WAR DEPARTMENT
Office of the Chief of the Air Corps,
Washington

Memorandum for:

Mr. Friedman: →

Serial # 300,212 deals with M-138 and in view of recent happenings it seems desirable to reclassify this patent —

70,412 and 443,320 — 134C, 228

Small 382,561
WDJ 682,096
WJF 107,244

Hall is returning Rosen's application. - BR

CHAS. A. ROWE
Patents Section S. C.
Room 3143 Branch 1313

Goes to clerks

Drawings go to Commercial Company for reproduction

Drawing Go to Richmond on Truck unattended (daily trips)

REPORT TO COLONEL LIPPINCOTT

Mr. Polton, Mr. Hall and the writer went to the Patent Office in Richmond on December 9, 1942. The purpose of the trip was to learn, first-hand, the manner in which secret applications were handled by the Patent Office and to determine both the procedures and the facilities for observing secrecy.

In Divisions 21, 16, 40, 53 and 55, it was found that secret applications were kept in the drawer of a steel desk belonging to the Chief of the Division in each case, and locked therein, the Chief of Division usually keeping the key. In Divisions 16 and 53 are kept some of the highly secret cryptograph applications of the Signal Corps. We were informed that in Division 16 these cases were given to the messengers for the purpose of carrying to other parts of the building to obtain photostats and to be delivered to other examiners. It is further understood that these messengers have not been cleared for secrecy. The status of examiners and others in this regard is not known. In Division 56, the cases are kept in a locked standard file. In Division 36, they are kept in an old standard file, which is provided with a lock. In Division 61, there is a key-locked file which most nearly approaches our combination file cabinets. The key for this cabinet was kept in the desk of the Assistant Chief Examiner of that Division.

Mr. Polton, under direction of Mr. Hall and with an order signed by Mr. Hall, proceeded to the photostat room and introduced himself as an employee of the Signal Corps, with no other identification, and personally being unknown to the members of the photostat room. He handed the order to the Chief of the Division, said order calling for a photostatic copy of each sheet of the drawing of an application filed by the Signal Corps, and asked if the photostat could be furnished that afternoon. The answer being in the affirmative, Mr. Polton return at the appointed hour and was handed the photostats. No further identification

was requested.

Each Division has a docket-book, which includes the Serial Number, filing date, name of the inventor, title of the application, the status thereof, and name of the examiner to whom it is charged. These books are kept on the desk of the clerk of the Division and are not in the safe. While these books are watched during the day, it would be readily possible for a foreign agent to examine these books and ascertain the Serial Number and filing date of several Signal Corps applications, provided they knew the name of the inventor or some other information, and thereby get the data with which to place an order similar to that given to the photostat room by Mr. Pelton.

When an application is filed, it is not put in a locked cabinet of any type, even though the case may be secret, until the examiner receives information that the case is secret. Before that time, the cases are kept in racks along the side of the wall and the drawings are kept in unlocked file cabinets, accessible to any person who might break in after hours. WSH

The security of the portion of the Patent Office in Washington has been under constant observation for some time by Mr. Hall and Mr. Pelton. This investigation has revealed the locked file cabinets in the War Division are not of approved construction, they being key-locked file cabinets. Mr. Welsh keeps the keys in the drawer of his steel desk. It may be added that Mr. Welsh's desk appears to be habitually locked, even throughout the day except when actual use requires it be temporarily unlocked.

Applications filed in the Patent Office include drawings. These drawings are sent to a commercial photostatic company in Washington for photostating. The applications are processed through the Patent Office in regular course of business similar to unclassified or perhaps "restricted" papers of the War Department.

Trucks transport the cases from Richmond to Washington and back. These trucks

~~SECRET~~

Report to Col. Lippincott (cont'd)

are not provided with an armed guard and generally have a negro truck driver. The present conditions of the trucks raise the possibility of serious breakdown which might endanger the security of the documents contained. The two trucks meet at Fredricksberg, where the drivers exchange trucks. It is suspected, on the basis of remarks made, that the drivers in exchanging pleasantries, possibly stop in for sandwiches, etc., leaving the trucks unguarded.

N. M. Moore
Captain, Signal Corps

William D. Hall
Patent Advisor

R. G. Pelton
Patent Advisor

~~SECRET~~

PAPERS

1. A means of providing an irregular wheel movement in cipher machine using cipher wheels

    1. Carbon copy of final
    2. Original of draft
    3. Carbon copy of draft with hand written corrections
    4. Early draft with photostat
    5. Hand written draft

2. Instruction sheet and blank for patent application

3. Report on M-228 (to Col. Corderman) carbon copy

4. Draft "Replacement of the Present Combined Cipher Machine" Carbon copy of staff study

5. Report to Col. Lippincott on visit to Patent Office in Richmond

6. Contribution of the Signal Corps. Carbon copy of pertinent passage from Naval history.

7. Excerpt from Drew Pearson on the Yalta Agreement

8. Informal memorandum on faults of cryptographic machine

CORRESPONDENCE

1. Letter dated May 16, 1935, subject: Blank forms for code accounting

2. Letter dated August 31, 1935 on principles of Converter Type M-134-T2.

3. Photostat of document dated June 26, 1935 on device to be attached to the electrical counting sorter, signed by Friedman and Rowlett

4. Photostat of memorandum dated July 6, 1935, forwarding draft of specifications upon which application for patent on Cipher Device Type M-138 may be based.

5. Photostat of Routing and Work sheet regarding evaluation of patent.

6. Copy of letter from Friedman and Rowlett setting forth the principles of M-134-T2, dated February 15, 1936.

7. Copy of letter dated 27 September 1945, subject: Release of Patent Application Serial No. 443,320.

8. Copy of memorandum dated 15 January 1946, subject: Release of cryptological inventions and developments.

9. Memorandum from AC of S, G-2, dated 29 April 1946, subject: Release of Cryptographic principles

10. Letter dated 20 May 1946, subject: Release of Patent Application Serial No. 443,320.

11. Memorandum dated 10 April 1947 on Procedure for release of information concerning secrecy patents.

12. Draft of indorsement on patent release of 443,320.

13. Comments on Patent Application No. 443,320, dated 29 December 1947.

14. Memorandum for record dated 25 September 1947 on Meeting with Captain Safford and engineers of Teletype Corporation.

15. Memo dated 20 September 1949, subject: Replacement of the CCM.

PAPERS

1. A means of providing an irregular wheel movement in cipher machine using cipher wheels

    1. Carbon copy of final
    2. Original of draft
    3. Carbon copy of draft with hand written corrections
    4. Early draft with photostat
    5. Hand written draft

2. Instruction sheet and blank for patent application

3. Report on M-228 (to Col. Corderman) carbon copy

4. Draft "Replacement of the Present Combined Cipher Machine" Carbon copy of staff study

5. Report to Col. Lippincott on visit to Patent Office in Richmond

6. Contribution of the Signal Corps. Carbon copy of pertinent passage from Naval history.

7. Excerpt from Drew Pearson on the Yalta Agreement

8. Informal memorandum on faults of cryptographic machine

CORRESPONDENCE

1. Letter dated May 16, 1935, subject: Blank forms for code accounting

2. Letter dated August 31, 1935 on principles of Converter Type M-134-T2.

3. Photostat of document dated June 26, 1935 on device to be attached to the electrical counting sorter, signed by Friedman and Rowlett

4. Photostat of memorandum dated July 6, 1935, forwarding draft of specifications upon which application for patent on Cipher Device Type M-138 may be based.

5. Photostat of Routing and Work sheet regarding evaluation of patent.

6. Copy of letter from Friedman and Rowlett setting forth the principles of M-134-T2, dated February 15, 1936.

7. Copy of letter dated 27 September 1945, subject: Release of Patent Application Serial No. 443,320.

8. Copy of memorandum dated 15 January 1946, subject: Release of cryptological inventions and developments.

9. Memorandum from AC of S, G-2, dated 29 April 1946, subject: Release of Cryptographic principles

10. Letter dated 20 May 1946, subject: Release of Patent Application Serial No. 443,320.

11. Memorandum dated 10 April 1947 on Procedure for release of information concerning secrecy patents.

12. Draft of indorsement on patent release of 443,320.

13. Comments on Patent Application No. 443,320, dated 29 December 1947.

14. Memorandum for record dated 25 September 1947 on Meeting with Captain Safford and engineers of Teletype Corporation.

15. Memo dated 20 September 1949, subject: Replacement of the CCM.

The Contribution of the Signal Corps

15. Mr. Friedman 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, the Signal Corps purchased two of Hebern's nonprinting models in 1924. At the request of the Navy Department, Friedman undertook solutions of the HCM in 1923 and again in 1932, being furnished the machine, code wheels, instructions, and test cryptograms in both instances. Friedman was successful both times, and developed a method of solution whereby, under certain conditions of meter action, solution could be achieved without possession of the code wheels. As the Navy Department did not intend to use a meter action in the stepping of its service models, these solutions did not worry us particularly. However, the techniques and experience gained in these solutions paid big dividends later on, as they were instrumental in the solution of certain systems which cannot be named. These solutions were published in SECRET status by the Signal Corps in 1935, as

Analysis of a Mechanico-Electrical Cryptograph - Part I
Analysis of a Mechanico-Electrical Cryptograph - Part II

The Navy Department was not consulted in the matter, although furnished copies of these pamphlets after printing. This caused bad feeling on both sides which lasted for several months and led to an order from the D.N.C. that the Signal Corps was not to be shown the ECM (Mark I) or to learn any of its details. This order was not revoked until January 1940, when Signal Corps representatives were invited by Admiral Noyes to inspect the Mark II ECM.

16. Late in 1935, or early in 1936, Friedman disclosed to Commander Wenger, of Naval Communications, his invention of an electric stepping control for the electric cipher machine, and three different methods for accomplishing this electric control. These are all covered in Secret Patent Application #70412, dated 23 March 1936, in the name of W.F. Friedman and F.B. Rowlett. An experimental model of an electric cipher machine using one of the Friedman-Rowlett electric control methods was built by the Signal Corps at Fort Monmouth, New Jersey, about this time and shown to me after its completion. About 25 or 30 of these machines were made in small lots up to 1939 or 1940 and used for special types of communication, such as Military Attaches and Commanding Generals. These Army machines indicated the reliability of electric control but the undesirability of the particular method used in the Signal Corps machine.

17. Friedman and Rowlett assigned the entire rights to their three inventions to the U.S. Government (Secretary of War). The Navy took another of the Friedman-Rowlett control methods (the "Stepping Maze"), experimented with it, and further developed it.

This was done without their knowledge until the day that the Mark I and Mark II ECMs were disclosed to the Signal Corps. On that occasion (3 February 1940), I acknowledged to Mr. Friedman, in the presence of General Mauborgne and Admiral Noyes, our use of his invention. The Navy also considered the third Friedman-Rowlett control method (the stepping circuits through the "Alphabet Maze") with the idea of conserving space, but abandoned it as unreliable and impracticable on the recommendation of the Teletype Corporation. At the suggestion of the Signal Corps, a last-minute change was made in the stepping of the code wheels in the "Stepping Maze".

18. 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 these contributions of the Signal Corps. The "Index Maze" adds to the security afforded by the "Stepping Maze," but it is 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 had not disclosed his 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 perfection, there would always be the desire to develop a new machine with electrical control. Friedman and Rowlett are entitled to full credit for their invention of electric control and the "Stepping Maze," which add so much to the excellence of the Mark II ECM.

19. The Signal Corps' willingness to accept the Navy ECM for their own use as well as joint Army-Navy use, and to drop the development of their own machine, reflects credit on all who made that decision. The joint Army-Navy ECM Cipher became effectiv

in July 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 by the two services 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 borrowed back and forth between the two services, Army messages sent in Navy ECM ciphers and Navy messages sent in Army ECM ciphers. One other contribution from the Signal Corps came in 1943, after the ECM was in service; namely, the "Plugboard Code Wheel." This was developed by the Army 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, and later distributed to all Navy holders of the ECM. The chief value of the "Plugboard Code Wheel" is possibly psychological, but we do have it in case of need.

Exhibit 4. This is the final version that Capt. Safford put in the record and which he sent me without comment. F.

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 weakness 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 meter action.

24. The first solution (that of 1924) was written up by Friedman in 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 ECM 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 form 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 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 (D.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 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 Nave 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 the Navy messages sent in Army ECM ciphers.

~~TOP SECRET~~

Informal Memorandum

The two primary faults of the cryptographic machine under discussion, and faults which alone permitted the soultion described, are, as described:

1. Non-pluggable cipher maze output endplate.
2. Provision for cipher rotors to move singly on occasions.

In section XIX, recommendations, P. 190, paragraph 48 (b) 1, a pluggable endplate is recommended. This takes care of "fault #1."

But paragraph 48 (b) 2 does not recommend, as we believe it should, a change in the cipher maze stepping provisions. It suggests instead that the stepping of the stepping rotors be changed by insertion of an additional fast moving wheel there, which is a good idea and certainly should be adopted. The cipher maze stepping rotors however should never be allowed to move singly, or they will "give themselves away" as this paper so aptly demonstrates.

Experience in B-III-Research tells us that in a Hebern-type of machine (which the SIGABA is except for motion) that there should always be THREE NON-ADJACENT WHEELS MOVING AT ALL TIMES. In an Engima type of machine, there should always be TWO NON-ADJACENT WHEELS MOVING AT ALL TIMES. We believe a recommendation should be made to the effect that two more fast moving wheels be provided for the cipher maze in addition to the one which might be moving at any one time, or else that one more fast moving

be provided the cipher maze and the cipher maze converted to Enigma type.

It has long been the contention of B-III-Research that wheels in cryptographs of Enigma type should never move singly, nor in Heber types ever in less than threes, and that endplates should be protected by plugging. We therefore read the attached paper with greatest interest.

March 28, 1944

OCSigO 461 Codes (Gen.)

WAR DEPARTMENT
OFFICE OF THE CHIEF SIGNAL OFFICER
WASHINGTON

8

SUBJECT: Blank forms for code accounting. MAY 16 1935

TO:

1. Par. 11, AR 105-25, dated September 1, 1934, requires that certain reports be accomplished whenever any registered War Department cryptographic publication is transferred from one holder to another, and that a semiannual report of possession be made on all such items. For purposes of facilitating the making of these reports a standard form has been established, designated as WDSC Form No. 84, "Semiannual or Transfer Report of Registered Secret and Confidential War Department Publications and Devices."

2. Attention is invited to the fact that the above-mentioned form (Stock No. 6D84) is now stocked at the Signal Section, New York General Depot, and issued on approved requisitions in the same way that other authorized Signal Corps forms are issued.

For the Acting Chief Signal Officer:

Geo. P. Bush

Geo. P. Bush,
Major, Signal Corps.

CONFIDENTIAL

8

June 26, 1935

MEMORANDUM FOR: Research and Development Division
(THRU: War Plans & Training Division)

1. In connection with the tabulating machinery now employed by the Signal Intelligence Section, the undersigned have invented a new and useful device which may be attached to the electrical counting sorter and which will be of importance in future employment of this machine in code compilation and in other work not related thereto, of a purely commercial character.

2. The principal object of the invention is to transform the electrical sorter into a device of exactly opposite function, viz., to "unsort", "scramble", or disarrange in a wholly random sequence a set of punched cards originally arranged in a definite or regular sequence. Another object is to provide a means and device for obtaining a wholly random, small sample from a large set of punched cards.

3. In view of the fact that such a device will be very useful in code production, it is desirable that patent application be made in order to protect the government's interests.

4. At the same time, in view of the usefulness of the device for certain commercial tabulating installations in which random selections of punched cards must occasionally be made, permission is requested to enter into negotiations with the International Business Machines Corporation or other companies, with a view to possible sale of commercial rights to this invention.

5. Attached hereto is a sketch and description of the invention, in the form of a preliminary draft of specifications.

William F. Friedman
Frankford Rowlett

Attached:
Sketch
Description.

CONFIDENTIAL

OCSigO-413.52-Gen. (6-26-35) 1st. Ind. 10.
War Department, OCSigO, Washington, August 21, 1935. To: Mr. W. F. Friedman and Mr. F. B. Rowlett, War Plans and Training Division.

