16

REF ID:A71739

70-283

58220
dir

Cryptanalysis Equipment for Electrical Printing Telegraphy

CONVERTER M228

Serial No.
443,320
Filed May 16, 1942

Reversionary Assignment Made

1 Memo to WP&T 5/9/41 :
Outline of project
Military Characteristics

2 WP&T funds to R&D 5/13/41
Rec mil char be presented to SC Tech Com

3 R&D, WP&T reports on meeting Tech Com 6/30/41
Adopt Mil Char
Sets up program
SCL will be directed to initiate project + funds to be prov.

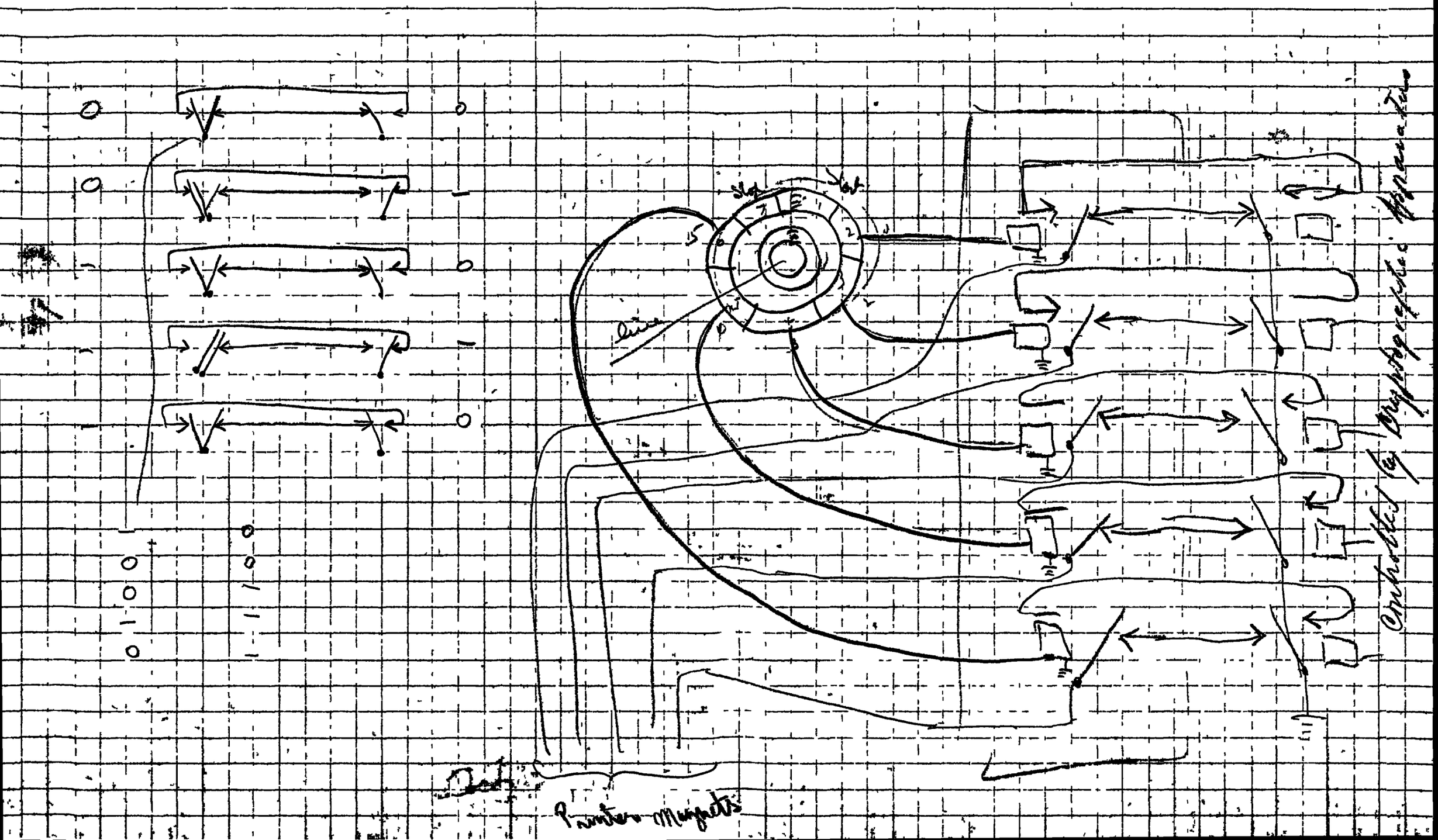
4 WP&T to SIS 7/2/41
Mil Char have been submitted to TAG for approval
Concurs in procedure proposed in action 3

5 SIS to R&D 7/7/41 ⟷ 15 Oct 41 Contract with Fabtyl:
Noting actions 2, 3, 4 — approval for "Rotor and Stepping
Diagram of circuit furnished — mechanism assembly $3680."
Nov 26, 1941

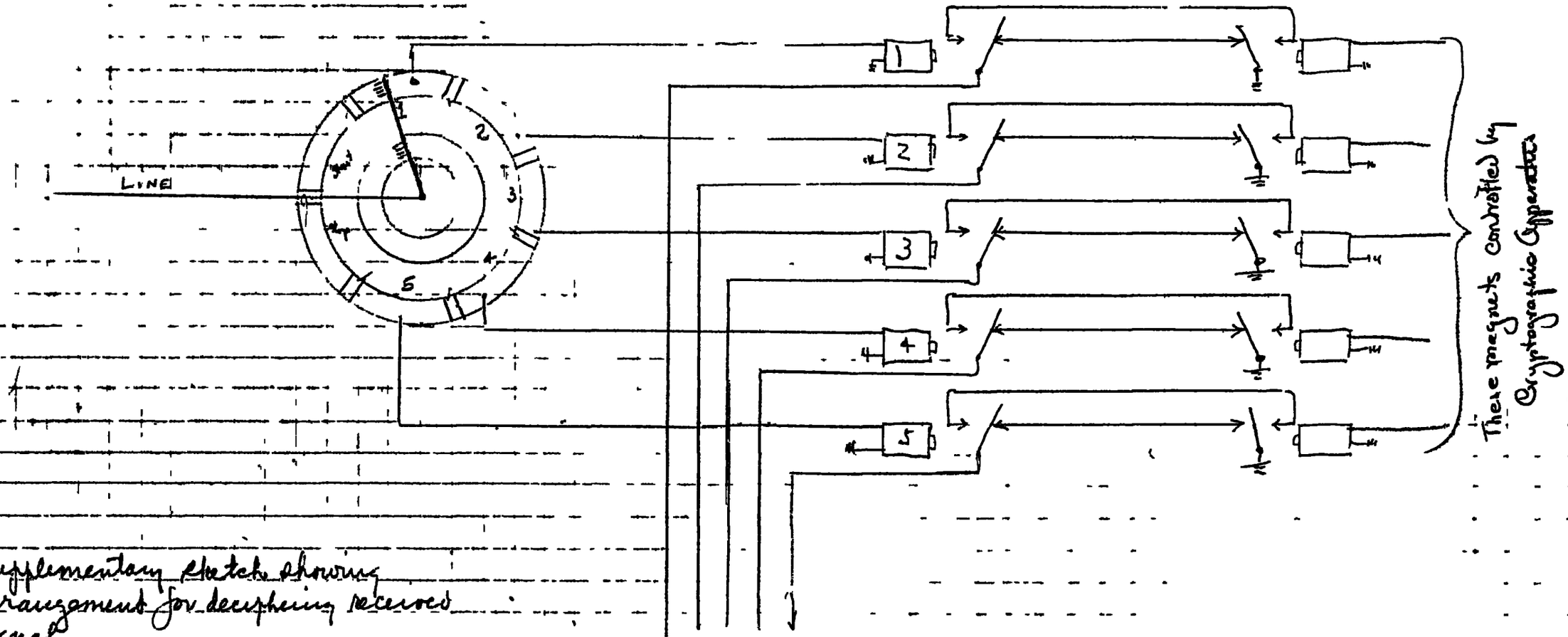
1 SIS to R&D 7/10/41
Furnishing sketch + note on operation

Patent Submission

May 10, 1941 - Memo to R&D req patent action + submission, pt disclosure 5/9/41
Sept 25, 1941 - R&D reports meeting SC Pat Bd
May 22, 1942 - Pat app filed
May 16, 1942, Ser. No. 443,320


Slip
Slip
Disc
Printer magnets
Controlled by Magnetophone Tape

~~SECRET~~



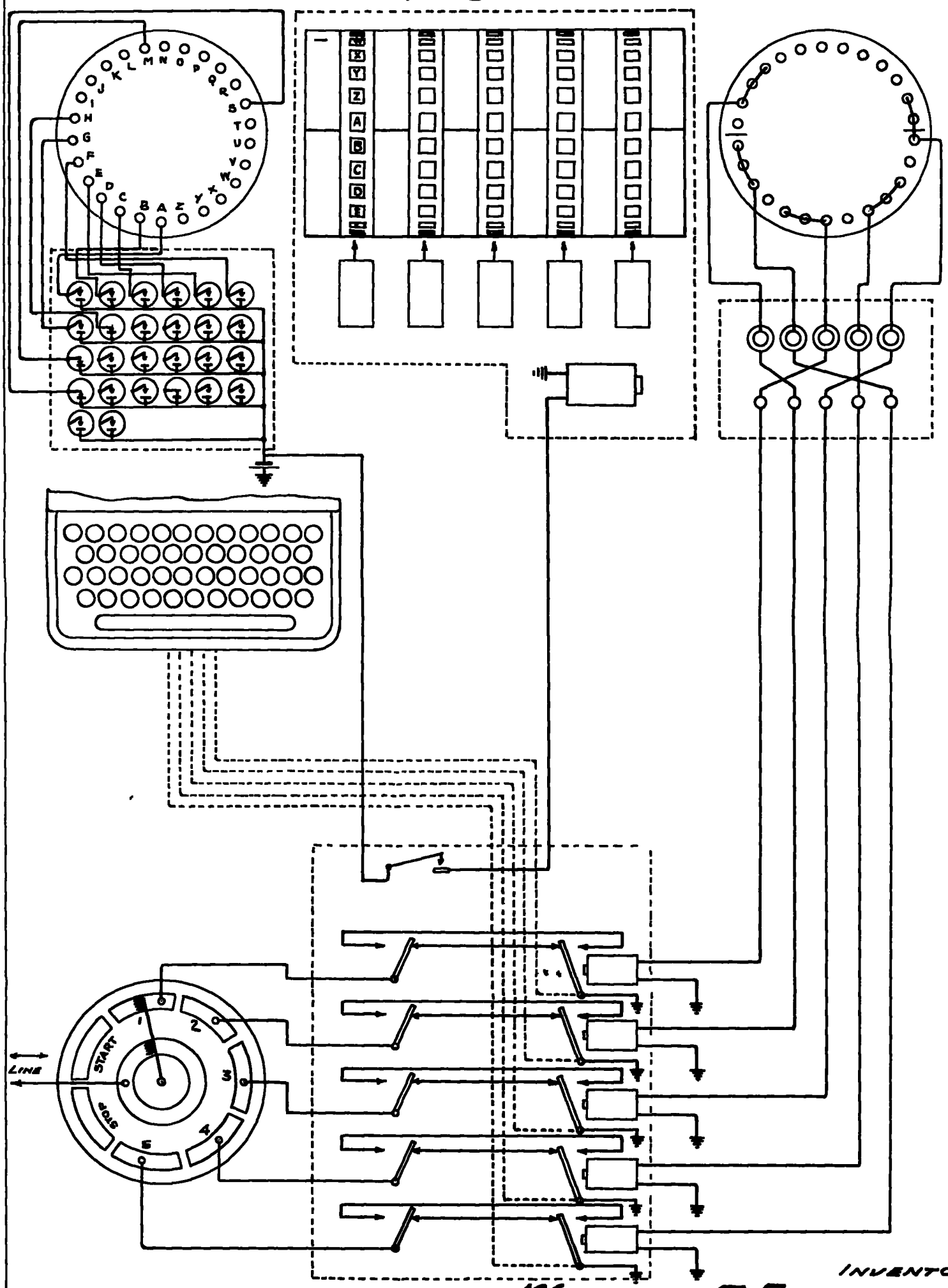
Supplementary sketch showing arrangement for deciphering received signal

