Patented Dec. 13, 1938

2,139,676

UNITED STATES PATENT OFFICE

2,139,676

CRYPTOGRAPHIC APPARATUS

William F. Friedman, Washington, D. C.

Application August 4, 1937, Serial No. 157,383

18 Claims. (Cl. 35—4)

(Granted under the act of March 3, 1883, as amended April 30, 1928; 370 O. G. 757)

The invention described herein may be manufactured and used by or for the Government for governmental purposes, without the payment to me of any royalty thereon.

This invention relates to cryptographic apparatus for automatically enciphering and deciphering messages.

An object of the invention is the provision of a cryptograph with a keyboard for high-speed manual operation, a bank of indicating devices or electro-magnets for noting or recording the cipher symbols of the messages as the latter are being enciphered, and for noting or recording the plain-text letters as the messages are being deciphered; and certain ciphering mechanisms interposed between the keyboard and the bank of indicating devices or electro-magnets for constantly changing the relationship between the message characters and the cipher symbols. The invention is primarily concerned only with the ciphering mechanism referred to above, which is of simple design but nevertheless yields cryptograms of great security. This ciphering mechanism employs means which are novel in the cryptographic art in that it involves operation along a time axis, and the exact cryptographic results are dependent upon a time factor which is constantly changing in an irregular manner.

The invention is described in connection with the accompanying drawings, in which:

Fig. 1 is a diagrammatic representation of the parts of the mechanism together with certain circuit arrangements;

Fig. 2 is a diagrammatic representation of means for imparting uniqueness to messages even when the latter are enciphered by the same keying sequence;

Fig. 3 is a diagrammatic representation of the electrical circuits applicable to the system shown in Fig. 2; and

Fig. 4 shows an alternative scheme for one of the basic elements of the mechanism shown in Fig. 1.

Referring to Fig. 1, the principal elements consist of a keyboard **1**, a bank of indicating devices **2**, a rotating cipher commutator hereinafter called a rotor **3**, a distributor **4**, a cam-wheel mechanism **5** for producing a cipher key, a permutation-translation mechanism hereinafter called a translator **6**, and a switchboard **7**.

According to the present invention, means are provided whereby the individual alphabets of a set of twenty-six or more mixed cipher alphabets are caused to present themselves for ciphering purposes in a fixed sequence and this sequence is regularly repeated. When a key on the keyboard is depressed only one of these cipher alphabets, however, is selected during one complete presentation of the sequence of alphabets and the cipher resultant obtained depends upon the cipher alphabet that has been selected. This selection is varied according to a very long cipher key.

Broadly speaking, the foregoing cryptographic operation is accomplished in practicing the invention in the following manner:—

The rotor **3** serves as switching means for changing the whole set of twenty-six connections between the keyboard **1** and the bank of indicating devices **2**. The rotor is caused to rotate with a constant angular velocity by the motor **93**, and the time required for the rotor to make one complete revolution will hereinafter be referred to as the operating cycle. Assuming a system employing twenty-six elements (to correspond with the twenty-six letters of the English alphabet) rotor **3**, in making a complete revolution will pass through twenty-six angular positions, each consuming $\frac{1}{26}$ of the time required for the rotor to complete one operating cycle. The operating cycle may therefore be regarded as being subdivided into twenty-six equal time-intervals during which a letter may be enciphered by the cryptograph. To each of these time-intervals or angular positions of the rotor, there corresponds a cipher alphabet, that is, a set of connections between the keyboard and the bank of indicating devices. Coordinated with the rotor is the distributor **4**, whose brush arm **16** causes brush **73** to sweep over the twenty-six equal segments of the face of the distributor synchronously with the rotation of the rotor. The distributor cooperates with the keying mechanism to determine which of the cipher alphabets will be selected, that is, which of the twenty-six angular positions of the rotor, or which of the twenty-six time-intervals, will be the one selected during a specific operating cycle for enciphering (or deciphering) a letter. This selection in each case varies with the successive operating cycles according to a cipher key which is produced by the cam-wheel cipher-key mechanism **5**. Each different one of the twenty-six time-intervals will yield a different resultant for the same letter; therefore there are twenty-six different resultants possible for each letter. Within the operating cycle, when a key of the keyboard is depressed, the letter corresponding to this key is enciphered (or deciphered) by that one of the

cipher alphabets which was selected in the aforesaid manner. Arrangements are made for locking up the keyboard so that when a key is depressed not only will the associated keyboard contact be closed but also it will remain closed for one whole operating cycle and no other key can be depressed during that same cycle. Thus, keyboard operation may be regarded as being rhythmic in character and may be performed with a cadence similar to that in teletype operation. The operation of the keyboard results in the action of the responsive indicating devices **2**, which may print the characters produced by the ciphering operation in a rhythmic manner. But it is obvious that this cadence does not have to be reproduced identically by the operator who is to decipher messages for the cadence is not at all an essential part of the functioning of the apparatus. In fact, if a clutch mechanism were provided whereby the rotor and the distributor would only be started consequent upon the depression of any key of the keyboard, and would be stopped automatically at the end of the operating cycle, then for each depression of the key the rotor and the distributor brush arm would start, would make one complete revolution, the letter would be enciphered (or deciphered) and upon completion of the revolution both the rotor and the distributor brush arm would stop. Thus, no cadence in keyboard operation would be required, and operating speed would only be limited by practical considerations. The foregoing apparatus and its operation will now be described in detail.

The keyboard **1**, comprising 26 characters equivalent to the letters of the alphabet, has a corresponding number of contacts of which only two are shown as at 10 and 11, corresponding to the letters E and Q, respectively. The bank of indicating devices **2** may take the form of glow lamps which are illuminated when current passes through them but a preferred embodiment is to have the indicating devices take the form of electro-magnets or solenoids which operate the keys of a recording typewriter, so that a printed record of the enciphered or deciphered message may be made.

