REF ID:A363367

Keyboard - switch buttons associated with indicating lamps in display panel

Depression of one button ass with lamps, its lamp & another are lighted.

As an authentication device - sets up a series of auth. symbols etc

Combination of crypto & authentication device

Means for stepping rotors - finger pieces, pawls, levers.

Declassified and approved for release by NSA on 07-23-2014 pursuant to E.O. 13526

REF ID:A363367

Mb "Q"
Condensed Progress
Reports (Mr. Murray)
Sec. 13

2781-A

Security Measures
in Handling Mail

F 3086
Rec'd Col Hotch 9 Feb
Ret'd 9 Feb 43 Hotch

Case RE[redacted]-ID-A363367
dust proof - other
features

Insertion switch
to permit shift from
crypt to authentication

Stylus + plate switch
means

Rebecca Schwartz

REF ID:A363367

~~CONFIDENTIAL~~

which may be used either as a cryptograph or as an authentograph for testing the authenticity of messages

This invention relates to a device or machine for enciphering and deciphering communications ~~which are to be transmitted secretly in coded or cryptographic form.~~

~~Among~~ The primary objects of this invention ~~is~~ to provide a cipher device which is simple in construction and maintenance, but nevertheless ~~yet~~ affords a high degree of security, is light and readily portable, and can be readily disassembled and rearranged to vary the cipher keying elements ~~code or deranged or destroyed to prevent its use by unauthorized persons.~~

Another object of this invention is to provide an authentograph, that is, a ~~authentication or~~ device for testing the authenticity of ~~the~~ signals, thereby ~~or~~ ~~means for indicating that~~ a message ~~which is to be decoded,~~ has means for assuring that such a message or signal originated at an authorized source and is therefore authentic to be considered.

Other objects of the invention will become apparent as this description proceeds.

In the drawings,

Fig. 1 is a top or plan view with the covers closed.

Fig. 1a is a side elevation of the front portion of the device with the keyboard cover folded back beneath the same.

Fig. 2 is a top or plan view on an enlarged scale with the keyboard cover and parts of the rotor cover omitted.

Fig. 3 is a side elevation with the covers closed.

Fig. 4 is a cross section on line 4-4 of Fig. 2 with the rotor cover omitted.

Fig. 5 is a perspective view of the rotor latch.

Fig. 6 is a perspective view of the rotor actuating mechanism.

Fig. 7 is a diagram showing schematically the electric circuits and the mechanical operating mechanisms.

Fig. 8 is a view of a portion of the device ~~cryptograph, of my invention,~~ illustrating a modified keyboard and switching means.

Fig. 9 is a view of a rotor such as is used in the device of this invention.

~~CONFIDENTIAL~~

REF ID:A363367

That embodiment of the invention selected from among others for illustration in the drawings and description in the specification is as follows. Referring to Fig. 7, the device will be seen, in general, to consist of a source 10 of electricity, ~~shown as a pair of dry cells,~~ connected to a pair of wires 11 and 12 across which are connected a plurality (in this instance, twenty-six) indicators 13A, 13B, 13C, etc. These indicators are illustrated as being electric lamps arranged beneath a keyboard and indicator panel 14 (see Fig. 2) and each arranged to illuminate one perforation closed by a transparent cover 15 bearing one letter 16 of the alphabet thereon. Panel 14 is secured in place over a gasket 14' of soft rubber or the like. Across lines 11 and 12 are also connected manually operable switches 17A, 17B, 17C, etc., each in series with one of the indicators 13A, 13B, etc., ~~and each~~ arranged for operation by ~~a~~ pushbuttons ~~or handle~~ 18 projecting through keyboard 14 ~~along side of one of~~ in proximity to the covers 15.

Connected to each of the indicators 13A, 13B, etc., is a multicontact electric switch, generally indicated as 19. It comprises a number of relatively ~~turnable~~ juxtaposable and rotatable cryptographic rotors, 19A, 19B, 19C, 19D, ~~19E~~, each having a plurality of contacts thereon, ~~and~~ connected in cascade, the output contacts of which are connected in pairs by ~~connections between pairs of the contacts~~ electrical paths through the rotor system 19 as shown diagrammatically at 20. Each ~~connection 20~~ leads from one stationary contact 20' through the cryptographic rotors and back, through 20'', to another stationary contact. These ~~connections~~ flatten circuits 20 are rearranged each time one of the rotors is turned.

In ~~lead wire 11 is connected~~ conductor 11 there is a normally-closed electric switch 21. Between one of the indicators, in this case 13E, and multicontact switch 19, ~~is connected~~ there is a normally-closed electric switch 22. In parallel with wire 11 is wire 11A containing an authenticating switch 23 having an operating handle 24. Wire 11A also contains a normally-open switch 25.

REF ID:A363367

~~CONFIDENTIAL~~

Turning now to Figs. 1, 2, and 3 for a disclosure of the mechanical features of the invention, the device is shown as enclosed in a casing 26 to which are hinged or otherwise attached a back cover 27 and a front cover, protecting the keyboard, 28. The front cover is secured to casing 26 by means of a double hinge 28', 28". This arrangement permits the cover to fit snugly upon gasket 14', thereby to provide a substantially dust-proof and water-proof closure for the keyboard 14. The cover may also lie flat in front of the machine, or may be folded therebeneath. The back part of the casing, adjacent the rotor assembly, is provided with a lip 26' (see Figure 2). Back cover 27 is adapted to fit over this lip, and has a gasket 27' which provides, upon closure of the back cover, a dust-proof and moisture-proof seal. In the top of casing 26 there is an opening 29 through which a counter 30 is visible. As is most readily seen in Fig. 6, casing 26 has two projecting walls 26A and 26B. The switching assembly 19 is retained between these walls by a mechanism which will now be described. Wall 26A has a hole in it through which may be pushed pin 30A having a knurled head 31 and a latch 32 co-operating with a retaining spring 33. Also pivoted on wall 26A is a spring latch 34 of U-shape, being bent parallel to itself. The free end 34A of latch 34 is perforated to allow pin 30A to pass through it and bears cam surfaces 35 thereon. Stationary cam 36 has a surface complementary to cam surfaces 35 so that when latch 34 is moved from the substantially horizontal position, in which it is shown in Figs. 2, 4, and 6, into the vertical position, in which it is shown in Fig. 5, the free end 34A of latch 34 is moved away from wall 26A and compresses the spring contacts 20A (see Fig. 2) of rotors 19 and locates the rotors themselves in desired positions.

