Paper Cipher Machines and the Cryptanalytic Methods of U.S. Coast Guard Cryptanalytic Unit 387, 1940–1945

A Historical and Technical Analysis of Pencil-and-Paper Rotor Emulation

April 2026

Abstract

This paper examines the development, operational use, and cryptanalytic significance of hand-drawn paper cipher machines employed by the United States Coast Guard Cryptanalytic Unit 387 during the Second World War. Between 1940 and 1945, Unit 387 intercepted more than 10,000 encrypted clandestine messages from 65 German Abwehr radio circuits operating across the Western Hemisphere and decoded approximately 8,500 of them. Because the clandestine Abwehr networks employed a variety of modified commercial Enigma variants that differed from the high-volume military Enigma targeted by electromechanical Bombes at Bletchley Park and OP-20-G, Unit 387 developed a portable, paper-based rotor emulation technique. This paper describes the technical basis of that technique, the cryptanalytic workflow it supported, the specific Abwehr Enigma variants it was used against, the transatlantic partnership with British intelligence that made it possible, and the unit's broader contribution to Allied signals intelligence in the Western

Hemisphere. The paper draws on declassified primary sources including the unit's own technical history, personnel records, and contemporary memoranda now available through the National Archives and the Internet Archive.

1. Introduction

The history of Allied signals intelligence in World War II is dominated by the story of Bletchley Park, the British codebreaking center in Buckinghamshire that industrialized the decryption of German Enigma traffic using electromechanical devices known as Bombes. Less well known, but operationally significant, is the parallel effort carried out by a small American unit operating under the United States Coast Guard: Cryptanalytic Unit 387, also known as Unit 387 or, after its absorption by the Navy, OP-20-GU and subsequently OP-G-70.

Unit 387's distinctive contribution was not the development of new electromechanical cryptanalytic machinery. It was the opposite: the systematic use of hand-drawn paper representations of cipher machine rotor wirings, manipulated manually by skilled analysts to decrypt German intelligence traffic. These paper instruments allowed a small team, working without industrial resources, to penetrate Abwehr clandestine radio circuits that no Bombe was ever assigned to attack.

This paper reconstructs the technical basis of Unit 387's paper cipher approach, traces its development from the unit's Prohibition-era pencil-and-paper tradition through its wartime

application against modified Enigma variants, and situates it within the broader Allied cryptanalytic partnership of the Second World War.

2. Background: The U.S. Coast Guard Cryptanalytic Unit

2.1 Origins and Founding

Unit 387 was founded in 1931 by Elizebeth Smith Friedman (1892–1980), appointed Cryptanalyst-in-Charge, who recruited and trained its initial personnel. The unit had its roots in the Coast Guard's Prohibition-era intelligence work. Between 1927 and 1930, Friedman and a single assistant decoded more than 12,000 shortwave radio messages transmitted by rum-running networks coordinating illegal liquor shipments along the Atlantic and Pacific coasts, all by hand, using pencil and paper against dozens of distinct cipher systems. [1]

This sustained pencil-and-paper cryptanalytic discipline, developed against real operational traffic under genuine time pressure, built the methodological foundation that would later be applied to German military communications. The experience of attacking many small, varied cipher systems with manual techniques translated almost directly to the challenge posed by the Abwehr's clandestine networks. [2]

By 1938, Secretary of the Treasury Henry Morgenthau had tasked the unit with tracking non-neutral communications in preparation for potential American involvement in the European conflict. In 1939 the Coast Guard operated a High Frequency Direction Finding (HF/DF) network of 20 primary and 9 secondary stations spanning the continental United States, supplemented by

mobile direction-finding equipment in cutters, trucks, and portable cases — capabilities first developed during the Rum War. [3]

2.2 Wartime Mission and Scale

Starting in 1940, Unit 387 assumed primary responsibility for monitoring the clandestine radio communications of German intelligence agents throughout the Western Hemisphere. Its decrypts were circulated to the Army, Navy, FBI, and British intelligence. [4]

The unit grew from two people at its Prohibition-era peak to approximately 150 personnel by the end of the war. In 1941 it was formally absorbed by the U.S. Navy and redesignated OP-20-GU, and later OP-G-70, under the command of Lieutenant Leonard T. Jones, with Friedman continuing as ranking civilian cryptanalyst. [5]

Friedman described herself with characteristic understatement as simply “one of the workers.” In practice she was the technical spine of the unit. By war's end, the unit had intercepted communications from 65 German clandestine circuits, decrypting approximately 8,500 of the roughly 10,000 messages intercepted — a penetration rate of approximately 85 percent.

