This Document is the property of the United States Government and may not be used for other than official purposes. NSA/CSS Regulation No. 60-7
10 December 1974

Declassified and approved for release by NSA on 09-13-2013 pursuant to E.O. 13526

REF ID:A273704

Pls ok
Return to
Mr Friedman

Op-20-S-5

30 October 1943

~~SECRET~~

HISTORY OF INVENTION AND DEVELOPMENT OF THE MARK II ECM

From the Cryptologic History Collection
Date 7/18/78
W.F.F.

REF ID:A273704

I N D E X

REF ID:A273704

In reply refer to Initials and No.

Op-20-S-5

~~SECRET~~

NAVY DEPARTMENT
OFFICE OF THE CHIEF OF NAVAL OPERATIONS
WASHINGTON

MEMORANDUM FOR OP-20.

Subj: History of Invention and Development of the Mark II ECM.

1. The Mark II ECM is in the direct line of evolution of the Hebern Cipher Machines and Mark I ECM, and incorporates cryptographic principles and mechanical features found in these machines. Its development covered a period of twenty years (1921-1940, incl.) and was sponsored and financed by the Navy Department. Our records show development costs as follows:

Machine	Years	Total Cost
Hebern Cipher Machines	1921-1932 (incl.)	$ 57,360.00
Washington Navy Yard Models	1930-1940 (incl.)	24,000.00
Mark I ECM (Teletype Corp.)	1934	50,000.00
Mark II ECM (Teletype Corp.)	1937-1940 (incl.)	122,000.00
TOTAL	1921-1940 (incl.)	$253,360.00

This represents a development cost of slightly over $25 per machine, on the basis of the 10,060 Mark II ECMs now built and on order, or authorized.

2. The present status of the Mark II ECM is as follows:

Status	Navy Machines	Army Machines	Total Machines
Delivered to date	3,370	1,180	4,550
Due on order	3,380	642	4,022
Contracts being negotiated	—	1,488	1,488
TOTAL	6,750	3,310	10,060

The Army obtained its first 322 ECMs by requisitions on the Navy Department. Subsequent Army machines were procured directly from the Teletype Corporation on independent contracts, in compliance with BuShips 2nd Endorsement, Serial 1471, of 8 September 1941.

SECRET

3. The Mark II ECM (CSP 888-889) was made effective as the Navy's primary cryptographic system, as follows:

Atlantic Waters	—	July 1, 1941
Joint Army-Navy	—	August 1, 1941
Asiatic Waters	—	November 20, 1941
Pacific Waters	—	January 10, 1942
World Wide	—	January 10, 1942

The CCM (modified ECM (CSP 1600 and 1700) became effective between the U.S. and Canadian Navies on October 1, 1943. It will become effective between the U.S. and British Navies about December 1, 1943, and for Combined (U.S.-British; Army-Navy-Air Force) use about July 1, 1944.

4. Secret patent applications for the Mark II ECM, being prepared by the Office of the Judge Advocate General, include the following items:

(a) Invented by Lieut. Comdr. Donald W. Seiler while serving at the Washington Navy Yard.
- (1) "Index Maze."
- (2) Circuits (and resistances) for 115-volt DC, 115-volt AC, or 24-volt DC (battery) operation - at option.
- (3) Emergency Hand Drive Gear.
- (4) Automatic Word Spacer, wherein "Z" is substituted for "space" and "X" for "Z" upon encipherment; and "space" prints as "space" and "Z" as "X" on decipherment.
- (5) "Zeroizer Switch."

(b) Invented by Captain Laurance F. Safford, Navy Department.
- (1) "Stepping Circuits" with the grouping of end contacts in the "Stepping Maze" and in "Index Maze," the utilization of 30 out of 32 possible stepping combinations in the "Alphabet Maze," and any variations thereof.
- (2) Three-way "Plain-Encipher-Decipher" Gang Switch.
- (3) Code-wheel Setting Circuits (involving the "Zeroizer Switch").
- (4) "Zeroizing Circuits" (involving the "Zeroizer Switch").

(c) Invented by the Teletype Corporation.
- (1) Printer.
- (2) Triggering Action of printer magnets and stepping magnets.
- (3) Circuits for "parallel operation."
- (4) Automatic Group Spacer.

One essential feature (electric control by means of the "Stepping Maze") is covered by Secret Patent Application #70412, dated March 23, 1936, in the name of W. F. Friedman and F. B. Rowlett, with complete assignment to the Secretary of War on April 2, 1936. Many of the details of the Mark II ECM were taken over bodily from the Mark I and are covered by Secret Patent Application #206040, dated 4 May 1938, or by various patents held by the Teletype Corporation. Other details were copied from the Hebern Cipher Machine.

SECRET

The Question of Security

5. The question of security is of immediate importance because of loose talk that has been circulated in the Navy Department with consequent lessening of confidence in our primary cryptographic system. The concept of a "machine solution" has not been accompanied by the invention of the "machine." A study of the cryptographic features of the Mark II ECM exposes the fallacy of this thinking.

6. It may be taken for granted that the "high-grade" ciphers of any major power will offer tremendous resistance to cryptanalytical attack; also that a certain amount of misuse and occasional capture must be anticipated. "High-grade" systems fall into four categories, in ascending order of security, as follows:

I. Ciphers capable of purely analytical solution without prior knowledge of the system and without possession of any of the physical elements. Subsequent solutions become progressively faster as "technique" is developed until current messages can be read with little delay. We know these ciphers by our own solutions. We also know that the methods of solution would be totally ineffectual against the Mark II ECM or CCM.

II. Ciphers whose keys are capable of analytical solution, under the condition that the same key is used for two messages and the general system is known. The U.S. Navy "One-Time-Pad" and the "Teletype Scrambler" (CSP 1515) fall in this category. They afford absolute security provided duplication of key can be avoided. The Mark II ECM and CCM do not have this weakness.

III. Ciphers whose keys can be solved and messages read, if given full knowledge of the system, possession of the physical elements (but not the keys), and an adequate number of intercepted messages. (Replacement of the compromised elements would, of course, completely block subsequent solutions.) We have an example in a system whose solution has been described as "the life blood of our war effort." The CCM offers far greater security under these conditions than the above system: solution of daily keys would be a matter of weeks rather than hours, and might well prove impossible. The Mark II ECM will withstand attack under these conditions.

IV. Ciphers which cannot be solved, regardless of compromise of physical elements, so long as the daily keys are not captured. The Mark II ECM is the only current system for which this can be guaranteed. The Mark I ECM approximated this security in theory but other considerations made its "practical security" less than that of the CCM.

SECRET

7. The security of the Mark II ECM depends on the following features, in combination:

(a) Sufficient number of code wheels in the maze to generate an astronomical number of "alphabets" and "starting points." The five-wheel maze of the ECM and CCM gives 11,881,376 alphabets for each arrangement of code wheels. A three-wheel maze, by contrast, gives only 17,576.

(b) Use of 10 reversible code wheels in a set instead of a lesser number of non-reversible wheels. This gives 967,680 possible wheel orders, as compared with 120 for a rival system, making "trial-and-error" solutions impracticable if not impossible. The CCM also has 10 reversible code wheels per set.

(c) Use of erratic stepping of code wheels instead of "meter" or "modified meter" action to fully exploit the potentialities of the Hebern "Maze," block a known method of analytical solution, and prevent "short-cut" solutions with captured code wheels.

(d) Stepping of the alphabet maze controlled by an independent source. This feature is restricted to the Mark II ECM, the obsolete Mark I ECM, and an experimental Signal Corps Cipher Machine.

(e) Use of a multiplicity of stepping actions (5,855), dependent solely on the key, instead of only one as in other machines. This feature puts the Mark II ECM in a class by itself. The only competitor is the experimental Signal Corps machine with 120 stepping actions.

(f) Replication of code-wheel sets--both "effective" and "reserve"--with prompt change of code wheels in case of known compromise, and periodic change - just to play safe. This is an added factor of safety that should dispell any lingering doubts as to the absolute security of our ECM ciphers.

8. With regard to the claims advanced for the alleged necessity of a plug-board, the following evidence is offered in rebuttal:

(a) Plug-boards were given due consideration and discarded for reasons of security and reliability before the first pilot model had reached the blue-print state. The same effect was obtained in other ways.

(b) Plug-boards have not prevented the initial solutions of six different cipher machines on which used and have given so little delay to subsequent solutions that the information was "red hot." Misplaced confidence in the plug-board beguiled the inventors into stopping short of really effective cryptographic measures.

