WAR DEPARTMENT
OFFICE OF THE CHIEF SIGNAL OFFICER
WASHINGTON

November 15, 1933

MEMORANDUM TO: Research and Development Division
(THROUGH War Plans & Training Division)

1 Attached hereto are draft specifications, claims and a drawing covering a new type of cipher machine upon which letters patent are desired It is requested that they be forwarded to the Patents Section with the request that they be prepared for submission to the Patent Office

2 This cryptograph represents a modification of the principles underlying cipher machine type M-134-T., which is being constructed at the Signal Corps Laboratories I not intended, however, that the development referred to be in any way affected by the present invention, which represents alternative scheme that may be desirable to develop at some future time

William F. Friedman,
Signal Intelligence Section

Attached:
Specifications, claims,
and drawing

This invention relates to cryptographs and has as its object the provision of means for automatically, continuously, and aperiodically changing the cipher equivalents representing the plain-text characters of a message to be communicated

The invention is explained in connection with the accompanying drawings Figures 1 and 2 which are merely diagrammatic In these figures, which represent alternative arrangements of but a part of the complete system, I treat the invention as applied to a system for enciphering a set of but ten elements, as for example, the ten digits, but my invention is not limited to this number of elements and can be applied to the encipherment of as large a set of elements as is comprised in the transmission of any kind of intelligence conveyed by written symbols

In Figure 1, there is shown a keyboard, 1, comprising ten contact-closing keys arranged as in the keyboard of a modern ten-key adding machine; 2 is a recording or indicating device which may take the form of a set of magnets of a printing mechanism or a bank of glow lamps to indicate by illumination of superimposed symbols the equivalents resulting from encipherment; 3 is a tape transmitter of the usual type employed in automatic telegraphy based upon the Baudot code, which transmitter, under guidance of a perforated tape, controls the permutative operation of the set of magnets 4, 5, 6, 7, and 8; the assemblies labeled 9, 10, 11, 12, 13 are connection-changing devices, to be explained in

detail below, for providing a multiplicity of paths for the passage of an electric current from the keyboard 1 to the indicating device 2

Taking up one of the assemblies referred to above, for example, assembly 9, this is composed of two fixed bars 16 and 17, a slidable bar 14, and a removable connector plate 21 The bar, 14, slides between the two fixed bars, 16 and 17, the former of which carries ten contact surfaces, the latter, twenty contact surfaces arranged in ten pairs Slidable bar 14 carries ten contact-making elements or springs insulated from one another and suitable for establishing connections between the contacts on bars 16 and 17 One of these springs is labeled 15 When bar 14 is in its normal or inoperative position held so by retractile spring, 18, the contact springs on bar 14 establish connections between the contacts on fixed bar 16 and the left-hand members of the paired contacts on fixed bar 17, when bar 14 is drawn to the right, under the action of magnet 8, then the contact springs on bar 14 establish connections between the contacts on fixed bar 16 and the right-hand members of the paired contacts on fixed bar 17 Thus, one of two alternative sets of ten connections between the contacts on bar 16 and those on bar 17, depending upon the action of magnet 8 can be established For example, when bar 14 is in its normal or retracted position, under the action of coiled spring 18, a current entering assembly 9 at contact 19 would continue along contact spring 15 and emerge at contact 20 on fixed bar 17, but when bar 14 is drawn to the right under the action of magnet 8, then the current would emerge at contact 26 on fixed bar 17

The connector plate 21 consists of one set of twenty insulated ball-bearing contacts on one face and another set of ten similar contacts on the other face The twenty contacts on the one face are connected by insulated conductors to the ten contacts of the other face, each of the ten latter being connected to two of the former contacts, in a random arrangement which can be varied at will This place merely serves to establish variable connections between the successive sets of fixed and slidable bars The plates 22, 23, 24, and 25 are similar in structure to plate 21, but the connections established by their internal conductors are different The plates are interchangeable