1. In compliance with request made in paragraph 4, of your memorandum, dated June 26, 1935, relative to an invention covering an attachment to an electrical counting sorter, there is no objection to your entering into negotiations with any industrial organization with a view to possible sale of commercial rights to your invention, described in the memorandum herein referred to.

By Order of the Chief Signal Officer:

Dawson Olmstead,
Colonel, Signal Corps,
Executive.

WAR DEPARTMENT

OFFICE OF THE CHIEF SIGNAL OFFICER

WASHINGTON

August 31, 1935

1. This is to record certain facts in connection with the invention of several alternative means of providing an aperiodic displacement of the substitution cipher wheels of a cipher machine as granted in claim 17 of the patent specifications having reference to Converter Type M-134-T2.

2. It is desired to record here that the fundamental principle of using one or more commutators in conjunction with a set of selector magnets as a means for effecting the aperiodic displacements discussed in par. 1 is the contribution of Frank B. Rowlett.

3. The subsidiary principle (subsidiary to that set forth in par. 2) of producing aperiodic displacements (discussed in par. 1) of the substitution cipher wheels by means of an independent set of commutators containing contacts equal in number to the number of substitution cipher wheels to be displaced, is the contribution of Frank B. Rowlett.

4. The subsidiary principle (subsidiary to that set forth in par. 2) of producing aperiodic displacements (discussed in par. 1) of the substitution cipher wheels by means of an independent set of cipher wheels, hereinafter called the control cipher wheels, and having the latter cipher wheels identical in number of contacts and construction with the former so that all cipher wheels are interchangeable, is the contribution of William F. Friedman.

5. The subsidiary principle (subsidiary to that set forth in par. 2) of producing the aperiodic displacements (discussed in par. 1) of the substitution cipher wheels by means of a second set of control contacts on each face of each of the substitution cipher wheels themselves, and providing appropriate electrical circuits for the control contacts to govern the operation of the displacement mechanism, is the contribution of Frank B. Rowlett.

6. The subsidiary principle (subsidiary to that set forth in par. 2) of producing the aperiodic displacements (discussed in par. 1) of the substitution cipher wheels by means of the same set of substitution contacts operating in connection with a gang switch which makes these contacts serve for substitution and control in alternate sequence, is the contribution of Frank B. Rowlett.

7. The application of the principle of aperiodic displacement of substitution cipher wheels to cryptographs of the original Enigma type (in which the electrical circuit through the cipher wheels is reversed by means of a reversing cipher wheel and again conducted through the other cipher wheels before reaching the signaling element) is the contribution of William F. Friedman.

8. The foregoing facts will be used as a basis for evaluation and division of interest in all financial benefits which may accrue from the prosecution of the invention and its reduction to practice.

William F. Friedman

William F. Friedman.

Witnesses:

Chas. A. Rowe

Louise N. Nelson

Frank B. Rowlett

Frank B. Rowlett

FLO M-138
Patent Application

6

July 6, 1935

MEMORANDUM FOR: Research and Development Division (ATTN: W.P. & T. Div.)

1. In accordance with provisions of Par. 4c, AR 850-50, there is attached a draft of specifications upon which application for patent on Cipher Device Type M-138 may be based.

2. It is understood that the Navy Department has pending an application for patent on their first type of strip cipher device, and are filing an application covering their second type. They are apparently satisfied to standardize, for the Naval Service, our Type M-138, and are planning to purchase 100 or 200 devices identical with ours, except as to name plate.

3. It is recommended that the attached draft be forwarded to the Signal Corps Patents Section for use in the preparation of detailed specifications and drawings. In view of the existence of similarities between our Type M-138 and the Navy types, it is probable that patent of only limited scope can be obtained. Nevertheless, the improvements devised by me, consisting in the use of metal channel ways, a slidable guide rule, and a construction which permits of setting up the text alternately at the left side and right side of the assembly, make our type of device a very much more practical instrument than any of those heretofore devised.

4. Since these improvements arose from my own studies, it is requested that application be made in my name as inventor.

William F. Friedman,
Signal Intelligence Section.

COPY FOR: Mr. Friedman.

85

Rec'd 7/18/45
Chas. A. Pope
Patent Section, S.C.

~~Confidential~~

ROUTING and WORK SHEET

(To be used under provisions of Par. 41.6 b, Office Regulations, OCSigO, 1934)

From: WP+T To: R+D.

Forwarded ltr

from R&D & WPT

Request following information

1 Has Mr. Friedman been designated or employed for the purpose of making this invention?

2 Do the inventions embodiment is important to National Welfare?

RBR

WP+T to R+D.

1. Mr Friedman was not designated or employed for the purpose of making this invention
2. The improvements are not considered to be of such character as to warrant being classified as "important to National Defense"

WPD

To NRS for patent action

RBR

(Check one) SECRET___ CONFIDENTIAL___ RESTRICTED___

DATE 29 July 49

TO	FROM	TO	FROM
CHIEF, ASA	(10) ✓	Tech Staff	(96)
Spec Asst to the Ch	(14)	Spec Proc Br	(97)
Ch, Hist Unit	(13)	CH, SECURITY DIV	(80)
Asst to the Chief	(11)	Tech Staff	(81)
Joint Secretariat	(12)	Ch, Materiel Br	(82)
DEPUTY CHIEF, ASA	(20)	Ch, Methods Br	(83)
Asst Deputy Chief	(20)	Ch, Protective Br	(84)
Executive	(20)	Ch, Maint Br	(85)
Secretariat	(20)	CH, RES & DEV DIV	(70)
Ch, Pres Sec	(21)	Tech Staff	(71)
Ch, Org & Tng Sec	(22)	Ch, C & C Br	(72)
Ch, Plans & Oper Sec	(23)	Ch, Equip Br	(73)
Ch, Logistics Sec	(24)	Ch, Electromech Br	(74)
Ch, Fiscal Sec	(25)	Ch, Lab Serv Br	(75)
Adjutant General	(26)	Ch, Cryptologic Br	(76)
Ch, Sec Cont Sec	(27)	Ch, Electronics Br	(77)
✓ CH, OPERATIONS DIV	(90)	Ch, Pers & Tng Br	(61)
Directives Br	(90x)	Ch, Supply Br	(62)
Ch, Lab Br	(91)	SIGRP-5	(62)
Ch, Machine Br	(92)	CO, Arlington Hall Sta	(40)
Ch, Gen Processing Br	(93)		
Ch, Facilities Br	(94)		
Ch, I & D Br	(95)		

( ) Approval & Return
(✓) As Requested
( ) Concurrence or Comment
( ) Information & Forwarding
( ) Information & Return
( ) Information & File
( ) Recommendation
( ) Signature if Approved
( ) Your Action (by_____)
( ) For recommended reply

Copy for you & one for the person writing up history of SIGABA.

One copy forwarded to F

AS - 80 AS 80 Aug 49

CSGAS 96 (Rev. 14) 15 Apr 49 8-411

C O P Y

WAR DEPARTMENT
Office of the Chief Signal Officer
Washington

February 15, 1936

1. In connection with a memorandum dated August 31, 1935, (copy attached) setting forth "certain facts in connection with the invention of several alternative means of providing an aperiodic displacement of the substitution cipher wheels of a cipher machine as granted in claim 17 of the patent specifications having reference to Converter Type M-134-T2," the following additional facts are made of record:

2. The principle of employing a set of juxtaposed rotating commutators as a means of selecting in an irregular, aperiodic manner, the successive alphabets (for encipherment or decipherment) from among a plurality of cipher alphabets is the contribution of Frank B. Rowlett.

3. The associated principle of controlling the stopping positions of a single substitution cipher wheel by a set of juxtaposed control cipher wheels is the contribution of William F. Friedman. Note: Thus, for example, in Friedman and Graham U. S. Patent No. 2,028,772 the cipher key transmitter and its associated mechanism would be replaced by a set of control cipher wheels, the 26 final contacts of which would be connected to pins which would stop the substitution commutator in the enciphering (or deciphering) position.

4. The idea as to the possibility of directly applying the foregoing principles to the stopping of a rotating printing wheel at cipher positions, the latter being superimposed upon the stopping position determined by the key depressed on the keyboard, is the equal and joint contribution of both William F. Friedman and Frank B. Rowlett. In this case, in order to prevent cumulative errors it is necessary to return the printing wheel to an initial position after each operation. The cipher stopping position of the printing wheel is determined after it has been stopped by the depression of a key of the keyboard.

/s/ WILLIAM F. FRIEDMAN

/s/ FRANK B. ROWLETT

Witnesses:
/s/ Louise N. Nelson
/s/ Chas. A. Rowe

COPY

WAR DEPARTMENT
Office of the Chief Signal Officer
Washington

August 31, 1935

1. This is to record certain facts in connection with the invention of several alternative means of providing an aperiodic displacement of the substitution cipher wheels of a cipher machine as granted in claim 17 of the patent specifications having reference to Converter Type M-134-T2. [Application Serial No. 682,096]

2. It is desired to record here that the fundamental principles of using one or more commutators in conjunction with a set of selector magnets as a means for effecting the aperiodic displacements discussed in par. 1 is the contribution of Frank B. Rowlett.

3. The subsidiary principle (subsidiary to that set forth in par. 2) of producing aperiodic displacements (discussed in par. 1) of the substitution cipher wheels by means of an independent set of commutators containing contacts equal in number to the number of substitution cipher wheels to be displaced, is the contribution of Frank B. Rowlett.

4. The subsidiary principle (subsidiary to that set forth in par. 2) of producing aperiodic displacements (discussed in par. 1) of the substitution cipher wheels by means of an independent set of cipher wheels, hereinafter called the control cipher wheels, and having the latter cipher wheels identical in number of contacts and construction with the former so that all cipher wheels are interchangeable, is the contribution of William F. Friedman.

5. The subsidiary principle (subsidiary to that set forth in par. 2) of producing the aperiodic displacements (discussed in par. 1) of the substitution cipher wheels by means of a second set of control contacts on each face of each of the substitution cipher wheels themselves, and providing appropriate electrical circuits for the control contacts to govern the operation of the displacement mechanism, is the contribution of Frank B. Rowlett.

6. The subsidiary principle (subsidiary to that set forth in par. 2) of producing the aperiodic displacements (discussed in par. 1) of the substitution cipher wheels by means of the same set of substitution contacts operating in connection with a gang switch which makes these contacts serve for substitution and control in alternate sequence, is the contribution of Frank B. Rowlett.

7. The application of the principle of aperiodic displacement of substitution cipher wheels to cryptographs of the original Enigma type (in which the elctrical circuit through the cipher wheels is reversed by means of a reversing cipher wheel and again conducted through the other cipher wheels before reaching the signaling element) is the contribution of William F. Friedman.

8. The foregoing facts will be used as a basis for evaluation and division of interest in all financial benefits which may accrue from the prosecution of the invention and its reduction to practice.

/s/ WILLIAM F. FRIEDMAN

/s/ FRANK B. ROWLETT

Witnesses:

/s/ Louise N. Nelson

7

DRAFT

WDGSS-14 15 January 1946

MEMORANDUM FOR ASSISTANT CHIEF OF STAFF, G-2

SUBJECT: Release of Cryptological Inventions and Developments

DISCUSSION

1. In the years preceding the outbreak of the present war and during the war itself, numerous cryptological inventions were made by military and civilian personnel. Applications for patent were filed on some but not on all of such inventions. In either case, information regarding such inventions has for the most part been denied the public. Since the most recent War Department policy is to release as much technical information as possible, it is necessary to reexamine inventions in the cryptologic field.

2. The inventions concerned fall into five categories. Army Regulation 850-50, 17 July 1942, paragraphs 7 and 9, (Tab A), refers to three of these categories and indicates the nature of the Government's rights. Additionally, there are inventions made by persons or companies under contract to the Government and in these cases normally the Government's rights depend upon the terms of the contract but usually amount to a royalty-free license to practice any inventions made, with ownership of the inventions remaining in the contractor. The last category involves the independent agent, one who, working entirely on his own, produces an invention of merit. In

such a case, the Government has no rights except through purchase or the taking of a license.

3. Further discussion in this memorandum will be limited to the second category of Army Regulations 850-50 wherein the Government takes a nonexclusive royalty-free license and the inventor has a theoretical right to exploit commercially for his own benefit. Where cryptologic inventions are involved, classification of the equipment and security restrictions placed upon information pertaining thereto have been used to prevent commercial promotion. Cash awards to civilian inventors in Government service are in some circumstances possible, but the Army Security Agency has held that where the invention is within the purview of the employment an award is improper. Virtually the only other possibility of compensation to an inventor is by Congressional action.

4. ~~With the cessation of hostilities,~~ cryptologic inventive and development by independent inventors and by contractors ~~can~~ has ~~be expected to fall off to nearly nothing~~ in the past produced very little, and reliance, therefore, ~~will~~ have to be placed on Government employees. It is believed that some incentive must be furnished if research and inventors in this field is to continue to be highly productive; the possibility of financial returns from commercial promotion of cryptologic inventions that can be released may be sufficient.

5. The latest War Department policy bearing on the matter appears in a memorandum, subject: Classification,

Reclassification, and Declassification of Scientific and Technical Information, for the Assistant Chief of Staff, G-2, Director, New Developments Division, Director, Bureau of Public Relations, Commanding Generals of the Army Air Force, Army Ground Force and Army Service Force (Tab B), which states in paragraph 3 that "as liberal a policy with respect to review and declassification of classified projects and material as is consistent with continuing only those items of information, the publication of which would cause exceptionally grave danger to the nation or endanger the national security or cause serious injury to the interest or prestige of the nation or any Governmental activity thereof or which would be of great advantage to a foreign nation or cause administrative embarrassment, etc., will be retained in a security classification." According to General Borden, New Developments Division, the policy of the said memorandum is such that very good reasons must be presented in order to prevent the release of information. Further of interest in this regard is the policy of the United States Patent Office with respect to applications on file, which policy is indicated in a letter from Colonel Donald K. Lippincott, Patents and Inventions Counsel, Legal Division, Office of the Chief Signal Officer, to Intelligence Branch (Tab C). Patent Office policy is based upon a memorandum from the Joint Chiefs of Staff (Tab D).

6. Since fundamental cryptographic systems are well known, the greatest danger involved in the release of information in the form of patents or otherwise appears to be that of acquainting foreign powers or unfriendly forces with effective adaptations and arrangements of these systems. Patent applications need not and rarely do contain key generating means, rotor wiring, and other specific features upon which the security of cryptographic text really depends. The main difficulty is that, by disclosing basic features of successful machines used by this country, the development of other adaptations is made possible, and our own cryptanalysts will be faced with text very difficult to decipher. On the other hand, many American machines already are known in principle to thousands of persons who either maintained or operated the same, and it is most unlikely that the principles can be now successfully suppressed. Added to this is the probability that independent inventors, and particularly contractors who have acquired techniques and know-how in the performance of war contracts, will produce machines similar to those at present in use. Such machines would not be classified nor is there any means of restraining their promotion.

7. It is the well-established policy and practice of the War Department to declassify material when the information can no longer be considered as secret, confidential, or

restricted. To maintain classification on information the control of dissemination of which is ineffectual only results in the degradation of the classification system itself.

8. To declassify any specific item does not establish a general policy applicable to other items in the same general category. If this were not true the declassification of any item, whether it be a document or a piece of equipment, would be impossible, except in the rare case in which the entire category consisted of but a single item. Hence, to declare that declassifying a specific item of cryptographic equipment would lead to the declassification of all other classified items of cryptographic equipment is not warranted by considerations of policy or practicability. In declassification, each item must be considered and evaluated on its own merits.

9. It should be stressed that the declassification of a patent application and thus the issue of a patent covering certain principles or features of a cryptographic apparatus does not usually have as a consequence the declassification of a machine as a whole or the traffic handled by it since, as indicated in paragraph 6, the working apparatus will depend for its security upon specific wiring and so forth not disclosed in the patent.

RECOMMENDATIONS

10. That no exception from the announced War Department policy of liberality with respect to the release of technical information be made in the case of cryptologic inventions.

11. That the Chief, Army Security Agency, determine specifically which cryptologic patent applications or developments may be released.

TOP SECRET

Jean from Personal file

29 April 1946

MEMORANDUM FOR THE CHIEF, ARMY SECURITY AGENCY:

SUBJECT: Release of Cryptographic Principles.