(c) The increased labor of solution is partially offset by the inconvenience to the users.

(d) Errors in plugging have led to direct compromise of the key, to say nothing of the effect on reliability of communications.

The disadvantages of the plug-board greatly outweigh its advantages and absence of a plug-board is a point of superiority for the Mark II ECM.

SECRET

Hebern Cipher Machines

9. On 2 January 1923, a Board consisting of Commander (now Admiral) R. E. Ingersoll, Commander (now Vice Admiral) Russell Willson, and Lieut. Comdr. (now Rear Admiral) W. W. Smith met to investigate and report on the adoption of the Hebern Cipher Machine by the U.S. Navy. The Board examined several models, including a 5-code-wheel nonprinting machine and a one-wheel machine electrically coupled to a standard typewriter. The Board reported:

> "Mr. Hebern, the inventor of the machine, has been in touch with the officers of the Code and Signal Section for two years or more, has received encouragement from the Code and Signal Section that his machine might ultimately be of some use to the Navy, and also has received suggestions and assistance from the Navy Department that made it possible for him to develop his machine from one of very doubtful security to its present state of practical security."

10. The Board recommended that the Hebern Machine be not purchased unless further improvements were made. The Board also recommended that no steps be taken towards coupling the cipher machine with the teletype until a satisfactory machine had been developed. The recommendations of the Board were approved by the Secretary of the Navy on 18 January 1923, and the Bureau of Engineering was directed "to make an agreement, or contract, with the Hebern Electric Code Company, Inc., of Oakland, California, to develop two electric printing cipher machines to fulfull Navy requirements." The sum of $50,000.00 was set up in the Bureau of Engineering 1925 Budget for the purchase of electric cipher machines, provided the pilot models proved satisfactory.

11. The "suggestions and assistance from the Navy Department" referred to above largely came from Mrs. Driscoll (then Miss Agnes Meyer) who was serving as technical assistant to the Officer-in-Charge of the Code and Signal Section.

12. The precept (dated 2 October 1922), report of the Board (dated 15 January 1923), and approval by Sec Nav (OP-20-G ltr. 9023-297:1, dated 18 January 1923) are the oldest official documents on hand. We also have pamphlets issued by the "H & H Patent Development Co." in 1920 and 1921, showing the early one-wheel Hebern machine, and by the "Hebern Electric Code, Inc.," in 1925, showing a three-wheel machine similar to one of the printer models developed under the 1924 contract. Mr. Hebern had been engaged in inventing cipher machines since 1912. U.S. Patent #1,141,055, dated 15 May 1915, covers a mechanical cipher machine of his invention. The first electric cipher machine built by Mr. Hebern (a one-wheel printer) is now in the "Museum" at the Communication Annex - a gift from Mr. Hebern.

REF ID:A273704

SECRET

13. The subsequent history of the development of the Electric Cipher Machine in its "Hebern" stage is given in the following tabulation:

Date	Contract Number	Number of Machines	Type	Total Cost	Remarks
3 Aug. 1924	#61155	2	Double Tape printer. Power operated.	--	Mr. Hebern submitted two or three different models under this contract but none were satisfactory. Contract cancelled on 3 March 1927 because of nonfulfillment.
July 1928	No record	4	Double typewriter. Hand operated. (CSP 604)	$ 3,320	Machines tested January - April 1929 by Navy Dept., CINCUS, COMBATFLT, and COM 12.
Sept 1929	#13798	2	Single typewriter. Hand operated. (CSP 534)	$ 3,240	Pilot models tested from January - June 1930 by CINCUS and Navy Dept.
7 June 1930	#17775	31	Single typewriter. Hand operated. (Identical with those on Contract #13798.) (CSP 534)	$46,500	Service tested in U.S. Fleet Problem XIII (1932) and completely "sold" the idea of electric cipher machines to the fleet. These machines were recalled for "modernization" in 1936, and remained in service until 1942. These machines handled all the important messages between the Navy Dept. and Naval Attache London from November 1938 to March 1942, inclusive.
1 Feb. 1932	#25436	1	Single typewriter. Power operated.	$ 4,300	OpNav Conf. Ltr. (SC)A6-3(7) dated 23 March 1933 advised BuEng: "The subject machine has been subjected to thorough test and is not considered suitable for service use." Mr. Hebern was notified by BuEng that the Navy had no further interest in his machine.
Oct. 1939	No record	2	"Commercial model". Converted to CSP 534 after delivery.	$ 1,500	Purchased to supplement the 30 Hebern machines still in service. This was our last transaction with Mr. Hebern.

SECRET

14. The chief difficulties with the Hebern Cipher Machine were due to mechanical deficiencies, particularly in the printer and in the power drive. The cryptographic features were capable of improvement, but it was decided in 1924 that the Navy would give Mr. Hebern no more suggestions which he could incorporate in machines offered for sale to foreign governments. It was planned to accept the cryptographic features "as is" and modify the machines after delivery to give greater inherent security. Plans for a modified meter action, very similar to what is used today in certain foreign cipher machines, were prepared by myself in 1924 but never used, due to non-acceptance of Hebern's earlier machines.

15. Hebern has never received adequate recompense for his part in the development of the Electric Cipher Machine. He is the original inventor. He brought his machine to the attention of the Navy Department, built numerous models, and by his perseverance developed it to the point where it almost became a practical machine. Hebern organized three or four different companies, which went bankrupt in turn. He lived in poverty, and during much of this period was supported by his wife who ran a boarding house. Hebern was put in jail by irate stockholders and would have been much better off personally if he had not invented the ECM or had not had any dealings with the Navy Department. However, Hebern has no legal claim on the Government because in the opinion rendered in J.A.G. Conf. ltr C-S67/68(8-25-29) of 30 Sept. 1932:-

> "Hebern has contributed substantial improvements in the ciphering art and while his claims are limited and are believed not to be infringed, yet there are several points of fact and law that may be urged. Taking the decisions of the courts as a guide, however, it is believed that any decision on the patents involved herein (Hebern #1,510,441, #1,683,072, and #1,861,857) would be in favor of the Government."

Washington Navy Yard Models

16. The following is quoted from OpNav Serial 310502 dated 2 May 1931:

"4. .....It is not the function of a division of the Office of Naval Operations to develop mechanical devices, and the Code and Signal Section has neither the personnel nor the equipment to prosecute the development of this ciphering device beyond its present point. The Bureau of Engineering will be called upon in the future, as in the past, to provide the funds for the development work and the procurement of the machines. It is therefore desired that the Bureau of Engineering take over now from the Code and Signal Section all phases of the work of developing and procuring mechanical ciphering devices. This work is of a highly specialized nature, and it is not expected that it can be satisfactorily performed except by an officer who is thoroughly familiar with the subject of cryptanalysis."

"6. In order to provide for the proper and pregressive development of mechanical devices for the phases of communications cited above; namely, secret ciphering and recognition systems; the Chief of Naval Operations requests that the Chief of the Bureau of Engineering take over the cognizance of the mechanical development work cited above."

17. In 1932, under the directive quoted in paragraph 8 above, the Bureau of Engineering (Radio Division) undertook the development of its own electric cipher machine. This resulted in the so-called Anderson-Seiler Machine, which was the prototype of the Mark I ECM. Instead of cutting cam contours in the periphery of the code wheels as in the "modified" HCM and CCM, Mr. Seiler devised a system of control wheels with sliding pins equally spaced around the rim. This same mechanism was independently developed in Sweden and used in the "Hagelin Cryptographer." Mr. Seiler also devised a system of control transfer through Bowden wires so that any pin wheel could control any code wheel. The cryptographic features were approved by the Code and Signal Section and the new machine started on this basis. The printer was a standard typewriter, stripped of nonessential parts, built into the machine, and operated by solenoids placed under the keyboard. The final model was bulky, rather heavy, and very unreliable in operation. It was felt that this machine had promise but would require redesign by experienced engineers to improve its operation and adapt it to standard manufacturing processes. In 1933, the Teletype Corporation indicated its willingness to undertake the development of the Anderson-Seiler Machine, and the third phase of ECM development was begun.