The magnets 4 to 8 are, as noted above, under control of the tape transmitter 3, through which is passed a perforated tape bearing holes corresponding to characters in the Baudot code Every time a key on the keyboard 1 is depressed, upon its release or back stroke a contact 30, operated by a universal bar not shown in the figure, is closed This contact controls the tape stepping magnet 36, power for which is supplied by source 37 Thus, with each depression of the key the tape is stepped forward to the next position bringing a new ciphering character into action; these characters form an entirely arbitrary, unintelligible sequence of ciphering elements for controlling the permutative operation of the magnets 4 to 8, and thus of the slidable bars of the assemblies 9 to 13 Since the arrangement is such that a current established by depressing a key of the keyboard 1 must traverse the entire set of connection- changers 9 to 13 before

reaching the indicating device 2, it will be seen that the final cipher resultant of a character on the keyboard depends upon the permutative arrangement of the five slidable bars 14, 26, 27, 28, 29 and thus the cipher resultants will vary with the sequence of ciphering characters on the perforated tape Since this sequence of ciphering characters is a random, unintelligible series of characters, the cipher resultants are entirely arbitrary and show now periodicity in the relationship between plain-text character and cipher equivalent

A particular encipherment operation will now be set forth in detail Let us assume that a key of the keyboard has been depressed and released so that on its backstroke the universal bar closed the contact 30, which operated magnet 36, thus bringing into play the next ciphering character on the tape Suppose this character is represented in Baudot code by - ǂ - - - Then the pins in the tape transmitter 3, passing through the proper holes in the tape, cause contact 32 to close A current from power source 39 flows along conductor 40, closed contact 32, conductor 41, through magnet 5, conductors 42 and 43, back to power source 39 Magnet 5 is energized and attracts its armature, to which bar is attached, thus drawing it to the right A mechanical locking arrangement associated with the sliding bars serves to hold the bars in their right-hand positions after the momentary impulse through the magnets 4 to 8 has drawn them to the right

Depression of a key or keyboard 1, for instance key "3", will close a circuit as follows: from power source 33 along conductors 46, 47, closed contact at key "3", conductor 48 to contact 19 of the first connection-changer assembly 9. All the bars of the connection-changer assemblies except bar 23 of assembly 12 are in their left-hand or unactuated positions. Hence, the current continues as follows: from contact 19 through contact spring 15, contact 20, conductor 49, contact 50, contact spring 51, contact 52, conductor 53, contact 54, contact spring 55, contact 56, conductor 57, contact 58, contact spring 59. Bar 23 being in its right-hand position, the current continues as follows: contact spring 59, contact 60, conductor 61, contact 62, contact spring 63, contact 64, conductor 65, contact 66, conductor 67, through indicator lamp or magnet "7", conductor 68, back to power source 38. Thus depression of key "3" yields cipher resultant "7". As soon as this result has been noted down or recorded and the key "3" on the keyboard is released, the first action of the releasing mechanism actuated by the back stroke of this key is to close a contact 69 which operates magnet 70, to release the locking bar 71, which in turn allows the sliding bar 28 to return to its left-hand position under the action of its coiled spring 72. At the end of the back stroke of key "3", contact 3 is closed, which through power source 37, conductors 73 and 74 allows the tape-stepping magnet 36 to function. This causes the tape to move to the next ciphering character, which brings the slidable bars 14, 26, 27, 28, 29 into their next ciphering position and completes the cycle of events.

The connections between the contacts of the keyboard 1 and the first assembly, 9, are made by means of a plug and jack arrangement which permits of varying the connections at will, in accordance with a change in key. A similar arrangement may, of course, be made for the connections between the row of contacts, 75, immediately beyond the final assembly, 13, and the recording and indicating device 2.

For decipherment it is necessary to reverse the positions of keyboard and indicating device relative to the assemblies 9 to 13, but since means of accomplishing this are well known in the art and do not form a part of my invention, these means are not shown here.