The rotor **3** is a cipher-commutator wheel of form now well known in the cryptographic art. It is mounted on a rotatable shaft **12**. Pressing against rotor **3** are two stators, a left-hand stator **13** and a right-hand stator **14**, each provided with a ring of 26 ball-bearing and spring contacts insulated from one another and exerting a slight pressure against the face of rotor **3**. A motor **93**, drawing power from source **94**, drives the shaft **12** and thus the rotor **3** at a constant speed between the stator **13** and **14**. The rotor is made of Bakelite or similar insulating material and consists of two faces, a left-hand face and a right-hand face each face bearing a ring of 26 contact surfaces A, B, C, . . . Z, equidistantly spaced from one another circumferentially on the outer face. Insulated conductors passing through the rotor connect the 26 contact surfaces of the left face to those of the right face, in a manner which is reciprocal in pairs. That is, if A on the left face is connected to X on the right face, then X on the left face is connected to A on the right face. Thus, with 13 paired contacts reciprocity in the enciphering-deciphering relationship is obtained without special switching arrangements therefor.

The distributor **4** consists of a set of 26 equal-area segments or contact surfaces **15**, insulated from one another and distributed circumferentially on the face of the distributor. A brush arm **16**, on the same shaft **12** as the rotor **3**, sweeps over the face of the distributor **4** at a constant rate of speed synchronous with that of the rotor **3**. The rotor **3** and brush arm **16** are keyed to the shaft **12** so that these two elements are always in a fixed angular relationship with respect to the shaft **12** and cannot be angularly displaced relative to each other, due to slippage on the shaft. Arrangements may be made, however, to change the relative angular positions of the rotor and the brush arm if desired. Brush arm **16** terminates in a brush **73** which sweeps over distributor segments **15** and establishes momentary contact with each of the latter successively. Distributor segments **15** are connected to the right-hand set of terminals **72** of switchboard **7** by a set of conductors **17**, of which only a few are shown.

The cam-wheel cipher-key mechanism **5** provides a long cipher key for cryptographic purposes. It consists of five or a multiple of five cam-bearing wheels **21**, **22**, **23**, **24**, **25** of different diameters. The periphery of each wheel is divided up into equal segments to which projecting lugs serving to act as cams may be attached or into which cams may be inserted; the numbers of segments on the different wheels are preferably prime to one another. For example, wheel **21** may have 100 segments, wheel **22** may have 99, wheel **23** may have 97, wheel **24** may have 91, and wheel **25** may have 89. Fixed to these wheels are ratchets **26**, **27**, **28**, **29**, **30**. The number of teeth in each ratchet **26** to **30** corresponds with the number of segments in the cam-bearing wheel with which the ratchet is associated. Pawls **31**, **32**, **33**, **34**, **35** on a rocker arm **36**, which is operated by magnets **37**, **38**, drive the cam-bearing wheels in a stepwise manner, under control of a universal bar key-board contact **39** through power source **40**. Each time a key is depressed rocker arm **36** and the pawls **31** to **35** serve to step wheels **21** to **25** forward one interval. The cams on the peripheries of the cam-bearing wheels **21** to **25** control contact levers **41**, **42**, **43**, **44**, **45** and the latter operate contacts associated therewith, **141**, **142**, **143**, **144**, and **145**. It will be understood that the segments on the periphery of each wheel **21** to **25** are smooth surfaces except where a cam is inserted in or affixed to the segment and each wheel may have a cam inserted in any number of the slotted segments. Contact levers **41** to **45** are therefore raised and their associated contacts **141** to **145** are closed only when cams are presented to them by the progressive movement of the wheels **21** to **25**. Furthermore these contact levers **41** to **45** will be operated in permutative groupings so that all 32 possible Baudot-code combinations may be set up by the contacts **141** to **145**, for keying purposes. Contacts **141** to **145** are connected to conductors **46** to **50** and control magnets **51** to **55**, the function of which will be described presently. Now since the cam-bearing wheels **21** to **25** are of different diameters and they all step forward one step for each depression of a key on the key-board **1**, if these wheels are initially aligned at a bench mark so as to correspond to a cipher key, this initial alignment will recur only after $100\times99\times97\times91\times89$ or 7,777,469,700 letters have been enciphered (or deciphered). Thus a cipher key of great length is made available for cryptographic purposes.

The translator **6** is an instrumentality well

known in the art of printing telegraphy. It consists of a set of five translator bars 61 to 65 which are normally held in position by the retractile springs 56 to 60. The translator bars are slotted according to the requirements of the Baudot or 5-unit printing telegraph code, so that 32 different alignments of slots may be presented to a set of 32 stunt bars labeled 66. Only one stunt bar can drop into a specific alignment of slots and when this occurs a contact associated with the selected stunt bar is closed. Several of these contacts are shown at 67, it being obvious that there are 32 such contacts in all. These contacts 67 are connected to conductors 68 which lead to the set of 32 terminals 69 of switchboard 7.

It will now become clear that the cam-wheel cipher-key mechanism 5 serves merely to select one out of 32 circuits leading to the terminals 69 of switchboard 7 and that this selection, being quite variable and depending upon the successive permutations set up by the cam-wheel mechanism 5, thus produces a long, variable sequence of keying circuits corresponding to keying characters and hereinafter referred to as the keying sequence.

