Volume 42, Number 1 Spring/Summer 2023

Journal of the

CALIFORNIA HISTORICAL RADIO SOCIETY

FOR THE RESTORATION AND PRESERVATION OF EARLY RADIO

FROM THE BIRTHPLACE OF BROADCASTING

California Historical Radio Society

HOME OF THE BAY AREA RADIO MUSEUM & HALL OF FAME

The California Historical Radio Society (CHRS) is a non-profit educational corporation chartered in the State of California. Formed in 1974, CHRS promotes the restoration and preservation of early radio and broadcasting. Our goal is to enable the exchange of information on the history of radio, particularly in the West, with emphasis on collecting, preserving, and displaying early equipment, literature, and programs. Yearly membership is $30 ($40 non-USA).

CHRS Museum in Alameda

CHRS has been fortunate, through the generosity of its donors, to purchase a home for the CHRS museum and education center. It is located at 2152 Central Avenue. The building was built in 1900 as a telephone exchange.

CHRS volunteers are actively restoring the building to make it optimal for use. Our goal is to create an environment to share our knowledge and love of radio and enable us to create an appreciation and understanding for a new generation of antique radio collectors and historians.

Please come visit us any Saturday 9am to 3pm. Visitors and groups welcome at other times by appointment; Contact Steve Kushman.

◊

Contact us:

CHRS, PO Box 31659, San Francisco, CA 94131
or info@californiahistoricalradio.com

Visit us at: www.CaliforniaHistoricalRadio.com

Officers & Directors

Mike Adams	– Chairman, Webmaster
Steve Kushman	– President, Radio Central Project Manager
Scott Robinson	– Vice President, Technical Ops.
Jaime Arbona	– Secretary, Mailing, Donations
Richard Watts	– Treasurer, Membership, Journal Editor
Philip Monego	– Director at Large
Dennis Monticelli	– Education

W6CF Trustee, John Staples, W6BM

CHRS Central Valley Chapter (CVC)

Eddie Steeves – Chairman

Staff

Bart Lee	– Historian, Archivist
Len Shapiro	– BARM Executive Director
Walt Hayden	– Collection Mgr., RC Planning
Cynthia Edwards	– Collection System Mgr.
John Stuart	– Resident Engineer, Networks
Kent Leech	– Auction Manager
Paul Bourbin	– Landscape Ops.
Tom Bonomo	– Investments, Name Badges
Dave Billeci	– Video Production
Dennis Monticelli	– Amateur Radio Operations
David Vasquez	– Electrical Transcription Project
Lunch crew:	Keith Scott, Betty Cosmos, Judy Mears

Contents of the Journal

COLUMNS

4 **From The President**
Steve Kushman

5 **From the Chairman**
Mike Adams

6 **CHRS Central Valley Chapter News**
Eddie Steeves

FEATURE ARTICLES

7 **The Wireless Boys of Alameda, Part 3 - The Adventures of George Hubbard**
Robert Rydzewski

15 **Amateur Night at Radio KLX, Oakland, 1924 —a young man wins the Ears of Oakland**
Bart Lee

19 **The Enigma of Ultra**
Richard Watts

Front Cover: **Enigma Machine circa 1936**

Rear Cover: **Images of CHRS volunteers**

From the Editor

I wish to thank all the authors for their articles, support, and scholarly contributions. Robert Rydzewski again takes us back to early wireless in Alameda and a look at another early wireless operator from Alameda; Bart Lee shares a performance in Oakland in 1924 and the resulting mail-in applause. I discuss a recent trip to England and to Bletchley Park and the National Museum of Computing where there was lots to learn and see regarding the importance of wireless, radio, and decryption during WWII. Steve Kushman and Mike Adams provide updates. Eddie Steeves gives us an update of the Central Valley Chapter.

I am always in need of quality content related to broadcast radio, ham radio, and television. If you have something to contribute, I urge you to let me know. I am especially interested in technical content. It can be of two types, a narrow topic in depth or a more broad topic with less depth. Enjoy . . .

Richard Watts, jrchrs@comcast.net

◊

From The President

by Steve Kushman

The state of the Society is **EXCELLENT!** CHRS is well on our way to becoming a world class organization for the celebration of radio and communications history; Well on our way to creating a visitor's destination in Alameda by building an inviting museum in our 123 year old telephone building; To foster curiosity about communications through an environment of educational exhibits and classes; To introduce youth to the history that is not always taught in schools these days; And to offer a unique facility for community use.

CHRS is lucky and very fortunate to be one of the only historical radio organizations in the country to own its facility outright. This is due to our remarkable donors and supporters. They donated enough to allow us to buy 2152 Central Avenue, the original Sunset Telephone building in Alameda, built in 1900. And the support continues from our passionate members. People donate to us because they believe in what we are doing and see our progress… which brings us to our present time… 9 years since our purchase.

We have done many projects to improve the facility. They include, voluntary earthquake retrofitting, new handicapped lift, new rear steel stairway and landing, new wiring and plumbing, new basement concrete slab, waterproofing and drainage system, new paving, building the library, building the wood shop on new concrete slab, building 2 restrooms, building the electronics repair shop, building the ham shack, the communications center, the TV display, the Bay Area Radio Hall Of Fame, the working 1958 radio control room and Audio Transfer Facility, rebuilding the kitchen, vacuum tube vault, office, utility room and conference area. Does it sound like we are done? No sir. We are now working on our 2 largest and most important projects. They are actually connected. Our 68 foot by 28 foot Great Room is being restored to its original 1900 appearance. New drywall, new efficient windows, (sash sliders and top half rounds), rebuilt wainscoting, replaced moldings & window trims, baseboards, flooring and paint. Then we will demolish the 1950s false flat front of the building and the 1950s added entrance doorway structure, to reveal the original 1900 California Mission Revival style, reposition our ADA entrance door, restore all front windows, rebuild the concrete and brick front stairs, rebuild the entrance doorway into the Great Room, repair and recreate stucco trim pieces and soffits as needed. You can help by donating to our project. Just go to www.chrsradio.com and select the Support tab, Facade Restoration Fund. Many people have donated but we can use much more. Remember it's a great and lasting project that you are helping to fund.

Radio Central Now.

Radio Central Soon.

Bob Rydzewski receives the 2022 Doc Herrold Award.

2022 'Doc' Herrold Award - For many years, CHRS has presented the Charles D. 'Doc' Herrold Award, which celebrates outstanding achievements in the preservation & documentation of early radio. Your Board of Directors unanimously nominated Bob Rydzewski for the 2022 Herrold award this past December. Bob is quite dedicated and has done a terrific job of archiving the SOWP collection. And due to circumstances, we only recently presented Bob with the award. This is the first Herrold Award presented since 2015. We have been pretty busy building a museum so 'Doc' was on hiatus. And now it's time again to recognize special individuals who have done so much to support radio preservation.

New CHRS Intern - Giuliana Meanns, a junior at Alameda's Encinal High School has started to volunteer for CHRS. Giuliana loves radio. She has her own weekly radio show on 96.1 KJTZ. She has begun to digitize some of our vintage Reel to Reel audio tapes; Interviews by Dusty Street from the 1980s and the Alex Bennett collection. How cool! We are always so pleased when we can grab the imagination and interest of the younger generations. Thank you Giuliana! We welcome your enthusiasm for CHRS! SEE GIULIANA'S PICTURE ON THE BACK COVER.

We want to hear from you. Please call or email me at: **(415) 203-2747** - Steve@chrsradio.com. Your comments and questions are most appreciated. Keep Smiling! Steve

◊

From The Chairman

by Mike Adams

"Hey Dig Me.!"

Those words, from the late comedian George Carlin are what CHRS would like you to respond with and "dig us," the California Historical Radio Society. I would like to introduce the parts of our organization, or interest areas, call them our "Brand Names." Whether you are long time member or one of the hundreds of new members, get to know these brands and what they mean. Behind each research and hobby brand are dedicated, passionate CHRS volunteers. After a deep dive into one of our websites you might exclaim, "why these people are just like me." The California Historical Radio Society is the organization that welcomes hundreds to collect and restore and learn about the centuries-old technology of the radio and the people who invented and created it.

The California Historical Radio Society had its beginning in 1974. In the 1970s radio collector clubs worldwide began their lives in the parking lots and borrowed spaces in schools and churches. This allowed fellow hobbyists to learn about the hardware and buy and sell and fix it. There were usually a few active collectors who organized the group and kept it going. Most clubs don't have the opportunity to grow beyond that. We have been fortunate to have been able, through the generosity of our members, to acquire a permanent home — a place to move from hobby to credible museum, to share our passion with the public, and have them get to know our brand. The museum provides a place to expand our many interests beyond radio into related areas of communication like vintage audio and telephone to engage more of your interests. Without a Steve Kushman, our generous donors, and all the volunteers, CHRS may have remained just a fading oily parking lot memory. Get to know us better at https://californiahistoricalradio.com/ .

The Bay Area Radio Hall of Fame brings to life the history of Bay Area broadcasting and the sound of broadcasters from the 1920s to now. Two local historians are major contributors. David Jackson created the Hall of Fame and maintains the Bay Area Radio Web. His passion for Bay Area Radio has kept the Hall of Fame afloat with web news and yearly luncheons. John Schneider used the Bay Area Radio History archives and wrote the book for the Hall of Fame, now at the CHRS book store. John also has colorized the images of dozens of local broadcast facilities. It's a very popular brand of CHRS, find out why at https://bayarearadio.org/ .

The Society of Wireless Pioneers archive is our latest "Brand." It is a continuation of a West Coast organization of wireless operators who used primitive radio devices to send coded messages in the era of crude spark transmitters, crystal receivers and earphones. In our SOWP archives you'll read first hand accounts of sinking ships featuring the radio operator who sends an SOS message that brings help from a nearby ship thus saving lives. Our Society of Wireless Pioneers archives tells the story of the lives of the many West Coast wireless operators. Chief Archivist Bart Lee and fellow archivist Bob Rydzewski, who is the most recent recipient of the Doc Harrold Award, have organized the SOWP archives and made them accessible on the Web. Using SOWP materials Bart and Bob have written articles for national scholarly-technical journals. It's fascinating reading, see for yourself at https://www.sowp.org/ .

We have events to engage the membership and public, and to strengthen our brand. In July of every year CHRS presents "Radio Day By the Bay" featuring a recreation of a live radio play and live 40's era music, and a radio auction. There are also quarterly swap meets.

There is lots going on. Every Saturday, volunteers engage in repairs, audio transcription, exhibit design and preparation, and collaboration. Fall, once the building restoration is finally complete, we will again offer radio repair, restoration, and history classes to members. We are just beginning to plan the first part of our Century of Radio exhibit, the wireless years. And finally, you are reading this because of Richard Watts, long time editor of this Journal. **It's all good!** ◊

CHRS Central Valley Chapter News

by Eddie Steeves

The Central Valley Chapter had a wonderful Holiday Luncheon at a local restaurant, Bella Italia. In January, we again had a booth at the Model A swap meet at the Turlock fairgrounds. The interest in our vintage radio restorer work was amazing. We had the opportunity to share in our passion to keep this wonderful aspect of our past alive and well. We were able to showcase our work with radios that our club members had restored during our Wednesday night weekly workshops.

Officer elections were held in December. Eddie Steve is our new Chairman, John Wallin continues as Vice Chairman, and our new Treasurer is Mark Borgatta.

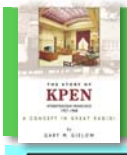
For an update on all our activities, visit CVC at www.cvantiqueradio.com .

CVC booth at the annual Model A swap meet.

CVC Holiday Luncheon in December.

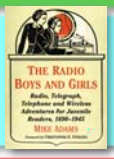
◊

CHRS Publications



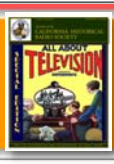
The Story of KPEN: A Concept in Great Radio! Gary Gielow has written a book chronicling the tales of two young men from Stanford, he and James Gabbert, who brought Stereo and new ideas to the FM radio band in the late 1950s and 1960s. This book is the definitive history of KPEN 101.3 FM, the 2015 BARHOF Legendary Station. 100% of the proceeds benefit CHRS. Available in the Museum Store or on the website.

The Radio Boys And Girls—Radio, Telegraph, Telephone and Wireless Adventures for Juvenile Readers 1890-1945 covers more than 50 volumes of wireless and radio themed fiction, offering a unique perspective on the world presented to young readers of the day. The values, attitudes, culture and technology of a century ago are discussed. Available at Amazon.com



Behind the Front Panel: The Design and Development of 1920's Radio by David Rutland has been remastered by Richard Watts for CHRS. With emphasis on radio technology, Rutland describes the development of 1920s tubes and radio circuitry designs by De Forest, Marconi, and other inventors and manufacturers. A classic! Buy at Amazon.com

CHRS Journal Special Edition — Television a compilation of original articles on television, including articles by Malcolm Baird on his famous father, British television pioneer-inventor, John Logie Baird, Don Godfrey's historical bios on CF Jenkins and Philo Farnsworth, plus restoration and technical articles from CHRS members. Available at Amazon.com



◊

The Wireless Boys of Alameda:

Part 3 - The Adventures of George Hubbard

By Robert Rydzewski, KJ6SBR

Sometimes history happens in our own backyards and seemingly ordinary neighbors do extraordinary things. Previous stories told of Alameda amateur radio operator Fred Mudgett and the San Francisco earthquake, and of Henry Heim Jr. and Albert Wolff Jr. and the 1912 U.S. radio law. The third and final part of this series tells the story of Alameda's George Hubbard, a man who failed 8th grade but became one of America's first government-licensed radiomen and went on to troubleshoot the cyclotron. As radio operator, George saved the lives of 300 people with his SOS, but later mostly remembered for the humorous side of it. Disillusioned with work as a sound man for Hollywood movies, he went on to install radio equipment for U.S. Navy, dodging Japanese bullets and worse at Pearl Harbor. Finally, this wireless pioneer spent his twilight years as a founding member of the Society of Wireless Pioneers and a volunteer for Santa Cruz charities. His life, which spanned nearly a century, was one "writ large," with radio electronics at the heart of it. Here is his story.

Getting His Feet Wet

George Shipton Hubbard, the oldest son of Frank and Susie Shipton Hubbard, was born in Springfield, Massachusetts in 1890[1]. His maritime adventures began at an early age and in an inauspicious way. When he was in grammar school he and his family were living in Milwaukee, Wisconsin. His academic performance there was less than stellar: rather than go on to high school he found out he'd need to repeat eight grade. "I knew it was my own fault," he said decades later, "My mind had been occupied with my love [a girl named Ethel] instead of my studies."[2] Afraid to tell his parents of his failure and despairing over his imminent separation from Ethel, who'd be moving on to high school, George took a streetcar to the Milwaukee waterfront. An impressively large steamer was just coming in. It was the *Christopher Columbus*, a type of vessel now nearly extinct, a whaleback ship that plied the waters between Milwaukee and Chicago, carrying as many as 5,000 passengers (Figure 1). Overhearing a steward firing a boy who'd worked in the galley pantry, George saw his opportunity. He went up to the steward and offered himself for the job, lying about his age and previous experience. Hired on, he befriended the chief cook, a Black man named Mr. Brown, and spent about 5 months happily helping with the crew's mess, including the sailors' favorite, creamed chipped beef on toast, known by another name. The downside to working on Great Lakes vessels came in the winter, though, when ice caused the trips to stop and the crews to be let go.

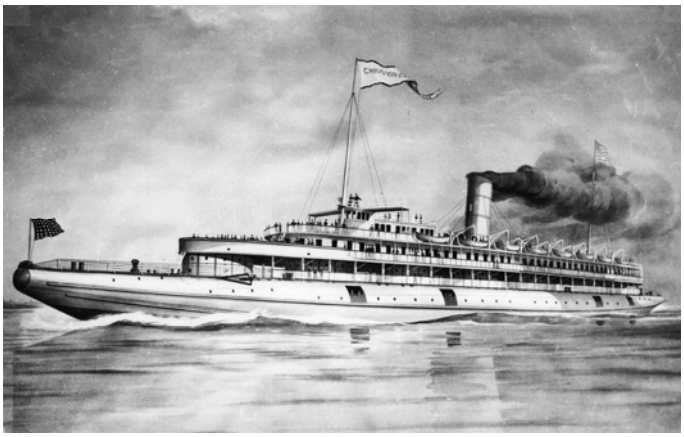


Fig. 1: The whaleback passenger ship *Christopher Columbus* on which the runaway George Hubbard got his first maritime experience. These ships were sometimes called "pig boats" for their snout-like bows. Painting by Howard Sprague. (Source: Wikipedia)

One day, standing on Chicago's Rush Street bridge and trying to decide whether to head out to the Atlantic for more shipboard work, George saw a familiar face: "Could I believe my eyes? There, standing before me, open-eyed and outraged, was my father! He just stood and looked at me for a long interval. He seemed torn between whether to embrace me or beat me. Tears were rolling down his face and he said not a word but took me firmly by the collar." George, whom they'd given up for dead, was reunited with his family and was soon forced to take his first bath since leaving home.

By 1910 the Hubbard clan had settled at 1112 College Avenue in Alameda.[3] George was interested in electricity and took a job with the Southern Pacific train service maintenance department, anticipating a chance to work with electrical equipment. Instead, he became an expert in grounds: his only job was to keep digging in them. Hoping for better things, he took classes at San Francisco's Wilmerding Technical High School and he spent his spare hours studying wireless theory and Morse code. One fateful day in 1910 he went to the United Wireless Telegraph office on Market Street to

apply for a job as a ship radio operator. The chief there, Lawrence Malarin, sent him to the Chronicle building for a code test, which he passed. Soon he was working aboard a small schooner, the *Falcon*. "On her 6 months and seasick the whole time," he later recalled.[4] "Did I meet Mal de Mer!" Relief came in an unexpected way. An Australian steward kept coming by to torment him with food and try to get him up. Finally pushed beyond his limits, George sprang from his bunk, went after his tormenter, and chased him around the deck, much to the delight of the crew. By the time the steward had escaped, George stopped to catch his breath and realized he was... cured! So his maritime radio career continued, and on June 20, 1911 George joined the exclusive ranks of those who had achieved a U.S. government "Certificate of Skill" (COS) in wireless, the precursor to the later commercial radiotelegraph license or "ticket." His COS was among the first ten ever issued.[5] His younger brother Irvin would also hear the call of dots and dashes at sea, earning his ticket and becoming a ship radio operator or "Sparks" a few years later.[6]

George's next assignment, aboard the oil tanker *J.A. Chanslor*, was quite an upgrade, with a roomier wireless cabin and a less vomit provoking ride. His first trip aboard it was between California and Treadwell gold mine at Douglas Island, Alaska. Figure 2 shows the site a few years later, with engineer Arthur Isbell marking off the location of commercial wireless station KDU that he was installing there for American Marconi.

Fig. 2: Hand-colored postcard of the Treadwell gold mine, Douglas Island, Alaska, marked up by wireless engineer Arthur Isbell, and dated June 13, 1914. (Society of Wireless Pioneers Archives)

During his time on the *Chanslor*, George's reputation as a formidable radio operator grew, largely because he believed in BYOD, that is, Bring Your Own Detector (an electrolytic one in this case). In those early radio days patents on basic equipment were in force and licensing was minimal, so professionals like George were technically forbidden to use devices that their employers didn't have legal rights to. Given the choice between following the law and getting poor reception or breaking it and pulling in stations. George, like many, "out at sea, away from prying eyes" chose the latter.[7] Listening at night he often heard other ships trying, but unable to contact commercial station PH in San Francisco. George's pet detector and the ship's powerful transmitter allowed him to relay the messages, which didn't go unnoticed. He soon received an even better, if more fateful assignment.

