NATIONAL CRYPTOLOGIC MUSEUM

Docent Book

January 1996

National Cryptologic Museum
Docent Book

January 1996

The material in this briefing book was prepared with contributions from the following individuals (listed in alphabetical order):

Charles Baker
Earl J. Coates
David W. Gaddy
David A. Hatch
John K. Hultstrand
Jack E. Ingram
Thomas R. Johnson
Jeanne-Rene Jones
Lawrence R. Sharp

1. This book should be studied by all who wish to serve as docents at the National Cryptologic Museum. Tour presentations should be based on this material, although it may (and should) be supplemented by individual research. This booklet is for background reading by docents and prospective docents and should not be disseminated to the general public.

2. This material should not be repeated in a rote manner, but presented naturally, adapted to the audience. While it is obvious there will be a great difference in the way material is presented to individuals and groups, cryptologic professionals vice the laity, or adults vice children, there will even be a good deal of variance between adult groups, depending on interest and focus of the group.

3. This briefing book should be considered a draft – it may be added to, supplemented, or revised at any time. Docents are encouraged to suggest changes based on their research and on responses from the public to tours. The museum office will furnish copies of any changes ore replacements.

* A cyber-tour of the museum is now available on the WorldWideWeb. The address is:

HTTP://WWW.NSA.GOV:8080/

Table of Contents

SUGGESTED READING FOR DOCENTS

* All unclassified publications from the Center for Cryptologic History

* Selected Special Research Histories, including:

SRH-003 *"The Influence of US Cryptologic Organizations on the Digital Computer Industry"*

SRH-256 *"The Attack on the USS Liberty"*

I. The following are generally reliable and will be of assistance in conducting museum tours:

Carl Boyd: Hitler's Japanese Confidant

Edward Drea: MacArthur's ULTRA

David Kahn: The Codebreakers; Seizing the ENIGMA

Ronald Lewin: The American MAGIC

Jurgen Rohwer: The Critical Convoy Battles of March 1943

Gordon Welchman: The Hut Six Story

II. The following should be used with special care, but have value for background reading. Many museum visitors will already be familiar with these works.

Ladislaw Farago, The Broken Seal

Robert Lamphere, The FBI-KGB War

Frederick Winterbotham, The ULTRA Secret

Herbert O. Yardley, The American Black Chamber

ENTRANCE CORRIDOR

The text and pictures in the entrance corridor contain basic definitions of cryptology, including both Signals Intelligence (SIGINT) and Information Systems Security (INFOSEC). Many museum visitors will know these by their former designations, "Communications Intelligence" (COMINT) and "Communications Security" (COMSEC).

NSA was formed in November 1952 by President Harry S Truman as a separately organized agency within the Department of Defense. The Agency drew on the experience and expertise of the service cryptologic units from World War II. Several methods for centralizing cryptologic work were tried in the period after the war, but none of them proved effective; Truman authorized a high-level committee, headed by New York lawyer George Brownell, which termed cryptology a "national asset" and recommended that it be centralized under a stronger organization. The first director of NSA (DIRNSA) was Lieutenant General Ralph Canine.

In addition to its original missions of Signals Intelligence and Information Systems Security, NSA in 1984 was charged with Operations Security training, again by presidential directive. Under a 1986 law, NSA became a combat support agency of the Department of Defense.

Initially, NSA was split between the campuses of the Army and Navy cryptologic organizations, at Arlington Hall Station and Nebraska Avenue. The Agency moved to Ft. Meade in the mid-1950s.

The original NSA seal has been in the museum collection for years. The large seal for the Electronic Security Command, along with the ESC flag, was presented to NSA by General O'Shaugnessy, commander of the ESC in 1992, when the command was reorganized.

The Director of NSA is always a three-star military officer, either a Navy admiral or an Army or Air Force general. This position rotates among the services in approximately three-year cycles. NSA's Deputy Director is a senior civilian, who provides continuity of management.

While the exact number of NSA employees remains classified, NSA is the largest single employer in Anne Arundel County and one of the largest employers in Maryland.

HALL NUMBER 1

RARE BOOKS

The central case contains a number of rare books, including the first book published in the western world on cryptology, the *Poligraphique* of Johannes Trithemius, published in 1518. This year the museum can display a first edition, thanks to a loan by Dr. David Kahn. (The museum owns a later edition of this rare book). Also on display is the second book on cryptology in the western world, the *Opus Novum* of Jacopo Silvestri, published in 1526.

It is necessary to qualify our statements about these books and note that they are the oldest -- and rarest -- books on cryptology "in the western world." Certain Arab scholars were writing about cryptology by about 1000 A.D.

Egyptian hieroglyphics puzzled and enthralled scholars for centuries; their use had been discontinued after the time of the Pharaohs. leaving inscriptions unreadable and keeping ancient Egypt a civilization only partially known. In 1799, Napoleon's troops in the city of Rosette uncovered a slab of basalt with three parallel inscriptions carved on it: hieroglyphics. an Egyptian "shorthand," and Greek -- which modern scholars could read. Even with this "crib," the secret of the ancient hieroglyphs was not solved until 1821. French scholar Jean-Francois Champollion made a number of important deductions about the texts on the Rosetta Stone, and began translating the Egyptian.

The vases are merely for decoration and have no special significance.

CYLINDER CIPHER

After the rare books, the oldest item in the collection is the cylinder cipher, which the museum has dated from the second decade of the nineteenth century, but which may possibly date from the time of the American Revolution.

The provenance of the cylinder is unknown; it was discovered in the Charlestown, W.Va. area. The cylinder's design is strikingly similar to a drawing of such a device found in the papers of Thomas Jefferson; but we cannot prove he built a working model. Our third president was an avid amateur cryptologist, but the only ciphers directly traced to him were strictly paper-and-pen systems. It is interesting to note that the cylinder is set up to encipher letters in French -- French was the diplomatic language of the 18th and 19th centuries -- and Jefferson was for some years American minister to France.

This pre-Civil War device has 35 of a possible 40 disks. Each disk has 42 mixed letters, digits, and punctuation. The method of encryption is fairly secure for the pre-electro-mechanical era -- the disks may be rearranged on the spindle in any order, as long as both sender and receiver know what that order is to be. A metal bar is laid across the top; the disks are turned until the desired plaintext message appears on the near side of the bar. The line on the far side of the bar is gobbledegook: this constitutes the encrypted text, which is sent to the other communicator. The recipient of the message reverses this process.

Interestingly, although the concept for this device was lost, the U.S. Army independently came up with an almost identical design in the early 20th century, a metallic version of this device -- given the nomenclature M94 -- for low-level tactical encryption through World War II.

AMERICAN CIVIL WAR

During America's first century, secret writing -- cryptography -- figured in many instances in which lives and fortunes were at stake and confidentiality was desired. In some instances the codes and ciphers of America's enemies were successfully broken. We can say that codemaking and codebreaking not only predated the establishment of the United States, but figured in gaining and keeping American independence.

Until nearly mid-century, large armies moved unassisted by any special technology to aid long-distance communications or even tactical communications over an extensive battlefield. By the same token, there was no reliable way for one side to obtain a steady source of enemy message traffic for intelligence purposes; collection was somewhat happenstance with the capture of enemy transports or the deliberate knock-over of an enemy courier.

A partial answer came in 1844, when Samuel F. B. Morse successfully tested his improved electromagnetic telegraph not far from here, along what is now Route One between Washington and Baltimore. With this practical demonstration came a dramatic communications revolution which made the United States a continental power but also made war possible on a continental scale. Telegraph tapping was one civilian method used to check communications lines, but quickly became a military source of secret information on enemy activities.

At the time of the American Civil War, both sides began encrypting high-level messages to be transmitted on the telegraph. More importantly, for the first time, it became possible to collect such messages from the enemy in volume and in near-real-time. Further, both sides established cipher bureaus in their respective capitals to work on enemy encrypted messages, one of the early examples of a centralized intelligence activity in the United States.