3. The Abwehr Cipher Problem

3.1 The Abwehr and Its Communications

The Abwehr, Germany's military intelligence and counterintelligence organization, maintained a large network of agents and station chiefs across Mexico, Central America, and South America throughout the war. These operators communicated with control stations in Hamburg and Berlin via shortwave radio. Unlike the Wehrmacht, Luftwaffe, and Kriegsmarine, which used the

standard military Enigma with a plugboard (Steckerbrett), Abwehr agents used a family of modified commercial Enigma variants, primarily the Enigma G (also designated Abwehr Enigma), which lacked a plugboard but incorporated several mechanical differences that complicated cryptanalysis. [6]

The Enigma G used four rotors, had multiple notches on each rotor rather than a single notch, and included a counter mechanism that incremented with each keypress. Crucially, its reflector was not fixed but was advanced by the stepping mechanism after being set by hand to a starting position — a configuration that differed fundamentally from the Wehrmacht and Navy models and required independent cryptanalytic approaches. [7]

Beyond the mechanical differences, individual Abwehr circuits employed distinct rotor wirings, different reflectors, different notch patterns, and in some cases additional modifications. Unit 387 ultimately dealt with at least four major cipher variants across 65 circuits: the Green Enigma, the Red Enigma, the Berlin-Madrid Machine, and Stecker-variant circuits including the Hamburg-Bordeaux codes.

3.2 Why No Bombe Was Available

By the spring of 1944, OP-20-G was operating 96 electromechanical Bombes, running around the clock against German naval Enigma traffic. Bletchley Park eventually operated more than 200 Bombes. But these resources were entirely committed to high-volume military traffic: U-boat communications, Luftwaffe tactical messages, Wehrmacht ground force orders. [8]

The clandestine Abwehr traffic intercepted by Unit 387 presented a fundamentally different operational picture. Individual circuits transmitted one to five messages per day. The cipher configurations changed frequently and differed between circuits. Running a Bombe against a

handful of daily intercepts from a single spy network in Rio de Janeiro or Buenos Aires was economically and logistically impractical. The paper approach was not a fallback — it was the correct engineering response to the problem's structure.

Three factors made paper the right solution. First, recovered rotor wirings are simply letter-substitution tables that can be written on paper. Second, the low message volumes did not justify electromechanical infrastructure. Third, the target diversity — 65 circuits with different configurations — required a system that could be rapidly reconfigured, which a folder of paper strips could accomplish in minutes.

4. Technical Basis of the Paper Cipher Machine

4.1 Recovering Rotor Wirings from Depth

The cryptanalytic prerequisite for any paper cipher machine was the recovery of the actual rotor wirings used by the target circuit. This was accomplished through depth analysis — the cryptanalytic attack on multiple messages enciphered at the same starting position. [9]

In January 1940, Unit 387 intercepted a series of messages from suspicious circuits transmitting one to five messages per day, initially of unknown language and cipher type. Once sixty to seventy messages had accumulated, analysts determined the language was German and the cipher was likely a commercial Enigma variant. The diagnostic marker was the observation that no plain letter was represented by itself in the ciphertext — a fundamental property of Enigma machines, arising from the reciprocal reflector design that prevents any letter from encrypting to itself. [10]

The unit possessed a commercial Enigma machine and its manufacturer's instructions. But the Germans never used stock commercial Enigma: they modified wirings, added notches, and changed reflectors. So the unit's task was to cryptanalytically recover all of those modifications from traffic alone, using depth. Messages in flush depth — correctly superimposed at the same starting point in the key — yield cipher alphabets for each rotor position that, when analyzed statistically and algebraically, allow the substitution tables to be reconstructed letter by letter.

Once recovered, a rotor wiring is nothing more than a permutation of 26 letters: a table mapping each input letter to an output letter through the rotor's internal wiring. Such a table can be written by hand on a strip of paper, one column per rotor position. That is the paper machine.