18. The Washington Navy Yard had previously constructed two pilot models of a contemplated HCM Adapter (CSP 535), designed by myself, and tested then in 1930 on the two Hebern Cipher Machines (CSP 534) purchased in 1929. When the HCMs were overhauled and "modernized" in 1937 and 1938, an improved stepping action of Navy design was installed by the Washington Navy Yard. This stepping action was designed by Mr. Seiler and myself, jointly, and represented an improvement and simplification of CSP 535. These modernized HCMs were reissued as CSP 903 and used until 1942. It is unfortunate that this line of development was departed from in the Anderson-Seiler model, as it set the Navy back about four years.

19. Early in 1938, plans were made for conversion of the Mark I ECM to cryptographic equivalence with the Mark II by replacing the "Internal Mechanism - Mark I" (CSP 692) with "Internal Mechanism - Mark II" (CSP 961) and a minimum of other changes. With a prospective procurement program of 100 machines a year, the 187 Mark I machines in service loomed very large. One model of CSP 961 was made by the Washington Navy Yard and one Mark I ECM was converted before the second pilot model of the Mark II ECM had been delivered. Eventually the Mark I ECMs were converted to Mark III HCMs (CSP 1127) instead, but the experience and confidence gained in designing CSP 961 paid big dividends a few years later when Mr. Seiler (by that time Lieut. Comdr. U.S.N.R.) was called upon to work out a method whereby the American ECM and British Type "X" Machine could be converted to a common cryptographic basis. This resulted in the following machines of his design:-

ECM Adapter	- CSP 1600	- 3500 being built at Washington ECM Repair Shop
CCM	- CSP 1700	- 631 ECMs converted by Washington ECM Repair Shop
"X" Adapter	- CSP 1800	- Pilot model built by Washington ECM Repair Shop
		4500 Adapters being made by Teletype Corp.

The stepping of the "modernized" HCM (CSP 903) was incorporated in the above machines. This same stepping action was originally contemplated for the Mark II ECM but it was not adopted because the electric control gave promise of quicker development and greater reliability, as well as higher security.

REF ID:A273704

SECRET

The Mark I ECM

20. The Chief of Naval Operations approved the Anderson-Seiler model on 28 September 1933, and requested that "the Bureau of Engineering proceed with this project as rapidly as possible." On 8 February 1934, Confidential Contract NOs 34703/71601 was negotiated, calling for delivery of six pilot models within a period of six months - total cost $50,000.

21. The urgency of equipping the fleet with a cipher machine at the earliest practical time was felt so strongly that, after a very brief test of one pilot model, the Chief of Naval Operations, on 10 August 1934, requested the Bureau of Engineering to procure a minimum of 94 Mark I ECMs for initial distribution and further advised, "It is the present plan of this office to eventually equip every combatant ship with this device." "Production" machines and associated equipment were purchased as follows:

Contract No.	Date	Article	No.	Amount
NOs 40349/76601	22 Jan. 1935	Mark I ECM	80	$218,528.00
NOs 43258/7X750	17 July 1935	Mark I ECM	101	218,664.58
NOs 49993/77601-2	5 Aug. 1936	Code Wheels (Mark I)	2,000	22,900.53
NOs 52271/7X750	4 Jan. 1937	Bowden Replacement Units	196	10,486.00
NOs 50918/———	7 Oct. 1936	Diehl Motor Generators	102	6,579.00
———————	(1937)	G.E. Motor Generators	85	5,440.00 Est.
———————	(1938)	Mark I ECM	2	5,000.00 Est.
		TOTAL	—	$487,600.00 Est.

Initial distribution to ships of the U.S. Fleet was made in April, 1936. The Mark I ECM (CSP 691) was made effective in May, 1936, as a fleet system and remained in effect until January, 1942, when it was superseded by the Mark II ECM. The Mark I machines were then recalled, modified to operate on the same cryptographic principle as the "modified" HCM (and CCM), and reissued as CSP 1127 (the so-called "Mark III HCM"). CSP 1127 was given a special distribution to Naval Attaches, Intelligence Activities, outlying Naval Bases, and certain State Department officials, and is still effective at this date.

22. The Mark I ECM gave trouble from the start and was in service five years before all the "bugs" had been worked out of it. Two new designs of patch-cord, one new design of plugs, and one new design of receptacles had to be substituted for the originals. The stepping action gave trouble, particularly when the machines got older. The chief objection to the Mark I ECM was in its bulk, its unnecessary complexity and difficulty of maintenance, and its lack of resistance to corrosion. Many of these defects would have been overcome had the pilot models been service tested before going into production. However, every defect which showed up in the Mark I ECM was eliminated in the Mark II, while all the good features of the Mark I were carried over to the newer device, so that we profited by our experience. We had enough Mark I ECMs to meet the needs of our peace-time Navy and we developed experience and confidence in cipher machines.

SECRET

The Contribution of the Signal Corps

23. Mr. William F. Friedman, Principal Cryptanalyst of the Signal Intelligence Service, and interested officers at Signal Corps Headquarters were familiar with the various models of the HCM, but not with the prospective changes which the Navy had concealed from Hebern. In fact, on Mr. Friedman's recommendation, the Signal Corps purchased two of Hebern's early 5-wheel nonprinting models late in 1923. At the request of the Navy Department, Friedman undertook a cryptanalytic test of the HCM in the spring of 1924, being furnished a set of 10 test cryptograms prepared by the Code and Signal Section. Friedman was successful, and developed cryptanalytic techniques whereby, under certain conditions of meter action, solution could be achieved even without possession of the code wheels. Again at the request of the Navy Department, in April 1932 Friedman undertook a second test on the much improved 1930 model of the HCM. This time he was furnished the machine, a description of the general system employed in setting up the message indicators, and a series of test messages. Again he was successful, with the aid of three or four of his assistants. As the test messages were enciphered with Hebern's stepping action and not with the irregular code-wheel stepping produced by the HCM Adapter (CSP 535), the solution did not worry us particularly. These solutions were very important, in three ways, namely:-

I. They showed the weaknesses of the meter action of the 1923 HCM and of 6 of the 30 optional stepping actions of the 1930 HCM.

II. The 1924 solution was the basis of further analysis by the Navy which disclosed stepping actions that would block analytical solutions or short-cut solutions based on possession of the code wheels. Friedman arrived at similar conclusions, independently. Otherwise, we would have had to abandon the Electric Cipher Machine as being deficient in inherent security.

III. In recent years, the principles and techniques of these solutions were instrumental in the solution of certain systems which are still using a modified meter action.

24. The first solution (that of 1924) was written up by Friedman in a secret, typewritten, technical paper completed early in 1924, which was not printed, however, until 1934, under the title "Analysis of a Mechanico-Electrical Cryptograph--Part I." The second solution (that of 1932) was also written up by him in a second secret paper completed in 1933 but not printed until 1935, under the title "Analysis of a Mechanico-Electrical Cryptograph--Part II." Both papers were very carefully safeguarded at all times and were employed only in the SIS for the advanced training of a very limited number of students. The documents were given no dissemination except that the Navy Department was furnished copies. But, because it was not consulted with regard to the advisability of printing these papers, combined with a serious mistrust of the Government Printing Office, the Navy Department entertained some apprehensions as to security and this led to an order from the D.N.C. that the Signal Corps was not to be shown the Mark I ECM or to learn any of its details. This order, which was not revoked until January 1940, was responsible for later misunderstandings. Certain Signal Corps representatives, including Friedman and Mr. Frank B. Rowlett, had been shown the pilot model of the Mark I ECM sometime in the winter of 1934-35, before the order was issued, so they were not entirely ignorant of what the Navy was doing along these lines.

SECRET

25. From 1924 to 1932 the Signal Corps appeared more interested in the Teletype Scrambler than in the HCM as a practical cipher machine which would meet Army requirements. However, under date of 25 July 1933, the Chief Signal Officer filed on behalf of Friedman a patent application (Serial No. 682,096) covering a cryptographic system and machine in which the stepping of the code wheels was very irregular and under the control of a keying tape. Electric control thus made its first appearance! Friedman made a complete assignment of his invention to the War Department and one or two preliminary models were built in 1935-36. These were successful and an order was placed with a relatively small and inadequately equipped manufacturer for a few machines, which were designated as Converter M-134A. It took a comparatively long time to build these few machines but by 1938 some of them were delivered and placed in service for communication between the War Department and the Commanding Generals of Overseas Departments. Later, additional ones were delivered and placed in service for intercommunication among the War Department and Corps Areas and between the War Department and the U.S. Military Attache in London. The first model of this machine was shown to me by the Signal Corps sometime in 1937. This machine indicated the reliability of electric control but the undesirability of the particular method (perforated tape) used in the Signal Corps machine.