A real answer to the problem of battlefield communications came from a visual, line-of-sight system developed in the 1850s by an Army doctor from New York, Albert J. Myer. He used a single flag, waved left or right like the dot and dash of Morse code, to transmit messages at a distance. At night, two torches substituted for the flag, with one placed at the operator's foot as a reference point, the other swung left or right like the flag. Although the system was point-to-point, its range could be extended by the use of telescope or field glasses, and networks of signal towers were built where the telegraph did not go. The system proved itself at the Battle of Manassas, the first great clash of the war.

The Myer flag system was adopted in 1864 as our first joint Army-Navy communication system in the form of a "General Service Code." Adapted by the end of the century to the International Morse Code, it continued to be used as a supplementary or emergency means of sending Morse even in the present day. Myer's flag came in different sizes, and he devised three alternate designs to contrast with the operator's backdrop -- red square on a white flag, white square on a red flag, and white square on a black flag. The two most common ones, with a stylized torch, today form the insignia of the U.S. Army Signal Corps, Myer's legacy.

Since both sides used the same basic system, each learned to intercept the other's signals and to break into encrypted messages. Each tried to obtain the advantage of "signals intelligence," while thwarting the enemy's efforts. Before being allowed to engage in signalling or "SIGINT," a candidate had to subscribe to an oath, what today would be called a "nondisclosure" agreeement.

One of Myer's innovations for morale purposes is illustrated by the extremely rare "star flag." In 1862, near the beginning of the war, the Army did not award medals to its soldiers for bravery. Myer saw the need for awards for signal officers, and introduced what he called the "honor flag," with a star in the center instead of a square. Every Signal Corps officer had a flag with a square in the center to identify his battlefield location or to carry on parade, but a star flag was given to those officers who distinguished themselves under fire. Early in the war, the officer would inscribe on the star point the name of the battle for which he was decorated. This system was abandoned later in the war, and only twenty-odd flags are known today; the flag in the museum's possession is one of only two known to exist today with all five star points filled.

This honor flag belonged to Second Lieutenant Frederick Wooster Owen of Brooklyn, N.Y., who served with the 38th New York Infantry Regiment. After the war, Owen became a medical doctor and was very active in YMCA work in New Jersey.

BATTLES ON SIGNAL CORPS FLAG

Yorktown -- 31 May 1861 during the Peninsular Campaign

West Point -- during the Peninsula Campaign

Fredericksburg -- 13 December 1862

Antietam -- 17 September 1862

Po River -- 11 May 1864 during the Spotsylvania Campaign

CONFEDERATE CIPHER CYLINDER

The Confederate Cipher Reel evidently could be used several ways: the simplest method was to set one stylus to point at a plaintext letter and the other to the cipher substitution letter. The reel or drum has a piece of paper wrapped around it with 26 mixed-alphabet lines drawn on it in pencil. It was a rather simple matter to turn the drum and copy the cipher letter from a pre-selected line and then reverse the process on the receiving end.

One of only two known to exist, our Confederate Cipher Reel was captured by Union forces at Mobile, Alabama, in 1865. It went first to the Signal Corps archives, then to the Army Research and Development Museum collection of captured cipher equipment. This collection was passed on to NSA in the early 1950s.

GENERAL HOOKER'S CODEBOOK

The telegraph came of age as an instrument of war during the American Civil War. Telegraphic communications were sent from various Army headquarters (or even the battle areas) directly to Washington, D.C., where President Lincoln read it -- the first national leader in the world to have the ability to "run the war" electrically from his capital.

This Union Army cipher book is dated 1861 and 1862, and was used primarily for messages sent by telegraph. It contains "Cipher no. 9," one of the official War Department cryptosystems used during the war. It contains codenames to be used for senior leaders, including the president and his cabinet, generals, governors, states, and other important geographic locations, as well as a "route" or column code. Each individual or location had two different code words to be used at he sender's discretion.

The "route" cipher was a formula for scrambling the order of words in a message by column and row. When the important words and names in a message had been rendered innocuous by substitution of terms from the codebook, this scrambling process then produced a thoroughly meaningless text. It did, however, consist of real words in English, which helped reduce garbles in telegraphic transmission.

This codebook is one of only five known still to exist and the only one attributed to a particular person. General Joseph Hooker was prominent during most of the war; he commanded the Army of the Potomac at the Battle of Chancellorsville in May 1863, where he was decisively beaten by the Confederates under Robert E. Lee. Hooker resigned his command just a few days before the battle of Gettysburg. This codebook was purchased from a private collector in 1995.

WORLD WAR I

Just as the telegraph revolutionized communications and American life in the nineteenth century, the twentieth century saw an even greater communications revolution. The invention of wireless radio made possible long-distance communications without regard to national or physical barriers; it also made possible the intercept of these communications without regard to proximity to transmission lines. The United States Army and Navy by no means were the last to undertake this.

The U.S. Army "direction finding tractor" -- "tractor" was army terminology of the time for "truck" -- was rather advanced for the time. Also known as a "goniometric tractor," this truck had a DF antenna, turned by hand from the inside: these would measure the angle of entry and skip of a signal coming in and bouncing off the ionosphere. By measuring the angle, they could pinpoint the distance the radio wave had travelled. With three intercept stations on the same signal, it was possible to triangulate it, that is, use a simple mathematical formula to "find the direction" from whence the signal came and locate the enemy transmitter. These devices were used along the Mexican border during the period of tension in the early 'teens, and were deployed with the American Expeditionary Forces in France.

The large case is a reproduction of the Verdun intercept site, established to support a major headquarters unit. Although Signals Intelligence was in its infancy, information from direction finding, radio intercept, traffic analysis, and decryption was used for both tactical and strategic advantage by the American Expeditionary Forces (AEF).

(This display was built by NSA craftsmen, based on the two extant photographs of the Verdun site; the photographs had been found in the National Archives. The alarm clock, the same model as the one in the photo and even has the corresponding time set, was discovered in a flea market by our former curator.)

Behind the case is a World War I-era uniform coat of a Master Signal Electrician, a technical rank equal in pay grade to a Master Sergeant. Although today we associate the single stripe on the sleeve with the rank of PFC, in this era it denoted overseas and/or wartime service. The actual rank is on the right sleeve: the patch with leaves and electronic flashes.

THE AMERCIAN BLACK CHAMBER

The horizontal exhibit case highlights the checkered career of Herbert O. Yardley (1889-1958), easily the most controversial figure in American cryptology.

Yardley began his career as a code clerk with the U.S. State Department, and during that service discovered his natural talent as a cryptanalyst. Upon U.S. entry into World War I, Yardley was commissioned an officer and served in the cryptologic section of Military Intelligence, overseas with the AEF.

Following the World War, the United States established its first permanent, centralized, peacetime cryptanalytic organization, sponsored jointly by the Army and the Department of State. It was officially known as MI-8, and placed under the direction of this raffish gentleman, Herbert Yardley. The organization located itself in New York City, where it was disguised as a company which made commercial codes for businesses. In New York, Yardley and his staff worked to solve the diplomatic cipher systems used by some two dozen countries.

MI-8 had an early success: in 1921-22, Yardley and his staff solved the cipher system used by Japanese negotiators at the Washington Naval Conference. They fed the decrypts to the U.S. chief negotiator, Charles Evans Hughes; these messages contained the Japanese minimum demands at the conference. When the final treaty was agreed upon, the Japanese had been finessed to their bottom line.

In 1929, with the change of administration and the worldwide depression, the State Department withdrew its share of MI-8's funding. According to legend, Secretary of State Henry Stimson at that time spoke the single most famous sentence in history about cryptology: "Gentlemen don't read each other's mail." Historians are still debating the validity of this story.

Yardley had expensive tastes and was always in need of money, so that finding himself out of work and in possession of his country's secrets, he could not resist writing a book. *The American Black Chamber* became a huge bestseller in 1931. His rationale for writing was the necessity, as he saw it, of awakening the public to the need for better communications security. Surprisingly, at the time, the wording of the espionage laws contained a loophole which prevented the government from prosecuting Yardley. (This gap was filled in 1933 when Franklin Roosevelt signed into effect the so-called "Yardley Law," imposing penalties for revealing cryptologic secrets.) Yardley, of course, was never again employable in the intelligence profession.