~~CONFIDENTIAL~~

entire rotor-reflector assembly so as to insure good contacts therethrough

The manually operated means for rotating the cryptographic rotors 19 will next be described. As seen in Figs. 1, 2, 3, and 6, casing 26 has a recess 37 in its top into which fits a finger-piece 38 having a sliding fit in the recess and mounted on a rod 39. Rod 39 causes U-shaped stirrup 40 to turn on its pivots in walls 26A and 26B. Stirrup 40 carries as a part cam 41 which actuates follower 42 fast on shaft 43 of counter 30. Stirrup 40 also has a member 44 to which spring 45 is attached and which carries cam face 46. Detent 47 is pivoted at 48 in walls 26A and 26B and is stressed by spring 49 so that cam 50 engages cam face 46. Spring detents 60 normally hold rotors 19 in their relative positions but allows movement of these rotors under the actuation of pawls 58. This permits detent teeth 51 to be moved in and out of the ratchet depressions in the surface of the rotors 19.

Stirrup 40 carries a pin 52 on which are pivoted a plurality of cam-and-pawl devices 53A, 53B, 53C, and 53D which are urged by springs 54 against cam surfaces 57 or ratchet depressions 56 (see Fig. 7) on rotors 19 (all figure 9). Device 53A, for example (figure 6), has a cam surface 55 and a pawl 58 cooperating, respectively, with cam surface 57 and ratchet recesses 56 on the rotor 19A. A tang 59 of device 53A underlies device 53B so that device 53B prevents device 53A from operating unless device 53B is also depressed and operated.

The operation of this device is as follows: To operate the cryptograph, cover 28 is opened to expose the keyboard. If, as frequently happens, limitations of space require, the cover may be folded back beneath the machine. For enciphering or deciphering, handle 24 is operated so that switch 23 is open. That push button

18 which is associated with the desired letter is depressed and the switch controlled thereby is operated. For example, if push button 18 associated with ~~switch 17E representing~~ the letter E, is ~~closed~~ depressed, connections ~~are~~ made from battery 10 through line 11, switch 21, and switch 17E, ~~through~~ lamp 13E, and line 12 back to source 10. This action also closes connections from ~~switch 17E~~, through switch 22, ~~and connections 20 or~~ rotors ~~19 to be~~, lamp 13Z, and ~~thence~~ line 12, back to source 10. Lamps 13E and 13Z are ~~therefore~~ simultaneously lighted and thus indicate that ~~E is to be encoded or decoded as the case may be, as Z.~~ Since rotors 19 connect all the lamps 13A, 13B, etc., together in pairs each letter has another corresponding to it.

For rotating the cryptographic rotors 19 and thus varying the connections between the various pairs of lamps 13 and switches 17, the ~~finger-piece 38~~ plunger 39 is depressed, stirrup 40 is rotated about its pivots and the ~~devices~~ members 53A, etc., moved. Whenever one of the cam faces 55 encounters a ~~depression~~ notch in the periphery of a rotor ~~(shown at 55D in Fig. 12)~~, ~~the corresponding cam 57,~~ its member 53 (53A?) ~~the device 53~~ is moved by spring 54, so that ~~the~~ its pawl 58 enters ~~the ratchet depression~~ a notch 56 unless prevented from doing so by the engagement of the tang 59 with the next ~~device 53~~ element 53. Whenever a pawl 58 enters ~~a ratchet depression~~ 56, and the movement of the ~~finger-piece 38~~ plunger 39 is completed, the corresponding rotor 19 is moved one step. This rearranges the connections ~~20~~ through the rotors and connects different pairs of lamps 13A, etc., together. Counter 30 is moved one numberal because follower 42 is depressed by cam 41 and spring returned. Detent 47 prevents backward movement of rotors 19 because teeth 51 enter ~~depressions~~ notches in rotors 19.

A detailed description of the operation of the device as an authentograph

for insuring the authenticating of a message. Switch 23 is closed by snapping handle 24. ~~Finger-piece 38~~ plunger 39 is then depressed, opening switches 21 and 22 and closing switch 25. This movement moves counter 30 one position forward, and also one or more rotors 19 one step. The following circuit is ~~closed from~~ source 10, line 11, line 11E, closed, line 20, thence through the rotor system line 11A, switch 23, switch 25, ~~rotor connections 20~~ to whichever lamp happens to be paired with lamp 13E. Circuit to lamp 13E is at this time open at switch 22. ~~The designation letter of the lamp which is~~ the letter which is thus paired with 13E ~~is transmitted as an~~ becomes an authenticator, ~~an agreement having~~ which will, of course, be duplicated on a machine similarly set to the same key. ~~been previously reached by the two parties concerned as to the wiring of the several rotors, their arrangement in the device, and the number of steps having been taken as indicated by counter 30.~~