26. Shortly before 15 June 1935, during the interval when preliminary models of the foregoing machine were being built, Mr. Frank B. Rowlett, principal assistant to Friedman, conceived the idea which constitutes the basis of the "stepping maze" in the present HCM. His concept was based upon the principle of sending an electrical impulse through the circuits of a code-wheel maze to generate a long, irregular sequence of events which could then be used for various purposes, such as keying. Rowlett and Friedman then jointly developed Rowlett's novel idea of a key generator as applicable to the Signal Corps machine and reduced it to more practical form in drawings. No model incorporating their ideas was built by the Signal Corps, however, because the Chief Signal Officer was committed to the type embodied in the Converter M-134A, pre-production models of which were then under manufacture, and he was reluctant to make any change in design, despite Friedman's urgent recommendations that this be done. The inventors proceeded to incorporate the results of their theoretical studies and their drawings, reducing the new principles to practice in a patent application filed in the Patent Office on 23 March 1936 by the Chief Signal Officer on their behalf as joint inventors (Serial No. 70,412). The inventors made a complete assignment of their invention to the Secretary of War on 2 April 1936 and the application was processed through the Patent Office, though, of course, it is held in the secret status. Nearly all of the claims (39) have been allowed in the case.

SECRET

27. In October 1935, Friedman and Lieutenant Wenger (of the Code and Signal Section) held a general discussion on cipher machines. Wenger expressed considerable dissatisfaction with the Mark I ECM and asked Friedman whether the Signal Corps had any "good" ideas along these lines. Friedman indicated that there were several ideas which the Signal Corps was not exploiting but which he was not at liberty to disclose, since they had been placed in the secret category. Friedman further indicated that if Wenger so desired, permission to disclose them to the Navy would be requested. Wenger asked that this be done. Accordingly, Friedman requested and was granted permission by his superiors to disclose the details of the Friedman-Rowlett patent application to representatives of the Navy Department. Therefore, on 21 October 1935, at a conference in Friedman's office, the details were disclosed to Commander McClaran and Lieutenant Wenger, who were shown the drawings that formed the basis of the patent application Serial No. 70,412. On 31 October 1935, a second and similar disclosure was made to Commander McClaran Lieutenant Wenger, and Lieutenant Harper. A third disclosure was made on 1 November 1935 to Lieutenants Wood and Dugan, also of the Code and Signal Section. Friedman and Rowlett were told very little as to the Navy Department's reaction to the disclosures; in fact, they were told that the principles disclosed were of no interest to the Navy at that time - which was the truth of the matter.

28. My first-hand knowledge of the Friedman-Rowlett invention began in the winter of 1936-37 when we were preparing initial specifications for the Mark II ECM. Wenger stated that Friedman had an idea for an electric control which had very interesting possibilities and produced from his safe a single sheet of cross-section paper containing three elementary wiring-diagrams by means of which electric control of an ECM could be achieved through an ECM mase. This paper was dated and signed (as I remember) by Harper, Wenger, and Wood, and by Friedman and Rowlett. (We have been unable to locate this paper since 1940.) I immediately realized that electric control gave us the answer to many of our unsolved problems and therefore had to be incorporated in the new machine. I was under orders not to discuss or show either the Mark I ECM or the Mark II ECM to the Signal Corps and, therefore, adopted electric control and further developed the basic idea without the knowledge of the original inventors. In January 1940 the Mark II ECM was offered to the War Department for Joint Army-Navy use and also for purely Army use. It was explained that the mechanical features were well developed and "frozen" in design, and that we believed the Army would be well satisfied with the cryptographic principles involved, but that we were willing to discuss any security features in order to get a machine that would be satisfactory to both services. We wanted the Army to join us on the first order for the machine in order to further the idea of using identical cryptographic systems in the two services, as had already been done with the Strip Cipher Device. Another reason was to share the overhead for tooling-up and thereby give us a better price. It had been previously suggested that the Army and Navy get together on the Signal Corps machine or the Mark I ECM. We advised that neither machine was acceptable because of mechanical deficiencies but that we were developing a new machine and as soon as we had a working model we would endeavor to get permission to make it available as a common Army-Navy machine.

SECRET

29. On 3 February 1940, Admiral Noyes (O.N.C.) invited General Mauborgne (Chief Signal Officer), Captain Cook, Mr. Friedman, and other Signal Corps representatives to inspect a pilot model of the Mark II ECM. On that occasion I acknowledged to Mr. Friedman, in the presence of General Mauborgne and Admiral Noyes, our use of his invention. Later there was a special conference attended by Mr. Reiber and Mr. Zenner of the Teletype Corporation, Mr. Friedman of the Signal Corps, Commander Safford and Lieutenant Zern of Naval Communications, and possibly others. The blue prints were carefully examined and a general discussion of cryptographic features followed. Friedman pointed out that the underlying principles of the control circuits of the Mark II ECM were those which had been disclosed by Rowlett and himself to the Navy Department in 1935, and this was confirmed by me. The four experimental changes to the Friedman-Rowlett circuit which had been made by Seiler and myself were discussed and the following decisions made:

I. "Index Maze," which replaced the plugboard in the Friedman-Rowlett invention - Retained. The "Index Maze" accomplished the same cryptographic result as the plugboard but was much more convenient to the operator.

II. Grouping of end contacts in the "Stepping Maze" and in the "Index Maze," which replaced the arrangements of the Friedman-Rowlett circuit - Retained. These groupings together with the ten circuits through the "Index Maze" gave 49 times as many stepping combinations as was possible with the Friedman-Rowlett invention (5,855 against 120).

III. Subdivision of "Stepping Maze" into two parts - Unanimous decision to return to the original Friedman-Rowlett "Stepping Maze." Friedman protested the subdivision as an unnecessary complication. Reiber and Zenner did not like it from the viewpoint of design and construction.

IV. Stepping order for the "Stepping Maze" proposed by the Navy was 3-1-5, the other two wheels being dead to simplify construction. The stepping order was changed to 3-4-2 upon Friedman's recommendation.

With these exceptions the Mark II ECM, as developed by the Navy and Teletype using the Friedman-Rowlett "Stepping Maze," was satisfactory to and accepted by the Army. Washington Navy Yard sketch RM68F201, dated 24 April 1940, used as a basis for specifications of the production model, is the earliest-dated drawing showing the "Stepping Maze" and associated circuits exactly in their present form.

30. One other contribution, Major Leo Rosen's "Plugboard Code Wheel," came in 1943 after the ECM was in service. This was developed by the Signal Corps for field use, where the danger of capture was greater than in the Navy. The "Plugboard Code Wheel" was adopted for joint Army-Navy use at the request of the Army, but is being distributed to all Navy holders of the ECM. The chief value of the "Plugboard Code Wheel" to the Navy is possibly psychological, but we do have it in case of need.

SECRET

31. Electric control of the ECM by means of the Friedman-Rowlett "Stepping Maze" is the essential feature that places the Mark II ECM in a class by itself as regards security. Those who have participated in the development of the Mark II ECM have always acknowledged the contributions of the Signal Corps. The "Index Maze" and grouping of end contacts add to the security afforded by the "Stepping Maze," but would be worthless without it. The importance of electric control can best be estimated by a consideration of what the Mark II ECM would have been if Friedman and Rowlett had not been permitted to disclose their invention to the Navy. Although the "Stepping Maze" appears obvious, now that it is in use, no one in the Navy thought of it in a period of 15 years, and no foreign machine employs it. Therefore, the Navy would have continued the development of the older methods and the new ECM would have used the mechanical stepping control found in CSP 903 or CSP 1700. We would have had a secure machine, superior to anything in use by foreign nations, but definitely inferior to our present ECM. This hypothetical machine (as well as CSP 1700) would defy attempts at solution until such time as machine and code wheels were captured. After this, each day's keys would resist solution for a long time. "Short-cut" solutions would be impossible, due to the erratic stepping of the code wheels, but a trial-and-error solution would be within the range of possibility. We could not make the flat statement, as we do for the Mark II ECM, that solution would be utterly impossible. In other words, the machine would be adequate to take us through World War II but, because we had stopped short of the ultimate step, there would always be the desire to develop a new machine and scrap the old one. Rowlett is entitled to full credit for his discovery of the principle of the key generator as embodied in the "Stepping Maze," which adds so much to the excellence of the Mark II ECM, and Friedman and Rowlett jointly are entitled to full credit for their joint invention of methods of applying and reducing the principle to practical form.