1. The following policy is announced to be effective immediately:

a. Cryptographic principles or devices developed by officers, enlisted men, or civilians employed in any War Department Agency, or patents or patent applications on such principles or devices which are owned by, assigned to, or licensed for use of the War Department will not be released for use of foreign governments or for foreign or domestic commercial or private use until such time as necessary information is available and a procedure established in the Army Security Agency whereby information which is cryptographed by means of such principles or devices can be cryptanalyzed and read under any and all circumstances.

b. Where it is in the interest of the Government of the United States that an employee have no patent rights in cryptographic principles or devices to dispose of, and for the Government to own the entire interest for security reasons throughout any foreseeable future; and where discovery or invention of cryptographic principles or devices has been made by a civilian employee and does not relate to a matter as to which the employee was specifically directed to experiment with a view to suggesting improvements nor was produced as a result of any specific employment or contract to invent a specific device or article; and where an application for patent on such principles or devices has been filed with an assignment-in-trust to the Government for the purpose of maintaining such application in secrecy, the Military Intelligence Division will support, subject to the availability of appropriations, any reasonable request for purchase of all commercially exploitable reversionary rights of the inventor in the patent application.

CARTER W. CLARKE
Colonel, GSC
Acting Deputy, A.C. of S.,G-2

TOP SECRET

Copy for Col Rowlett

~~CONFIDENTIAL~~

27 September 1945

SUBJECT: Release of Patent Application Serial No. 443,320

TO: Commanding General
Army Security Agency

1. The subject patent application covers a cryptographic means and device for automatic encipherment and decipherment of teletypewriter signals and was filed in the U. S. Patent Office on 16 May 1942 in the name of the undersigned and Frank B. Rowlett, as co-inventors.

2. The principles involved in the subject application have been utilized in Converter M-228 and Converter M-294.

3. It is requested that the subject application be officially declassified in order that it may be allowed to go to issue, whereupon the right and title will revert to the undersigned and Frank B. Rowlett, subject to an irrevocable, non-exclusive, and royalty-free right and license remaining vested in the United States of America.

4. This action is desired because of the commercial applications of the invention, interest in which is believed to exist on the part of the U. S. communication companies.

5. Declassification of the patent application does not necessarily involve the declassification of the specific embodiments thereof represented in the apparatuses mentioned in paragraph 2.

WILLIAM F. FRIEDMAN

~~CONFIDENTIAL~~

SECRET A4126886

AS-70 AS-23 10 Apr 47 Procedur[illegible]elease of Information
AS-80 Concerni[illegible]crecy Patents
AS-90

Lt. Chapman, Ext 462

1. All previous instructions pertaining to the above subject are rescinded.

2. Research Laboratories Division is charged with the primary responsibility for making recommendations related to the control and evaluation of all patents and patent applications affecting cryptologic equipment and processes. In view of the above, the following procedure will be adopted for the handling of requests relating to the release of patents held in secrecy:

a. If the request is received by Research Laboratories Division, comments and recommendation will be forwarded by AS-70 to AS-20 after coordination with AS-80 and AS-90.

b. If the request is received by the Deputy Chief, it will be forwarded to AS-70 who will coordinate with AS-80 and AS-90 and return comments and recommendation to AS-20.

3. Comments should include sufficient background material to determine that recommendation is in accord with current policy on release of cryptographic principles, a copy of which is attached. The last sentence of paragraph 1a of attached policy will be interpreted on the basis that the Army Security Agency could expect to solve communications which may be passed therein, assuming the device were to be used in a practical manner by adequately trained personnel and resulting in a normal military or commercial traffic expectancy.

1 Incl
Memo for Ch, ASA fr
ACofS, G-2 dtd 29 Apr 46
subj: Release of Cryptographic Principles

/s/ Harold G. Hayes
HAROLD G. HAYES
Colonel, Signal Corps
Chief, ASA

CYS FURNISHED
AS-14
23
24

SECRET

Encl 9

COPY

HEADQUARTERS
ARMY SECURITY AGENCY
WASHINGTON 25, D. C.

File my personal file

WDGSS-23

20 May 1946

SUBJECT: Release of Patent Application Serial No. 443,320

TO: Mr. William F. Friedman, WDGSS-14

1. Reference your letter dated 27 September 1945, subject as above, the attached memorandum from the Acting Deputy Assistant Chief of Staff, G-2, outlines the War Department policy on the release of cryptographic principles.

2. Analysis of the policy would indicate that:

a. Patent application No. 443,320 will not be released unless it can be shown that the employment of the principles involved are susceptible to cryptanalysis under all circumstances; and

b. If not released, a request for purchase of all commercially exploitable reversionary rights may be entertained provided it can be shown that Frank B. Rowlett and yourself were not directed or employed to experiment on or to invent the principles or improvements embodied in Converter M-228 or Converter M-294.

3. If it is felt that subject Patent Application should be released under (a) above; or if and when it is felt a case should be presented for purchase of rights in conformity with stipulations contained in (b) above, an application for release or purchase, containing pertinent facts and necessary proofs, may be prepared and submitted to the Director of Intelligence through the Chief, Army Security Agency.

1 Incl
Cy ltr dtd 29 Apr 46
subj: "Release of Cryptographic Principles

/s/ HAROLD G. HAYES
Colonel, Signal Corps
Chief, Army Security Agency

29 April 1946

MEMORANDUM FOR THE CHIEF, ARMY SECURITY AGENCY:

SUBJECT: Release of Cryptographic Principles.

1. The following policy is announced to be effective immediately:

a. Cryptographic principles or devices developed by officers, enlisted men, or civilians employed in any War Department Agency, or patents or patent applications on such principles or devices which are owned by, assigned to, or licensed for use of the War Department will not be released for use of foreign governments or for foreign or domestic commercial or private use until such time as necessary information is available and a procedure established in the Army Security Agency whereby information which is cryptographed by means of such principles or devices can be cryptanalyzed and read under any and all circumstances.

b. Where it is in the interest of the Government of the United States that an employee have no patent rights in cryptographic principles or devices to dispose of, and for the Government to own the entire interest for security reasons throughout any foreseeable future; and where discovery or invention of cryptographic principles or devices has been made by a civilian employee and does not relate to a matter as to which the employee was specifically directed to experiment with a view to suggesting improvements nor was produced as a result of any specific employment or contract to invent a specific device or article; and where an application for patent on such principles or devices has been filed with an assignment-in-trust to the Government for the purpose of maintaining such application in secrecy, the Military Intelligence Division will support, subject to the availability of appropriations, any reasonable request for purchase of all commercially exploitable reversionary rights of the inventor in the patent application.

/s/ CARTER W. CLARKE
Colonel, GSC
Acting Deputy, A.C. of S., G-2

These are my original work sheets of Hebern Solution

W.F.F.

1936

FRIDAY, NOV.

27

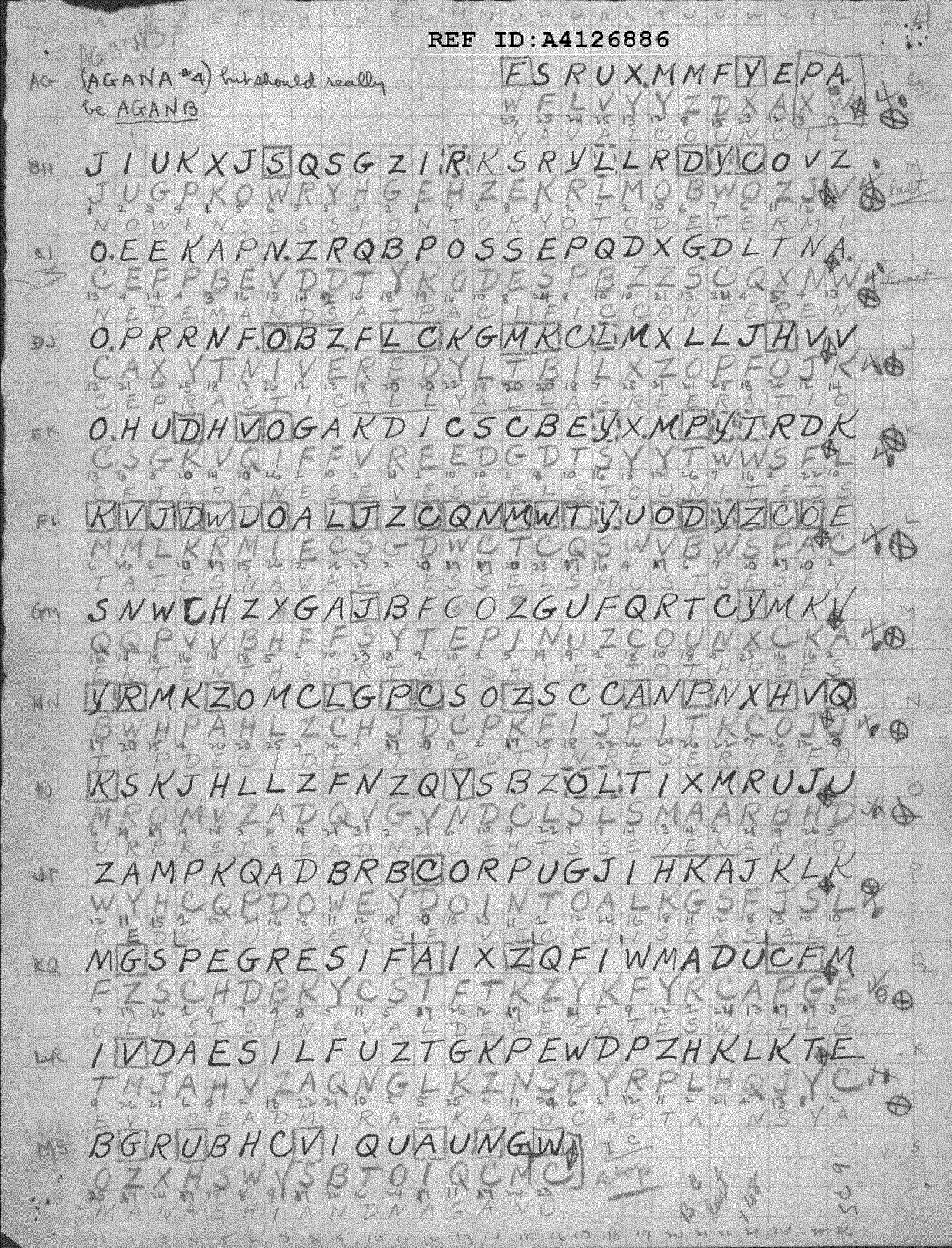
332 34

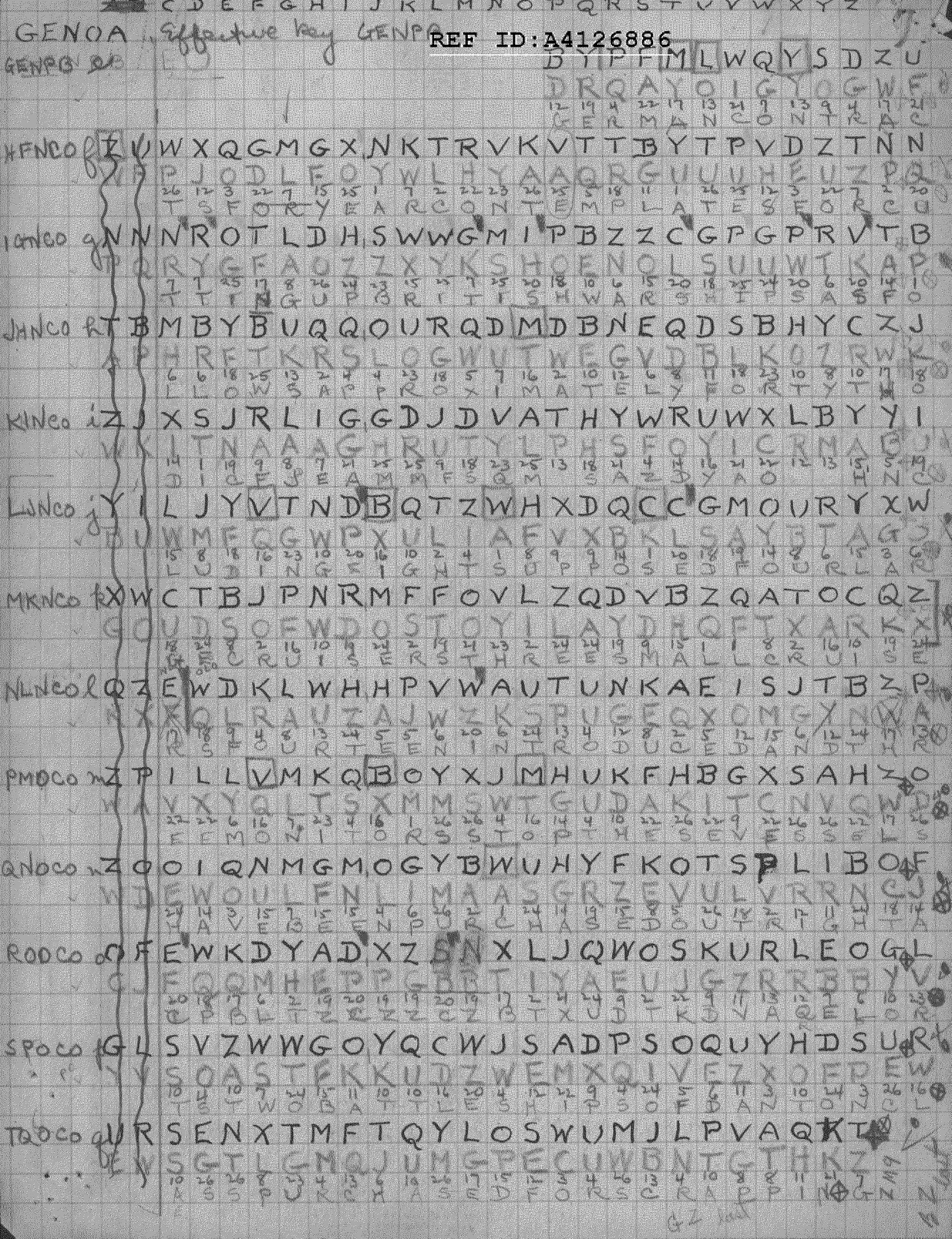
MONTE #9

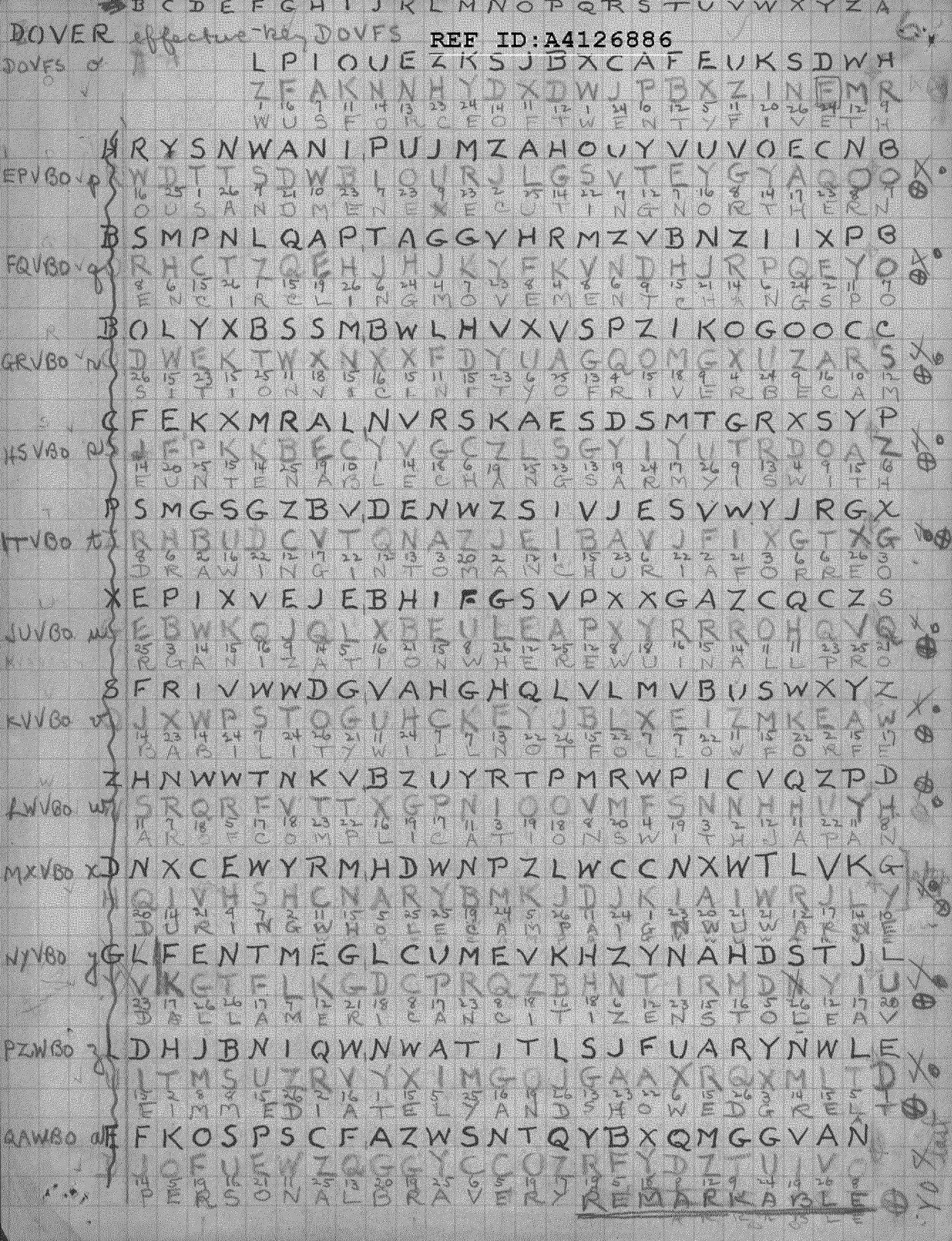
HAGUE #8

Illegible portion represents error in encipherment

REF ID:A4126886




REF ID:A4126886



E F G H I J K L M N O P Q R S T U V W X Y Z A B C D

CUNEO #5 L 4 UE

REF ID:A4126886

H K W Z A R R P B Q B I V Y S M P D M Q M Y U D C
W S U E G F G L B Y D J C T J Z U D C I E L F Q V
12 6 13 18 20 12 18 1 18 22 12 25 1 12 22 12 25 5 21 18 1 13 21 13 21
S M I T H S T A T E S C A S E S C O N T A I N I N