NAVY CIPHER

In the Navy cipher system -- hanging in the corner by the World War I uniform -- the little card with the punched holes would be placed over a written text, and the letters would be scrambled according to the numbers written atop the holes. A reverse process would decrypt the message. This system merely scrambled the plain text, rather than transposing it into other letters or numbers.

THE FRIEDMANs

William F. Friedman (1891-1969), considered the dean of American cryptologists, was born in Kishinev, Russia, and brought to the United States in 1892. He received his BS in genetics from Cornell University. He served as a first lieutenant with the Code and Cipher Solving Section, G-2, AEF, and became a consultant cryptographer in the Office of the Chief Signal Officer in 1921. (He retired from NSA in 1955 after 35 years of government cryptologic service.)

Friedman's interest in codes and ciphers was first stimulated during his pre-World War I employment at Riverbank Laboratory, a "think tank" near Chicago. Riverbank's eccentric owner, "Colonel" George Fabyan, established a section at the Laboratory to research cryptologic problems. One of those hired to do this research was Elizebeth Smith, an English teacher from Indiana. Although originally hired to do genetic research, William Friedman became interested first in Ms. Smith, then in cryptology. William and Elizebeth were married just prior to World War I -- William saw service overseas as a cryptologic officer in Military Intelligence.

William Friedman's accomplishments are justly heralded: he put American cryptologic efforts on a scientific basis, coined cryptologic terminology, wrote textbooks which were used to train generations of American cryptologists, hired and trained the civilian nucleus of the Army's Signal Intelligence Service, supervised the team that solved the Japanese diplomatic ciphers prior to World War II, and supervised the prewar development of the SIGABA, which kept high-level U.S. communications inviolable during the war.

It is less often appreciated that Elizebeth S. Friedman (1892-1980) was an equally skilled cryptologist, who made important contributions to the development of the science and also had a very distinguished career in government service. In particular, she worked for the Treasury Department in the 1920s, breaking cipher or code systems used by "rum runners" who were violating Prohibition. She helped in the apprehension and prosecution of numerous criminals by decrypting their communications and serving as an expert witness in court.

* Note the variant spelling of Ms. Friedman's given name: according to the story, her mother spelled it that way to prevent anyone from nicknaming the girl "Eliza."

* The main auditorium at NSA was originally named for William Friedman. In recognition of Elizebeth Friedman's contributions to the study of cryptology and her distinguished government service, in 1994 NSA officially changed the auditorium's name to include both William and Elizebeth.

William Friedman was the author of many classified and unclassified works on cryptologic theory and cryptologic history. In retirement, in 1958, William and Elizebeth won the Fifth Annual Shakespeare Award from the American Shakespeare Festival Theater and Academy for their book, *The Shakespearean Ciphers Examined.* (They drew no conclusions about the authorship of the literature, but stated that no cipher systems exist in it).

NAVY CRYPTOLOGISTS

Just as the Army was creating a cryptologic service in the 1920s and 1930s, the U.S. Navy also developed a modern service, which eventually came to be designated OP-20-G. The Navy had a slightly different policy, however: whereas the Army hired civilian cryptologists and gave them direct commissions in case of war, the Navy insisted that its cryptologists be active-duty officers, even in peacetime.

The Navy's cryptologic officers and men -- the early veterans known as the "On the Roof Gang" -- contributed greatly to American knowledge of Japanese naval developments in the 1930s. Without their efforts, the United States would have entered World War II at an even greater disadvantage in naval power than was the case in 1941.

Laurance F. Safford was one of the outstanding talents in the Navy program; he has been called the "Father of Naval Cryptology." As early as 1924, he established a Naval Radio Intelligence Section and later became head of OP-20-G. He also helped develop the ECM Mark 1, a cipher machine which preceded the SIGABA, both of which are on display in another gallery in this museum.

HEBERN MACHINE

We don't know what attracted him to cryptology, but American inventor Edward H. Hebern spent some time thinking about the subject. While serving time for horse theft in the early 1900s, Hebern first conceived one of the more innovative cryptologic ideas, the electro-mechanical cipher machine, incorporating a mechanical rotor.

Hebern never achieved success. In 1926, he fell into bankruptcy and became embroiled in patent and contract disputes. Although he had hoped for a government contract that would allow him to pursue additional research and development, the U.S. Army and Navy decided to use an in-house rotor-based machine rather one of Hebern's.

Hebern had submitted a prototype machine to the government, but William Friedman was able to solve messages encrypted on it, demonstrating that it was not sufficiently secure. Reputedly, Friedman snidely commented that Hebern was a better machinist than cryptographer.

FARLEY DISPLAY

The World War II-era uniform on display in the alcove belonged to Robert Farley. Bob spent a career in the service, beginning with work at Central Bureau Brisbane, a combined unit which supported General MacArthur's operations in the Southwest Pacific. Bob worked with the Center for Cryptologic History as our Oral Historian until his death in 1992.

ENIGMA

Non - Responsive

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. However, in the 1920s the German Navy sought a new method of keeping its communications secure, and adopted a modified version of the ENIGMA. Eventually, the German Army, Air Force, and Intelligence Service also adopted it, making it the workhorse of German military communications security prior to and during World War II.

Non - Responsive

* ENIGMA was the actual trademark name for the German machine, not a codename bestowed on it by the Allies.

The ENIGMA machine was successfully cryptanalized first by the Polish Cipher Bureau, which also developed the concepts for the *bombe*, the countermachine which applied brute force cryptanalysis against ENIGMA messages. When France and Britain guaranteed Polish sovereignty against the Germans, Poland's Cipher Bureau shared the secrets of the ENIGMA and the *bombe* with those two countries. The British later shared these secrets with the United States.

The ENIGMA is an electro-mechanical device, using a combination of rotors and plugs to encipher messages letter by letter. When a letter is depressed on the keyboard, an electrical impulse passes through three (or, in some models, four) rotors, hits a reflecting plate and passes back through the same three rotors. Each rotor scrambles the alphabet in different combinations, thus enciphering each individual letter six times. Note that on early versions when a key is pressed, the righthand rotor steps one place: when this rotor has travelled a full rotation of 26 steps, the middle rotor will step one time; when the middle travels 26 steps, the leftmost rotor steps once. Thus, the path of enicpherment changes for each letter! In later versions, additional notches in the rotors allowed for more stepping. In addition to this, each plug on the plugboard scrambles a pair of letters. The possible permutations per letter are 2^{380}

The ENIGMA was a cumbersome machine to use: generally, operations took three people -- one operator to type in the plain text, one to call out the lighted letter representing the encrypted text, and one to copy it down. Since the ENIGMA was an off-line device, once the encrypted text was written down, it was taken to the unit's communications center for transmission. The Germans put up with this, however, because the ENIGMA represented a high level of security in a small, portable, and rugged package. [In some cases, notably U-Boats, the location itself prevented use by three people, thus some ENIGMAs were outfitted with printers. In this situation, the resultant paper tape was then taken to the communications center for transmission.]

It should also be noted that the ENIGMA is a reciprocating device: a pair of letters will match at the same settings. That is to say, at the same settings, if the letter D becomes P, then P would become D. This means that the machine could be used for either encryption or decryption.

The case on the right displays wartime ENIGMAs as used by different services. Notice that the Luftwaffe ENIGMA could be hooked up to an external source of power in the aircraft.

CRYPTANALYTIC *BOMBE*

The cryptanalytic *bombe* was the essential tool which enabled Great Britain and the United States to read ENIGMA-enciphered messages quickly enough to be of operational value. The *bombe* was not a computer, but a fast processing machine somewhat analagous to the IBM "sort" machines of a generation ago. The original idea for the *bombe* came from the Polish Cipher Bureau, which had made the initial breakthrough into the ENIGMA machine; the British improved on the original design and installed dozens of units at the headquarters of the Government Code and Cipher School (GC&CS) at Bletchley Park, near London.

