ENIGMA and PURPLE: How the Allies Broke German and Japanese Codes During the War

David A. Hatch

Director of the Center for Cryptologic History, National Security Agency, Fort George Meade, MD

1 Introduction

Cryptology consists of two aspects: Signals Intelligence (SIGINT), which seeks to exploit the encrypted communications of enemies or potential enemies, and Information Systems Security, which seeks to protect American communications from those who might wish to exploit them. Americans utilized cryptology even before the foundation of the United States, particularly in the American Revolution and the Civil War. However, it was not until the Twentieth Century that the United States began sustained Communications Intelligence (COMINT) activities.

One probable reason for this was the feeling of security two oceans gave Americans; without a sense of immediate external menace, there was no stimulus for an American government to obtain regular and timely information about potential overseas enemies. The United States was late in forming organizations for military and naval intelligence, and even once in existence, these organizations remained rudimentary until two world wars brought American leaders to the realization that American territory was now vulnerable.

The "golden age" for American cryptology was the Second World War. Both the U.S. Navy and Army solved and exploited a wide variety of enemy codes and ciphers at all levels. These achievements in reading enemy systems enabled U.S. commanders to make wiser decisions that saved thousands of American lives and shortened the war. Out of the many achievements of wartime cryptanalysis, this article will discuss PURPLE, the high-level Japanese diplomatic system, and ENIGMA, the high-level German military cryptographic machine.

2 Origins of radio intelligence

The invention and widespread use of wireless radio made collection of foreign communications less of a technical challenge. With this Twentieth Century invention, it became possible to acquire a potential enemy's messages without knocking over couriers or tampering with telegraph wires. Elementary efforts at radio intercept began in the first decade of the Twentieth Century, and most industrialized countries engaged in Signals Intelligence to some extent in the years immediately prior to World War I. However, few countries created organizations to manage the activity until war made it necessary for them to do so.

The War to Make the World Safe for Democracy found American radiomen intercepting German communications for both strategic and tactical purposes. The revitalization of Military Intelligence on the eve of the war provided a suitable organizational structure for the exploitation and dissemination of Communications Intelligence. After the war, however, the radio intelligence organization was eliminated in the general demobilization.

With a nascent sense of international menace and perhaps based on the favorable wartime experience, at the conclusion of the Great War, the United States for the first time created a national-level intelligence organization, a cryptologic organization. This was MI-8, jointly funded by the U.S. Army and the State Department, with some Navy participation, and headed by Herbert O. Yardley. The story of MI-8, usually known by its colorful nickname, the "Black Chamber," is well-known, so it is not necessary to recount its exploits here; suffice it to say that this organization was successful against a number of foreign diplomatic cryptosystems during the 1920s.

Equally well-known is the demise of the Black Chamber, marked by the mythical moral utterances of Secretary of State Henry Stimson, who is alleged to have said "Gentlemen don't read other gentlemen's mail!" Stimson withdrew the State Department's funding from MI-8 largely for budgetary reasons in the Great Depression, effectively closing it down. Subsequent to the closure of MI-8 in 1931, Yardley published his expose of American codebreaking, The American Black Chamber. This book caused Japan, among other countries, to change its communications security practices, with increasing dependence on machine systems in the 1930s.

Whatever the truth of Stimson's statement, the U.S. Army and Navy, for their part, wanted to go on reading other gentlemen's mail. The Navy from the 1920s began building an organization for cryptologic activities, and expanded this service in the 1930s; it was primarily concerned with training intercept operators and cryptanalysts who would be ready for operations in case of war. The Army, for its part, in 1929 hired one of its consultants, William F. Friedman, to form a modern Signal Intelligence Service (SIS).