4.2 The Paper Strip Architecture

A completed paper cipher folder represented a single Abwehr circuit's complete cipher configuration for a given period. The folder contained three main strips, one per rotor, each consisting of 26 rows representing the 26 possible positions of that rotor as it stepped through a message. Each row showed the letter-to-letter substitution table for that rotor at that position. A separate lookup table at the edge of the folder represented the reflector.

The strips were hand-drawn with steel-nib pens by Unit 387 analysts. The red pencil marks visible on surviving folders represent the current day's starting positions, updated as key settings changed. Ink corrections, pencil smudges, and erasures on surviving documents confirm these were operational working instruments, not archival reference materials.

Color-coded tabs — GGG RED, GGG BLUE, GGG GREEN — allowed an analyst to retrieve the correct folder from a filing cabinet in seconds during an operational shift. Each color designation corresponded to a specific circuit or configuration variant.

Archival stamps reading “FILED” along with file numbers such as F-3591 and S-3591 are post-war National Archives accession marks, added when the folders were transferred from OP-G-70 custody to the Navy historical collection in the 1950s and 1960s. A margin annotation reading “checked 2-G by analysis” on surviving GGG folders is an authenticity note from a Unit 387 analyst confirming that the wirings on that folder matched the OP-20-G (the Navy's cryptanalytic section) reference solution — evidence of the cross-validation process between the Coast Guard and Navy partnerships.

4.3 The Decryption Workflow

An analyst's operational workflow proceeded as follows. An intercept arrived from one of the HF/DF listening stations. Traffic analysis identified which circuit it was from, using call signs, preamble formats, and transmission timing patterns. That identification determined which folder to retrieve.

The analyst opened the folder to the current day's rotor settings, derived from captured key sheets, cryptanalytic breaks, or systematic guesswork. Using the benchmark — the red pencil line indicating the day's starting position — the analyst aligned the strips. For each ciphertext letter, the analyst traced the signal path: input letter down the left column of the first strip, across through the three rotor columns, to the reflector lookup table, back through the strips in reverse, out to the right column as the plaintext letter.

After each letter was processed, the rightmost strip advanced one row, simulating the rightmost rotor's step. When that strip crossed its notch position, the middle strip advanced one row. This mechanical progression replicated the Enigma's characteristic rotor stepping behavior.

A skilled operator could process approximately 20 to 30 letters per minute — slow by electromechanical standards, but entirely sufficient for the message volumes Unit 387 encountered. The entire cryptanalytic capability for a given circuit could be carried in a standard briefcase, a portability that had no electromechanical equivalent.

5. The GGG Enigma and the Transatlantic Intelligence Partnership

5.1 The British Break

The Allied approach to the Abwehr Enigma began at Bletchley Park under Dilly Knox and his small team, which included Mavis Lever (later Batey) and Margaret Rock. The Abwehr machine had proved difficult because its irregular rotor stepping — with multiple notches creating unpredictable advancement patterns — made cycle analysis far more complex than for the standard military Enigma. [11]

On December 8, 1941, Lever broke a message on the link between Belgrade and Berlin, enabling the reconstruction of one of the machine's rotors. Within days Knox's team had broken into the Abwehr Enigma. Shortly afterward, Lever broke a second Abwehr machine, designated GGG by the Allies. This was primarily the Iberia circuit — Berlin-Madrid-Lisbon traffic handling Abwehr operations against Britain — not, as some sources loosely describe it, a machine “used near the Spanish border.” [12]

Bletchley Park's section that solved the spy Enigmas was known as ISK (Intelligence Service Knox). Its American counterpart was Unit 387. The two sections worked independently

and arrived at solutions around the same time, cross-validating through exchanges of intercepts and solutions. [13]

5.2 The Coast Guard's South America Application

Once the British had passed the GGG solution to Unit 387, the Americans applied the recovered wirings to their own intercepts. Between October and December of the year of the break, the unit intercepted 28 messages exchanged between stations designated TQI2 and TIM2. Traffic analysis indicated TQI2 was in Europe and TIM2 was in South America. [14]

Applying the cryptanalytic techniques refined against the commercial Enigma and the new methods received from the British, Unit 387 decoded those 28 messages and confirmed they were communications between Berlin and Argentina. This was the Green Enigma break. The unit determined the wheel motion patterns and monthly ring settings from the decrypts, confirmed in January 1943, and further validated by Berlin-Argentina messages in June and July of that year. [15]