When the German Navy deployed a four-rotor ENIGMA, U.S. personnel undertook redesign of the *bombe* to meet this new cryptologic threat. The American *bombe*s were manufactured by National Cash Register at Dayton, Ohio; most were deployed at the headquarters of OP-20-G on Nebraska Avenue in Washington, D.C.

Intercepted text would be processed on the *bombe* by running it against expected German military terms until readable text appeared. The *bombe*s were then able to determine the setting of rotors and plugs on the original ENIGMA machine, and the entire message could be decrypted. This type of processing was facilitated by the fondness of military establishments for short, stereotyped messages.

It is unclear how the *bombe* got its name. One tale has it that the Polish Cipher Bureau, when it had solved the German ENIGMA machine celebrated with its favorite dessert, an ice cream *bombe*. Another story says the Polish bombe was so nicknamed because it ticked like a time bomb when it ran. Neither story is likely true; the word "*bombe*" was probably just a cover designation.

NSA's *bombe* was on loan to the Smithsonian Institution for four years (and was a strategic display in the Information Age exhibit in the Museum of American History). It was returned to NSA in the spring of 1996.

WAVEs AND WACs

During World War II, thousands of women volunteered for military service in all branches of the U.S. armed forces. Serving in hundreds of skilled technical, clerical, and support functions, they made significant contributions to the Allied victory.

The photograph on the wall shows a *bombe* at the Navy station at Nebraska Avenue. Much of the wartime *bombe* operation was done by WACs. Many Navy WAVEs assigned to OP-20-G in Washington worked on the cryptanalytic *bombe* in shift work around the clock, seven days a week. Women in the Army and Navy also did many of the "traditional" forms of the work on enemy codes and ciphers, and several of the women who began their careers in cryptology during the war became seniors at NSA in the postwar period.

THE *BIG* MACHINES OF WORLD WAR II

We take our theme from the interesting description of the American SIGABA, which the Germans nicknamed the "American Big Machine." Less well-known than the ENIGMA, these machines were directly involved in the cryptanalytic war between communications intelligence and communications security. Our gallery contains several Allied cipher machines, plus two German devices and two Japanese.

Although ENIGMA remains the best-known German cipher machine of World War II, in the early 1940s, the German military introduced several new cryptographic teletypewriters known under the collective name *Geheimschreiber* -- translated as "secret writer." These machines offered on-line encryption and decryption, that is, plain text could be fed directly into the machine and automatically converted to encrypted text (and vice versa) and broadcast in large volumes at high speed.

Learning that the Germans had nicknamed an early version of these machines SWORDFISH, the British and Americans bestowed covernames associated with fish on these machines and the communications links on which they were used. The two most famous machines in this family are TUNNY and STURGEON.

Just as the British made extensive use of the *bombe* to exploit ENIGMA traffic, the British also developed data processing equipment to attack the "fish" family of machine ciphers. This led to construction of COLOSSUS, which British historian F. H. Hinsley says is "justly claimed as a pioneer programmable electronic digital computer."

TUNNY

When the British first encountered the *Schlusselzusatz 40* (SZ40), they nicknamed it the TUNNY -- after a fish better known to Americans as the "tuna."

The SZ40, manufactured by the German firm Lorenz, was used by the German Army for upper-echelon communications, generally at Army Group level. It provided on-line encryption and decryption of messages and was capable of handling large volumes of traffic at high speed.

Behind the TUNNY display is a picture of the inside of a German command/communications truck, captured by the Allies. The companion picture of this truck was taken at Arlington Hall in 1945. The truck was declared surplus in the late 1940s and scrapped.

STURGEON

Prototypes of this machine were developed at the request of the German Navy, and first units were manufactured in 1932. The German Air Force began using the Siemens T-52 in 1942, at which time the British gave it its fish nickname.

Like TUNNY, the STURGEON provided the German military with on-line encryption and decryption, capable of high volumes at high speed. Unlike ENIGMA, the STURGEON did not substitute letters; rather, it encrypted elements of the Baudot Code used in telegraphic transmissions. One interesting facet of the STURGEON is that the machine does not use wired rotors. The rotors have a series of cogs that open and close on electrical contacts, quite a different concept from most of the cipher machines from this time period.

PURPLE

In the late 1930s, cryptanalysts employed by the U.S. Army and Navy worked on Japanese military and diplomatic codes, achieving success against some -- but not all -- high-level systems. On 20 March 1939, Japan introduced a new cipher system for its diplomatic communications; the U.S. Army Signal Intelligence Service (SIS) nicknamed this new system "PURPLE."

Under the direction of Frank Rowlett, the SIS PURPLE Section worked to decipher this new system. During the autumn of 1940, this section finally produced an analog for rapid decryption of the new diplomatic traffic. Possibly because William Friedman referred to his cryptanalysts as "magicians," deciphered PURPLE messages were codenamed "MAGIC."

Before the war, PURPLE traffic gave forewarning of Japanese intentions in diplomatic negotiations and, finally, intention to break relations. During the war, PURPLE traffic provided information on many aspects of Japanese diplomacy -- and, thanks to the Japanese ambassador in Berlin, many details of German order of battle, defenses, and intentions. Despite this access, however, PURPLE gave no indication of the intended Japanese attack on Pearl Harbor; Japanese diplomats were never privy to Japanese military planning.

Frank Rowlett told the museum curator that when the piece of PURPLE on display and the few found with it were brought in and placed on his desk, it was the first time he had ever seen any part of an actual PURPLE machine. Examining it, he found that the analog of the PURPLE, his creation, used the same telephone stepping switches as the original.

The case contains one of several pieces of the PURPLE machine which were dug out of the cellar of the former Japanese embassy in Berlin. To our knowledge, the U.S. never captured a PURPLE machine intact. It is likely that the PURPLE machine itself greatly resembled the JADE machine, although probably a bit smaller.

Also shown is "PURPLE Analog No. 1." This analog comprises fourteen 25-position telephone stepping switches. Modified electric typewriter equipment (not displayed) was used for input of cipher text, and, after passing through the switching set-up, output of the resultant plain-text. Several Analogs were produced and used throughout World War II. The model on display is the first of several produced in the autumn of 1940; it began decrypting high-level Japanese diplomatic communications on 27 September 1940, and is the machine that solved the famous 14-part message the night before Pearl Harbor was attacked.

JADE

The JADE machine, probably of the same family of equipment as the PURPLE, was a Japanese Navy fleet machine. Although JADE was designed to be used at sea -- bolted down -- this unit had been set up on land at a headquarters unit. The model on display was actually captured on Saipan. The late Frank Raven, a veteran cryptanalyst at NSA, who had been a naval officer during World War II, told the curator that when this machine was captured, there was a typewriter connected to it, and the Japanese code clerk was in the process of smashing the typewriter, but hadn't touched the cipher machine!

TYPE-X

The British brought the cipher machine TYPE-X into use in 1937. It worked on the same principle as the German ENIGMA, with an identical rotor turnover mechanism, but substituted paper tape for the light board. Two additional rotors served the same principle as the ENIGMA plugboard.

The model on display in the museum, TYPE-X MARK III, is a combined cipher machine, not a pure model. The U.S. considered it insecure, so, when used for inter-Allied communications, it was modified by adding a rotor mechanism designed to make it compatable with U.S. cipher equipment.

SIGABA

American cryptologists also created electro-mechanical systems to protect high-level U.S. communications, systems sufficiently secure to prevent the Germans and Japanese from doing to us what we were secretly doing to them. There is, in fact, no known instance in which the Axis Powers successfully decrypted American secure communications from this machine.

The ECM MARK 1 is the early machine, a Navy development, one that Laurance Safford worked on. Cooperating with Frank Rowlett and William Friedman, the combined services came up with the SIGABA or M134C (Army designation) or CSP 888 (Navy).

The SIGABA was used for some time after World War II. In fact, it is believed that the device was taken out of service only because it was an off-line machine which did not meet the speed requirements of modern communications.