Converter M-228

William F. Friedman, Dec. 1, 1941
Frank B. Rowlett Dec 1, 1941

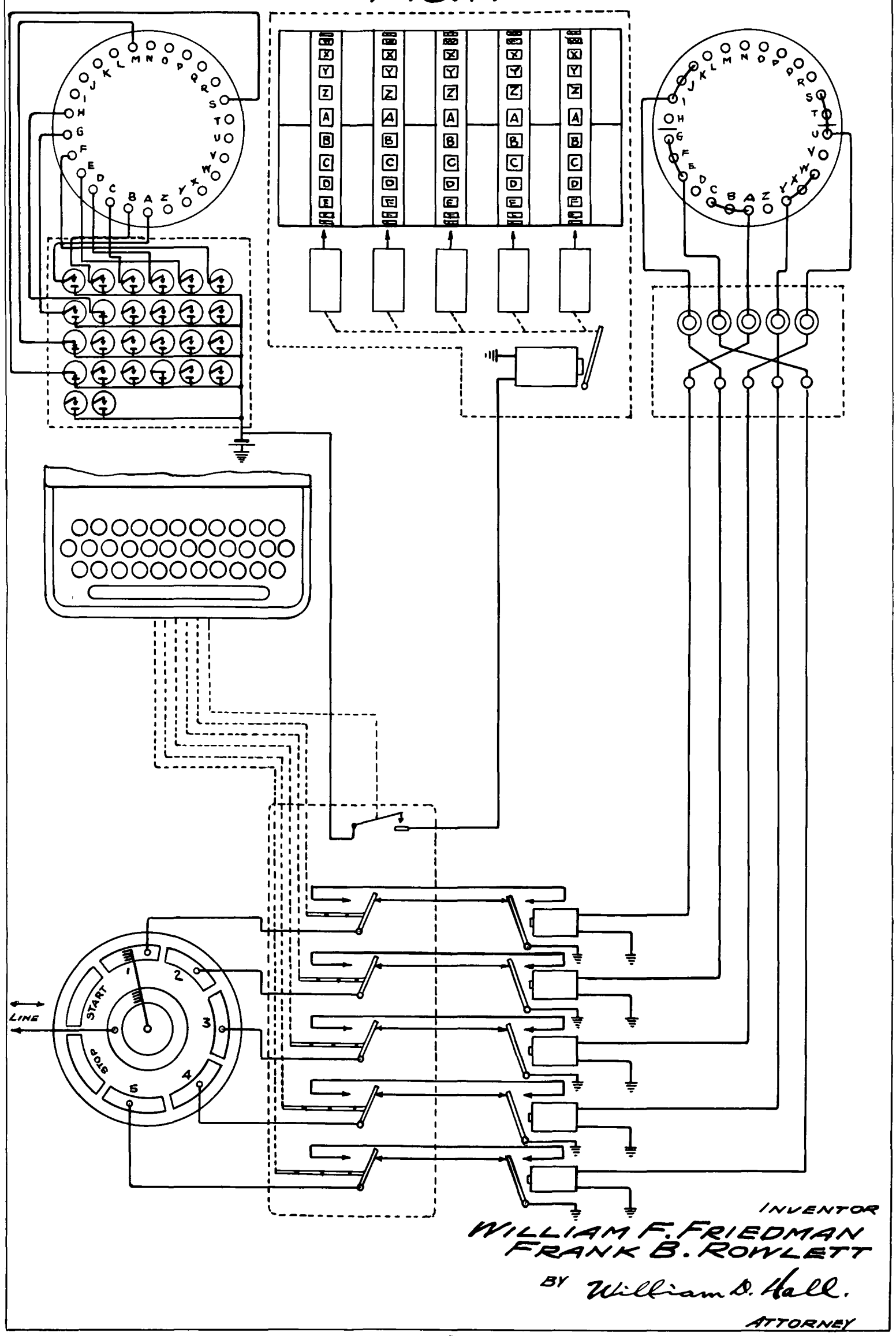
~~SECRET~~

FIG. 1.



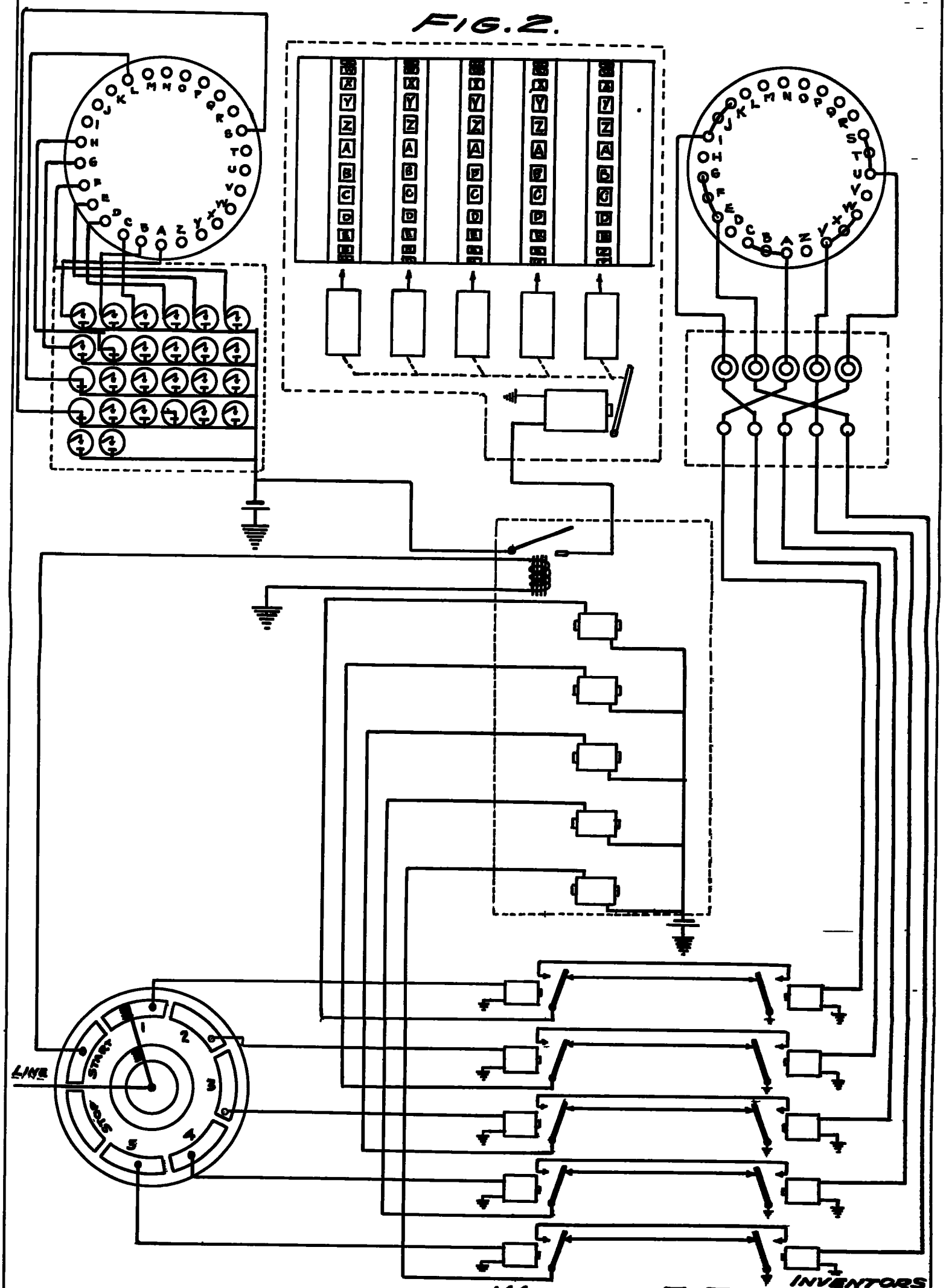
INVENTOR
WILLIAM F. FRIEDMAN
FRANK B. ROWLETT
BY William D. Hall.
ATTORNEY

FIG. 1.



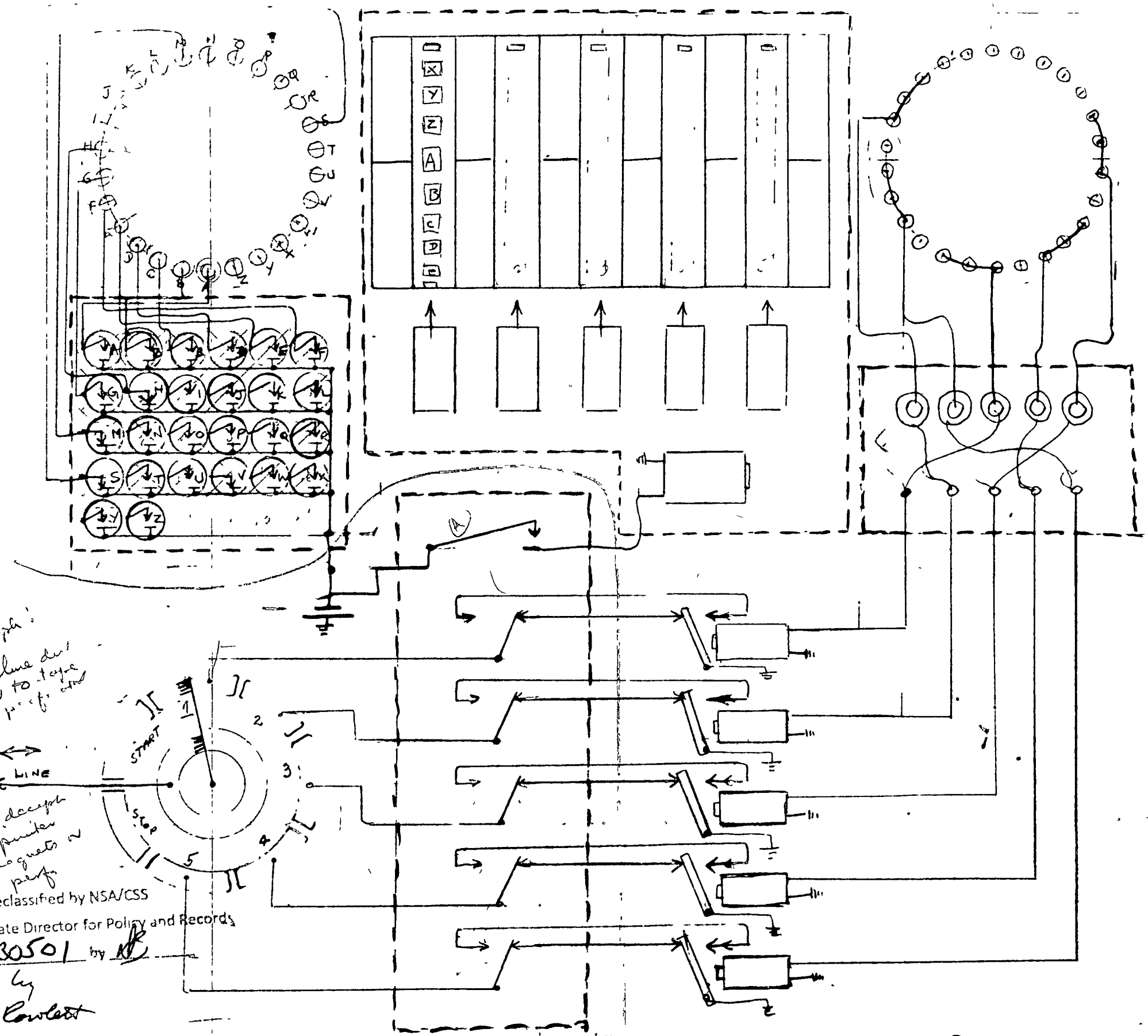
INVENTOR
WILLIAM F. FRIEDMAN
FRANK B. ROWLETT
BY William D. Hall.
ATTORNEY

FIG. 2.



INVENTORS
WILLIAM F. FRIEDMAN
FRANK B. ROWLETT
BY William D. Hall
ATTORNEY

Fig 1.



Prepared by
Frank B Cowlett
Oct 21, 1941

COPY

REF ID:A71739 May 9, 1941.

~~SECRET~~

Extras

MILITARY CHARACTERISTICS OF CONVERTER

FOR USE ON ELECTRICAL PRINTER CIRCUITS.

1. The converter should be designed for the purpose of automatic encipherment and decipherment of messages transmitted by teletype or similar printing telegraph apparatus based upon a multiple-impulse-code such as the Baudot.

2. It should be designed so as to encipher the signals established either by tape or keyboard operation, causing enciphered text to be transmitted instead of the plain text represented on the tape or set up on the keyboard. At the receiving end the apparatus should decipher the received cipher signals, converting the cipher text into plain text before the signals are fed into the printer, or into the perforator in the case of tape operation. In other words, encipherment, transmission, reception, and decipherment are to be accomplished in a single step rather than in two separate steps at each end.

3. The converter should use as its cryptographic principle a non-repeating keying sequence of multiple-impulse characters, the latter to interact with the plain-text signals according to the rule that "like signs produce spacing current, unlike signs produce marking current." (The latter principle is well known in the art.)

4. The keying sequence mentioned in Par. 3 should be produced by a plurality of electrical cryptographic rotors in cascade, through which impulses are sent and recombined in a manner so as to produce the equivalent of a random sequence of characters according to the multiple-impulse-code used by the transmitter. (If teletype, the characters will be 32 in number and should be in random order.) The number of rotors in cascade should be at least three and preferably five.