An alternative scheme for effecting the variable paths between the keyboard, 1, and the indicating device, 2, is shown in Figure 2. In this figure, the structure shown is one of four other and similar assemblies to replace the assemblies 9 to 13 of Figure 1. Instead of a bar carrying contact springs, such as bar 14 of Figure 1, the assembly in Figure 2, consists of a holder, 1, in which can be inserted a removable connector plate, 2, carrying two sets of spring contacts, 3 and 3'. The spring contacts are arranged in opposite sets, and are interconnected at random by means of the insulated conductors, 4, as shown. The connector-plate, 2, may consist of any number of contact springs arranged in opposite pairs, and it is constructed in such a manner that it can be inserted in the holder in [redacted] a number of possible positions depending upon the number of pairs of contact springs. For example, if the

connector-plate consists of fourteen contact springs on each side, then it can be inserted on the carrying holder 1 in five different positions, each giving different paths for the passage of currents from the set of lower fixed contacts, 5, to the set of upper fixed contacts, 5'. In such a case the only limiting factor imposed upon the randomized interconnections between the sets of contact springs 3 and 3' is that the insulated conductors, 4, must be so arranged that in each of the five possible positions of the connector plate 2 there will always be a full complement of conductors for continuing a current from the fixed contacts 5 to the fixed contacts 5'. Such an arrangement is depicted in Figure 2, wherein it is noted that of the set of fourteen contact springs, 3, four of these springs have two conductors each, which lead to separate contact springs of the set 3', four of these springs have two conductors each, which lead to separate contact springs of the set 3. The particular four contact springs of set 3, which will have two conductors instead of one leading away from them are determined by the random initial connections established when the connector plate 2 is set into its successive positions, and it will be noted that the two terminals of the double conductors leading away from spring contact 6, for example, end up at spring contacts 10 and 11, which are ten places removed from each other. The same is true of the members of the respective pairs of terminals leading away from spring contacts 7, 8 and 9; they lead to contacts separated by ten places from each other.

The holder, 1, in which the connector plate 2 is inserted is attached to a bar, 14, which is equivalent in function with bar 14 of Figure 1; it is brought to the right, when the magnet 12 associated with it is energised, so that each contact spring makes contact with the next fixed contact to the right For example, spring contact, 3, resting on fixed contact 15 as shown in Figure 2 would, upon bar 14 being drawn to the right, rest on fixed contact 16 The same would be true of all the other spring contacts. Therefore, for each positi n of the connector-plate 2 on the holder, 1, there will be two separate paths established for the passage of a current from one of the fixed contacts of the set 5 to one of the fixed contacts of the opposite set 5', depending upon whether bar 14 is drawn to the right under the action of magnet 12 or remains in its left-hand position under the action of retractile spring 13

The assembly shown in Figure 2 is, as stated above, similar in function to assembly 9 of Figure 1. I is merely necessary to connect the set of fixed contacts 5' to the set of contacts 5 belonging to the next assembly These connections may be direct, or in a random manner by means of removable connector plates with variable conductors, such as those indicated in Figure 1, so that the connections between one assembly and the next may be changed at will

If removable connector plates are employed, additional secrecy is afforded, since by a change in arrangement of these plates the same keying tape will produce widely different cipher results.

3rd Draft

This invention relates to cryptographs and has as its object the provision of means for automatically, continuously, and aperiodically changing the cipher equivalents representing plain-text characters of a message

The invention is explained in connection with the accompanying drawing, Figure 1, which is merely diagrammatic. In this figure, I treat the invention as applied to a system for enciphering a set of but ten elements, as for example, the ten digits, but my invention is not limited to this number of elements and can be applied to the encipherment of as large a set of elements as is comprised in the transmission of any kind of intelligence conveyed by written symbols

In Figure 1, there is shown a keyboard, 1, comprising ten contact-closing keys arranged as in the keyboard of a modern ten-key adding machine; 2 is a recording or indicating device which may take the form of a set of magnets of a printing mechanism or a bank of glow lamps to indicate by illumination of superimposed symbols the equivalents resulting from encipherment; 3 is a tape transmitter of the usual type employed in automatic telegraphy based upon the Baudot code, which transmitter, under guidance of a perforated tape, controls the permutative operation of the set of magnets 4, 5, 6, 7, and 8; the assemblies labeled 9, 10, 11, 12, 13 are switching devices, to be explained in detail below, for varying the paths for the passage of an electric current from the keyboard 1 to the indicating device 2.

