

The Friedman Authentograph

General description

1. The object of the Friedman Authentograph is to provide an absolutely safe, foolproof, simple, and practical machine for protecting a bank against fraud or error in the transfer of funds by telegraph, cable, or radio. It will afford a check upon the authenticity of the message, the name of the payee, the amount to be paid, the date of the transfer, and any other additional data as may be desirable to include to meet special circumstances.

2. In certain respects the machine is a modified cryptographic device, operated by depressing the keys of a keyboard very similar to that of a modern, 10-key adding machine. It produces a 3-letter or a 3-figure code group representing the cumulative value of the automatically enciphered text data. A 2-letter or a 2-figure group, derived as stated below, is added to complete the test, making it a 5-letter or a 5-figure code group, chargeable as one word. For the sake of simplicity of description, in what follows it will be assumed that the machine is designed to produce a 3-letter group.

3. The basic principles of operation and control are as follows:

a. At the commencement of each business day the machine is "set up" according to a secret combination, hereinafter called the "key". This is to be done only by properly authorized officers of the bank, who are specifically designated for this duty in rotation, as is the case in connection with the daily opening of the bank's vault. The keying mechanism is covered and protected by lock and key, and can be opened only by the officer provided with the proper passkey.

b. It is estimated that the time required to set the machine to the daily key will not exceed 2 minutes per machine.

c. All machines throughout the world can be set up according to the same key. However, different keys may be set up on different machines intended for testing messages exchanged between members of different groups of corresponding banks. Thus, group A may use one key, group B another key. A member of group A corresponding with a member of group B would use a third key, and so on.

d. Each test is made in connection with a punched card bearing perforations which specifically control the results produced by the machine under the general control of the daily key. These cards will hereinafter be called test cards. They are very much like the punched cards used in Hollerith tabulating machines and may be of a good grade or of very thin metal.

g. For each correspondent bank there is provided a set of test cards for outgoing payments and a set for incoming payments. Each card carries an identifying 2-letter group; it also shows the name of the correspondent bank and such other identifying data as may be necessary. Each set consists of as many cards as may be required to cover the usual number of transfers to or from that bank per day, week or month of normal business, according to pre-arrangement.

f. These cards are filed in sets in a filing cabinet and are readily accessible for instant use. A supervisor is in charge of the cabinet. The cards of each set are seldom disturbed in their serial order, so that the members of each pair of correspondent banks are always "in step", card for card and payment for payment, as will be explained below.

Operating the machine

4. a. When the test clerk has to prepare a test for an out-payment, he is given a test card by the supervisor, who takes it from the set of out-payment test cards for the correspondent bank. The very first or top card in the set is the one taken. Suppose it to be the 47th card in that set, and suppose it carries as its identifying symbol the 2-letter group BU.

b. The test clerk places this card in a slot in the machine, closes a switch, and depresses the keys of the keyboard to correspond with the test data. Assume that the data consist of the full name of the beneficiary, the designation of monetary unit (dollars, francs, etc.), and the amount of the payment. Each key of the keyboard, besides bearing a designating number, bears three letters of the alphabet (except the zero key, which has no letters, and the "9" key, which has two letters). The test clerk depresses the keys corresponding to the letters of the name and the amount. It is estimated that this operation will require on the average at most 60 seconds for a name of 15 letters and an amount running into 6 figures. The machine shows on an indicator the cumulative value of the automatically enciphered test data. As stated in par. 2 this may consist of a 3-letter or a 3-figure group. Assuming that the machine produces letter groups, and that the test produced in this case is the group "PRI," the clerk adds as a prefix the 2-letter group "BU" applying to the test card used, making the 5-letter code group BUPRI. This group he writes on the message (or the machine may print the test group directly in the message).

c. The test clerk now opens the switch, the test card is ejected and the clerk returns the ejected card to the supervisor, who places it at the bottom (or back) of the set of test cards from which he originally took the card and to which it belongs. The supervisor also takes the message and passes it on for transmission.

d. Suppose the very next payment is to the same bank for the account of the same beneficiary and in the same amount as before. The supervisor now selects the very next test card in the same series, which

is the 48th card, bearing the identifying symbol BV, and hands it to the test clerk, who goes through the same operation as before. The test word in this case will be entirely different, although the operation is exactly as before, because the BV test card is entirely different from the BU card. The test in this case might be the group BVEPO.