5. The rotors mentioned in Par. 4 may be identical with those now used in Converter M-134-C. Mechanism should be provided to cause meter-like stepping of these rotors, at least one being displaced angularly for each character to be enciphered and transmitted. The order of stepping of the entire set of rotors, however, should be capable of being varied so that the complete set of factorial n motions may be available for use, n being the number of rotors in cascade.

6. The converter should be motor-operated from the same power source as that employed for the telegraph printer. It should, however, be designed to function as a separate unit and not as an integral part of the printer itself, so that either normal plain-text operation or cryptographic operation of the printer circuit can be effected at will. The converter should be capable of being electrically connected or

~~SECRET~~

associated with the tape (or keyboard transmitter) and with the printer by means of a suitable plug and jack or multiple plug arrangement, so that it may be readily connected or disconnected from operation.

7. The converter should be of approximately the following dimensions 12"x8"x8", and its weight should not exceed 50 lbs.

Enclosure #1

IN THE UNITED STATES PATENT OFFICE

RE: Application for Patent of
WILLIAM F. FRIEDMAN and
FRANK B. ROWLETT

Serial Number
443,320

Filed
16 May 1942

For
- CRYPTOGRAPHIC SYSTEM

Division 70

AMENDMENT

Filed - 21 July 1953

* * * * * * * * * *

The Honorable Commissioner of Patents
Washington 25, D. C.

Sir:

This is in response to Patent Office action of 21 July 1950 in the above-identified application for patent which is being prosecuted under the so-called three-year rule. Please amend the case as follows:

IN THE SPECIFICATION

Page 4, following the amendment of 24 October 1949 in line 19 - Insert the following - The stationary end plates 15 and 21, it should be understood, are analagous to the end plates 20 and 21 of Hebern and the end "cylinders" 4 and 5 of Korn. The actuators 22-26 (of this application) are similarly analagous to the "fingers" 72a-72e of Hebern and the "pawls" 42 of Korn. Actuators 22-26 are, in fact, electromagnetically-operated pawls although functionally they may be considered to be gears, cams, pistons, or any of various other devices, connected to their respective wheels by appropriate linkages (as indicated by the dotted lines in the drawings).- ,

IN THE CLAIMS

Please cancel Claims 11 and 12.

-REMARKS

The specification has been amended to point out the manner in which the several parts of the Applicants' structure cooperate with each other. Since the parts of the present case are now related to specific elements shown and described in the patents to Hebern and Korn, it is believed that the structure and operation of the present case should be clearly understood.

Reconsideration is requested, in view of the present amendment, of the requirement for additional illustration. No further illustration seems to be necessary, and, if the requirement is to be repeated, Applicants would appreciate more specific directions therefor.

With the cancellation of Claims 11 and 12, the claims remaining in the case are 2, 3, 4, 5, 6, and 9, all of which have been rejected only on the grounds of insufficient disclosure. With the present amendment, the disclosure appears to be complete, and allowance of the claims is, therefore, requested.

Respectfully,

WILLIAM F. FRIEDMAN and
FRANK B. ROWLETT, Applicants

By Henry B Stauffer
Their Attorney

IN THE UNITED STATES PATENT OFFICE

RE: Application for Patent of
WILLIAM F. FRIEDMAN and
FRANK B. ROWLETT

Serial Number
443,320

Filed
16 May 1942

For
CRYPTOGRAPHIC SYSTEMS

Division 16

AMENDMENT

Filed 24 Oct 1949

* * * * * * * * * *

The Honorable Commissioner of Patents
Washington 25, D. C.

Sir:

This is in response to Patent Office action of 24 October 1946 in the above-identified application for patent which is being prosecuted under the so-called three-year rule. Please amend the case as follows:

IN THE SPECIFICATION

Page 2, line 25 - Change "tro" to - two - .

Page 3, line 15 - Cancel "and" and insert - are - .

Page 4, line 12 - Change "18" to-18" - .

12 - Change "and" to - end - .

19 - Before "The" insert - The manner in which the end plate feeds the cryptographic mase and representative means for providing substantially unpredictable movements for the commutators thereof

may both be found in prior art, see, for example, Hebern, 1,683,072, and Korn, 1,733,886. - .

IN THE CLAIMS

Claim 1 - Cancel.

Claim 3, line 7 - Cancel "a plurality of output wires at least one of which is connected".

8 - Cancel "to a plurality of output terminals" and insert - means for electrically connecting together said output segments in groups thus effectively diminishing the number of output contacts, and an output wire connected to each of said groups - .

Claim 4, line 6 - Before "groups" insert - electrically connected - .

Claim 5, line 9 - Before "opening" insert - substantially unpredictably - .

Claim 6, line 8 - Before "commutation" insert - substantially unpredictable - .

Claim 7 - Cancel.

Claim 9, line 10- After "segments" insert - any one of which output segments may according to a substantially unpredictable rule effectuate and stop the aforementioned current flow - .

REMARKS

The specification has been amended in minor particulars (to correct typographical errors, etc.). On page 4, line 12, "18" has been changed to 18" because of a duplication of reference characters. The Chief

Draftsman will be requested to make the necessary change on the drawing.

The specification, on page 4, has been clarified by reference to the patents of Hebern, 1,683,072, and Korn, 1,733,886. The function of elements 22 through 26 was explained to some extent in the original specification on page 6, lines 21 and 22.

It is assumed that, in view of the above-mentioned amendments to the specification, the rejection of the claims on the ground of inadequate disclosure will not be pressed.

Claim 1 has been cancelled.

Claim 2 was not rejected on references and, therefore, is believed to be allowable.

Claims 3 and 4 have been amended to require with more or less specificity that the output contacts of the keying generator are strapped together in groups, it following, of course, that there are fewer output contacts than input contacts. This thought is missing from the references and goes much beyond a "pure matter of choice" as was claimed in the official letter of 23 November 1942, as the device produces a keying sequence difficult of solution far out of proportion to the apparent magnitude of the change.

Claim 5 has been amended to define a structure wherein certain of the switches are open and closed in substantially unpredictable order. In Lipp, et al., 1,912,983, the order can easily be calculated from the cams, whereas in Applicants' arrangement the closing of a comparable

switch is dependent not only upon a complex electrical maze but also upon the pressing of one of keys 10, 11, 12, etc., with even the operator having no idea when a key is pressed which switch or switches will be affected. The same remarks apply to Claim 6, rejected as fully met by Jipp, et al.

Claim 7 has been cancelled.

Claim 9 has been amended to include the concept of actuating a particular switch by any one of the output signals according to an unpredictable rule and, thus, differentiates from Jipp, et al., and Hebern.

It appears that the rejection of Claims 10 and 11 was meant to apply to Claims 11 and 12 since Claim 10 already has been cancelled. Viewed in this light, it is requested that the rejection be reconsidered as Jipp, et al., Pierce, 1,426,669, and Parker, 1,442,819, fail completely to show that any keying sequence, once initiated, is enciphered before use. Reconsideration is requested also of the rejection of Claim 10 (probably Claim 11) for indefiniteness; it cannot fairly be said that "providing a keying sequence" may be purely mental if the result thereof is capable of physical treatment as called for by the claim.

Continued prosecution under the so-called three-year rule is desired.

Reconsideration and favorable action are desired.

Respectfully,

WILLIAM F. FRIEDMAN and FRANK B. ROWLETT,
Applicants

By _____
Their Attorney

3 March 1949

Memo for Deputy Chief, Army Security Agency

SUBJECT: Return of papers in re Patent Application Serial No. 443,320.

1. The accompanying file of documents, all in connection with Patent Application Serial No. 443,320, was under study when I went on sick leave last August and it remained in my basket until recently, awaiting attention.

2. In accordance with direction on top routing sheet, I am returning file herewith, having noted its contents carefully.

3. This file was initiated by a formal letter dated 8 Dec 47 from the undersigned to the Director of Intelligence, THRU Chief, Army Security Agency.

4. It is requested that the case be completed by a formal reply addressed to me in response to the letter referred to in Par. 3 above.

William F. Friedman

WAR DEPARTMENT
OFFICE OF THE JUDGE ADVOCATE GENERAL
WASHINGTON 25 D C

Mr. William F. Friedman
1823 Que Street, N. W.
Washington 9, D. C.

15 JUL 1947

Mr. Frank B. Rowlett
216 So. Pershing Drive
Arlington, Virginia

Gentlemen:

By direction of The Judge Advocate General, receipt is acknowledged of your letter to the Secretary of War dated 6 June 1947, tendering to the Government of the United States for its use, under the provisions of the act of October 6, 1917, as amended (35 U.S.C. 42), the invention described and claimed in your application for patent, Serial No. 443,320, filed 16 May 1942, for Crytographic Systems, which application and the invention covered thereby were placed in secrecy by the Commissioner of Patents on 16 May 1947. It is noted that your letter includes a power to inspect and make copies of the application.

The records of this office show that the above-mentioned application and the invention covered thereby are assigned to the United States Government and were filed under the act of March 3, 1883, as amended (35 U.S.C. 45). However, the present tender will be made of record for the protection of whatever interest you may have in this invention.

Very truly yours,

George W. Gardes.

GEORGE W. GARDES
Colonel, JAGD
Chief, Patents Division

6 June 1947

Secretary of War
Washington
D. C.

Attention: The Judge Advocate General

A Secrecy Order under Public #700, 76th Congress, having recently been served upon, and acknowledged by, the undersigned in connection with Patent Application Serial Number 443,320, filed 16 May 1942, the invention covered by the said application is, in accordance with the recommendation contained in the Secrecy Order, tendered to the Government of the United States for its use. The application may be inspected and copies made, if desired.

Respectfully yours,

WILLIAM F. FRIEDMAN
1823 Que Street, N.W.
Washington 9, D. C.

FRANK B. ROWLETT
216 So. Pershing Dr.
Arlington, Virginia

(detach here)

Form D-23 Nov '44 REF ID:A71739

107-244

Secrecy order dated 19 March 1947
" 20, 1947
2 June 1947

marked
Signed by me

Modification of M-134 A wherein can wheels replace tape

To the applicant above named or his heirs, and any and all his assignees and attorneys or agents

Enclosed is your copy of a Secrecy Order under Public No 700, 76th Congress You are required to fill out and personally sign the receipt form above and return it to the Commissioner of Patents If the acknowledgement is not received within a reasonable time it will be necessary to take other steps to establish service of this order on you

Complete assignment made 11 April 1938 but a license reserved to me,

E G Haggett Jr
Patent Office War Division

Please advise this Office of change of address

Form D-2-nn

REF ID:A71739

MAILED

MAY 16 1947

DEPARTMENT OF COMMERCE

UNITED STATES PATENT OFFICE

WASHINGTON

Serial No 443,320 Filed May 16, 1942 Division 16

For Cryptographic Systems

Applicant William F. Friedman and Frank B. Rowlett

Assignee U.S.Government

SECRECY ORDER

NOTICE - To the applicant above named his heirs and any and all his assignees, attorneys and agents, hereinafter designated principals

You are hereby notified that your application as above identified has been found to contain subject matter, the unauthorized disclosure of which might be detrimental to the public safety or defense, and you are ordered in nowise to publish or disclose the invention or any material information with respect thereto, including hitherto unpublished details of the subject matter of said application, in any way to any person not cognizant of the invention prior to the date of the order, including any employee of the principals, but to keep the same secret except by written permission first obtained of the Commissioner of Patents, under the penalties of the act of October 6, 1917 (Public No 80), as amended July 1, 1940 (Public No 700) as amended August 21, 1941 (Public Law 239), and June 16, 1942 (Public Law 609) 35 U S C 42, 40 Stat 394, 54 Stat 710, 55 Stat 657, 540 O G 233 248

Any other application which contains any significant part of the subject matter of the above identified application falls within the scope of this order If such other application does not stand under a secrecy order it and the common subject matter should be brought to the attention of the Patent Office War Division

If prior to the issuance of the secrecy order any significant part of the subject matter has been revealed to any person, the principals shall promptly inform such person of the secrecy order and the penalties for improper disclosure set out in Public No 700, 76th Congress, and Public Law 239, 77th Congress

This order should not be construed in any way to mean that the Government has adopted or contemplates adoption of the alleged invention disclosed in this application, nor is it any indication of the value of such invention In order to make the details of your invention available for inspection by various governmental agencies concerned therewith for consideration of its possible use in the war program and at the same time to preserve your rights under the Act, it is suggested that you promptly tender this invention to the Government of the United States for its use Such tender may be effected by a communication addressed to the Secretary of War or the Secretary of the Navy and should be accompanied by a power to inspect and make copies of the application

This order is modified by the provisions of accompanying permit A (form D-3n)

Thomas E. Murphy
Conder C. Fahey

MAY 16 1947

Assistant

~~Acting~~ Commissioner

Form D-3-m

REF ID:A71739

DEPARTMENT OF COMMERCE

UNITED STATES PATENT OFFICE

WASHINGTON

MAILED

MAY 16 1947

Serial No 443,320 Filed May 16,1942 Division 16

For Cryptographic Systems

Applicant William F. Friedman and Frank B. Rowlett

Assignee U.S.Government

PERMIT A

An order of secrecy having been issued in the above-entitled application by the Commissioner of Patents, the principals as designated in said order are authorized to disclose the subject matter to any person of the classes hereinafter specified if such person is known to the principal disclosing to be concerned directly in an official capacity with the subject matter, provided that all reasonable safeguards are taken to otherwise protect the invention from unauthorized disclosure The specified classes are -

(a) Any officer or employee of any department, independent agency, or bureau of the Government of the United States

(b) Any person designated specifically by the head of any department, independent agency or bureau of the Government of the United States, or by his duly authorized subordinate, as a proper individual to receive the disclosure of the above indicated application for use in the prosecution of the war

The principals under the secrecy order are further authorized to disclose the subject matter of this application to the minimum necessary number of persons of known loyalty and discretion, employed by or working with the principals or their licensees and whose duties involve cooperation in the development, manufacture or use of the subject matter by or for the Government of the United States, provided such persons are advised of the issuance of the secrecy order

When requested in writing by a responsible official of the United States Government known to the party making disclosure to be directly concerned in an official capacity with the subject matter, authorization is further given to disclose the subject matter to accredited representatives of an allied government For the sake of the record and for their protection, the principals should promptly inform the Commissioner of Patents of such disclosures together with the names and official designations of the persons to whom disclosure is made

The provisions of this permit do not in any way lessen responsibility for the security of the subject matter as imposed by any Government contract or the provisions of the existing laws relating to espionage and national security

Thomas F. Murphy,

Assistant Commissioner

Copy sent to:

William F. Friedman
3932 Military Road, N.W.
Washington, D.C.