Taking up one of the switching devices referred to above, for example, th one labeled 9, this is composed of two fixed bars 16 and 17, a slidabl bar 14, an electromagnet 8, and a removable connector plate 21 The bar, 14, slides between the two fixed bars, 16 and 17, the former of which carries ten contact surfaces insulated from one another, the latter, twenty contact surfaces arranged in ten pairs all insulated from one another Slidable bar 14 carries ten contact-making elements or springs insulated from one another and suitable for establishing connections between the contacts on fixed bar 16 and those on the opposite fixed bar 17 One of these springs is labeled 15 When bar 14 is in its normal position, held so by retractile spring, 18, the contact springs on it establish connections between the contacts on fixed bar 16 and the left-hand members of the paired contacts on fixed bar 17, when bar 14 is drawn to the right, under the action of magnet 8, then its contact springs establish connections between the contacts on fixed bar 16 and the right-hand members of the paired contacts on fixed bar 17 Thus, one of two alternative sets of ten electrical paths between the contacts on bar 16 and those on bar 17, depending upon the action of magnet 8 can be established For example, when bar 14 is in its normal or retracted position, under the action of coiled spring 18, a current entering switching device 9 at contact 19 would continue along contact spring 15 and emerge at contact 20 on fixed bar 17; but when bar 14 is drawn to the right under the

action of magnet 8, then the current would emerge at contact 26 of fixed bar 17

The connector plate 21 consists of one set of twenty insulated ball-bearing, spring contacts on the lower face which is juxtaposed against the contacts on fixed bar 17, and nother set of ten similar contacts on the other face, which is juxtaposed against the lower fixed bar of the next switching device, 10 The twenty contact of the one face are connected by insulated conductors to the ten contacts of the other face of the connector plate 21, each of the ten latter contacts being connected to two of the former contacts, in a random arrangement which can be varied at will The plates 22, 23, 24, and 25 are similar in structure to plate 21, but the connections established by their internal conductors are different; the plates are interchangeable

The magnets 4 to are, as noted above, under control of the tape transmitter 3, through which is passed a perforated tape bearing holes corresponding to characters in the Baudot code This tape comprises a cipher key to control the neiphermen Every time a key of the keyboard 1 is depressed, upon its release or back stroke, a contact 30, operated by a universal bar not shown in the figure, is closed This contact controls the tape-stepping magnet 36, power for which is supplied by source 37 Thus, with each depression of the key the tape is stepped forward to the next position, bringing a new ciphering character into action; these characters form an entirely arbitrary, unintelligible sequence of ciphering elements for controlling the permutative operation

of the magnets 4 to 8, and thus of the slidable bars of the switching devices 9 to 13 Since the switching devices are in series, the electrical arrangement is such that a current established by depressing a key of the keyboard 1 must traverse the entire set of switching devices 9 to 13 before reaching the indicating device 2; consequently, it will be seen that the final cipher resultant of a character on the keyboard depends upon the permutative operation of the set of five slidable bars 24, 26, 27, 28, 29. And since this permutative operation is controlled by the transmitter 3, which in turn is controlled by the perforated tape, the cipher resultants will vary with the sequence of ciphering characters on the perforated tape Since this sequence of ciphering characters is a random, unintelligible series of characters, the cipher resultants are entirely arbitrary and show no periodicity in the relationship between plain-text character and cipher equivalent Tape transmitter 3 employs only one of the usual two sets of contacts, only the front set in this case, so that contact is made and a circuit established through one of the magnets 4 to 8 when the proper pin passes through a corresponding hole in the tape

A particular encipherment operation will now be set forth in detail Let us assume that a key of the keyboard has been depressed and released so that on its backstroke the universal bar closed the contact 30, which operated magnet 36, thus bringing into play the next ciphering character on the tape

Suppose this character is represented in Baudot code by - ∔ - - -, which in this case means that the tape has a hole in the second position, the other four positions being unperforated. Then the second pin in the tape transmitter 3, passing through this hole in the tape, cause contact 32 to close, the other four contacts in transmitter 3 remaining open A current from power source 39 flows along conductor 40, closed contact 32, conductor 41, through magnet 5, conductors 42 and 43, back to power source 39 Magnet 5 is energized and attracts its armature, to which slidable bar 28 is attached, thus drawing it to the right, as shown in the figure. A locking bar 71, associated with sliding bar 28 serves to hold this bar in its right-hand position after the momentary impulse through magnet 5 has drawn it to the right Slidable bar 28 will stay in this locked position until bar 71 is withdrawn, as explained subsequently

