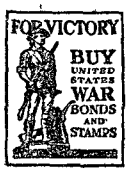



~~CONFIDENTIAL~~

HEADQUARTERS, ARMY SERVICE FORCES SPSIS-3

OFFICE OF THE CHIEF SIGNAL OFFICER

WASHINGTON 25, D. C.

8 June 1944.

MEMORANDUM for ~~Signal Corps Patents Board.~~ Legal Division, OCSigO
(Thru Channels)

Subject: Invention of Authenticating Device for Commercial Usage.

1. A number of years ago I invented a message authenticating system, which was formally processed through the then existing Patents Section of the Research and Development Division, OCSigO. (Tab A shows the papers in the case.) The invention was covered in U. S. Patent No. 2,080,416, dated May 18, 1937, and the apparatus described therein may be manufactured and used by or for the Government for governmental purposes without the payment to me of any royalty thereon. (Tab B is a copy of the patent.) The invention has thus far not been reduced to practice because of its complexity.

2. I have recently conceived of a modification and simplification of the authentication device covered in the above-mentioned U. S. Patent No. 2,080,416, the same being briefly described in the accompanying sketch and general specifications (Tab C). It is requested that the usual forms be supplied me for purposes of recording the date of conception, etc.

3. Primarily, this invention, as was the previous one, is intended for use by banks in authenticating messages involving the transfer of money from one bank to another. However, it may have military applicability in connection with the authentication of messages and it may be desirable for the Government to acquire rights similar to those pertaining to U. S. Patent No. 2,080,416. However, permission is requested to allow me to construct a model at my own expense and to prosecute the present invention for commercial usage, at my own expense, immediately upon the termination of the present war.

William F. Friedman,
Director of Communications
Research.

Inclosures:
Tabs A, B, and C.

~~CONFIDENTIAL~~

WAR DEPARTMENT
Office of the Chief Signal Officer
Washington

April 19, 1935

MEMORANDUM FOR: Major Akin.

1. Under date of November 15, 1933, I forwarded a memorandum, drawing, and draft specifications covering a cipher device on which I desired a patent application be drawn. The papers are attached hereto.

2. This device presents excellent possibilities for a commercial device for banking purposes in connection with authentication of money transfers by cable. An opportunity has recently presented itself for disposing of my commercial rights to this invention, the government retaining license and shop rights as usual.

3. It is requested that permission be granted to enter into negotiations with a prospective purchaser of these commercial rights.

/s/ William F. Friedman
William F. Friedman.

Attached:
File on case.

C
O
P
Y

Jak A

# 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 630. 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



2ahC

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

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.

_____ _____
(Date)

_____ _____
(Date)

1st Memo Ind. 8

War Plans & Training Division, April 20, 1935. To: Research and Development Division.

Approval recommended provided it is understood that should the letters patent be granted the government will be able to obtain any and all machines desired without the payment of royalty.

/s/ S. B. Akin
S. B. Akin,
Major, Signal Corps.

Incl.
1 Incl. added - Memo. from Mr. Friedman to Major Akin, 11/15/33.

2d Memo. Ind. 10

Research & Development Division, OCSigO, May 2, 1935. To: War Plans & Training Division.

1. Where an invention is originated by an employee of the Government, as in this case, the Government acquires the usual license rights irrespective of whether he negotiates the sale of his commercial rights either before or after the filing of a formal patent application and the purchaser of such rights takes title subject to an irrevocable, non-exclusive license to the Government, which license should be executed at the time the formal patent application is executed.

2. The following procedure is recommended:

a That the patent application be filed thru the Patent Section of the Signal Corps and that attorneys representing the Government be made attorneys of record in the original application, but that patent counsel for the purchaser of the commercial rights prepare the specification, claims and drawings for the application. Handled in this way, the case would come under the Act of 1883 as amended and the payment of a filing fee would be waived.

3. Upon the actual filing of the application in the Patent Office, andassociate power of attorney would be given to patent counsel representing the purchaser of commercial rights, with the understanding that said patent counsel would be responsible for the prosecution of application. All replies to patent office actions prepared by outside patent counsel should be transmitted to the Signal Corps Patent Section for actual filing in the patent office.

4. (a) If during the pendency of said patent application

and prior to the grant of a patent thereon, applicant should make a formal assignment of title and have said assignment recorded, the assignee (i.e. the owner of the commercial rights) would then become responsible for the payment of the final government fee.

(b) On the other hand, if the formal assignment of title be deferred until after the actual grant of the patent, the payment of a final government fee would thereby be avoided.

/s/ John H. Gardner, Jr.
John H. Gardner, Jr.,
Captain, Signal Corps.

Incls-n.c.