32. The Signal Corps' acceptance of the Mark II ECM for Army as well as Joint Army-Navy use reflects credit on all who made that decision. The joint Army-Navy ECM Cipher System became effective on 1 August 1941, and the two services had a common high-security cipher system in effect and in use prior to the attack on Pearl Harbor. This use of an identical machine with interchangeable code wheels has been of great military value, particularly in the early stages of the war when the distribution of machines and code wheels was incomplete. In the Philippines, Java, Australia, and even in North Africa, Navy wheels have been used in Army ECMs, Army wheels in Navy ECMs; machines have been borrowed back and forth between the two services; Army messages have been sent in Navy ECM ciphers and Navy messages sent in Army ECM ciphers.

SECRET

The Mark II ECM

33. The directive for developing the Mark II ECM was given by the Chief of Naval Operations (over the signature of Admiral Taussig) on 22 November 1935 in Serial 828 as follows:

> "It is therefore requested that any funds which can be made available for equipping the naval service with cipher machines be used for the development of a small cipher machine which will be more practical in small vessels."

This directive amplified by Admiral Rowcliff (DNC) when I reported for duty on 6 May 1936, in substantially the following words:

> "The most important task ahead of you is to develop a small printing cipher machine for the fleet - something small enough to put aboard submarines and destroyers - something that will always function. Do not design a cipher machine for the Navy Department. Build one that will work aboard a minesweeper!"

Development could not be commenced prior to 1 July 1937 because of non-availability of funds and the peace-time practice of preparing budget estimates two years in advance. This delay was not detrimental because the reports from the fleet relative to the mechanical derangements and other deficiencies of the Mark I ECM were of tremendous importance in the design and specifications for the Mark II. We realized that mechanical reliability and simplicity were even more important than smaller dimensions, and that operation from either DC or AC power would be very desirable. During this period of waiting, the mechanical stepping control designed for the HCM was further improved cryptographically, but we were unable to achieve mechanical reliability in time to embody it in the new ECM.

34. The design and development of the Mark II ECM was prosecuted by the Teletype Corporation under Development Contract NOs-58864 dated 25 January 1938 for one pilot model at $65,000 and NOs-67249 dated 21 June 1939 with modifications dated 9 October 1939 and 6 June 1940 for building two pilot models and altering one of them at a total cost of $57,000. It covered three years and required three pilot models, as predicted by Mr. Reiber, the chief design engineer. The first specifications for the Mark II ECM were dated 7 April 1937. At the first conference between the Teletype Corporation, Radio Division (BuEng), and Communication Security Group (Naval Operations), the following facts were brought out:

(1) The Mark I ECM, after a year of service, was still unsatisfactory.

(2) The Teletype Corporation had not been allowed sufficient time for the design and development of the Mark I ECM.

(3) The Teletype Corporation had been unduly restricted in basic design of the Mark I machine as they were limited to refinements in a design worked out by others.

(4) The Navy Department had failed to inform the Teletype Corporation as to what was really wanted in an electric cipher machine, particularly in the matter of size.

(5) The Navy Department would have to supply and be responsible for the cryptographic features of the new machine. The company would gladly guarantee the electrical and mechanical features if given a free hand in the design.

The specifications for the Mark II ECM, therefore, covered the general description of the machine, ciphering circuits, size allowable, tape printer, and operational requirements. The specifications were changed several times during the process of development but the production models had every feature originally desired, with two exceptions:

I. An increase in size to be permitted, as a compromise with reality. Even so, the Mark II ECM is only 37% as large as the Mark I.

II. Interchangeable AC and DC motors had to be permitted, because the universal motor did not stand up under test.

35. The Teletype Corporation was given a free hand in design until it failed to produce mechanisms or circuits that would accomplish a desired end, or until Navy personnel had worked out simpler or more reliable methods than those proposed by the company. Working models, made at the Washington Navy Yard, were demonstrated in every case and the new designs were not adopted unless approved by the Teletype Corporation. Electrical control of the stepping of the code wheels was adopted for reasons of reliability and security. The Teletype Corporation investigated the Friedman-Rowlett plan of using the "Alphabet Maze" to control the stepping, prepared sketches showing the circuits and gang switches involved, and strongly recommended that we accept a second Maze to accomplish the same thing in a simpler manner. In fact, the Teletype Corporation thought it had invented the "Stepping Maze." The Navy then took the "Stepping Maze" as a matter of necessity, and accepted an increase of three inches in the length of the machine. We tested numerous circuits and combinations to exploit the flexibility of electrical control without increased size, complexity, or number of moving parts. For example, we tested two, three, four, and five circuits through the "Stepping Maze" and determined experimentally that four circuits gave the most random stepping action. The Teletype Corporation is responsible for the general layout, mechanical features, speed, ruggedness, and reliability of the Mark II ECM and is entitled to full credit for the part it played in its development. We must acknowledge that without Mr. Reiber's creative genius the Mark II ECM would be lacking much of its excellence. The "printer," adapted by Teletype engineers from an earlier tape printer but designed and built as an integral part of the machine, is possibly the most important mechanical feature of the Mark II ECM.

SECRET

First Pilot Model

36. The first pilot model of the Mark II ECM was delivered in January, 1939, and tested for a period of six months at the Washington Navy Yard. Despite serious defects, the pilot machine presented our ideas in three dimensions and gave us a better basis to work from. This model represented a departure in cryptographic principles from our familiar "Hebern" circuit. It had the "Enigma" (or return) circuit through the Alphabet Maze, "bucking coils" in the printer, double contacts (added by the Teletype Corporation) in the keyboard, and electrical control with the Friedman-Rowlett "Stepping Maze." The electrical stepping of this machine was very reliable and the most encouraging feature in the whole model. This model operated at 40 w.p.m., which was 67% better than the minimum speed required by the specifications. Tests with higher speed motors showed that it was reliable at 60 w.p.m. (the speed of the Mark I ECM) and this speed was demanded thereafter.

37. The model enciphered and deciphered satisfactorily but made a hash of plain language, due (it was discovered three months later) to the transformer action or "inductive kick" of the double coils and the hair-trigger action of the printer magnets. We had required the new ECM to print plain language (for indicators and headings) as well as to encipher and decipher. This feature had not been included in the Mark I ECM or in any Hebern machine except his 1928 model (CSP 604). Hebern handled this feature in the obvious way - by adding a "Plain-Cipher" gang switch with the same number of switch points as the "Encipher-Decipher" switch. The Teletype Corporation handled it by adding a second set of contacts to the keyboard but these were critical in adjustment, gave a heavy "touch" and were somewhat unreliable in operation. To solve this problem, I invented a three-way "Plain-Encipher-Decipher" gang switch with no more contact points than on the two-way "Encipher-Decipher" switch of the Mark I ECM. Mr. Seiler constructed a bread-board model to prove to ourselves (and later to Mr. Reiber) that this switch would work. The new switch or "Controller" could be installed in an unoccupied corner of the machine and would not increase its dimensions. This removed the last objection to the "Hebern" circuit.

38. This model had several novel features which were found undesirable or unnecessary on test, and eliminated or modified, including the following:

"Checking or Locking Circuit" on Alphabet Maze - Eliminated.
"Checking or Locking Circuit" on Stepping Maze - Eliminated.
Null Letter Selector for replacing "space" by J,K,Q,X or Z - Replaced by Seiler's "Z-X" method, installed on the Mark I ECMs in service.

39. Numerous experiments were made on this model at the Washington Navy Yard to attain greater security by more erratic stepping. The present combination of end-wirings on the stepping circuit was worked out and tested. A Plug-board was added to provide for changing combinations conveniently. Seiler proved by a working model that a ten-circuit maze was more compact, more reliable, and more convenient than the plug-board arrangement, and that it would fit an unoccupied space over the printer drive gear and clutch; so the "Index Maze" was adopted. Seiler also designed and installed "spark suppressors" similar to those designed by him for the Mark I ECM. The circuits for "zeroizing" and automatic code-wheel setting were developed and tested on this model.

SECRET

Second Pilot Model

40. The second pilot model of the Mark II ECM was delivered in January 1940, and tested for a period of five months. It had the familiar "Hebern" ciphering circuit (used in the Mark I ECM) with the improved controller, and "Input" and "Output" receptacles" for plugging to an external keyboard and an external printer. Its operating speed was 60 w.p.m. and it ran perfectly on encipher, decipher and plain.