Depression of a key on keyboard 1, for instance key "9", will close a circuit as follows: from power source 38 along conductors 46, 47, closed contact at key "9", conductor 48 to contact 19 of the first switching device 9 All the bars of the switching devices 9 to 13, except bar 28 of 12 are in their left-hand or unactuated positions Hence, the current continues as follows: from contact 19 through contact spring 15, contact 20, conductor 49 of connector plate 21; contact 50, contact spring 51, contact 52, and conductor 53, of switching device 10; contact 54, contact spring 55, contact 56, and

conductor 57 of switching device 11; contact 58, contact spring 59 of bar 23 of switching device 12. Bar 23 being in its right-hand position, the current continues as follows: contact spring 59, contact 60, and conductor 61, of switching device 12; contact 62, contact spring 63, contact 64, and conductor 65 of switching device 13; contact 66 of final fixed bar 75, conductor 67, through indicator lamp or magnet "7", conductor 68, back to power source 38 Thus depression of key "9" yields cipher resultant "7" As soon as this result has been noted down or recorded and the key "9" on the keyboard is released, the first action of the releasing mechanism actuated by the back stroke of this key is to close a contact 69 which operates magnet 70, to release the locking bar 71, which in turn allows the sliding bar 28 to return to its left-hand position under the action of its coiled spring 72 At the end of the back stroke of key "9", contact 30 is closed, which through power source 37, conductors 73 and 74 allows the tape-stepping magnet 36 to function. This causes the tape to move to the next ciphering character, which brings the slidable bars of switching devices 9 to 13 into their next ciphering position and completes the cycle of events

The connections between the contacts of the keyboard 1 and the first switching device 9, are made by means of a plug and jack arrangement which permits of varying the connections at will, in accordance with a change in key as previously determined by the correspondents A similar arrangement may,

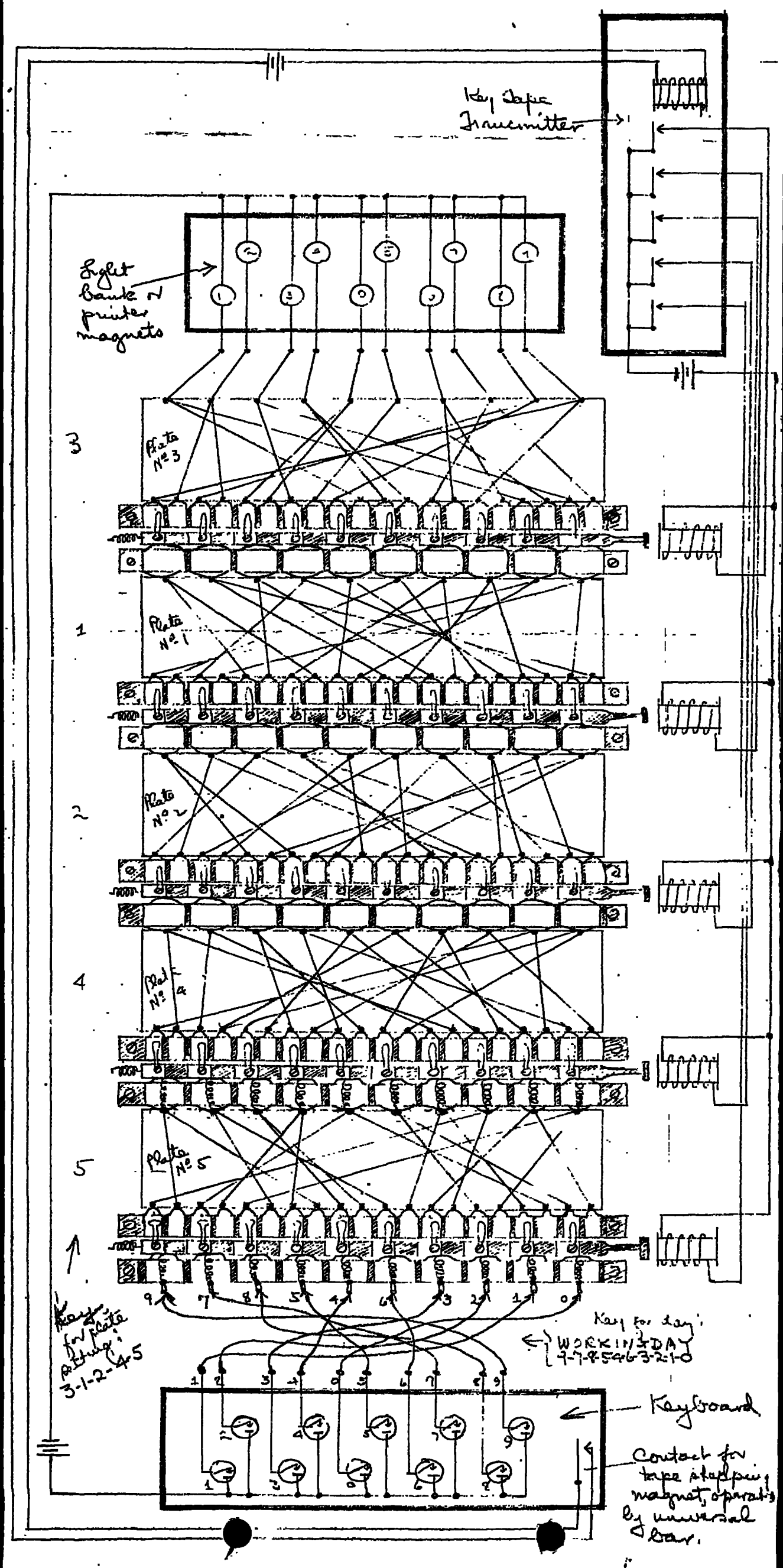
of course, be made for the connections between the row of contacts on final fixed bar 75, immediately beyond the final switching device 13, and the recording and indicating device 2