M-209

The Converter M-209 (Navy nomenclature CSP-1500) was designed by Swedish inventor Boris Hagelin and built by the L.C. Smith Corona Typewriter Co. It was used for short-term (24-48 hour) tactical cipher messages. The M-209 was completely mechanical, utilizing a pin-set rotor and gears which interacted with a cylindrical drum, all of which turned when the operator cranked the black handle on the right side of the machine.

The M-209 was difficult to set up and thus was prone to misuse by operators, who sometimes would not change the the key set-up often enough for good security. For this reason, the Axis Powers were able to read the M-209 fairly early. However, when used properly, it would give the short-term security needed by forces in the field.

Many veterans who visit the museum used the M-209 and frequently ask to see it, just as many do with the SIGABA.

USS LIBERTY

In June 1967, the *USS Liberty*, AGTR 5, while on patrol duty in the Eastern Mediterranean, was the victim of an unprovoked attack by Israeli air and naval forces.

The flag on display in the National Cryptologic Museum was the ensign flying on the ship at the time of the attack. It was taken down and stowed in a locker, as the *USS Liberty* raised its holiday flag, a much larger and more visible symbol. The original flag was held in private hands and donated to the National Cryptologic Museum in May 1993 by Mr. Mellon Baird, a civil engineer who assisted in damage assessment of the vessel after it reached port. The flag was raised for one final salute at a memorial service held at the National Security Agency on Armed Forces Day, 10 May 1993.

The alarm signal on display was the actual signal in use on the *USS Liberty* and which sounded when the attack began. There are very few artifacts remaining from the vessel, and this one was loaned to the National Cryptologic Museum by the Navy.

The memorial plaque contains the names of the fallen from the *Liberty* incident. Among them is Mr. Allen Blue, an NSA civilian.

Visitors frequently raise the question of whether or not the Israeli attack on the *USS Liberty* was deliberate. This question has also been discussed in any number of books, articles, and media presentations. While there is no unassailable evidence either way, the attack may have been due to misidentification and misunderstanding of communications between Israel and the United States. The Israeli government apologized officially for the attack and paid compensation for the lives lost and property damage. The United States officially accepted the apology and Israel's explanation of the circumstances.

What is important to remember about the Liberty incident is this: a tour of the National Cryptologic Museum shows the importance of Signals Intelligence in American history, but a tour also leaves the misimpression that SIGINT is a safe, academic way to collect intelligence. The *Liberty* incident reminds us that those who produce intelligence on behalf of their country are frequently asked to risk or give their lives for their country.

GREAT SEAL

The Great Seal is an exact reproduction of the seal that was presented to the U.S. ambassador to the Soviet Union in 1946; the original hung in his office in his Moscow residence for six years!

Opened, it reveals the actual type of bugging device the Soviets placed inside the original seal, molded from the original. It was exceedingly sophisticated for its time and not detectable by the normal sweep methods then in use.

[The U.S. State Department owns the original of the seal and the bugging device.]

KGB MUSEUM

The photographs in the KGB case are from the KGB museum, where photography is generally not allowed. These were taken by a friend of the National Cryptologic Museum who happens to be a collector of intelligence memorabilia and author of several books on the subject. Shortly after the collapse of the former Soviet Union, he was given a private tour of the KGB Museum and allowed the rare privilege of taking photographs. He was kind enough to share a set of them with us.

The photograph of Felix Dzerzhinsky's death mask is fairly significant. Dzerzhinsky (1877-1926), sometimes nicknamed "Iron Felix," was one of the Old Bolsheviks and founder of the CHEKA, a predecessor of the KGB. Apparently, even though the Russians pulled down the statue of him which stood in Dzerzhinsky Square, just outside the KGB headquarters, they still remember and revere him inside.

Notice the long-barrelled pistol in the bottom photograph on the left: that was issued to U-2 pilot Francis Gary Powers prior to his ill-fated reconnaissance flight in 1960. The yellow tube beneath it contains a poison syringe also issued to him.

The badges are all authentic, some from the KGB, some from the former Soviet militia. They were procured through a dealer and include school, commemorative, and proficiency badges. One was the type given to outstanding border guards. The topmost badge is an award for Friendship Among Peoples, honoring the diversity of the former Soviet Union. The second shield from the top is a police badge, associated with the KGB. Between the buckles on the upper left is the Soviet equivalent of a "good conduct medal."

U-2 FRAGMENT

On 1 May 1960, while flying over Sverdlovsk, deep in Soviet territory, American pilot Francis Gary Powers was shot down in a U-2 high-altitude reconnaissance aircraft. The Soviets accomplished the shootdown with fourteen SA-2 missiles and MiG-19 jet interceptors. All fourteen SA-2s reached the altitude and exploded at the same time; the shockwaves damaged the U-2 and one of the MiGs.

On 7 May, Soviet premier Nikita Khrushchev held a news conference in which he displayed Powers and accused the United States of spying. The resulting international political turmoil caused the cancellation of a summit meeting scheduled in Paris between President Dwight Eisenhower and the Soviet premier.

Powers was sentenced to ten years in a Soviet prison. However, he was released after only twenty-one months, when the Soviets exchanged him for convicted spy Rudolph Abel, who was in a U.S. prison. Powers died in August 1977 in Los Angeles, when the traffic helicopter he flew ran out of fuel and crashed.

In late 1994, two Russian officers, including a lieutenant general, paid a private visit to the National Cryptologic Museum. In token of their visit, they presented the museum with a fragment from the U-2 piloted by Francis Powers.

VENONA

On 1 February 1943, the U.S. Army Signal Intelligence Service began a small, secret program to examine and possibly exploit Soviet diplomatic communications; this program eventually was given the codename "VENONA." One analyst who pioneered the program was Miss Gene Grabeel. Initial analysis indicated that five cryptographic systems were in use between Moscow and a number of overseas Soviet missions: diplomatic, trade, -- plus KGB, and two organizations of the GRU, the Soviet military intelligence organization.

* Given the complicated organizational history of the Soviet espionage organization and the many names by which it was known during this period, we are referring to the organization simply as "KGB" for the sake of convenience.

In the summer of 1946, after more than three years of a team effort, Meredith Gardner, an analyst at Arlington Hall Station, began to read portions of KGB messages that had been sent between the KGB Residency in New York and Moscow. In December, after reading some other, more routine KGB messages, he broke into a message sent to Moscow in 1944 which contained a list of names of the leading scientists working on the Manhattan Project -- the American effort to develop the atomic bomb during World War II!

As more messages were decrypted, they showed that the Soviet Union had engaged in a massive espionage effort against the United States during the war, including penetration of the Manhattan Project. When this became apparent, General Carter W. Clarke, then Assistant G-2, called in the FBI liaison and shared these secrets; in October 1948, FBI Special Agent Robert Lamphere became the FBI's liaison directly to those working on the VENONA project.

The break into the VENONA messages came strictly from cryptanalysis. A number of myths have arisen in the popular literature about this; some attribute the U.S. ability to read the messages to captured codebooks or pinches of code material. None of these myths are correct; VENONA was a success because of superior analytic work.

These messages provided early leads to Soviet espionage agents, including many who later became infamous in the 1950s. Among these Soviet agents were Klaus Fuchs, a German-born British physicist, and Julius and Ethel Rosenberg. The Rosenbergs, who became a controversial political case, were arrested in 1950, tried, convicted of conspiracy to commit espionage, and executed in 1953; they steadfastly maintained their innocence, and many believed they had been framed by the government. The VENONA messages show clearly that Julius Rosenberg --

identified first by the codename ANTENNA, then LIBERAL -- was heavily engaged in espionage; one message shows that his wife may have been cognizant and possibly active in this endeavor, but are not definite on the type or scope of her activities.

* It is commonly and inaccurately stated that the Rosenbergs were convicted of espionage. Note that they were convicted of *conspiracy to commit* espionage -- a different charge, which required a lesser standard of proof than espionage itself.