Frank B. Rowlett
2306 N. Madison St.
Arlington, Virginia

William D. Hall
c/o Chief Signal Officer
Munitions Bldg.
City

HEADQUARTERS ARMY SERVICE FORCES

MEMO ROUTING SLIP

TO THE FOLLOWING IN ORDER INDICATED

	NAME OR TITLE	ORGANIZATION	BUILDING AND ROOM	INITIALS
1	Mr. Friedman			DATE
2				
3				

This is your 228 file brought up to date. You will note that the amendment filed in November is one to which you objected. The Legal Division recommended that it be filed, and that a supplemental amendment be prepared when convenient.

FROM	NAME	ORGANIZATION	BUILDING AND ROOM	DATE
				TELEPHONE

W D, A G O Form 0115
1 October 1944

This Form supersedes W D A G O Form 0115 23 March 1944, which may be used until existing stocks are exhausted

16—41046-2 GPO

HEADQUARTERS, ARMY SERVICE FORCES

REF ID:A71739

MEMO ROUTING SLIP

TO THE FOLLOWING IN ORDER INDICATED:

	NAME OR TITLE	ORGANIZATION	BUILDING AND ROOM	INITIALS / DATE
1				
2				
3				

making any further changes thought desirable, and explaining that the remarks of the earlier amendment were in error on theory. Mr. Hall said that the case would not be prejudiced in any way.

Some time soon we should get together with Col. Rowlett and draft a complete and satisfactory supplemental amendment

FROM: NAME	ORGANIZATION	BUILDING AND ROOM	DATE
Stauffer	WDGSS-7		16 Jan

TELEPHONE 227

WAR EXPANDED 71739

MEMO ROUTING SLIP

1 NAME OR TITLE	INITIALS		CIRCULATE
ORGANIZATION AND LOCATION	DATE		CONCUR-RENCE
2			FILE
			INFORMATION
3			NECESSARY ACTION
			NOTE AND RETURN
4			SEE ME
			SIGNATURE

REMARKS

Mr. Friedman —
Here is the assignment you asked for — seems to be the usual reversioning type.

FROM NAME OR TITLE Stauffer	DATE 30 Jul
ORGANIZATION AND LOCATION	TELEPHONE

WD AGO FORM 1 JUN 1946 895

16—48487-1 U. S. GOVERNMENT PRINTING OFFICE

TOP SECRET SECRET CONFIDENTIAL RESTRICTED

TECHNICAL DIVISION
AFSA-14

DATE _____

TO		FROM
___	Mr. Friedman	___
___	Mr. Rhoads	___
___	Dr. Sanford	___
___	Mr. Douglas	___
___	LCDR Pendergrass	___
___	Dr. Pettengill	___
___	Mr. Callimahos	___
___	Capt Lane	___
___	_____	___
___	_____	___
___	_____	___

( ) As discussed
( ) As requested
( ) Concurrence or comments
( ) Information & forwarding
( ) Information & return
( ) Information & file
( ) Info upon which to base reply
( ) Recommendation
( ) Signature if approved
( ) Your action by

29 Nov 49

Ser. No. 443,320
Filed May 16, 1942

REF ID:A71739

10871

ASSIGNMENT

LIBER US1 PAGE 582

WHEREAS, we, William F. Friedman and Frank B. Rowlett, of 3932 Military Road, N. W., Washington, D. C., and 2308 N. Madison Street, Arlington, Virginia, respectively, have invented certain improvements in Cryptographic Systems, Sig. Corps Case SC-B-W18FR, for which the undersigned on even date herewith executed an application for Letters Patent of the United States; and

WHEREAS, the invention was made while the undersigned was in the employ of the War Department, and pertains to a device useful in the National Defense, and

WHEREAS, The Government of the United States is desirous of acquiring the entire right, title, and interest in and to the said invention and in and to any patents that may issue thereon.

NOW, THEREFORE, in consideration of the premises and one dollar ($1.00), the receipt of which is hereby acknowledged, the undersigned have sold, assigned, and transferred, and by these presents do hereby sell, assign and transfer unto the Government of the United States of America, as represented by the Secretary of War, the entire right, title and interest, throughout the United States of America, and the territories and dependencies thereof, and not elsewhere, in and to the said invention and to the invention as described in the specification executed by the undersigned on even date herewith, preparatory to obtaining Letters Patent in the United States therefor, and to all Letters Patent issuing thereon and any continuations, divisions, renewals, and reissues or extensions of such Letters Patent, the said entire right, title and interest as well as the control of the prosecution of the application and all continuations, reissues and divisions thereof to be held by the Government of the United States of America (as represented by the Secretary of War) and all Letters Patent including any divisions, reissues, renewals or extensions thereof as there are or that may be granted, to be held by the Government as fully and entirely as the same would have been held by me had this assignment and sale not been made. The undersigned hereby gives the Government of the United States of America the non-exclusive right to make, use or sell the invention for governmental purposes in all foreign countries.

RECORDED U.S. PATENT OFFICE DEC 18 1943 Commissioner of Patents

LIBER US1 PAGE 582

Provided, however, that upon any subsequent notice of allowance of said application or of any renewals, substitutions, divisions, continuations or continuations-in-part being given by the Commissioner of Patents, the entire right, title, and interest in and to said invention and said application or any renewals, substitutions, divisions, continuations, or continuations-in-part, and such patents as may be issued thereon, will thereupon revert to William F. Friedman and Frank B. Rowlett subject to an irrevocable, non-exclusive, and royalty-free right and license remaining vested in the United States of America as represented by the Secretary of War, to make, have made, to use, and to sell the subject matter of said invention for governmental purposes only, to the full end of the term or terms for which any Letters Patent, divisions, reissues, renewals, extensions, continuations or continuations-in-part are or may be granted.

William F. Friedman

Witness

Frank B. Rowlett

Before me, a notary public in and for the District of Columbia appeared the above-named William F. Friedman and Frank B. Rowlett, personally known to me, who in my presence executed the foregoing assignment and acknowledged that ~~his~~ their execution thereof was ~~his~~ free act and deed.

Signed ~~in~~ Washington D.C. this 13th day of May, 1942

Mary B. Conner
Notary Public D.C.

(Seal)

3

IN THE UNITED STATES PATENT OFFICE

IN RE: Application of WILLIAM F. FRIEDMAN and FRANK B. ROWLETT	*	
Serial Number 443,220	*	
Filed 16 May 1942	*	Division 53
For CRYPTOGRAPHIC SYSTEMS	*	

* * * * * * * * * *

POWER OF ATTORNEY

TO: The Honorable Commissioner of Patents
Washington 25, D C.

Sir:

The undersigned having, on or about the 16th day of May 1942, made application for letters patent for an improvement in Cryptographic Systems (serial number 443,220), and having this day revoked a power of attorney given on or about the 13th day of May 1942 to William D Hall of the Office of the Chief Signal Officer, hereby appoint Henry B. Stauffer, of Arlington County, Virginia, Registration No 14786, their attorney, with full power of substitution and revocation, to prosecute said application, to make alterations and amendments therein, to receive the patent, and to transact all business in the Patent Office, connected therewith

Signed in the County of Arlington and State of Virginia this 21st day of April, A D 1947

Respectfully,

William F. Friedman, Applicant

Frank B Rowlett, Applicant

IN THE UNITED STATES PATENT OFFICE

IN RE: Application of WILLIAM F. FRIEDMAN and FRANK B. ROWLETT	*	
Serial Number 443,220	*	
Filed 16 May 1942	*	Division 53
For CRYPTOGRAPHIC SYSTEMS	*	

* * * * * * * * * *

REVOCATION OF POWER OF ATTORNEY

TO: The Honorable Commissioner of Patents
Washington 25, D. C.

Sir:

The undersigned having, on or about the 13th day of May 1942, appointed William D. Hall, of the Office of the Chief Signal Officer, their attorney to prosecute an application for letters patent which application was filed on or about the 16th day of May 1942, for an improvement in Cryptographic Systems (serial number 443,220), hereby revoke the power of attorney then given.

Signed in the County of Arlington and State of Virginia, this 21st day of April, A. D. 1947.

Respectfully,

William F. Friedman, Applicant

Frank B. Rowlett, Applicant

W. Friedman

COPY

SPSLG-3a 11 October 1945

Subject Patent application of William F Friedman, Serial Number 443,320 on CRYPTOGRAPHIC SYSTEMS

TO: Chief, Army Security Agency
Pentagon Building
Washington 25, D C
Attention Lt Stauffer

Your recommendation is requested as to whether subject patent application should be withheld from publication and whether your office desires to prepare an amendment An amendment on subject patent application is due in the patent office on November 23, 1945.

FOR THE CHIEF SIGNAL OFFICER

/s/ DONALD K LIPPINCOTT
DONALD K LIPPINCOTT
Colonel, Signal Corps
Patents & Inventions Counsel
Legal Division

WDGSS-85 (11 October 1945) 1st Ind

Army Security Agency, Washington 25, D C , 23 October 1945

TO Office of the Chief Signal Officer, Director, Legal Division, 4D 331, The Pentagon, Washington 25, D C
ATTENTION Colonel D K Lippincott

1 The subject application is undergoing study with a view to determining whether the application shall be prosecuted further under the three-year rule

2 An amendment responsive to the Patent Office action of 23 November 1942 will be prepared by this Agency

FOR THE CHIEF, ARMY SECURITY AGENCY

/s/ MATTHEW G JONES
MATTHEW G JONES
Colonel, Signal Corps

COPY

COPY

January 19, 1943

Ex parte William F. Friedman :
and Frank B. Rowlett :
Serial No. 443,320 :
Filed May 16, 1942 :
Cryptographic System :

In compliance with the request in the letter of the Secretary of War, dated December 1, 1942, this application is placed under the provisions of U. S. Code, Title 35, Section 37.

The assignment accompanying said letter, conveying to the Government of the United States of America the entire right, title and interest in and to the above noted application, has been recorded in accordance with the Commissioner's Order No. 3250, of September 5, 1933, for recording assignments of applications that are to be preserved in secrecy, and the assignment is returned herewith.

This application will not become abandoned prior to the expiration of three years from the date of the last Office action.

CONWAY P. COE

Commissioner

Mr. William D. Hall
c/o Chief Signal Officer
Munitions Building, Washington, D. C.

COPY

IN THE

UNITED STATES PATENT OFFICE

IN RE: Application of WILLIAM F. FRIEDMAN and FRANK B. ROWLETT		
Serial Number 443,320		Division 16
		Room 305
Filed 16 May 1942		
For CRYPTOGRAPHIC SYSTEM		

* * * * * * * * * * * * * * * * * * * *

AMENDMENT

TO: The Honorable Commissioner of Patents
Washington, D. C.

Sir:

This is in response to Patent Office action, 23 November 1942, in the above identified case.

Please amend the application as indicated below.

IN THE SPECIFICATION:

Page 2, Line 19 - Change "like" to - as - .

IN THE CLAIMS:

Claim 1, Line 2 - Before "keying", insert - variable - .

Claim 2, Line 6 - After "law" and before the comma, insert - said last mentioned means including a source of electrical impulses and means for enciphering the same - .