The 32 terminals 69 of switchboard 7 are connected to a corresponding number of flexible conductors 70, and the latter terminate in jacks, which may be inserted into plugs 71 connected to terminals 72 on the other side of switch 7. There are but 26 such plugs 71 and each of them has a pair of holes for receiving jacks, but only six of these double-hole plugs will have both holes occupied by jacks. By this arrangement the 32 possible resultant keying circuits set up by translator 6 are reduced to 26, of which six will be "double-effects", that is, in six cases the same keying character may be brought about by two different Baudot permutations set up by the translator 6. Which six keying circuits these will be depends upon the way in which the flexible conductors 70 are connected to plugs 71 at any given time. It will be seen later that no ambiguity is occasioned by the presence of a keying circuit which is of the double-effect type.

Still referring to Fig. 1, the electrical circuit for cryptographic functioning will now be described. It will be seen that the circuit from power source 18 to the keyboard 1 must pass through contact 19, which is controlled by main relay 8. Hence, depression of any key of keyboard 1 during the time contact 19 remains open will produce no effect since no power is being delivered to the key board 1 and hence no circuit to the bank of indicating devices 2 is established. Let us see now upon what circumstance closure of contact 19 depends; in other words, let us see when main relay 8 will be energized. Let us consider a specific operating cycle x in the long sequence of operating cycles n. During this operating cycle brush arm 16 of distributor 4 will make a complete revolution and a corresponding complete revolution of the cipher commutator or rotor 3, will take place. This operating cycle x may be regarded as being divided up into 26 equal time-intervals of very short duration, each corresponding to a specific angular position of the brush arm 16 and of rotor 3 in the circumferences through which these two elements are in motion. The circuit for relay 8 includes brush 73, brush arm 16, and one of the 26 segments 15 of distributor 4. Which of the 26 segments 15 of distributor 4 will be "alive", that is, connected to power source 20 during operating cycle x depends upon the wiring at switchboard 7 and upon the particular contact of the set of 32 contacts 67 which happens to be closed during operating cycle x. The latter depends upon the specific permutation of operated and non-operated translator bars 61 to 65 of translator 6, and this depends in turn upon the specific position and composition (as regards cams) of the cam-wheel cipher-key mechanism 5. Let us assume that during this specific operating cycle x the segment designated 74 in Fig. 1 is the one which is "alive". A circuit is completed as follows: power source 20, conductor 75, main relay 8, conductor 76, armature 77 and back contact 78 of relay 9, conductor 79, brush arm 16 and brush 73 of distributor 4; the brush then being on segment 74 the current continues through segment 74, conductor 80, to one of the contacts 72 of switchboard 7, and thence through the switchboard along one of the flexible conductors 70 to one of the contacts 69 on the other side of the switchboard, thence along one of the conductors 68 to that one of the contacts 67 which is closed by the selected stunt bar 66 of translator 6, finally along common return conductor 81, back to power source 20. Relay 8 is energized at the instant that brush 73 is passing over live segment 74, and since rotor 3 revolves synchronously with brush arm 16, the angular position of rotor 3 with respect to its stators 13 and 14 corresponds to the angular position of brush arm 16 at that instant. The cipher resultant produced by depressing a key on key-board 1 will be determined by the angular position of rotor 3. The reason for this is that since rotor 3 has 26 ciphering positions each yielding a completely different set of cipher resultants for the 26 character keys of keyboard 1, the specific cipher resultant for a specific keyboard character enciphered within a specific operating cycle x depends upon the specific segment of distributor 4 which is alive during that cycle.

The circuit through the keyboard 1, the rotor 3 and the bank of indicating devices 2 will now be described. When a key 10 corresponding to the letter "E" is depressed during operating cycle x, nothing happens until brush 73 reaches segment 74 of distributor 4, for the keyboard remains "dead" until that moment. The instant that relay 8 is energized, current is delivered from power source 18 through closed contact 19 and armature 82 of relay 8, along conductor 83 to the contacts of keyboard 1. Since contact 10 is closed, the current continues along conductor 84 to a contact on stator 13, thence through the rotor 3, which is at that instant in an angular position corresponding to that of brush arm 16, to a contact 86 on right stator 14, thence along conductor 87 to indicating device or solenoid 88, which corresponds (in this figure) to letter "Q" thence along conductor 90 through slow acting relay 9, finally along conductor 91 back to power source 18. Solenoid 88 is actuated (or if lamps are used a lamp is lighted) to indicate the cipher resultant "Q" for plain-text letter "E".

When slow-acting relay 9 is energized the circuit for main relay 8 is broken at 78 when armature 77 is withdrawn. A mechanically controlled trip 92 engages lever 77 and holds it away from contact 78 until the universal bar on keyboard 1 returns to normal when the key is released, whereupon lever 77 is allowed to fall back and close 78. The purpose of this arrangement is to insure that not more than one letter will be indicated or printed per operating cycle, that is, per depression of a key on the keyboard.

When the universal bar on the keyboard 1 reaches the end of its downward stroke it closes contact 39, which controls the circuit to magnets 37 and 38. Rocker arm 36 is operated, causing pawls 31 to 35 to engage ratchets 26 to 30 and advancing cam-bearing wheels 21 to 25 one step forward to the next position, setting up a new Baudot permutation of contact-levers 41 to 45, associated contacts 141 to 145, and magnets 51 to 55. A new keying character is thus established by translater 6 and the system is now ready for the next operating cycle. Even if the same key is depressed on the keyboard the equivalent produced at the bank of indicating devices will be different, unless the keying character happens accidentally to be the same as before. Continued depression of the same key will produce a varying sequence of equivalents corresponding in length with the length of the keying sequence produced by the cam-wheel mechanism 5. This latter sequence is of great length, as has already been explained, being the resultant of the interaction of five wheels of different diameters with different numbers of teeth, these numbers being prime to one another.

Since the connections within the rotor 3 are reciprocal in pairs, as explained, the decipherment of a message takes place by resetting the wheels of cam-wheel mechanism 5 to the initial key position, and operating the keyboard 1 to correspond with the cipher letters, whereupon the plain-text equivalents will be produced at the bank of indicating devices 2.