Following the Green Enigma break, subsequent successes followed: the Red Enigma, the Berlin-Madrid Machine, and several Stecker-variant circuits including the Hamburg-Bordeaux codes. Each success produced new paper folders. A November 1943 intercept decoded on the Green Enigma contained the revealing message: “THE TRUNK TRANSMITTER WITH ACCESSORIES AND ENIGMA ARRIVED VIA RED. THANK YOU VERY MUCH. FROM OUR MESSAGE 150 WE SHALL ENCIPHER WITH THE NEW ENIGMA. WE SHALL GIVE THE OLD DEVICE TO GREEN. PLEASE ACKNOWLEDGE BY RETURN MESSAGE WITH NEW ENIGMA.” This and similar intercepts provided operational insight into the Germans' own cipher management practices. [16]

5.3 The GGG Folder Nomenclature

The “GGG” designation in surviving folder names was the Allied codename for the specific Abwehr Enigma variant used on the Iberia circuit. Color suffixes — RED, BLUE, GREEN — referred to configuration variants or key periods within that circuit designation, not to separate machines. The “A-1214” designation visible on other surviving folders followed the standard OP-20-GU internal notation: the “A” prefix indicated Abwehr, and the number was the circuit's internal register designation.

Other folder designations — 3-Nan, Group II, Y-J — were operator shorthand for specific rotor configuration sets the Germans cycled through on different days. The notation “TWIST-FREE” on certain folders referred to machines without the “Uhr” plugboard randomizer attachment used on some later Abwehr variants. “OLD STYLE 1-NAN” designations identified superseded wirings retained because backlogs of captured messages from before the key change still required decryption.

6. Operational Significance

6.1 Intelligence Outcomes

The operational consequences of Unit 387's work were strategic. The unit's decrypts of Abwehr traffic across the Western Hemisphere revealed the structure, personnel, and communications of the Nazi spy network operating throughout Latin America. Biographer Jason Fagone has described Friedman as the nemesis of Johannes Siegfried Becker (codename “Sargo”), the SS agent who headed the South American operation and used two Enigma machines to communicate with Germany. [17]

The direct political consequence of Unit 387's success in breaking the South American Abwehr networks was the rupture of those networks' operational effectiveness. Following the intelligence derived from these decrypts, Argentina, Bolivia, and Chile severed their relationships with the Axis powers and aligned with the Allies. [18]

At the strategic level, Unit 387's decrypts were shared with the Army, Navy, FBI, and British intelligence. The unit appeared in cables between Bletchley Park and Washington as the American counterpart to ISK, and the intelligence products of both sections were treated as equivalent sources within the Allied signals intelligence framework. [19]

6.2 The Paper Machine as a Model for Low-Volume SIGINT

The paper cipher machine technique represents a solution to a specific signals intelligence problem that recurs whenever a target population uses diverse, low-volume cipher systems that do not justify dedicated electromechanical infrastructure. The economic logic that made paper the correct approach for Unit 387 in 1940 is structurally identical to the logic that governs resource allocation in modern SIGINT contexts: the marginal cost of a cryptanalytic capability must be commensurate with the intelligence value and volume of the traffic it addresses.

Bletchley Park's Bombes were optimized for a specific cipher system at massive scale. Unit 387's paper machines were optimized for variety at small scale. The two approaches were not competitors but complements, each appropriate to its target set.

7. Institutional Erasure and Posthumous Recognition

Despite the breadth and consequence of her contributions, Elizebeth Friedman received almost no official recognition during her lifetime for her wartime work. The Unit 387 history remained classified for 62 years, until 2008. Her name never appeared on official wartime memoranda; only her initials “ESF” at the bottom of Coast Guard decrypts alerted later scholars to her role. Lieutenant Commander Leonard T. Jones received numerous awards for the unit's work, including the Legion of Merit and the Order of the British Empire. Friedman received a salary increase from $4,200 to $5,390. [20]

None of her obituaries upon her death in 1980 mentioned her codebreaking work. She spent her final years beginning her memoirs and organizing her papers, which were donated to the George C. Marshall Foundation Library in Lexington, Virginia, where they remain the principal archival source for research on Unit 387. [21]

Scholarly and public recognition came primarily after declassification. Jason Fagone's 2017 biography *The Woman Who Smashed Codes* (HarperCollins, 2017) brought Friedman's story to a broad audience. In 2022, the United States Coast Guard named the eleventh Legend-class National Security Cutter (WMSL-760) in her honor. The National Cryptologic Museum at Fort Meade maintains a section dedicated to her contributions. [22]