One Asia on the Rocks

In 1911 he was assigned to the Pacific Coast Mail steamer *Asia.* This was an iron-hulled vessel built in the 1880s that originally was fully rigged for sail. The rigging made it top-heavy, causing it to sway a lot in heavy seas. A triple expansion steam engine was later installed, and most of the rigging (but not the masts) was removed. That helped, but the ship still rolled more than was comfortable. Because of that it was considered a "second class" passenger vessel, a favorite of travelers to "the Orient" looking to economize. The *Asia* also carried mail and some cargo.[8]

The ship flew the British flag and was staffed with British officers. Years later George recalled that they seemed fairly resentful of his presence, referring to him dismissively as "the wireless boy." In those pre-Titanic days, ship wireless operators—typically teenagers who were technically "officers" but had little or no seagoing experience, couldn't command anyone, and were paid no more than an ordinary seaman—were often treated with disrespect. Hubbard was one of only 3 Americans onboard (the crew being mostly Indian, Chinese, and Filipino), and that wouldn't have helped. The only one who showed him any respect was a Chinese cabin boy who called him "Topside Talkee Man."

The *Asia*'s wireless set was a typical United Wireless spark installation of those days, which is to say "as primitive as can be." George described the emergency transmitter for us: "Fifty-five glass storage batteries in series produced 110-volt current which fed a motor-generator which converted 110 DC to 110 AC. This was keyed to the primary of a step-up transformer, 110 to 12,000 volts which charged a rack of Leyden jars, which in turn discharged into a tuned oscillating circuit that was made resonant to the antenna by an auto transformer arrangement."[9] Its output was 1 kW. There was also a similar but "more ponderous" 5 kW transmitter powered by the ship's main generator (Figure 3). The station's callsign was WWT.

Hubbard's first round trip aboard the *Asia* was uneventful, but his second, from San Francisco to China and back, was something he'd remember for the rest of his life. A couple of celebrity passengers, balloonist Thomas Scott Baldwin[10] and "The Curtis Daredevil" J.C. "Bud" Mars[11], befriended him and hung around the wireless shack on the trip west, but much more memorable was what happened on the way back.

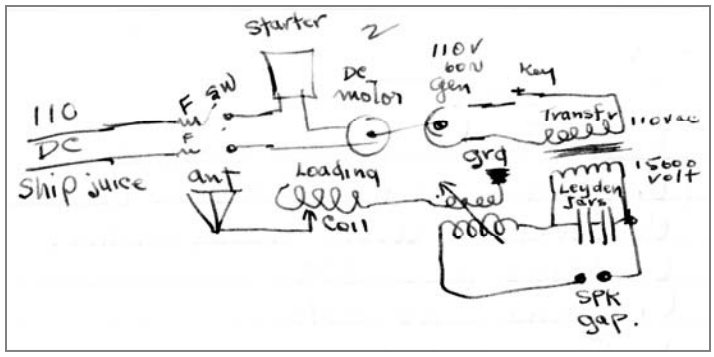


Fig. 3: Schematic of United Wireless transmitter on the *Asia*, hand-drawn in an undated letter from George Hubbard to Ed Marriner.
(Society of Wireless Pioneers Archives)

On the night of April 23, 1911, as the *Asia* was returning to San Francisco and just a day's voyage out from Hong Kong, a heavy fog settled over the sea, limiting visibility to a few hundred yards.[12] George was in his bunk trying, without much luck, to sleep despite the constant bellowing of the ship's foghorn. The only person on the bridge was a newly minted fourth officer, a Mr. Johnson, this being the first time he'd ever had that responsibility. He got worried when he didn't sight the lights that should have been visible, and called Captain Gaukroger with a request that he come to the bridge. His request was denied. He then asked for permission to reduce speed. Also denied. Finally, Johnson called the first mate. As soon as he got there the fog lifted to reveal towering rocks dead ahead. Putting the engines full astern wasn't enough. Horrified, the best they could do was to steer the *Asia* into a cleft between two of the rocks, jamming enough of the ship onto the shore to keep it from sinking (Figure 4). Before it struck, the first mate rushed out of the bridge and rousted out the steerage passengers, likely saving their lives.

Back in the radio room, "I was just rolling out of my bunk when she struck," recalled George. "The sensation was almost indescribable. She bumped up and down mightily, then heeled 45 degrees to port where she finally set in." The crash had torn the iron bottom of the ship apart. One quarter of the vessel was now ashore and the rest in deep water. When enough water had flooded in, the ship would slide off and go down by the stern. Experienced sailors guessed that this would happen in a few hours. Now was the time for Radio Officer Hubbard to act.

He needed to find the captain and get the ship's position and an order to send out the SOS. But first he had to answer a question that wasn't in the wireless manual: Should he have his pants on while doing so? Dressed only in his underwear, but pants in hand, he found Captain Gaukroger, also sans trousers, "busily banging away at a large Chinese junk, several hundred feet away, with an out -sized pistol." They were thought to be "river pirates" swooping in for plunder (Figure 5). "Shall I send out a distress signal?", George asked the captain. Yes, he was told. He started to return to the shack but remembered that he needed the ship's position. He turned and asked the captain "Where are we?"

Fig. 4: The *S.S. Asia* run aground on Finger Rock, south of Formosa (Taiwan) on April 23, 1911. Photographer unknown.
(Society of Wireless Pioneers)

"That does not concern you—" Gaukroger started to say before realizing that an SOS would be useless without it. "We have hit 'Finger Rock' on Heachu Island at the south end of Formosa," George was informed. There was just one problem. "The skipper was English. I didn't know if he was dropping an 'H' or adding one," he recalled.[13] So he asked him to spell it, which the captain did after a remark about ignorant Americans not knowing how to spell.

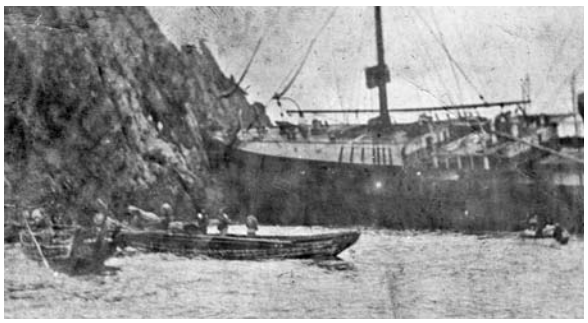


Fig. 5: Chinese boats, believed to be pirates, approached the stranded *Asia* and were fired upon. Photographer unknown.
(Society of Wireless Pioneers)

As he rushed back into the wireless shack the barefoot George had to wade through some puddles on the floor. A minute later a strange tingling under his toenails told him what that liquid was. Like the mythical kid in the high school chemistry poem, he found that "what he thought was H_20 was H_2SO_4."[14] The ship's list had caused containers of extra battery acid to spill out. He made for

some nearby fire buckets and doused his burning feet, then tried to start up the main wireless transmitter. No luck. The engine room that powered it was out of commission. Next, to the battery-powered emergency transmitter, which spun into action. George tapped out the SOS, sparks flew, and he was happy to get replies back almost immediately. Three ships were on their way.

When the mate found that George knew how to handle boats from his Alameda days, he was put in charge of one of the lifeboats. Some were already underway filled with passengers "shouting, screaming, and crying." "Drama unfolds rapidly when one is an occupant of a lifeboat... you learn more about human nature in fifteen minutes than in the ordinary course of a lifetime," he later reflected. "I found myself at the tiller of a 28-foot steel lifeboat, filled to the gunnels with mail sacks, provided with a crew of Chinese waiters and mess boys, none of whom had ever handled an oar, I suspect," he said. The inexperienced oarsmen were having a hard time with the heavy 10-foot oars. Also aboard were some passengers, mostly missionaries.

They needed to get farther away if they were to be rescued by a Chinese mailboat that soon made its appearance, but were now drifting into dangerous water where the swell could dash their boat against the rocks. Two of the panicked passengers started shouting directions, confusing the Chinese oarsmen, but George, threatening to throw them overboard, put down the mutiny and took charge. He knew he was responsible for all of their lives, but "most importantly, I didn't want to die." To the horror of his passengers, he ordered the Chinese crewmen to toss all the mail sacks overboard, lightening the load. They then made slow progress, but the oarsmen were soon exhausted. The prospects got bleaker: one of the "river pirate" boats that had tried to get to the *Asia* earlier was now approaching the lifeboat. What fate awaited them? Kidnapping? Or worse?

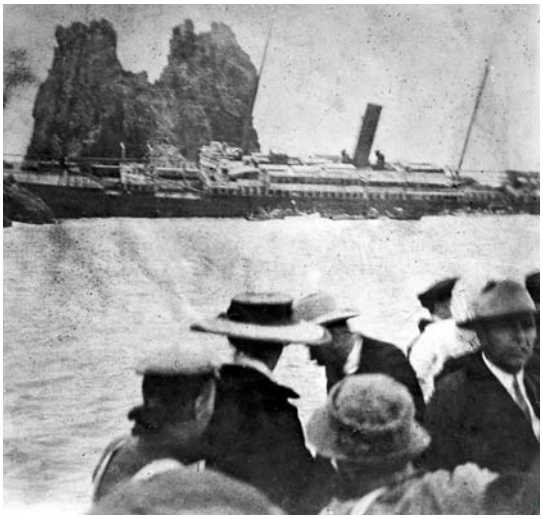


Fig. 6: Evacuated passengers gazing back at the *Asia* from a distance. Photographer unknown. (Society of Wireless Pioneers)

Remembering Captain Gaukroger's potshots, the "river pirates" circled carefully at a distance and began talking with a Chinese oarsman. They turned out to be just fishermen. River pirates were real enough in China at the time,[15] but these weren't them. The fisherman wanted to make them a deal: a tow for whiskey. The lifeboat didn't have any whiskey but came equipped with food. Soon the provisions were on the sampan and the lifeboat was towed out toward the rescue vessel. The fishermen left them with much waving and friendly grins. "If those chaps were pirates," said George, "they were the nicest ones I have ever heard about." Once the passengers and crew had left the *Asia*, though, those aboard some of the Chinese boats took the once-in-a-lifetime opportunity to strip the foundering vessel of its cargo and all the brass fixtures they could carry off (Figure 6). At least one account has the Chinese ship *Shaoh Sing*, one of the rescue ships, firing on them with some resulting carnage.

ALAMEDA MAN HERO
HUBBARD SAVES SHIP

GEORGE HUBBARD, wireless operator on the Pacific Mail liner Asia which was sunk Sunday off the coast of China.

Fig. 7: Bay Area newspapers hailed radioman George Hubbard as a hero for his part in the *Asia* rescue. Oakland Tribune, April 25, 1911.

A bit more drama followed. Some of the *Asia*'s crew (but not George, so far as we know) were caught trying to smuggle in silk when they later arrived in Honolulu.[16] They'd probably helped themselves to the cargo on the sinking ship, rationalized that it was better left with them than the pirates. A board of inquiry later faulted Captain Gaukroger for sailing too close to shore and not keeping a proper watch. He was demoted to deckhand.[17] Gaukroger, in his accounts, not once mentioned George, wireless, or the SOS.[18] The tale was quickly forgotten as a more prestigious ship, the *Titanic,* made its last fateful—and fatal—voyage a year later. Today the only accounts of the *Asia* come from newspapers in California and Hawaii, and records from the Society of Wireless Pioneers, an organization George would help found more than half a century later.

After the rescue he was taken to Shanghai and feted, then returned to Alameda to enjoy a hero's welcome (Figure 7), with a story he could—and did—tell (with several variations and enhancements) for the rest of his life. But this wasn't the last of his adventures.

Moving on Up

He continued his career as shipboard wireless operator for several years after the *Asia* incident, working for American Marconi after it snatched up the remains of the failed United Wireless. Wireless operators like George gained quite a bit of prestige as news of the *Titanic* and the heroism of its Marconi operators, Jack Phillips and Harold Bride, seized the public's imagination. Under those circumstances, what red-blooded American "Sparks" *wouldn't* take every opportunity to reassure attractive young female passengers that they were in good hands (Figure 8)? Certainly not George Hubbard, whose devotion to the opposite sex far outlived his grammar school obsession with Ethel.

On one of his journeys aboard the *S.S. Beaver* in 1912 he met a showgirl, Bertha Jarvis, "a beauty of the blond type and most charming" (Figure 9).[19] Not three hours after he first met her George proposed. They were married the next day. The couple briefly made their home next door to George's parents in Alameda, but within a year a live-in mother-in-law came between them, and they were divorced. "I hate you and I do not expect that you will live very long," she is alleged to have told him.[20] About the latter she couldn't have been more wrong.

Fig. 8: The position of ship wireless operator came with some fringe benefits. Cartoon from *Wireless Age*, August 1916, page 792.

Fig. 9: George Hubbard and his first wife, Bertha Jarvis (left) aboard the *S.S. Beaver,* August, 1912. (Society of Wireless Pioneers)

In all the rest of his many days George would never send out another SOS as he had aboard the *Asia.* One time, though, it was only because he couldn't. Aboard the *Beaver* crossing the Columbia River bar on December 23, 1913, "suddenly, for no explainable reason, a feeling of Terror possessed me. Without any preliminary thought, I sprang from my chair and raced out of the door onto the after deck where I saw an unbelievably great wave a half a mile astern. It looked 75 ft. high, and it was bearing down upon us!"[21] With the roar of the oncoming tidal wave behind him he scrambled up a mast in record time and hung on to watch from on high as it hit. Much of the deck below, including the wooden superstructure that was his radio shack, was torn off and washed over the side. The ship rolled sickeningly to starboard, suspending George above the boiling sea, but soon righted itself as the wave went on to wreak havoc in Astoria, Oregon.

But this cloud (actually this wave) had a silver lining. George rebuilt the wireless station with the help of a notable Portland amateur, Charles Austin,[22] replacing the smashed Leyden jars (capacitors) with window glass and tinfoil ones and making the tuning coil out of bent copper pipe. The new station worked fine on 300 and 600 meters (1000 and 500 kHz, respectively), the wavelengths ships used in those days. The experience eventually helped him "swallow the anchor" and go on to a series of land-based jobs installing radio equipment on ships and at coastal stations for American Marconi, RCA, Federal Telephone, and the U.S. Navy.[23] The shipboard installations required him to climb up the masts to string the antennas, dirty, dangerous work that left him covered with soot from the ship's smokestack. Another job was cleaner but cold: he spent 8 years installing radio equipment in frozen Alaska.

For a while he quit the radio business, in 1928 going into the brand-new, high-tech motion picture sound industry in Hollywood and was able to rent an apartment in Beverly Hills. Among the pictures he worked on was Howard Hughes' "Hell's Angels," "The Taming of the Shrew" (with Mary Pickford), and "The Lottery Bride" (with Santa Cruzan ZaSu Pitts). But the Great Depression of 1929 cost him—and millions of others—his job.[24] On the bright side, George hadn't been fond of Tinseltown life anyway; he'd found working in the movies a cut-throat business.

So he took what he could get, a temporary job with Mackay painting a 300 ft. radio tower in Bellflower, CA. Once again disaster came knocking when an earthquake struck while he was near the top, almost shaking him off.[25] He'd already survived a shipwreck, a tidal wave, and an earthquake. There would be more to come, including a car accident in Los Angeles that took the life of his teenage son but spared his own.[26] What other disasters could still be in store?

Bullets, Bordellos, and Sewers: Pearl Harbor

After working as a civilian contractor for the Navy at Mare Island, George was sent to Pearl Harbor in the 1930s as a senior radio engineer. "It had long been an open secret," he recalled, "that the Army had arranged for the transportation of many young women of easy virtue to Hawaii, 'for the good of the service.'"[27] George, who at this point was living with his wife and small children in a respectable Honolulu neighborhood, was asked by officials if he would object to some of these ladies moving to the house next door where they might perform their "social chores". He did and so they didn't.

George was at home on Sunday, December 7, 1941 and was ordered to report to his station at the Navy Yard as Japanese planes buzzed overhead. "It was a harrowing experience," he later remembered. To get there "it was necessary to drive very slowly through bumper-to-bumper traffic... As we crawled along, the Japanese planes dived down upon us constantly. None of us were brave and daring - all of us were frightened stiff! Don't ever let anyone tell you he can remain calm under these conditions."

Stuck in his car in stopped traffic he was a sitting duck. Next to the road he saw a pile of steel pipes where a new sewer line was being put in. "I dove into one of the big pipes. Soon I heard the familiar rat-tat-tat of machine gun bullets striking the pipe. I crawled ahead, seeking daylight. Then the noise increased." To his surprise and disgust, "it was not machine-gun fire. I had run into a nest of rats." Backing out as fast as he could, George chose Japanese bullets over an army of rodents.[28]

"There was nothing a radio man at Pearl Harbor could do while the attack was in progress," he observed. With a Japanese invasion of the island a real possibility, "I took it upon myself to assemble all of the emergency gear and remove it to a place of safety. I took it into the hills near Wahiawa 25 miles away, where I found a suitable hiding place."[29]

Two days later at the Naval Hospital he saw row after row of wounded and dying servicemen and civilians lined up side-by-side. And here he learned a lesson about humanity. Tending to the wounded was someone he thought he had seen once before, one of the ladies that the Army had tried to make his neighbor. "Are you Nancy?" he asked. "Yes I am. Who are you?" she answered. "I might at one time have been your neighbor," George said, "but it was me who objected to your presence in our neighborhoods." Whatever he and society thought of her profession, "she nevertheless retained her God-given love and pity... for the wounded she was called upon to serve." A strange feeling of guilt engulfed him.

The Gadgeteer

Never one to worry too much about rules, George left Hawaii for the mainland the following year without getting the required permission of the military governor. He bought 28 acres in Lake County, California, built some large henhouses and raised hens, then sold the operation at a profit the following year. "No sooner had I sold the chicken ranch," he recalled, "than I was called upon by a pair of well-dressed strangers in their middle thirties."[30] They inquired about his future plans. Wondering what it was all about, he answered that he was thinking of going back to the Mare Island Navy Yard. The F.B.I. agents (which is what they turned out to be) suggested that he might instead be interested in something they called "The Thing" at the University of California at Berkeley.[31]

He was invited to meet with Dr. Ernest O. Lawrence there. Perhaps surprisingly, he and Lawrence hit it off almost from the start and he was hired on the spot. "The Thing" turned out to be the Berkeley 184-inch cyclotron (Figure 10 and Figure 11), a key part of the ongoing Manhattan Project that would soon produce the first atomic bomb. Like almost everyone else there, of course, he had no idea what the project was really all about.

Here he earned himself another nickname. In Hawaii, he was sometimes referred to as "Pop." But in Berkeley his talent for improvising equipment earned him the sobriquet of "the Gadgeteer" from Dr. Lawrence himself. Though no expert on particle physics, George was the quintessential field engineer: he knew wiring and heavy equipment installation, was good at troubleshooting and could stick to deadlines. At one point no one could figure out why the 37-inch cyclotron near Sather Tower seemed to "go haywire" every day around 4 PM. George noticed that this was also the time at which

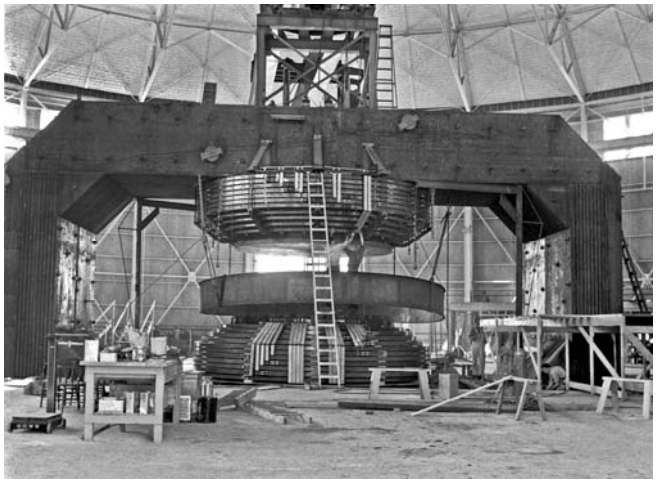


Fig. 10: Berkeley 184-inch cyclotron in 1942.
(Lawrence Berkeley National Laboratory)

Fig. 11: Berkeley Advanced Light Source Booster Synchrotron in 2015. The inverted U-shaped magnet structure from the 1940s (in grey) was too large to remove and remains there today.
(Collection of John Staples)

many trucks rumbled by. He traced the problem to coils that had been wound on coil forms that weren't sturdy enough. Vibrations caused the distances between turns to vary a little, changing the inductance values just enough the throw things off. The problem was soon fixed.[32]

After a while, though, George increasingly felt that the place was overrun with scientists, engineers, technicians, and helpers "milling around in endless circles" not knowing what to do and lacking any clear instructions. Perhaps, he surmised, this was just the way these "braintrusters" were supposed to operate? But it wasn't the way he liked to work. So one day he went to Dr. Lawrence to tender his resignation. Instead of accepting it, Lawrence, he relates, put him in charge of correcting the situation, making him something of an efficiency expert. "I had to step on many toes," he noted. "I made more enemies in one week than in my entire earlier life." He was later awarded a certificate of commendation for the part he played in the development of the atomic bomb. Personally, he considered his role "insignificant," but like many he had mixed feelings about it as the years went by.[33]

The Last QSL

He later worked at Mare Island again, then went back to Hawaii for a job with the Civil Aeronautics Administration in Honolulu. Here he was given a full office job, completely detached from any hands-on electronics. He was put in charge of planning. It wasn't for him; he returned to California and spent his last 4 decades there, most of it in retirement, much of it on a 46-foot power cruiser and an island in the Sacramento River. In 1968 he became a charter member of the Society of Wireless Pioneers. In his later years he and his 5th and last wife Bea spent time giving back to the community as volunteers for the local Meals on Wheels and Live Oak Senior Center in Santa Cruz (Figure 12).