3 PURPLE

On April Fool's Day in 1930, William Friedman welcomed the first of three cryptologists he had hired for the SIS. His first employee was Frank B. Rowlett, a young mathematician who was brought to Washington as a junior cryptanalyst at $ 2,000 per year. Shortly after, Friedman brought in Abraham Sinkov and Solomon Kullback – two graduates of the City College of New York – into the service. John Hurt, a talented Japanese linguist, who had the added advantage of a Congressman for an uncle, was hired later. For much of the decade they served as the nucleus of the Army's cryptologic service.

The organizational placement of SIS, it should be noted, was not in Military Intelligence, but the Army Signal Corps. Its primary mission was devising cryptosystems for U.S. use, with the solution of foreign systems as a secondary activity. The Army at this time evinced minimal interest in peacetime SIGINT, except to keep skills current in case of war.

William Friedman proved to be a genius at training and put his staff through rigorous exercises, including codes used in the Great War, files of the Black Chamber, and rudimentary machine systems. This regimen was validated by the eventual achievements of this group: in the period from 1933 to 1941, SIS cryptologists studied eleven Japanese diplomatic and military attache systems – and solved them.

The Navy's cryptologic organization developed considerable skill in exploiting Japanese communications during fleet maneuvers. Their discoveries of Japanese naval preparedness and likely Japanese strategies in case of war between the two countries helped the U.S. naval senior commanders to reevaluate their own policies and practices.

Initial progress was made against some Japanese diplomatic messages done in traditional systems, when, in 1935, working as a team, Frank Rowlett and Solomon Kullback detected exploitable weaknesses in a Japanese machine cipher "Angooki Type A" used by the Foreign Ministry. As they began to read messages enciphered in this system, the Americans gave it the codename RED – the first color of the spectrum for the first cipher machine actually solved.

Both Army and Navy cryptanalysts solved the Japanese RED system, independently of each other and in the same general time frame. The production of real intelligence from the cipher machines of a potential foreign enemy quickly came to the attention of the Army authorities. Rowlett recalled that for the first time their military superiors began according SIS personnel real respect. More importantly, the Army increased SIS resources, and had Friedman draw up regulations on distribution of the decrypted material, closely restricting those who would be given access to it. This may have been the first instance of a compartmentation program in modern American intelligence activities.

Cryptologic operations never remain static, however, and the Americans all too soon lost their access to this inside information. In February 1939, Japan's Foreign Ministry introduced the TYPE-B Cipher Machine, nicknamed PURPLE by American cryptanalyts. The Japanese distributed this machine to their most important embassies – Washington, Berlin, Rome, and London – precisely those locations from which U.S. policymakers most wanted information. The Americans were able to exploit PURPLE partially until May 1939, when the Japanese introduced significant security improvements to the system.

It took U.S. Army cryptanalysts until late November 1940 to recover and produce usable decrypts from this improved PURPLE system. (If this seem excessive, it should be noted that after the war, American cryptologists discovered that their German counterparts had also attempted the PURPLE system – and failed!) While the cryptosystem itself was named PURPLE, the product of SIS efforts, that is, decrypts prepared for circulation, were stamped with the restrictive codeword MAGIC – a possible reference to William Friedman's fond joke that his cryptanalysts were "magicians."

In addition to solving the system, SIS personnel designed items of equipment to speed the processing of PURPLE. Drawing on the talents of Leo Rosen, a reserve officer with a background in electrical engineering, SIS created a range of equipment, including an "analog" which would enable automatic decryption of PURPLE-based messages.

The ability to read RED and PURPLE led SIS into cooperation with the U.S. Navy. The amount of material involved, compounded by lengthy processing time, had brought the Army to share the secret of RED with its sister service. The ability to exploit PURPLE greatly increased the need for inter-service cooperation. The Navy's organization, OP-20-G, had assets the Army did not: a better position to collect Japanese communications and a larger pool of Japanese-trained language officers, to begin with.