For decipherment it is necessary to reverse the positions of keyboard and indicating device relative to the set of switching devices 9 to 13, but since means of accomplishing this are well known in the art and do not form a part of my invention, these means are not shown here

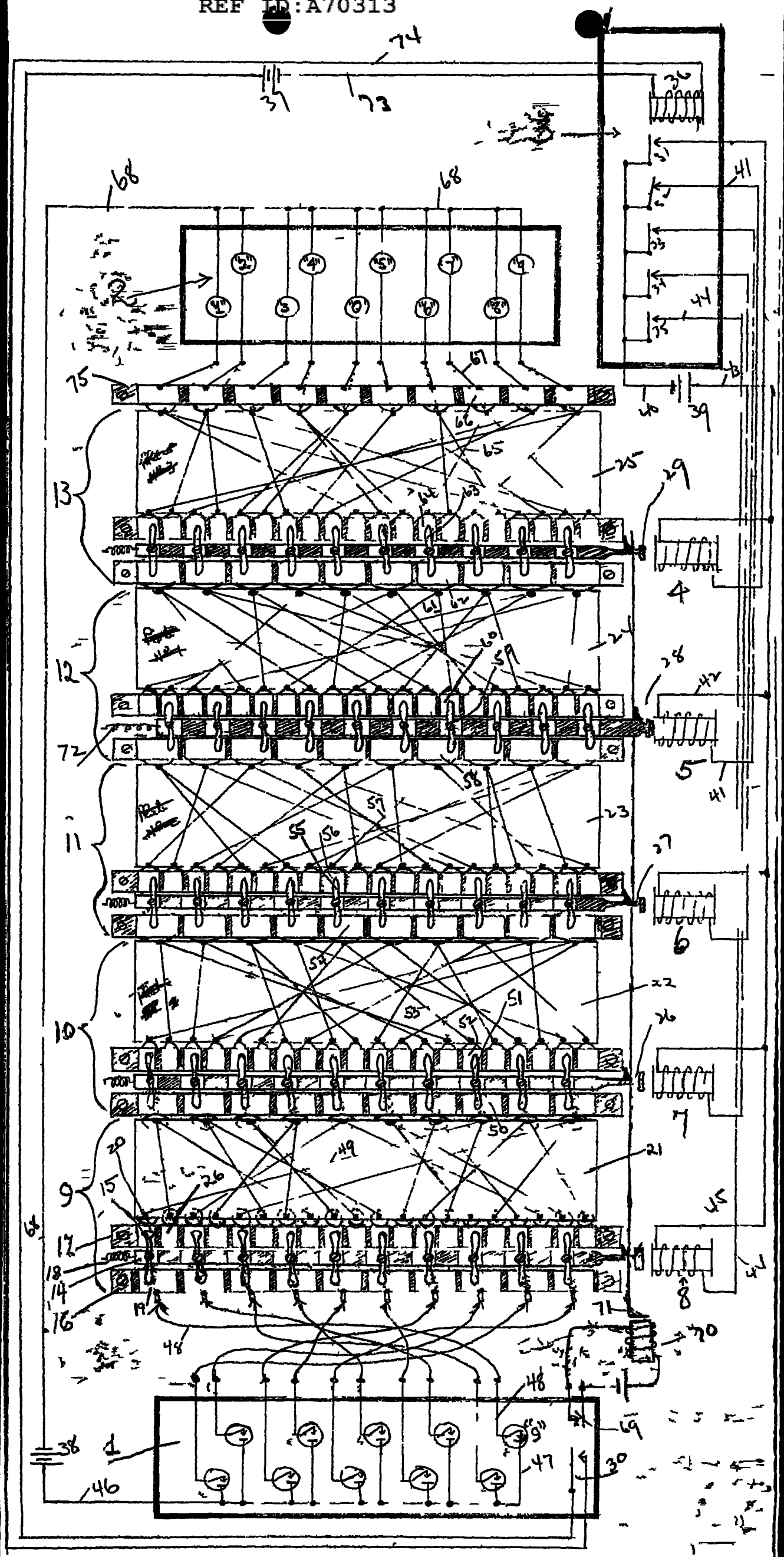
Disclosed to ~~writer~~
April 30, 1932 at Washington D.C.

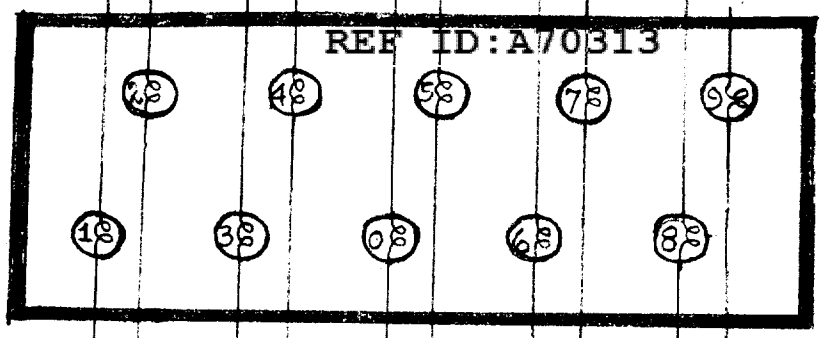
Inventor:
William F. Friedman,
O.C. Sig. O.
Washington, April 30, 1932