The mechanism shown in Fig. 1 and described in the foregoing terms is such, however, that if several messages are enciphered by the same keying sequence they will be in the same series of cipher alphabets, and in this case there exists a possibility of a solution by cryptanalytic procedure. To explain what is meant by these statements it is necessary to call attention to the fact that the cipher commutator 3 provides a set of 26 cipher alphabets and that basically the cryptographic principle of the system as described is one in which the individual alphabets of this set of 26 cipher alphabets are brought into play in an order determined by the keying sequence set up by the cam-wheels. For example, suppose we consider this keying sequence to be such that for a given key as set up on the cam-wheels the first 20 alphabets to be brought into play are alphabet numbers 16, 4, 19, 26, 15, 3, 18, 21, 12, 6, 1, 18, 22, 7, 13, 17, 26, 2, 18, 24. Now if several messages start with the same initial cam-wheel setting, the successive letters of all these messages will be in the same sequence of cipher alphabets, and therefore the several messages may be superimposed, yielding columns of letters which are monoalphabetic in composition. Or, even if the messages do not start at exactly the same point in the keying sequence, but portions of these messages overlap one another with respect to the keying sequence, then the overlapping portions which are in the same alphabets, may be superimposed. For example, using the same sequence of alphabet numbers mentioned above, suppose a first message begins with alphabet number 16, a second message, with alphabet 4, a third one, with alphabet 19, and so on, it is merely necessary to shift the second message one letter to the right of the first, shift the third message one letter to the right of the second, and then all three messages will be properly superimposed with respect to the keying sequence; the letters in columns are now in the same cipher alphabets, and the messages are susceptible of solution by monoalphabetic principles. The proper points for superimposition can be ascertained even without a knowledge of the particular key settings for these three messages, from a detailed study of the repetitions between messages. It is necessary, therefore, in order to circumvent this possibility of superimposing messages or parts thereof so that they will be in the same keying sequence, to impart a cryptographic uniqueness to the messages so as to destroy, mask, or suppress repetitions brought about by the chance encipherment of identical words by identical sequences of alphabets.

Mechanism for accomplishing this is shown in Fig. 2. Here the shaft 121 carries several cipher commutators or rotors, 3*a*, 3*b*, 3*c*, 3*d*, and 3*e*. These rotors are separated from one another by stators 122, 123, 124, 125, each carrying rings of contacts on both faces, to provide for continuity of circuit from one rotor into the next. The contacts in these stators, as are those in stators 13 and 14, already described, are ball-bearing spring contacts and they press against the rotors so as to hold each rotor in place, and keep it from rotating on the shaft 12, except when rotatory motion is imparted to it by means to be described. The periphery of each rotor 3*a* to 3*e* bears a collar 215 in which 26 gear teeth have been cut so as to engage with gear wheels 213 and 214 which are mounted on shaft 12, the latter now corresponding to shaft 12 of Fig. 1. Gear wheels 213 and 214 can be independently slid sidewise along the shaft 12 and keyed into position on the shaft, by means not shown, so as to engage the toothed collars of any two of the five rotors 3*a* to 3*e*, at the will of the operator. Gear wheels 213 and 214 have 26 teeth and their pitch is the same as those on the collars of rotors 3*a* and 3*e*, so that the motion imparted to a rotor by wheel 213 or wheel 214 is a 1:1 drive. The shaft 12 is rotated by motor 93, as in Fig. 1; the distributor 4 of Fig. 2 is the distributor similarly numbered in Fig. 1, with the brush arm 16 and brush 73. Thus, instead of driving one rotor 3, as in Fig. 1, the motor 93 and shaft 12 may drive any two of the five different rotors 3*a* to 3*e*. The function of the distributor 4 and brush arm 16, is now the same as described in connection with Fig. 1, but the rotor that will be associated with these elements is now susceptible of variability.

The rotors 3*a* to 3*e* are to be set to a key, by aligning the letters on their peripheries at a bench mark. Since there are 26 individual rotatory positions of each rotor on the shaft, there are 26^5 different initial settings of these rotors, each such setting providing a different set of 26 paths for the passage of electric currents from the keyboard 1 to the bank of electro-magnets 2. The circuits from the keyboard 1 through the set of rotors 3*a–e* to the bank of solenoids 2 are shown diagrammatically in Fig. 3. In this figure stators 13 and 14, and rotors 3*a* to 3*e* correspond to the similarly designated stators and rotors of Fig. 2. The internal wirings of rotors 3*a*, 3*b*, 3*c*, and 3*d* are not reciprocal in pairs, as is the case with the single rotor 3 of Fig. 1, but are all random connections. The rotor 3*e* is, however, different in its construction from the other rotors, in that it has a ring of contacts on only one face and these contacts are interconnected in pairs. Thus rotor 3*e* serves as a means for reversing a current coming into the set of rotors from a contact in stator 13, passing through rotors 3*a*, 3*b*, 3*c*, 3*d*, and sending it back through rotors 3*d*, 3*c*, 3*b*, 3*a* to another contact in stator 13. Stator 14 now serves no electrical function but merely

as a mechanical bearing against which rotor 3e presses. Relay 8, contact 19, armature 82, and battery 18 correspond to similarly designated elements of Fig. 1. The keys of the keyboard 1 now serve a double function instead of a single function as in Fig. 1. Each key operates a lever which opens one contact and closes another. For instance, when the E key is depressed contact lever 10 is withdrawn from contact 111 and makes contact at 112. When relay 8 is energized a current flows from battery 18, along conductor 83, contact 112, lever 10, conductor 85 to a contact 115 in stator 13, thence through the rotors and back to another contact 116 in stator 13 thence along conductor 84, lever 11, contact 113, solenoid "Q", back to battery 18. Solenoid "Q" is actuated and the cipher resultant of E is Q. In deciphering, assuming that the rotors are in the identical position they were in when enciphering (the cipher key being the same), on depressing the Q key of the keyboard it will be seen that the following reciprocal deciphering circuit is established: Battery 18, conductor 83, contact 114, lever 11, conductor 84, contact 116 in stator 13, through and back through the rotors to contact 115, conductor 85, lever 10, contact 111, solenoid "E", back to battery. Thus, the plain-text resultant of Q is E. In this manner a reciprocal enciphering-deciphering relationship is readily established.