3d Memo Ind. 8

War Plans & Training Division, May 6, 1935 - To: Executive Officer.

Approval of request contained in paragraph 3 of Mr. Friedman's memorandum of April 19, 1935 is recommended subject to the provisions of 2d Memo Indorsement.

/s/ S. B. Akin
S. B. Akin,
Major, Signal Corps.

Incls. (no change).

4th Memo. Ind. 2

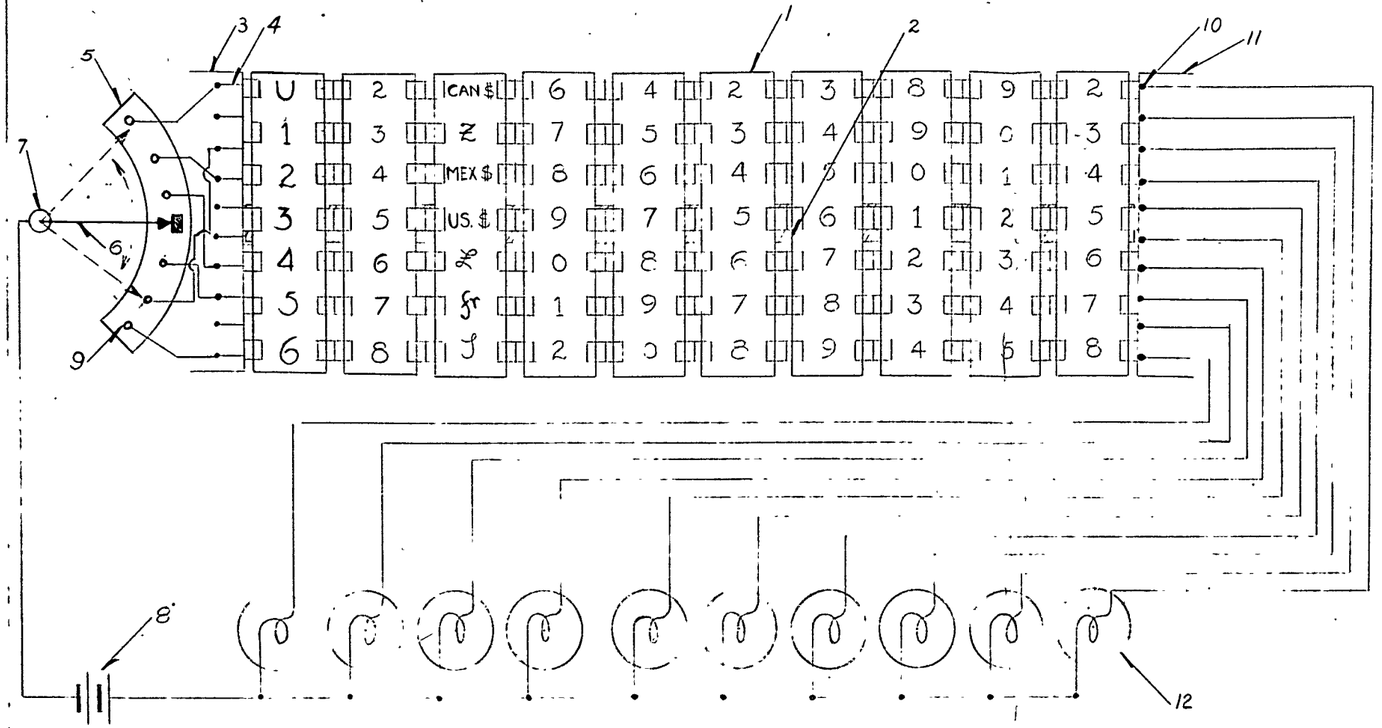
Executive Office, May 7, 1935 - To Major Akin.

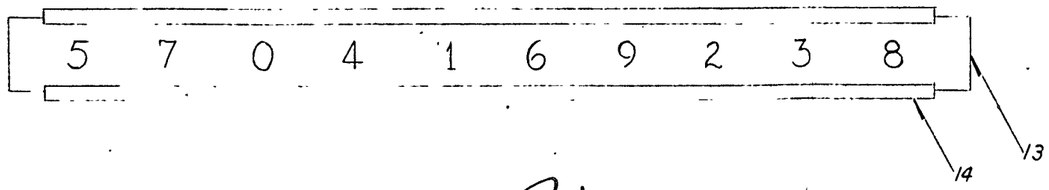
Approved as recommended in 3d Memo Indorsement, hereon.

/s/ Dawson Olmstead
Dawson Olmstead,
Lt. Col., Signal Corps,
Acting Chief Signal Officer of the Army.

Incl. n/c

C
O
P
Y




William F. Friedman