It is important to note that no individuals were tried or convicted on the basis of VENONA messages. These messages provided initial investigative leads to many espionage agents: the FBI subsequently had to develop information from other sources which could be used for indictment and prosecution. Neither the existence of VENONA nor any of its product was ever produced in court. Nevertheless, this still represents an excellent example of cooperation between the intelligence and law enforcement communities.

There were about 2,200 VENONA messages translated. Of these, 49 were released in July 1995, when NSA declassified the project and made its existence public. All 2,200 messages will be released over the course of 1996.

In a circular message of 12 September 1943, the MGB, predecessor to the KGB, explained that the dissolution of an organization known as the COMINTERN required a change in espionage procedures. The COMINTERN -- or Communist International -- was founded by Vladimir Lenin in 1919 to assert Communist leadership among socialist parties; it was also used to promote communist revolutions in some countries. During World War II, however, the Soviet Union undertook a "united front" policy and disbanded the COMINTERN to ease the suspicions of its western allies.

In the September 1943 message, the MGB explained that the dissolution of the COMINTERN eliminated one of the MGB's liaisons for intelligence work with communist parties around the world. Therefore, to avoid exposing MGB officers in Soviet missions abroad, intelligence meetings with local communists should be carried out only by "special reliable undercover contacts," not MGB officers resident in a Soviet embassy. This message confirms the suspicions that the COMINTERN was engaged in espionage on behalf of the Soviet Union.

The problems common to intelligence agencies worldwide also affected Soviet espionage. A circular message of December 1943 reveals that the MGB, predecessor to the KGB, was worried about security in its overseas operations -- insufficient attention to secrecy and the principle of "need to know." Moscow headquarters gave explicit instructions on procedure and warned ominously that if there were "violation of the rules of secrecy, we will take strict measures."

Our KGB guard is a captain in service uniform. The badge he wears is a school badge, that is, KGB school. The fact that he is wearing his sidearm indicates that he is on special duty, perhaps as a prison guard, since KGB officers rarely went about under arms.

HALL NUMBER 2

NATIVE AMERICAN CODETALKERS

While the "Big Machines" of World War II were relied on heavily for security of graphic communications, there was no comparable equipment for tactical voice. Some equipment had been developed in the immediate prewar period, but was considered unreliable. Therefore, the U.S. military turned to the minority languages of the country for voice security. The basic idea, however, can be traced back to World War I.

The first U.S. military unit to use Native American codetalkers in combat was the Army's 142nd Infantry Regiment, 36th Infantry Division. The first use came in October 1918 in the Argonne Forest. After suffering losses attributed to German intercept of U.S. communications, the 36th Infantry mobilized eight Choctaws to provide security. This use supported the successful withdrawal of a unit, followed by a successful attack on the Germans. The communicators substituted Choctaw words for English military terms, thus it could be called "Codetalking."

The U.S. entered World War II with voice security equipment suitable only for the highest levels. The Army early began utilizing Native Americans to fill this need, using Choctaws, Comanches, Winnebagos, Pawnees, Kiowas, Cherokees, Navajos, and possibly others. These Native American communicators worked in both the North African and European theaters. (Although there was opposition by some in Army headquarters, notably William F. Friedman, local commanders responsible for local security used Native Americans anyway.)

The Marine Corps use of codetalkers admittedly was stimulated by news of the Army training. The Corps chose to use Navajos exclusively; over 400 Navajos served in this program over the course of the war. With the backing of headquarters, the program was more extensive than the Army's, and also was codified and incorporated into training. Thanks to numerous articles, books, public broadcasting documentaries, and mention in such popular entertainments as the movie *Battle Cry*, the Navajo codetalkers have become the best known of the many Native Americans who served their country in this capacity.

Both the Army and Marine Corps programs would have continued, even been enlarged, but the supply of combat-eligible Native Americans who knew both English and their native language was exhausted. The Army established a school to teach Navajos English, but the war ended before this source could be tapped.

The overseas bag that we are happy to place on exhibit belonged to Wilson H. Price, one of the early Navajo codetalkers. Mr. Price stayed in the Corps and retired about 1970 as a master sergeant.

The Navajo Codetalkers, who served with the U.S. Marines throughout the Pacific Campaigns of World War II used the Type CRI-43007 transmitter-receivers. These rugged, 32-lb. radios were manufactured for the Navy Department by Westinghouse. An example of this radio is in the case with the SIGJIP.

SIGJIP (AN/GSQ-1)

Human or machine? In 1944 this became a real question for all the Codetalkers. Indeed, had SIGJIP prevailed in combat, the Codetalkers might not have been called upon to provide their unique skills in the decisive terminal battles of World War II.

In 1994, the U.S. fielded over 200 of these AN/GSQ-1s, known as SIGJIP. The U.S. had entered World War II with no tactical voice encryption capability. In late 1940, recognizing the need, the Army began developing a device which would provide at least one-hour's worth of security, be small enough to carry into fast-moving tactical operations, and work with current low-level, HF voice, radio, and wireline communications.

When fielded in 1944, SIGJIP was one of the earliest embodiments of the Time Delay Scramble technique for speech protection, wherein speech was broken up into a number of discrete blocks on bands (narrow for SIGJIP) and each band then delayed in time and transmitted in scrambled order. For keying, it used code cards and keyboard key changers. It was portable: 1 1/4 cubic feet (small for that era), 25 lbs, and required 24 volts for operation. SIGJIP was deployed in every theater of the war, but ended by receiving limited use: while it did work as required, it had difficulty synchronizing with various field communications equipments.

The Codetalkers, who had already proven many times they were faster than the several literal encryption devices specified for tactical use, thus triumphed also over their main competitor, the SIGJIP voice encryptor. Not only did the Codetalkers synchronize better with both humans and machines, they could also still provide security longer than one hour, since they used a non-systematic encryption system, rather than the systematic one used by SIGJIP. Further research in the postwar years would succeed in the production of fully secure field-hardened tactical voice encryption equipment -- a development which would end the "Codetalking Era."

COMMUNICATIONS SECURITY EQUIPMENT

KL-7: This device (Navy nomenclature KL-47) was used by the U.S. Army and Air Force from the early 1950s through the early 1980s. It was an off-line rotor-based system which replaced the SIGABA/ECM. The basket behind the keyboard held eight rotors. In its later years, the KL-7 was used for SECRET-level communications only and was used by NATO troops for interoperability with U.S. forces.

KY-38: Also known as the NESTOR Digital Secure Voice System, the KY-38 was a "Man-pac" digital radio encryption device. Together with the PRC-72 radio, the gear weighed about 75 pounds. The equipment was designed very quickly in the mid-1960s for use in the Vietnam War, and was used into the 1980s. The KY-8 and KY-28 were NESTOR equipment used at base stations and in vehicles.

KY-65: Also known as PARKHILL, this was an analog secure voice system. The KY-65 scrambled voice by time and frequency, thus producing poor voice quality as compared to a digital signal. It is the only analog system used by U.S. forces. By 1995, virtually all PARKHILLs had been phased out of use.

KY-57: The VINSON Digital Secure Voice System is widely used by the U.S. military and government. It offers excellent voice quality and can be electronically re-keyed over the air from a remote site. The KY-57 weighs only 11 pounds.

EVOLUTION OF VOICE SECURITY EQUIPMENT

SIGSALY

The first true secure voice system to be put into use, the SIGSALY was developed by Bell Laboratories without a government contract. Bell Labs realized such a system would be needed and developed the first such system to use spread spectrum techniques. SIGSALY had 40 racks of equipment; took up to 13 people to operate effectively and cost $1,000,000 per station. During World War II SIGSALY terminals were set up in Washington, D.C., London, Paris, North Africa. and Australia. Although voice quality was poor, it was secure and never broken by the Axis Powers.

SECURE TELEPHONES

Developed in the 1970s, Secure Telephone Units (STU) I and II were intended for executive use. The main drawback to these telephones was the need to call a Key Distribution Center (KDC) to set up the call, with a resulting 2-3 minute delay, often unacceptable to users.