We will now consider the cryptographic operation of the system after the introduction of the foregoing features. The key for a message will now consist of the following elements:

(1) The composition of the cam wheels, (that is, the positions of the cams on the wheels) and their initial setting or alignment at a bench mark; the connections at switchboard 7.

(2) The composition of the rotors, that is their internal wiring; the relative order of rotors 3a, 3b, 3c and 3d on the shaft, and the initial setting or alignment of all the rotors at a bench mark.

(3) The rotors which are selected for engagement with gear wheels 213 and 214.

It becomes obvious that even if two messages are identical, letter for letter, even if they begin at exactly the same point in the keying sequence produced by the cam wheel assembly, and even if gear wheel 213 is engaged with the same rotor, so long as the setting of the rotors 3a to 3e on shaft 121 is different by at least one letter for these two messages, or so long as either of gear wheels 213 and 214 is set to drive different rotors, the cipher texts will be different and externally there will be no sign of the internal identity of the two texts. Furthermore, there is nothing to prevent there being three gear wheels similar to 213 instead of only two, as shown in Fig. 2, in which case three of the five rotors can be driven. And, of course, if there were say 10 rotors it would be possible to have any number up to 9 of such driving gear wheels, thus affording a very wide range for keying purposes. In other words, as now fully developed, the system provides for a multiplicity of keys, such that a uniqueness may be imparted to messages even in the same cam wheel keying sequence, with a correspondingly high degree of cryptographic security.

The translator mechanism 6 in Fig. 1 may be replaced by a system of interconnected contact-levers 96, and associated paired contacts shown schematically in Fig. 4. In the latter figure, the contact levers 41 to 45 and the magnets 51 to 55 are homologous with similarly designated contact levers and magnets of Fig. 1 and serve the same function; the bars 61 to 65 of Fig. 4 are homologous with similarly designated bars of Fig. 1 and serve an equivalent function, viz., to set up, by permuative arrangements of actuated and non-actuated bars, permutative arrangements of contact-levers operating switches to establish one of 32 different circuits to the terminals of switchboard 7. It will be seen that permutative arrangements of the contact-levers as to the left or right positions will result in selecting one of 32 paths for a current flowing from power source 20 to the switchboard 7. The magnets 51 to 55 and their associated bars 61 to 65 may be replaced by multiple-contact relays well known in the art.

Changes, modifications and equivalent arrangements are contemplated within the scope of the invention as defined by the appended claims.

I claim:

1. In a cryptograph, a keyboard comprising a set of character elements, and a corresponding set of signaling elements in operative electrical connection; means including a cipher rotor mechanism for varying the connections between the character elements and the signaling elements, said mechanism having a multiplicity of potential ciphering positions and being driven sequentially and repetitively at a uniform angular velocity through all said positions, each complete revolution of said rotor mechanism constituting a ciphering cycle and each said ciphering cycle corresponding to the time during which a key of the keyboard is depressed; and means for selecting one of said potential ciphering positions to become the operative ciphering position within a ciphering cycle.

2. In a cryptograph, a keyboard comprising a set of character elements, and a corresponding set of signaling elements in operative electrical connection; a cipher rotor mechanism for varying the connections between the character elements and the signaling elements, said rotor mechanism having a multiplicity of potential ciphering positions and being driven sequentially and repetitively at a uniform angular velocity through all said positions, each complete revolution of said rotor mechanism constituting a ciphering cycle and each said ciphering cycle corresponding to the time during which a key of the keyboard is depressed; means for selecting one of said potential ciphering positions to become the operating ciphering position within a ciphering cycle; and means for varying the selection with successive ciphering cycles, the latter corresponding to successive depressions of the keys of the keyboard.

3. In a cryptograph, a keyboard comprising a set of character elements and corresponding contacts electrically associated therewith; an indicating mechanism comprising a set of signaling elements corresponding in number with the number of character elements and in circuit relation therewith; means for establishing and varying the electrical connections between the character elements and the signaling elements, said means including a cipher rotor having therein a set of insulated conductors, said rotor being capable of assuming a multiplicity of potential ciphering positions; means for driving said rotor sequentially and repetitively at a uniform angular velocity through all said ciphering positions; each complete revolution of said rotor constituting a ciphering cycle and each said ciphering cycle corresponding to the time a key of the keyboard is depressed; means for selecting one of

said potential ciphering positions to become the operative ciphering position within a ciphering cycle, said means comprising a distributor mechanism and a brush timed to revolve about the face of said distributor synchronously with said rotor; a circuit including a relay, which when actuated connects the keyboard for operation, said relay being controlled through said circuit in which is included the brush of said distributor mechanism; a translator, and contacts closed by said translator; a set of cam wheels for controlling said translator; and means for angularly displacing the respective cam wheels of said set with successive depressions of the keys of the keyboard.