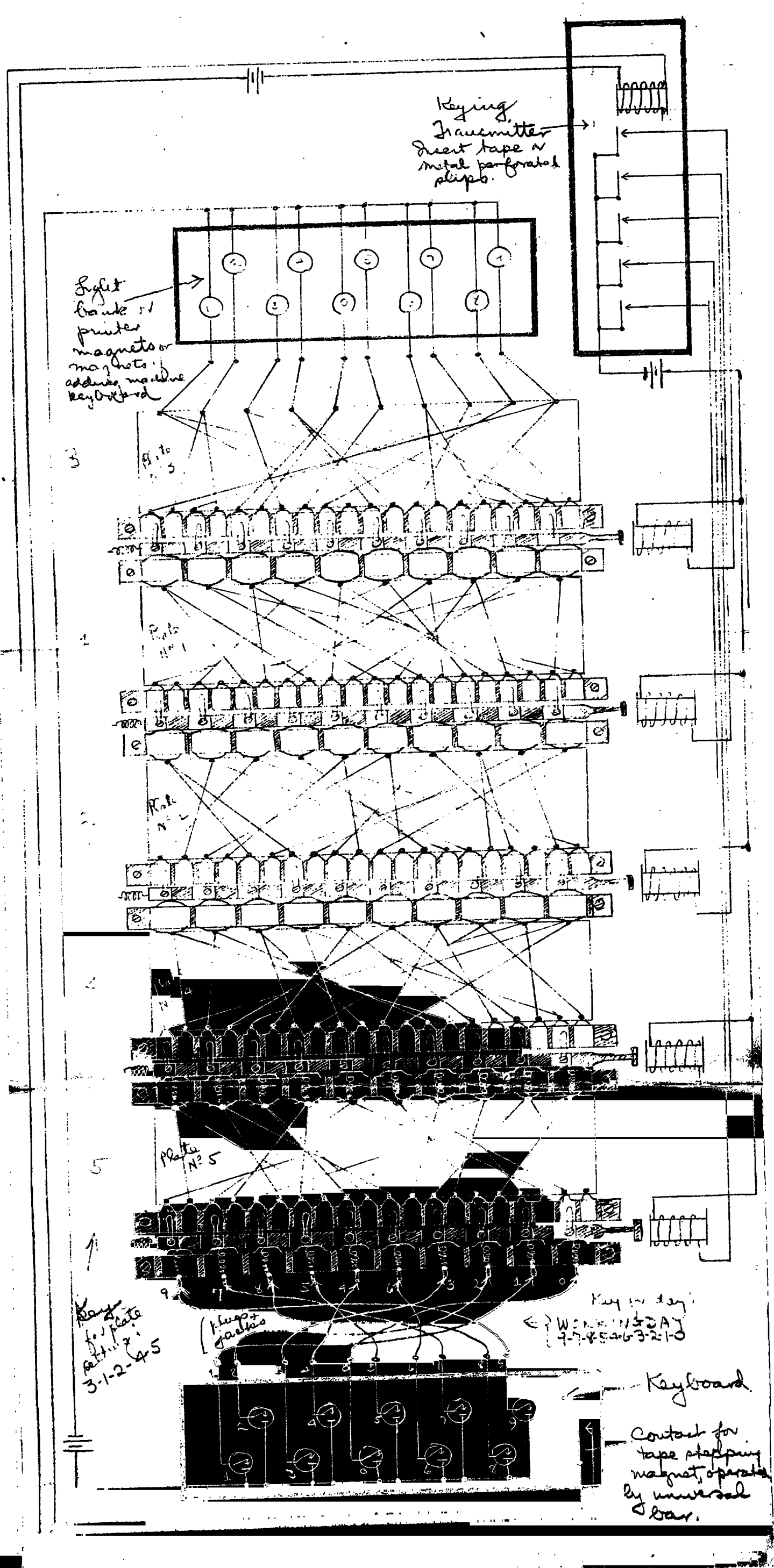
g. On a different day, the test for the same bank, beneficiary, and amount would be entirely different, since the daily change in set up of the key provides for this difference. For example, suppose the BU card were employed to test exactly the same data as before; since the key to which the machine is set is different now, the test might be BURON. Thus, the test automatically carries an authenticator for the date of payment.

h. In the case of an incoming transfer the procedure is exactly the same, except that the supervisor must select the proper test card (in correct serial order) from the set of test cards applicable to incoming messages from the correspondent bank. The test group the test clerk obtains must check with the one indicated in the message. If it does not check, it is proof that either an error was made in the preparation, transmission, or reception of the message, or that the message is not a bonafide or valid message from the bank from which it purports to come.

