Read. files

SISDE-30 AUTHENTICATION DEVICE (ROSEN & FRIEDMAN)

8870
dll

SECRET

Memo for Major Cook:

Herewith carbon copy of document on a recognition-
Authentication device.

Note par. (3) thereof.

Please let me know if the recommended action thereon was initiated.

J.

Info. recd. that the subject is more or less dead in that there does not appear to be much use for this. Rowen says he doesn't believe patent is necessary on worth while. Seth Thomas does not one experimental model. Other replies were received but not too encouraging.

6

IN REPLY
REFER TO

0-3-C

WAR DEPARTMENT
OFFICE OF THE CHIEF SIGNAL OFFICER
WASHINGTON

November 6, 1941

MEMORANDUM FOR: Colonel Minckler

Herewith is preliminary write-up with rough drawings of the recognition-authentication device concerning which I told you yesterday.

Recommend (1) that we be permitted to start at once to build a first model in our shop. Materials for same are practically all on hand, except for clock mechanism.

(2) that Lieut. Rosen be sent to see clock manufacturers, with a view to finding a clock suitable for the purpose of the proposed new device.

(3) that copy of these papers be forwarded to Signal Corps Patents Board for processing.

William F. Friedman.

SECRET

Preliminary description of an invention concerning a mechanism for producing secret recognition, identification, or authentication symbols.

A. This description consists of this sheet of explanation and four figures. The following elements are incorporated in the device:

1. Three or more rotors, conventionally wired, and arranged with associated lamps, bar key and battery as shown in the circuit details diagram, Fig. 1.
2. A clockwork mechanism so arranged as to drive one of the rotors periodically at specified time intervals. Thus in diagram of "step mechanism details", Fig. 2, is shown a form of drive suitable for rotating rotor in number 2 position forward at specified time intervals by means of a clockwork, camshaft, cam and associated pawl. The clockwork is also provided with a conventional dial (preferably of the 24 hour variety). This dial is further subdivided into 26 segments, marked alphabetically as shown in the general view, Fig. 3.
3. Both the left and right end stator wirings are variable, and can be changed by means of a plug and jack arrangement.
4. A ring so constructed that it will fit on the outside of any one of the rotors is provided. Details of this ring are shown in the figure showing rotor details, Fig. 4.

B. Operation of the machine is accomplished in this way. (all settings according to key):

1. The ring referred to in 4 above is placed on the rotor which will be placed in position 2, the arm on the ring falling into the appropriate stepping notch in the rotor.
2. The end stator wirings are fixed.
3. Rotors are inserted.
4. The clock is wound and set to the correct time.
5. Center rotor is set to letter corresponding to that shown by clock on its alphabetical dial. (Letter visible through the cover window on rotor in #2 position is actually the letter on the removeable ring rather than the true rotor letter.)
6. Set other rotors and end plate to hourly setting.
7. Challenge is letter showing through the cover window of rotor in number 2 position.
8. Answer is letter (or letters) shown by lights when key bar is depressed.
9. If challenge letter does not correspond to letter shown in cover window of rotor in number 2 position, this rotor is reset manually before challenge is answered.
10. Rotors are reset manually on the hour. Delayed setting can be made by checking with alphabetical dial on clock. At beginning of setting period new setting is shown by the fact that the challenge is a letter at the beginning of the alphabet. (Rotor in number 2 position will not move from Z to A automatically.) Therefore if challenge is received as a letter near the beginning of the alphabet, it is known that the new setting is in effect. (This provision is for the purpose of eliminating possible errors due to slight differences in clock speeds and thus system does not require accurate synchronization.

Disclosed to us at Washington, D.C., on November , 1941.

Earle P. Cook
1020 S Barton St Arlington, Va.

Vernon E. Cooley
1402 N Abingdon St Arlington, Va.

Invented at Washington, D.C., November 3, 1941, by

William F. Friedman
William F. Friedman

Leo Rosen
Leo Rosen

SECRET

Preliminary description of an invention concerning a mechanism for protecting secret, identification, or authentication system symbols.

A. This description consists of this sheet of explanation and four figures. The following elements are incorporated in the device:

1. Three or more rotors, conventionally wired, and arranged with associated lamps, bar key and battery as shown in the circuit details diagram, Fig. 1.

