Authenticating Device

1. Reference is made to my previous invention of a "Message Authenticating System" covered by U. S. Patent No. 2,080,416, issued 18 May 1937. Said patent was processed through the Signal Corps and the invention described therein may be manufactured and used by or for the Government for governmental purposes, without the payment to me of any royalty thereon.

2. The present invention has a similar purpose but accomplishes it in a simpler way, which will be briefly described in the succeeding paragraphs, in connection with Fig. 1.

3. A series of 10-point cipher rotors, 1, of the type commonly employed for cryptographic purposes, are assembled "in cascade" upon a shaft, 2, in some key order. The internal wirings of the rotors are all different and each rotor carries an identifying symbol. A complete circuit through the set of rotors traverses a path which is determined by the specific order in which the rotors are arranged on the shaft, the specific rotatory positions in which the rotors are placed, and the wiring of the rotors. The left-hand stator, 3, has ten input contacts, 4, six of which are connected by plugs and jacks to the six contacts arranged in an arc on insulator strip, 5. A contact lever arm, 6, pivoted at 7, serves to establish contact from battery, 8, to one of the six contacts, 9, on the strip, 5, and thence into one of the input contacts, 4, of the stator, 3. The current thereupon traverses the rotors, emerges at one of the ten contacts, 10, of the right-hand stator, 11, and thence returns to battery, 8, through one of ten indicating lamps, 12. The specific lamp which will be illuminated will be determined by the rotor setting and the particular contact made at the contact strip, 5. Thus, as lever 6 is moved to one of the contact positions, a certain lamp will be illuminated momentarily; another lamp will be illuminated as lever 6 is moved to another contact position, and so on. Thus, moving lever 6 through its three top positions successively will cause three lamps to be lighted successively. A removal cardboard strip, 13, in the card-holder, 14, serves to identify the lamps and represents another variable element in the keying system. Thus, with a given key and a specific strip 13, moving the lever 6 through the three upper positions will cause three lamps to be lighted, giving a number such as 759, for example. Moving the lever 6 through the three lower positions will yield a different 3-digit number, for example 63Ø. A connection-changing plugboard may be inserted between the right-hand stator, 11, and the bank of indicating lamps, this serving to take the place of the variable cardboard strip 13, or as an additional variant in the system.

4. The method of using the device as an authenticating means is as follows. It is the usual current practice first to encode the telegram in the Bank's private code or else in

W. F. F. 8 June 44
WF 10 June 44
LR 10 June

Sal C

some other suitable code. The test group is then composed, based upon certain test elements in the telegram, as arranged by preagreement among the banks concerned. The test group is usually a numerical group of two or three digits, which group is then looked up in the code and its letter group equivalent is set down as the final group of the message. All the foregoing procedure remains unchanged in practicing my invention except that the composition of the numerical test group is accomplished by the machine discussed herein. This part of the operation will now be described. Having the machine at hand, the daily key is set up, consisting of the specific order in which the rotors are assembled on the shaft. The first two rotors are set to the serial number of the message; the next rotor is set to indicate what currency is involved (dollars, pounds, etc.); the next six rotors are set to correspond with the amount of money to be checked or authenticated, six rotors providing for all amounts from 1 to 999,999. Fig. 1 shows the rotors set to message serial number 35, and to the quantity, U. S. $9,756,125. (Additional rotors may be provided to take care of other test elements, such as the initial letter or letters of the name of the beneficiary of the transfer.) If the telegram transferring $9,756,125 is going from New York to London, for example, then the switch lever 6 may be moved, by preagreement, through the upper three positions successively, yielding, for example, the authenticating group 759; if the telegram is going from London to New York, the switch lever 6 may be moved through the lower three positions yielding, for example, the group 63Ø. Thus the authenticating group is different, depending upon the message serial number, the currency, the amount involved, and the direction of the transfer. On each day, since a different permutation of rotors, a different plugging arrangement at the left-hand stator, and a different card can be employed, the test number would be different. The test number would then be encoded as usual, by reference to the codebook employed. The number 759 might be represented by the code word ROXIP; 63Ø by PILYD.