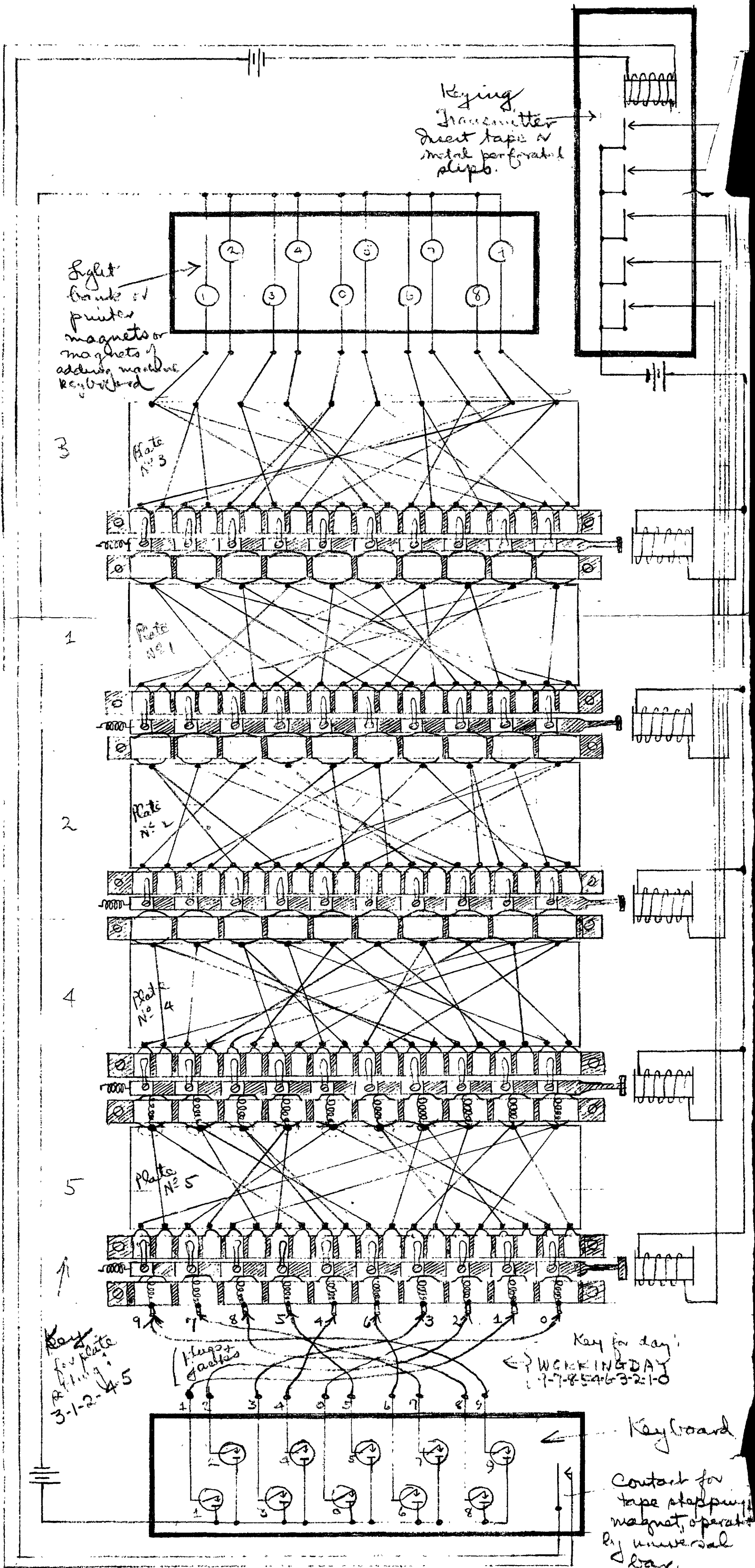
5. Preparation, distribution, and accounting for test cards can be accomplished from the head office of the group of corresponding banks. Simple apparatus for the production of the test cards is now available in the form of standard equipment used in tabulating machinery. Similarly, preparation and distribution of the daily keys can be accomplished from the head office; annual or semiannual distribution of keys will probably be sufficient.