E M Z X D P I D L I A W W U B Q M E Z P I X I S N H
H K C N P I D S G G L C D V G D Z Y S W R F T R R U
4 14 12 16 20 7 17 1 17 16 25 3 11 7 11 8 12 15 16 20 11 23 4 6 7 17
G C O N T R A B A N D W E R E P O I N T E D O U T

R I Q O W Y I N R C X Y M X H J Z C R H A T H S B Z
Z Y Q J V K D A H F U Q V X J C Q N R O V Z R R Q
2 5 15 8 16 10 17 3 22 9 6 6 8 8 23 25 1 2 13 10 26 7 9 8 19
O H I M B Y M A J O R R S S N I V E L Y W H O S T

P M L K V O U Z R S A U G O H L T K O U Z J E C X L
D K A T T L O H H D L T O T J N U H Y B U I D T I X
23 14 8 23 22 4 23 23 22 14 25 15 17 13 23 4 26 13 14 8 22 17 1 3 14 2
T E D T H A T T H E Y C O N T A I N E D H O U S E H

S K D H W B I L E S K S W G Z G P R U I Q L H J J P
U R N Y V X D F P D A F D P O R T Q A Q I T R K L O
16 4 17 3 16 16 17 11 16 14 26 7 11 11 15 16 10 26 18 24 18 5 9 18 11 15
O L D G O O D S O F H I S S T O P H E R E Q U E S T

M K D Q E U D K M I G E O J L R Z D K N N P N Y X Y
J R N R L N R X R G M S S A M O Q C I M N Y P C I F
11 4 17 2 5 14 25 14 23 16 23 23 22 23 19 14 1 23 20 14 25 11 2 17 14 2
E D S M I T H T O L O O K O U T F O R T H E M S T

H N M S S Y W Q D W D K V O B B G L U E B W M Z X D
V U L X Y K X V T A V B B T G H S P A A M M F X I K
20 15 7 18 2 10 15 13 18 1 10 16 15 13 11 15 18 7 18 17 13 12 22 24 14 16
P S M I T H S A I D H E S A W S I M I L A R B O X I

W K S A V U E A S U L C O G R Q L Z W U K I K T J Z
R R W E T N N J C R I H S P N D O R J B K S M B L
5 4 11 19 22 14 13 5 6 22 2 19 22 11 5 8 13 14 19 8 21 13 11 4 11 3
S I N C O U R S E O F C O N S T R U C T I O N I N G

P O W I I X H L J B H F K B W V G G L A G G Y I C Y
D H T A B P B F Y B F X C F F E S T Q U W X B U U E
23 3 24 7 23 14 21 11 12 18 8 10 2 5 4 7 18 9 25 23 19 26 5 19 18 2
A C K Y A R D O F S N I V E L Y S Q U A R T E R S A

V C J A B X N D I W C C C E M H G K Q Q D C B I G R I
P X P E W P Z S F A G H T W J R G F G I Q N T Z X W
24 20 22 19 9 19 22 1 10 1 15 19 14 26 23 16 9 1 7 3 23 24 4 5 23
N D S A W A S I M I L A R B O X W I T H O N E C O R

A Z E H O F O R Z F F J O N F I V S M O Q W T Z I S
B B J Y K R M G I V W Y S G A M F L B Z I M A X V T
1 26 9 3 11 26 1 18 9 11 3 21 22 21 12 22 18 2 18 9 9 18 12 14 22
N E R O P E N A T P O L I C I A B A R R A C K S I

W Z L I E U E Y Z P B Q E Z I Q G O P L V W B T I X
K B A A L N N M I M C Z T N L D S X V R J M O B V J
5 20 8 7 5 14 13 26 4 24 9 17 14 6 21 8 18 4 2 12 17 12 7 4 22 12
T H I S B O X H E R E C O G N I Z E D A C A S E M A

H Q B X R Z S I V Z M C S P Z
V P U N D F A E X J T H G Q O
20 23 14 16 19 13 4 15 13 2 16 19 13 4 15
R K E I D H A I G A N D H A I G

Underlined portions were incorrectly deciphered.

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

AGANA

~~(… AGAN B)~~

DISPATCH No. 4

Key: AGANA. [1]

REF ID:A4126886

4

F S R U X M M F Y E P A

AGAOC g W F L V Y Y Z D X A X W

N A V A L C O U N C I L

J I U K X J S Q S G Z I R K S R Y L L R D Y C O V Z

BHAAO h J U G P K O W R Y H G F H Z F K R L M O B W O Z J V

N O W I N S E S S I O N T O K Y O T O D E T E R M I

O E E K A P N Z R Q B P O S S E P Q D X G D L T N A

CIAAO i C E F P B E V D D T Y K O D E S P B Z Z S C Q X N W

N E D E M A N D S A T P A C I F I C C O N F E R E N

O P R R N F O B Z F L C K G M K C L M X L L J H V V

DJAAO j C A X Y T N I V E R E D Y L T B I L X Z O P F O J K

C E P R A C T I C A L L Y A L L A G R E E R A T I O

O H U D H V O G A K D I C S C B E Y X M P Y I R D K

EKAAO k C S G K V Q I F F V R E E D G D T S Y Y T W W S F L

O F J A P A N E S E V E S S E L S T O U N I T E D S

K V J D W D O A L J Z C Q N M W T Y U O D Y Z C O E

FLAAO l M M L K R M I E C S G D W C T C Q S W V B W S P A C

T A T E S N A V A L V E S S E L S M U S T B E S E V

GMAAO m S N W T S F Y C G P X V R V J C E Y Y V L G W P I P

Q Q P D V U N K Z F F S Y M E P X I N U S Z C O U N X W K A

E N T E N T H S O R T W O S H I P S T O T H R E E S

HNAAO n Y R M K Z O M C L G P C S O Z S C C A N P N X Y W Y

B W H P A H L Z C H J D C P K F I J P I T K C X J A

T O P D E C I D E D T O P U T I N R E S E R V E F O

IOAAO o K S K J H L L Z F N Z Q Y S B Z O L T I X M R U J U

M R O M V Z A D Q Y G V N D C L S L S M A A R B H D

U R P R E D R E A D N A U G H T S S E V E N A R M O

JPAAO p Z A M P K Q A D B R B C O R P U G J I H K A J K L K

W Y H C Q P D O W E Y D O I N J O A L K G S F J S L

R E D C R U I S E R S F I V E C R U I S E R S A L L

KQAAO q M G S P E G R E S I F A I X Z Q F I W M A D U C F M

E Z S C H D B K Y C S I F T K Z Y K F Y R C A P G E

O L D S T O P N A V A L D E L E G A T E S W I L L B

LRAAO r I V D A E S I E U O Z S O B H M Q N W N D U R G O L

T M J A H V Z K N G R B Z F K S D Y R P L A Y J A Y

E V I C E A D M I R A L K A T O C A P T A I N S Y A

MSAAO s B G R U B H C V I Q U A U N G W

O Z X H S W Y S B T O I Q C M C

M A N A S H I A N D N A G A N O

[1] The key as given was in error. It should have read AGAN B instead of AGANA

No 3 BLOCKS

E F G H I J K L M N O P Q R S T U V W X Y Z A B C D

BLOCK L

P Z X X O Z W T S R S F F B X K H Y X B Y
7 19 24 26 15 5 3 5 17 5 22 24 6 23 9 21 22 5 7 19 23
C O M P L E T E G E R M A N F I R E C O N

CMOCK M

J N I R N L I F K V O R A R B V Z U G V A C C N B T
19 15 26 11 17 18 17 19 24 23 7 4 7 20 11 7 1 11 24 19 26 10 12 20 19 24
T R O L S Y S T E M A V A I L A B L E T O U N I T E

DNOCK N

Y L P C W T O L Q D V H A Z Z G Z P G J P F E R M Q
18 1 16 25 16 6 1 11 5 7 18 14 7 6 5 16 1 25 24 6 1 9 1 16 6 20
D S T A T E S F O R D I R E C T S A L E S Y S T E M

EOCK O

U D P K F K Q E M D S O D L M O K R T D U V C A N L
12 6 16 23 13 15 10 22 23 7 12 20 9 22 7 5 9 26 21 3 20 20 12 9 7 22
E M P L O Y S A L T E R N A T I N G C U R R E N T A

FPOCK P

Z Q B O R W I U P F H Q O O G X M T M I J M V U B Z
10 23 14 8 19 8 17 17 1 11 8 17 22 13 3 13 12 3 9 24 10 1 13 21 19 3
N D H A S A C C U R A C Y T O T W O M I N U T E S O

GQOCK Q

G A H P N G Q R J F T L S I P N L W C K I E T H I K
14 13 19 22 17 25 10 18 12 1 1 9 26 13 2 17 23 13 21 11 18 11 19 14 11 22 25
F A R C S T O P G E R M A N S H A V E P E R F E C T

HROCK R

O S E R O I B J O P H X S V X G L Y U F Y A E L G K
25 19 9 11 11 9 26 9 21 24 8 9 13 1 18 16 13 22 18 25 8 18 1 23 12 25
E D A P P A R A T U S A L O N G L I N E S N O W B E

ISOCK S

O L A L F V E F H R N Z D X I X Z K V B G I Q P M L
25 1 21 24 13 11 13 19 15 3 13 24 9 8 21 13 11 13 12 16 19 13 19 13 6 22
I N C R E A S E L O P E D B Y G E N E R A L E L E C T

JTOCK T

R Y H A Q H Q U G Q X O U K C M P A Q U R N Z E A C
2 24 19 19 4 5 10 17 7 12 6 20 4 10 1 17 10 17 7 8 6 8 17 25 9 21
R I C C O M P A N Y S T O P J A P A N E S E A B O U

KUOCK U

X N T X I C L R S Z O A A P H B I K S D C H R Y R S
15 15 23 16 23 22 16 18 6 2 7 22 7 4 23 15 3 13 15 3 23 22 24 17 23 1
T T O C O N C L U D E N E G O T I A T I O N S F O R

LVOCK V

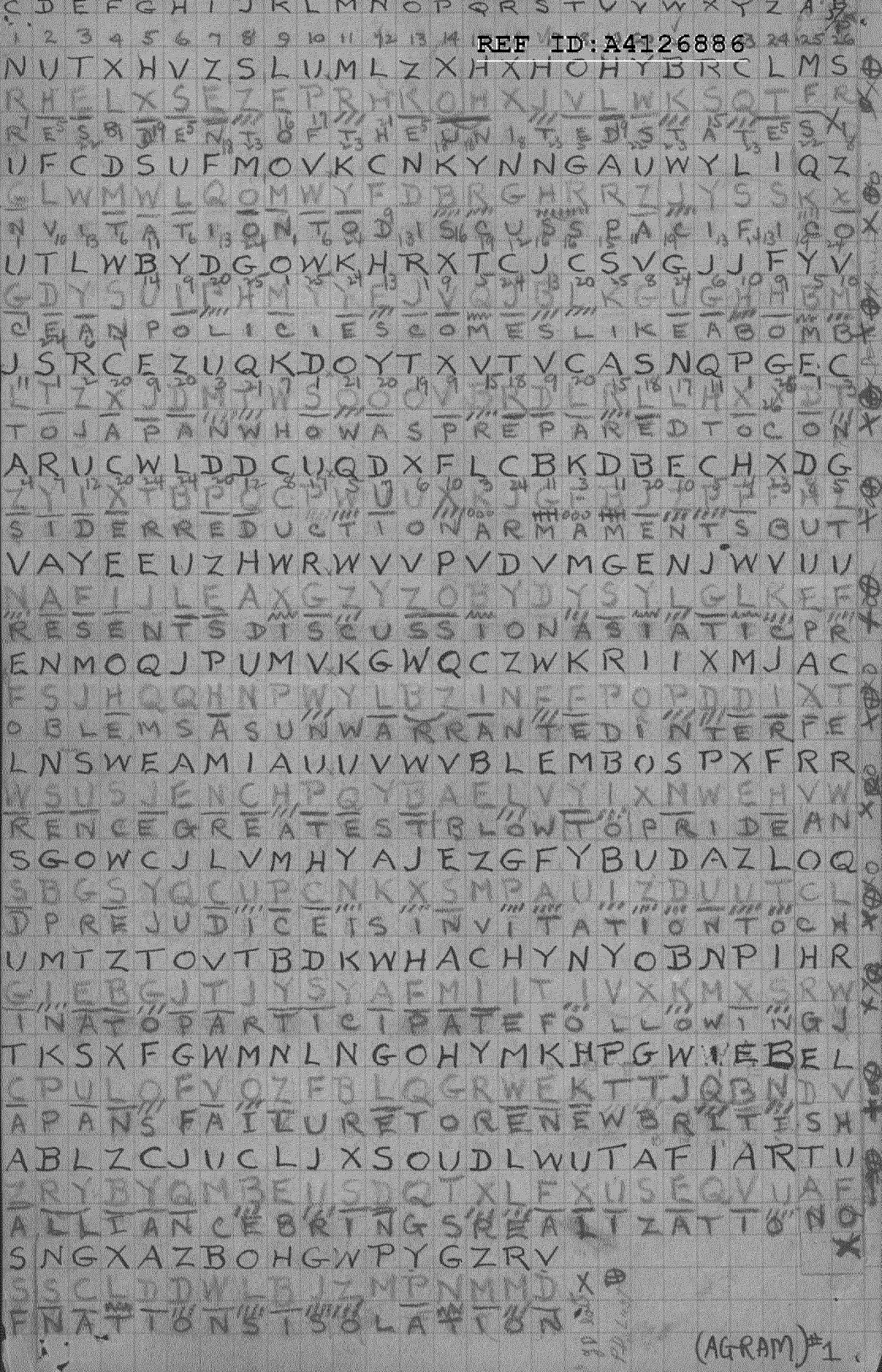
W W D Y C Q S K K U B J I Q W Q F J H N U K Z U S D
5 7 17 9 6 21 4 14 24 22 4 21 25 14 4 8 24 5 1 14 20 14 17 21 10 16
P U R C H A S E O F S A M E S T O P G E N E R A L D