5. No means are shown in Fig. 1 for automatically angularly displacing the rotors during a single test but the addition of such means is within the scope and forms a part of the invention.

6. The bank receiving the telegram after the usual decoding of the code message, notes the test data and the test group contained therein. It then sets up its plugs, card strip, and rotors according to the daily key and then aligns the rotors to correspond to the test data carried by the telegram. Upon operating the lever 6 it will obtain exactly the same test number which is conveyed by the telegram itself, thus attesting to the authenticity of the transfer as well as to the accuracy of the

W. F. F. 8 June 44
WK 10 June 44
LK - 10 June 44

amount, insofar as the latter is possible, considering that 10 x 9 x 8 or 720 different test groups is the maximum number obtainable from one key setting of the rotors and there are 10 million amounts which can be set up. This, however, is a feature which is unavoidable, is common to all testing systems of this nature, and does not vitiate the system to any serious degree.

* * * * *

I believe that I am the inventor of the device disclosed in the foregoing sheets.

8 June 1944.

William F. Friedman.

* * * * *

I have read and understand the above disclosure.

10 June 1944
(Date)

Mark Cloud
Arlington Hall Station, Arlington Va

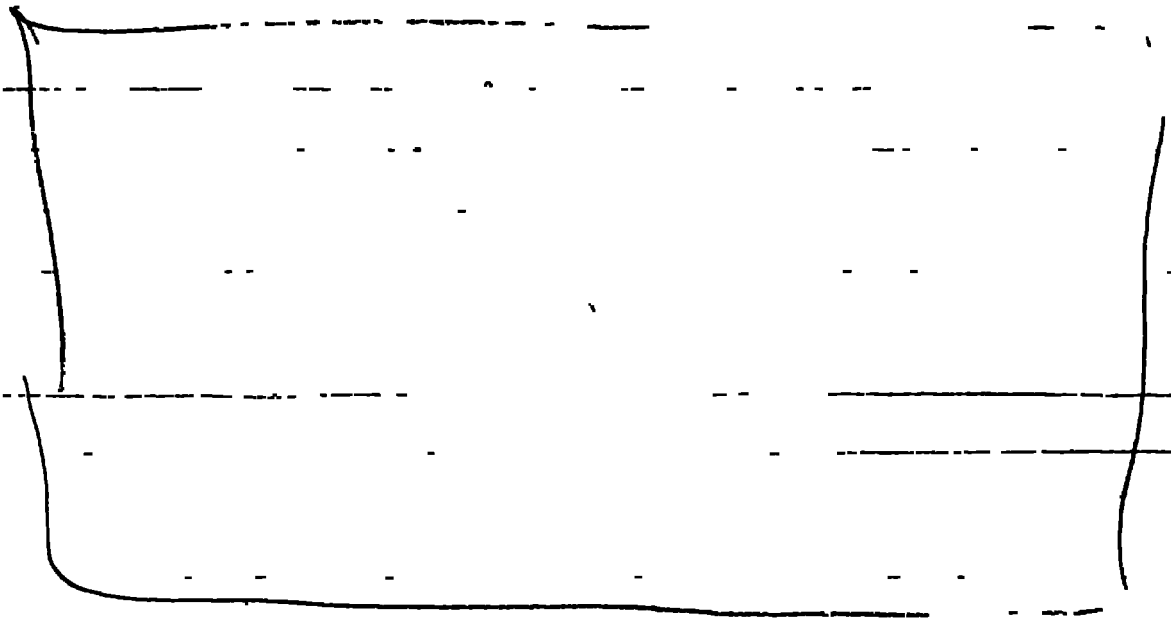
10 June 1944
(Date)

Lev Rosen
2819-12 St So
Arlington Va

CONFIDENTIAL

REF ID:A67673

Authenticating Device



Date of conception:

Disclosed to us:

Inventor

William F. Friedman

Leo Rosen
Major, Sig. C.
Arlington Hall Station

Mark Rhoads