To remove the rotors 19, cover 27 is opened, latch 34 moved from the upright position of Fig. 5 to the horizontal position of Fig. 6, and pin 30 withdrawn by grasping head 31. This allows cam 35 to enter the corresponding groove in stationary cam 36. Rotors 19 can then be lifted out and ~~destroyed if it is desired to prevent their use by unauthorized persons. Or, if the code is to be changed the rotors can be reinserted in the casing 26 in a different order or their connections 20 changed and the rotors then inserted in casing 26.~~ Pin 30 is then placed in position, latch 34 raised, and cover 27 closed.

or a signal will now be given. Agreement

the counter is set to zero and

Now suppose that the device is being used to authenticate a plain-language message sent from station A to station B. Having transmitted the message, station A operates its device and finds the authenticating letter to be K, for example. The letter is transmitted as the authentication; station B, operating its device finds that K is the correct and hence is warranted in its belief that the message comes from an authorized source. Upon the next authentication, the letter will be different, since one or more of the rotors will have advanced on the operation of the plunger 39.

-7-

REF ID:A363367

The modification of Fig. 8 includes a viewing panel 60, similar in appearance to the viewing panel and keyboard 14 of Fig. 2. In place of the push buttons 18, however, viewing panel 60 is provided with contacts only, as 61. These contacts, as shown, consisting merely of small circular elements of conducting material. With reference to Fig. 7, contacts 61 may be considered to be represented by switches 17A, 17E, etc. In place of the push buttons 18, a stylus 62 is provided and this may be considered to be connected to conductor 11 of Fig. 7. Encipherment is accomplished by making contact between stylus 62 and a desired contact 61 on panel 60.

The above description is in specific terms, but it is to be understood that the invention is not limited to the precise structures and circuits shown and described. Instead, for the true scope of the invention, reference should be nad to the appended claims.

I claim:

REF ID:A363367

1. In a cryptograph having relatively rotatable electric switches arranged in cascade, therein, means for angularly displacing said switches so as to vary the connections therebetween, comprising a plunger or the like arranged for manual operation, means associated with said plunger and cooperating upon depression thereof with one of said electric switches for angularly displacing the same, means associated with said plunger and cooperating upon depression thereof with another electric switch for angularly displacing the same after a predetermined ~~rotation~~ angular displacement of said first mentioned switch, and a brake operable by said plunger through a lost-motion connection for preventing more than a desired angular displacement of any switch.

2. In a cryptograph, the combination of a source of current, a plurality of ~~inputs, a plurality of~~ input-output contacts, a plurality of indicating devices each with a normally open circuit between it and an input contact, and a normally open circuit between it and every output contact, and a switch associated with each of said indicating devices and adapted when closed to complete its said first mentioned circuit and one of said second mentioned circuits.

3. The combination of claim 2, further characterized by means for varying the selection of a second mentioned circuit to be completed upon the closing of a switch.

4. The combination of claim 2, further characterized by a plurality of mixing rotors, the normally open circuit between a said indicating device and the said outputs including said rotors.

REF ID:A363367

5. In a cryptographing machine, a plurality of cryptographic rotors, stationary input output contacts and stationary output contacts adapted to be connected variably in pairs through said rotors, an indicator connected to each of said stationary contacts, a switch associated with each indicator, and a source of current, whereby the closing of one of said switches will close a circuit through a selected input contact and its associated indicator and an output and its indicator.

6. The invention of claim 5 further characterized by means for stepping the rotors.

7. The invention of claim 5 further characterized by a plunger or the like adapted when depressed to (advance one or more rotors STEP A ROTOR. one or more) a predetermined number of steps.

8. The combination with a cryptographing machine device having a plurality of electrical inputs for the characters to be enciphered, a plurality of electrical outputs for the enciphered equivalents of said characters, a viewing panel or the like including a lamp for each character, a switch associated with each lamp and with a source of current, and a plurality of circuits each including said source, one of said switches, a lamp associated therewith, an input corresponding to the character represented by said lamp, and a lamp corresponding to the output associated with the last mentioned input, whereby the closing of one of said switches will light a lamp representing a character to be enciphered and a lamp representing the enciphered equivalent of said character.

REF ID:A363367

9. In a cryptographing machine, the combination of a plurality of electrical inputs for the characters to be enciphered, a plurality of electrical outputs for the enciphered equivalents of said characters, a source of current, a viewing panel or the like including a lamp for each character, an electrical contact associated with each lamp, a contacting member, and a plurality of normally open circuits each including said source, said contacting member, one of said electrical contacts, the lamp and input corresponding to the character associated with said contact, and a lamp corresponding to the output associated with the last mentioned input, whereby a contact between said contacting member and one of said contacts will light a lamp representing the enciphered equivalent of said character.

10. In an authentograph, a cryptographing machine, a source of current, a plurality of cryptographic rotors, stationary input contacts in pairs and stationary output contacts adapted to be connected variably through said rotors, an indicator connected to each of said stationary contacts, a plunger or the like adapted when depressed to angularly displace one or more of said rotors, rotate a rotor a predetermined number of steps, a switch associated with each indicator, an additional normally open switch controlling a circuit between a predetermined input one stationary contact and another stationary an output contact and its indicator, and a further normally open switch adapted to be closed by said plunger thereby to energize the indicator associated with said output only if said additional normally open switch is closed.

11. In a combination with a cryptographing ~~machine~~ device adapted to receive input signals representing characters to be enciphered and to mix the signals and to indicate to an operator both input and enciphered characters, an authenticator adapted when actuated to indicate the output character associated with a predetermined input character.

12. In combination with a cryptographing ~~machine~~ device adapted to receive input signals representing characters to be enciphered and including a ~~rotor~~ set of cryptographic rotors in cascade for mixing the signals, means for indicating to an operator both input and enciphered characters, means for stepping the rotors, and means for recording the steps of said rotors, and an authenticator adapted when actuated to indicate only the enciphered character instantaneously associated with a predetermined input character.