STU-III

The STU-III is the most sophisticated secure voice telephone system in the world. It was developed in the mid-1980s; over 300,000 were in service as of 1995. The telephone has excellent voice quality and takes only about 10 seconds to "go secure." It can be used as a plain old phone (POTS), but at the push of a button can go to the highest levels of security. It has FAX, DATA, and Secure Video capability, and has gained unprecedented acceptability at all levels of government. The unit is unclassified until a Crypto Ignition Key (CIK) is inserted, which enables the user to make a secure telephone call; when the CIK is removed, the unit is once again an unclassified telephone.

THE HOT LINE

The original Washington-to-Moscow Hotline was a one-time tape/teletype system for which the Soviets and Americans exchanged compatible equipment. This East German teletypewriter, made by Gerdlewerk, Karl-Marx-Stadt, was donated to the NCM by a former U.S. Army officer who had been in charge of the Pentagon end of the link. The original Hotline went into use just a few months before the assassination of President John F. Kennedy in 1963; it was phased out in the early 1980s and replaced by a computerized system.

COMPUTER DEVELOPMENT

The PACE 10, as nearly as we have been able to discover, is the first analog desktop computer used at the Agency. It was self-contained to the extent that the logic is in the interior. The output was a printing device. The plug-in units have a wire associated with them and each panel is set up to do a different mathematical function. For a fairly complex mathematical problem, one would plug all the appropriate panels and hand-wire them together. The manual was quite proud of the fact that once it was set up, the problem could be completed in 15-60 seconds.

HARVEST

Samuel Snyder, in his reference work on computer development (SRH-003), calls HARVEST "undoubtedly the most sophisticated computer of the second generation." It was one of a limited number of systems built by IBM. In 1954, under a program known as "STRETCH," planners worked to increase circuit speed, lower memory access time, improve the logical design, and employ higher speech and capacity disks and tapes.

Although a greatly improved computer model embodying these features was offered to NSA in 1955, NSA turned the proposal down because the overall logic was not directed toward Agency needs. After some modifications were made, NSA contracted for a "STRETCH" computer in 1958, and it was delivered in 1962. This computer, known as HARVEST, turned out to be one of a kind; no successor was built and no commercial models marketed. However, it served as an excellent learning experience for the engineers involved, and its design had influence on computer logic technology, core memories, and tape drive systems.

SUPERCOMPUTERS

Supercomputers are defined as those used for numerically intense computations, with high scalar and vector processing capacity, "with appropriate primary and secondary memory resources," and, of course, appropriate price. What this means is, the difference between supercomputers and regular computers is speed and power. Supercomputers provide a sustained performance of over 2 billion Floating Point Operations Per Second (*GFLOPS*). Supercomputers also require much larger amounts of power and cooling.

MICROCHIPS

NSA has taken a leading role in U.S. government research, development, and production of microelectronics technology. The Agency's Special Processing Laboratory, opened in 1991, is a facility designed to fabricate classified and otherwise unobtainable devices to support the needs of the Defense Department and the intelligence community. The SPL is a 20,000-square-foot building in which are produced state-of-the-art metal-oxide-semiconductor technology Applications Specific Integrated Circuits (ASIC).

When the SPL began producing in 1991, it fabricated at 1.0-micron feature sizes. A micron is a micrometer or one-millionth of a meter. For comparison, one human hair typically measures 100-microns in diameter. The SPL is not capable of producing at 0.8 microns, and is seeking the capability for a 0.5-micron process.

The mannequin in the white gown and face mask represents an individual dressed to enter the "clean room," where microchips are manufactured. The SPL operates a Class 10 clean room -- that is, it does not allow the prescence of more than 10 particles per cubic foot of air; the particles can be no larger than one-half micron in size. Clear air is circulated through ceiling filters six times a minute.

OILSTOCK

OILSTOCK is a high-resolution interactive geographic-based software system developed and supported by the National Security Agency. It is used to store, track, and display near-real-time and historical data over a map background. OILSTOCK was developed on the UNIX System V environment and was written in the C Programming Language. Since 1984, OILSTOCK has matured into a standard product used by thousands of analysts throughout the intelligence community and the Department of Defense.

AUTOMATED CARTRIDGE SYSTEM

The Automated Cartridge System (ACS) from Storage Technology Corporation, in a dodecagon (12-sided) shape, is an electronic filing cabinet with the capacity to hold up to 6,000 cartridges. The vision system uses red, light-emitting diodes (LEDs). The rotobotic arm of the StorageTek system has two cameras and a "hand"; the cameras find the bar code of the requested cartridge, and the "hand" moves it to the retrieval area where the needed information can be extracted. When the cartridge is no longer needed, the process is reversed and the cartridge is placed back in its holder. The "Arm" can move up to 35 mph, and can perform up to 175 cartridge exchanges per hour.

The cartridges have 50 gigabytes of information; thus the entire system holds 300 terabytes. As examples, 300 terabytes can store the equivalent of 1.5 million years of the *Wall Street Journal*, fill enough pieces of paper to circle the globe 3,000 times, or fill a stack of books 11-deep that would run from New York City to Los Angeles. This automated system became available in 1988. Bell Atlantic also uses these devices and has 50 in Maryland.

QUESTIONS FREQUENTLY ASKED ABOUT THE MUSEUM

Q: How can you justify spending so much money on a museum in these tough times?

A: In actuality, the National Cryptologic Museum was established at very low cost.

A majority of the exhibit cases were donated to us by the Smithsonian Museum of African Art or the Westinghouse-sponsored Historical Electronics Museum. One case was purchased directly by NSA, but that one (the Verdun Intercept Site) was bought for a display elsewhere, before NSA decided to establish a museum; when the other display did not materialize, the case was placed in storage and retrieved once the museum became a reality.

The books and most of the artifacts were already in NSA's possession and cost nothing to acquire for the museum. Some items have been loaned to the museum by other government agencies or private collectors. The only direct costs to the museum were the display graphics, and the salaries of several NSA craftsmen who helped put the exhibits together.

Thus, even though the museum "looks like a million," in reality the direct costs were rather small. Many of us believe that these costs have already been recouped in terms of the specialized education the facility provides the NSA/CSS work force and the benefits it has in other areas, such as employee morale.

Q: When did the museum open?

A: The National Cryptologic Museum opened in July 1993 for NSA/CSS personnel only. This enabled us to gain much-needed experience in the day-to-day operation of a museum, as well as a chance to use the facility without interruption for the professional education of the work force. The museum opened to the public in December 1993.

Q: Are these exhibits permanent?

A: Most of the material relating to pre-World War II cryptology will be permanent. In 1996 we will begin changing or rotating some of the other exhibits.

Q: Where did the museum collection and books come from?

A: The equipment came to the museum in several ways. Some of it was U.S. cryptologic gear actually used in operational work. Some of it was equipment captured by the U.S. military in World War II and sent to NSA's predecessors for study. A few items were purchased directly by NSA in previous years for study.

The rare books also were acquired in the 1930s by America's cryptologists. These were not purchased for display or merely because they were rare -- these were working textbooks used to train the generation of cryptologists who served in the world war.

Q: Have the rare books been appraised?

A: We have tried to set a value on them. About fifteen years ago, we took some of them to the Smithsonian -- the rare book library in the Museum of American History -- but they could not give us a set value. The problem is twofold: it is difficult to place an accurate value on items so rare and specialized. One way value is set for antiques or rare books is by comparison with recent sales of similar items, and in the world of cryptologic history, many of our holdings are unique.

Q: Are there special precautions about preservation for these rare items?

A: Yes, many of the rare items, particularly the books, are stored more suitably in the museum than before they were put on display. The items are fairly well protected from humidity and heat change, and the rare books each have a separate UV-filter cover over them.

QUESTIONS FREQUENTLY ASKED ABOUT VENONA

N.B. For all but the most general questions about the investigation, indictment, prosecution, or conviction of the espionage agents mentioned in the VENONA material, please refer the questioner to the FBI or the Justice Department.

Q: What does VENONA mean? Why was that name assigned to the material?

A: So far as we can determine, it is a made-up term that was applied to the project and material as a short-hand reference. Earlier terms for the same program were BRIDE and DRUG.