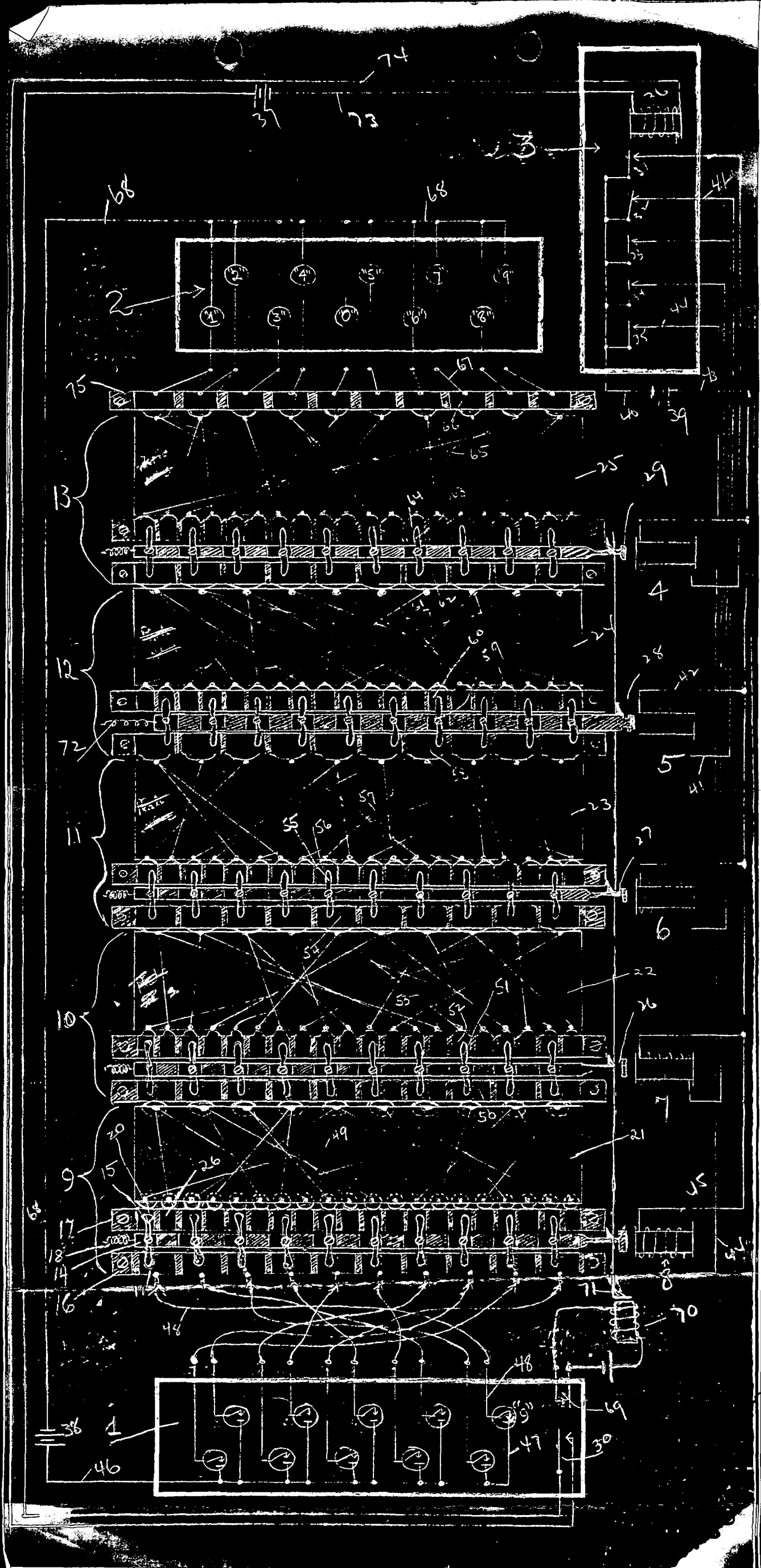
June 25, 1935.