Claim 5, Line 10- After "switches", insert - by electrical impulses - .

Claim 5, Line 10 - After "sequence", insert a comma and add - said last mentioned means including means for enciphering said impulses before applying the same to said additional switches - .

Claims 8 and 10 - Cancel.

Add the following claims:

11. The method of enciphering text composed of characters which includes providing a keying sequence and enciphering the components of said sequence before enciphering said text.

12. The method of secret intercommunication with printed text or the like through switch controlled means which includes actuating one switch in accordance with a plain text character and actuating a complementary switch in accordance with an enciphered keying element.

REMARKS:

The amendment to the specification is in accordance with the Examiner's suggestion on page 2 of the official action.

With respect to the references cited, the rejection is believed to be unsound notwithstanding certain changes in the claims are herein proposed.

Referring especially to Jipp, et al., 1,912,983, principally relied upon, the fundamental feature of the Applicants' invention is not to be found, that being the encipherment of a keying sequence before application of the key to the clear text. The concept and its adaptation to a

and are of the utmost importance, the encipherment of the key adding enormously to the difficulties of successfully attacking the resulting cipher text. In Jipp, et al., as well as in the other cited references, the most that can be claimed for the Patentees is that they attempted in one fashion or other to provide a key, the cycle of which was as long as possible.

Further regarding Jipp, et al., it seems unfair to use elements 1t through 5t so as to anticipate Applicants' commutator 15-21 and associated parts, particularly if the parts 1t through 5t are also to be utilized to meet the "control elements" or switches called for by some of the claims and, moreover, when Applicants' structure is commonly known in the art as a cryptographic commutator, whereas neither Jipp, et al., nor those familiar with the art would ordinarily thus refer to the switches 1t through 5t.

Claim 1 has been amended only to bring out that the output of the key generator is variable (by means of keyboard 10, 11, 12, etc.). The claim is believed patentable over Jipp, et al., for the reasons above indicated. In addition, the rejection of the claim as "obviously fully met" by Jipp, et al., is not justified since in any event the patent fails to show "a distributor having a plurality of segments." Applicants state, page 6, that this distributor 60-66 is not a mere mechanical expedient.

Claim 2, as amended, clearly shows that the elements of Applicants' keying sequence are electrical impulses, and that said impulses are enciphered before utilization, a feature altogether absent from the principal reference as already pointed out.

Reconsideration is requested of the rejection of Claims 3 and 4 on the ground of indefiniteness. The terms used in the claims are all properly identified on page 4 of the Specification; for example, "input segments" are defined in line 4, "circuit closers", line 2, and "output terminals", line 20; and the claims appear to be complete.

The dominant feature of both claims is the connecting together in groups of the output terminals of the commutating system. This means that a solution of the keying sequence generator is virtually impossible even though the output thereof be known. This condition results from the fact that, with the commutators 16a, 17a, 18, 19, and 20 in one condition, the circuits established by the closing of keys 10, 11, and 12 may come out in one group, as 37, whereas, after commutator 20 advances one step, the three circuits mentioned may come out in three different groups or two in one group and one in another.

The amendment to Claim 5 is similar to that made to Claim 2, and Claim 5 is believed to be patentable over Jipp, et al., for the reasons already indicated.

Reconsideration of the rejection of Claims 6, 7, and 9 on Jipp, et al., is requested in view of the inclusion in the claims of "commutation means" or the equivalent, not to be found in terms or spirit in the cited patent unless the elements 1t through 5t are considered the equivalent of not only switches 40 through 44 and 50 through 54 but also commutator 15 through 21 of the Applicants.

Claims 8 and 10 have been canceled, and two method claims, 11 and 12, added. The new method claims are free of mechanical limitations and are believed clearly patentable over any of the references cited.

The present address of Applicant Frank B. Rowlett is 216 South Pershing Drive, Arlington, Virginia. Please make the necessary correction.

It is desired that prosecution of the application continue under the three-year rule.

Favorable action is requested.

Respectfully,

WILLIAM F. FRIEDMAN and
FRANK B. ROWLETT, Inventors

BY: _____
Their Attorney

23 November 1942

This case has been examined, and the search discloses the following references:

Jipp, et al.	1,912,983	June 6 , 1933	178-22
Hebern	1,683,072	Sept 4 , 1928	"
Korn	1,733,886	Oct. 29, 1929	"
Friedman	1,522,775	Jan. 13, 1925	"
Hovland	1,111,695	Sept 22, 1914	"
Vernam	1,310,719	July 22, 1919	"
Pierce	1,426,669	Aug. 22, 1922	"

Claim 1 is rejected on Jipp as obviously fully met.

Claim 2 is rejected on Jipp as substantially met. Jipp uses a double pole double throw switch instead of a single pole double throw, but this is so only because Jipp desires to use a polarized current system instead of the current and no current system used by applicants. The circuits between the relays 6 to 10 and 11 to 15 of Pierce are identical to the circuits between relays 40 to 44 and elements 50 to 54 of applicants.

Claims 3 and 4 are rejected on the ground that applicants have not disclosed the construction and mode of operation of their scrambling unit in "such full clear, concise and exact terms" as are required by the statutes and Rule 34.

Claims 3-4 are further rejected as Hebern as substantially met. To connect any of the output wires to a plurality of contacts seem a pure matter of choice.

Claims 5 and 6 are rejected on Jipp as obviously fully met.

Claim 7 is rejected on Jipp as substantially met. No invention would be required to insert a control board between the Battery 3A and the input to the commutator 1t to 5t.

Claims 8 and 9 are rejected on Jipp as fully met. The scrambling unit of Jipp is a commutator.

Claim 10 is rejected as obviously fully met by any of the above cited patents ans as being vague, and as including apparatus limitations in a method claim.

Unapplied references are cited to show the state of the art and may be relied on in future actions.

"like", on page 2, line 19 should be as.

The residence of the second inventor, as given in the oath, does not correspond with that given in the petition and preamble. Correction is required.

Examiner

Patent Application of Wm. F. Friedman and Frank B. Rowlett - S.N. 443,320

1.	Wm F. Friedman and Frank B. Rowlett, Sig. Intel. Serv.	Your patent application prepared on recent date was filed in the United States Patent Office May 16, 1942, and received Serial No. 443,320.

W.D H.

N.M
H. Nelson Moore,
1st. Lt., Sig. Corps
SPSLG
May 22, 1942

SECRET

ASSIGNMENT

WHEREAS, ~~we~~, ~~William F. Friedman and Frank B. Rowlett~~, of ~~5555 Military Road, N. W., Washington, D. C., and 2800 N. Madison Street, Arlington, Virginia, respectively~~, have invented certain improvements in ~~Cryptographic Systems~~, ~~Sig. Corps Case SC-B-WIGWN~~ for which the undersigned on ~~even date herewith~~ executed an application for Letters Patent of the United States, and

WHEREAS, the invention was made while the undersigned was in the employ of the War Department, and pertains to a device useful in the National Defense, and

WHEREAS, The Government of the United States is desirous of acquiring the entire right, title, and interest in and to the said invention and in and to any patents that may issue thereon.

NOW, THEREFORE, in consideration of the premises and one dollar ($1.00), the receipt of which is hereby acknowledged, the undersigned have sold, assigned, and transferred, and by these presents do hereby sell, assign and transfer unto the Government of the United States of America, as represented by the Secretary of War, the entire right, title and interest, throughout the United States of America, and the territories and dependencies thereof, and not elsewhere, in and to the said invention and to the invention as described in the specification executed by the undersigned on ~~even date herewith~~, preparatory to obtaining Letters Patent in the United States therefor, and to all Letters Patent issuing thereon and any continuations, divisions, renewals, and reissues or extensions of such Letters Patent, the said entire right, title and interest as well as the control of the prosecution of the application and all continuations, reissues and divisions thereof to be held by the Government of the United States of America (as represented by the Secretary of War) and all Letters Patent including any divisions, reissues, renewals or extensions thereof as there are or that may be granted, to be held by the Government as fully and entirely as the same would have been held by me had this assignment and sale not been made. The undersigned hereby gives the Government of the United States of America the non-exclusive right to make, use, or sell the invention for governmental purposes in all foreign countries.

Provided, however, that upon any subsequent notice of allowance of said application or of any renewals, substitutions, divisions, continuations, or continuations-in-part being given by the Commissioner of Patents, the entire right, title, and interest in and to said invention and said application or any renewals, substitutions, divisions, continuations, or continuations-in-part, and such patents as may be issued thereon, will thereupon revert to ~~William F. Friedman and Frank B. Rowlett~~ subject to an irrevocable, non-exclusive, and royalty-free right and license remaining vested in the United States of America as represented by the Secretary of War, to make, have made, to use, and to sell the subject matter of said invention for governmental purposes only, to the full end of the term or terms for which any Letters Patent, divisions, reissues, renewals, extensions, continuations or continuations-in-part are or may be granted.

_____ _____
Witness

_____

Before me, a notary public in and for the _____ appeared the above-named _____, personally known to me, who in my presence executed the foregoing assignment and acknowledged that his execution thereof was his free act and deed.

Signed_____ this_____day of

(Seal) _____
Notary Public

SECRET

CRYPTOGRAPHIC SYSTEM

This invention relates to secret signaling systems, and, more particularly, to cryptographic systems.

In the particular embodiment of our invention described below, the apparatus is designed to be connected to existing telegraph machines to make them secret, but it is understood that the invention may be built in the machines so that the machine and our secrecy effecting improvement is a single entity.

One object of this invention is to provide a simple device that may be connected to an existing standard "Teletype" machine to effectuate secrecy of the communication conducted over a wire line between a transmitting station and a receiving station. Another object of the invention is to provide a system of changing the characters applied to a secret code sending or receiving machine, to thereby modify the code transmitted (or received) so that secrecy is effected. Many other objects and advantages of our invention exist, and can best be understood by reading the following detailed discussion of the drawings and studying the appended claims. The invention has been illustrated in detail; except that the conventional "Teletype" machine has not been illustrated in all of its details. Due to the detailed showing in the drawings, it is under tood that only such features as are recited in any appended claim are essential to the novelty of such claim.

Briefly speaking, the "Teletype" machine has a distributor device which, for each letter, connects the line sequentially to each of five circuits. These five circuits may be open or closed, depending on the particular letter sent, and in a standard "Teletype" machine, are operated by a set of five single throw switches which in turn are operated by the keys of the "Teletype" keyboard. In our invention the circuits to the distributor are control ed not only by a first group of switches, as mentioned above, but by another set as well which are so connected, that when the pole arms of any parti ular pair of switches are moved to certain complimentary positions a circuit through th t pair of switches to the distributor is completed.

When the pole arms of a particular pair of switches are not in complementary positions, the circuit therethrough is broken. The primary feature of novelty of this invention resides in a combination of the second group of these switches with a keying sequence generator for controlling the position of the second group of switches, although some novelty is believed to exist in the arrangement of switches as such, and in the keying sequence generator per se. The "keying sequence generator" comprises a commutating structure (such commutation structure per se being of the common, very well known type) with its output randomly connected to the relay coils of the second group of switches. The input of the commutation device is controlled by a keyboard that may be used to establish the "key" of the coded message.

In the drawings, Figure 1 is a schematic diagram of a transmitting station utilizing our invention, while Figure 2 is a schematic diagram of a receiving station utilizing the invention. The transmitting station utilizes an output line 68 that connects to the input line 68' at the receiving station.

In Figure 1, the "Teletype" machine 100 has a spacer bar 101, as well as a plurality of keys. The keys are depressed just like typewriter keys are depressed. As each key is depressed the "Start" segment 60 is energized, thus energizing the "Start" segment 60' through line 68 and 68', thereby actuating an electromagnetic release mechanism R and R' causing the rotation of brush arms 67 and 67', at both the transmitting and the receiving station, in synchronism with each other. The two brush arms 67 and 67' respectively pass across their complementary segments 61, 62, 63, 64, 65 and 66, and 61', 62', 63', 64', 65' and 66' at the same time. When segment 66' is energized, due to energization of

"Stop" segment 66, brush arm 67 stops when the "Start" segment 60 is reached. Circuits are established to segments 61 to 65 by the switches 54, 53, 52, 51 and 50, respectively. These switches are moved to the right or left positions by operation of keys at the keyboard and an example of the positions of the arms 50-54 for a few letters is given:

Letter	Switch 50	51	52	53	54
A	Right	Right	Left	Left	Left
B	Right	Right	Right	Left	Right
C	Left	Left	Left	Right	Left
D	Right	Left	Right	Left	Right
etc.					

The group of switches 45 to 49 also have right and left motions. These motions are controlled by relay coils 44, 43, 42, 41 and 40, respectively.

When switch arms 54 and 45 and both to the right, or both to the left, there is no circuit to the segment 61. When either of switch arms 54 or 45 is to the right, with the other to the left, a circuit to segment 61 is completed. This effectuates control of energization of 61 depending not only upon the position of arm 54 as determined by the "Teletype" key depressed, but also upon the position of arm 45 which in turn depends upon the position of the scrambling mechanism 15-21 of Figure 1.