Fig. 12: George and Bea Hubbard as volunteers for Meals on Wheels of Santa Cruz, probably from the late 1970s.
(Society of Wireless Pioneer Archives)

On his 75th birthday he received a card from the *S.S. Asia*'s ship doctor. He and George were the last known survivors of the shipwreck.[34] At the age of 91, living at the Casa Del Rey Hotel across from the Santa Cruz Boardwalk, he tapped out his final code message, sending Christmas greetings to fellow old-timer Robert Estes.[35] Finally, in 1985 George Hubbard took his final voyage, departing landlocked Ben Lomond and this world for parts unknown.

Conclusion

The lives and fortunes of Alamedans Fred Mudgett, Henry Heim Jr., Albert Wolff Jr., George Hubbard and others were completely intertwined with the developing field of wireless as it gave birth to modern electronics. From learning, implementing, and expanding the then-mysterious new technology to exposing the folly of unregulated, free-for-all communications to saving lives at sea and ashore, what these largely forgotten local boys did more than a century ago helped shape modern communications and the world we live in today.[36]

Acknowledgements

Special thanks go out to George's grandson Gary Hubbard without whose guidance and help many parts of this account would be incomplete or outright wrong. We hope to see his grandfather's informative and entertaining autobiography, which he generously shared, in print soon. Thanks are also due to John Staples (CHRS) and Marcy Dunning (Columbia River Maritime Museum). Finally, without Bart Lee and others at CHRS who were responsible for preserving the Society of Wireless Pioneers archives, this story would not have been possible.

References

1. 1892 Washington State Census, Pierce County, p, 198; World War I registration card, Alameda, CA, June 5, 1917; both available from ancestry.com.
2. Much of this information comes from George Hubbard's unpublished autobiography as graciously supplied by his grandson, Gary Hubbard.
3. 1910 U.S. Census, Alameda, CA; available from ancestry.com.
4. Society of Wireless Pioneers membership application for George S. Hubbard. Available at https://www.sowp.org/wp-content/uploads/2019/01/LR-2801101903-George-Hubbard-MA.pdf.
5. Society of Wireless Pioneers 1972 Directory and Newsletter, p. 10. Available at http://www.sowp.org/wp-content/uploads/2018/06/LR-0005301801-SoWP-Directory-Newsletter.pdf.
6. W. Esterline, "Wireless Operator Recalls Days of Pancho Villa," Blade-Tribune (Oceanside, CA), November 16, 1969. Unlike George's career, Irvin's shipboard career was fairly short, which he blamed on 3 things: seasickness, poor pay, and dangerous cargo (transporting explosives).
7. Hubbard autobiography, p. 31.
8. R. Weinberg, "Asia Disaster is Funny Now to Heroic Radio Operator," Honolulu Star Bulletin April 23, 1940.
9. Hubbard autobiography, p. 32.
10. See https://nationalaviation.org/enshrinee/thomas-scott-baldwin/.
11. See https://en.wikipedia.org/wiki/James_C._Mars.
12. As with any catastrophe, accounts of exactly what happened vary, even when told by the same person at different times. Here we've tried to go with the consensus, which could still be wrong on some details.
13. Weinberg, "Asia Disaster is Funny Now..." op cit.
14. "Johnny drank some water/ water he'll drink no more/ For what he thought was H2O/ was H2SO4." - Rev. Paul Balcer, C.R.
15. Frank C. Brown, "Degeneration of Chinese Pirates," Pacific Marine Review, February 1927, Vol 24, p. 78.
16. "Mongolia Yielded Many Scattering Tins of Dope," Honolulu Evening Bulletin, May 20, 1911.
17. "Once Skipper of P. M. Vessel, Now Deckhand," Honolulu Star Bulletin, August 16, 1912.
18. "Steamer Asia on the Rocks," Honolulu Evening Bulletin May 20, 1911.
19. "Reception Given for Bride and Groom," Alameda Daily Argus, August 23, 1912.
20. "Hogarty's Trials Were Numerous, He Relates," San Francisco Call, April 13, 1913.
21. Hubbard autobiography, p. 53.
22. Austin went on to be Portland's first radio broadcaster. See https://www.sowp.org/charles-l-austin-portlands-first-broadcaster/.
23. Letter from George Hubbard to Ed Marriner dated November 16, 1960. Available at: http://www.sowp.org/wp-content/uploads/2018/07/LR-2307041802-Hubbard-111660-Letter.pdf.
24. Society of Wireless Pioneers membership application for George S. Hubbard, op cit.
25. This was probably a 6.0 earthquake in the Gulf of California on September 27, 1929. See https://en.wikipedia.org/wiki/List_of_earthquakes_in_1929.
26. "Driver Dies When Truck Overturns," Los Angeles Times January 3, 1930.
27. Henry Dickow, "The Hubbard Brothers," p. 4 (Society of Wireless Pioneers archives).
28. In another version of the story, though (George's autobiography), he didn't dive into metal pipes while stuck in traffic but instead dove into concrete sewer pipes later at Pearl Harbor as he tried to reach the emergency radio transmitters.
29. Dickow, "The Hubbard Brothers," ibid. p. 4.
30. George Hubbard SOWP membership application op cit.
31. Dickow, "The Hubbard Brothers" op cit. p. 6.
32. Hubbard autobiography op cit. p. 134.
33. Dickow, "The Hubbard Brothers" op cit. p. 7.
34. "Meet the People," San Francisco Chronicle February 18, 1965.
35. Mark Bergstrom, "Dots and Dashes Spell Out Have a 'Merry Christmas'," Santa Cruz Sentinel December 24, 1981.
36. George Shipton Hubbard family tree, available at https://www.ancestry.com/family-tree/person/tree/26203882/person/240034690105/facts.

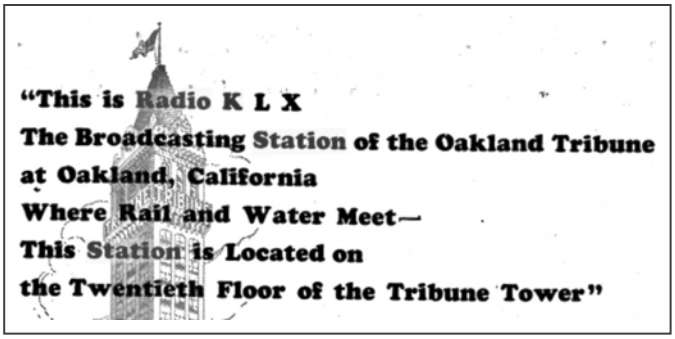
◊

Amateur Night at Radio KLX, Oakland, 1924
— a young man wins the Ears of Oakland

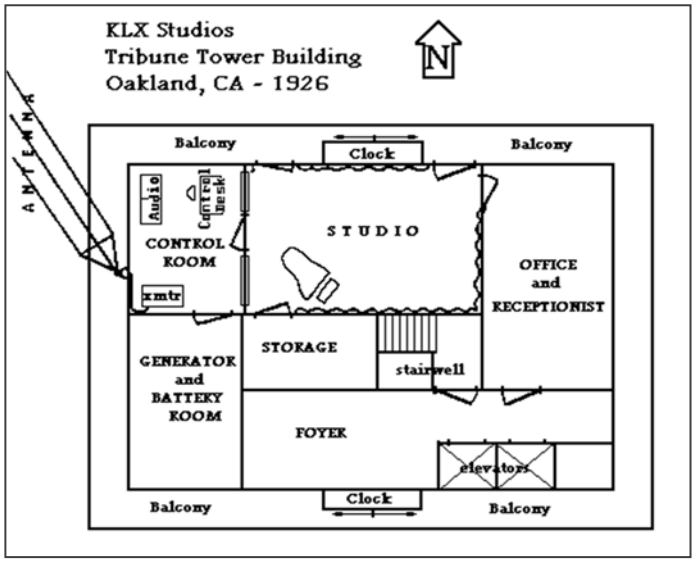
By Bart Lee, K6VK, CHRS Archivist

Oakland radio broadcasting station KLX, in 1924 – the early days of broadcasting – featured an "amateur night" for aspiring musical talent. The *Oakland Tribune* newspaper owned the station.

KLX sited its broadcasting studio pretty much at the top of the building, no doubt for shorter lines to its 500-watt transmitter and antenna. The San Francisco Bay Area enjoyed good reception from KLX, even at its one tenth the power of the local GE "flamethrower" KGO at 50,000 watts. As of 1920, Oakland had a population of 216,000 people. San Francisco was larger, over 500,000. Nearby cities and towns also contributed to the listening audience.



From a flyer with the words KLX used to announce itself. Perham Collections at History San Jose.

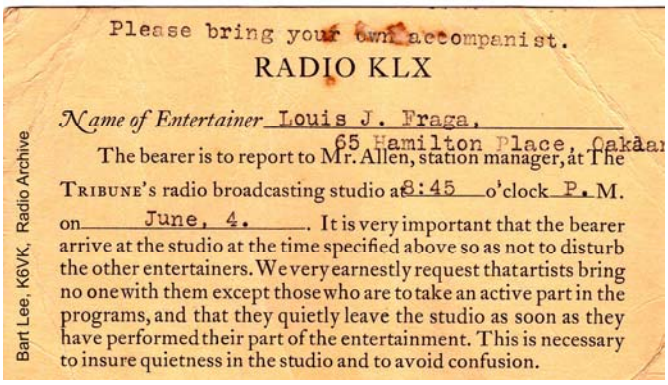


A diagram of the radio operation, studio, transmitter, etc.

KLX invited a young singer, Louis J. Fraga to appear at 8:45 PM, June 4, 1924.

The day after the program featuring Mr. Fraga (number 12 on the show) and others, listeners sent in mailed responses to KLX. These cards are from Mr. Fraga's cache of saved mailed-in responses, etc. as I received them at an ephemera show in San Francisco. (He was born in 1896, his daughter died in 2015).

At the time, manufacturers and dealers of home radios, to promote the new "fad" of radio broadcast reception, encouraged listeners to send "Applause Cards" (as post cards) to stations with favored programs. An example that Crosley made available to its dealers follows; radio stations also encouraged listeners to write in.


Please bring your own accompanist.

RADIO KLX

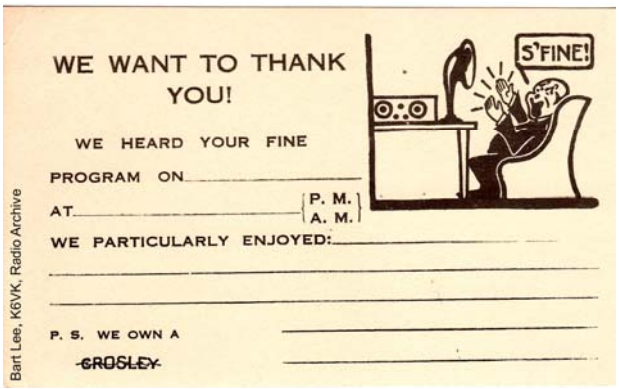
Name of Entertainer Louis J. Fraga,

65 Hamilton Place, Oakla

The bearer is to report to Mr. Allen, station manager, at The TRIBUNE's radio broadcasting studio at 8:45 o'clock P. M. on June, 4. It is very important that the bearer arrive at the studio at the time specified above so as not to disturb the other entertainers. We very earnestly request that artists bring no one with them except those who are to take an active part in the programs, and that they quietly leave the studio as soon as they have performed their part of the entertainment. This is necessary to insure quietness in the studio and to avoid confusion.

Bart Lee, K6VK, Radio Archive

The appointment card for Louis Fraga's performance.

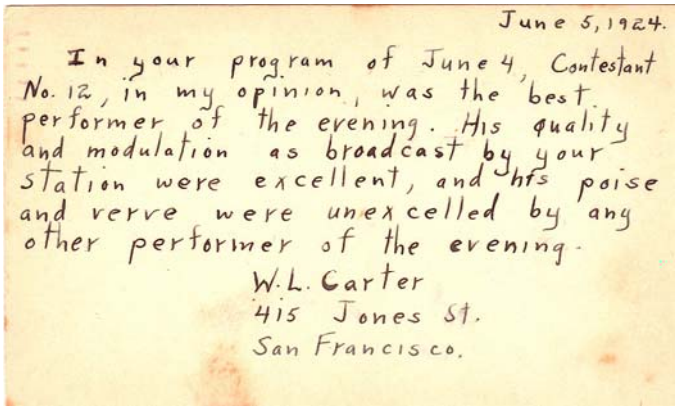


Bart Lee, K6VK, Radio Archive

Listeners could express their enjoyment by sending in an Applause Card.

In favor of Mr. Fraga, listeners sent in about 150 postal responses, being 128 (or so) post cards, and 12 letters, one including six attached voting notes, mostly dated June 5, 1924. While radio dealer "Applause Cards" made up many of the mailings, most listeners responding just sent in "penny" postcards. (That's at least 18 cents in today's money. A letter with a two-cent stamp would cost about 36 cents in today's money to mail, although such a "Forever" stamp today costs about 63 cents. The total 1924 postage was about $27, in today's money: at least $475, and perhaps as much as $800 – paid by the listeners).

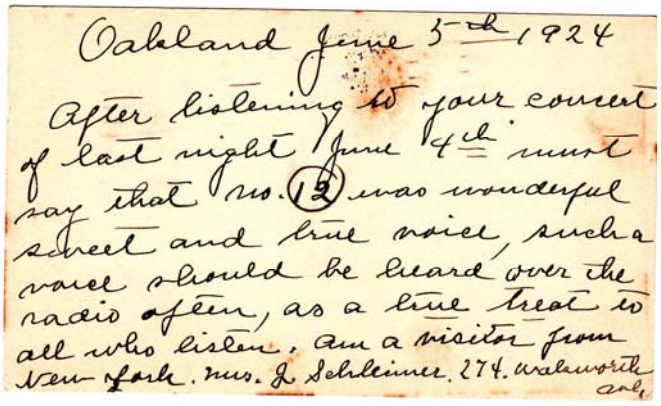
Oakland made up most of the mailings, with San Francisco coming in second. But a few came in from other Bay Area towns, such as Mill Valley. KLX seems to have given the responses to Mr. Fraga, and this archive somehow survived. One can infer that he won the night. The prize seems to have been a five-tube broadcast receiver. (An RCA Radiola XI would have cost something over $200 then, or about $3,500 in today's money).



June 5, 1924.

In your program of June 4, Contestant No. 12, in my opinion, was the best performer of the evening. His quality and modulation as broadcast by your station were excellent, and his poise and verve were unexcelled by any other performer of the evening.

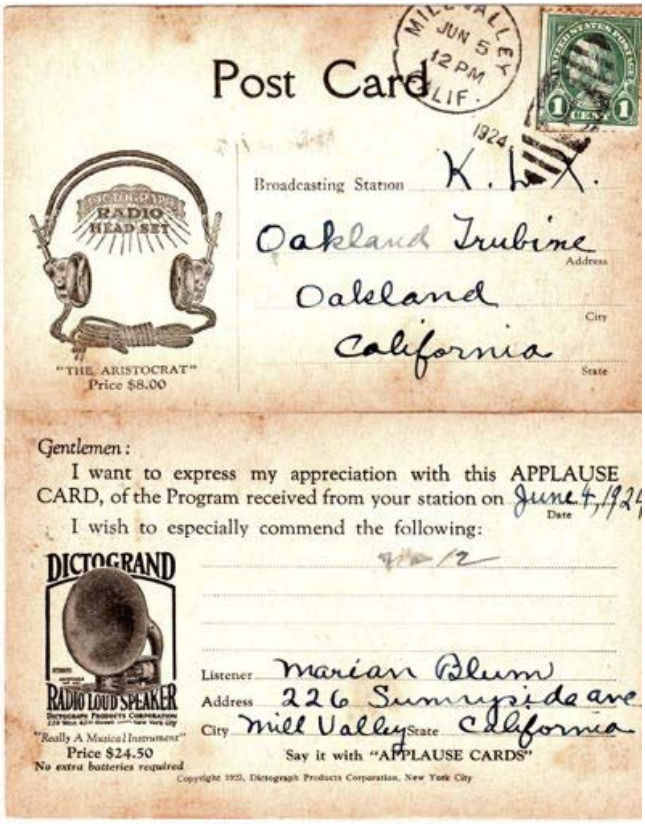
W. L. Carter
415 Jones St.
San Francisco.



Oakland June 5th 1924

After listening to your concert of last night June 4th must say that no. 12 was wonderful street and true voice, such a voice should be heard over the radio often, as a true treat to all who listen. am a visitor from New York. Mrs. L. Schleimer. 274. Walworth ave.

Some responses were telegraphically brief (*e.g.*, "Score one for # 12"), and some were effusive.



Post Card

JUN 5 12 PM 1924 MILL VALLEY CALIF.

"THE ARISTOCRAT" Price $8.00

Broadcasting Station K. L X.

Address Oakland Trubine

City Oakland

State California

Gentlemen:

I want to express my appreciation with this APPLAUSE CARD, of the Program received from your station on June 4, 1924 Date

I wish to especially commend the following:

#12

DICTOGRAND RADIO LOUD SPEAKER

"Really A Musical Instrument" Price $24.50 No extra batteries required

Listener Marian Blum

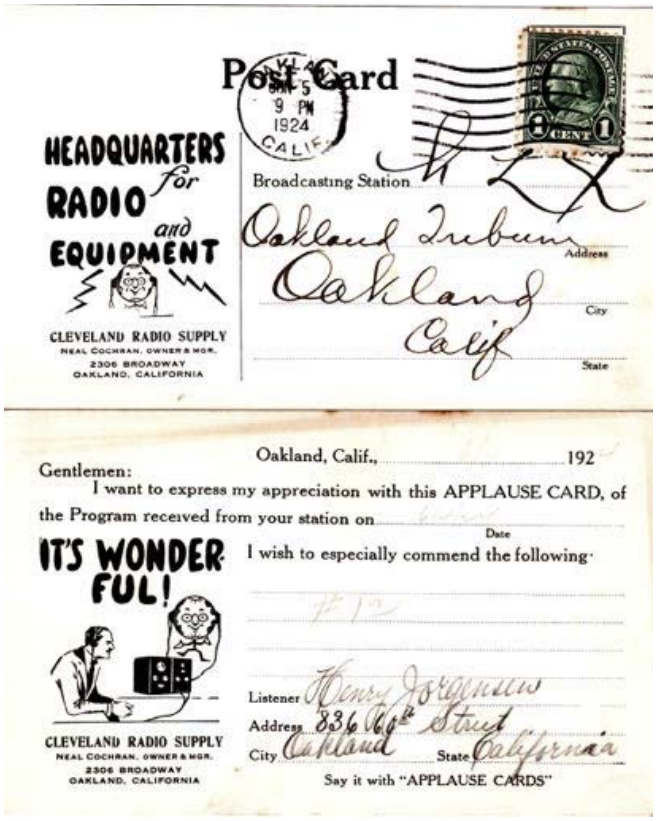
Address 226 Sunnyside ave

City Mill Valley State California

Say it with "APPLAUSE CARDS"

Copyright 1925, Dictograph Products Corporation, New York City

Two Applause Cards from Marian and Bud Blum of Mill Valley display graphic radio advertising by Dictograph.