13. The method of providing an authentication for a ~~secret~~ message comprising characters enciphered by a stepping set of cryptographic rotors which includes recording the steps of the rotors and utilizing the enciphered equivalent of a predetermined character after a predetermined number of steps of said rotors.

14. The method of authenticating a message ~~of~~ by characters enciphered by an electrical system of stepping cryptographic rotors having an input contact and an output contact for each character which comprises providing a circuit including a predetermined input contact and an output contact dependent upon the instantaneous positions of said rotors, and utilizing the enciphered equivalent of the character associated with said predetermined input contact for known conditions of said rotors.

REF ID:A363367

Friedman. 14 January 1944.
Objects. Title: Cipher Device.

RP

This invention relates to a device or machine for enciphering and deciphering communications which are to be transmitted secretly in coded or cryptographic form.

Among the objects of this invention are to provide a cipher device which is simple yet affords a high degree of security, is light and readily portable, and can be readily disassembled and rearranged to vary the code or deranged or destroyed to prevent its use by unauthorized persons.

Another object of this invention is to provide an authenticator or means for indicating that a message, which is ~~secret~~ to be decoded, has originated at an authorized source

Other objects of the invention will become apparent as this description proceeds.

#2.

In the drawings—
Fig. 1 is a top or plan view with the covers closed.
Fig. 2 is a top or plan view on an enlarged scale with the keyboard cover and part of the rotor cover omitted.
Fig. 3 is a side elevation with the covers closed.
Fig. 4 is a cross section on line 4-4 of Fig. 2 with the rotor cover omitted.
Fig. 5 is a perspective view of the rotor latch.
Fig. 6 is a perspective view of the rotor actuating mechanism.
Fig. 7 is a diagram showing schematically the electric circuits and the mechanical operating mechanisms.

That embodiment of the invention selected from among others for illustration in the drawings and description in the specification is as follows. Referring to Fig. 7, the device will be seen, in general, to consist of a source 10 of electricity, shown as a pair of dry cells, connected to a pair of wires 11 and 12 across which are connected a plurality (in this instance twenty-six) indicators 13A, 13B, 13C, etc. These indicators are illustrated as being electric lamps arranged beneath a keyboard 14 (See Fig. 2) and each arranged to illuminate one perforation closed by a transparent

#3.

covers 15 bearing one letter of the alphabet 16 thereon. Across lines 11 and 12 are also connected manually operable switches 17A, 17B, 17C etc. in series with one of the indicators 13A, 13B, etc. and each each arranged for operation by a push button or handle 18 projecting through keyboard 14 along side of one of the covers 15.

Connected to each of the indicators 13A, 13B, etc. is a multi-contact electric switch, generally indicated at 19. It comprises a number of relatively turnable cryptographic rotors, 19A, ... 19E, each having a plurality of contacts thereon and connections between pairs of the contacts as shown diagrammatically at 20. Each connection 20 leads from one stationary contact through the cryptographic rotors to another stationary contact. These connections 20 are rearranged each time one of the rotors is turned.

In lead wire 11 is connected a normally-closed electric switch 21, between one of the (over)

REF ID:A363367

indicators, in this case 13E, and multi-contact switch 19 is connected normally-closed electric switch 22. In parallel with wire 11 is wire 11A containing an authenticating switch 23 having an operating handle 24. Wire 11A also contains a normally open switch 25.

Turning now to Figs. 1, 2 and 3 for a disclosure of the mechanical features of the invention, the device is shown as enclosed in a casing 26 to which are hinged or otherwise attached a rotor cover 27 and a keyboard cover 28. Casing 26 has an opening 29 through the top by means of which a counter 30 is visible. As is most readily seen in Fig. 6, casing 26 has two projecting walls 26A and 26B. The cryptographic rotors 19 are retained between these walls by mechanism which will now be described. Wall 26A has a hole in it through

REF ID:A363367

which may be pushed in 30 having a knurled head 31 and a latch 32 co-operating with a retaining spring 33. Also mounted on wall 26A is a spring latch 34 of U-shape having bent back parallel to itself. The free end 34A of latch 34 is perforated to allow pin 30 to pass through it and bears cam surfaces 35 thereon. Stationary cam 36 has a surface complementary to cam surfaces 35 so that when latch 34 is moved from the substantially horizontal position, in which it is shown in Figs. 2, 4 and 6, into the vertical position, in which it is shown in Fig. 5, the free end 34A of latch 34 is moved away from wall 26A and compresses the contacts of springs 20A (see Fig. 2) locates the rotors themselves in desired position.

The manually operated means for rotating the cryptographic rotors 19 will next be referred to. As seen in Figs. 1, 2, 3 and 6 casing 26 has a recess 37 in its top into which fits a finger piece 38 having a sliding fit in the recesses and mounted on a rod 39. Rod 39 carries U-shaped

(over)

REF ID:A363367

H 6

A pawl detent 60 engages hold rotors 19 in their relative positions to allow movement of these rotors under the actuation of pawls 58.

stirrup 40 to turn about its pivots in walls 26A and 26B. Stirrup 40 carries as a part cam 41 which actuates lever 42 fast on shaft 43 of counter 30. Stirrup 40 also has a part 44 to which spring 45 is attached and which carries cam face 46. Detent 47 is pivoted at 48 in walls 26A and 26B and is pressed by spring 49 so that cam 50 engages cam face 46. This prompts detent teeth 51 to be moved in and out of the ratchet depressions in the surface of the rotors 19. Stirrup 40 carries a pin 52 on which are pivoted a plurality of cam-and-pawl devices 53A 53B, 53C, and 53D which are urged by springs 54 against cam surfaces 57 of ratchet depressions 56 (see fig 7) of rotors 19. Device 53A for example has a cam surface 55 and a pawl 58 cooperating respectively with cam surface 57 and ratchet recesses 56' on the rotor 19A. A tang 59 of device 53A overlies device 53B so that device 53B prevents device 53A from operating unless device 53B is also depressed and operating.