41. The first improvement made on this model by the Washington Navy Yard was to make it operate on either AC or DC. Because of the triggering action of the magnets the machine worked equally well with the magnets "locked" or "bussing", and it was merely necessary to provide an AC motor and change circuit resistances to permit AC operation. This was demonstrated to Mr. Reiber on his next visit to Washington. Encouraged by this, Seiler was directed to attempt battery operation. He ascertained that the magnets would operate reliably on a 24-volt battery when all resistances were cut out. Suitable circuit changes were made and the machine ran for many hours on flashlight batteries and also on the 22½-volt tap of a "B" battery, the current drain being negligible. At the same time, Seiler developed the "fan gear" for driving the main operating shaft by hand. This feature has been little used by the Navy (although quite valuable to the Army) but it removed one of the phobias against the ECM.

42. The printer had been redesigned by Teletype Corporation to make it more easily serviced. The Washington Navy Yard made a further alteration to remove binding of the "stop bars." The bearing surface of the rear casing was bored out larger, a retainer ring added to keep the "stop bars" in place, and all moving parts suspended from the front of the casing. No more troubles with the printer were experienced.

43. The machine passed the heat, cold and humidity tests at Bellevue with flying colors, but the "shock and vibration" test proved a shock to us. The machine failed to step properly during the test and refused to step properly thereafter. Investigation showed that the fault was due to the design of the "basket", the split separators jamming the U-shaped contacts. This construction was intended to facilitate construction and decrease costs, but had to be abandoned. It was considered necessary to return to the button-type of contacts (encased in a cylindrical shell) molded in a single piece separator plate found in the 1936 (Mark I) ECM and the 1923 Hebern Machine. The "vibration test" also indicated the need for making the stepping of the stepping mass as simple as possible to facilitate checking. This was easily done as it merely required a few circuit changes. In view of these deficiencies it was decided to hold up the order for production machines until a model could pass the vibration test.

REF ID:A273704

SECRET

Third Pilot Model

45. The third pilot model of the Mark II ECM was nearing completion when the above-mentioned test took place, and all the alterations found necessary by this test were incorporated in this model prior to delivery. In as much as the basket had to be redesigned, the "Index Mase" was increased to five wheels (to facilitate construction) and the "Stepping Mase" was changed to a single mase with modified meter stepping of the first, third, and fifth wheels. This was later changed to second, third, and fourth wheels at the suggestion of the Signal Corps. Various other changes made on the second model by the Washington Navy Yard were made on the third model by the Teletype Corporation. This model was identical with the first production model except for being hand made.

49. The third pilot model was delivered in June, 1940, and immediately subjected to the vibration test, which was passed successfully. It was connected by patch cord to the second pilot model and parallel operation was demonstrated. The machine was then returned to the Teletype Corporation on a loan basis for use as a guide by the assembly lines and for instructing shop personnel in the functioning of the various mechanisms.

46. By the time the last pilot model had been tested the Battle of France was nearing the end, and the international political situation looked very serious. Further tests and further delays were unthinkable. We had to go into production on the basis of pilot model number three. The design as a whole was sound, but the possibility existed that the production job might not work as well as the hand-made model. Arrangements were made for emergency design changes and immediate replacements of unsatisfactory parts or units. The development stage was drawing to a close.

Alterations to Production Models

47. Four machines were assembled from tool-made parts (in advance of the assembly line) and "tested to destruction" by Telstype. These machines were operated for 12 million to 16 million letters and then disassembled for inspection and overhaul. Stainless steel proved too soft for bearing surfaces (as predicted by Mr. Reiber) and was replaced by hardened steel in all but the first lot of 459 machines. The only serious wear was on the printer worm wheel, which was soon replaced by a case-hardened wheel in connection with another alteration. The other "soft" parts can be replaced by ECM repair shops when they wear out--a few years hence. The badly-worn parts of these four machines were renewed by Teletype and the machines were then issued to the service.

48. The flat "star" spring on the printer drive clutch broke frequently during the destruction tests and also on the early machines in service. Different materials and a double spring failed to stand up, but a simple coil spring solved the problem perfectly. Replacement springs (with recessed worm wheels to accommodate them) were sent out for the machines in service, and this trouble is entirely a thing of the past. Emergency repairs were sometimes made by inserting a soft fiber washer, or by wrapping a rubber band around the printer drive shaft. (Necessity is the mother of invention.)

SECRET

49. The "Clutch Trip Magnet Contact Spring" has given more trouble than all other parts combined. It puts the machine out of commission when it breaks and no method of emergency repair has been discovered. Spare springs were not included in the original spare-part boxes and replacement was really a repair-shop job. About seven different types of contact springs have been designed and about four issued to the service, on new machines or as replacements. The latest type (on all but the first 1422 machines built) should last about two years. Previous attempts to eliminate this contact, by performing its function in some other way, have resulted in failure, but the possibility still remains that this is the ultimate solution.

50. The early machines developed trouble in the wiring circuits due to the factory using the guide studs of the Jones Plugs for electrical contacts. This was overcome by parallelling these guide studs with unused contacts in the plugs. Shifting from the guide studs was undesirable because every machine and every printer had to be interchangeable. The alteration was made on the machines in service by the ECM repair shops.

51. The Teletype Corporation used an improved type of through contact in the baskets of all but the first 1422 machines. The old contact cracked the bakelite separator plate when removed for repairs, and the new contact was designed to facilitate replacement as well as to reduce production cost. This contact, incidentally, is of the type used in the Anderson-Seiler model of 1933. This difference in construction of the baskets is the chief remaining difference between various lots of the Mark II ECM.

52. Automatic (or semi-automatic) operation of the ECM was anticipated by Admiral Hooper in 1922, and the "Ingersoll Board" recommended in 1923 that it be postponed until the cipher machine had been perfected. It had been considered for the Mark I ECM but was dropped. External receptacles to permit this eventuality were incorporated in the second and third pilot models and in all but 651 of the production models (CSP 888) which omitted the receptacles as a measure of economy in time and labor as well as money. Test equipment has shown the practicability of semi-automatic operation of the ECM with semi-automatic teletype transmission. After the new ECM was well into production, a development contract was let with the Teletype Corporation for design and construction of one complete semi-automatic ciphering-transmitting system. (NXs dated 14 April 1942 for $9,500.00.) Three more units were purchased on Contract NX dated 19 November 1942 for $14,600.00. After delivery the addition of page printers and means for automatically punching "stunt signals" in the perforated tape became apparent. These were worked out and added by Lieut. Comdr. Seiler's ECM repair shop - which, in the meantime, had been transferred from the Washington Navy Yard to the Communication Annex of the Navy Department. A contract for two additional equipments, incorporating the above Navy additions, is being negotiated; estimated cost - $10,000.00, chargeable to Lend-Lease (British).

REF ID:A273704

SECRET

53. The cryptographic features of the ECM are contained, essentially, in the "basket" and code wheels. Consequently, substituting new "baskets" of appropriate design gives a new and different machine. Three different "conversions" of the Mark II ECM have been made as follows:

Mark II ECM plus CSP 1136 (basket) became the HCM Mark IV;
Mark II ECM plus CSP 1600 (basket) became the CCM;
Mark II ECM (converted) with built-in basket became CCM (CSP 1700).

56. The alterations found necessary as a result of two years' service experience have been very few. It is possible that further changes will be made, substituting a part or unit of superior design or material for the original piece. This eventuality was given due consideration in the design and an attempt was made to allow sufficient space around each part or unit to permit such replacement. Our future concern should be to prevent trivial changes which would complicate the spare-part situation and increase the difficulty of overhaul without compensating advantages.