4. In a cryptograph, a keyboard comprising a set of character elements; an indicating mechanism comprising a set of signaling elements, both sets of elements being in circuit relation; a cipher rotor for establishing a multiplicity of connections between the character elements and the signaling elements; means for driving said rotor sequentially and repetitively through the entire series of such connections, the time required for the rotor to pass through said series of connections corresponding to an operating cycle; a distributor the face of which is divided up into insulated segments corresponding in number with the number of character elements, and having a brush sweeping said segments synchronously with the rotor; a cam wheel mechanism for establishing a cipher key; a translator mechanism for combining the effects of said cam wheel mechanism; a switchboard for reducing the said effects to a number corresponding with the number of character elements; a source of potential; and a relay controlled by the cam wheel mechanism through the intermediacy of said translator mechanism and distributor for the purpose of connecting the keyboard to said source at a selected instant within the operating cycle.

5. In a cryptograph, a keyboard comprising character elements, an indicating mechanism comprising signaling elements, and a cipher rotor for establishing and automatically, rhythmically, and sequentially varying the connections between the character elements and the signaling elements; means for selecting one of a set of said connections during the time a key of the keyboard is depressed; and means for varying the selection with successive depressions of the keys of the keyboard.

6. In a cryptograph, a cam-wheel mechanism for establishing a cipher key sequence consisting of permutations of a plural-unit code; and means for translating the permutations set up in said code by said cam-wheel mechanism into a limited number of single-unit keying characters.

7. In a cryptograph, a cam-wheel mechanism for establishing a cipher key sequence consisting of permutations of a plural-unit code; means for translating the permutations set up in said code by said cam-wheel mechanism into a limited number of single-unit keying characters; and a switchboard for reducing said keying characters to a smaller number.

8. In a cryptograph which employs a translator assembly having permutation bars and stunt bars in operative electrical connection; means for producing a relatively long cipher key sequence composed of single-unit keying characters, said means including a cam-wheel mechanism for controlling said permutation bars; a set of contacts controlled by said stunt bars; and a distributor provided with segments which are in electrical connection with said contacts.

9. In a cryptograph, which employs a translator assembly having permutation bars and stunt bars in operative electrical connection; means for producing a relatively long cipher key sequence composed of single-unit keying characters, said means including a cam-wheel mechanism for controlling the permutation bars of said translator; a set of contacts controlled by the stunt bars of said translator; a circuit including a switch board; and a distributor, the segments of which are connected to said contacts through said switchboard for reducing the number of effects obtainable from the translator to the number of segments on the distributor.

10. In a cryptograph which employs a translator assembly including permutation bars and stunt bars in operative circuit arrangement; means for producing a relatively long cipher key sequence, said means comprising a cam wheel mechanism for controlling said permutation bars; a set of contacts controlled by said stunt bars; a switchboard; and a distributor having segments in electrical connection with said contacts through said switchboard adapted to reduce the number of effects obtainable from said translator to the number of segments on the distributor; and to vary the connections between the contacts of the translator and the segments of the distributor.

11. In a cryptograph, a keyboard comprising a set of character elements; a corresponding set of signaling elements, both sets of elements being in operative electrical connection; a set of rotatable ciphering commutators for varying the connections between the character elements and the signaling elements, each of said commutators having a multiplicity of potential ciphering positions; means for selecting one or more of said commutators to function as rotors; means for driving said selected rotor or rotors sequentially and repetitively at a uniform angular velocity through all of their potential ciphering positions, each complete revolution of said selected rotor or rotors constituting a ciphering cycle, and each said ciphering cycle corresponding to the time during which a key of the keyboard is depressed; and means for selecting one of said potential ciphering positions to become the operative ciphering position in said ciphering cycle.

12. In a cryptograph, a keyboard comprising a set of character elements; a corresponding set of signaling elements, both sets of elements being in operative electrical connection; a set of rotatable ciphering commutators for varying the connections between the character elements and the signaling elements, each of said commutators having a multiplicity of potential ciphering positions; means for selectively operating one or more of said commutators as rotors, including means for driving the same sequentially and repetitively at a uniform angular velocity through all of their potential ciphering positions, each complete revolution of said selected rotor or rotors constituting a ciphering cycle and each said ciphering cycle corresponding to the time during which a key of the keyboard is depressed; means for selecting one of said potential ciphering positions to become the operative ciphering position in said ciphering cycle; and means for varying the selection of said potential ciphering position with successive ciphering cycles.

13. In a cryptograph, a keyboard comprising a set of character elements and a corresponding set

of contacts electrically associated therewith; an indicating mechanism associated with the keyboard and comprising a set of signaling elements corresponding in number with the number of character elements of the keyboard; a circuit system including said sets of elements and a source of potential; means for automatically, rhythmically, and sequentially establishing a multiplicity of sets of different paths for the passage of electric currents from the contacts of the keyboard to the signaling elements of the indicating mechanism; means for momentarily selecting one of said sets of paths and simultaneously connecting the common terminal of the set of contacts of the keyboard to said source so that an electric current initiated by depressing one of the keys of the keyboard will flow along one of the paths in said selected set of paths to one of the signaling elements of the indicating mechanism; and means for varying said momentary selection of a set of said paths with successive depressions of the keys of the keyboard.

14. In a cryptograph, a keyboard comprising a set of character elements and a corresponding set of contacts electrically associated with the character elements; an indicating mechanism associated with said keyboard and comprising a corresponding set of signaling elements; multiple sets of electric conductors, and means for rhythmically and sequentially interposing said conductors between said keyboard and said indicating mechanism; means for selecting one of said sets of conductors and establishing operative electrical connections between the contacts of said keyboard and the signaling elements of said indicating mechanism; and means for varying said selection irregularly and with successive depressions of the keys of said keyboard.