The operation of this device is as follows. For coding or decoding handle 24 is located so that switch 23 is open. That push button 18 which is associated with the desired letter is depressed and the switch controlled thereby is closed. For example if switch 17E representing the letter E is closed connections are made from battery 10 through line 11 switch 21 and switch 17E through lamp 13E, and line 12 back to source 10.

#7

REF ID:A363367

This action also closes connections ~~are also closed~~ from switch 17E through switch 22 and connections 20 of rotor 19 to lamp 13Z and thence through line 12 back to source 10. Lamps 13E and 13Z are therefore simultaneously lighted and thus indicate that E is to be encoded or decoded as the case may be as Z, and vice versa. Since rotor 19 connects all the lamps 13A, 13B etc. together in pairs, each letter has another corresponding to it.

For rotating the cryptographic rotors 19 and thus varying the connections between the various pairs of lamps, finger piece 38 is depressed, stirrup 40 is rotated about its pivots and the devices 53A, etc. moved. Whenever one of the cam faces 55 encounters a depression (shown at 55D in Fig. 4) in the corresponding cam 57, the device 53 is moved by spring 54 so that the pawl 58 enters the ratchet depression 56 unless prevented from doing so by the engagement of the tang 59 with the next device 53. Whenever a pawl 58 enters a ratchet depression 56, and the movement of the finger-piece 38 is completed, the corresponding rotor 19 is moved one step. This rearranges the connections 20 through the rotors and connects different pairs of lamps 13A, etc. together. Counter 30 is moved one numeral because follower 42 is depressed by cam 41 and spring returned. Detent 47 prevents backward movement of rotors 19 because teeth 51 enter ratchet depressions in rotors 19.

For insuring the authenticity of a message, switch 23 is closed by ~~en~~ applying handle 24.

(over)

RELEASED:A363867

finger piece 38 is then depressed, opening contacts 21 and 22 and closing switch 25. This movement moves counter 30 one position and also one or more rotors 19 one notch. Circuit is closed from source 10, line 11, line 11A, switch 23, switch 25, rotor connections 20 to whichever lamp it happens to be wired with lamp 13E. Circuit to lamp 13E is open at switch 22. This action insures that the rotors 19 are connected up in the same way and by agreement upon the setting of counter 30, that the message is authentic or, in other words, originates at an authorized source.

To readily remove the rotors 19, cover 27 is opened, pin 30 withdrawn by grasping head 31 and latch 34 moved from the upright position of Fig. 5 to the horizontal position of Fig. 6. This allows cams 35 to enter the corresponding groove in stationary cam 36. Rotors 19 can then be lifted out and destroyed if it is desired to prevent their use by unauthorized persons. On if the code is to be changed the rotors can be reinserted in the casing 26 in a different order of their connections 20 changed and the rotors then reinserted in casing 26, pin 30 placed in position, latch 34 raised, and cover 27 closed.

Ed. By.   Friedman   REF ID:A363367   January 1944.

authenticator.   Claims.

A. ↓ 1. In a cryptographing machine, means for insuring the authenticity of the message transmitted, said means comprising, a transposing device for transposing characters from text to cipher or the reverse, a handle connected so as to be operable to move said device into each of its ciphering combinations,

and indicators, one of which is actuated upon each actuation of said handle, which, upon actuation, indicate a selected character.

2.- A plus

B a source of electricity,

~~connected to one side of said source and each~~

C. electric lamps each adapted, when lighted,

to designate one character,

E a multi-contact electric switch connected

into circuit between said ~~source and said~~

lamps and operable to connect said lamps to

~~not connect~~ in various arrangements,

and

D a record switch mechanically arranged so as

to be closed when said multi-contact

switch is operated from one position to another and

connected into circuit between said multi-contact switch

whereby circuit is closed through one lamp which

gives an authenticating signal.

3. Claim 2 omitting "and" plus - and

H a third switch connected in series with said

record switch and said source so as to control

the connections therebetween.

and the other side of said source

Elwood Friedman. 7 January 1944.

REEL/FID:A363367

4. A, B, C, plus -

E a multi-contact electric switch connected into circuit between said ~~source and said~~ lamps and operable to connect said lamps in pairs, ~~across said battery~~, and

F a normally-closed electric switch connected between said source and each of said lamps the other side of so as to control the connection therebetween and mechanically arranged so as to be opened when said multi-contact switch is operated from one position to another.

5. Claim 4 omitting "and" plus -, P.

6. A, B, C, plus - ~~normally open~~ manually operable switches, each connected between the other side of said source and one of said lamps.

6 A B C - plus

G manually operable, normally open electric switches, each connected between the other side of said source and one of said lamps, whereby, when one of said manually operable switches is closed, circuit is established through the lamp to which it is adjacent and through said multi-contact switch and another of said lamps to indicate a letter character, E, and, D.

7. Claim 6, omitting "and" plus, and a normally closed electric switch connected between the other side of said source and each of said manually operable switches and mechanically arranged so as to be opened when said multi-contact switch is moved from one position to another.

REF ID:A363367

Ellsberg.