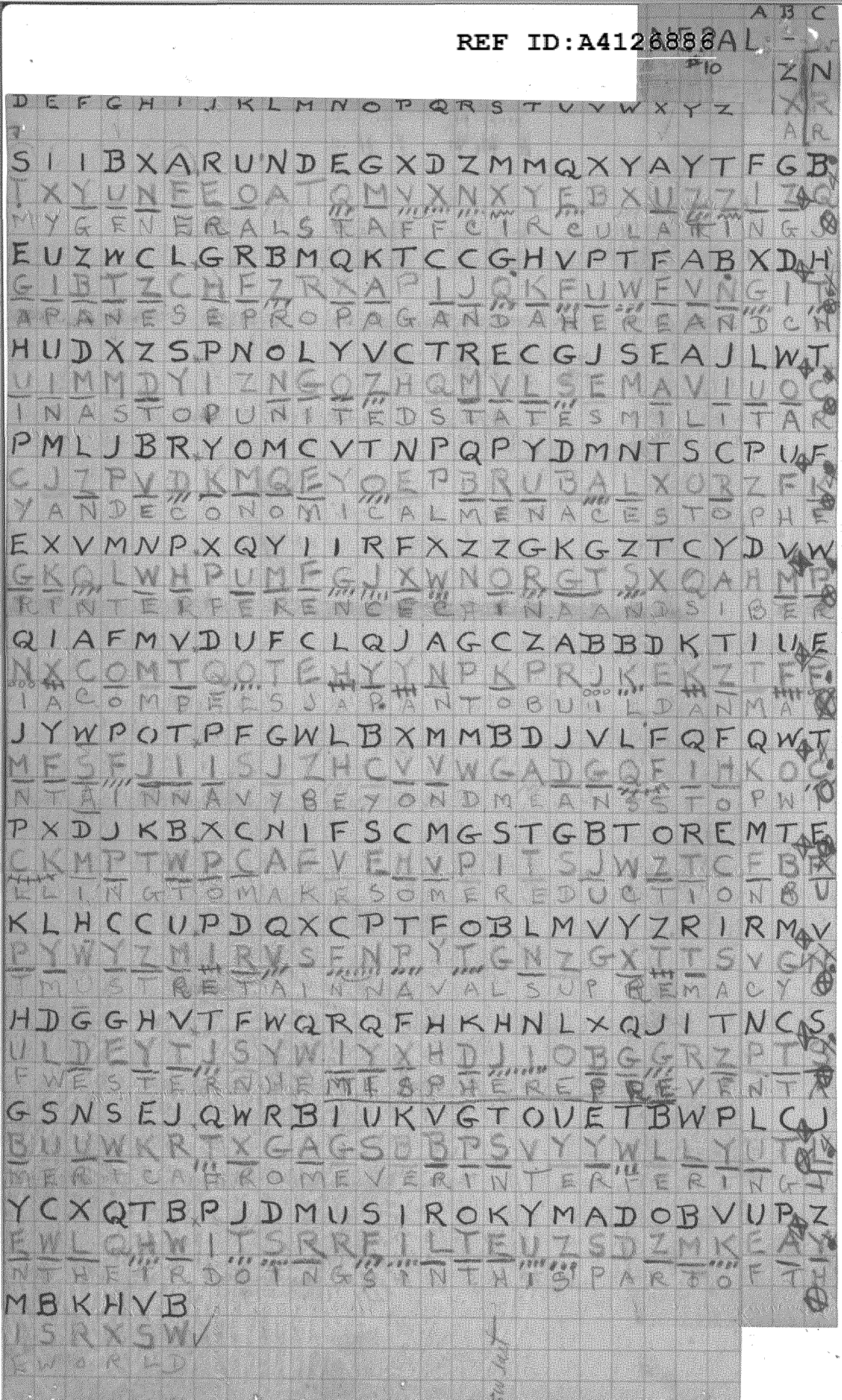
MWOCK W

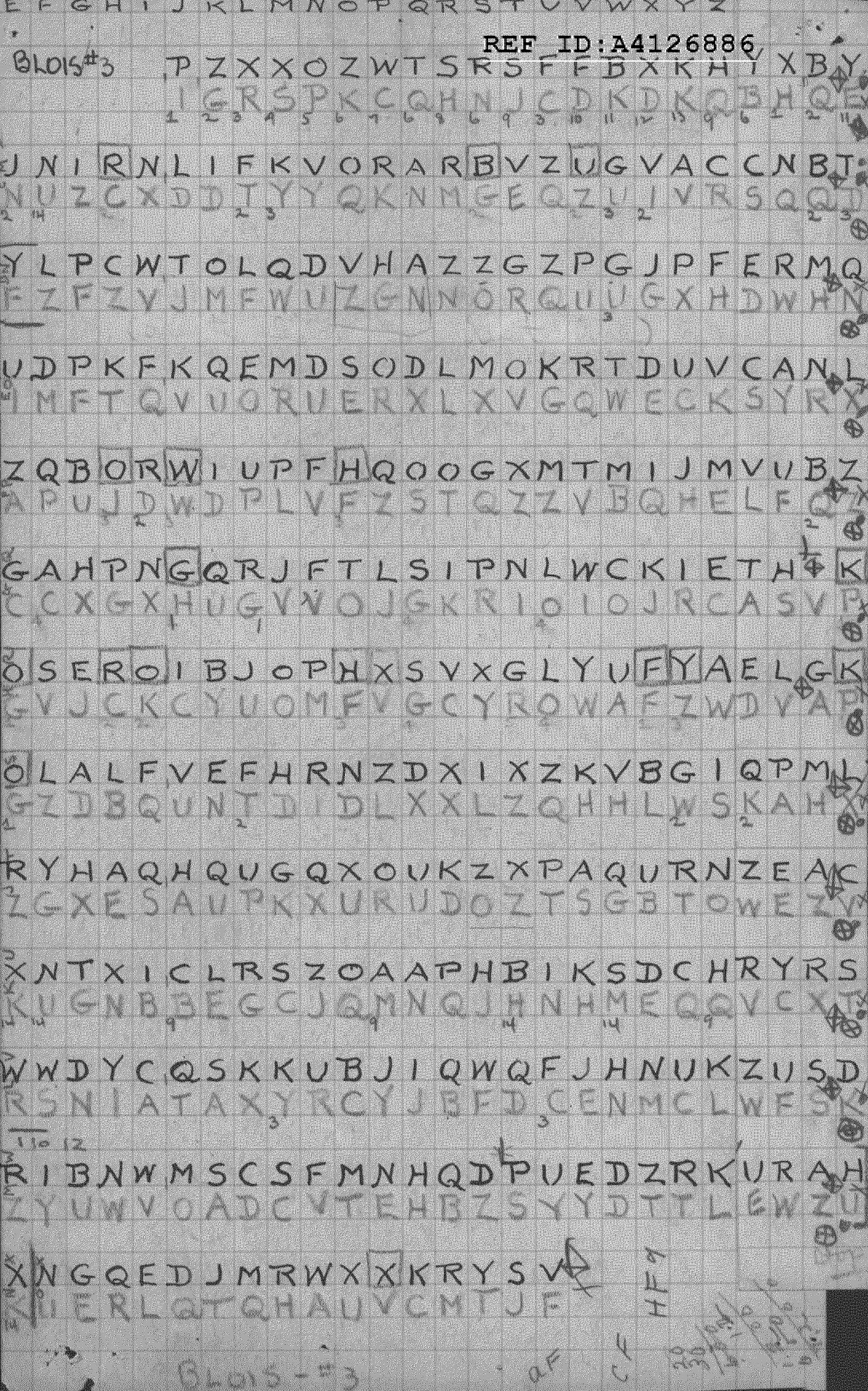
R I B N W M S C S F M N H Q D U P P U Q L U U R A H
2 5 14 10 16 24 4 16 6 11 16 11 18 14 14 6 10 25 18 11 14 2 26 16 4 17
E S C R I P T I O N I N A C C O R D A N C E W I T H

NXOCK X

X I N G Q E D J M R W X X K R Y S V
15
M Y R E P O R T N U M B E R O N E
E F G H I J K L M N O P Q R S T U V W X Y Z A B C








REF ID:A4126886

SECRET CONFIDENTIAL REF ID:A4126886 RESTRICTED

DATE 11 April 47

TO	FROM	TO	FROM
Chief, ASA (10)		Ch, Security Div (80)	
Executive O (11)		Tech Staff (81)	
Co'r Joint Oper (12)		Ch, Materiel Br (82)	
Deputy Chief, ASA (20)		Ch, Methods Br (83)	
Dir, Comm Res (14)	✓	Ch, Protective Br (84)	
Ch, Pers Sec (21)		Ch, Maint Br (85)	
Ch, Org & Tng Sec (22)		Ch, Res & Dev Div (70)	
Ch, Plans & Oper (23)		Tech Staff (71)	
Ch, Materiel Sec (24)		Ch, Ch. Ciph & Cif Br (72)	
Ch, Fiscal Sec (25)		Ch, Int Equip Br (73)	
Adjutant, ASA (26)		Ch, Elec & Elec Br (74)	
Ch, Sec Cont Sec (27)		Ch, Lab Serv Br (75)	
✓ Ch, Operations Div (90)		Ch, C'logic Br (76)	
Ch, Lab Br (91)		Ch, Pers & Tng Br (61)	
Ch, Machine Br (92)		Ch, Supply Br (62)	
Ch, Crypt Br (93)		Co, Arlington Hall (40)	
Ch, Int Cont Br (94)			
Ch, I & D Br (95)			
Tech Staff (96)			

( ) Approval & Return
(✓) As Requested
( ) Concurrence or Comments
( ) Information & Forwarding
( ) Information & Return
( ) Information & File
( ) Recommendation
( ) Signature if approved
( ) Your action by
( ) Info upon which to base reply

Pse look this over at your earliest convenience + then call me. I think this is a good way to go at the problem.

You might suggest rearrangement of the order of the enclosures - I am not sure its the best as I have it now.

WDGAS FORM NO. 96 (Rev. 11) 31 Oct 46 44412

7

1st Ind

William F. Friedman, WDGAS-14 11 April 1947

TO: Chief, Army Security Agency

1. Reference is made to paragraph 1a of the inclosure to the basic letter. In view of the interpretation made of the meaning of that paragraph, as set forth in ASA Memorandum dated 10 April 1947, Subject: "Procedure for Release of Information Concerning Secrecy Patents", information is requested as to the bearing that interpretation has on the question dealt with in the basic letter in regard to the status of Patent Application No. 443320. It is also requested that clarification be made as to what rights, if any, the inventors may have in regard to Patent Application No. 443320 under paragraph 1b of the policy directive forming Inclosure 1 to basic letter, in the light of the recent interpretation of the meaning of paragraph 1a thereof.

2. This indorsement is submitted on the premise that it would be to the advantage of the Army Security Agency, the War Department, and the Government as a whole, as well as to the inventors as individuals, to seek some clarification of the rights of inventors of equipment which must be safeguarded and held in a classified status for a relatively long period of time, since a clarification of this point might assist in formulating

a policy which would be most conducive to the stimulation of invention by Army Security Agency personnel.

3. In connection with the foregoing, there are submitted herewith, as information pertinent to the circumstances, nine inclosures listed below.

4. This matter has been discussed with Mr. F. B. Rowlett, co-inventor in the case of Patent Application No. 443320, and this indorsement is submitted on behalf of both inventors.

9 Incls

1. Ltr dtd 27 Jan 47 to President frm Acting Secretary of War w/incls-3
2. Cy of Memo for Record, dtd 19 December 46, Subj: Conference on Proposed Patent Policy
3. Cy of Brief by Chief of the Patents and Inventions Br, Legal Div., OCSigO dtd 10 March 47
4. Cy of Memo for Judge Advocate General, dtd 14 Apr 44
5. Cy of 2nd Ind from JAGO to Asst. Sec. of War, dtd 17 Jan 36
6. Cy of 2nd Ind from JAGO to Adj. General, dtd 19 Apr 35
7. Cy of Brief by Chief of Patents and Inventions Br., Legal Div., OCSigO dtd 15 Feb 47
8. Cy of ltr from Patents & Inventions Council, Legal Div., OSCigO, dtd 10 June 46 to Mr. W.F.Friedman
9. Cy of ASA Memo dtd 10 Apr 47, Subj: Procedure for Release of Info. Concerning Secrecy Patents

WILLIAM F. FRIEDMAN

~~SECRET~~ CREET ID:A4126886

HEADQUARTERS
ARMY SECURITY AGENCY
WASHINGTON 25, D. C.

WDGSS-23 20 May 1946

SUBJECT: Release of Patent Application Serial No. 443,320

TO: Mr. William F. Friedman, WDGSS-14

1. Reference your letter dated 27 September 1945, subject as above, the attached memorandum from the Acting Deputy Assistant Chief of Staff, G-2, outlines the War Department policy on the release of cryptographic principles.

2. Analysis of the policy would indicate that:

a. Patent application No. 443,320 will not be released unless it can be shown that the employment of the principles involved are susceptible to cryptanalysis under all circumstances; and

b. If not released, a request for purchase of all commercially exploitable reversionary rights may be entertained provided it can be shown that Frank B. Rowlett and yourself were not directed or employed to experiment on or to invent the principles or improvements embodied in Converter M-228 or Converter M-294.

3. If it is felt that subject Patent Application should be released under (a) above; or if and when it is felt a case should be presented for purchase of rights in conformity with stipulations contained in (b) above, an application for release or purchase, containing pertinent facts and necessary proofs, may be prepared and submitted to the Director of Intelligence through the Chief, Army Security Agency.

Harold G. Hayes

HAROLD G. HAYES
Colonel, Signal Corps
Chief, Army Security Agency

1 Incl
Cy ltr dtd 29 Apr 46,
subj: "Release of Cryptographic Principles"

~~SECRET~~

SECRET

29 April 1946

MEMORANDUM FOR THE CHIEF, ARMY SECURITY AGENCY:

SUBJECT: Release of Cryptographic Principles.

1. The following policy is announced to be effective immediately:

a. Cryptographic principles or devices developed by officers, enlisted men, or civilians employed in any War Department Agency, or patents or patent applications on such principles or devices which are owned by, assigned to, or licensed for use of the War Department will not be released for use of foreign governments or for foreign or domestic commercial or private use until such time as necessary information is available and a procedure established in the Army Security Agency whereby information which is cryptographed by means of such principles or devices can be cryptanalyzed and read under any and all circumstances.

b. Where it is in the interest of the Government of the United States that an employee have no patent rights in cryptographic principles or devices to dispose of, and for the Government to own the entire interest for security reasons throughout any foreseeable future; and where discovery or invention of cryptographic principles or devices has been made by a civilian employee and does not relate to a matter as to which the employee was specifically directed to experiment with a view to suggesting improvements nor was produced as a result of any specific employment or contract to invent a specific device or article; and where an application for patent on such principles or devices has been filed with an assignment-in-trust to the Government for the purpose of maintaining such application in secrecy, the Military Intelligence Division will support, subject to the availability of appropriations, any reasonable request for purchase of all commercially exploitable reversionary rights of the inventor in the patent application.

/s/ CARTER W. CLARKE
Colonel, GSC
Acting Deputy A.C. of S., G-2

SECRET

~~SECRET~~ RELEASED: A4126886 NND 820-95-820899

CSGAS SUBJECT: Patent Application Serial No. 443,320

TO: The Judge Advocate General
Department of the Army
ATTN: Chief, Patents Division

FROM: Director of Intelligence

DATE: 19 Feb 48 COMMENT No. 4
Capt. Rambo/147 Ext 462

1. With reference to the request contained in Comment No. 2, a search of the files of the Army Security Agency fails to reveal the specific evidence upon which the Signal Corps Patent Board based its decision regarding subject patent application.

2. The following information from the files of the Army Security Agency is submitted as evidence which may have been considered by the Signal Corps Patent Board in reaching its decision.