2. A clockwork mechanism so arranged as to drive one of the rotors periodically at specified time intervals. Thus in Fig. 2 diagram of "step mechanism details" is shown a form of drive suitable for rotating rotor in number 2 position forward at specified time intervals by means of a clockwork, camshaft, cam and associated pawls. The clockwork is also provided with a conventional dial
3. (preferably of the 24 hour variety). This dial is further subdivided into 26 segments, marked alphabetically as shown in the general view, Fig. 3.

3. Both the left and right end stator wirings are variable, and can be changed by means of a plug and jack arrangement.

4. A ring ~~is provided~~ (IS PROVIDED) so constructed that it will fit on the outside of any one of the rotors. Details of this ring are shown in the figure showing rotor details, Fig. 4.

B. Operation of the machine is accomplished in this way (all settings according to key):

1. The ring referred to in 4 above is placed on the rotor which will be placed in position 2, the arm on the ring falling into the appropriate stepping notch in the rotor.
2. The end stator wirings are fixed.
3. Rotors are inserted.
4. The clock is set to the correct time and wound.
5. Center rotor is set to letter corresponding to that shown by clock on its alphabetical dial. (~~Center rotor~~ #2 position rotor letter visible through the cover window is actually the letter on the removeable ring rather than the true rotor letter.) on rotor in #2 position
6. Set other rotors and end plate to hourly setting.
7. Challenge is letter showing throughthe cover window of rotor in number 2 position. (or letters)
8. Answer is letter shown by lights when key bar is depressed.
9. ~~XXXXXXXXX~~ If challenge letter does not correspond to letter shown in cover window of rotor in number 2 position, this rotor is reset manually. before challenge is answered.
10. Rotors are reset manually on the hour. Delayed setting can be made by checking with alphabetical dial on clock. At ~~end~~ beginning of setting period new setting is shown by the fact that the challenge is a letter at the ~~end~~ beginning of the alphabet. (Rotor in number 2 position will not move from Z to A automatically). Therefore if challenge is received as a letter near the beginning of the alphabet, it is known that the new setting is in effect. (This provision is for the purpose of eliminating the possible errors due to slight differences in clock speeds. And thus system does not require accurate synchronization.

Disclosed to us at Washington D.C., on Nov. ,1941.

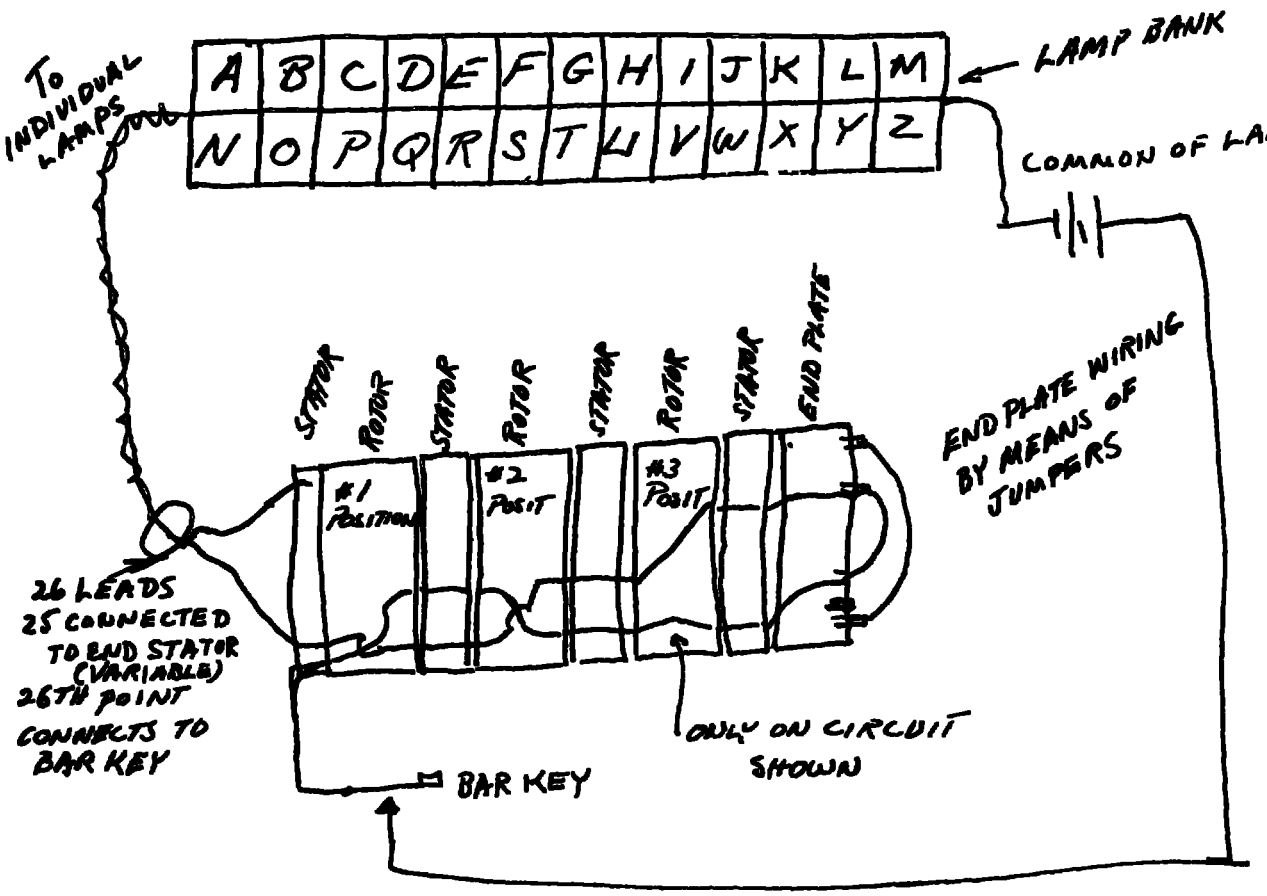
Invented at Washington, D.C., Nov. 3, 1941, by