8 January 1944.

8. A coding device comprising,
a panel having a plurality of electric-switch-operating handles projecting therethrough, a plurality of electric switches each operated by one of said handles,
a plurality of electric lights each associated with one of said handles and each carrying character-indicating indicia thereon,
a plurality of cryptographing rotors having stationary contacts each connected to one of said lights and bridging contacts connecting said lights in pairs,
an operator having a lost-motion connection with said rotors to move said rotors step-by-step,
a normally-closed electric switch in series with each of said handle-operated switches and a source of current,
and
a normally-open electric switch in series with one of the stationary contacts of said rotors and said source of current.

(over)

said operator acting to open said normally-closed switch and to close said normally-open switch upon each step in the movement of said rotors.

9. Claim 8 omitting "and" thus - and a counter connected under the control of said operator so as to indicate the number of actuations of said rotors.

REF ID:A363367

2213 Gp.

17 January 1943.

Friedman: Claims.

10. In a cryptographing machine having relatively rotary electric switches therein, means for manually rotating said switches individually so as to vary the connections therebetween, said means comprising, a finger piece arranged for manual operation, a pivotally mounted stirrup located under the control of said finger piece, and a plurality of cam-and-pawl devices pivotally mounted on said stirrup and each stressed against a cam surface on one of said switches and arranged to enter one ratchet opening on said switch when not restrained by said cam surface and movable together with said stirrup to turn said switch.

11. The [illegible] 10 omitting "and" "then add-and tangs on all but one of said devices, said tangs each overlying the preceding device whereby one of said devices is operative at each actuation of said finger piece, and each successive device can become operative only when it is permitted to do so by the cam surface which controls it and by all the preceding devices.

12. In a cryptographing machine containing a number of rotors a latch for steering said rotors in position comprising a U-shaped member of spring material having

(over)

REF ID:A363367

12 (cont.) one end pivotally mounted and the other end free for longitudinal movement into and out of contact with the end one of said rods, a cam surface on said free end, and a stationary cam co-operating with said cam surface to move said free end when said latch is turned about its pivot.

This invention relates to a device or machine for enciphering and deciphering communications which are to be transmitted secretly in coded or cryptographic form.

Among the objects of this invention are to provide a cipher device which is simple yet affords a high degree of security, is light and readily portable, and can be readily disassembled and rearranged to vary the code or deranged or destroyed to prevent its use by unauthorized persons.

Another object of this invention is to provide an authenticator or means for indicating that a message, which is to be decoded, has originated at an authorized source.

Other objects of the invention will become apparent as this description proceeds.

In the drawings,

Fig. 1 is a top or plan view with the covers closed.

Fig. 2 is a top or plan view on an enlarged scale with the keyboard cover and parts of the rotor cover omitted.

Fig. 3 is a side elevation with the covers closed.

Fig. 4 is a cross section on line 4-4 of Fig. 2 with the rotor cover omitted.

Fig. 5 is a perspective view of the rotor latch.

Fig. 6 is a perspective view of the rotor actuating mechanism.

Fig. 7 is a diagram showing schematically the electric circuits and the mechanical operating mechanisms.

That embodiment of the invention selected from among others for illustration in the drawings and description in the specification is as follows. Referring to Fig. 7, the device will be seen, in general, to consist of a source 10 of electricity, shown as a pair of dry cells, connected to a pair of wires 11 and 12 across which are connected a plurality (in this instance, twenty-six) indicators 13A, 13B, 13C, etc. These indicators are illustrated as being electric lamps arranged beneath a keyboard 14 (see Fig. 2) and each arranged to illuminate one perforation closed by a transparent cover 15 bearing one letter 16 of the alphabet thereon. Across lines 11 and 12 are also connected manually operable switches 17A, 17B, 17C, etc., each in series with one of the indicators 13A, 13B, etc., and each arranged for operation by a pushbutton or handle 18 projecting through keyboard 14 along side of one of the covers 15.

Connected to each of the indicators 13A, 13B, etc., is a multi-contact electric switch, generally indicated as 19. It comprises a number of relatively turnable cryptographic rotors, 19A ——— 19E, each having a plurality of contacts thereon and connections between pairs of the contacts as shown diagrammatically at 20. Each connection 20 leads from one stationary contact through the cryptographic rotors to another stationary contact. These connections 20 are rearranged each time one of the rotors is turned.

In lead wire 11 is connected a normally-closed electric switch 21. Between one of the indicators, in this case 13E, and multi-contact switch 19 is connected normally-closed electric switch 22. In parallel with wire 11 is wire 11A containing an authenticating switch 23 having an operating handle 24. Wire 11A also contains a normally-open switch 25.

Turning now to Figs. 1, 2 and 3 for a disclosure of the mechanical features of the invention, the device is shown as enclosed in a casing 26 to which are hinged or otherwise attached a rotor cover 27 and a keyboard cover 28. Casing 26 has an opening 29 through the top by means of which a counter