The already-complicated relationship between the Army and Navy became considerably more complex in the struggle to exploit PURPLE. When Army analysts designed an analog machine to speed PURPLE recoveries, it was constructed by the Navy at the Washington Navy Yard, which had more experience in making cryptographic devices. Subsequently, the Navy cooperated with the Army in collecting message traffic, and making code recoveries. However, the two services found themselves competing in exploiting and distributing the product, particularly vying for the privilege of disseminating decrypts to senior civilian officials.

The two services tried various schemes to avoid duplication of effort in processing PURPLE until finally they agreed that the Navy would process PURPLE messages on odd-numbered days, the Army on even-numbered ones. This was a cumbersome system with frequent points of conflict but it was an important step toward interservice cooperation in the whole process of cryptology. During the war, another step was taken as the two services exchanged liaison officers to each others' cryptologic organization.

As the military itself expanded in the late 1930s, SIS and OP-20-G also expanded, and when war came, the expansion became more rapid. With the advent of war, SIS moved from its tiny quarters in a vaulted area in the Munitions Building in downtown Washington, D.C., to Arlington Hall Station, a former girls' school across the Potomac in Virginia. The Navy also moved its cryptologic headquarters to Mt. Vernon Academy, a former girls' school in northwest Washington.

Just prior to the U.S. entry into the Second World War, the United States and Great Britain began cautious exchanges of technical information, including some sharing of data on cryptanalysis. Each was delighted to learn that the other had made major solutions to the cryptosystems used by their common enemies, Germany and Japan – the U.S. against PURPLE, Great Britain against ENIGMA, the German high-level system. (Both the U.S. Army and Navy had separate agreements with the British organization). This sharing was just one factor among many aspects of wartime cooperation between the two countries, but it certainly helped build a solid bilateral working relationship.

4 ENIGMA

The ENIGMA began as a commercial machine, around the time of World War I, but was not an initial success – it was too far ahead of its time and too expensive for businesses. However, in the 1920s, the German Navy learned that the British Navy had broken traditional German codes during World War I, and sought a new method of keeping its communications secure. The Navy adopted a modified version of the commercial ENIGMA, and, eventually, the German Army and Air Force also adopted it, making it the workhorse of German military communications security prior to and during World War II. (Note that ENIGMA – a Greek word meaning a puzzle or mystery – was the actual trademark name for the German machine, not a codename bestowed on it by the Allies).

Each German service used ENIGMA machines with slight variants from the others to suit its own special military needs. For example, the German Navy, most security conscious of the services, added mechanical features and changed procedures from time to time. In general, however, the ENIGMA appears to be a simple device: it is an electromechanical device which uses a combination of rotors (rotating disks) and plugs to encipher messages letter by letter. Its mechanical and electrical operations were state-of-the-art in the 1930s, and the Germans had good reason to believe that the ENIGMA would keep their communications absolutely secure.

Despite its obvious strengths, the ENIGMA device was solved by mathematical analysis in the 1930s. The Polish Cipher Bureau, assisted by a little inside information about the machine, came to an understanding of its operational methods and devised methods of solving ENIGMA-based messages. Most of the Polish methods were too slow to be used in combat situations, but the Cipher Bureau's mathematicians invented a machine they called a bombe, which would apply their decryption principles faster than the human hand could work.

Despite good intelligence on the German military, Poland fell when the Nazis attacked – the German military was the best in the world. However, before this happened, the Polish Cipher Bureau shared the secret of the ENIGMA machine, including how to construct bombes with the French and the British.

Great Britain's Government Code and Cipher School (GC&CS), its cryptologic organization, put great efforts into improving the speed and efficiency of the bombe. Among those who worked on it were Alan Turing and Gordon

Welchman. GC& CS also created an efficient organization for intercepting German military communications, processing them and passing the resultant intelligence to commanders quickly. The secret intelligence derived from ENIGMA decrypts was marked with the codeword ULTRA.