Post Card

JUN 5 9 PM 1924 CALIF.

HEADQUARTERS for RADIO and EQUIPMENT

CLEVELAND RADIO SUPPLY
NEAL COCHRAN, OWNER & MGR.
2306 BROADWAY
OAKLAND, CALIFORNIA

Broadcasting Station K L X

Address Oakland Trubine

City Oakland

State Calif

Oakland, Calif., 192

Gentlemen:

I want to express my appreciation with this APPLAUSE CARD, of the Program received from your station on Date

I wish to especially commend the following:

#12

IT'S WONDER FUL!

CLEVELAND RADIO SUPPLY
NEAL COCHRAN, OWNER & MGR.
2306 BROADWAY
OAKLAND, CALIFORNIA

Listener Henry Jorgensen

Address 836 66th Street

City Oakland State California

Say it with "APPLAUSE CARDS"

An Oakland radio dealer, Cleveland Radio Supply, seems to have provided its customers with graphic Applause Cards.

Cleveland Radio Supply also, around this time, advertised in the *Tribune*. Since the store sold "fixed crystals," perhaps the free sets (with the *paid* headphones) were crystal sets, many a listener's first radio receiver. Maybe the cartoon figure is Mr. Neal Cochran, the proprietor.

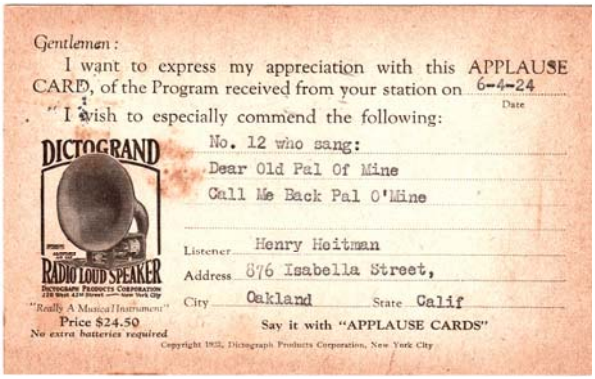
Listeners hand-wrote most of the cards and letters. A few typed responses also came in. The stationery of a San Francisco oil company bore a handwritten vote from Berkeley, for No. 12, Mr. Fraga: who " … came through like a dream." Some responses praised Mr. Fraga's piano accompanist. An Oakland plumber just sent in his business card, with a vote for "#12, also pianist."

KLX marked some postcards "Not Counted" but why is not noted, perhaps the absence of an address for the listeners voided them. (It may be that the radio prize came from a shop that wanted listeners' addresses). Two such cards featured identical handwriting, although different signatures. One not-counted card came in from Boulder Creek. The lady wrote on June 5: "No. 12 had such a clear nice voice and every word of his songs I heard so well… He also has a good radio voice." Boulder Creek is about 60 miles south of Oakland, and perhaps the mail was late… But a counted listener decided to forgo an address but wrote down an amateur radio callsign: "6AJM". One song stood out.

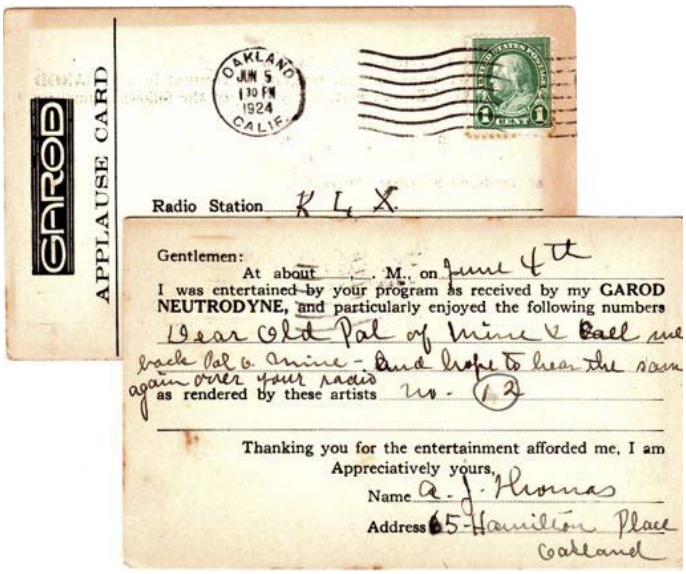
Those listeners who noted a particular song favored "Dear Old Pal of Mine" (1916) which was a World War One sentimental ballad (and also "Call Me Back, Pal of Mine"(1922)).

Cleveland Radio Supply also, around this time, advertised in the *Tribune*. Oakland Tribune, Volume 100, Number 25, 25 January 1924.

The wiki says: "Dear Old Pal of Mine is a World War I song written by Harold Robe and Gitz Rice. The song was first published in 1916 by G. Ricordi & Co. in New York, NY. Irish tenor John McCormack earned the nickname the "Singing Prophet of Victory" by popularizing this wartime song. It was in the top 20 from January to March 1919 and reached number 10 in February. The idea for the song, according to an editorial note on the sheet music, was conceived by Rice while on sentry duty at the front lines at Ypres, Belgium." (https://en.wikipedia.org/wiki/Dear_Old_Pal_of_Mine)


Gentlemen:
I want to express my appreciation with this APPLAUSE CARD, of the Program received from your station on 6-4-24 Date
I wish to especially commend the following:
DICTOGRAND
RADIO LOUD SPEAKER
No. 12 who sang:
Dear Old Pal Of Mine
Call Me Back Pal O'Mine
Listener Henry Heitman
Address 876 Isabella Street,
City Oakland State Calif
Price $24.50
No extra batteries required
Say it with "APPLAUSE CARDS"

The Garod company supplied several applause cards; it made a well-received Neutrodyne four-tube receiver in 1923.




Garod RAF 4-tube radio; Henry Ford Museum website.

Of the 128 or so post cards sent in, 44 appeared as pre-printed Applause Cards. Presumably listeners got these when they bought their radios or accessories. Twenty of these cards bore Dictograph advertising graphics. Nineteen of these cards bore advertising graphics from Cleveland Radio Supply. Five bore Garod Neutrodyne graphics.

John Schneider, CHRS writes about KLX:

> "The [Oakland] Tribune went on the air as KLX July 25, 1922, sharing the single broadcast frequency of 360 meters with all other area stations."
>
> "In the fall of 1923, the Tribune Tower building was completed, and KLX moved into the 20th floor of the tower. An antenna was strung from the top of the tower to the Oakland Bank Building, located at the other end of the block at Twelfth and Broadway. A 500-watt transmitter was purchased and installed in the Tribune Tower, and studios were constructed adjacent to the transmitter room. The station moved to the 590 kc. dial position. KLX began an operation which would continue operating from the Tribune Tower for thirty years." (From The History of KZM, KLX and KEWB Oakland, California By John F. Schneider https://bayarearadio.org/sf-radio-history/klx).

The wiki, citing Schneider, says:

> "In the fall of 1923, KLX moved to its own studio on the 20th floor of the recently completed Tribune Tower at Thirteenth and Franklin, where it would be for the next thirty years. An antenna was strung between the tops of the Tribune and Oakland Bank buildings, and the transmitter was upgraded to 500 watts."

The opening quote in this note comes from a *Tribune* flyer (see right).

By 1925 some 6,000,000 radios informed and entertained Americans.

"The Rise of Radio [-] Beyond belief is the rapid development of the radio communication art. Herbert Hoover, Secretary of Commerce, recently told an audience that radio broadcasting had developed in the United States in five years from one station to over 600 stations, with 6,000,000 home receiving sets; that the probable expenditure this year for radio entertainment would be in excess of four hundred millions of dollars; …"


RADIO

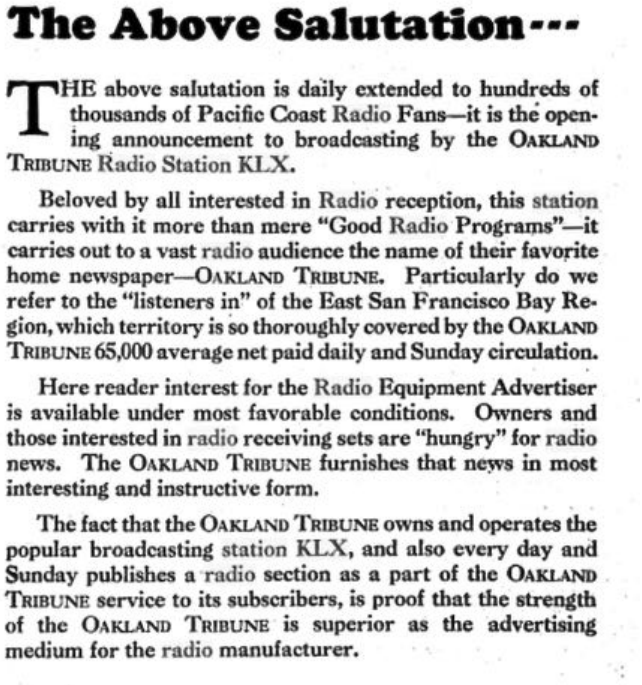
KLX

The Oakland TRIBUNE
Portable Call KGA
AMATEUR CALL 6BVO
Phone Lakeside 100.
Official broadcasting station for the city of Oakland and the United States Department of Agriculture.
TODAY
7:00 to 7:30 P. M.—Music and official weather reports.

KZM

Hotel Oakland Station.
(This Evening)
6:45 to 7:00 P. M. Broadcasting news bulletins furnished by The OAKLAND TRIBUNE.
KLX is owned and operated by The OAKLAND TRIBUNE. KZM is owned and operated by the Western Radio Institute. At the present time The TRIBUNES transmitting set is temporarily being used by KZM as a matter of convenience.

Radio station KLX used more than one callsign.


The Above Salutation---

THE above salutation is daily extended to hundreds of thousands of Pacific Coast Radio Fans—it is the opening announcement to broadcasting by the OAKLAND TRIBUNE Radio Station KLX.

Beloved by all interested in Radio reception, this station carries with it more than mere "Good Radio Programs"—it carries out to a vast radio audience the name of their favorite home newspaper—OAKLAND TRIBUNE. Particularly do we refer to the "listeners in" of the East San Francisco Bay Region, which territory is so thoroughly covered by the OAKLAND TRIBUNE 65,000 average net paid daily and Sunday circulation.

Here reader interest for the Radio Equipment Advertiser is available under most favorable conditions. Owners and those interested in radio receiving sets are "hungry" for radio news. The OAKLAND TRIBUNE furnishes that news in most interesting and instructive form.

The fact that the OAKLAND TRIBUNE owns and operates the popular broadcasting station KLX, and also every day and Sunday publishes a radio section as a part of the OAKLAND TRIBUNE service to its subscribers, is proof that the strength of the OAKLAND TRIBUNE is superior as the advertising medium for the radio manufacturer.

Oakland radio station KLX got in on broadcast radio from the beginning. Mr. Fraga was but one of its beneficiaries, as was its radio audience in the Bay Area. KLX's link to the *Tribune* enlarged its audience, and hence its advertising revenues. For the *Tribune* to put on the air its own radio station likely enlarged its readership, thus advertising revenues as well. This sort of marriage (if not made in Heaven, at least "made in the ether"), was a nationwide phenomenon. It fostered broadcasting in regions with metropolitan newspapers. The "Radio Fad" offered 1920s big money all around, as well as enthusiasm for the new technology of broadcast radio. It also offered artists like Mr. Fraga a way into the worlds of entertainment that they sought to enter.

◊

The Enigma of Ultra

By Richard Watts

Last October I was able to visit Bletchley Park and the neighboring British National Museum of Computing located about an hour north of London. It was extremely interesting and I can attest that a one-day visit is not nearly enough time to absorb it in any depth.

On display are many artifacts of WWII Ultra wireless, code breaking, and intelligence accomplishments. Below is a working reproduction Bombe on display, an exceptionally brilliant bit of kit.

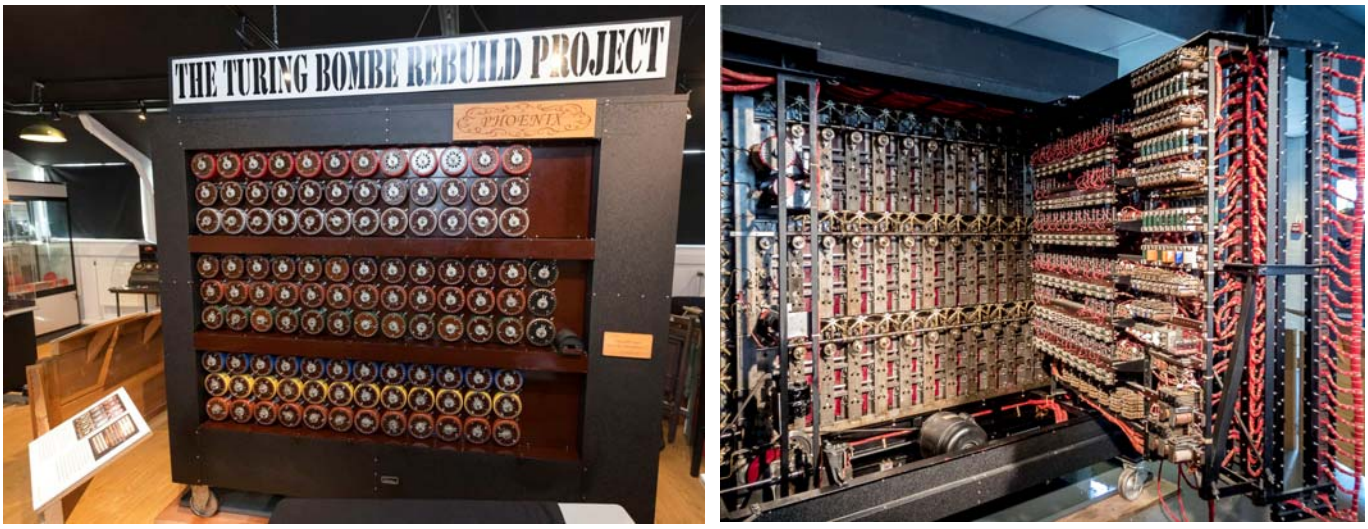
Bletchley Park mansion. The mansion house with the odd architecture and carriage houses behind served as work space for the first staff. As staff increased, several barracks-like wooden buildings called Huts and, later, block buildings were built on the grounds. Source: Bletchley Park website

In 1937, Admiral Sinclair, then head of the Secret Intelligence Service (SIS) or MI6, purchased the 58-acre Bletchley estate for £6,000 of his personal funds as a potential location for the Government Code and Cipher School (GC&CS) and SIS should war break out. He chose the rural location provided as it was more isolated and less vulnerable, which proved to be true as it never came close to being bombed.

Ultra

During WWII, Ultra was a trilogy of listening, deciphering, and understanding enemy (primarily German) military signals communications. Ultra was more secret then 'Top Secret', it was 'Ultra Secret.' German signal communications were intercepted by Y-Service, a network of wireless stations throughout England. The messages were forwarded to GC&CS at Bletchley Park to be processed, translated, and decrypted. Special Communications Units organized, indexed, interpreted the intelligence and the Special Liaison Units dispatched the intelligence as appropriate.

Having the capability to decipher and read German communications became an essential war time asset. It was essential that the Germans not know that their ciphers had been compromised or they would have changed their methods. The Allies went to great lengths to make sure there was a plausible explanation for how intelligence was known in an



The British National Museum of Computing has a working reproduction of the Turing-Welchman Bombe on display. Right is the front view and left is a view of the rear showing internals. A docent demonstrated its use and how it expedited the process to solve the Enigma.

alternative way. For instance, if a deciphered message indicated the location of a ship or U-boat, the Allies would send up a spotter plane to "just happen" fly over the ship and report its position.

Y-Service

Y-Service was a network of wireless interception sites established in WWI and operated by Navy, Army, RAF, and civilian organizations. Most of the intercept operators were members of the WRNS (Women's Royal Naval Service), ATS (Auxiliary Territorial Service, Woman's branch of the British Army) , and WAAF (Women's Auxiliary Air Force), who received extensive training.

During WWII, Y-service monitored German communications from over 43 stationary sites plus many more temporary mobile sites. Most stationary sites had hardwired teletype links with Bletchley Park. Dispatch riders delivered the messages when a teletype link wasn't available.

The preferred receivers for Y-Service were the HRO S and M models because of their sensitivity and precise tuning. In addition, RCA AR88, and Hallicrafters SX28 Super Sky Rider, S-27, and S-36 receivers were also used. Several Y-Service sites were also equipped with Direction Finding capability.

There was considerable intelligence to be learned beyond the message content, just in the intercept of German communications. The radio intercept operators recorded the frequencies and call signs of the different German military groups. From this they were able to determine the command hierarchy of the groups and their geographic location. They also tracked the movement of troops and military units and naval vessels. When signal was weak or a messages source was critical, two operators might be assigned to receive the same traffic to increase accuracy and provide error checking.

Dispatch riders delivered messages from the many intercept sites all over Great Britain to Bletchley and Whaddon Hall if there was no teletype link connecting the site. Source: Imperial War Museum

Intercept operators were able to recognize the 'fists', voices, or accents of individual German operators. A U-boat could be tracked by identifying the operator and taking Direction Finding bearings. There were times when they received a message from an operator call sign that clearly wasn't him. It could be an indication that group had moved and the message is being transmitted from the old location to disguise the move.

Radio Security Service (RSS) was formed from about 1500 amateur radio operators, now called Voluntary Interceptors (VIs). RSS amateurs tended to use the more affordable Hallicrafters Sky Pilot, and Sky Rider. They were no longer able to be on the air as their transmitters had been impounded at the beginning of the War. RSS was tasked with monitoring short-wave bands for any suspicious outgoing transmissions. The intent was to uncover spies working clandestinely in England. RSS operators were successful at identifying Abwehr (German intelligence service) traffic and in some cases were able to decrypt messages. In 1943, over 10,000 messages a day were received by VIs and forwarded to Bletchley Park. With their proven effectiveness, they were transferred formally into MI6, and called Section 8c and headquartered first at Arkley near London, then at Hanslope Park near MI6 communications headquarters at Whaddon Hall, just a few

WWII Y-service wireless intercept operator using a National HRO receiver. Source: CryptoMuseum.com

WWII Y-service wireless intercept site at Dunstable, England. Source: Unknown

miles from Bletchley Park. Hanslope Park has since become His Majesty's Government Communications Centre, the secret home of 'Q' who still make really cool stuff for '007'.

The Germans primarily used two methods of encryption, the Enigma and Lorenz machines. The Enigma machine was used for Morse Code traffic generally for tactical German land forces (Heer, Panzer), Air Force (Luftwaffe), and Naval (Kriegsmarine). The Lorenz machine was used to encrypt higher speed teletype traffic and was used for the German High Command. The Bletchley Park code breakers were successful in breaking both machines. This article will focus on the breaking of Enigma; the breaking of Lorenz is a story for another day.

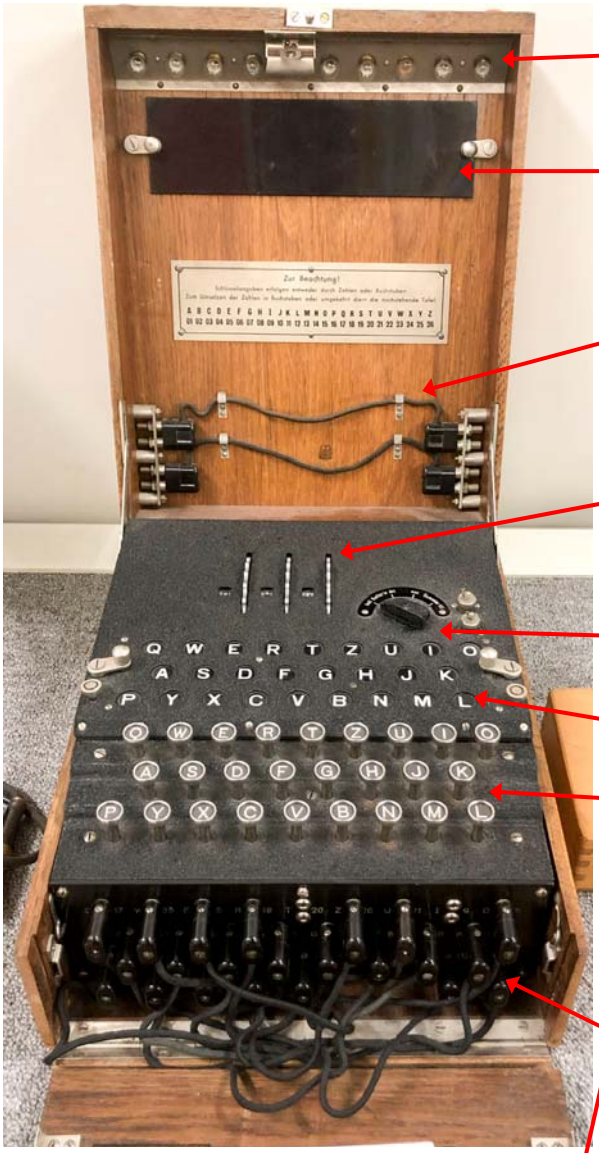
I present some detail of their code breaking methods and theory to facilitate an appreciation for their effort, creativity, and genius.