30 is visible. As is most readily seen in Fig. 6, casing 26 has two projecting walls 26A and 26B. The cryptographic rotors 19 are retained between these walls by mechanism which will now be described. Wall 26A has a hole in it through which may be pushed pin 30A having a knurled head 31 and a latch 32 co-operating with a retaining spring 33. Also pivoted on wall 26A is a spring latch 34 of U-shape being bent parallel to itself. The free end 34A of latch 34 is perforated to allow pin 30A to pass through it and bears cam surfaces 35 thereon. Stationary cam 36 has a surface complementary to cam surfaces 35 so that when latch 34 is moved from the substantially horizontal position, in which it is shown in Figs. 2, 4, and 6, into the vertical position, in which it is shown in Fig. 5, the free end 34A of latch 34 is moved away from wall 26A and compresses the spring contacts 20A (see Fig. 2) of rotors 19 and locates the rotors themselves in desired positions. The manually operated means for rotating the cryptographic rotors 19 will next be refered to. As seen in Fig. 1, 2, 3, and 6, casing 26 has a recess 37 in its top into which fits a finger piece 38 having a sliding fit in the recesses and mounted on a rod 39. Rod 39 causes U-shaped stirrup 40 to turn about its pivots in walls 26A and 26B. Stirrup 40 carries as a part cam 41 which actuates follower 42 fast on shaft 43 of counter 30. Stirrup 40 also has a part 44 to which spring 45 is attached and which carries cam face 46. Detent 47 is pivoted at 48 in walls 26A and 26B and is stressed by spring 49 so that cam 50 engages cam face 46. Spring detents 60 normally hold rotors 19 in their relative positions but allows movement of these rotors under the actuation of pawls 58. This permits detent teeth 51 to be moved in and out of the ratchet depressions in the surface of the rotors 19. Stirrup 40 carries a pin 52 on which are pivoted a plurality of cam-and-pawl devices 53A, 53B, 53C, and 53D which are urged by springs 54 against cam surfaces 57 or ratchet depressions 56 (see Fig. 7) on rotors 19. Device 53A for example, has a cam surface 55 and a pawl 58 cooperating, respectively,

with cam surface 57 and ratchet recesses 56 on the rotor 19A. A tang 59 of device 53A overlies device 53B so that device 53B prevents device 53A from operating unless device 53B is also depressed and operating.

The operation of this device is as follows: For coding or decoding handle 24 is located so that switch 23 is open. That push button 18 which is associated with the desired letter is depressed and the switch controlled thereby is operated. For example if switch 17E representing the letter E is closed, connections are made from battery 10 through line 11, switch 21 and switch 17E through lamp 13E, and line 12 back to source 10. This action also closes connections from switch 17E through switch 22 and connections 20 or rotors 19 to lamp 13Z and thence through line 12 back to source 10. Lamps 13E and 13Z are therefore simultaneously lighted and thus indicate that E is to be encoded or decoded as the case may be, as Z and vice versa. Since rotors 19 connect all the lamps 13A, 13B, etc., together in pairs each letter has another corresponding to it.

For rotating the cryptographic rotors 19 and thus varying the connections between the various pairs of lamps, finger-piece 38 is depressed, stirrup 40 is rotated, about its pivots and the devices 53A etc., moved. Whenever one of the cam faces 55 encounters a depression (shown at 55D in Fig. 4) in the corresponding cam 57 the device 53 is moved by spring 54 so that the pawl 58 enters the ratchet depression 56 unless prevented from doing so by the engagement of the tang 59 with the next device 53. Whenever a pawl 58 enters a ratchet depression 56, and the movement of the finger-piece 38 is completed, the corresponding rotor 19 is moved one step. This rearranges the connections 20 through the rotors and connects different pairs of lamps 13A, etc., together. Counter 30 is moved one numeral because follower 42 is depressed by cam 41 and spring returned. Detent 47 prevents backward movement of rotors 19 because teeth 51 enter depressions in rotors 19.

For insuring the authenticating of a message, switch 23 is closed by snapping handle 24. Finger-piece 38 is then depressed, opening switches 21

and 22 and closing switch 25. This movement moves counter 30 one position and also one or more rotors 19 one step. Circuit is closed from sources 10, line 11, line 11A, switch 23, switch 25, rotor connections 20 to whichever lamp happens to be paired with lamp 13E. Circuit to lamp 13E is open at switch 22. The designation letter of the lamp which is paired with 13E is transmitted as an authenticator, an agreement having been previously reached by the two parties concerned as to the wiring of the several rotors, their arrangement in the device, and the number of steps having been taken as indicated by counter 30.

To readily remove the rotors 19, cover 27 is opened, latch 34 moved from the upright position of Fig. 5 to the horizontal position of Fig. 6, and pin 30 withdrawn by grasping head 31. This allows cam 35 to enter the corresponding groove in stationary cam 36. Rotors 19 can then be lifted out and destroyed if it is desired to prevent their use by unauthorized persons. Or if the code is to be changed the rotors can be reinserted in the casing 26 in a different order or their connections 20 changed and the rotors then inserted in casing 26, pin 30 placed in position, latch 34 raised, and cover 27 closed.

1. In a cryptographing machine, means for insuring the authenticity of the message transmitted, said means comprising, a transposing device for transposing characters from text to cipher or the reverse, a finger piece connected so as to be operable to move said device into each of its ciphering combinations, and indicators, one of which is actuated upon each actuation of said finger piece, and which upon actuation, indicates a selected character.

2. In a cryptographing machine, means for insuring the authenticity of the message transmitted, said means comprising, a source of electricity, electric lamps each connected to one side of said source and each adapted, when lighted, to designate one character, a multi-contact electric switch connected into circuit between said lamps and operable to connect said lamps in various arrangements, and a second switch mechanically arranged so as to be closed when said multi-contact switch is operated from one position to another and to be connected into circuit between said multi-contact switch and the other side of said source whereby circuit is closed through one lamp which gives an authenticating signal.

3. In a cryptographing machine, means for insuring the authenticity of the message transmitted, said means comprising, a source of electricity, electric lamps each connected to one side of said source and each adapted, when lighted, to designate one character, a multi-contact electric switch connected into circuit between said lamps and operable to connect said lamps in various arrangements, a second switch mechanically arranged so as to be closed when said multi-contact switch is operated from one position to another and connected into circuit between said multi-contact switch and the other side of said source, whereby circuit is closed through one lamp, which gives an authenticating signal, and a third switch connected in series with said second switch and said source so as to control the connections therebetween.