55. Procurement

Order No.	Navy Machines (CSP 888-889) No.	Navy Contract No.	Army Machines (SIGABA) No.	Army Contract No.	Remarks
1	374	NOa 74515 dated 19 June 1940	85	Reqn. #79-OCSIGO-40 dated 11 June 1940 on Navy Dept.	These Army machines were purchased by the Navy on Navy Contract and then invoiced to the War Dept.
2	726	NOa 77973 dated 21 Oct. 1940	237	Reqn. #9-OCSIGO-41 dated 12 July 1940 on Navy Dept.	do
3	2,900	NXs-1728 dated 26 Mar. 1942	240	#4688 - Chicago -42	Army negotiated its own contract
4	2,750	NXs-33375 dated 30 June 1943	760	#1266 -Phila, - 43	do
5			500	#29218 - Phila.-43	do
6			288	Contract being negotiated	do
7			1,200	Contract being negotiated	do
					Grand Total 10,060
Total	6,750		3,310		

SECRET

56. The first contract called for delivery at the rate of 50 ECMs per month, beginning June 1941, in accordance with an earlier agreement. Teletype reported inability to better this schedule so the I.B.M. Company was approached and tentatively offered the second contract - the machine to be a Chinese copy of the machine made by Teletype. Mr. Walter Lemmon, on behalf of I.B.M., agreed to do this, if Teletype called our bluff. Teletype was then given an ultimatum - expedite delivery or share future contracts. Within 48 hours we received word that:

(a) A.T.& T. had made the Western Electric plant at Hawthorne, Illinois, available for manufacture of ECM parts or units.

(b) Assembly and test would be undertaken at the Teletype Plant at Chicago, Illinois, on a two-shift (and if necessary a three-shift) basis.

(c) Delivery would commence in January 1941, unless unforeseen delay occurred, and an output of 100 machines per month could be guaranteed by May, 1941.

(d) Due to increased labor costs for this new schedule, it would be necessary to increase the contract by 5%.

These conditions were agreed to, the second contract was placed, and the Navy felt happier. There was a slight delay in deliveries at first but by December 1941 Teletype was ahead of schedule. At the date of writing, the output has been increased to 300 ECM's per month: the "war effort" of Teletype's Production Department has been praiseworthy. Machines have been prorated between Navy and Army on a percentage basis except when one service had urgent need of machines and the other agreed to relinquish some of its quota. With no difference except the nameplate, it was a simple matter to make the switch.

57. Financial Investment

Quantity	Item	Total Cost	Average Cost
6,750	Mark II ECMs with 3 sets of Code Wheels per machine and Tender Spares	$10,176,000	$1,507.55 per machine
20 Sets	Spare Parts Kits for Major ECM Repair Shops	$ 1,008,700	$50,435.00
51,250 Sets	Spare Wheel Sets (10 Per set in metal box)	$ 3,515,300	$ 68.59 Per set
- - -	Tools and Special Equipment for Repair Facilities	$ 82,000	- - - -
	NAVY TOTAL:	$14,782,000	
3,310	U. S. Army ECMs with Spare Wheel Sets and Spare Parts (Estimated Cost)	$ 5,627,000	Per Machine $ 1,700.00 (Estimated)
10,060	GRAND TOTAL ECMs (Navy-Army)	$20,409,000	(Estimated)

SECRET

58. **ECM Repair Facilities**

Major Facilities (10)	Minor Facilities (25)	Repair Ships and Tenders (40)	
Washington D. C.	NYd. Portsmouth	USS Melville	USS Vestal
NYd. New York	NYd. Philadelphia	USS Dobbin	USS Vulcan
NYd. Mare Island	NYd. Charleston	USS Whitney	USS Ajax
NYd. Puget Sound	NOB Newport	USS Black Hawk	USS Hector
NYd. Pearl Harbor	NOB Key West	USS Altair	USS Delta
NOB Londonderry	NOB San Francisco	USS Denebola	USS Rigel
NOB Oran	NOB Kodiak	USS Dixie	USS Jason
NOB Noumea	NOB Iceland	USS Prairie	USS Holland
NOB Sydney	NOB Argentia	USS Cascade	USS Beaver
NOB Dutch Harbor	NOB Bermuda	USS Piedmont	USS Fulton
	NOB Guantanamo	USS Sierra	USS Sperry
	NOB San Juan	USS Yosemite	USS Griffin
Intermediate Facilities (6)	NOB Trinidad	USS Hamul	USS Pelias
	NOB Recife	USS Markab	USS Bushnell
	NOB Auckland	USS Argonne	USS Howard Gilmore
NYd. Boston	NavSta Great Lakes	USS Alcor	USS Nereus
NYd. Norfolk	NavSta New Orleans	USS Maumee	USS Orion
RMO San Diego	NavSta Codo Solo	USS Patoka	USS Proteus
RMO San Pedro	NavSta Tutuila	USS Medusa	USS Otus
RMO Miami	Subbase New London	USS Prometheus	USS Antaeus
RMO Balboa	Subbase Midway		
	RMO San Francisco		
	NAS Kansas City		
	CGYd. Curtis Bay (Md.)		

These ECM repair facilities were established in compliance with Opnav Conf. Serial 042820 dated 22 March 1940.

CODE WHEEL WIRING

59. Wiring of ECM code wheels has become an undertaking of considerable magnitude. Navy wheels are wired at the Washington ECM Repair Shop although plans have been made for emergency rewiring at the other major ECM Repair Facilities. Army wheels are wired by WACS at Arlington Hall, but the Navy has wired 30,000 ECM wheels for the Army. From Dec. 7, 1941 to May 1943 a force of 78 Navy Yard electricians were engaged in ECM wheel wiring, the labor estimates for fiscal 1942 being $175,000 and for fiscal 1943 being $100,000. Navy wheels have been wired by WAVES since June 1, 1943 the present complement being 200 and the present allowance 240. The WAVES work up to their maximum wiring speed in about three months and are doing a splendid job as indicated by the following data:

High WAVE	- 22 Wheels per day.
Average WAVE	- 14 Wheels per day.
Average Navy Yard Electrician	- 7 Wheels per day.

SECRET

60. Wired code wheels are tested in a machine designed by Lieut. Comdr. Seiler which automatically tests and indicates:

I. Correctness of wiring
II. Grounds or shorts
III. Breaks or open circuits.

There has never been an occasion of incorrect wiring and only one occasion of incorrect marking of code wheels turned over to the Registered Publication Section. This is, indeed, an enviable record.

Distribution

61. Distribution of the Mark II ECM has been handled by the Registered Publication Section and has not occasioned particular difficulty except at the very beginning. We were racing against time to get the Mark II ECM distributed, and the Mark I ECM superseded, before the United States entered the war. The first 1100 ECMs were shipped in lots of 50 to 100 direct from the factory to the ECM Repair Shops at Washington (D.C.), New York, Mare Island, Bremerton, and Pearl Harbor. There, they were carefully inspected, given minor repair work averaging ten hours per machine, and distributed to ships present. The directive for distribution, given in Opnav Conf. Serial 045120 dated 20 March 1941, was followed without modification. Opnav Conf. Serial 0116120 dated 3 November 1941 to CINCLANT shows the following status of distribution:

No.	Mark II ECM Distribution as of 3 November 1941
353	Atlantic Fleet, Shore Establishment, and East Coast Issuing Offices.
67	Washington Navy Yard (Just received and awaiting inspection).
221	Pearl Harbor and West Coast Issuing Officers (For further distribution to Pacific Fleet and Shore Establishment).
29	CINCAF (2), Com 16 (2), and en route from Pearl Harbor to Cavite, via USS HENDERSON (25).
670	Total Mark II ECMs received to that date.
430	Due for future deliveries under existing contracts.
1100	GRAND TOTAL OF NAVY MACHINES.

On this date about 130 Mark I ECMs were distributed in the Pacific Fleet and the remaining 57 scattered throughout the rest of the Naval Service.

SECRET

62. The Atlantic Fleet was given first priority in distribution because, except for a few flags and cruisers, it did not have the Mark I ECM. The Mark II ECM became generally effective in Atlantic Waters on 1 July 1941, although some of the smaller craft not engaged in ocean escort duty did not receive their machine until two or three months later. We had a wide margin of safety in this theatre of operations.

63. Four ECMs for CINCAF and COM 16 were shipped to Cavite in May 1941, and made effective on 1 July 1941. The ECMs aboard the HENDERSON were transferred to "Task Force One," Asiatic Fleet, and made effective by CINCAF on 20 November 1941. We beat "too little and too late" by 17 days.

64. The Pacific Fleet was given last priority because it already had the Mark I ECM, which by this time was giving reasonably good service. The first shipment of machines (37) was received at Pearl Harbor on 21 August 1941; 180 more were sent direct from San Francisco in September, October, and November 1941. The following directives for distribution were sent to COM 14, with information copies to CINCPAC:

OpNav Conf. Serial 045120 of 20 March 1941
OpNav Rest. Serial 285120 of 13 August 1941
BuShips Conf. Serial 483-266 of 15 September 1941
OpNav Conf. Serial 0124620 of 17 November 1941.