The Enigma Machine

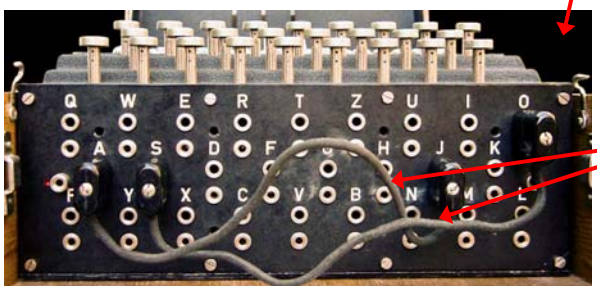
The Enigma is a member of a family of rotor based cipher devices. Its sole purpose is to substitute one letter for another. When a letter is keyed in via the keyboard, a lamp on the lamp board is lit showing the substitute. To encrypt a message is enciphered one letter at a time. To encrypt an entire message, the user has to first initialize the machine (more on this later). Then the user would key each letter of the message one letter at a time and generally with the help of a second user, would simultaneously write down the lit encrypted letter. Once the entire encrypted message was created and written down, the message could then be delivered to the receiver. Messages usually transmitted and received via morse code over wireless.

The Enigma is reciprocal. That is, if one types in a "Q" and the "O" lamp is lit then it will be the case that had an "O" been typed instead, the "Q" lamp would have lit. This characteristic enables both encryption and decryption of a message. Thus, to decrypt the received encrypted message, one has to initialize their Enigma machine in exactly the same manner as the machine used for encryption; the encrypted message is then typed in and lamps light; the result will be the original message. Accuracy is important. The message being sent and received by morse code has to be exact.

When initializing the Enigma machine, the user must install the plug board jumpers. In the literature, the jumpers are steckers and the plug board is a steckerbrett. The plug board has jumper sockets for the entire alphabet. Inserting a jumper between two letters swaps those letters in the cipher. At right, there are two jumpers: one that swaps A and J, and another that swaps S and O. It is possible to install 13 jumpers but typically only 10 were used at a time. Plug board jumpers were usually set on a daily basis according to a key book.



German Enigma machine.
Source: Wikicommons, Arnold Reinhold

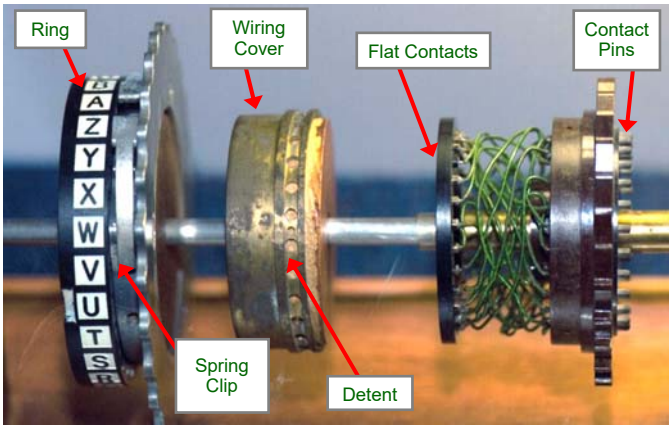


Front view of the Enigma plug board.
Source: Wikicommons, Bob Lord

The user must also initialize the rotors. Every 3-rotor Enigma machine came with a set of 5 rotors numbered I to V. Each rotor had a nest of wires that connected the pins on one side to the flat contacts on the other (see photo right). The wiring pattern for a rotor was different for each of the rotors in the set of five. The rotors can be installed in an Enigma in any order as prescribed in the key book.

Each rotor had a moveable ring called the ringstellung. Rings could be numbered (preferred by the Army) or lettered (preferred by the Navy). In this article, for simplicity I will present the rotor's rings as lettered. The user clips the position of the alphabet ring on each rotor according to the key book for that day.

Each rotor has a ratchet wheel that meshes with a pawl mechanism to advance the rotors like an odometer when a letter key on the keyboard is pressed. With this rotor advancement, a 'Q' might encode as an 'O', but if 'Q' is pressed a second time, it will be encoded as a different letter.

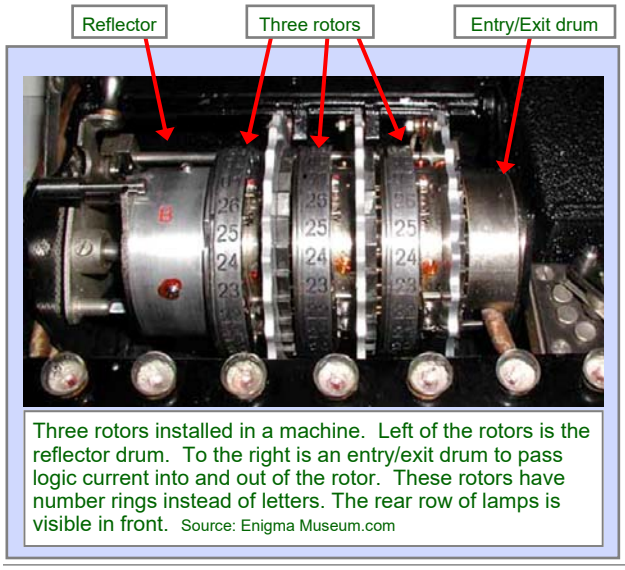


A disassembled rotor. Right is the wiring of the rotor. Each pin is wired to a contact. The contact pins of one rotor make contact with the flat contacts of the next rotor.

Left is the ring with the alphabet and thumbwheel. This ring is movable around the brass wiring cover and can be clipped in any position in relation to the inner wiring assembly with the spring clip locked into the detent in the wiring cover. This increases the possible configurations of the wiring pattern to the alphabet.
Source: British National Computer Museum

A three-rotor set shown from the side with flat contacts. The thumbwheel is used to turn each rotor for the initial setting. The rod in front is the axle. Source: Enigma Museum.com

Other side of the three-rotor set showing the contact pin side. The ratchet wheel meshes with a pawl mechanism that advances the rotors like an odometer during operation.
Source: Enigma Museum.com



Three rotors installed in a machine. Left of the rotors is the reflector drum. To the right is an entry/exit drum to pass logic current into and out of the rotor. These rotors have number rings instead of letters. The rear row of lamps is visible in front. Source: Enigma Museum.com

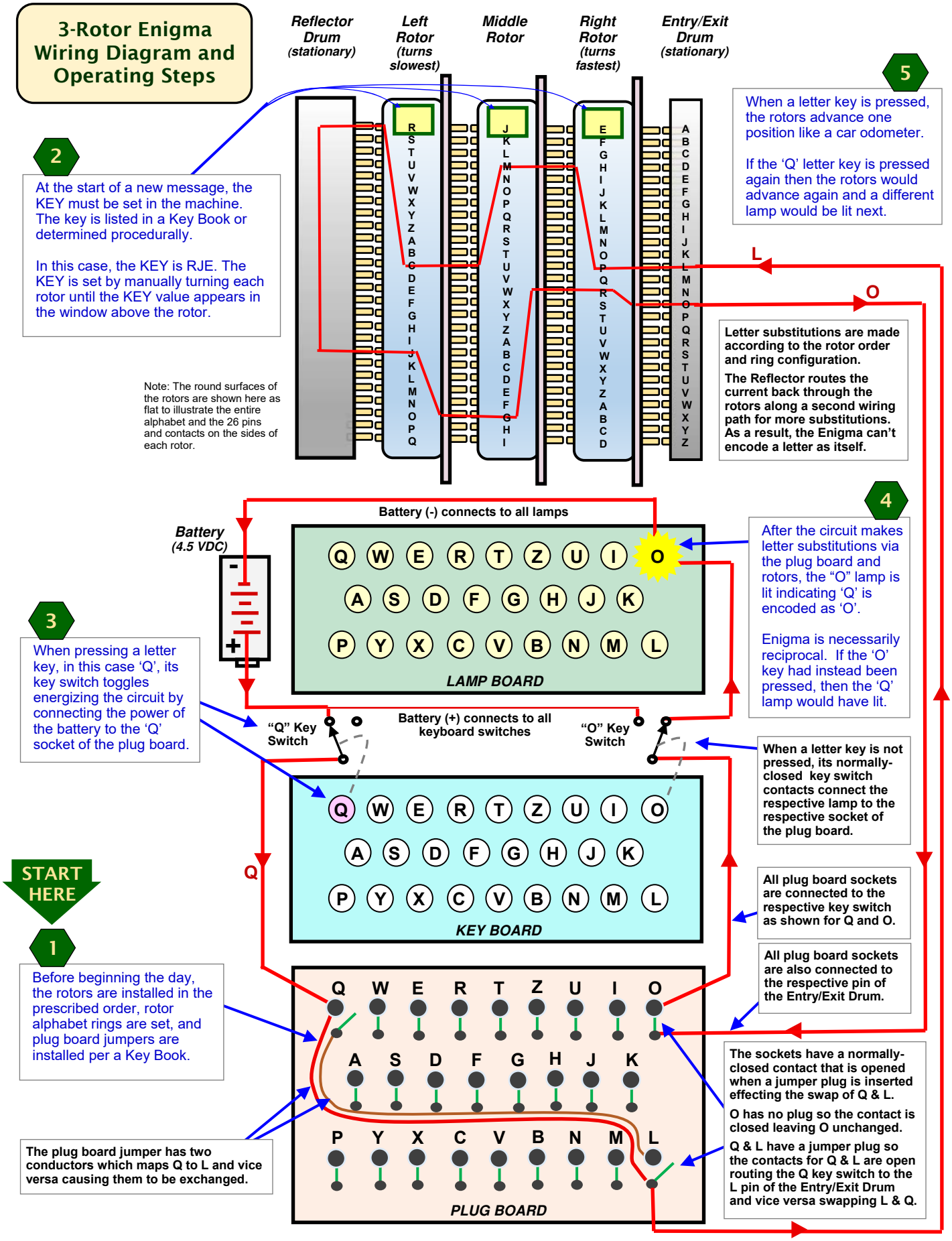
The odometer advancement works as one would expect. The rightmost rotor advances after each key press. Once it has completed a full revolution, the middle rotor advances one letter position. Once the middle rotor has made a complete rotation, the left rotor advances one letter position.

When one rotor causes the next to advance, it is called a turnover. There is a notch on the side of the alphabet ring that determines when the next rotor will turnover. In the rotor above, the white notch next to the "U" is the point in rotation where the rotor to the right will turnover. The notches are at a different position on each of the five rotors.

The reflector has pins only on one side and makes contact only with the leftmost rotor. The reflector contains thirteen wires that map each pin to another. Current entering from one of the leftmost rotor contacts is routed to another pin which sends the current back through the rotors along a second wiring path (see the Enigma Wiring Diagram on a following page). This increases the number of letter substitutions. It has a side effect of preventing a letter from being encoding as itself which is a weakness that was exploited in breaking the Enigma codes. The reflector is stationary, doesn't rotate, and can't be removed by the user. The reflector is called an Umkehrwalze or UKW.

To send a message, the rotors have to be set with a key of three letters, e.g. RJE. It is called the grundstellung (start position). The user must rotate the rotors until 'R', 'J', and 'E' appear in the rotor windows. The grundstellung is either from a key book or derived in a procedure. The goal of breaking the Enigma code is to determine the grundstellung key for a particular day. More about this later.

3-Rotor Enigma Wiring Diagram and Operating Steps



2

At the start of a new message, the KEY must be set in the machine. The key is listed in a Key Book or determined procedurally.

In this case, the KEY is RJE. The KEY is set by manually turning each rotor until the KEY value appears in the window above the rotor.

Note: The round surfaces of the rotors are shown here as flat to illustrate the entire alphabet and the 26 pins and contacts on the sides of each rotor.

5

When a letter key is pressed, the rotors advance one position like a car odometer.

If the 'Q' letter key is pressed again then the rotors would advance again and a different lamp would be lit next.

Letter substitutions are made according to the rotor order and ring configuration.

The Reflector routes the current back through the rotors along a second wiring path for more substitutions. As a result, the Enigma can't encode a letter as itself.

4

After the circuit makes letter substitutions via the plug board and rotors, the "O" lamp is lit indicating 'Q' is encoded as 'O'.

Enigma is necessarily reciprocal. If the 'O' key had instead been pressed, then the 'Q' lamp would have lit.

3

When pressing a letter key, in this case 'Q', its key switch toggles energizing the circuit by connecting the power of the battery to the 'Q' socket of the plug board.

When a letter key is not pressed, its normally-closed key switch contacts connect the respective lamp to the respective socket of the plug board.

All plug board sockets are connected to the respective key switch as shown for Q and O.

All plug board sockets are also connected to the respective pin of the Entry/Exit Drum.

The sockets have a normally-closed contact that is opened when a jumper plug is inserted effecting the swap of Q & L.

O has no plug so the contact is closed leaving O unchanged.

Q & L have a jumper plug so the contacts for Q & L are open routing the Q key switch to the L pin of the Entry/Exit Drum and vice versa swapping L & Q.

START HERE

1

Before beginning the day, the rotors are installed in the prescribed order, rotor alphabet rings are set, and plug board jumpers are installed per a Key Book.

The plug board jumper has two conductors which maps Q to L and vice versa causing them to be exchanged.

Key Space

In cryptography, key space is the set of all valid possible distinct key configurations for a cryptographic system. For example, my Little Orphan Annie decoder pin has a ring of the alphabet that is opposite a ring of numbers 1 through 26. The key given by the Annie's trusted radio announcer, Pierre Andre matched a letter with a number, say B-11. The two rings were then twisted to align to that key. Pierre would then read the all important message as a string of numbers. The anxious listener would find the letter that corresponds to each number and write down this most important message from Annie.

Little Orphan Annie decoder pin, 1940.
Source: Author's collection

If one should encounter an encoded number-string message but didn't have the key to decode it, one might try a brute force attack in which one tries all the possible combinations of aligning the alphabet ring with the number ring. There are only 26 possible alignments of the alphabet ring to number ring which equates to a tiny key space of 26. A brute force attack trying all 26 possibilities to find a readable message would be trivial, and it should only take a few minutes to reveal Annie's vital secret message: Be sure to drink your Ovaltine.

The key space for the Enigma is a bit larger. The theoretical maximum key space considers all construction and configuration possibilities. The factors for the 3-rotor Enigma are (from Cybermachines.com):

- The possible permutations for plugboard settings using any number if jumpers up to 13 = 532,985,208,200,576
- Rotors can be wired in 26! ways, the total possible ways of selecting 3 rotors from this large rotor set = 65,592, 937,459,144,468,297,405,473,480,371,753,615,896,841,298,988,710,328,553,805,190,043,271,168,000,000
- Each of the three rotor alphabet rings could be initially set to any letter = 17,756
- The rightmost rotor advances one letter after each key is pressed, the second and third rotors advance one letter after a full revolution of the rotor to its right. The setting for the notch to enable this was also changeable to any letter of the alphabet = 676
- The reflector wiring is between any two pins, all pins are paired. The total possible ways this can be wired = 7,905,853,580,625

The theoretic maximum key space is the product of the above factors which is 3.28×10^{114}. This is larger than the total atoms estimated in the observable universe ($\sim 10^{80}$). The 4-rotor German Naval Enigma was even larger at 2×10^{145}.

The 3-rotor Enigma machine encountered by the Allies had a much smaller key space as the Germans made certain practical compromises like using only a 5-rotor set instead of a huge rotor set of all 6.56×10^{79} possible rotors above. The practical key space for the compromised factors above is then calculated as follows (from Cybermachines.com):

- 10 plugboard jumpers were always used out of 13 possible = 150,738,274,937,250
- Only 5 rotors were issued and could be installed in any order, so selecting 3 out of 5 is 5 x 4 x 3 = 60
- Each of the three rotor alphabet rings could initially be set to any letter = 17,576
- The setting of the rotor the notch for rotor advancement still = 676
- Reflector was stationary and its wiring was known and remained unchanged = 1

Note: the configuration of plugboard jumpers is now the largest single factor in the German Enigma key space.

The practical key space is a much smaller 1.07×10^{23}. versus the 3.27×10^{114} maximum key space. The practical key space is quite still large. To put this in perspective, to do a brute force attack to test all 1.07×10^{23} key settings, 100,000 operators each checking one setting every second would take twice the age of the universe to break the code.

Needless to say, the Germans felt supremely confident that the Enigma machine was more than adequately secure.

Early Rotor Encryption Machines

Edward Hugh Hebern.
Source: Wikipedia.com

The earliest inventor of a rotor encryption machine was Edward Hugh Hebern (1869-1952) born in Illinois and moved west and to Oakland, CA and in 1922 created a manufacturing company at 829 Harrison St. His first drawings of the machine date to 1917. He applied for a U.S. patent in 1921 which was granted in 1924.

Hebern's business struggled for lack of sales and over investment. He tried to interest the US Army and Navy and was able to sell them a few 5-rotor machines. However, William Friedman, a noted U.S. Navy cryptologist was able to break the machine in short order exploiting the weakness of rotors that advance in an orderly odometer-like fashion. He was never told why there was no interest, or of the vulnerabilities.

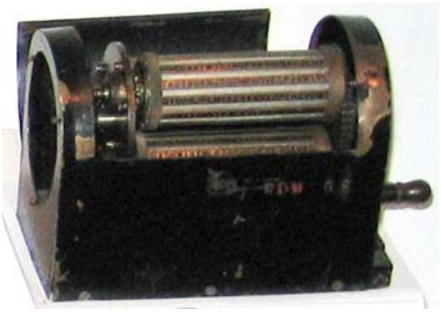
This is an early version of the Hebern encryption machine. It had just one rotor. Later models had 5 rotors that advanced like an odometer. Source: Ciphermachines.com

William Friedman and Frank Rowlett invented the SIGABA rotor encryption machine which had a much more complex mechanism. It utilized three banks of 5 rotors. The first bank operated in a similar way as the Enigma rotors. The second bank was for stepping control indexed by the third bank of smaller 10-pin rotors. This produced rotor patterns of irregular movement, and a larger key space than Enigma. The U.S. SIGABA was not broken.

Arvid Damm.
Source: Wikipedia.com

Boris Hagelin with an M-209.
Circa 1940. Source: Wikipedia.com

Arvid Damm (1869-1927) was a Swedish engineer and inventor. He founded AB Cryptograph in 1916 to develop and promote his various inventions and ideas. Damm patented several rotor based cipher machines, the first in 1919 just three days after Hugo Koch filed a patent file for a similar device in the Netherlands. Of the machines he patented, a 1921 model one could print on tape. One from 1923 (right) had a cylinder with 26 alphabet strips around its circumference forming a cylinder cipher.



Damm cipher machine prototype.
Source: Wikipedia

When Damm died in 1927, the Swedish company was purchased by Boris Hagelin, the company controller and manager. Hagelin developed the successful C-38 pin and lug cipher machine (a.k.a. M-209). When the Germans invaded Norway in 1940, Hagelin came to the United States where he was able to sell the M-209 to the U.S. Army. It was not the most secure machine the U.S. had available, but it was lightweight and easy to use. It was utilized in several other counties as well. The machine saw continued use through the Korean War. Hagelin returned to Sweden in 1944 a millionaire. In 1948 he moved the company to Switzerland; in 1952 the company became Crypto AG, which has had a close relationship to U.S. Intelligence, but that's another story.