3. Mr. Friedman has been a civilian employee of the Department of the Army since 31 December 1921. His duties as described in the original appointment were: the compilation and preparation of all methods for secret correspondence to be used in the Army; the supervision of instruction of commissioned personnel in the proper use of codes and ciphers; preparation of instructions and papers on such subjects; and compilation of special problems for instruction purposes (Inclosure 2). Formal job descriptions of the type currently in use for civilian employees were not initiated within the OCSigO until 1942 and therefore no such formal job descriptions are available for periods before 1942. However, in the case of Mr. Friedman, written indications of his duties in a form somewhat equivalent to that followed in the currently used job descriptions were found for the years 1930 and 1942. In 1930, Mr. Friedman's job was designated as that of "Principal Cryptanalyst," P-6, and in the year 1942 this title was changed to read "Head Cryptanalyst," P-7, concomitant with a promotion to the next grade (Inclosure 2). Mr. Friedman has held a comparable position since his original appointment under Section 10, Rule II, on 30 December 1921. The responsibilities of the position have greatly increased with the growth of the Army Security Agency, but the basic duties of the position are essentially those for which he was originally appointed (Inclosure 2).

4. Mr. Rowlett was appointed "Junior Cryptanalyst," P-1 in the year 1930. His duties were largely of an independent nature, under the general supervision of "Principal Cryptanalyst," Mr. Friedman. As in the case of Mr. Friedman, his duties remained relatively the same through the years, although his title changed in accordance with his promotions. Descriptions of the duties performed by Mr. Rowlett for the years 1936 and 1941 are inclosed (Inclosure 3). No written descriptions of the work performed by Mr. Rowlett are available between these years for reasons cited in the case of Mr. Friedman, paragraph 3 above.

5. Relative to the rights of Mr. Rowlett in the subject invention, he has been contacted personally and states that he has full knowledge of his rights in the matter and that he concurs fully with the action being taken by Mr. Friedman.

FOR THE DIRECTOR OF INTELLIGENCE:

FEB 20 1948
SIGNED AND SENT OUT

HAROLD G. HAYES
Colonel, Signal Corps
Chief, Army Security Agency

COPIES FURNISHED:
AS-71F
Mr. Friedman
Mr. Rowlett

3 Incls
1. n/c
Added 2 Incls
2. Job info on Mr. Friedman
3. Job info on Mr. Rowlett

~~SECRET~~

~~SECRET~~ 126886

REF DISPOSITION FORM

SUBJECT: Patent Application Serial No. 443,320

TO: JAG FROM: D/I, GSUSA 29 DEC 1947 COMMEN
Colonel McGarr/6967/rsr

1. Mr. William F. Friedman, a civilian government employee of the Army Security Agency, Intelligence Division, has requested certain information on which to prepare a case looking towards disposition to the Government of all commercially exploitable reversionary rights as an inventor in the subject patent application.

2. The policy of the then War Department, A. C. of S., G-2, as announced 29 April 1946 (Tab B-1 of Incl "), is that where it is in the interest of the Government an employee have no patent rights for security reasons in a device he was not specifically directed to invent, the ID will support any reasonable request for purchase of commercially exploitable reversionary rights of the inventor.

3. The Signal Corps Patent Board has rendered a decision that the subject invention was not the result of "- - - specific designation to invent - - ", Tab B-1 to Incl 5.

4. It is considered that the secrecy order now standing against the subject application must be continued (Incl 4).

5. From a legal viewpoint, information is requested on the actions to recover outlined in paragraph 2 a and b of subject letter 8 December 1947 by Mr. Friedman, and the manner in which final action should be accomplished.

FOR THE DIRECTOR OF INTELLIGENCE:

/s/ Bruce W. Bidwell
BRUCE W. BIDWELL, Col, GSC
Assistant Executive

1 Incl
Ltr dtd 8 Dec 47
w/incls (5)

FILE No. JAGP 1948/103-S (5 Jan 48) SUBJECT As above

TO FROM DATE 7 JAN 1948 COMMENT NO. 2

Chief Signal Officer Patents Division, Col. G. W. Gardes/6822
ATTN: Mr. Pernice, Chief, JAGQ
Legal Division.

Reference is made to paragraph 3, Comment No. 1, which states that the Signal Corps Patent Board has rendered a decision that the subject invention was not the result of "specific designation to invent". It is requested that this office be advised of the underlying facts determined by the Board in connection with the employee's status and assignment, including his job designation, which resulted in above decision.

FOR THE JUDGE ADVOCATE GENERAL:

/s/ George W. Gardes
GEORGE W. GARDES, Col, JAGD
Chief, Patents Division

ncl: n/c

~~SECRET~~

COPY

SECRET A4126886

SIGLG-3HMS (29 Dec 47) Patent Application Serial No. 443,320

TO: Chief, Army Security Agency From: Legal Div., OSCigO Date: 15 Jan 48 COMMENT NO. 3
Washington 25,D. C. Saragovitz/73720
Att: Mr. Stauffer

1. In accordance with telephone conversation 14 January 1948 with Colonel Gardes, JAG Patents Division, the inclosed correspondence is forwarded for your direct reply for the reason that subject patent application is now being prosecuted and is under the general jurisdiction of the Army Security Agency, and also because the joint inventors are now employees of the Army Security Agency.

2. A search of the files in this Office failed to reveal any written or documentary evidence upon which the Signal Corps Patent Board based its decision that the subject invention was not the result of specific designation to invent.

3. It is noted that the other joint inventor, Mr. Rowlett, has not entered into the question being raised by Mr. Friedman. It is believed that the rights of Mr. Rowlett in the subject invention must also be taken into account in this matter.

FOR THE CHIEF SIGNAL OFFICER:

/s/ J. E. Pernice
JOHN E. PERNICE
Chief, Legal Division

Incl. n/c

SECRET

~~SECRET~~

CSGAS-14 25 September 1947

MEMORANDUM FOR RECORD

1. Pursuant to an invitation from Captain Safford to participate in a meeting with engineers from Teletype Corporation, the undersigned, accompanied by Dr. Kullback and Dr. Sinkov went to Captain Safford's office at 1000 hours on 9 September 1947.

2. Captain Safford explained that the Teletype engineers were delayed and that he really did not know why they were coming or whether they were bringing any model or models.

3. While waiting for the Teletype engineers to appear, Captain Safford demonstrated two recently completed developments of his own laboratory:

a. A modification of Converter M-228 (SIGCUM) to be known as CSP-3300. This equipment is designed to give improved security for SIGCUM usage especially in connection with the transmission of intercept traffic for OP-20-2. The modified machine eliminates the 131 mixing cabinet and uses relays mounted underneath the frame of the SIGCUM for this purpose. These relays also are used in connection with a baud transposition feature so that the plain text bauds undergo transposition before Vernam-rule substitution. The motion of the rotors has also been modified, with the introduction of reversed stepping in the case of two of the five rotors as an added feature. Off-line (tape) operation was demonstrated but it was my understanding that provision has been or will be made for on-line operation also. This machine is worth ASA's study; however, it will only operate from tape and hence its application is limited.

b. A modification of SIGABA for the production of one-time key tapes. The output of the cryptographic rotors is reduced to 5-unit code symbols. The control and cryptographic rotors are subjected to a different motion control than in SIGABA. The purpose of this equipment is to permit local stations to produce "one-time tapes" from machine settings, so as to have the equivalent of "one-time" intercommunication among a large number of stations when conditions permit.

~~SECRET~~

Otherwise, the one-time tapes can be produced by a central station and distributed to users by courier, as is normally the case. Captain Safford claims that the output is perfectly random. This machine also should be investigated by ASA.

4. Since the noon hour was approaching and the Teletype engineers had not yet arrived, the ASA representatives left, with the statement that other representatives would replace them for a meeting at 1400.

5. The other ASA representatives, Messrs. Rosen and Barlow from AS-70 and Messrs. Kuhn and Brann from AS-80 attended the conference in the afternoon. Mr. Rosen reported to me that the Teletype engineers brought nothing with them, stating that the model of the HOCM would not be completed until sometime in November. The project is apparently not going forward as had been anticipated.

6. The ASA representatives were then shown the model of CSP-3300 discussed under Paragraph 3a above. Mr. Rosen reports that he regards the equipment as too complex, that it uses relays which will not stand up under ordinary usage, and will not perform the functions required of the Converter MX-519()/TG. Mr. Brann, having read the foregoing, makes the following comments:

> "It might be noted that Navy is placing the greater emphasis upon modification of existing equipments instead of development of new ideas. It is believed the CSP 3300 will cause very awkward operational practices in that transmission and encryption will have to be on-line with reception on-line and consequent decryption off-line. This method of operation would not be acceptable to any of the Army using services."

Mr. Kuhn adds the following:

> "In addition to the remarks made by Mr. Brann in connection with the CSP 3300 I believe it might be more economical in the end to build a complete new unit rather than attempt to convert the M-228 unit. The work involved would exceed that now being done to convert a SIGABA to a SIGROD."

WILLIAM F. FRIEDMAN
Chief, Communications Research
Ext 215

A means of providing an irregular wheel movement
in Cipher Machine using cipher wheels.

The basic principle of this invention utilizes the cipher wheels of the cipher machine to provide an irregular selection of the particular wheel which is to be moved. A method of effecting this selection is to provide, in addition to the present ring of 26 contacts on each face of the wheel, a second ring of 26 contacts, which contacts are independent of the first mentioned set of contacts, but are connected to each other in an irregular manner, analogous to the manner in which the first mentioned set of contacts are connected. Also the end plates will bear a double ring of contacts which coincide exactly with the two rings of contacts on the face of each cipher wheel. These two rings of contacts on each end plate are connected as indicated in Figs. 1 and 2 of the attached drawing.

The action of the machine is as follows: When a key is depressed, two contacts are closed, namely, (1) the key contact which allows a current to pass through one of the above-mentioned rings of contacts to operate an indicating device giving the encipherment of the letter corresponding to said key and (2) a universal contact which permits current to enter at a single contact of the other of the aforementioned rings of contacts on one of the end plates, pass through one of the contacts of the corresponding rings of contacts of all the cipher wheels, and pass out at one of the contacts on the corresponding ring of contacts of the other end plate, and thence to a selecting magnet which permits the cipher wheel corresponding

thereto to move forward.

Figure 1 is a schematic diagram of the invention. 1, 2, 3, 4, and 5 are the hereinbefore described cipher wheels; 19 and 20 are the end plates, 6, 7, 8, 9, 10 are the wheel selector magnets which allow a mechanism to step one of the wheels forward at each depression of a key; 11 and 13 are the rings of contacts through which the current passes to the wheel selector magnets; 12 and 14 are the rings of contacts through which the "key to lamp" current passes; 15 is the key contact; 16 is the above-mentioned universal bar contact; 17 is the source of power; 18 the reversing switch; 21 is the indicating device; and 22 is the connection to the universal contact which may be connected to any contact of the rings of contacts 11 on end plate 19.

Fig. 2 shows one manner in which the ring of contacts on end plate 20, through which the current passes to the selector magnets, are connected to the wheel selector magnets.

A means of providing an irregular wheel movement in Cipher Machine ~~of the Hebern and Enigma type~~ using cipher wheels.

The basic principle of this invention utilizes the cipher wheels of the cipher machine to provide an irregular selection of the particular wheel which is to be moved. A method of effecting this selection is to provide, in addition to the present ring of 26 contacts on each face of the wheel, a second ring of 26 contacts, which contacts are independent of the first mentioned set of contacts, but are connected to each other in an iregular manner, analogous to the manner in which the first mentioned set of contacts are connected. Also the end plates will bear a double ring of contacts which coincide exactly with the two rings of contacts on the face of each cipher wheel. These two rings of contacts on each end plate are connected as indicated in Figs. 1 and 2 of the attached drawing.

The action of the machine is as follows: When a key is depressed, two contacts are closed, namely, (1) the key contact which allows a current to pass through one of the above-mentioned rings of contacts to operate an indicating device giving the encipherment of the letter corresponding to said key and (2) a universal ~~bar~~ contact which permits current to enter at a single contact of the other of the aforementioned rings of contacts on one of the end plates, pass through one of the contacts of the corresponding rings of contacts of all the cipher wheels, and pass out at one of the contacts on the corresponding ring of contacts of the other end plate, and thence to a selecting magnet which permits the cipher wheel corresponding

thereto to move forward.

Figure 1 is a schematic diagram of theinvention. 1, 2, 3, 4, and 5 are the hereinbefore described cipher wheels; 19 and 20 are the end plates, 6, 7, 8, 9, 10 are the wheel selector magnets which allow a mechanism to step one of the wheels forward at each depression of a key; 11 and 13 are the rings of contacts through which the current passes to the wheel selector magnets; 12 and 14 are the rings of contacts through which the "key to lamp" current passes; 15 is the key contact; 16 is the above-mentioned universal bar contact; 17 is the source of power; 18 the reversing switch; 21 is the indicating device; and 22 is the connection to the universal ~~bar~~ contact which may be connected to any ~~one~~ contact of the rings of contacts 11 on end plate 19.

Fig. 2 shows ~~the~~ one manner in which the ring of contacts on end plate 20, through which the current passes to the selector magnets, are connected to the wheel selector magnets.

A means of providing an irregular wheel movement in Cipher machine of the Hebern and Enigma type.

The basic principle of this invention utilizes the cipher wheels of the cipher machine to provide an irregular selection of the particular wheel which is to be moved. A method of effecting this selection is to provide, in addition to the present ring of 26 contacts on each face of the wheel, a second ring of 26 contacts, which contacts are independent of the first mentioned set of contacts, but are connected to each other in an iregular manner, analogous to the manner in which the first mentioned set of contacts are connected. Also the end plates will bear a double ring of contacts which coincide exactly with the two rings of contacts on the face of each cipher wheel. These two rings of contacts on each end plate are connected as indicated in Figs. 1 and 2 of the attached drawing.

The action of the machine is as follows: When a key is depressed, two contacts are closed, namely, (1) the key contact which allows a current to pass through one of the above-mentioned rings of contacts to operate an indicating device giving the encipherment of the letter corresponding to said key and (2) a universal contact which permits current to enter at a single contact of the other of the aforementioned rings of contacts on one of the end plates, pass through one of the contacts of the corresponding rings of contacts of all the cipher wheels, and pass out at one of the contacts on the corresponding ring of contacts of the other end plate, and thence to a selecting magnet which permits the cipher wheel corresponding

thereto to move forward.

Figure 1 is a schematic diagram of theinvention as applied to a cipher type machine. 1, 2, 3, 4, and 5 are the hereinbefore described cipher wheels; 19 and 20 are the end plates, 6, 7, 8, 9, 10 are the wheel selector magnets which allow a mechanism to step one of the wheels forward at each depression of a key; 11 and 13 are the rings of contacts through which the current passes to the wheel selector magnets; 12 and 14 are the rings of contacts through which the "key to lamp" current passes; 15 is the key contact; 16 is the above-mentioned universal bar contact; 17 is the source of power; 18 the reversing switch; 21 is the indicating device; and 22 is the connection to the universal ~~bar~~ contact which may be connected to any one of the rings of contacts 11 on end plate 19.

Fig. 2 shows ~~the~~ one manner in which the ring of contacts on end plate 20 through which the current passes to the selector magnets are connected to the wheel selector magnets. ~~[illegible] connections may be made at random and the [illegible] of any multiple of each connection~~

A random selection of these contacts may be made for connections to the ~~[illegible]~~ wheel selector magnets. Also current may enter at one or more ~~points~~ contacts on the opposite end plate, effecting a movement of one or more wheels per cycle.

A means of providing an irregular wheel movement in Cipher Machine of the Hebern and Enigma type.