When the United States and Great Britain began cooperating in Signals Intelligence during the War, U.S. cryptologic organizations learned much from the British, and, in fact, SIS and OP-20-G modeled their distribution systems on that of their ally. Eventually, to avoid confusion, all high-level decrypts, whether from German or Japanese communications, were labeled "ULTRA."

Signals Intelligence proved a labor-intensive business, even with advanced machines such as the bombe, but, together, the U.S. and British organizations developed a working system that gave their senior leaders and commanders unprecedented types and amounts of secret information.

5 Cryptology during the war

It might be argued that World War II was the first true "information war." It is also true that the United States in many ways found itself ill-prepared for global war at the beginning, intelligence information being one important instance: America's military was forced to fight on unfamiliar fronts where the state of intelligence ranged from barely adequate to non-existent. It should not be surprising then that all PURPLE/MAGIC and ENIGMA/ULTRA material was eagerly ingested by consumers anxious for reliable information. PURPLE, though used by the Japanese for diplomatic communications, became a major ingredient in Allied military decision-making.

The German and Japanese military used a variety of cryptographic systems to protect their communications prior to and during the war. Allied cryptanalysts solved many of these systems over this period, but for the purposes of this article, we will discuss PURPLE and ENIGMA only.

Prior to December 1941, exploitation of PURPLE gave American policymakers access to the instructions sent by Tokyo to their negotiators in Washington and the negotiators' reports of the meetings with State Department officials. This was very useful for U.S. diplomats in day-to-day interaction with the Japanese, and somewhat helpful to the U.S. military, but did not reveal to the American eavesdroppers the most valuable secret of all – the question of war and peace.

The Japanese military did not trust the Japanese Foreign Ministry with details of its operational planning, least of all that a large strike force was moving through the north Pacific toward Hawaii. Thus, although Japanese diplomatic messages in early December 1941 implied that war was a matter of days, perhaps hours, away, the MAGIC material contained no specific clues about the impending attack at Pearl Harbor.

American Army and Naval cryptanalysts exploited several Japanese military systems after Pearl Harbor, enabling U.S. commanders to get an unprecedented window on enemy military operations in the Pacific and South Asian theaters. With the coming of war, the Navy discontinued its work against non-Naval system, thus the continued exploitation of the PURPLE diplomatic system became strictly an Army effort, although, of course, Navy consumers still received distribution of the decrypt intelligence.

By an interesting turn of fate, PURPLE, even though a Japanese system and intended for diplomatic communications, became an essential ingredient in Allied military operations in Europe.

With their fate linked inextricably to Germany's, Japanese leaders demanded accurate and detailed data about all aspects of the war in Europe, and this was forthcoming from their diplomatic stations there – much of it transmitted to Tokyo in the PURPLE system. Thus, the source known as MAGIC provided detailed insight into the thinking and activities of Nazi leaders, Mussolini, and the leaders of Vichy France, among others. MAGIC provided anecdotal evidence of the coordination – or lack of it – among the Axis nations. MAGIC also provided the most reliable source of hard data on the Russo-German front.

The Japanese Ambassador to Germany was Baron Oshima, concurrently a lieutenant general on the active list, who was well-treated by his hosts. His tours sponsored by Albert Speer, for example, led him to write several detailed reports about Germany's new weapons and weapons production.

In late 1943, Ambassador Oshima and some of his subordinates were given an inspection tour of German defenses erected along the coast of France. Their detailed reports not only listed fortifications and shore emplacements, but unit identities, locations and areas of responsibility, training, and locations of reserves. This proved rather useful when Eisenhower was planning Operation OVERLORD.

As the war turned against Germany, U.S. policymakers read in MAGIC the scary prospect of a Russo-German peace settlement, which the Japanese were promoting. MAGIC reports from Japanese diplomats in Berlin and Moscow, however, reassured American readers that Germany declined to pursue this settlement, and that the Soviet Union in any case was standing firm against it.