What has been said above relative to complementary switch arms 54 and 45 equally applies to complementary switch arms 53 and 46, 52 and 47, 51 and 48, and 50 and 49.

The energization of the several segments 60 to 65 inclusive therefore depends upon the conjoint action of switch arms 45 to 54 inclusive of which the arms 50 to 54 are controlled by the plain language text of the message, whereas arms 45 to 49 are controlled by the sequence generator (the scrambling means).

The scrambling means utilizes a control board having a plurality of circuit closers such as 10, 11, and 12, one side of each circuit closer being connected to ground 14 through a battery 13. The other side of the circuit closers connect to the input segments of the end plate 15 of the input commutator. For example, the circuit closer 10 connects to segment S, circuit closer 11 connects to segment 16, and key 12 connects to segment 18. The other keys connect to one or more of the remaining segments in any orderly or irregular fashion. It is not necessary that an equal number of circuit closers and input segments be used. For example, there may be only thirteen circuit closers (such as 10, 11, 12, etc.) connected to thirteen of the twenty-six segments. The input stationary end plate 15 feeds the several rotatable commutators 16a, 17a, 18, 19, and 20 successively, in the well-known manner. The rotatable commutators are rotated in a controlled manner which may, in simple embodiments, be periodic and correspond to that in an odometer; but where greater complexity is desired the control may be of an irregular type causing aperiodic displacements of the commutators. Means for such periodic or aperiodic control are well known in the art and their details per se do not form a part of this invention. The output end of the commutation machine includes a stationary receptor commutator plate 21 having a plurality of contact terminals lettered from A to Z inclusive. These contact terminals are irregularly connected so that there are five resulting circuits 30, 31, 32, 33, and 34, each of which connect to one or more of the twenty-six contact points of output receptor plate 21. For ease of illustration the wire 32 connects to wire 39 that connects to adjacent points S, T and U; wire 31 connects to wire 29 that connects to adjacent points W, X, and Y; wire 34 connects to wire 35 that connects to adjacent points A, B and C; wire 33 connects to wire 37 that connects to points I, J, and K; and wire 30 connects to wire 36 that in turn connects to points E, F and G. Various variable arrangements are possible, some of which are now mentioned. The wire 39, for example, could connect to any one or more points, not necessarily to the three adjacent ones S, T, and U. The wire 30, for example, does not need to

connect to wire 36 but can be connected to any of the wires 29, 35, 36, 37 or 39. A plug board is provided in the dotted rectangle 38 for effecting such a change. Any one or more of the wires 30, 31, 32, 33 and 34 may be disconnected entirely except, of course, if all are disconnected, there will be no secrecy whatever effectuated by the scrambling means.

The receiving station of Figure 2 is similar to the transmitting station of Figure 1 in most respects and parts which are similar in construction and operation to corresponding parts of Figure 1 bear like reference numbers. The reference numbers applying to the receiving equipment are, however, primed.

The incoming line 68' connects to the brush arm 67'. When the "Start" impulse for each letter is applied to the line 68 due to depressing a key of the "Teletype" 100, the "Start" segment 60' is energized, hence the solenoid 70' is likewise energized. This operation energizes the solenoid 27' through the battery 13' and ground 14'. The armature 28' operates the actuators 22', 23', 24', 25' and 26' in the same manner as the corresponding actuators of Figure 1 are simultaneously operated. Hence the five commutators 16a', 17a', 18', 19' and 20' operate in like manner to corresponding parts of Figure 1.

It is necessary for the operator at the receiving station to depress keys 10', 11', and 12' and the others of the same series, in the same manner that they are depressed at the transmitting station. These keys may be depressed and released from time to time at the transmitting station and receiving station in order to confuse possible interceptors of the message. Similarly the commutators 16 to 20 and the corresponding ones at the receiving end may be moved manually from time to time to confuse unauthorized interceptors of the message.

If the operator at the receiving station adjusts his apparatus to operate properly, the relays 45', 46', 47', 48' and 49' will

always have the same positions respectively as the corresponding relays 45, 46, 47, 48 and 49 which are at the transmitting station. Accordingly, the circuits through switches 50', 51', 52', 53' and 54' will be modified in like manner to the circuits through switches 50, 51, 52, 53, and 54, respectively. Hence the energization of solenoids 72', 73', 74', 75' and 76', which are at the receiving station, will be energized in the same order that they would be if the second sets of switches 45 to 49, inclusive, and 45' to 49' were eliminated at both the transmitting and receiving stations.

The solenoids 72' to 76' may be the printer magnets of a receiving "Teletype" machine (or the printer or perforator magnets of any similar device).

In Figure 1, the parts identified by reference numbers 10 to 39, inclusive, comprise what we call a "Keying Sequence Generator." The keying sequence generator shown in the drawings and hereinbefore described is believed to be novel per se and performs the function of generating a predetermined sequence by which the wires 30, 31, 32, 33 and 34 are respectively energized. The respective energizations of these wires are determined by:

(a) The positions of the keys 10, 11, 12, etc.;

(b) The law by which the several devices 22, 23, 24, 25 and 26 advance the commutators;

(c) The method of irregular wiring of the commutators 16a, 17a, 18, 19 and 20;

(d) The output segments to which the output wires 29, 35, 36, 37 and 39 are connected, and;

(e) The positions of the several plugs in the plug and jack board 38.

The distributor 60-66 aids in effecting a secret signaling system, but we wish to distinctly state that it is not essential to the basic characteristics of our invention. The distributors 60-66 and 60'-66' may be completely eliminated and the wires A, B, C, D and E connected directly (or in any indirect way) respectively to wires A', B', C', D' and E'.

We Claim To Have Invented:

1. In a secret signaling system, in combination; enciphering means comprising a keying sequence generator, a plurality of pairs of control elements, one element of each pair being connected to and controlled by the sequence generator to operate in a predetermined manner, means controlling the other element of each pair in accordance with the text to be transmitted, a distributor having a plurality of segments, each segment being controlled by one of said pairs of elements, and means cooperating with said elements and segments whereby each segment is actuated in accordance with the text of the message as modified by the operation of the sequence generator on the elements; a line fed by said distributor; and deciphering means fed by said line for deciphering the signals transmitted by said enciphering means.

2. In a secret signaling system, a plurality of pairs of single pole double throw switches, each pair having first and second individually operable switches and each switch having a pole arm and two contacts, means for controlling the first switch of each pair in accordance with the plain text of the message, means operating the second switch of each pair depending upon a predetermined law, wire means cooperating with each pair of switches for independantly connecting together one contact of the first switch of the pair to a contact of the second switch of the same pair, and for connecting the remaining contacts of the switches of each pair together, means connecting one of the pole arms of each pair of switches to a source of current, the distributor having a distributor segment for each of said pairs of switches, and means connecting the remaining pole arms of each pair of switches to the distributor segments respectively.

3. A keying sequence generator comprising a commutating system having a plurality of irregularly connected input and output segments, an input system having a plurality of input terminals respectively connected to the input segments of the commutating system, an output system having a plurality of output terminals respectively connected to the output segments of the commutating system, individual circuit closers for some of the input terminals, and a plurality of output wires at least one of which is connected to a plurality of output terminals.

4. A sequence generator comprising a commutating system for establishing random permutations of connections, said commutating system having input segments and output segments with means for establishing random permutations of connections between the input and output segments, a plurality of means respectively controlling the input segments, means dividing the output segments into a plurality of groups of segments, and means having a plurality of output devices respectively responsive to each group of output segments; whereby an output device is operated each time its corresponding group of segments is actuated.

5. In a secret signaling system, a transmitting station, a receiving station, a plurality of feeding circuits at the transmitting station and a like number of fed circuits at the receiving station, means connecting the feeding circuits respectively to the fed circuits, switches in each of the feeding circuits for closing and opening them according to the message to be enciphered and transmitted, means at the transmitting station for modifying the operation of said switches in their respective effects upon energization and deenergization of said circuits comprising additional switches in each of the feeding circuits, means for opening and closing said additional switches in a predetermined sequence; means associated with the switches in the fed circuits for indicating the intelligence received, the last-named means including additional switches and means for opening and closing the same in the same sequence that the said additional switches at the transmitting station are opened and closed, whereby to decipher the message on reception.

6. A system of secret transmission between a transmitting station and a receiving station including a plurality of sending and receiving circuits at each of said stations respectively of which there are complementary circuits at the respective stations sequentially and intermittently connected to each other; means at the transmitting station for modifying the energization of the circuits comprising a switch connected in one of the transmitting circuits for opening and closing such circuit intermittently, and commutation means operable to control opening and closing of said switch; means at the receiving station for modifying the energization of the circuits comprising a switch connected in one of the receiving circuits for opening and closing such receiving circuit intermittently, and commutation means for operating the last-named switch in similar manner to the operation of the first-named switch by the commutation means at the transmitting station; transmitting means controlling the energization of the circuits at the transmitting station; and receiving means responsive to energization of circuits at the receiving station for receiving the intelligence.

7. A secret signaling system comprising a transmitting station and a receiving station; said transmitting station comprising a line output circuit and a plurality of feeding circuits therefor, means for sequentially connecting said feeding circuits to said line output circuit one at a time, a plurality of devices each respectively in one of said feeding circuits to control energization thereof, each of said devices comprising two parts, both of which have first and second positions of operation, each of said devices having means for energizing its respective feeding circuit when the two parts thereof are in complimentary positions, and for deenergizing the circuit when the two parts thereof are in positions other than complimentary positions, a transmitting keyboard, means operated by the keyboard for shifting one of the parts of each of said devices from first to second positions and vice versa, commutating means, a control board controlling the input of said commutating means, and means responsive to the output of the commutating means for controlling the remaining parts of said devices in a predetermined manner; said receiving station having a line input circuit connected to and fed by the line output circuit of the transmitting station, a plurality of fed circuits, means for sequentially connecting said fed circuits to said line input one at a time and in synchronism with the rate that the feeding circuits at the transmitting station are connected to the line output, a plurality of receiving devices one in each of said fed circuits which devices have two parts and each part of which has two positions of operation, indicating means controlled by said receiving devices and having a plurality of actuating elements respectively connected to said receiving devices, each of said elements being actuated when the parts of its respective device are in complimentary positions, second commutating means similar in construction and mode of operation to that at the transmitting station, a control board similar in construction and mode of operation to the control board at the transmitting station, means whereby the last-mentioned control board controls the input of said second commutation means, and means responsive to the output of said second commutation means for controlling the remaining parts of said receiving means in like manner that the first-named devices are controlled whereby the receiving devices will effectuate reproduction by said indicating means of the intelligence transmitted at the transmitting station.

8. In a signaling system, a transmitting station comprising first and second groups of elements of which each element of each group is adapted for operation to a plu ality of positions, means controlling the position of the elements of the first of said groups of elements according to the text to be transmitted, a sequence generator for effectuating a predetermined operation by sequentially changing the position of the elements of the second of said groups; and a receiving station comprising third and fourth groups of elements of which each element of each group is adapted for operation to a plurality of positions, means whereby the position of the elements of the third group is controlled by the conjoint action and in dependance upon the positions of the elements of the first and second group, means whereby elements of the fourth group of elements are operated in a sequence similar to the sequence of said second group of elements, and means responsive to the conjoint operation and acting in dependance on the positions of the third and fourth groups of elements for giving indications of the text transmitted.