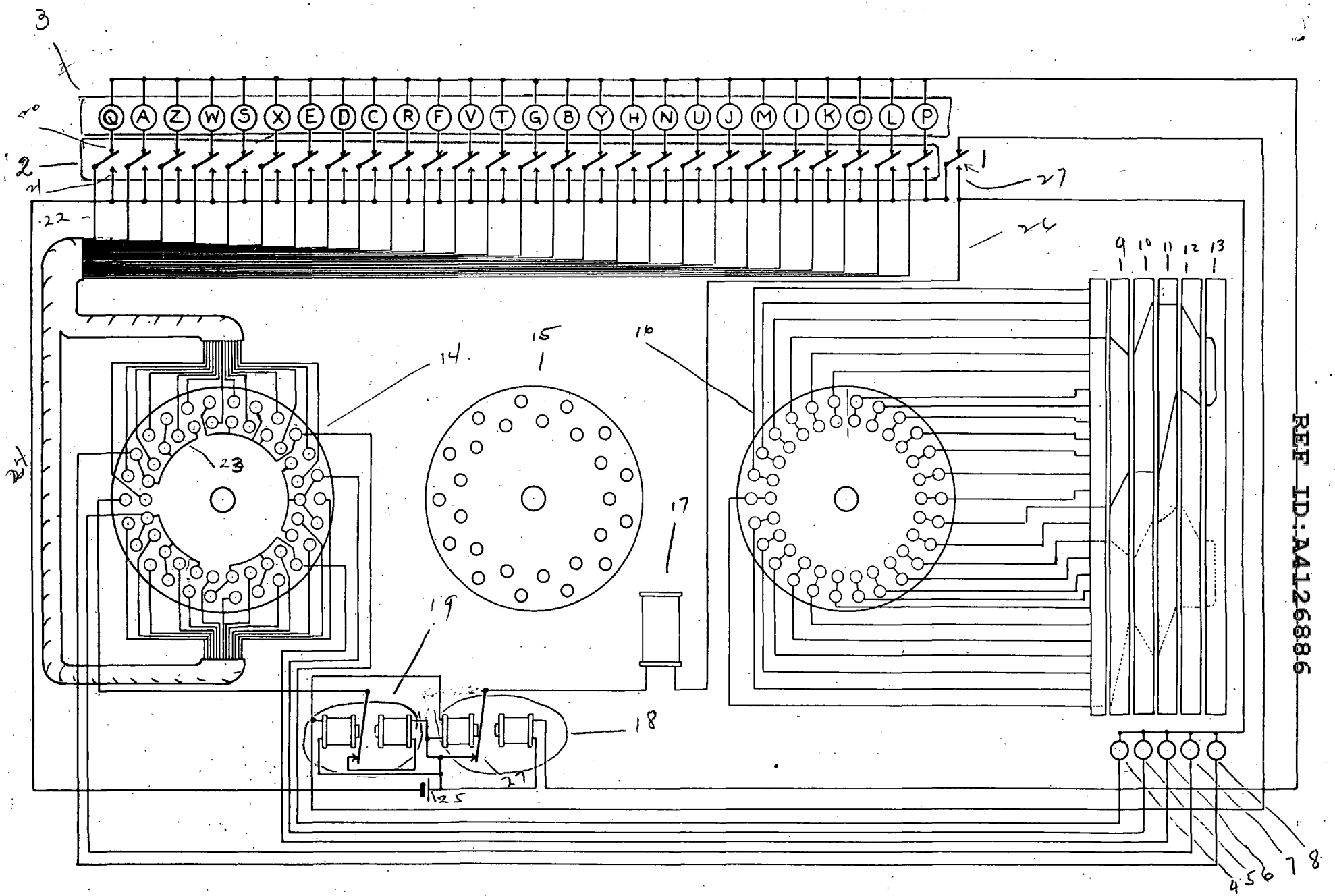
The basic principle of this invention utilizes the cipher wheels of the cipher machine to provide an irregular selection of the particular wheel which is to be moved. A method of effecting this selection is to provide, in addition to the present ring of 26 contacts on each face of the wheel, a second ring of 26 contacts, which contacts are independent of the first mentioned set of contacts, but are connected to each other in an iregular manner, analogous to the manner in which the first mentioned set of contacts are connected. Also the end plates will bear a double ring of contacts which coincide exactly with the two rings of contacts on the face of each cipher wheel. These two rings of contacts on each end plate are connected as indicated in Figs. 1 and 2 of the attached drawing.

The action of the machine is as follows: When a key is depressed, two contacts are closed, namely; (1) the key contact which allows a current to pass through one of the above-mentioned rings of contacts to operate an indicating device giving the encipherment of the letter corresponding to said key and (2) a universal bar contact which permits current to enter at a single contact of the other of the aforementioned rings of contacts on one of the end plates, pass through one of the contacts of the corresponding rings of contacts of all the cipher wheels, and pass out at one of the contacts on the corresponding ring of contacts of the other end plate, and thence to a selecting magnet which permits the cipher wheel corresponding

thereto to move forward.

Figure 1 is a schematic diagram of theinvention. 1, 2, 3, 4, and 5 are the hereinbefore described cipher wheels; 19 and 20 are the end plates, 6, 7, 8, 9, 10 are the wheel selector magnets which allow a mechanism to step one of the wheels forward at each depression of a key; 11 and 13 are the rings of contacts through which the current passes to the wheel selector magnets; 12 and 14 are the rings of contacts through which the "key to lamp" current passes; 15 is the key contact; 16 is the above-mentioned universal bar contact; 17 is the source of power; 18 the reversing switch; 21 is the indicating device; and 22 is the connection to the universal bar which may be connected to any one of the rings of contacts 11 on end plate 19.

Fig. 2 shows the manner in which the ring of contacts on end plate 20 through which the current passes to the selector magnets are connected to the wheel selector magnets.


Q A Z W S X E D C R F V T G B Y H N U J M I K O L P
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
REF ID: A4126886

A means of providing an irregular wheel movement in cipher machines of the Hebern ~~type~~ and Enigma type.

The basic principle of this ~~invention is~~ utilizes the cipher wheels of the Hebern cipher machine to provide an irregular selection of the particular wheel which is to be moved. A method of ~~effecting this~~ selection is to provide, in addition to the present ring of 26 contacts on ~~each~~ face of the wheel, a second ring of 26 contacts, which contacts are independent of the ~~first set of co~~ first mentioned set of contacts, but are connected to each other in an irregular manner, analogous to the manner in which the first mentioned set of contacts are connected. Also the end plates, ~~providing a means of~~ will bear a double ring of contacts

which coincide exactly with the two rings of contacts on the face of each cipher wheel. These two rings of contacts on each end plate are connected as indicated ~~in the fig 1 of~~ on the 2 of the attached drawing. ~~and in the description thereof which follows. Upon the key the current~~

R/ The action of the machine ~~will~~ is as follows: When a key is depressed, two contacts are closed, namely (1) the key contact which allows a current to pass through pairs of the aforementioned rings of contacts to operate an indicating device giving the encipherment of the letter corresponding to said key and (2) a universal bar contact which permits current to enter at a single contact on one of the end plates, pass through one of the contacts of the corresponding rings of contacts of all the cipher wheels and pass out at one of the corresponding contacts on the other end plate, and thence to a selecting magnet which permits the cipher wheel corresponding thereto to move forward.

Figure 1 is a schematic diagram of the invention. 1, 2, 3, 4, and 5 are the hereinbefore described cipher wheels; 19 and 20 are the end plates, 6, 7, 8, 9, 10 are the wheel selector magnets which allow a mechanism to step one of the wheels forward at each depression of a key; 11 and 13 are the rings of contacts through which the current passes to the wheel selector magnets; 12 and 14 are the rings of contacts through which the "key lamp" current passes; 15 is the key contact; 16 is the aforementioned numeral bar contact; 17 is the source of power; 18 the reversing switch; and 21 is the indicating device; and 22 is the connection to the numeral bar which may be connected to any one of the rings of contacts on end plate 19.

Fig 2 shows the manner in which the rings of contacts through which the current passes to the wheel selector magnets on end plate 20 are connected to the wheel selector magnets.

RECORD OF MILITARY INVENTION

WAR DEPARTMENT
Office of the Chief of Air Service
Patents Section
Munitions Building, Washington, D. C.

(Use separate sheet for each invention)

FOLLOW INSTRUCTIONS ON BACK

(a) Inventor:
(1) Name: W. F. Friedman — J B Rowlett
(2) Rank, position or employment: Cryptanalyst — Jr Cryptanalyst
(3) Permanent address: Wash D C — Falls Church, Va

(b) Title of Invention: System for Randomizing the Relation of Electrical Circuits

(c) Description of Invention. See Description and drawing attached.

(d) Dates and places of Invention:
(1) Conception by inventors: June 15, 1935 at Wash. DC
(2) Disclosure to others: No at
(3) First sketch or drawing: June 24 1935 at Wash
(4) First written description: June 24. 1935 at Wash
(5) Completion of model or full sized device: None at
(6) First test or operation of invention: None at

(e) Results of tests, and extent of use of invention: None

(f) Names of persons having knowledge of facts stated under (d) and (e): None

(g) Prior Reports: None

(h) Patents and Patent applications: None other than present application

(i) Rights of U.S.Government: Usual license

(j) Licenses or Assignment: None

(k) Contracts involved: None — Orig & 1 Carbon

Contractors
Contract No. and date
Subject matter
Location of Plant
Official title or status of employment of inventor:

Address

Type of Contract

(l) Signature of witness and date:

Signature of inventor and date: WFF & JBR

(m) Remarks of Forwarding Officer:

Signature of Forwarding Officer and date:

W-892, A.S. Rev. 6/2/24

INSTRUCTIONS

The following information will be given under the headings indicated:

(a) The inventor should give his permanent address. He should also give his rank, corps, position or status of employment at the time invention was made.

(b) The title of the invention should start with words indicating the class to which the invention belongs, such as "Method of" or "Process of" in case the invention relates to a method or process; or the name of the article, device or type of machine in case the invention relates to an article, device or machine, or the name of the material or composition in case the invention is an improvement in material or composition.

(c) The description of the invention may be brief, provided reference is made to detailed specifications and drawings, which should be identified by date and file number if official, or should be attached to the report if not part of the official records of the War Department. In either case, all drawings and descriptive pamphlets relating to the invention should be listed.

(d) Care should be taken to give the earliest date on which the invention suggested itself to you, even though it was not completely in mind. If the invention comprises different inventive ideas, give the dates with reference to each part of the invention separately, taking care to identify each part clearly in the description of the invention.

(e) State whether or not the invention was found to be operative, and the degree of success attained at each test of the model or full sized device. In stating the extent of use of the invention, separate "use by the Government" from "commercial use".

(f) State the names of persons who had knowledge of the invention and facts concerning it on or about the dates mentioned.

(g) Has description of invention or report of test, if any, been submitted to officers of the War Department? If so, when and to whom? Give references to all prior reports, including all information needed to locate same in files.

(h) List all applications for patents by filing dates, serial number and title. List all patents by patent number, date of grant, and title.

(i) Has tender to the United States been made? If so, when and to whom? If not, tender the use of the invention to the United States or explain why not.

(j) State what, if any, rights in the inventions have been granted to others; including extent of interest granted and date of recording assignment or license in Patent Office.

(k) If contracts have been placed for the invention, or if the invention was made in connection with the performance of a contract in which the United States is interested, the facts should be given briefly, including contractor's name and address; Contract No. and Date of Contract; Subject Matter; Location of Contractor's Plant where work was done; and Official Title or Status of Employment of Inventor.

(l) It is desirable that the witness be familiar with the facts stated concerning the invention and have a sufficient understanding of the invention to describe its construction and operation.

(m) The forwarding officer should give his opinion of the value of the invention to the U.S. and whether or not the prospective development or the art to which the invention relates would make it advisable to protect the invention and the Government's right to use the same by an application for patent.

Report on M-228

1 Col.Corderman

1. There is appended herewith a report on the security of the M-228. The material on which this study was based was taken from War Department channels and is a true indication of the type of security which may be expected from usage of this equipment.

2. The recommendations given below were arrived at in a conference among Major Rosen, Major Hiser, Captain Douglas and myself:

a. It is recommended that a study be undertaken immediately by the ablest cryptanalysts in SSS to determine if it is possible to reconstruct the cryptographic elements used in the M-228 under the conditions stated in the appended discussion.

b. It is further recommended that the M-228 be used for confidential and lower classification on radio, and then only under special conditions where complete supervision and control can be exercised by personnel properly trained in handling the M-228 both from operational and security standpoints; that for such use special keys will be arranged; that typing reperforators or equivalent equipment be used; and that under no circumstances will conference calls be permitted.

c. It is further recommended that no change be made in the present use of the M-228 on circuits such as land lines which are reasonably secure from interception.

d. It is further recommended that a study be undertaken to determine the most expeditious method of handling traffic over channels similar to the

Report on M-228

1 (cont'd) Washington-London, Washington-Brisbane, or Washington-Algiers channels. This study should be directed towards evaluating the relative merits of fully automatic versus systems using the 134-C and usual transmission agencies.

Att: Report w/10 Incls.

Frank B. Rowlett
Major, Sig.C.
SPSIS-4
8 June 1943

Report To: Colonel Corderman

Subject: Report on the M-228

1. The M-228 is the mechanism for generating a key which is used for the encipherment of plain-text signals generated by a teletypewriter mechanism. The invention of the cryptographic principle was made at SSS and reduced to practice at the SCGDL. The electrical application of the cryptographic key generated by the M-228 is almost identical with that proposed by Gilbert S. Vernam in 1918 and later. (See Vernam patents attached.) The M-228 was proposed initially for encipherment of messages to be transmitted on land lines. It was not contemplated that it should be used for enciphering signals to be transmitted by radio.

2. The relationship between the teletype, the M-228 (key generator) and the device (applique unit) which "scrambles" the plain-text signals is shown in the schematic diagram of Fig. 1. The teletype generating the plain-text signals is standard equipment which feeds the signals into a group of relays inside the applique unit. The M-228 consists of a set of 5 cipher wheels which, in conjunction with a teletype distributor head, generate an extremely long sequence of impulses similar to the plain-text signals. The impulses of the M-228 are fed into the relays of the applique unit where the combination of the plain-text and key impulses are effected as described below, to produce cipher text. On the receiving end the conditions are reversed. The signals of the enciphered text are fed into the relays of the applique unit where the key generated by the M-228 is removed and the remaining plain-text signal is fed into a standard teletype printer to produce the plain text version of the message.

3. a. Cryptanalytically, the encipherment effected by the applique unit can be expressed as a mathematical equation with elements of a limited binary system of 32 combinations. The Baudot Code used by the teletype is nothing more than the expression of 32 conditions by means of combinations of elements referred to hereinafter as + and —. The equation stating the conditions of encipherment is simply $P + K = C$.

b. In the case of the encipherment of a single letter, say the first letter of a message, the specific equation will become $P_1 + K_1 = C_1$. Likewise, the second, third, and fourth

encipherment, etc., may be expressed by the same type of equation using the appropriate subscripts, $P_2 + K_2 = C_2$ etc. Given the conditions that two messages are enciphered by the same key, if the second message is represented by primes, these equations may be written as $P_1' + K_1 = C_1'$ etc.

c. Given the first letters of two messages enciphered by the same key the equations pertaining to those two letters are:

$$P_1 + K_1 = C_1$$

$$P_1' + K_1 = C_1'$$

Since C_1 and C_1' are the cipher texts of the messages which will be available to the cryptanalyst, C_1 and C_1' may be considered as known, giving 2 equations with 3 unknowns. By subtracting one equation from the other, the K_1's can be eliminated giving $P_1 - P_1' = C_1 - C_1'$, a single equation with 2 unknowns. This equation can be solved since the conditions that P_1 and P_1' must be plain-text letters can be applied. Practically, this would be effected by considering several equations at one time and examining a probable word for either the P or the P', as indicated in the following paragraphs.