MAGIC enabled American policymakers to follow both the beginning and the end of the Russo-Japanese Neutrality Pact. MAGIC reports showed the progress of its negotiation and signing in 1941, the vain attempts of Japan to find out whether the Soviets would extend it in 1946, and, finally, the shock to Japan when the USSR announced its intention to abrogate the pact in 1945.

With the defeat of Germany, Japanese diplomats in neutral nations, such as Sweden and Switzerland, began proposing feeble schemes by which Japan could seek a brokered end to the war without unconditional surrender. MAGIC reported these, and also showed that the idea of unconditional surrender was anathema to leaders in Tokyo.

In the European Theater, the ability to decrypt ENIGMA-based military messages quickly became an essential ingredient in combat planning for the British, and the Americans, after their entry into the war, also learned to use its essential insights.

Early in the war, ULTRA enabled the outnumbered Royal Air Force to outfox the German Air Force in its bombing campaigns against Britain. ULTRA intelligence was important to General Montgomery, and later to General Eisenhower, in fighting Rommel's Afrika Corps.

ULTRA was an essential ingredient in winning the Battle of the Atlantic. German U-Boats were a serious threat to Allied shipping, and could possibly have prevented American intervention in Europe. However, decryption of submarine messages enabled the Allied navies to hunt and destroy a large number of subs as well as their replenishment ships. Here, ULTRA had to be augmented carefully with other sources of data, including sightings and direction finding, but was the sine qua non of the U-Boat battles.

Decrypts from ENIGMA-based messages became the staple of Allied secret intelligence in the Italian campaigns and in the drive across France after D-Day. Messages provided copious amounts of data on enemy order of battle and often gave Allied commanders advance warning of impending German attacks.

6 Conclusions

I would offer the following conclusions about the American and Allied experience with PURPLE/MAGIC and ENIGMA/ULTRA:

The U.S. solution of the PURPLE system and British exploitation of ENIGMA gave Allied decision makers continuous insight into what the enemy was saying to itself. This unprecedented – and sustained – insight into the activities, thinking, and intentions of our enemies worldwide and at the highest levels gave the Allies an incalculable advantage.

The ability to read the PURPLE system provided much wider access than might have been expected. It not only produced information on the immediate users, that is, the Japanese diplomatic service, it gave the Allies a superior source of information useful in both theaters of war and for military purposes as well. It might be argued that PURPLE at some stages was more important in the struggle against Germany than it was in the fight against Japan itself.

The ability to exploit the RED system was the catalyst which spurred the growth of SIS from a tiny cadre into a large and active organization and prepared the organization to take advantage of the later solution of PURPLE. It also necessitated the development of mechanisms for widespread collection and dissemination of SIGINT materials and the doctrine under which these activities would be conducted.

The facts that exploitation of the PURPLE system was manpower-intensive and speed of processing was imperative, forced the two branches of the military services, even while they were domestic rivals for resources, to cooperate to produce this source in a timely way. This helped prepare the ground for increased interservice cooperation in the post-war era.

Most senior and many mid-level military and civilian leaders in the war had some level of access to MAGIC reports. They retained their memories of World War cryptologic successes, and supported the continuation of cryptologic capabilities in the brave new post-war world.

The solutions of PURPLE and ENIGMA were intellectual accomplishments of the first brilliance. Both were team efforts and the members of these teams ought to be listed among the important contributors to victory in World War II. Unfortunately, however, for most of the contributors, their names and deeds are generally known only to the few who are interested in intelligence activities.

Finally, SIGINT did not win World War II. The war was won by those sailors, soldiers, airmen, and marines who took the fight to the enemy at the risk and, sometimes, cost of their own lives. However, Signals Intelligence gave commanders inside information about the enemy in such detail that it allowed them to make wise decisions that saved uncounted thousands of American and British lives and shortened the war by many months.

That is what is expected of an intelligence organization in wartime, and, in World War II, the American and British SIGINT personnel delivered their product with war-changing and lifesaving effects.