Exhibit 4. This is the final version that Captain Safford put in the record (Navy) of which he sent me without comment. W.F.F.

Safford's writing

Nov. 2, 1943.

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 [redacted] 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.

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 ECM. 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-producation 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.

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-deagrams by means of which electric control of an ECM could be achieved through an ECM maze. 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.

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 [redacted] 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 RW68F201, 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.

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.