15. In a cryptograph, a keyboard comprising character elements; a corresponding set of signaling elements in a potentially operative electrical connection with the keyboard; means comprising a rotatable commutator for varying the connections between the keyboard elements and the signaling elements; a motor to rotate the commutator at a constant speed, each complete revolution of the commutator comprising one operating cycle during which the keyboard may be operated in enciphering or deciphering; a cam-wheel mechanism comprising a set of cam-bearing rotatable members; means for angularly displacing the cam-bearing members upon operation of the keyboard; a set of contact levers and associated contacts controlled by the cam-wheel mechanism; a translator mechanism controlled by the cam-wheel mechanism for combining the effects of the cam-controlled contacts and causing the selection of one of a plurality of cipher-keying circuits; a switchboard for reducing the plurality of cipher-keying circuits to a number of circuits corresponding with the number of character elements of the keyboard; a distributor comprising a plurality of insulated segments corresponding in number with the number of character elements of the keyboard and connected to one side of the switchboard; a brush arm carrying a brush which sweeps over the segments of the distributor, the brush arm being keyed to the same shaft on which the commutator is rotated so that the commutator and the brush on the distributor face rotate synchronously; and a relay controlled by said distributor for connecting the keyboard to a power source for a specific instant in the operating cycle, said instant being determined by the cipher-key combination established by the cam-wheel mechanism.

16. In a cryptograph, a keyboard comprising a set of character elements with associated contacts; an indicating mechanism electrically associated with the keyboard and comprising a corresponding set of signaling elements; means for connecting the contacts with the signaling elements and for varying said connections sequentially and rhythmically in a multiplicity of ways, said means comprising stators and including ciphering rotors which are interposed between pairs of said stators and which have a multiplicity of potentially-operative ciphering positions with respect to said stators; a shaft carrying said rotors; means for rotating one or more of said rotors at a constant angular velocity; means for momentarily connecting the common terminal of the contacts of the keyboard in circuit relation when said selected rotors have reached a selected ciphering position, thus causing the selected ciphering position of the rotors to act as the operative ciphering position; and means for varying the selection of the driven rotors and of their operative ciphering position with successive depressions of the keys of the keyboard.

17. In a cryptograph including a keyboard comprising a set of character elements and a corresponding set of signaling elements; a circuit system including a source of potential: means for connecting the keyboard to said source for the purpose of establishing operative electrical connection between the keyboard and the signaling elements, said means being actuated only during a specific time-interval within a set of equal time-intervals into which each cycle of keyboard operation is divisible.

18. In a cryptograph including a keyboard comprising a set of character elements and a corresponding set of signaling elements; a circuit system including a source of potential; means for connecting the keyboard to said source for the purpose of establishing operative electrical connection between the keyboard and the signaling elements, said means being actuated only during a specific time-interval within a set of equal time-intervals into which each cycle of keyboard operation is divisible; and means for changing the successive actuating time-intervals.

WILLIAM F. FRIEDMAN.