8. Archival Status of Primary Sources

The primary documentary record for Unit 387 is distributed across several repositories. The unit's technical history, written by Jones and Friedman in October 1943 and revised at war's end in 1945, is now fully declassified and available through the Internet Archive. The 1944 memorandum to OP-20-G describing the unit's accomplishments, authored by Jones, is also available through the

Internet Archive. Friedman's government personnel file, covering her work for the Army, Navy, Treasury, Coast Guard, and International Monetary Fund between 1921 and 1946, is likewise available through the Internet Archive.

The physical paper cipher folders — the hand-drawn operational instruments described in this paper — are distributed between the National Archives and Records Administration and the National Cryptologic Museum at Fort Meade, Maryland. The George C. Marshall Foundation Library in Lexington, Virginia holds Elizebeth and William Friedman's personal and professional papers, including materials unavailable in the official government record.

The post-war archival stamps on surviving folders (National Archives accession marks added during the 1950s and 1960s transfer from OP-G-70 custody) are legible on the physical documents and confirm the chain of custody from the operational unit through the Navy historical collection to the current archival repositories.

9. Conclusion

The paper cipher machines of U.S. Coast Guard Cryptanalytic Unit 387 represent a distinctive and historically underappreciated contribution to Allied signals intelligence in the Second World War. They were not primitive stopgaps but technically correct solutions to a well-defined operational problem: how to read a large number of diverse, low-volume cipher systems without electromechanical infrastructure, using analysts trained in manual cryptanalytic techniques developed over a decade of Prohibition-era pencil-and-paper work.

The technique required three prior conditions: the cryptanalytic recovery of rotor wirings through depth analysis, the translation of those wirings into portable paper strip form, and the development of an operational workflow that could process a message one letter at a time by manual rotor emulation. Unit 387 achieved all three, developed the workflow independently from the British, and maintained productive intelligence exchange with Bletchley Park's ISK section throughout the period.

The result was the penetration of 65 German clandestine radio circuits, the decryption of approximately 8,500 messages, the destruction of the Abwehr's South American spy network, and the strategic alignment of three Latin American nations with the Allied cause — all accomplished with folders of hand-drawn paper strips, pencil, and careful bookkeeping.

These instruments are, in a meaningful sense, the last major operational use of hand cryptanalysis in American signals intelligence before the machines took over completely. The surviving folders in the National Archives and the National Cryptologic Museum are not merely artifacts of a particular war. They are the terminus of a cryptanalytic tradition that stretches from the ancient world to the age of electromechanical computing, ending quietly in a filing cabinet at OP-G-70, sometime in 1945.

References

[1] Eleventh National Security Cutter Named for Elizebeth Smith Friedman. United States Coast Guard. https://content.govdelivery.com/accounts/USDHSCG/bulletins/293c4ec

[2] Jones, Leonard T.; Friedman, Elizebeth S. (1945). *History of Coast Guard Unit 387 (Cryptanalytic Unit), 1940–1945*. National Archives and Records Administration. Available via Internet Archive: https://archive.org/details/HistoryOfCoastGuardUnit387

[3] The TOP SECRET story of Coast Guard code breaking. United States Coast Guard Compass (official blog), August 8, 2016. https://coastguard.dodlive.mil/2016/08/the-top-secret-story-of-coast-guard-code-breaking/

[4] Memorandum to OP-20-G on Clandestine Radio Intelligence (1944). Lt. Leonard T. Jones, U.S. Coast Guard. Internet Archive: https://archive.org/details/MemorandumToOP20GClandestineRadio/mode/1up

[5] United States Coast Guard Unit 387 Cryptanalysis Unit. Wikipedia. https://en.wikipedia.org/wiki/United_States_Coast_Guard_Unit_387_Cryptanalysis_Unit

[6] Enigma machine. Wikipedia. Section: Abwehr Enigma. https://en.wikipedia.org/wiki/Enigma_machine

[7] Cryptanalysis of the Enigma. Wikipedia. Section: Abwehr Enigma. https://en.wikipedia.org/wiki/Cryptanalysis_of_the_Enigma

[8] Mowry, David P. *German Cipher Machines of World War II*. National Security Agency Center for Cryptologic History. Available: https://www.nsa.gov/portals/75/documents/about/cryptologic-heritage/historical-figures-publications/publications/wwii/german_cipher.pdf

[9] Jones, Leonard T.; Friedman, Elizebeth S. (1945). *History of Coast Guard Unit 387*, op. cit. See also: United States Coast Guard Unit 387 Cryptanalysis Unit, Wikipedia, op. cit.