WILLIAM F. FRIEDMAN

LEO ROSEN

~~SECRET~~

CIRCUIT DIAGRAM. REF ID:A67602 SECRET



ROTORS IN #1, #2, AND #3 POSITIONS AND END PLATE MAY BE ROTATED BY HAND, ONLY ROTOR IN #2 POSITION IS ROTATED BY MECHANICAL MEANS

Invented at Washington, D.C., November 3, 1941, by

William F. Friedman

Leo Rosen

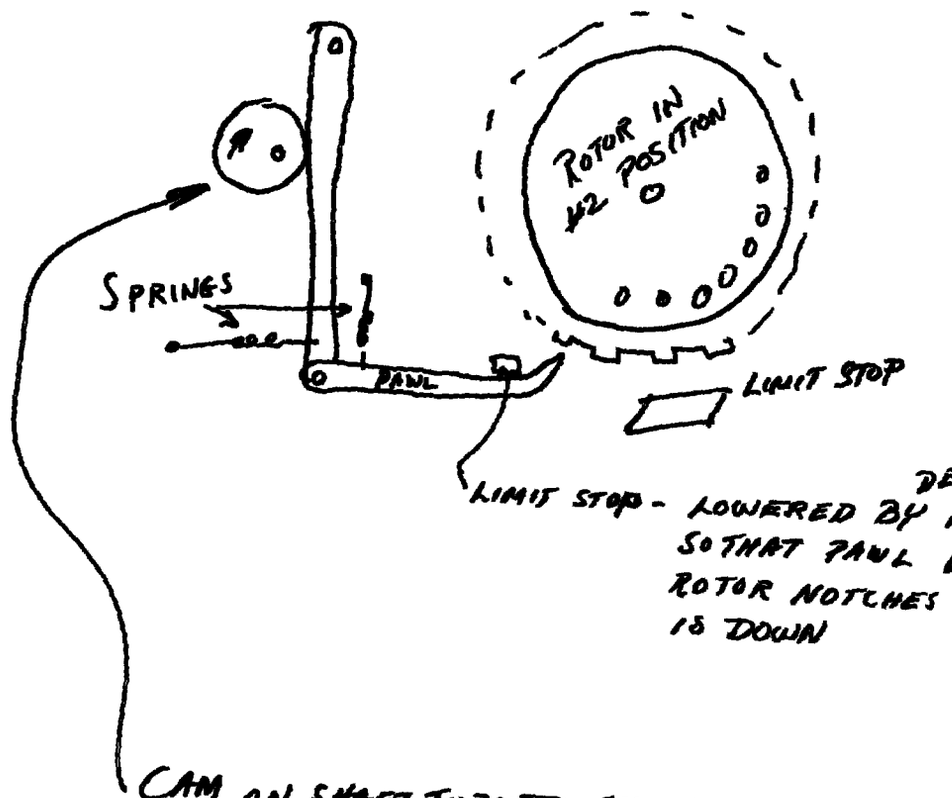
Fig. 1

Disclosed to us at Washington, D.C. November 3, 1941:

Coree P. Cook
1020 S Barton St Arlington, Va

Vernon E Cooley
1402 N Abingdon St
Arlington, Va

POSITION #2 SET-MECHANISM DETAIL



LIMIT STOP - LOWERED BY DEPRESSION OF KEY BAR SO THAT PAWL WILL NOT ENGAGE ROTOR NOTCHES WHEN KEY BAR IS DOWN

CAM ON SHAFT TURNED BY WOUND SPRING (OR MOTOR THROUGH FRICTION CLUTCH) RELEASED FOR ONE REVOLUTION AT SPECIFIED TIME INTERVALS BY CLOCKWORK. [ROTOR IN #2 POSITION IS CAUSED TO ROTATE ONE STEP AT SPECIFIED TIME INTERVALS BY THIS MECHANISM]

Fig. 2

Invented at Washington, D.C.
November 3, 1941, by
William F. Friedman
Leo Rosen

Disclosed to us at Washington, D.C.,
November 3, 1941

Earle P. Cook
1020 S Barton St Arlington Va

Vernon C. Cooley
1402 N Abingdon St
Arlington, Va.

GENERAL VIEW

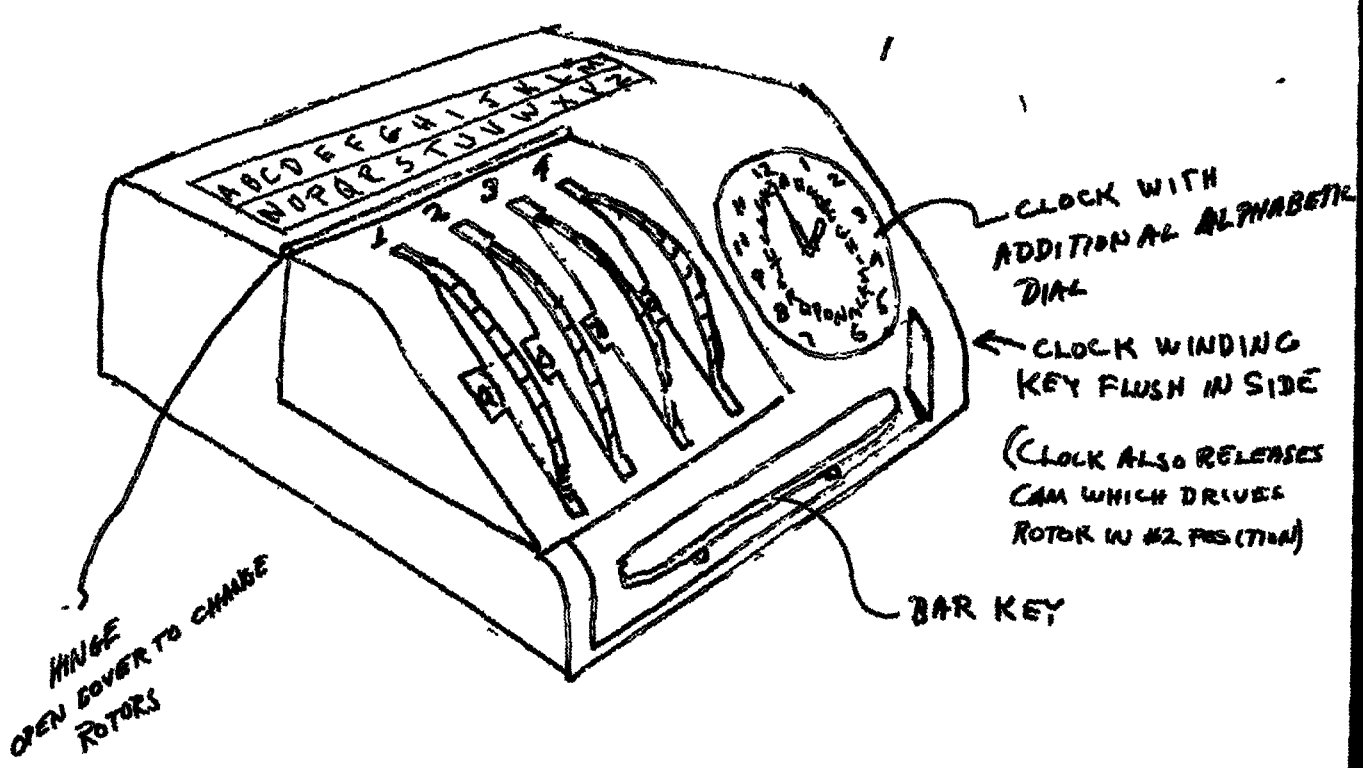


Fig. 3

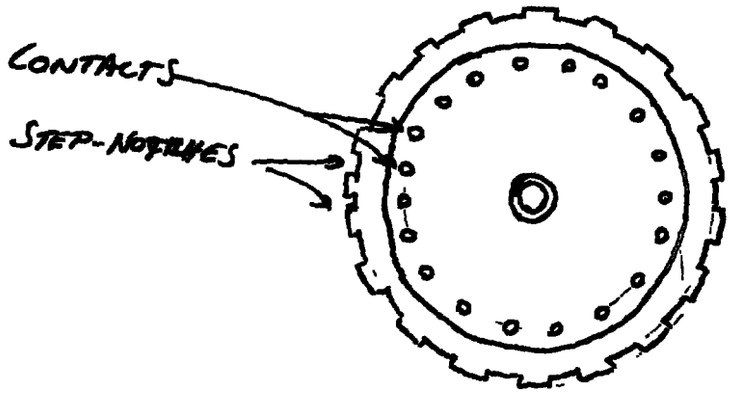
Invented at Washington, D.C., November 3, 1941, By
William F. Friedman
Leo Rosen

Disclosed to us at Washington, D.C., November 3, 1941:

Earle L. Cook
1020 S. Barton St Arlington, Va.

Vernon E Cooley
402 W Abingdon St
Arlington, Va

ROTOR DETAILS