Q: What are the meanings of BRIDE, DINAR? What is the circle on the bottom of the page?

A: These are various codewords and symbols formerly used to identify signals intelligence information. DINAR was used from 1961 to 1965 to differentiate signals intelligence from general intelligence, not special programs like VENONA. The codewords BRIDE. DRUG and VENONA all referred to the same special program at different periods of time.

Q: Why did NSA decide to release the VENONA material after so many years?

A: After exhaustive study, NSA decided it could release the VENONA translations without harming current or future intelligence sources and methods.

Q: Why are there so many deletions in the documents?

A: These deletions (AKA, redactions) were made where technical information still in use today might be revealed, or where privacy issues were involved.

The release of VENONA translations involved careful consideration of the privacy interests of individuals mentioned, referenced, or identified in the translations. Some names have not been released when to do so would constitute an invasion of privacy.

Q: What could be harmful in releasing intelligence reports 40 years old? Even the CIA has released its CORONA holdings.

A: Cryptologic information is exceptionally fragile. These documents are under constant review by archival and declassification experts so that those which can be released without harm to national security will be.

Q: Don't you have an obligation to *history* to release all Cold War intelligence documents?

A: The obligation of the intelligence community is to provide U.S. policymakers with the best information possible to assist them in deliberations and decisions; in the second place, the community must protect sources and methods so we may continue to provide quality information to policymakers. We do have an obligation to *history*, although not necessarily to individiual *historians*. We are preserving materials in accordance with public law, so that when documents may be released for historians' use, we will be able to do so.

Q: How do you answer allegations that this information may have been fabricated?

A: The material speaks for itself.

Q: Why were you targeting Americans in the VENONA project?

A: No Americans were targeted in the VENONA project. The VENONA project examined and exploited encrypted Soviet messages sent between Soviet entities. Information about U.S. persons was incidentally discovered while exploiting a legitimate foreign intelligence target.

Q: Why were some names redacted and others not? What criteria were applied to redacted names? What, if any, consideration did you give to the disruption in people's lives based on disclosure of this information?

A: The release of VENONA translations involved careful consideration of the privacy interests of individuals mentioned, referenced, or identified in the translations. Some names have not been released when to do so would constitute an invasion of privacy.

Q: What about Oppenheimer? or Fermi? Was he identified in the VENONA documents? Was he implicated? Who was VEKSEL? Is (fill in the blank) mentioned in VENONA? Can you confirm information that appeared in (pick the author's book)?

A: The translations have been released & speak for themselves. It is up to interested individuals to review the material and decide if information published in a particular book is accurate or not.

Q: Why will it take 12 months to release all VENONA material? Why not release everything now and let the historians, media and general public look at all the information so that they can decide for themselves if history was accurate?

A: There are approximately 2,200 final translations. All of this information must be carefully examined and the criteria for protecting information where required must be applied appropriately and in accordance with the law. This is an important responsibility we take very seriously.

Q: How were the equations made of true names to covernames? Did NSA reason these out? What is the degree of certainty that Julius Rosenberg equates to the ANTENNA/LIBERAL covernames?

A: The method of equating people to covernames varies: sometimes, individuals were identified by actual name in the message; sometimes, the context of a message clarified an individual's identity; at other times it was through FBI analysis and/or a combination of these. The equation of Rosenberg is without question.

Q: When was the information provided to the FBI? Were they given the new translations in the 1970's also?

A: Beginning in 1947. ((G2 handled the initial investigative work the first year, then turned this responsibility over to the FBI.)) The FBI also received the translations from the 1970's.

Q: Are there still investigations ongoing?

A:: You will need to contact the FBI for any information about investigations.

Q: Which spies were identified and prosecuted because of VENONA?

A: The information from VENONA was merely used to provide early tip-off to the law enforcement community, which then had to develop its own sources of information. No individuals were prosecuted on the basis of the VENONA translations. NSA and its predecessors have not had and do not have a law enforcement function; we provide information which may be used by law enforcement for the identification of suspects. Only the FBI and Department of Justice can speak authoritatively on investigation and prosecution which resulted from VENONA intercepts.

Q: Did Arlington Hall/NSA help the FBI by explaining the VENONA material and pointing out what it meant?

A: Arlington Hall/NSA and FBI collaborated on this information.

Q: Why were some of these documents retranslated in the 1970's? Is it common practice for the Agency to re-do work so many years later? Were the original translations wrong so that they had to be readdressed? What value did revisiting the translations have?

A: Progress in cryptanalysis facilitated the creation of more complete translations. The partial translations done in the 40s and 50s provided sufficient information for the FBI to develop leads. The original information was not incorrect, it was only partially recovered.

Q: Why do some areas say "unrecoverable" and other areas say "unrecovered"? Is there a difference in meaning?

A: One is an optimist and one is a pessimist -- "Unrecovered" was used to indicate that the analyst thought he or she might have been able to figure out the text in the future. "Unrecoverable" meant the analyst concluded that they would probably never be able to determine the meaning of the text analytically.

Q: What does C%, D% mean in translations?

A: These were translators' designations to indicate validity. A% = certain, B% = probable, C% = possible, D%= tenuous

Q: What does "double encrypted" mean?

A: Two levels of keys were applied to the messages before they were sent.

Q: Is this the first time the Agency has admitted that the have the capability to break double-encrypted information?

A: We will confirm that this information was double encrypted and was read as you see here. We will not comment on the Agency's capabilities any further than providing these documents.

Q: You mention that some codes were never broken. Is that true using today's technology?

A: We do not comment on current operational capabilities.

Q: How many times were each of the messages reworked or retranslated?

A: Some of the messages were translated only once, others were translated as many as ten times.

Q: Did you save any of the old translations? When will they be released?

A: Prior translations do exist. Prior translations are not part of this voluntary release because they do not represent the most complete translation.

Q: What is the significance of the different formats in which the translations are written?

A: Formats change from time to time and in earlier times may have even been somewhat individual and subject to the particular analyst's reporting style.

Q: What SIGINT are you holding on crisis (fill in the blank)?

A: We cannot comment about whether there is or is not SIGINT concerning other postwar crises. If there is such data, it will be reviewed and released in accordance with the law and the new Executive Order.

Q: Does NSA already have a history of the VENONA program written? Will it be released?

A: Yes, and, like the VENONA documentation itself, this document will be reviewed for declassification and release in accordance with the Freedom of Information Act and the Mandatory Declassification Review Process.

Q: How did you get the messages? Was it by intercepting signals?

A: We will not comment on how this information was obtained.

Q: Why were you working Soviet messages in 1943, a time when the USSR was an ally in the war against Nazi Germany?

A: American policymakers in 1943 had a very real fear that Germany might defeat the USSR or at least force Moscow to withdraw from the war, with enormous consequences for the U.S. military in the struggle against Germany in the west. It was only responsible of U.S. intelligence organizations to seek accurate information about the Soviet-German theater of war through cryptanalysis of Soviet messages.

Q: What was the working relationship between British and U.S. Intelligence? Between MI5 and the FBI?

A: The British and U.S. governments did work together on VENONA. There was an excellent relationship between the Intelligence and Law Enforcement organizations of each country.

Q: Why are some of the spellings in the translations British - did the British translate these documents?

A: There were a number of British integrees in several SIGINT disciplines.

Q: Given the fact that some of the translations date from the 1970s, does that mean that the U.S. and Britain cooperated on VENONA throughout the timeframe?

A: Yes

Q: Did NSA distribute these reports to its allies? If so, who and when?

A: The distribution list is on the documents. They were released immediately following completion of the decryption, translation and analysis.

Q: Who authorized the VENONA project?

A: The War Department General Staff.

Q: Who in the government decided who would see the VENONA documents?

A: The U.S. Army Chief of Staff and the War Department General Staff.

Q: Did Senator McCarthy or the Government Loyalty Committees have access to VENONA?

A: Not as far as we know.

Q: Did President Truman or President Eisenhower see the VENONA information?

A: We do not know.