in all of the armed forces forbade any action to be taken on the basis of Enigma intercepts unless some cover, such as air reconnaissance, was provided. The security implies Ultra's significance." (Kahn, "Seizing the Enigma," p. 276) Churchill sacrificed lives to keep his secret; it is quite possible that he succeed.

If it were not for mistakes made by enemy cipher clerks, the Allies may never have solved the ciphers. These mistakes were dubbed 'cillies' by the scientists at Bletchley, and included the clerk's early practice of choosing poor keys (such as 'AAA' or a girlfriend's or famous German's name), and failing to follow guidelines strictly. This is not to say that the enemy was ignorant, quite the opposite. Both the German and Japanese cipher machines were works of art, performing encryption that was years ahead of its time. The enemy did actually alter their machines quite often, which kept the Allied cryptanalysts on their toes. Sometimes changes in the enemy's machines would prohibit the Allies from reading transmissions for up to ten months. The cipher machines simply could not compete with the genius characteristic of the likes of Marion Rejewski, Frank B. Rowlett, and Max Newman.

The importance of Allied decryption efforts during World War II has not yet been fully realized. Governments are still withholding information concerning military intelligence during the war. However, what we do know is enough to conclude that the Polish efforts, combined with projects Ultra and Magic, probably shortened the war by at least two years. The men and women who contributed to the war against the enemy's cipher machines, be they from the US Signals Intelligence Service, Bletchley Park, or Biuro Szyfrów (BS-4) in Warsaw, are war heroes. They played a large part in feeding Britain (by protecting merchant ships from U-Boats), returning soldiers to their families, and defeating a deranged madman intent on taking over the world. The cryptanalysts were also successful in attaining victory over an enemy without physical violence. This paper concludes that the solving of enemy cipher machines such as Enigma and Purple was due to astute and resourceful codebreaking by intelligent Allied men and women, whose

genius and ingenuity were underestimated by an enemy that would pay the price.

References

Bennet, Ralph. "Knight's Move at Drvar: Ultra and the Attempt on Tito's Life, 25 May 1944" Journal of Contemporary History, April, 1987.

Coghlan, Andy. "A core of special Allied intelligence" Forum, Mar 6, 1993.

Garli ski, Józef. "The Enigma War" (New York: Charles Scribner's Sons, 1980)

Fox, Barry and Webb, Jeremy. "Colossal Adventures" New Scientist, May 10, 1997.

Hawker, Pat. "Breaking the code" Electronics & Wireless World, January 1988.

Hinsley, F.H. "The Enigma of Ultra" History Today, September, 1993.

Jedd, Joseph. "Poland's Contribution in the Field of Intelligence to the Victory in the Second World War" http://www.dnai.com/~salski/No05-06Folder/Jedd'sPoland'sContribution.htm" (The Summit Times, 1994)

Kahn, David. "Hitler's Spies" (Toronto: Hodder and Stoughton, 1978)

Kahn, David. "Seizing the Enigma" (Boston: Houghton Mifflin Company, 1991)

Kahn, David. "The Intelligence Failure of Pearl Harbour" Foreign Affairs, Winter 91/92.

Keegan, John. "What the Allies Knew" New York Times, November 25, 1996. http://www.mtholyoke.edu/acad/intrel/allied.htm

Kozaczuk, Wladyslaw. "Enigma" (USA: University Publications of America, 1984)

Momsen, Bill. "Codebreaking and Secret Weapons in WWII" http://members.aol.com/nbrass/enigma.htm (Nautical Brass Online, February 1997)

Payne, Michael J. "Cryptography Timeline" http://www.ns.net/users/payne-o/timeline.html (NSNet, June 1996)

Pinkney, David. "World War II: The Development and Impact of Cryptology" http://glug.cs.uml.edu/~dpinkney/suff/suff.shtml (University Of Massachusetts Lowell, 1992)

Prados, John. "Combined Fleet Decoded" (Toronto: Random House, 1995)

Rusbridger, James. "Winds of Warning: Mythology & Fact about Enigma and Pearl Harbour" Encounter, January, 1986.

Rusbridger, James. "The Sinking of the Automedon, the Capture of the Nankin" Encounter, May, 1985.

Sale, Tony. "Bletchley Park Home Page" http://www.cranfield.ac.uk/ccc/bpark/ (Cranfield University, 1997)

Stevenson, William. "A Man Called Intrepid" (New York: Harcourt Brace Jovanovich, 1976)

Wark, Wesley K. "Cryptographic Innocence: The Origins of Signals Intelligence in Canada in the Second World War" Journal of Contemporary History, October, 1987.

Zorpette, Glenn. "Breaking the enemy's code" IEEE Spectrum, September, 1987.

"The Enigma Machine" http://www.msichicago.org/exhibit/U505/ENIGMA.html (Museum of Science and Industry, Chicago, 1996)

"Secrets of War" http://www.secretsofwar.com/ (Documedia Group, California, 1997)

"WWII Timeline" http://www.historyplace.com/worldwar2/timeline/ww2time.htm (The History Place, 1998)