ROTORS MAY BE INSERTED EITHER WAY. ONLY ONE ALPHABET APPEARS IN COVER WINDOW

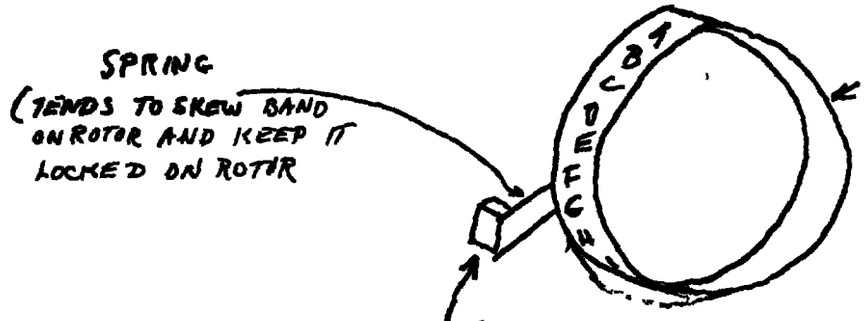


Fig. 4

Disclosed to the Government at Washington, D.C., November 3, 1941:

Earle P. Cook
1020 S. Barton St. Arlington, Va.

Vernon E. Cooley
1402 N. Abingdon St.
Arlington, Va.

Invented at Washington, D.C., November 3, 1941, by:

William F. Friedman

Leo Rosen

Memo for Capt. Cook:

Re possible usage - distribution of the proposed recognition - authentication device, it appears to me that such a mechanism would be highly useful for the following purposes:

1. Identification - recognition between friendly:
   (a) Aircraft in flight in night operations
   (b) Aircraft and ground stations of anti-aircraft installations at night.
   (c) Tanks and other armored vehicles in night operations
   (d) Ships and shore batteries
   (e) Ships at sea in night operations
2. Authentication of messages exchanged between friendly
   (a) Fixed and semi-fixed radiotelegraph installations of the larger headquarters (Division and above)
   (b) Ships at sea
   (c) Ships and shore stations

FJ