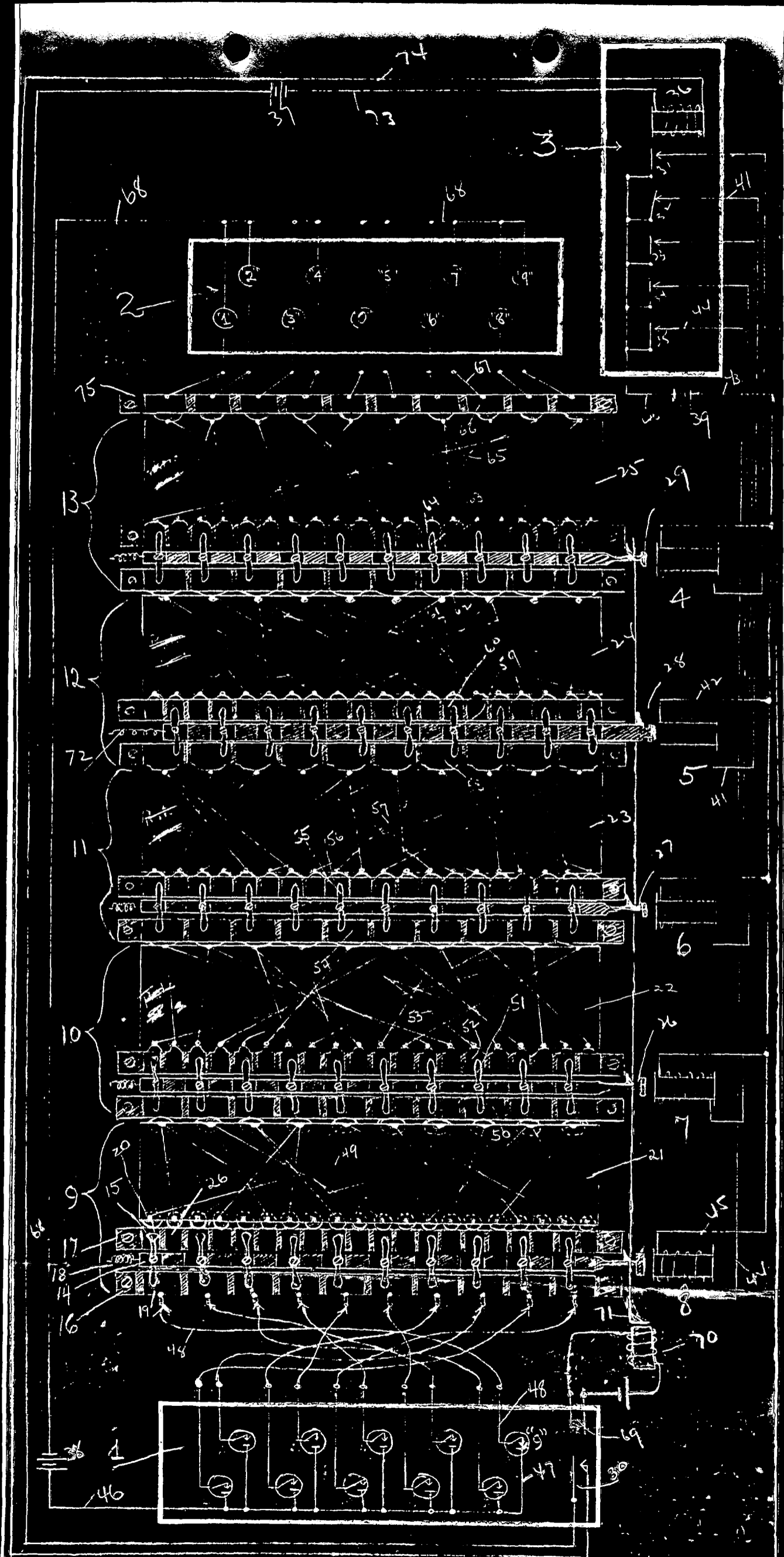
REF ID: A39421
 Washington, April 30, 1932
 Solomon Fullback 1900 F St NW Wash. D.C.
 Mark L. Board 70 Adjutant General
 Abraham Sinkov 1412 Chapin St Wash DC
 Frank B. Rowlett 21st Rowlett Ave Wash. D.C.