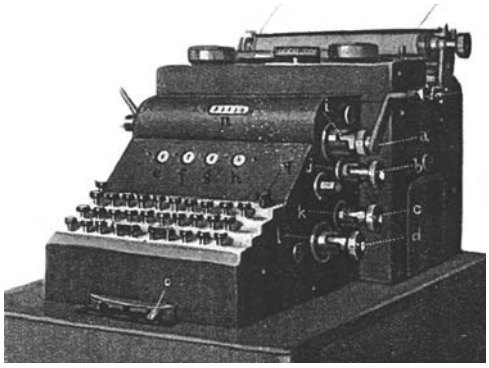
Arthur Scherbius.
Source: Wikipedia.com

The Enigma was invented by Arthur Scherbius (1878-1929) who was born in Frankfurt, Germany. He applied for a patent for his Enigma rotor cipher machine in 1918. Also in 1918, Scherbius with E. Richard Ritter founded the Scherbius & Ritter. In 1923, this company morphed into Chiffriermaschinen Aktien-Gesellschaft (AG) with Scherbius and Ritter on the Board of Directors.

Another inventor Hugo Koch, filed a patent for a similar device in 1919 in the Netherlands, a year after Scherbius but he never did anything with it or produced a device. Koch sold his patent rights to Scherbius in 1927.

Scherbius offered the first Enigmas to the German Navy but, while they felt it was secure, they didn't see the need. It was also offered to the German Foreign Service for diplomatic use, but

again there was also no interest. His first models were large and heavy. The Model A circa 1923 (right) had a printer that on could type the encrypted message or type plain text like a typewriter.. It had four 28-pin rotors that were driven by four geared drive wheels which had different numbers of teeth, plus some also had gaps which made the rotor movement irregular and not orderly like an odometer. Since the military wasn't interested at that time, he targeted the commercial market. Sales were slow.



First model of Enigma, the Model A.
Source : The Commercial Enigma - Kruh & Deavours

A commercial Model D Enigma circa 1926 or 1927. Source : Cryptomuseum.com

The Enigma continued to evolve. A reflector was added to reduce the number of rotors, and other changes were made to make the machine more portable. The early model D (left) has 3 rotors; the leftmost thumbwheel is a settable reflector.

The early versions of Enigma didn't have a plugboard reducing the key space significantly. Only 3 rotors were included with the early model D Enigma, later they would be issued with a set of 5 rotors.

Finally, in 1926, the German Navy renewed interest in the Enigma as did the German Army in 1928. A number of changes were made to meet the German military requirements that resulted in 1930 as the Enigma I (right). The rotors wiring patterns were changed and the plugboard was added to strengthen the security of the machine. The reflector wiring was changed and it was fixed in place and no longer able to be settable

Enigma I. Source : Bonham Auctions.com

The Enigma was only available to the military. It was at this time that the German Army took control of Enigma manufacture. Chiffriermaschinen (AG), which was renamed Heimsoeth & Rinke in 1934, was the sole manufacturer of the machines through the 1930s. The German military ordered increasingly more, clearly preparing for war. In 1939 there were 40,000 Enigmas. By 1940 it was manufactured by four more companies.

Breaking the Enigma - The 1930s

As direct neighbors of Germany, in the late 1920s and early 1930s France and Poland were very motivated to understand Germany's intentions and gave more intention to breaking encrypted German communications than Great Britain, who at that time, were more focused on the larger threat they perceived from Russia. Polish cryptographers were having some success in deciphering German communications, then in 1926 German Naval communications were becoming unreadable and again in 1928 with German Army communications. Their conclusion was that Germany had adopted a new enciphering device and their prime suspect was the Enigma, which at that time wat the commercial version. The Poles were able to acquire a commercial Enigma.

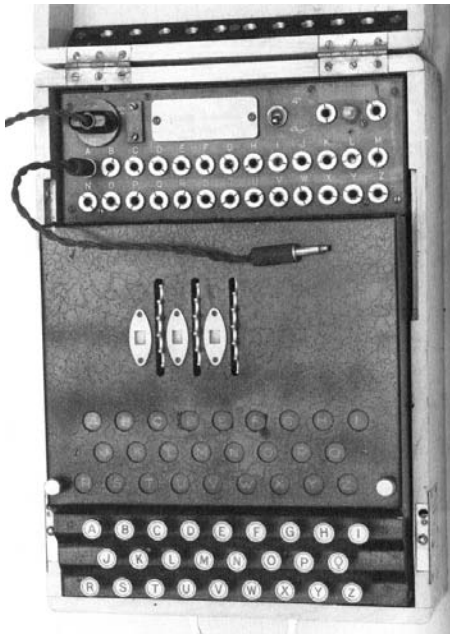
By 1930, the Germany military had adopted the Enigma I which as explained above had significant differences with the commercial Enigma. Up to Fall of 1932, only slight progress was made in understanding Enigma I. Major Ceizki, the head of the Polish Cipher Bureau, enlisted three outstanding students from a cryptology course of study at University of Poznan, where the three had previously graduated with advanced degrees in Mathematics. They were young, in their mid -twenties, and demonstrated an adeptness for cryptology. They were Marian Rejewski, Henryk Zygalski, and Jerzy Rozycki. This team of Polish mathematicians were the first to break the Enigma. Their work in the 1930s would be done in complete secrecy.

In October 1932 Rejewski was assigned to work alone, at first part-time in the evenings, toward understanding the workings of the Enigma I. He had available a commercial Enigma machine; German military user documentation clandestinely received from the French that November which included the daily keys from a year earlier, September and October 1931; and encrypted German messages from that same September -October 1931 period. Withinin ten weeks Rejewski had come to understand the differences of the Enigma I from the commercial model, and he developed a mathematical model of the Enigma I and reconstructed the internal wiring without having seen one — no small feat!

Polish code breaking team, circa 1932; l-r Henryk Zygalski (1908-1978), Jerzy Rozycki (1909-1942), and Marian Rejewski (1905-1980).
Source :Museum for Communication Frankfurt, Germany

Because the rotors rotate like an odometer, when a letter is typed, the rightmost rotor turns first. Thus, the first few letters of any message are encrypted only by the movement of the right rotor until a turnover (advancement of the next rotor) occurs. Until there is a turnover, the remainder of the Enigma encrypting elements including the plugboard and other two rotors can be considered as fixed. Since the team had both the keys and messages for the same period in September and October 1931, Rejewski was able to determine the permutations that the Enigma employed to encode the messages from those keys. By focusing on the first part of the messages and analyzing the permutations of just the right rotor, Rejewski was able to determine its wiring. Since, according to German procedure, the order of the rotors was swapped periodically, it wasn't long until each of the rotors would have been swapped into the rightmost position enabling their wiring orders to be determined as well. Once Rejewski knew the wiring of the three rotors, he could then determine the wiring of the reflector.

Windows showing rotor values. The rotors advance one at a time like an automobile odometer. The right rotor turns first followed by the middle, then left rotor. A notch on each rotor causes the turnover (i.e. advancement) of the next.



A replica of the Polish Enigma "Double" built by the French from Polish design. From its appearance, this may have been converted from a commercial Enigma. Note the addition of a make-shift plugboard on top. On display at the Jozeph Pilsudski Institute in London.

Alas, the full inner workings of the Enigma were known to the Polish team. From this the Polish Cipher Bureau constructed working replicas of Enigma I referred to as the Polish Enigma Double (left). Initially 15 were made by AVA Radio Manufacturing Co. of Warsaw, Poland.

Breaking the Enigma Key

To decipher a message, their challenge was to determine the rotor order, ring setting, and daily key. In 1932, the order of the rotors changed every three months and the ring settings every month — the plugboard settings and key changed every day. Rejewski was able to devise methods to solve the encrypted user keys without knowing the plugboard, rotor order, alphabet ring settings, or the start key.

To start, the Enigma documentation provided by the French described a two step operating procedure to set keys. First the encipherer looked up the grundstellung key in a code book for that day. Second, the encipherer would then create another 3-character code of their own choosing and send two copies of it (six characters total) encrypted by the grundstellung daily key. For example, an encipherer might choose the key DOG which would be sent as DOGDOG. The reason for duplicating the user key was to insure it could be

received in poor signal conditions. Next, the encipherer would change the rotors to his user key (DOG) and encrypt the message. Then the message would be sent via Morse Code.

To decrypt the message, the receiver used the daily grundstellung key to decrypt the first six letters to get the sender's defined key (DOG). The receiver reset the rotors in their machine to that user key and decrypted the message.

Sending a duplicate key created a major vulnerability that the Polish team exploited. In the replicated key (i.e. DOGDOG), the 1st and 4th character are the same, as are the 2nd and 5th, and the 3rd and 6th. An encryption of DOGDOG might be AUQAMN. Thus the first and second As are both an encryption of the letter "D." Similarly U and M are an encryption of "O", and Q and N are an encryption of "G."

As described previously, the team's analysis focused on the rightmost rotor as it was the only rotor involved in the encryption provided a turnover didn't occur. Since the rotor has 26 positions, in typing the first six key characters, a turnover would occur in 5 out of 26 cases (only about 19% of the time); The remaining 81% of the cases (21 out of 26 cases) there would be no turnover.

Rejewski set out to compile a **Catalog** of the six possible ways to order the three rotors, coupled with possible daily key setting of which there is 26^3 = 17,576. The total possibilities is 6 x 17,576 = 105,456 catalog entries. He worked out cataloging scheme based on permutations cycles. Working through the calculations would be tedious and time consuming, so the team devised a machine, the Cyclometer (reproduction shown below) to expedite finding the permutation cycle groups for each entry. There is more about this technique on the next page.

The **Cyclometer** has two banks of three Enigma rotors each. They are initialized in the same order and with the same start setting except the right rotor in one set is advanced ahead three letters of the right rotor in the other set. Thus one rotor set is in the first character position of the message, and the other rotor set is in the fourth. As discussed, these positions encrypt the same letter of the user key. The Cyclometer wires the two rotor sets together in such a way that when a switch for a letter is flipped, the wiring path that includes that letter in a permutation group is energized and the lights for all the letters included in that group are lit. The discussion on the next page should provide more insight.

The team worked to compile that catalog when they had time available; even with the use of the Cyclometer, it took the team about a year to compile the catalog. Due to secrecy, this was work that couldn't be delegated. The card catalog was finished in 1937. Rejewski stated that the card catalog worked well and finding a key would only take 10 to 20 minutes.

Finding the key was also made easier when the encipherer through bad habits happened to pick easily guessed keys like keyboard repetitions (AAA, QQQ, SSS, etc.), or adjacent keyboard patterns (QWE, QAY, ASD, etc.), or familiar words like my personal favorite DOG. The team kept track of various operators and came to know which were careless in selecting a key, paying particular attention to their messages.

A reproduction of the Cyclometer built by Henry Evans, University of Cambridge. The cyclometer finds permutation cycles for possible solutions of Enigma keys. Two sets of 3 Enigma rotors are mounted in the compartments at top to left and right. The panel has lamps (A-Z) and a rheostat (left) that controls the brightness of the lamps. The intent was to make a faithful reproduction based on the scant information available. Henry Evan explains its operation on Youtube (search for Cyclometer Evans).

Even when a key was found, there was more to do to decipher the message. The plugboard configuration still had to be solved. The German operating practice at this time was to use 6 plugboard jumpers (steckers). Thus 12 of the 26 letters were swapped in pairs, while the remaining 14 were not changed. Since half the letters were unchanged, the message might be partially readable. Then from the message content, it may become apparent which pairs of letters had been swapped.

Unfortunately, according to Rejewski, on 2 November 1937, the Germans changed to Reflector B with different wiring. The catalog was immediately out of date and would have to be redone, however, the time it would take would be too much.

Since the catalog was obsolete, the team devised new techniques. **Zygalski Sheets** exploited the occurrence of 'females.' They were designed as series of punched sheets with 26 columns and rows that encoded right rotor wiring orders, and a larger 51 x 51 sheet with

Permutation Cycles

Rejewski used permutation cycles extensively as did the code breakers at Bletchley Park. This tool produced the patterns that were the basis of Rejewski's catalog and is the process that the Cyclometer directly implements. Insight can be gained by taking a quick look at this.

Rejewski focused on the duplicated user key in the first six characters of each message, and the Enigma configuration permutations that encrypted them. Rejewski named the permutations that encrypted those first six characters positions as **A, B, C, D, E,** and **F** respectively.

He didn't know what the permutations were, but he did know that permutation **A** encrypts the key letter 1 to message character-1; and permutation **D** encrypts key letter 4, which happens to be the same as key letter 1, to message character-4.

Since they encrypt the same letter, the product of permutations **A** and **D** can be analyzed to reveal, as Rejewski said, the machine's "characteristics" of the day. The joining process shown right maps the encrypted values of character-1 (**A**) and character-4 (**D**) to form permutation cycles.

Needed were enough messages encrypted on the same day such that the entire alphabet is found in each column. Rejewski said he typically needed 60 to 80 messages. This list of only 32 encrypted message keys (right) has this property.

The process starts with one of the encrypted keys, say from message 1, and follows the path mapping character-1 to character-4, then to another message key whose character-1 matches the previous character-4. This continues until a character-4 has the same value as the beginning character-1. Thus, it loops back and ends that cycle group.

In the case of mapping the key from the first message **AUQ AMN**, it is a small group with only one permutation. Since the characters 1 & 4 are the same, it maps to itself. This is called a 'female' and has a special use -- more later.

Then find the next group by selecting another message key that has a character-1 value that hasn't been used yet, say the key from message 2 with a character-1 value of "B". Repeating the process, this cycle maps only two permutations.

The process continues on to reveal each cycle group and ends when all the character values (i.e. the alphabet A-Z) have been used in one of the cycles.

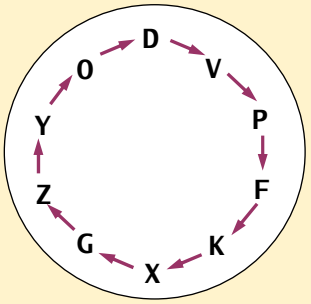
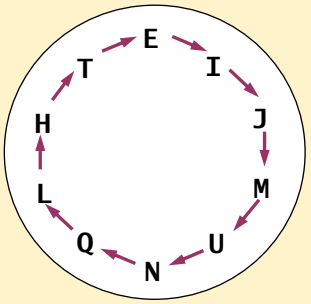
Once all the cycles groups for **AD** have been found, the same process can be used to map the permutations for characters 2 & 5 (**BE**), and for characters 3 & 6 (**CF**). Try it; it's actually pretty easy once you see the pattern.

The cycle groups are shown (right) for **AD**, **BE**, & **CF** using a condensed cycle notation. Each has different characteristics. **AD** has 2 groups of 10, 2 of 2, and 2 of 1. **BE** has 2 groups of 8, 2 of 3, and 2 of 1. **CF** has just 2 groups of 13. These are the characteristics that Rejewski cataloged.

First six characters of 32 messages for the same day

Message #	Encrypted User Key
1	AUQ AMN
2	BCT CGJ
3	BNH CHL
4	CIK BZT
5	DDB VDV
6	EJP IPS
7	FBR KLE
8	GPB ZSV
9	HNO THD
10	HXV TTI
11	IKG JKF
12	JWF MIC
13	KHB XJV
14	LDR HDE
15	MAW UXP
16	NLU QFZ
17	NXD QTU
18	OBU DLZ
18	PVJ FEG
20	QGA LYB
21	RFC WQQ
22	RJL WPX
23	SYX SCW
24	TMN EBY
25	USE NWH
26	VQZ PVR
27	WTM RAO
28	XOI GUK
29	XRS GNM
30	YPC OSQ
31	ZEF YOC
32	ZZY YRA

Permutation Cycle Groups for the encryption of character positions 1& 4 [a.k.a **AD**]

Permutation Groups for Characters 1 & 4	Graphic Representation of the Cycles
AUQ AMN	A
	Cycle notation: **(A)**
BCT CGJ CIK BZT	B C
	Cycle notation: **(BC)**
DDB VDV VQZ PVR PVJ FEG FBR KLE KHB XJV XRS GNM GPB ZSV ZEF YOC YPC OSQ OBU DLZ	
	Cycle notation: **(DVPFKXGZYO)**
EJP IPS IKG JKF JWF MIC MAW UXP USE NWH NLU QFZ QGA LYB LDR HDE HNO THD TMN EBY	
	Cycle notation: **(EIJMUNQLHT)**
RFC WQQ WTM RAO	R W
	Cycle notation: **(RW)**
SYX SCW	S
	Cycle notation: **(S)**

Permutation Cycles for the encrypted key character pairs **AD, BE, CF** are:

AD = **(DVPFKXGZYO) (EIJMUNQLHT) (BC) (RW) (A) (S)**

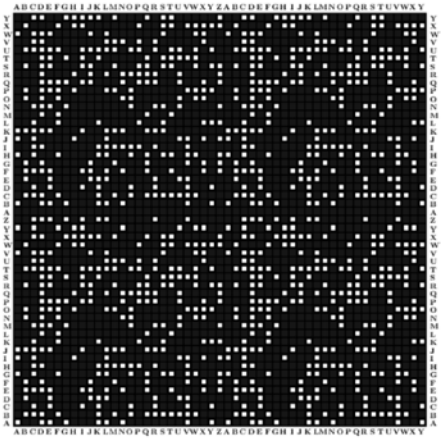
BE = **(BLFQVEOUM) (HJPSWIZRN) (AXT) (CGY) (D) (K)**

CF = **(ABVIKTJGFCQNY) (DUZREHLXWPSMO)**

middle and left rotor configurations. The larger sheet would have a hole punched where a 'female' was present as determined from the rotor wiring patterns. 156 sheets were needed for a 3-rotor set (1,560 for a 5-rotor set).

As discussed, 'females' occur when two encryptions of the same letter are also the same letter, for example **A**UX **A**MN, the two 'A's are encryptions of the same first letter of a duplicated user key. 'Females' occur in pairs, i.e. from our earlier example on the previous page, the second 'female' was from **S**YX **S**CW where the two 'S's are encryptions of the same letter. Therefore the permutations (A) and (D) which includes the 'female' 'A' must also include 'S'.

In the case of rotor configurations that are three positions apart, as when a user key is encoded, the percentage of time a rotor configuration will be a 'female' is about 40%. When a 'female' is found then rotor wiring permutations can be scanned for those that contain the 'female.' Zygalski sheets were a more expedient way to scan rotor wiring permutations. On a light table, sheets were superimposed, added, and adjusted until only one punched hole was visible. When the condition occurred, a start position key could be more easily determined.



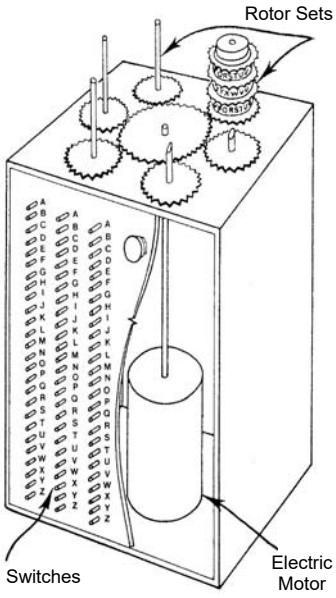
Zygalski Sheet designed by Henryk Zygalski.

The term 'female' came from a play on words; it started as "samiczki" which is Polish for 'The same' — this is phonetically close to "samica" which is Polish for 'female.' The cyclometer was used to find 'females' and earned the nickname 'sex machine.' The team was not without a sense of humor.

To expedite the search for 'females', the team designed the **Bomba** to find rotor positions that contain a 'female' in the rotor wiring configuration. The Bomba was designed to analyze three pairs of rotors at a time, all with the same rotor order. The first pair of rotors were set to the character positions 1 & 4, the second rotor set to positions 2 & 5, and the third set to positions 4 & 6. Rejewski recalled it took about 100 to 120 minutes for the Bomba to do the analysis of one rotor order. When a 'female' was detected, the Bomba would halt enabling the operator to record the rotor position where the 'female' was found. Multiple bomby were constructed to analyze multiple rotor orders in parallel. The Bomba was manufactured by AVO Radio Manufacturing Co.