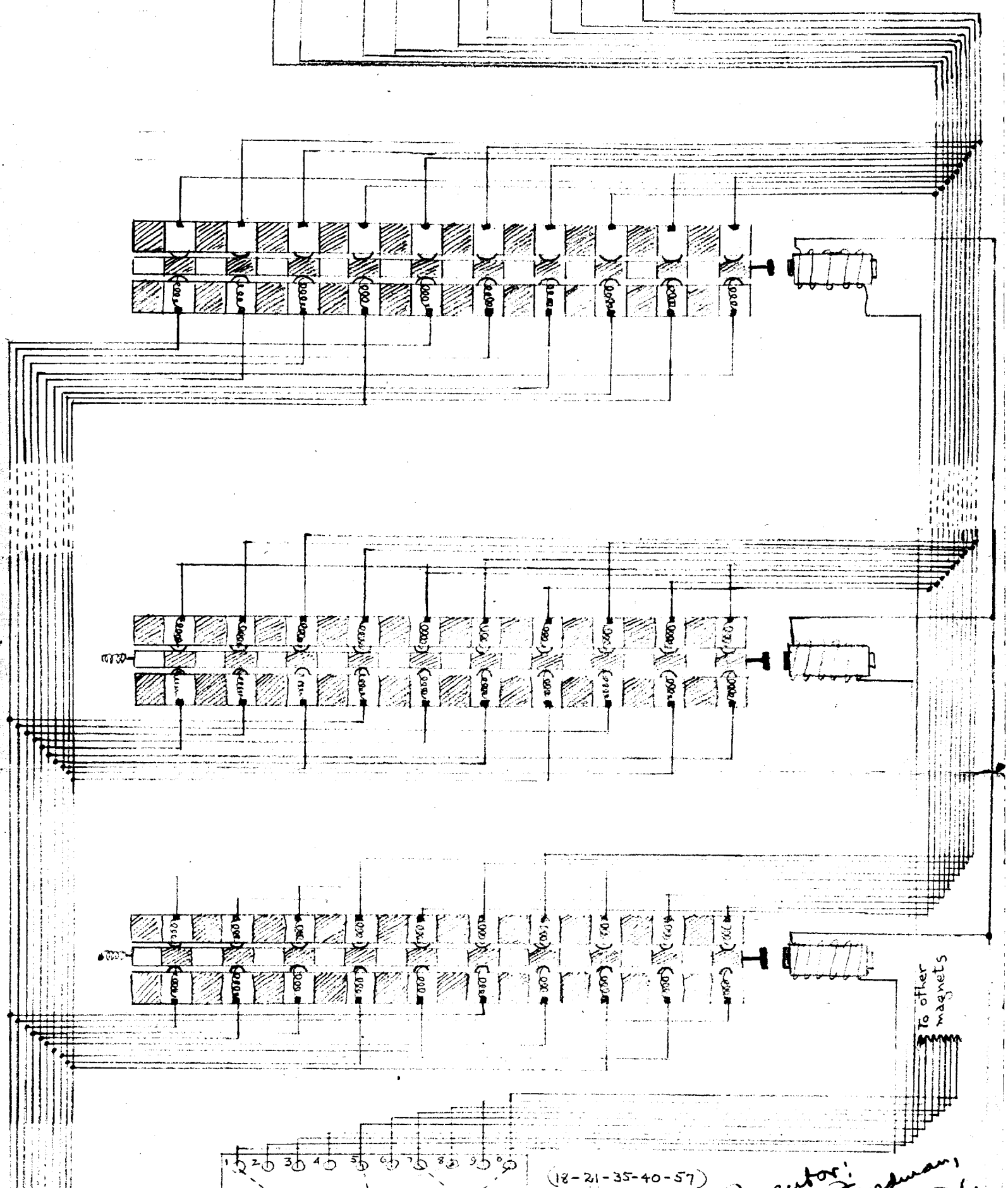
Solomon Kullback 1900 F St NW Wash. D.C.
Mark Kroak % Adjutant General
Abraham Sinkov 1412 Chapin St Wash DC
Frank B. Rowlett 3121 New York Ave, NE Wash D.C.

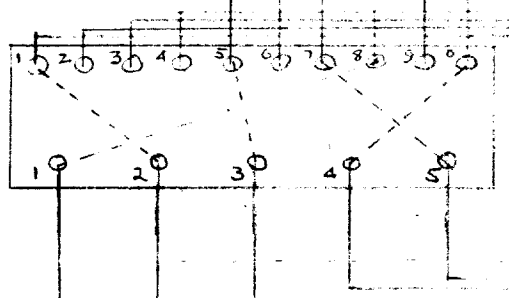


REF ID:A70313









Inventor:
William F. Friedman,
O.C. Sig. O.
Washington, D.C.
April 30, 1932

Disclosed to us at Washington, D.C. on April 30, 1932:

Solomon Fullback 1900 F St. NW Wash DC
Mark Woods c/o Adjutant General
Abraham Sinkov 1412 Chapin St. Wash DC
Robert Blowett 212 New York Ave. NW. Wash. D.C.