Instructions called for initial distribution to Class 4 and above, so the Mark I could be superseded at the earliest possible date, but distribution bogged down badly. The Mark I ECM, of course, could not be superseded until its distribution had been paralleled by the Mark II. A personal letter from the Issuing Officer, Pearl Harbor, to the Registered Publication Section, written about this time, complained about the apathy of the Pacific Fleet. The ECMs filled his vaults and blocked the shelves. Battleships and cruisers, which held the Mark I Machine, refused to draw the Mark II ECM without specific orders from CINCPAC. The only ships that would take the Mark II ECM were the small ones at the bottom of the priority list. Finally, on 28 November 1941, CINCPAC ordered the Pacific Fleet to draw the Mark II ECM, and so advised the C.N.O. A subsequent check showed the following status of ECM distribution at Pearl Harbor:

No.	Local Mark II ECM Distribution as of 1 December 1941
96	Issued by Com 14 I.O. to Pacific Fleet and shore activities of the 14th District.
100	On hand at Com 14 I.O., waiting to be drawn.
25	In Pearl Harbor ECM Repair Shop, undergoing inspection and overhaul.
221	Total sent to Com 14 prior to attack on Pearl Harbor.

As a result of this delay the Mark II ECM could not be made effective in Pacific Waters until 10 January 1942, although we had hoped to do this early in November 1941. The attack on Pearl Harbor thus caught the Pacific Fleet "changing horses in midstream" as regards the ECM.

REF ID:A273704

SECRET

Type #8 Safe Locker

65. Small ships without a code room had need of a special ECM cabinet which would serve as:

I. Operating desk for ECM
II. Stowage cabinet for ECM
III. Safe for other registered publications.

A preliminary design was worked out by Seiler and a working model of the top section constructed at the Washington Navy Yard. This was sent to Norfolk Navy Yard by BuShips and a detailed design was prepared. Norfolk suggested the trunnion mounting of the "scuttle," which was much simpler than the original design. Norfolk constructed a pilot model of boiler plate, which was designated as "Metal Safe Locker - Type #8." The first lot of 600 were built at Norfolk Navy Yard under authority of BuShips letter 832-9(3631) of 24 May 1941. Others were built by commercial concerns. The Type #8 Safe Locker holds a complete "Class 3" allowance of cryptographic aids and is installed on all ships allowed the ECM, section bases, and other shore stations.

66. Army-Navy Joint Policy Concerning Distribution and Disclosure of Cryptographic Design of the ECM-M134C (June 24, 1942)

It is mutually agreed that the ECM-M134C will not be placed ashore in foreign territory except at such places where armed personnel of U.S. forces are stationed in sufficient numbers to properly safeguard the physical security of the machine.

The Army or Navy may make the machine available to the Allies of the United States if the machine is accompanied by a Liaison Officer and Communication Group. It will be the duty of the Liaison Officer to prevent the viewing of the machine or its operation or associated equipment by other than authorized personnel of U.S. armed forces.

The U.S. Army and Navy mutually agree that they will regard as secret information to be divulged only to the armed forces of the U.S. or to any U.S. citizen required to possess this information in the interests of the United States, any details concerning the ECM-M134C including rotors, wiring diagrams, keys, keying instructions and operating instructions.

If at any time either the Army or the Navy considers it necessary to deviate in any way from this policy, the one shall fully inform the other of the facts and circumstances and the change in policy, if any, shall be by joint agreement.

Frank W. Bullock
Colonel, Signal Corps

Joseph R. Redman
Captain, U.S.N.
Director Naval Communications.

The foregoing was promulgated as CSPM 182, still effective.

REF ID:A273704

SECRET

Patents

67. The following U.S. patents and patent applications pertaining to cipher machines are listed for possible value in subsequent investigations:

Patent No.	Patentee	Date	Opinion of J.A.G. - Sept. 30, 1932
1,414,496	Beyer	—	"The claims are beyond question not infringed."
1,472,775	Wahnoe	—	do.
1,502,376	Damm	July 22, 1924	No opinion by J.A.G. (Electric cipher machine which has no similarity to ECM.)
1,510,441	Hebern	Sept. 30, 1924	"Covers a reciprocally wired code wheel and therefore no infringement." (One-wheel machine.)
1,556,964	Scherbius	—	"The claims are beyond question not infringed."
1,584,660	Scherbius	—	do.
1,657,411	Scherbius	—	do.
1,683,072	Hebern	Sept. 4, 1928	"Plurality of code wheels with meter action from ratchet wheels and therefore no infringement."
1,705,641	Korn	—	"Claim #1 would be infringed <u>if</u> it were valid but it is clearly readable on Hebern 1,683,072 and is therefore invalid."
1,733,886	Korn	—	"The claims are beyond question not infringed."
1,777,425	Bernstein	—	do.
1,846,105	Hagelin	—	do.
1,861,857	Hebern	—	"Cam profiles on code wheels; double printer; no infringement."
2,116,683	Lemmon & Holt	1938	No opinion by J.A.G.
2,116,731	Noll	1938	No opinion by J.A.G.

Patent Application No.	Applicant	Date	Remarks
682,096	Friedman	July 25, 1933	Electric Control by perforated tape.
70,412	Friedman & Rowlett	March 23, 1936	Electric Control by auxiliary mase. (Applicable to Mark II ECM.)
206,040	Anderson & Seiler	May 4, 1938	Mark I ECM.
232,995 (7 applications in preparation)	Hebern	—	Details not known.
	Teletype & Navy Dept.		Mark II ECM.

The CCM possibly infringes on Hebern 1,861,857. The Mark II ECM does not infringe on any U.S. patents, but is based in part on Friedman & Rowlett Application #70,412.

SECRET

68. The following "opinions" are quoted from J.A.G. Confidential letter C-S67/68(8-25-wg) dated 30 September 1932:

"(a) That some of the patents — (listed above in par. 62) — cover basically the utilization of a rotating drum to change the circuits in a coding and decoding machine, but all merely cover the means whereby such drums are utilized.

"(b) That the Bureau of Engineering (Anderson-Seiler) design does not infringe any of the patents — (listed above).

"(c) — That the (Anderson-Seiler) design — appears to disclose patentable novelty —.

"(d) That the Bureau of Engineering would incur no liability under any of the patents — (listed above) by building and using the (Anderson-Seiler) design —."

Destruction in Emergency

69. This discussion of self-destructive features for the ECM is made a matter of record in case this question should arise again. Because of criticisms of the Mark I machine by the forces afloat, we made extensive use of stainless steel in the Mark II and did everything practicable to make the machine durable, indestructible, and unaffected by damp, salt atmosphere. One Naval officer recommended that the code wheels be made of sodium, or some other material soluble in salt water, and that demolition charges be installed inside the machine itself. We were unable to convince him that the forces afloat would not tolerate the explosive charges or soluble code wheels. He was so insistent that the matter was finally referred to the D.N.C. for decision, and we were upheld. Recent tests by Army engineers of the 40-lb. M-1 thermite bomb designed for emergency destruction of the ECM showed that in 97 seconds it will burn the insulation and bakelite and melt the wiring of the ciphering unit plus two sets of code wheels but will leave the printer and base relatively intact.

Conclusion

70. The Navy has been committed to the Electric Cipher Machine since 1923. The eighteen-year delay, in getting the actual machine, was due to difficulties in developing a machine that was mechanically reliable, rapid, and compact. The 1923 Hebern machine with contemplated "Navy modifications" was as good cryptographically as any 1943 cipher machine in use by foreign countries. Every D.N.C. has supported the development and ultimate adoption of the ECM. Admiral Hooper, for example, recommended the adoption of the Hebern Machine in 1922 and further recommended coupling it to the Teletype. The late Admiral Ridley McLean stated in 1925 that he hoped the Hebern Machine could be completed while he was still D.N.C. so he could leave it behind him as a milestone. The Mark II ECM was developed in conformance with a directive from the Chief of Naval Operations - to overcome the deficiencies of the Mark I. I had cognizance of the Electric Cipher Machine during 1924-25, 1929-32, and 1936-41. I examined all the ideas submitted for the Mark II ECM, made the decisions as to which ones should be adopted, and bore the responsibility for the success or failure of the machine. I write from personal experience as well as from the records.

Respectfully,

L. F. Safford,
Captain, U.S.N.