Why they called it 'Bomba' is not certain. It has been surmised that it may have been the effect it will have on the enemy, or maybe it was the ticking sound that it made, or perhaps it was named after the ice cream Rozycki was eating when it was being designed. All have been suggested.

A reproduction of the Polish Bomba on display at Bletchley Park. A radio of the era is on the shelf to the right. The wall size video displays behind tells the story of the Polish code breaking team.



A sketch of the Polish Bomba drawn by Rejewski from memory.

In December 1938, the Germans had made more changes to Enigma including the addition of two more rotors increasing the rotor set to five. The possibilities of rotor order went from 6 to 60. Procedures to set changed as well.

Pyry forest location near Warsaw of the July 1939 meeting where the Poles shared their cryptographic knowledge, devices, and accomplishments with the French and British.
Source: British Government Communications Headquarters (GCHQ) website.

A meeting between the French, British and Poles occurred in France in January 1939, but the parties kept their cards close to the vest and not much was shared. In July 1939, it was a very different story as a German invasion seemed imminent and unavoidable. A second meeting was held in the Pyry Forest near Warsaw where the Poles shared everything including an Enigma with the French and British teams. The British team included Alastair Denniston, the head of the British Government Code and Cipher School (GC&CS), and Dillwyn "Dilly" Knox, the lead British crypto analyst at GC&CS.

In late 1939 when the German invasion of Poland had begun, the team evacuated south making their way to France where they continued code breaking. Before evacuating they destroyed all they could. They evacuated with remaining equipment including the documentation, Enigmas, and bomby. However, when they were in route, they experienced vehicle problems and were forced to destroy, burn, and bury everything in a remote location believed to be just across the boarder in present day Ukraine.

Breaking the Enigma - British Efforts in WWII (1939-1945)

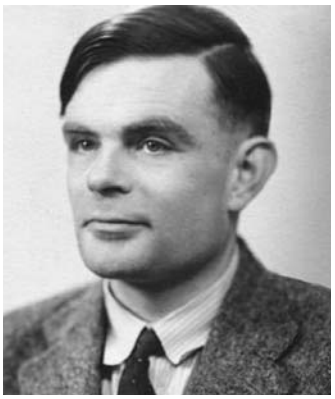
The Government Code and Cipher School (GC&CS) had its beginning as Room 40, located in London, which was the center for code breaking in WWI. In August 1939 it had moved from London to a somewhat more remote Bletchley Park. As mentioned, the head of GC&CS was Commander Alastair Denniston and the lead code breaker was Dillwyn "Dilly" Knox. Both had history dating back to WWI and Room 40. In 1938, Denniston recruited several talented individuals including Alan Turing and Gordon Welchman, both mathematicians from Cambridge.

The staff quickly outgrew the mansion, and many huts were built on the grounds for various purposes. German communications related to Naval activity were handled separately from German Army/Air Force. This was done in part because of the traditional command separation between the British Admiralty and Army, and because the German Navy format of encrypted keys and messages differed significantly from the German Army. Consequently, Huts 3 & 6 processed German Army communications while Huts 4 & 8 processed German Naval communications. Hut 4 did the prioritization, translation, interpretation, cataloging, and dissemination/distribution of Naval communication, while Hut 8 did the code breaking. Hut 4 would received the raw German Naval communications, assess its importance, catalog it, and if needed, send it to Hut 8 for decryption. Once decrypted Hut 8 would return it to Hut 4 for translation, further cataloging, and dissemination as appropriate. Alan Turing became head of Hut 8 and Hugh Alexander served as his deputy. Since Turing's principle focus was on devising methods for code breaking, Alexander was largely responsible for Hut 8 staffing and operations.

Bletchley Park Hut 4 circa 1939. The staff in front are from the GC&CS Naval communications section.
Source: Bletchley Park website

Huts 3 & 6 worked in a similar fashion. German Army communications were processed in Hut 3, while Hut 6 did the code breaking. Peter Calvocoressi was responsible for the Air section of Hut 3. Gordon Welchman was responsible for Hut 6 operations. Welchman was a very capable mathematician and, in his own assessment, excelled at organization and administration.






Left to Right: Commander Alastair Denniston (1881-1961), Alfred Dillwyn "Dilly" Knox (1884-1943), Alan Turing (1912-1954), and Gordon Welchman (1906-1983). Source: Wikipedia

Alan Turing was exceptionally brilliant and proved to be most invaluable. A comment made by Hugh Alexander in his *Cryptographic History of Work on the German Naval Enigma* said of Frank Birch, Head of the German Naval Section in Hut 4, and of Alan Turing regarding the Enigma: "Birch thought it could be broken because it had to be broken. Turing thought it could be broken because it would be so interesting to break it."

This article will focus on the accomplishments of the code breakers in Huts 6 & 8.

The German Enigma machine had evolved since it was broken by the Polish. In 1938, the Enigma rotor set was five from which three would be designated in the key book. By 1940 rotors were changed daily, the number of plug board jumpers increased from 6 to 10. Key formats and procedures were changed as well.

Conel Hugh O'Donel Alexander (1909-1974). Twice the winner of the British Chess Championship, in 1938 and 1956.
Source: Chessgames.com

German Army and Air Force Enigma Code Breaking

According to Gordon Welchman, "there were four distinct phases of Hut 6 activity: preparatory phase, the days of Jeffreys apparatus, the era of Sillies, and the period of Bombes."

The preparatory phase involved recruiting and setting procedures. Recruiting was of the best and brightest, but due to the need for trust, there was a strong preference to recruit those who were known personally. Recruits were almost exclusively men. Code breaking was the work of puzzle masters and out-of-the-box thinkers. The work was stressful, exacting, meticulous, tedious, and time consuming. Much of the work was paper and pencil, trial and error, working alone to tease meaning out of a meaningless jumble encrypted text. They did this 24/7 in three 8-hour shifts.

In the early days in 1939 and until May 1940, one of the Hut 6 code breakers, John Jeffreys created sets of punched sheets styled after the Zygalski sheets. Since the Germans were using 5-rotor sets, 1560 sheets were needed for each set. Creating this sets took a few months. **Jeffreys' sheets** were used in the same manner as Zygalski's sheets to exploit the 'females' found in duplicated user keys.

In May 1940, the German Army and Air Force Enigma stopped use of duplicated user keys and revised their procedure. It utilized a monthly key sheet that listed for each day the selection of three of the five rotors, the order of the rotors, ring settings, plugboard jumper settings, and group ID. The encipherer created a random 3-letter key as the grundstellung that is transmitted in the clear, and a second 3-letter key of their own choosing encrypted by the grundstellung key. Since the key was no longer duplicated, Jeffreys' sheets could no longer be used.

In the interim until the Bombe was operational, the code breakers had to devise techniques to exploit poor habits of operator error and laziness. For example, each operator had to reconfigure his machine at 12am with new settings from the key sheet. To set the rings, the operator held the rotor, released the spring clip, rotated the ring to the correct setting, then closed the spring clip to lock the ring setting, then mounted the rotor into the machine in the correct order. It occurred to Hut 6 code breaker, John Herivel, that when they placed the rotors back into the Enigma, the ring setting would be at or near the top window if user hadn't spun the rotor as he should. In that case, Herivel reasoned some

Geheime Kommandosache!
Nicht ins Flugzeug mitnehmen

Armee-Stabs-Maschinenschlüssel Nr. 28

für Oktober 1944

Nr. 00008

	Datum	Walzenlage	Ringstellung	Steckerverbindungen	Kenngruppen
St	31.	IV V I	21 15 16	KL IT FQ HY XC NP VZ JB SB OG	jkm ogi ncj glp
St	30.	IV II III	26 14 11	ZN YO QB ER DK XU GP TV SJ LM	ino udl nam lax
St	29.	II V IV	19 09 24	ZU HL CQ WM OA PY EB TR DN VI	nci oid yhp nip
St	28.	IV III I	03 04 22	YT BX CV ZN UD IR SJ HW GA KQ	zqj hlg xky ebt
	Date	Rotor Order	Ring Setting	Plugboard Setting	Indicator Group

German Army Staff Enigma settings for the month of October 1944. Note, the dates are in reverse order. To save space, only October 28th through 31st are shown. Source: Cyber Machines and Cryptology website

operators simply used that setting as their first key (the key that was sent in the clear and used to encrypt the second key). To test this, several messages that were the first received that day were analyzed. If some of those messages had this characteristic, then the letters of the first key would cluster around the same letters of the ring setting. This was called "**Herivel's Tip**" and proved to be true in many cases enabling the discovery of the daily ring settings.

Another technique, which has been discussed, was to explore messages for evidence of keys of recognizable patterns or words, like keyboard patterns, successive strokes of the same letter, or familiar words like a girl friend's name, or DOG. They called these "**Sillies**" or "**Cillies**" and were not uncommon. They could be exploited to reveal the message.

German Naval Enigma Code Breaking

At first the German Navy used a similar model of Army Enigma, except they used lettered rotor rings instead of Army numbered rings. In 1941, the Navy adopted a new model of Enigma, the M4 which had four rotors instead of three. To make it fit, they reduced the width of the reflector and made the 4th rotor narrow. The 4th rotor also had two turnover notches causing it to advance more frequently as it was at the slow end of the rotor odometer chain. The rotor sets increased from five to eight, with two of those being versions of the new narrow 4th rotors. Each day the operator had to set the rotor order, ring settings every other day (on paired days), and the grundstellung key and plugboard jumpers were changed each day. Some setting procedures varied for different Naval communication groups.

From 1937, the Navy also utilized a more challenging key structure. The "indicator" procedure was for the operator to choose a trigram (3-letter groups) from a Kenngruppenbuch in the column designated for the applicable column allocated to the operators group (for example 385), choosing say **FFA** from that column. Then a second trigram is chosen at random, say **BGE**. The steps to form the indicator are as follows using the Trigram and Bigram tables below. The Grundstellung key will be the trigram chosen at random **BGE**, and be used to set the rotor positions. The receiving operator reverses the process to decipher the key.

Steps to form the Indicator:

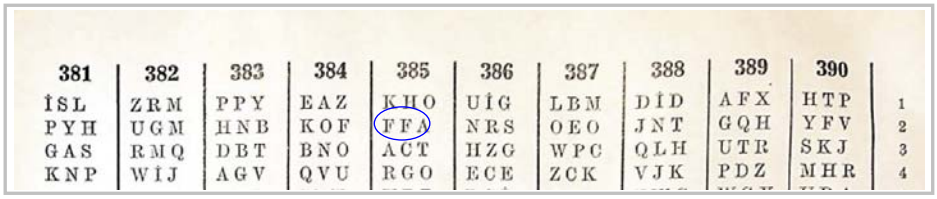
1. Arrange the trigrams with the first over the second and add a blank as the first and last character. → **. FFA BGE .**

2. Select two random letters for the first and last characters, say **A** and **D**. → **AFFA BGED**

3. For each vertical pair. Look up its equivalent in the Bigram Table. For the first pair **AB,** look in the A column down to the B row and find **CH.**

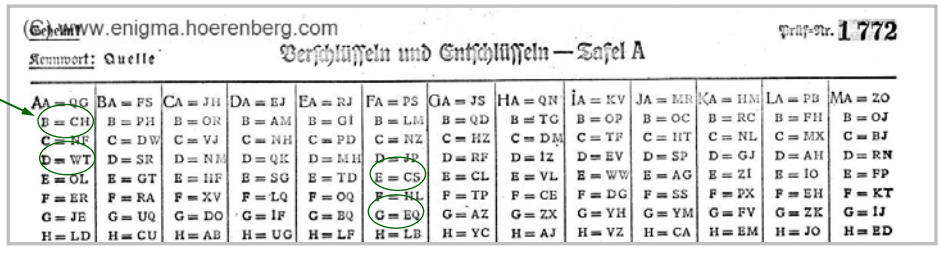
A=CH	F=EQ	F=CS	A=WT
B	G	E	D

4. Arrange the substitute bigrams horizontally and place at the beginning of the message as the indicator groups. → **CHEQ CSWT**



381	382	383	384	385	386	387	388	389	390	
ÍSL	ZRM	PPY	EAZ	KHO	UÍG	LBM	DÍD	AFX	HTP	1
PYH	UGM	HNB	KOF	FFA	NRS	OEO	JNT	GQH	YFV	2
GAS	RMQ	DBT	BNO	ACT	HZG	WPC	QLH	UTR	SKJ	3
KNP	WÍJ	AGV	QVU	RGO	ECE	ZCK	VJK	PDZ	MHR	4

Upper portion of a page from a 1941 German Naval K Book listing random trigrams. A second section of the book had trigrams for various groups.



(C) www.enigma.hoerenberg.com

Geheim! Kennwort: Quelle

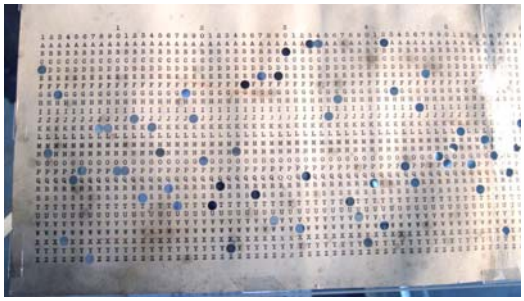
Verschlüsseln und Entschlüsseln — Tafel A

Prüf-Nr. 1772

AA = QG	BA = FS	CA = JH	DA = EJ	EA = RJ	FA = PS	GA = JS	HA = QN	IA = KV	JA = MR	KA = HM	LA = PB	MA = ZO
B = CH	B = PH	B = OR	B = AM	B = GI	B = LM	B = QD	B = TG	B = OP	B = OC	B = RC	B = FH	B = OJ
C = NF	C = DW	C = VJ	C = NH	C = PD	C = NZ	C = HZ	C = DM	C = TF	C = HT	C = NL	C = MX	C = BJ
D = WT	D = SR	D = NM	D = QK	D = MH	D = JB	D = RF	D = IZ	D = EV	D = SP	D = GJ	D = AH	D = RN
E = OL	E = GT	E = HF	E = SG	E = TD	E = CS	E = CL	E = VL	E = WW	E = AG	E = ZI	E = IO	E = FP
F = ER	F = RA	F = XV	F = LQ	F = OQ	F = HL	F = TP	F = CE	F = DG	F = SS	F = PX	F = EH	F = KT
G = JE	G = UQ	G = DO	G = IF	G = BQ	G = EQ	G = AZ	G = ZX	G = YH	G = YM	G = FV	G = ZK	G = IJ
H = LD	H = CU	H = AB	H = UG	H = LF	H = LB	H = YC	H = AJ	H = VZ	H = CA	H = EM	H = JO	H = ED

Upper portion of a page from a book of German Naval Bigram Tables (Doppelbuchstabentauschtafeln). Source: www.enigma.hoerenberg.com

Breaking this double-letter exchange key required a copy of the bigram tables. These tables were changed about once a year. In April 1940 there was a capture of instructions for the indicator system and other documents from the German ship Narvik, (i.e. the Narvik "pinch"). From this the code breakers were successful in partially reconstructing the bigram table. There were other "pinches" in 1940 and 1941 that provided more information leading to the reconstruction of more complete tables. In May 1941, the U-boat U-110 was captured and a complete 4-rotor Enigma set to the day's key plus all the code books and documentation were collected.



Banbury sheet with holes punched in a letter row for each letter of the message. It was thought they were all destroyed but this one was found above the ceiling in Hut 6 in 2014. They could be several feet long and were used to compare text of two messages on a light table. Source: Bletchley Park

Knowing the impact to the Poles when the Germans changed their key structure in 1937 causing them to essentially have to start over, Turing's goal was to develop code breaking methods that were, as much as possible, independent of key structures or specific procedures that the Germans could easily change. Methods he developed were instead designed to attack the content of the message.

One technique Turing developed in 1939 was the **Banburismus** process. Sheets used in the process (above) were called Banburies because they were printed in the town of Banbury. This process exploited a weakness in the indicator procedure where the grundstellung key was the same for all messages on a day. The message indicators produced that day were different for each message, but it was possible that different messages had the same rotor positions part way through the message. Text of messages of at least 200 characters in length from the same day were needed. They were slid horizontally past each other comparing them for letter matches. If the letters were totally random to each other, then one would expect the letter repeat rate to be 1 in 26. But if the repeat rate was found to be more in the range of 1 in 17 as with plain language, it would indicate the messages had a correlation. If by chance character matches were found with 4 or 8 more letters, then that would indicate a "fit." When a strong correlation was found, the difference in position of the messages could indicate the difference in rotation of the rotors that produced them. Once bigram tables were available, this technique, while tedious and time consuming, proved successful and produced decryptions just a few hours after the completion of the day's traffic. This technique was not needed once the Bombes were in full production in 1943. A. Patrick Mahon, who succeeded Hugh Alexander as head of Hut 8 in 1944, wrote, "Banburismus was a delightfully intellectual game."

Banburismus relied on having bigram tables. Until they were available in May 1941, Turing had some success with a method developed by the Poles that involved messages that were sent in two or three parts. The messages would have a header starting with FORT followed by YWEEPYYWEEPY which were encoded numbers that matched the headers in the other parts. At that time the Germans embedded a sequence of numbers between two 'Y's, then used the upper row keys for the numbers. Thus, WEEP would be 2330; this portion of the message would appear as **FORTYWEEPY-WEEPY**, thus the nickname for this technique. In 1938, the Germans changed the format and actually spelled out the numbers (i.e. FORT ZWO DREI DREI NUL) at which point this technique no longer worked. Turing guessed this and went back and investigated old messages and found this to be the case, and again this technique was viable.

Another technique was the creation of the **EINS Catalog**. EINS, the German word for 'ONE', was a word used frequently. The catalog listed the encryption of 'EINS' for all possible 105,456 start positions of 3-rotor machine; a catalog created by hand. The catalog could then be scanned for occurrences of an encoded EINS that match a message; when found, the associated start position could be tested to see if the message could be decoded.

Bletchley Hut 7 became a center for processing Hollerith type punch cards to enable better processing/searching/sorting of high volumes of data. The head of this section was Frederick Freeborn, and Hut 7 was called the "Freebornery." The EINS catalog was punched to cards to enable faster searching and sorting.

One of the small rooms for code breakers that have been recreated in one of the Bletchley Park huts.
Source: Bletchley Park website

Cribs and Bombes

A **Crib** is an educated guess of content that may be contained in the message. German messages were often very structured and used specific phrases. If code breakers knew the message was a weather report, the message may well contain "weather forecast" as is used in the example below.

Sometimes the Germans were "helped" to use specific message content. For instance, messages were being received from a German mine sweeper of the grid locations where Allied mines were found. So Allied mine layers were instructed to lay mines in just a few specific grids. When a mine sweeper messaged the locations of the new mines, the code breakers used the expected grid locations in their crib to retrieve the day's keys.

The German U-boats utilized codebooks that contained codes and abbreviations to shorten the length of messages thus shortening the transmitted signals as a precaution against shore high-frequency direction-finding. The most important codebooks were the short-signal book used for reporting incidents like sighting convoys, and a book for weather reporting. The code breakers had some success recreating the code books and used them in formulating cribs for that signal traffic. Complete codebooks were "pinched" in October 1942 from the captured U-boat U-559.

When at Bletchley Park last Fall, a docent demonstrated to me the use of cribs and the operation of the Bombe (really, really interesting). Since the Enigma can't encrypt a letter as itself, the deciphered message (crib) cannot have a letter that matches the encrypted message. So the crib is shifted right along the encrypted message until a position is found that has no matches between the two. Once found, a "Menu" is mapped between the crib and aligned encrypted text. It is possible that further right-shifts might reveal other alignments and other possibilities to try in the Bombe.

Turing found the more loops (i.e. permutation cycles) the Menu contains, the more likely the Bombe run will produce results with fewer stops. So, ideally cribs needed to be long enough to have multiple loops.

Preparing a Bombe Menu from a Crib

The Crib in this example is WETTERVORHERSAGE which translates to "weather forecast."

Align the Crib under the encrypted message.

Shift the Crib to the right until a position is found that doesn't have any letters of the Crib matching the encrypted text, as is the case when the crib is shifted right by 2.