[10] United States Coast Guard Unit 387 Cryptanalysis Unit. Wikipedia, op. cit.

[11] Mavis Batey. Wikipedia. https://en.wikipedia.org/wiki/Mavis_Batey

[12] Mavis Batey. Spartacus Educational. https://spartacus-educational.com/Mavis_Batey.htm See also: Mavis Batey. World War II Database. https://ww2db.com/person_bio.php?person_id=1122

[13] Elizebeth Smith Friedman. Wikipedia. https://en.wikipedia.org/wiki/Elizebeth_Smith_Friedman

[14] United States Coast Guard Unit 387 Cryptanalysis Unit. Wikipedia, op. cit. (Green Enigma section).

[15] Ibid.

[16] United States Coast Guard Unit 387 Cryptanalysis Unit. Wikipedia, op. cit. (November 1943 intercept).

[17] Fagone, Jason. *The Woman Who Smashed Codes.* New York: HarperCollins, 2017. Cited in: Elizebeth Smith Friedman. Wikipedia, op. cit.

[18] Elizebeth Smith Friedman. Wikipedia, op. cit.

[19] Elizebeth Smith Friedman. Wikipedia, op. cit. See also: Memorandum to OP-20-G, op. cit.

[20] Smith, G. Stuart. *A Life in Code: Pioneer Cryptanalyst Elizebeth Smith Friedman.* Jefferson, NC: McFarland & Company, 2017. Cited in: The Mother of Cryptology. *Naval History Magazine,* April 2022. https://www.usni.org/magazines/naval-history-magazine/2022/april/mother-cryptology

[21] Elizebeth Smith Friedman Personnel File. National Personnel Records Center. Internet Archive: https://archive.org/details/ESFPersonnelFile

[22] Eleventh National Security Cutter Named for Elizebeth Smith Friedman. United States Coast Guard, op. cit. See also: The Long Blue Line: Mrs. Friedman—the Coast Guard's "Cryptologist-in-Charge" and NSC namesake. United States Coast Guard History, February 2022. https://www.history.uscg.mil/Research/THE-LONG-BLUE-LINE/

Submitted for scholarly use. April 2026.

U.S. COAST GUARD CRYPTANALYTIC UNIT — OP-20-GU
ENCRYPTED MESSAGE TRANSMISSION

TOP SECRET — ULTRA — DECLASSIFIED 2008 — NSA CRYPT HERITAGE COLLECTION

FROM:	T. FRIEND
DATE:	20 APRIL 2026 / 2026-04-20
CIRCUIT:	GGG RED #3 [FOLDER F-3591]
VARIANT:	GGG PAPER MACHINE — COAST GUARD
ROTORS:	I II III (LEFT TO RIGHT / SLOW TO FAST)
REFLECTOR:	REFLECTOR B
RING SETTINGS:	A A A
START POSITION:	A A A
MSG LENGTH:	75 LETTERS
INDICATOR:	GGG / RED / BENCH MARK: ROW A

PLAINTEXT:

HELLO WORLD IHOPE YOUFO UNDTH EPAPE ROFIN TERES TTOMF RIEND
APRIL TWOTH OUSAN DTWEN TYSIX

"Hello World. I hope you found the paper of interest. Tom Friend. April Two Thousand Twenty Six."

CIPHERTEXT:

MFNCZ BBFZM ESQGC NEBTS JDSKB
JNXOH TJQBV BKGDP GOPQV TPWUM
YFBJU ZHZJT UGTSB UYBHU XFBVI

TO DECRYPT: Set GGG Paper Machine to Rotors I-II-III, Reflector B, Ring Settings AAA, Start Position AAA. Type each ciphertext letter in sequence. The plaintext will emerge letter by letter. Simulator available at the ESF memorial page. This message was encrypted using the same rotor wirings hand-drawn by analysts of U.S. Coast Guard Cryptanalytic Unit 387, 1940-1945.

checked 2-G by analysis

F-3591 / S-3591 / FILED