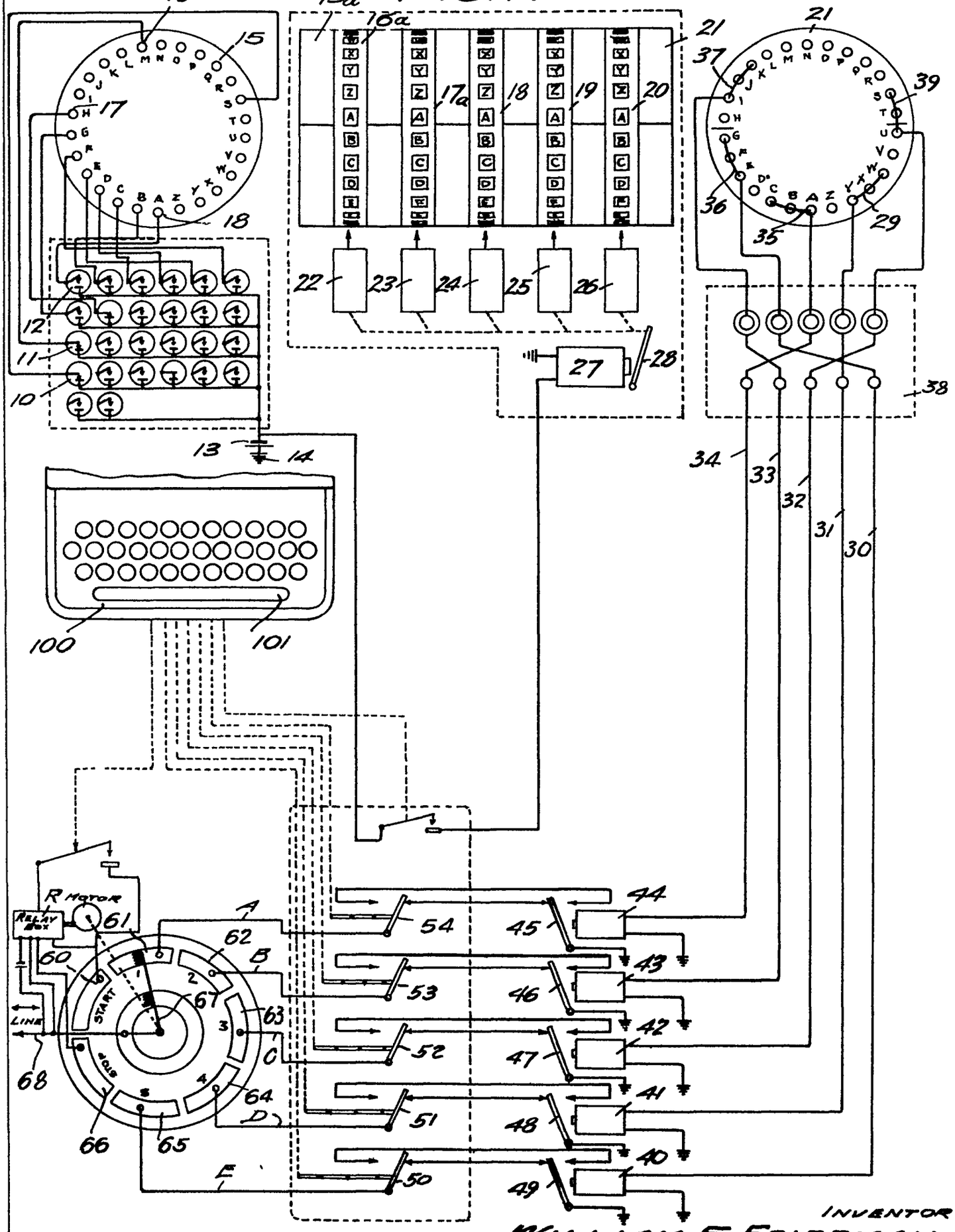
9. In a signaling system; a transmitting station; a receiving station; means for transmitting energy intermittently from said transmitting station to said receiving station, said means including scrambling means at the transmitting station which is subjected to predetermined operation and which when operated in a predetermined manner effectuates a current flow at a predetermined time if current would not otherwise flow at that time and stops current flow at such predetermined time if current would otherwise flow; and a keying sequence generator for effecting said predetermined operation intermittently comprising a commutator having randomly connected input and output segments, means for moving said commutator according to a predetermined law, stationary brush means for feeding current into a part of the input segments, output stationary brush means for receiving current from a part of said output segments, and means energized by the output stationary brush means for effectuating said predetermined operation of said scrambling means in said predetermined manner intermittently.

SECRET

10. The method of secret communication which includes applying a "key" to a commutating means, relay means operated by the commutation means, and deciphering the signals by the operations of the relay means.

SECRET

FIG. 1.



INVENTOR
WILLIAM F. FRIEDMAN
FRANK B. ROWLETT
BY William D. Hall.
ATTORNEY

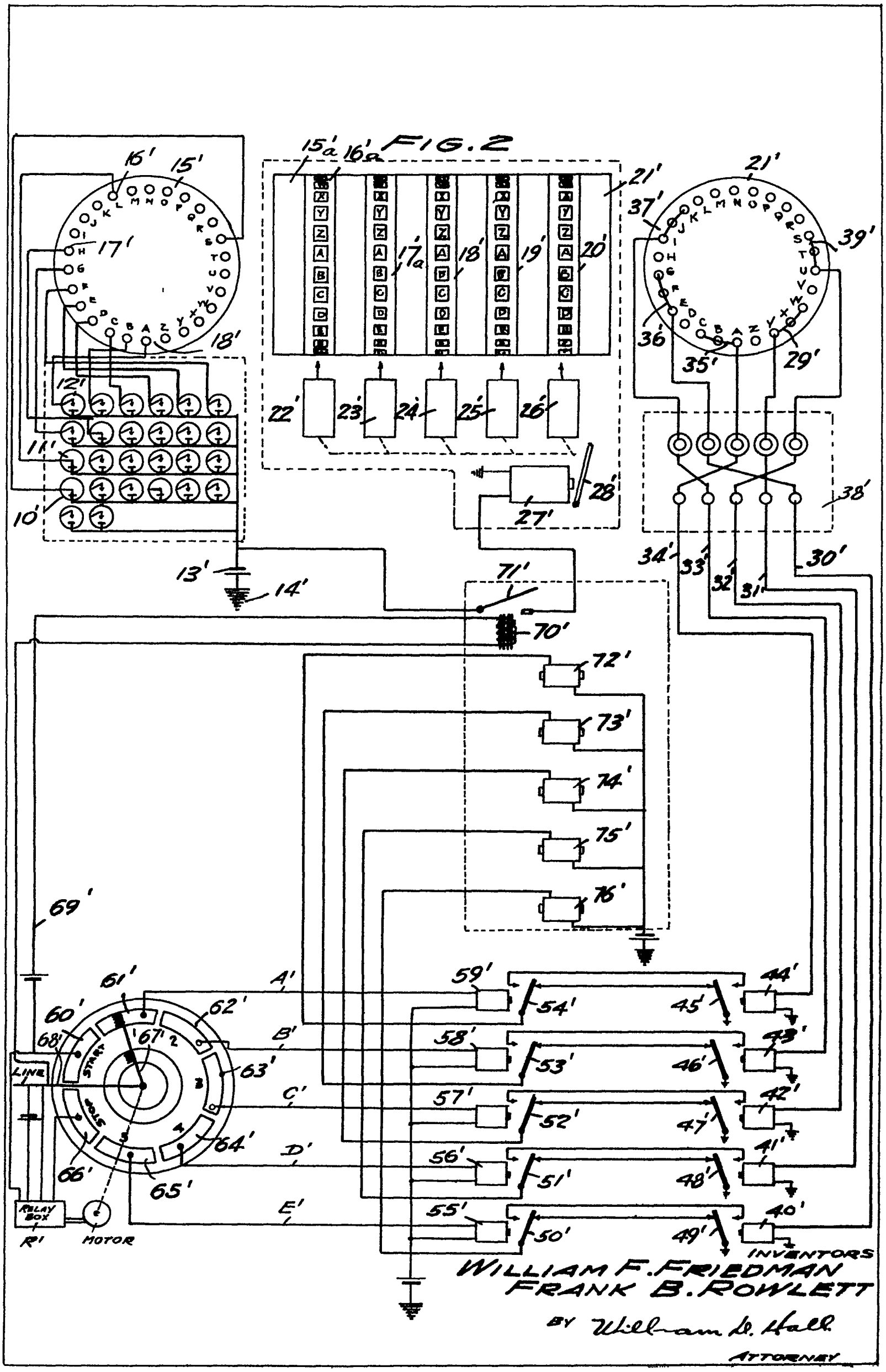


FIG. 2
LINE
START
STOP
RELAY BOX
MOTOR
R'
INVENTORS
WILLIAM F. FRIEDMAN
FRANK B. ROWLETT
BY William L. Hall
ATTORNEY

IN REPLY REFER TO
R&D Patents
OCSigO Friedman & Rowlett

WAR DEPARTMENT
OFFICE OF THE CHIEF SIGNAL OFFICER
WASHINGTON

#10
(C-3)

September 25, 1941

Subject Invention - Cryptograph

To Mr W. F Friedman, Cryptanalyst and
Mr. Frank B Rowlett, Cryptanalyst
Signal Intelligence Service - Room 3341

THRU - Officer in Charge, Signal Intelligence Service

1. At a meeting of the Signal Corps Patent Board held on September 23, 1941, the subject invention was considered and found to possess sufficient merit to warrant preparing and filing a patent application at government expense.

2 It is the policy of this office to prepare patent applications in the order in which inventions are submitted, and accordingly it will be several months before this case is reached for action.

By order of the Acting Chief Signal Officer:

Donald K Lippincott
Donald K Lippincott,
Major, Signal Corps

OCSigO 201-Friedman & Rowlett (9/25/41) 1st Ind. 13

Signal Intelligence Service, OCSigO, September 26, 1941.
To: Messrs. W. F.Friedman, Principal Cryptanalyst, and Frank B Rowlett, Cryptanalyst.

A.W.M.

SECRET

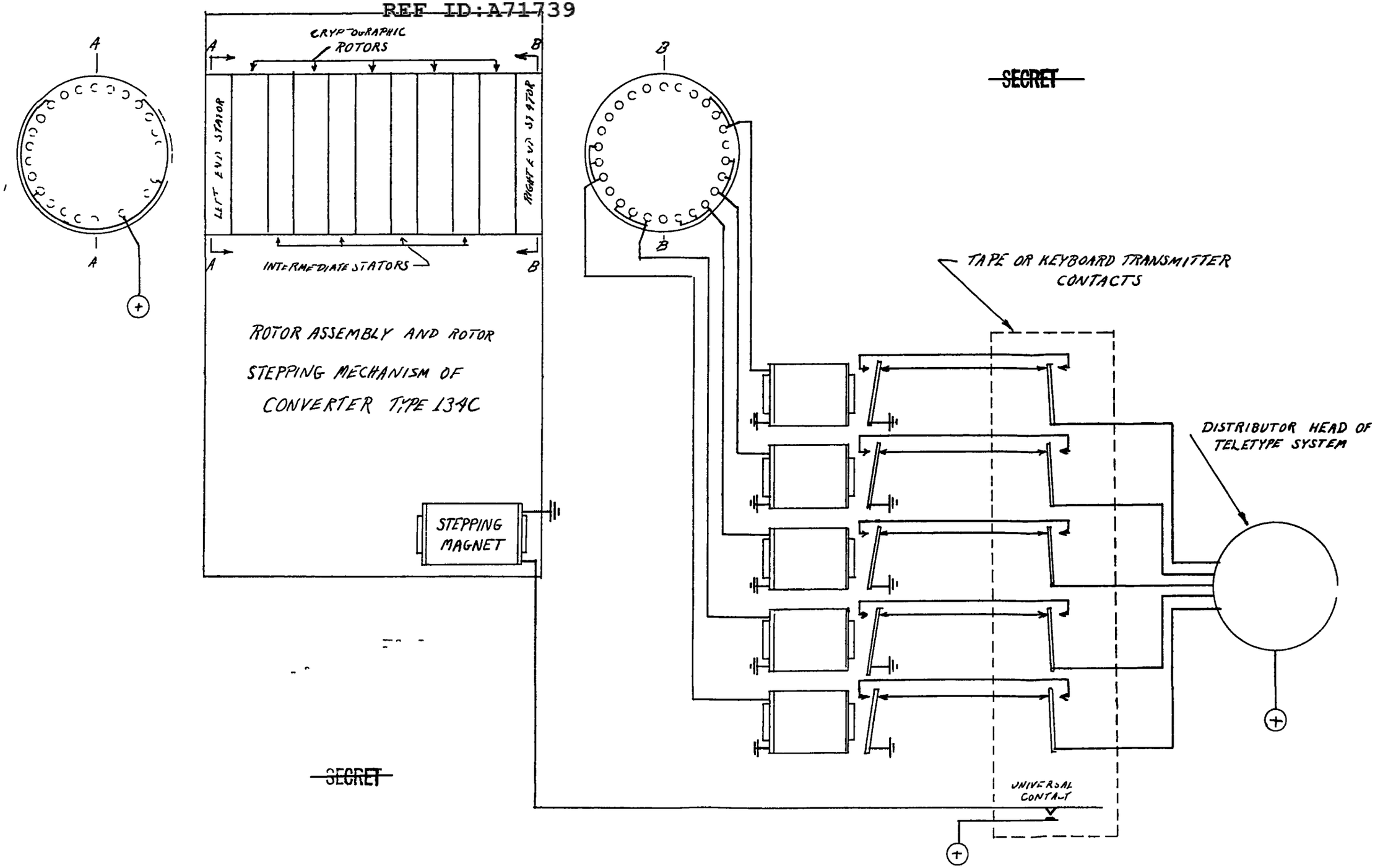
Converter Type M-228

1 R&D Herewith are two copies of a sketch showing the principal mechanisms and circuit diagram for the proposed Converter M-228 for enciphering teletype messages. The parts included under the designation "Rotor Assembly and Rotor Stepping Mechanism of Converter M-134C" are now being manufactured by the Teletype Corporation, under secret contract (Navy) and can be very easily adapted for use with Converter M-228 by eliminating from an M-134C the keyboard, printer unit, reversing switch and certain other minor parts unnecessary for operation of Converter M-228. The "stepping magnet" shown in the sketch is intended to represent the clutch release magnet of M-134C which is operated with each depression of a key of the keyboard in the latter machine. In M-228 the clutch release (or stepping) magnet would be operated by a universal contact on the keyboard of the teletype or on the tape transmitter, in case of tape operation of the teletype circuit. This would insure that the cryptographic rotors step with each letter or character transmitted.