Encrypted message	Z	W	R	W	I	V	T	Y	R	E	S	X	B	F	O	G	K	U	H	Q
Crib under first character	W	E	T	T	E	R	V	O	R	H	E	R	S	A	G	E				
Crib - shifted right 1 position		W	E	T	T	E	R	V	O	R	H	E	R	S	A	G	E			
Crib - shifted right 2 positions			W	E	T	T	E	R	V	O	R	H	E	R	S	A	G	E		
Crib - shifted right 3 positions				W	E	T	T	E	R	V	O	R	H	E	R	S	A	G	E	

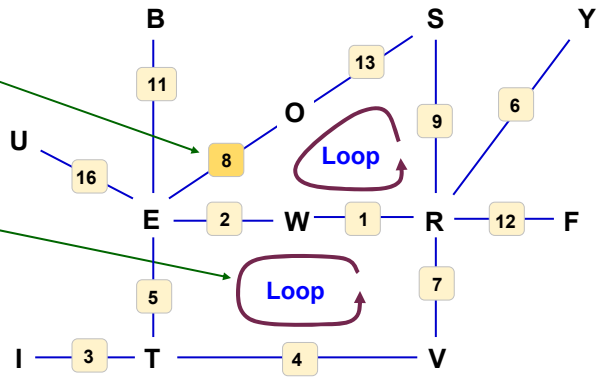
For this alignment of the Crib, map the Crib with encrypted text using relative positions. This is done in a similar fashion as with permutation cycles.

Relative position	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Portion of the encrypted message that aligns with the crib.	R	W	I	V	T	Y	R	E	S	X	B	F	O	G	K	U
Crib - shifted right 2 positions	W	E	T	T	E	R	V	O	R	H	E	R	S	A	G	E

Graphically, this is the result. For example, at position 8 'O' maps to 'E' and, since Enigma is reciprocal, vice versa.

Loops are a closed set of permutations between the encrypted text and Crib, (i.e. a permutation cycle). Loops are desired for Bombe processing, a minimum of two or three loops were needed for an efficient Bombe run (the more, the better). In this loop, E -> W -> R -> V -> T -> E.

The graph was called a Menu. From this, instructions to configure the Bombe for this message would be prepared for the Bombe operator.



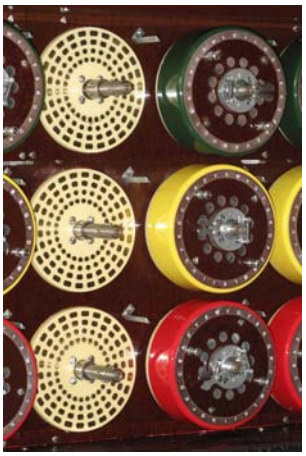
This is a partial example from Graham Ellsbury. The full example with analysis to solve plug board jumpers is at http://www.ellsbury.com/bombe1.htm

Harold Hall 'Doc' Keen circa 1939. He was an engineer with the British Tabulation Machine Co. and translated Turing's design into a working Bombe.
Source: *Harold 'Doc' Keen and the Bletchley Bombe* by John Keen.

Bombe Design

Alan Turing designed the **Bombe** in 1939. He didn't follow the Polish design that relied on the duplicated key. Instead, he intended to design a machine that implemented a logic process in a more general way. Turing retained the Polish name Bomba, anglicized to Bombe. In early 1940, the British Tabulating Machine Co. (BTM) was contracted to build the Bombe. Their lead engineer was Harold 'Doc' Keen who worked closely with Turing to implement his design using similar technology used for Hollerith punch card equipment, in which relays were used as logic elements. The four prototype machines were delivered in August 1940.

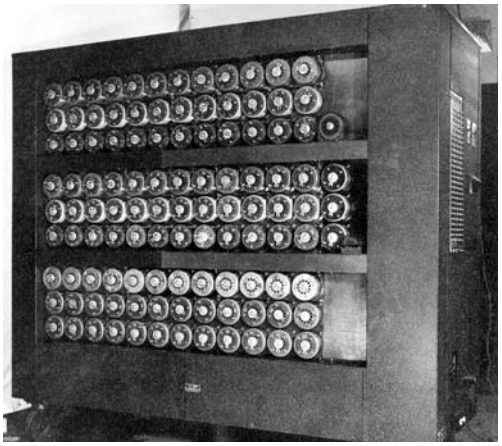
In late 1939, Gordon Welchman suggested an improvement called the diagonal board that implements Enigma's reciprocal encoding. The diagonal board helped reduce the permutations of stecker (plugboard jumper) configurations reducing false stops. It was immediately added to Bombe design. For that improvement, it is called the Turing-Welchman Bombe.



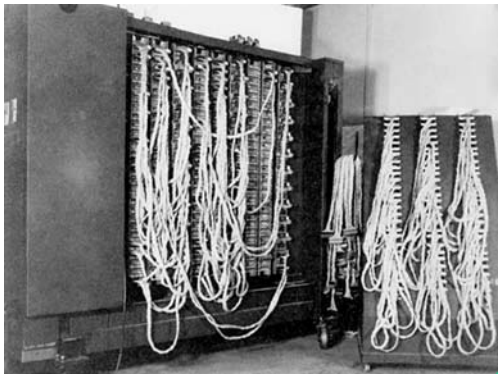
A close-up of a 3-rotor column and of the 4 rings of concentric contacts in the adjacent column of the reproduction Bombe.
Source: Bletchley Park.

The rotors are arranged in 12 columns of 3 rotors. There are three banks of these 36 rotor arrays. In a 3-rotor column, the top rotor corresponds to the right Enigma rotor, the middle to the middle, and the bottom to the left Enigma rotor. When operated, the top rotor spun fastest. On earlier models it rotated at 100 RPM. The speed of the rotors was limited by the response time of the relays.

Rotors are larger than those in the Enigma as they have twice the number of contacts. The contacts are arranged as four concentric circles of 26 contacts each. Each rotor has two identical sets of internal wiring; one set is connected to the outer two rings of contacts, and the second set is connected to the two inner concentric ring contacts. The rotors make connection with wire brushes. There are five Bombe rotors in a set; the wiring of each matches the corresponding rotor in a 3-rotor Enigma set. The rotor double wiring enabled cross-connecting with other rotors in the column.



To prepare for a Bombe run, the operator configures diagonal board cabling according to the Menu. Each column of rotors is configured to have a designated specific position. For instance from the crib example, the fourth rotor column three may be configured to have relative position 8 . The top rotor in that column is advanced forward by that many clicks relative to position 1. Continuing the example, the cabling to one side of this rotor column is to 'E' on the diagonal board and the other is to 'O'. The remainder of the rotor columns are configured in a similar manner. When finished, all the rotor columns included in this run would be set to one of the relative positions of the crib, and be connected to the corresponding letter pair of that position. Because each rotor has two sets of wiring, the total wiring configuration of the closed crib loop cross connects every rotor set. Thus, all of the rotor positions then are evaluated simultaneously.



Turing-Welchman Bombe machine. The front shows the three rows of twelve 3-rotor sets. The rear shows the cables plugged into the Diagonal Board that configured the machine according to a Menu. Each cable contains 26 wires.
Source: Bletchley Park Trust

Once the Bombe run is started, the rotors spin through all 17,456 possible rotor positions. The purpose of the Bombe is to find a rotor position that is logically consistent with the Menu. If a position is detected, the Bombe Stops instantly to freeze that position. In the Bombe demonstration during my visit, the Stop truly was instantaneous. The operator then records the settings for that Stop. The result is then tested on a separate device like a modified Enigma. If the test isn't successful, then the Bombe run is restarted to continue to another Stop.

Enigma like device to test the results of a Bombe Stop. Source: The National Museum of Computing.

Cribs and Bombes became the preferred method of decryption, and in 1942 there was a great effort to scale-up this capability. The first Bombes took 6 weeks for BTM to manufacture; later it took a week. By 1944, about 152 3-rotor Bombes were built.

Bletchley Park, the British Post Office, and British Tabulating Machines designed the 4-rotor. They incorporated vacuum tube thyratron technology enabling the rotor speed to be increased substantially to 1200 RPM, then later to 2000 RPM. The 4-rotor Bombe became available mid 1943. A total of 59 4-rotor Bombes were built.

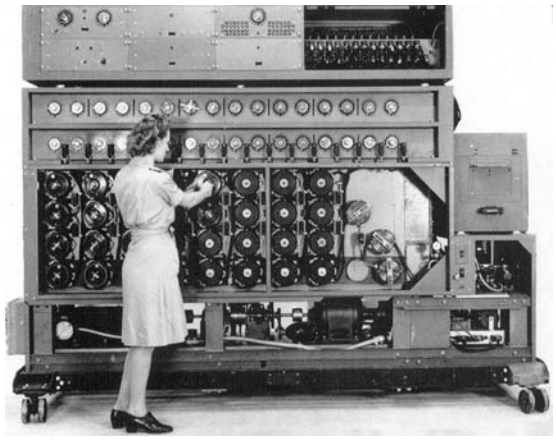
To reduce vulnerability to air attack, Bombe centers were scattered around England in about 30 outstations like Eastcote and Stanmore, and were operated by 800 to 900 WRNS.

A portion of the Bombe outstation at Eastcote. Source: GCHQ.

The United States needed a Bombe capability as well. In 1942, U.S. Naval Operations (OP-20-C) contracted with National Cash Register Co. in Dayton, Ohio to develop and manufacture the Bombe. In December 1942, Turing went the U.S. to OP-20-G as an advisor. The U.S. design also utilized vacuum tube technology for the logic elements and, as a result, performed with very fast rotor speeds. The first units went on-line in April 1943 and were operated primarily by WAVES. By the end of 1943, there were 73 Bombes operating continuously, and at the end of 1944 the United States had 121. The U.S. Army contracted with Bell Laboratories to build 3-rotor Bombes. Their design used Enigma rotors instead of Bombe rotors.

The U.S. and British maintained a secure line between Bombe operations enabling cooperation and workload balancing. At the end of the war all of the U.S. Bombes were destroyed except one that is on display at the U.S. National Cryptologic Museum.

At the end of WWII, all British decryption supplies and equipment were ordered to be destroyed including the Bombes and records of the Bombes original design and operation. In 1994, a group led by John Harper of the BCS Computer Conservation Society formed a team to build a reproduction. The project took 13 years and was installed at the National Museum of Computing in 2018.



U.S. Navy version of the Bombe. Source: NSA

Alan Turing

The success of Ultra was made possible through the remarkable work of many individuals. The contributions of Alan Turing made on code breaking were indispensable and brilliant for which he has been given much credit. In his life, he made many other very significant accomplishments. In 1936, he published his paper "On Computable Numbers, with an Application to the Entsheidungsproblem" in which he proved that a "universal computing machine" (i.e. the Turing machine), is capable of performing any mathematical computation defined as an algorithm. Alonzo Church, for whom Turing was a doctoral student, published a parallel thesis using a different approach with the same conclusion. The two papers are known as the Church-Turing Thesis and is a theoretical cornerstone of Computer Science.

Later in 1944/45, after his work at Bletchley and time as advisor to the U.S. Bombe effort, he was at Hanslope Park designing the 'Delilah' project to encipher speech, a technology in its infancy. Later in 1945, he designed the Automatic Computing Engine at the National Physics Laboratory. He developed software on one of the first stored-program computers, the Mark I. He had an interest in how games might be played with using a computer and continued to do more abstract work in mathematics with an interest in Artificial Intelligence. He devised the Turing Test to assess a machine's attainment of artificial intelligence. He then developed an interest in mathematical biology publishing another paper in 1952 entitled "The Chemical Basis of Morphogenesis." Tragically, he died in 1954 at the young age of 43.

The Impact of Ultra

The achievements of the work done by Y-Service radio and wireless operators, Bletchley code breakers, and follow-on Ultra intelligence groups hastened the end of the war, by some estimates, possibly as much as two years. Specific achievements in code breaking include:

German Army and Air Force Enigma ciphers compromised (adapted from Wikipedia):

Air Force: Although the German army, SS, police, and railway all used Enigma with similar procedures, it was the Air Force (Luftwaffe) that was the first and most fruitful source of Ultra intelligence during the war. The messages were decrypted in Hut 6 at Bletchley Park and turned into intelligence reports in Hut 3. The network code-named 'Red' at Bletchley Park was broken regularly and quickly from 22 May 1940 until the end of hostilities. Indeed, the Air Force section of Hut 3 expected the new day's Enigma settings to have been established in Hut 6 by breakfast time.

Army: In the summer of 1940 following the Franco-German armistice, most Army Enigma traffic was travelling by land lines rather than radio and so was not available to Bletchley Park. The air Battle of Britain was crucial, so it was not surprising that the concentration of scarce resources was on Luftwaffe and Abwehr traffic. It was not until early in 1941 that the first breaks were made into German Army Enigma traffic, and it was the spring of 1942 before it was broken reliably, albeit often with some delay. It is unclear whether the German Army Enigma operators made deciphering more difficult by making fewer operating mistakes.

Abwehr: Dilly Knox's last great cryptanalytical success, before his untimely death in February 1943, was the solving of the Abwehr Enigma in 1941.The Abwehr was the intelligence and counter-espionage service of the German High Command. Interception and analysis of Abwehr transmissions led to the remarkable state of affairs that allowed MI5 to give a categorical assurance that all the German spies in Britain were controlled as double agents working for the Allies under the Double Cross System.

German Naval Enigma ciphers compromised, listed by the Bletchley code name (from Ralph Erskine):

Dolphin: It was used by all U-boats and ships in "home waters" (an area which included the Atlantic) until 5 October 1941 (see Shark). Bletchley broke Dolphin from 1 August 1941 until the end of the war.

Shark: Used by the Atlantic and Mediterranean U-boats from 5 October 1941. Shark used three-rotor Enigma (M3) until 1 February 1942, when it switched to the four-rotor version (M4). Bletchley broke Shark in M3 form. The M4 version was only broken 10 December 1942. From then until the end of August 1943, it was generally broken, but quite often late. From September 1943 onwards, Shark was normally broken within about 24 hours.

Turtle: Used by the Mediterranean U-boats from June 1943 to October 1944. Turtle was broken from June 1943 onwards.

Narwhal: Used by the Northern U-boats based in Norway from 25 June 1944 to the end of the war. Narwhal was broken from September 1944.

Grampus: Used by U-boats in the Black Sea from October 1943 to August 1944. Grampus was broken from October 1943.

Sunfish: Used by supply ships and U-boats in the Far East from September 1941. Sunfish was intermittently broken from August 1943.

Meeting the Imperative

In 1941, there were large unfilled staffing needs for typists and others to decrypt and process the immense message traffic in a timely fashion, however, the requests were ignored at Whitehall. Winston Churchill knew the critical importance of code breaking, and when he visited Bletchley Park in September 1941 he committed that he would give the effort his highest priority. Six weeks later, having failed to get additional staff, Turing, Welchman, Alexander and Milner-Barry wrote directly to Churchill. His response was "Action this day make sure they have all they want on extreme priority and report to me that this has been done." It was done.

In 1939, there was staff of only about 130 at Bletchley Park. In 1945, staffing had increased to 10,000 including the Bletchley and remote Bombe locations. About three-quarters were women.

There was very real personal sacrifice for those recruited on several levels. Many would have rather joined with their mates doing their part in the thick of the action. Many were genuinely conflicted because, as important as this work was, they would have to be isolated and sworn to secrecy — no one including close family or future employers could know of their wartime role and duties both during the war years and for decades after. Secrecy was dutifully maintained until this became public in 1974, only then could their contributions and accomplishments finally be revealed. "Grandma, during the war YOU did WHAT?!"

We are so very fortunate they were willing and able to do it!

Bletchley Park and the British National Museum of Computing very effectively tells this important story of the reality and challenges of this troubled time, the critical importance of radio and communications intelligence, and the dedication of so many unrecognized for their indispensable contributions that made possible expediting the end of this devastating extermination and bloodshed saving so many untold lives and defeating an insane vicious tyranny.

General Heinz Guderian in armored command vehicle with an Engima machine in use. May/June 1940.
Source: NSA from the German Federal Archive

Sources

Alexander, C. Hugh O'D.; *Cryptographic History of Work on the German Naval Enigma*, 1945, British National Archive. **First hand history of Hut 8.**
"Banburismus", Wikipedia.com. **An overview of the Banburismus process**.
Bauer, Craig P.; *Secret History: The Story of Cryptology*, 2 ed. , CRC Press, 2021
Calvocoressi, Peter; *Top Secret Ultra*, 2001, M&M Baldwin **A first hand account of intelligence work done in Hut 3 (Army/Air Force) through WWII.**
Carter, Frank; "From Bombe Stops to Enigma Keys", Technical Papers, Milton-Keynes, Bletchley Park Trust, 8 January 2010
Christensen, Chris; "Polish Mathematicians Finding Patterns in Enigma Messages", Mathematics Magazine, Vol. 8 No. 4, October 2007
Elsberry, Graham; "The Turing Bombe", www.ellsbury.com/bombe1.htm **An excellent discussion of Cribbing, Menus, and Bombe configuration.**
Erskine, Ralph; "Naval Enigma Ciphers", https://uboat.net/technical/enigma_ciphers.htm.
Gilbert Bloch translated by C. A. Deavours; "Enigma Before Ultra Polish Work and The French Contribution". Cryptologia July 1987, Vol. XI No. 3.
Gilbert Bloch translated by C. A. Deavours; "Enigma Before Ultra The Polish Success and Check (1933-1939)". Cryptologia October 1987, Vol. XI No. 4.
Gilbert Bloch translated by C. A. Deavours; "Enigma Avant Enigma Before Ultra". Cryptologia July 1988, Vol. XII No. 3.
Hosgood, Steven; "All You Ever Wanted to Know About Banburismus but were Afraid to Ask", 2008, https://web.archive.org/web/20160309155544/http://stoneship.org.uk/~steve/banburismus.html. **A complete description of the Banburismus process.**
Kahn, David; "An Enigma Chronology"; Cryptologia July 1993, Volume XVII Number 3.
Kahn, David; *The Code Breakers*, 2 ed., Scribner, New York, 1996
Keen, John; Harold 'Doc' Keen and the Bletchley Park Bombe, M&M Baldwin, 2003.
Kruh, Louis and Deavours; Cipher, "The Commercial Enigma: Beginnings of Machine Cryptography", Cryptologia, January 2002, Vol. XXVI, No. 1.
Lee, Bart; *Radio Spies: Episodes in the Ether Wars*, AWA Review, 2007, Vol. 21
Mahon, A.P.; *The History of Hut Eight 1939-1945*, 1945, held by the British National Archive. **First hand history of Hut 8 (Naval).**
Miller, A. Ray; "The Cryptographic Mathematics of Enigma", Center for Cryptologic History National Security Agency, 2019.
Perera, Tom; *Inside Enigma: The Secrets of the Enigma Machine and other Historic Cipher Machines*, 2nd ed., Radio Society of Great Britain, 2019.
Pidgeon, Geoffrey, *The Secret Wireless War: The Story of MI6 Communications 1939-1945,* Arundel Books, 2018
Rejewski, Marian; "Mathematical Solution of the Enigma Cipher", Cryptologia, January 1982, Vol. 6 No. 1
Turing, Alan; *The Prof's Book: Turing's Treatise on the Enigma*, late 1940; Public Domain, reprinted by Kronecker Wallis, 2021.
Turing, Durmot; *XYZ: The Real Story of How the Enigma Was Broken,* History Press, 2018 An account of the
Welchman, Gordon; *The Hut Six Story: Breaking the Enigma Codes*, McGraw-Hill Book Co., 1982. **First hand history of Hut 6 (Army/Air Force).**
Wilcox, Jennifer; "Solving the Enigma: History of the Cryptanalytic Bombe", Center for Cryptologic History, NSA, 2015

A wealth of detailed information is available at these Websites:
Perera, Tom; Website: **EnigmaMuseum.com**.
Reavers, Paul and Simon; Marc, Website:**CryptoMuseum.com.**
Rijmenants, Dirk; Website: **CipherMachinesAndCryptology.com**.
Simpson, Ralph; Website: **CipherMuseum.com**.
Weierud, Fred; Website: **CryptoCellar.org**.
Wikipedia.com; various topics.

◊

Lots going on at CHRS!


Scott


Giuliana


Bart


Steve


Denny and John


Jon

Jeff