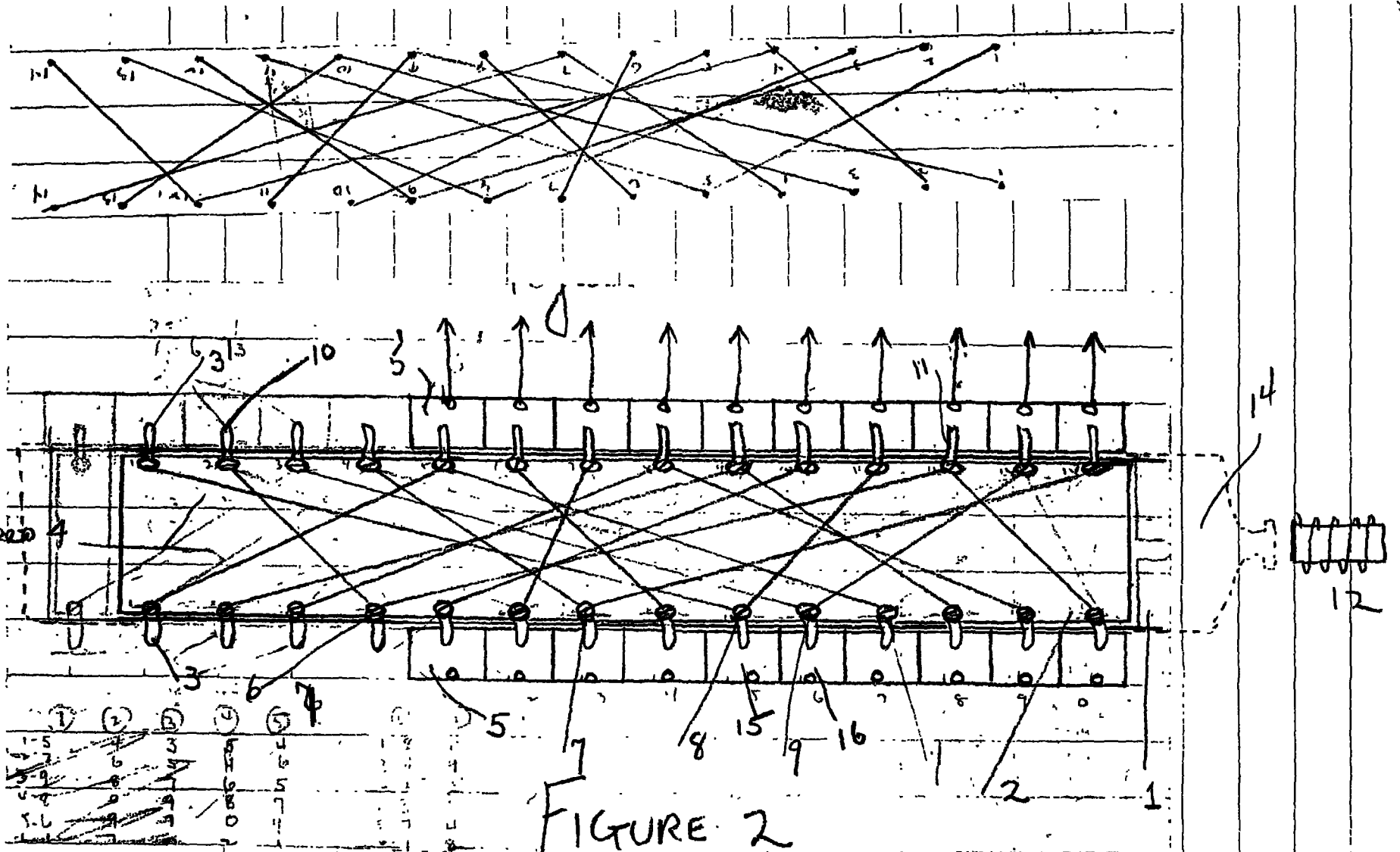


Abraham Sinkov 1412 Chapin St Wash DC
Frank B Rowlett 2121 New York Ave, N.W. Wash. D.C.









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

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

Simon F. Fuback 1900 F & N W Wash D.C.
Mark H. Good 70 Adjutant General
Abraham Sinkov 1412 Chapin St Wash DC
Frank B. Rowlett 2111 P St N.W. Wash D.C.