Attached: 2 Copies of sketch

S.I.S. 7-10-41

SECRET



ROTOR ASSEMBLY AND ROTOR STEPPING MECHANISM OF CONVERTER TYPE 134C

Converter for Use on Electrical Printer Circuit.

1 WP&T 1. Due to the constantly expanding use of the teletype and TWX service between the fixed headquarters of the military establishment, and the possibility that much confidential and some secret matters pass over the circuit pertaining thereto, it appears highly desirable that an automatic system of enciphering and deciphering this traffic during its transmission be instituted.

2. A system and mechanism for this purpose has been conceived by members of this section and forms the subject of a separate paper soon to be filed for action by the Signal Corps Patents Board. The cryptographic mechanism would yield the highest degree of security and for this reason it would be desirable that the entire subject be placed in the secret category.

3. The cryptographic mechanism makes use of certain parts and apparatus now employed in Converter M-134-C which is being manufactured in quantity by the Teletype Corporation in Chicago. It is highly desirable that two models of the proposed apparatus be constructed, as promptly as practicable, and in view of the facts

presented in the preceding paragraphs it would further seem desirable that the two models be constructed by the Teletype Corporation. The proposed mechanism formed the subject of informal discussions with Mr. Rieber of the Teletype Corporation last week. In his opinion the apparatus can be made extremely practicable and would, without question, do the job for which it is intended.

4. In connection with the contemplated use of this converter, it may be necessary to secure from the American Telephone and Telegraph Co. permission to superimpose a cipher converter on their equipment.

5. In view of the foregoing, it is requested:

a. That a converter for use on electrical printer circuits be considered as a required type.

b. That a type number be assigned to this converter.

c. That a project be set up for the design, development, and construction of two models based upon the accompanying statement of

military characteristics.

d. That the subject equipment and all matters pertaining to its development and contemplated use be placed in the secret classification.

S. I. S.
5/9/41

1 Enclosure:

1. Statement of Military Characteristics.

May 9, 1941.

MILITARY CHARACTERISTICS OF CONVERTER

FOR USE ON ELECTRICAL PRINTER CIRCUITS.

1. The converter should be designed for t e purpose of automatic encipherment and decipherment of messages transmitted by teletype or similar printing telegraph apparatus based upon a multiple-impulse-code such as the Baudot.

2. It should be designed so as to encipher the signals established either by tape or keyboard operation, causing enciphered text to be transmitted instead of the plain text represented on the tape or set up on the keyboard. At the receiving end the apparatus should decipher the received cipher signals, converting the cipher text into plain text before the signals are fed into the printer, or into the perforator in the case of tape operation. In other words, encipherment, transmission, reception, and decipherment are to be accomplished in a single step rather than in two separate steps at each end.

3. The converter should use as its cryptographic principle a non-repeating keying sequence of multiple-impulse characters, the latter to interact with the plain-text signals according to the rule that "like signs produce spacing current, unlike signs produce marking current." (The latter principle is well known in the art.)

4. The keying sequence mentioned in Par. 3 should be produced by a plurality of electrical cryptographic rotors in cascade, through which impulses are sent and recombined in a manner so as to produce the equivalent of a random sequence of characters according to the multiple-impulse-code used by the transmitter. (If teletype, the characters will be 32 in number and should be in random order.) The number of rotors in cascade should be at least three and preferably five.

5. The rotors mentioned in Par. 4 may be identical with those now used in Converter M-134-C. Mechanism should be provided to cause meter-like stepping of these rotors, at least one being displaced angularly for each character to be enciphered and transmitted. The order of stepping of the entire set of rotors, however, should be capable of being varied so that the complete set of factorial n motions may be available for use, n being the number of rotors in cascade.

6. The converter should be motor-operated from the same power source as that employed for the telegraph printer. It should, however, be designed to function as a separate unit and not as an integral part of the printer itself, so that either normal plain-text operation or cryptographic operation of the printer circuit can be effected at will. The converter should be capable of being electrically connected or

associated with the tape (or keyboard transmitter) and with the printer by means of a suitable plug and jack or multiple plug arrangement, so that it may be readily connected or disconnected from operation.

7. The converter should be of approximately the following dimensions: 12"x8"x8"; and its weight should not exceed 50 lbs.

Enclosure #1

~~SECRET~~

2 R & D

It is recommended that the attached military characteristics be presented to the Signal Corps Technical Committee for consideration.

1 Incl. n/c

R. B M.
WP&T 5-13-41.

3 WP & T and S I S IN TURN

1. SCTC at Meeting #194 on June 9, 1941, recommended that military characteristics in accordance with the inclosed "Military Characteristics of Converter for Use on Electrical Printer Circuits" be adopted and that a project be initiated for the development of Converter M-228, the military characteristics and equipment to be classified as "secret".

2. Following approval by the Adjutant General of the SCTC recommendations above, SCL will be directed to initiate a project for the development of Converter M-228 and for the procurement of service test models with funds to be made available from this office.

3. It is understood that SIS has constructed a model of Converter M-228 and it is recommended that this model be turned over to R&D for shipment to SCL so that negotiations for development and production of service test models by a commercial firm may be expedited.

1 Incl.
M/C of Converter for Use on Electrical Printer Circuit.

H M.
.10 R & D
6-30-41

4 S I S

1. Military Characteristics for Converter M-228, as recommended at SCTC Meeting No. 194, have been submitted to The Adjutant General for approval.

2. WP&T concurs in procedure proposed in paragraph 3 of Action 3 above.

WP&T 7-2-41

1 Incl. n/c

~~SECRET~~

Converter for Use on Electrical Printer Circuit (cont'd.)

5 R&D

1. Actions 2, 3 and 4 have been noted.

2. Reference paragraph 3, action 3, you are advised that no model of the Converter M-228 has been built by this division, nor was one contemplated As an enclosure to R&W sheet from this division to R&D, dated May 10, a diagram of the proposed converter was furnished. It is suggested this diagram be made available to the SCL.

S.I.S. 7-7-41

C
O
P
Y

SIS DE-29

1. R. & D.

1. Attached hereto is a memorandum addressed to the Chairman of the Patent Board covering an invention of a cryptographic system and apparatus for electrical printing telegraphy conceived by two members of the SIS. A rough sketch accompanies the disclosure. It is recommended that steps be taken to obtain a patent on this invention under the provisions of AR 850-50, paragraph 2.

2. Inasmuch as one of the principal elements in this invention is similar to the cryptographic element embodied in Converter M-134-C, and inasmuch as the present invention is regarded as providing a very high degree of cryptographic security, it is recommended that this invention be placed in the secret category.

3. When the time comes for drafting the specifications describing the invention for the purpose of making patent application, Mr. Friedman and Mr. Rowlett will be glad to cooperate with the Signal Corps Patent Section.

SIS 5-10-41

To the Chairman, Patent Board

We believe ourselves to be joint inventors of a cryptographic system and apparatus for electrical printing telegraphy and request that you investigate its military value, patentability, and inventorship. In support of this request the following information is submitted:

At the time we conceived the invention, our employment was in Signal Intelligence Service, OCSigO. We originally conceived the idea September 1, 1939 and communicated it to: Robert O. Ferner and Solomon Kullback, October 10, 1939.

The first written and dated records are September 1, 1939.

The invention has not been developed or tried, but informal opinion by Mr. Reiber of Teletype Corporation is that system and apparatus is perfectly practical and easy to build and operate.

Its uses are for direct automatic encipherment and decipherment of printer traffic.

Others associated with us in this development or having knowledge concerning it are:

Captain H. G. Hayes
Captain Eric H. F. Svensson
Lieutenant Paul W. Albert
Mr. Vernon E. Cooley
Mr. A. H. Reiber (Teletype Corporation)

Attached is 1 sheet, initialed and dated by us and two disinterested witnesses, giving a rough sketch of the invention.

We agree to abide by the decision of the Patent Board or of the Chief Signal Officer and will promptly execute all papers re uired of us by these authorities including an assignment of the invention to the Government if it is decided by the Patent Board and confirmed by the Chief Signal Officer, that the application should be assigned.

William F. Friedman
Principal Cryptanalyst

3932 Military Road,
Washington, D. C.

Date of signature 9 May 1941

Witnesses: Date 9 May 1941
Robert O. Ferner

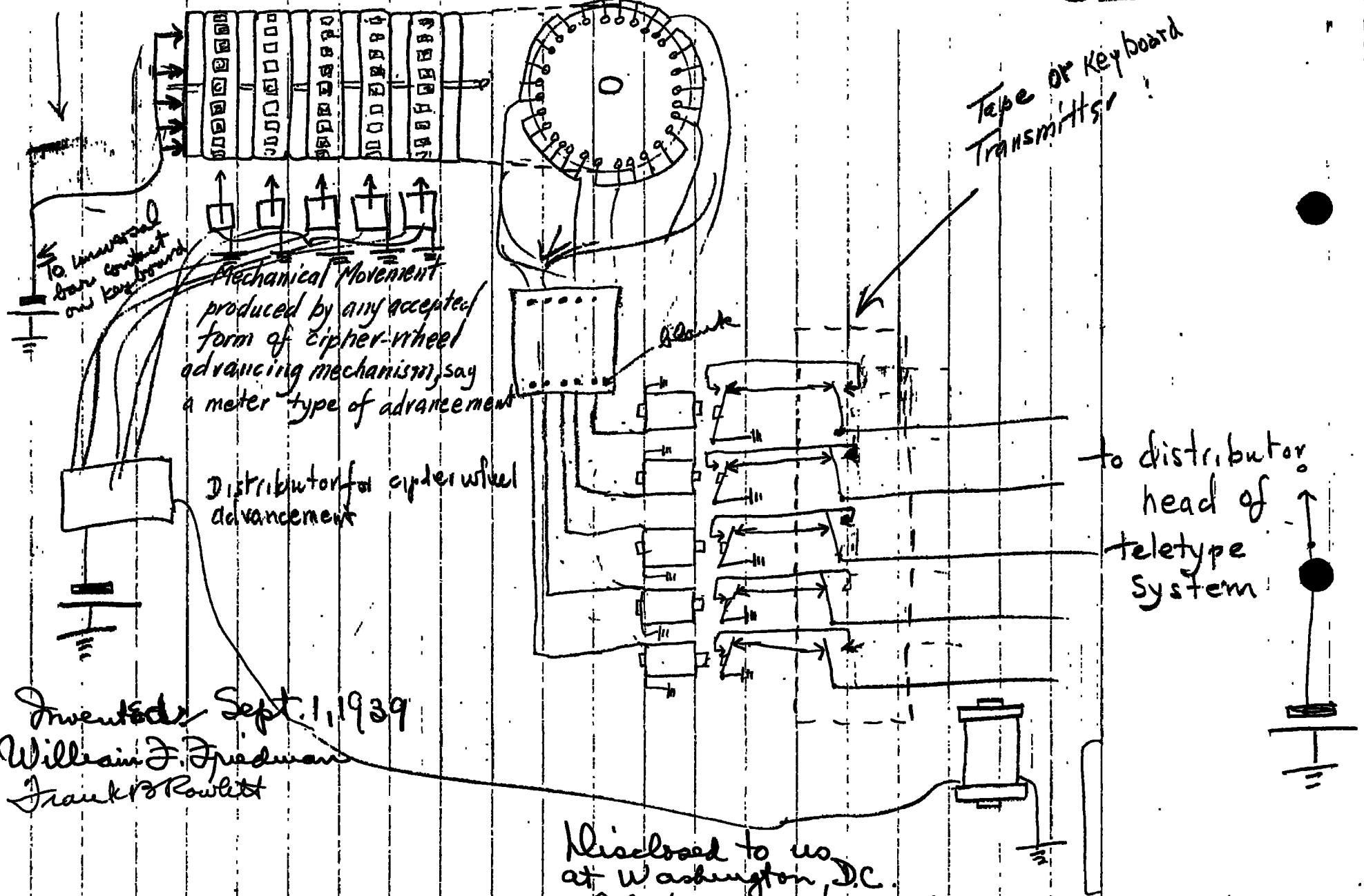
Frank B. Rowlett
Cryptanalyst

East Falls Church,
Virginia

Date of signature 9 May 1941

Witnesses: Date
Solomon Kullback

SECRET



Invented Sept. 1, 1939
William F. Friedman
Frank B. Rowlett

Disclosed to us at Washington, D.C.
Robert A. Fisher October 10, 1939
Solomon Kullback October 10, 1939

SECRET