4. In a cryptographing machine, means for insuring the authenticity of the message transmitted, said means comprising, a source of electricity, electric lamps each connected to one side of said source and each adapted, when lighted, to designate one character, a multipcontact electric switch connected into circuit between said lamps and operable to connect said lamps in various arrangements, and a normally-closed electric switch connected between the other side of said source and each of said lamps so as to control the connection therebetween and mechanically arranged so as to be opened when said multi-contact switch is operated from one position to another.

5. In a cryptographing machine, means for insuring the authenticity of the message transmitted, said means comprising, a source of electricity, electric lamps each connected to one side of said source and each adapted, when lighted, to designate one character, a multi-contact electric switch connected into circuit between said lamps and operable to connect said lamps in various arrangements, a second switch mechanically arranged so as to be closed when said multi-contact switch is operated from one position to another and connected into circuit between said multi-contact switch and the other side of said source, whereby circuit is closed through one lamp which gives an authenticating signal, a third switch connected in series with said second switch and said source so as to control the connections therebetween.

6. In a cryptographing machine, means for insuring the authenticity of the message transmitted, said means comprising, a source of electricity, electric lamps each connected to one side of said source and each adapted, when lighted, to designate one character, a multi-contact electric switch connected into circuit between said lamps and operable to connect said lamps in pairs, manually operable, normally open electric switches, each connected between the other side of said source and one of said lamps, whereby, when one of said manually operable switches is closed, circuit is established through the lamp to which it is adjacent and through said multi-contact switch and another of said lamps to indicate a cipher character, a normally-closed

electric switch connected between the other side of said source and each of said lamps so as to control the connection therebetween and mechanically arranged so as to be opened when said multi-contact switch is operated from one position to another and a second switch mechanically arranged so as to be closed when said multi-contact switch is operated from one position to another and connected into circuit between said multi-contact switch, and the other side of said source, whereby circuit is closed through one lamp, which gives an authenticating signal.

7. In a cryptographing machine, means for insuring the authenticity of the message transmitted, said means comprising, a source of electricity, electric lamps each connected to one side of said source and each adapted, when lighted, to designate one character, a multi-contact electric switch connected into circuit between said lamps and operable to connect said lamps in various arrangements, manually operable, normally open electric switches, each connected between the other side of said source and one of said lamps, whereby, when one of said manually operable switches is closed, circuit is established through the lamp to which it is adjacent and through said multi-contact switch and another of said lamps to indicate a cipher character, a normally-closed electric switch connected between the other side of said source and each of said lamps so as to control the connection therebetween and mechanically arranged so as to be opened when said multi-contact switch is operated from one position to another, a second switch mechanically arranged so as to be closed when said multi-contact switch is operated from one position to another and connected into circuit between said multi-contact switch and the other side of said source, whereby circuit is closed through one lamp, which gives an authenticating signal, and a third electric switch connected on series with said second switch and said source so as to control the connection therebetween.

8. A coding device comprising, a panel having a plurality of electric-

switch-operating handles projecting therethrough, a plurality of electric switches each operated by one of said handles, a plurality of electric lights each associated with one of said handles and with a character-indicating indicia, a plurality of cryptographing rotors having stationary contacts each connected to one of said lights and having bridging contacts connecting said lights in pairs, an operator having a lost-motion connection with said rotors to move said rotors step-by-step, a source of current, a normally-closed electric switch in series with each of said handle-operated switches and said source of current, and a normally open electric switch in series with one of the stationary contacts of said rotors and said source of current, said operator acting to open said normally closed switch and to close said normally-open switch upon each step in the movement of said rotors.

9. A coding device comprising, a panel having a plurality of electric-switch-operating handles projecting therethrough, a plurality of electric switches each operated by one of said handles, a plurality of electric lights each associated with one of said handles and with a character-indicating indicia, a plurality of cryptographing rotors having stationary contacts each connected to one of said lights and bridging contacts connecting said lights in pairs, an operator having a lost-motion connection with said rotors to move said rotors step-by-step, a source of current, a normally-closed electric switch in series with each of said handle-operated switches and said source of current, a normally-open electric switch in series with one of the stationary contacts of said rotors and said source of current, said operator acting to open said normally-closed switch and to close said normally-open switch upon each step in the movement of said rotors, and a counter connected under the control of said operator so as to indicate the number of actuations of said rotors.

10. In a cryptographing machine having relatively rotary electric switches therein, means for manually rotating said switches individually so as to vary the connections therebetween, said means comprising, a finger piece arranged for

manual operation, a pivotally mounted stirrup located under the control of said finger piece, and a plurality of cam and pawl devices pivotally mounted on said stirrup and each stressed against a cam surface on one of said switches and arranged to enter one ratchet opening on said switch when not restrained by said cam surface and movable together with said stirrup to turn said switch.

11. In cryptographing machine having relatively rotary electric switches therein, means for manually rotating said switches individually so as to vary the connections therebetween, said means comprising, a finger piece arranged for manual operation, a pivotally mounted stirrup located under the control of said finger piece, a plurality of cam-and-pawl devices pivotally mounted on said stirrup and each stressed against a cam surface on one of said switches and arranged to enter one ratchet opening on said switch when not restrained by said cam surface and movable together with said stirrup to turn said switch and tangs on all but one of said devices, said tangs each overlying the preceding device whereby one of said device is operative at each actuation of said finger piece, and each successive device can become operative only when it is permitted to do so by the cam surface which controls it and by all the preceeding devices.

12. In a cryptographing machine containing a number of rotors, a latch for stressing said rotors in position comprising, a U-shaped member of spring material having one end pivotally mounted and the other end free for longitudinal movement into and out of contact with the end one of said rotors, a cam surface on said free end, and a stationary cam co-operating with said cam surface to move said free end when said latch is turned about its pivot.

13. A cryptographing, coding or ciphering machine substantially as shown and described.