4. a. There is attached a chart (inclosure #2) which gives the Baudot equivalents of the 26 letters of the alphabet plus the 6 functions of the teletype giving a total of 32 distinct combinations. As stated above in Par. 3b these combinations may be considered as elements of a system of binary notation and the customary processes of addition, subtraction, multiplication, and division may be applied. The cryptographic function of the relays of the applique units is to perform addition of the 5 impulses of the plain text letters generated by the teletypewriter with the 5 impulses generated by the M-228. Since all 32 possible combinations are generated by the M-228, a total of 32 x 32 conditions will arise from the addition of a plain-text signal and a key signal. This can be best demonstrated by performing an example in addition which simulates the action of the relays. Suppose the plain text to be enciphered is the plain-text word THE. The Baudot equivalents for the 3 letters are shown below:

T = - - - - +
H = - - + - +
E = + - - - -

Let it be assumed that the key generated by the M-228 at the instant is:

1st Key combination: + - + + +
2nd Key combination: - + + + +
3rd Key combination: + - + - +

In reference is made to the accompanying chart (Incl. No. 2), it will be noted that the first key combination corresponds to the letter X, the second to the letter V, and the third to the letter Y. The addition performed by the relays of the applique unit can be effected by the application of the following rule: If two like elements are added a + is obtained; if two unlike elements are added, a - is obtained. The addition in this case will be non-carrying, and since only two elements are used in the system it will be noted that addition and subtraction produce identical results. Based on this rule,,the addition of T and the first key combination produces a combination which corresponds to the letter L; H and V give Y; and E and Y give J, as shown herewith:

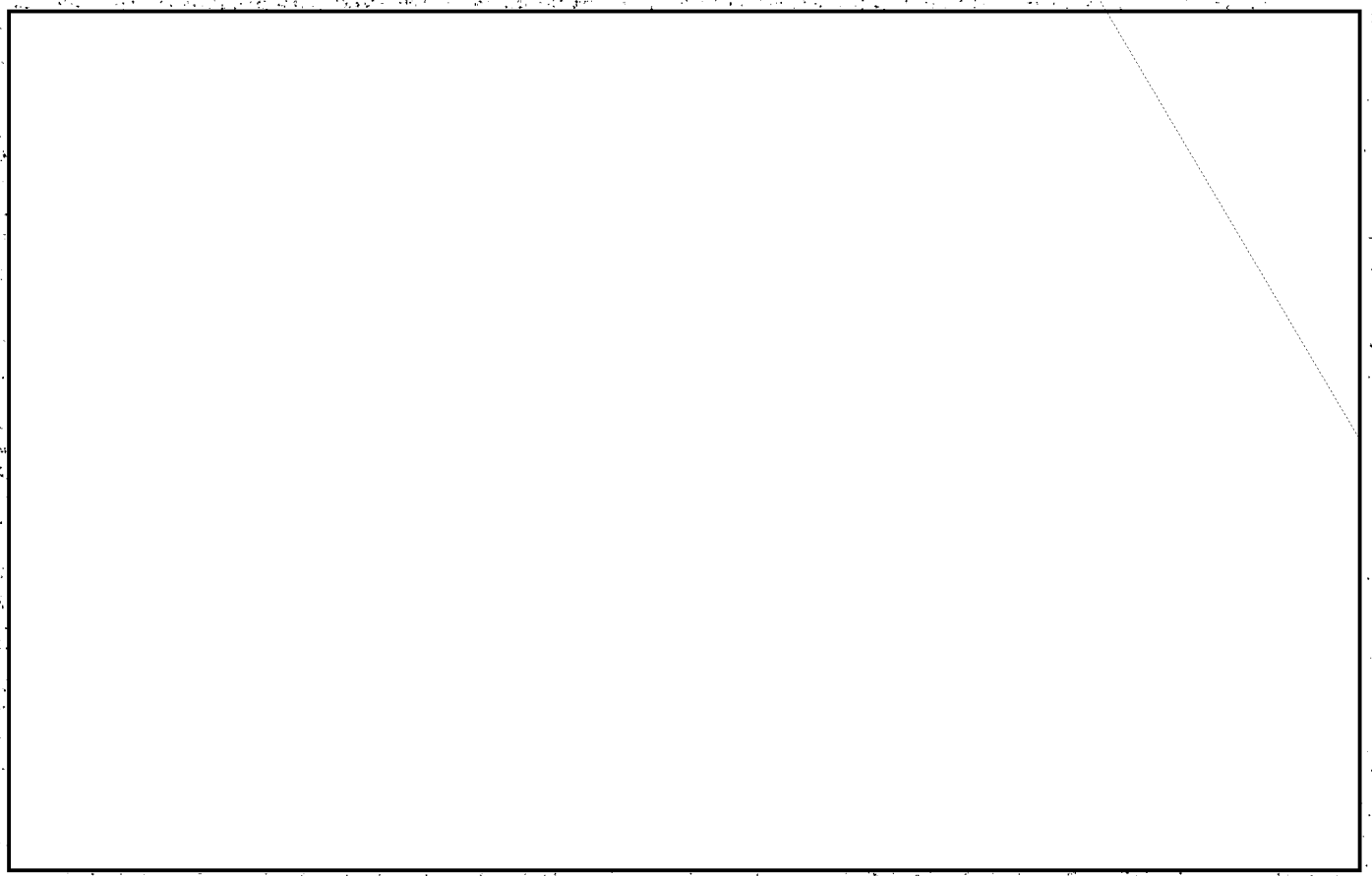
First key combination	T (X)	- - - - +	
		+ - + + +	1st Letter
		- + - - + =	L
2nd Key combination	H (V)	- - + - +	
		- + + + +	2nd Letter
		+ - + - + =	Y
3rd Key combination	E (Y)	+ - - - -	
		+ - + - +	3rd Letter
		+ + - + - =	J

b. As stated above, the addition of each of the 32 elements with itself and all the other elements gives $(32)^2$ combinations. These combinations are represented in table attached (Incl. No. 3). Reference to this table permits rapid addition of plain text and key to give cipher, or an addition of cipher and key to produce plain text. The table is reciprocal in nature and may be used as follows: The plain-text letter is sought in the sequence at the left hand side of the table; the key letter is sought in the sequence at the top of the table; at the intersection of the row and column so defined, the cipher-text letter is found.

~~SECRET~~

Given a cipher text message with an assumed plain text and a second message prepared in the same key,

c. The solution of the equation referred to in Par. 3 b $P_1 - P_1' = C$ can be effected empirically for two texts enciphered by the same key as follows. If the assumption is correct the exact key used for its encipherment can be obtained by use of the chart. This key can then be applied to the other of the two ~~superimposed~~ messages to produce the plain text corresponding thereto, as demonstrated in the following paragraph.



There are attached as Tables 5, 6, 7, 8 etc., examples of messages appearing on War Department radio circuits using the M-228 for which identical setting of cipher wheels were used. The solution of these messages is fairly simple. It can be greatly speeded up by application of machine methods and detailed worksheets are appended. A description of the method used, while fairly simple, is not within the scope of this paper.

5. The M-228 is misleading in appearance. The fact that it uses the same type of cipher wheels as the SIGABA immediately suggests to the observer that it effects the same type cryptographic treatment as the SIGABA. The SIGABA uses an entirely different cryptographic principle, and consequently its security is much greater than that of the M-228. The fallacy in assuming that the M-228 affords equal or comparative security with the SIGABA is dangerous since it produces a false feeling of security in the minds of those who do not appreciate the cryptographic principles about which the two machines are constructed.

6. Insofar as the security of the M-228 itself is concerned, considering the machine as it is now being used, the writer is aware of no method for reconstructing the wheels in case a large portion of the pure key is available. However, this appears to be a difficult problem, but in view of the fact that the principle is new in the art and that no extensive study of it has been made, there is some doubt in the writer's mind as to the validity of the assumption that the wheels can not be reconstructed under the circumstances of its present usage. For example, in the solution of the messages of Table 5, 6, etc. considerable pure key was recovered, which might be sufficient to permit a complete solution of the system.

7. A primary weakness of the M-228 lies in the fact that transmission can be made in the clear due to failure of contacts of the applique unit, or a simple failure on the part of the operator to throw a switch to cipher. In tape transmission on certain circuits the entire message could be transmitted without the operator's being aware that the message had gone out in the clear. It is therefore necessary to monitor all M-228 transmissions between the time of the encipherment and the time at which the impulses are fed into the transmission medium.

8. In view of the fact that the M-228 was designed for rapid handling of messages to be cryptographed, retransmissions of messages are made without paraphrasing. This happens most frequently with new operators and in general it is due to operational difficulties rather than functional or machine difficulties. No security study has been made to determine the effect of such transmissions on the fundamental security of the system.

9. The M-228 lends itself for use in conference calls. The nature of the language and text appearing in such a call cannot be readily controlled from the standpoint of security, and it is possibly more stereotypic in nature than any other type of communication other than "synoptics". This is because conferences usually consist of questions and answers and if a simultaneous recording is made of both channels, the assumption of plain text by the cryptanalyst is simplified considerably. Such things as OK, CAR RET, LINE FEED, GAPLS, and THAT IS ALL, will appear and can be readily recognized. If the system has any inherent weakness this type of usage will permit of its utmost exploitation.

10. In the foregoing discussion the emphasis was placed on solution of two messages sent in the same key. No fair estimate of the security of a properly phrased, well-composed, and correctly cryptographed message can be given. However, for such communications the security of the M-228 can be estimated as lying somewhere between one tenth and one fourth that afforded by the SIGABA. In view of this statement, if the SIGABA is considered as the ultimate in security and the criterion of secret classification is based on the security afforded by it, it would appear that the M-228 on radio would afford only "confidential" security. When it is considered that the bulk of traffic will tend to move on M-228 channels this estimate makes it appear doubtful as to whether the M-228 should be used for messages of secret classification, when such channels are subject to interception.

D-R-A-F-T

~~TOP SECRET - U.S. EYES ONLY~~

REPLACEMENT OF THE PRESENT COMBINED CIPHER MACHINE

THE PROBLEM

1. To determine the U.S. Position toward the United Kingdom's proposals in RDC 5/99 (attached as Appendix "A") that:

(1) there be a full and complete interchange of cryptographic principles and policy on a reciprocal basis.

(2) if the U.S. Chiefs of Staff cannot agree to (1) above, they authorize the disclosure of the principles of the ECM (SIGABA) so that these may be incorporated in a new British Cipher Machine.

FACTS BEARING ON THE PROBLEM AND DISCUSSION

2. Of the two foregoing proposals, the first is unacceptable. The United States Government adheres to the following generally accepted basic principle of national sovereignty and security: the means and methods which a government employs for the protection of its own communications constitute a private matter not to be shared in toto with any other government. This principle is sound because it is impossible to be certain that a former ally will not be someday over-run by a common enemy or may even become a foe, in which case a well-forged weapon may be turned against its originator. As regards the effects of such a contingency, the primary danger in the cryptologic field is not that the security of communications may be destroyed or impaired but that the sources of communication intelligence may be dried up.

3. With regard to the second or alternative proposal, it is felt that this solution should be accepted by the United States, for the following reasons:

a. In the spring of 1947 there were Combined discussions on this same subject. These resulted in a decision to withhold the ECM and to study possible improvements in the CCM. The results of this study have been largely negative, the only possibility being the BCM, a machine which represents some improvement in security over the CCM but not deemed sufficient in degree to meet with British acceptance. Moreover, the modifications which would be required in the British Typex machine to convert it into a BCM are such that there is grave doubt as to their accomplishment. Also, the British have decided that they must replace the Typex in any case and the introduction of a suitable replacement would be expensive in terms of time required for research, development and service testing. It would be to the advantage of the U.S. as well as to the British if such a delay could be avoided so that British equipment suitable also for Combined Communications would become available at an early date.

b. During the Combined discussions referred to above, the British indicated that they were aware of the principles of the ECM. They described them quite accurately and indicated that they considered their security to be of the highest order. They admitted, in fact, that they had incorporated those cryptographic principles in a radioteletype cipher machine for their own use. Furthermore, even as regards the engineering know-how which went into the construction of the ECM, this knowledge has been disclosed to the British, since they were provided with CSP 1700. This machine was simply an ECM chassis with certain of the ECM cryptographic features eliminated.

c. Disclosure of the ECM to the British and its adoption by them would give the two governments a suitable piece of equipment ensuring the highest degree of security for vital combined U.S. - British communications.

d. Disclosure of the ECM will not leave the U.S. without equipment unique to the U.S. As a matter of fact, a modification of the ECM has already been developed (CSP 2900) and is available in quantity. This modification, which improves the security of the ECM, does so without in any way impairing its use as an ordinary ECM or as a CCM. By means of a simple switching arrangement it is possible to make the CSP 2900 serve as a device purely for U.S. communications, or as an ECM for U.S. - British combined communications, or as a CCM. However, the principles of the CSP 2900 would not be disclosed to the British.

e. Release of the ECM to the British would leave the way open to the adoption of the CCM for North Atlantic Pact communications if such a decision should be found to be necessary in the national interest. British - U.S. use of the ECM would be easily adaptable to North Atlantic Pact communications since the addition of a simple already available adapter to either the ECM or the CSP 2900 would permit communication with any North Atlantic Pact nation holding the CCM. In addition, disclosure of the CCM to the other signatories to the North Atlantic Pact would not impair the security of U.S. - British communications since the CCM system would then be reserved for that specific purpose.

f. At the time of the 1947 Combined discussions on this subject, one of the principal U.S. objections to disclosing the ECM to

the British was the increased danger of compromise arising from the wider distribution of the equipment if the British were permitted to have it. This increased danger is recognized but it is believed that the advantages cited above outweigh this objection.

g. Also at the time of the 1947 Combined discussions there were indications that the British did not provide and enforce physical security protective measures for their crypto-equipment equal to those required and enforced by the U.S. services. Because of this it was agreed on a Combined level that a prerequisite to further discussions regarding a replacement for the CCM would be a Combined agreement covering the measures both governments would apply in the handling and protection of combined cryptomaterial. Such an agreement has been concluded and concurred in by both Governments (CCB-285, 11 Oct 1948). A review of that document in order to insure identity in security regulations applicable to the ECM and an acceptance of such changes therein as may be deemed necessary by the U.S. should be a preliminary to entering upon discussions leading to a full disclosure of the ECM to the British.

CONCLUSIONS

4. It is concluded that:

a. The first proposal made by the United Kingdom in RDC 5/99 of 13 July 1949 should be rejected.

b. The details of construction of the ECM (SIGABA) should be disclosed to the U.K. in discussions which will include a review and acceptance by both Governments of identical security regulations to insure the physical protection and proper use of the equipment.

RECOMMENDATIONS

5. It is recommended that:

a. A memorandum substantially as in Appendix "B" be forwarded to the British Joint Services Mission.

COORDINATION

6. Coordination with AFCIAC has been effected.

JOINT COMMUNICATIONS - ELECTRONICS COMMITTEE

SECURITY AND CRYPTOGRAPHIC PANEL

REPLACEMENT OF THE PRESENT COMBINED CIPHER MACHINE

(Proposed reply to the British Joint Services Mission)

1. The U.S. Joint Chiefs of Staff have carefully considered the proposals made in RDC 5/99 of 13 July 1949 concerning the replacement of the existing Combined Cipher Machine. The U.S. Joint Chiefs of Staff regret that they are unable to accept the proposal for a full and complete interchange of cryptographic principles and policy on a reciprocal basis. However, they are prepared to authorize discussions which can commence in Washington at any time, leading to the disclosure of the principles of the ECM (SIGABA) so that these may be incorporated in a new British Cipher Machine, these discussions to be preceded by a review and acceptance by both Governments of identical security regulations to provide for the physical protection and proper use of the equipment.

APPENDIX "B"

CSGAS-14 20 September 1949

MEMORANDUM FOR: CHIEF, ARMY SECURITY AGENCY

SUBJECT: Replacement of the CCM

REFERENCE: (a) AFCIAC Document 13/4 of 14 Sept 49

1. a. In connection with reference (a), it is deemed advisable to note that the ECM-SIGABA is covered by a number of patents or patent applications.

b. Certain of these patents or patent applications are owned by the Teletype Corporation. The exact number of these cases, their serial numbers, and specific nature are unknown to this Agency, as they are being handled under Navy control.

c. There are certain other patents or patent applications, covering certain subsidiary features which were invented by Navy personnel. Details of ownership are not known to this Agency.

d. The basic cryptographic principles employed in the equipment are covered by the following patent applications, still in a secrecy status under the "Three-Year Rule" (Sec. 4894, R.S., as amended) and also under Public Law No. 700 (War-time secrecy for patent applications):

App. Serial No.	Inventors	Date filed
682,096	Friedman	25 July 1933
70,412	Friedman & Rowlett	23 Mar 1936

In each of these two cases the U. S. Government owns the entire right, title and interest in the invention, throughout the U.S. and territories and dependencies thereof, but not elsewhere; the inventors have an irrevocable, assignable, and exclusive license to make, use and/or sell and to license others to make use and/or sell the invention. Attached hereto is a copy of the assignment in each case. (Incl. 1 and 2).