Dec. 13, 1938. W. F. FRIEDMAN 2,139,676

CRYPTOGRAPHIC APPARATUS

Filed Aug. 4, 1937 3 Sheets-Sheet 1

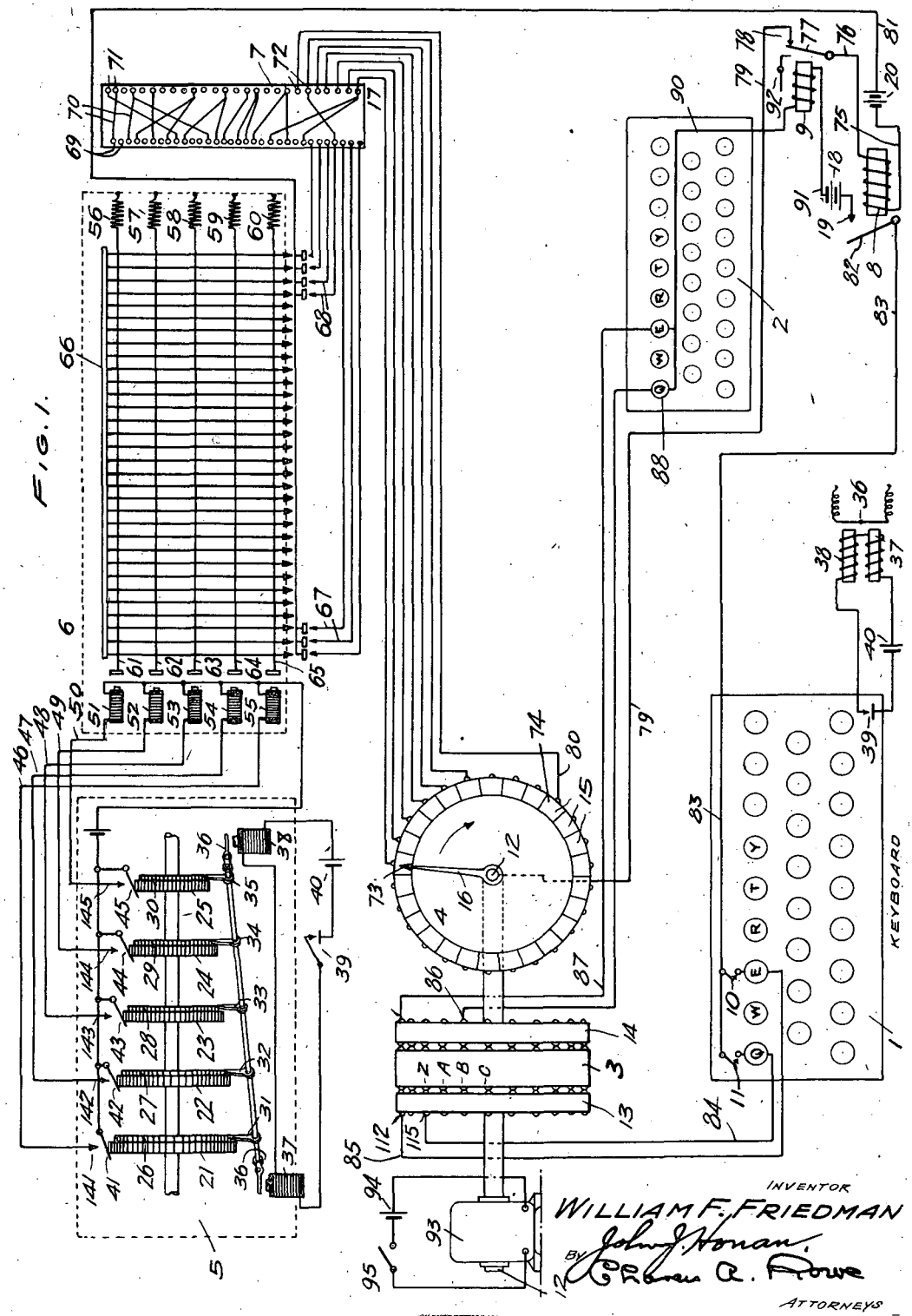


FIG. 1.

INVENTOR
WILLIAM F. FRIEDMAN
By John J. Honan
Lorenzo A. Rowe
ATTORNEYS

Dec. 13, 1938. W. F. FRIEDMAN 2,139,676

CRYPTOGRAPHIC APPARATUS

Filed Aug. 4, 1937 3 Sheets-Sheet 2

FIG. 2.

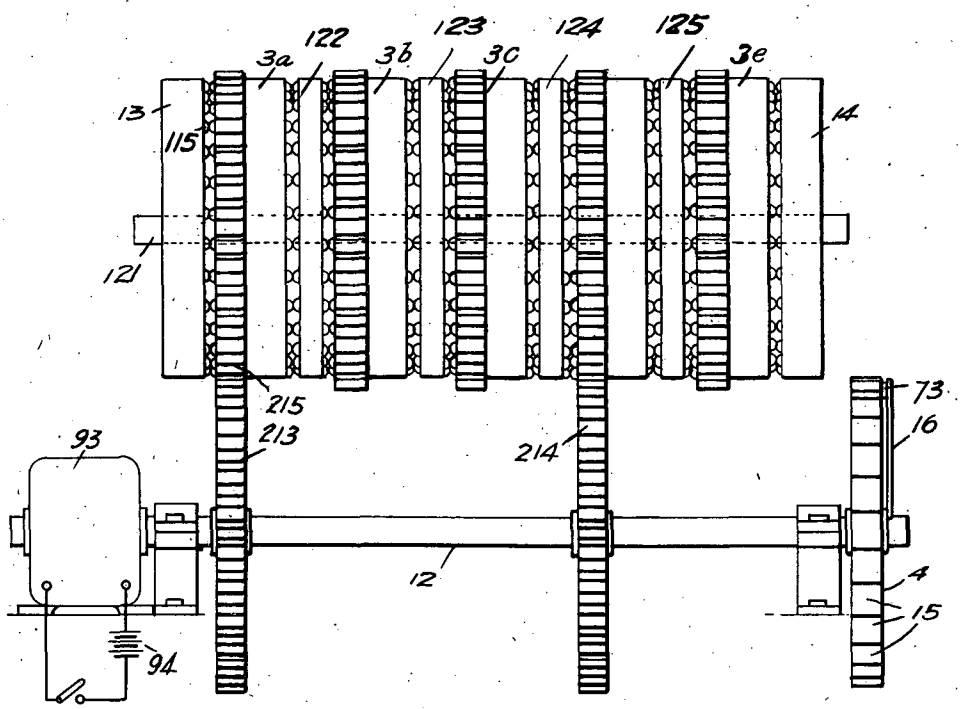
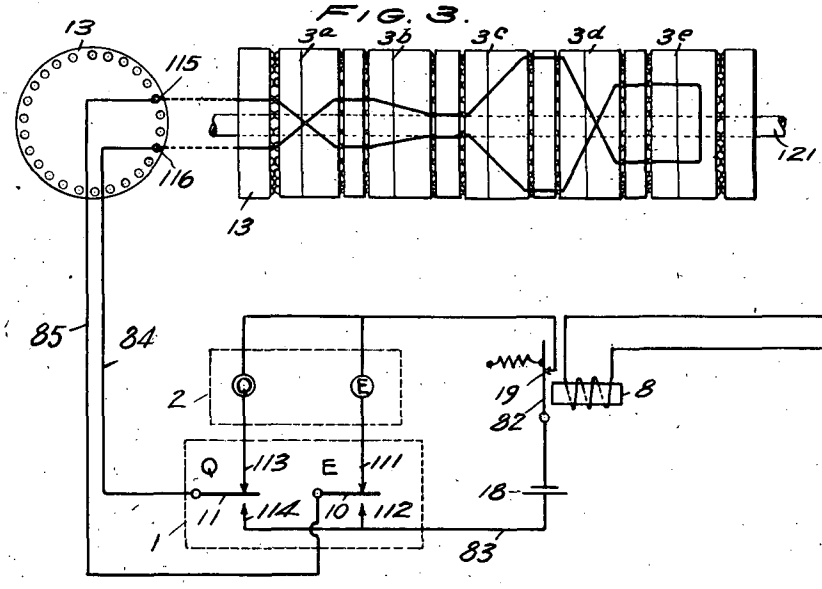


FIG. 3.



INVENTOR
WILLIAM F. FRIEDMAN
BY John J. Honan
Charles A. Howe
ATTORNEYS

Dec. 13, 1938. W. F. FRIEDMAN 2,139,676

CRYPTOGRAPHIC APPARATUS

Filed Aug. 4, 1937 3 Sheets-Sheet 3

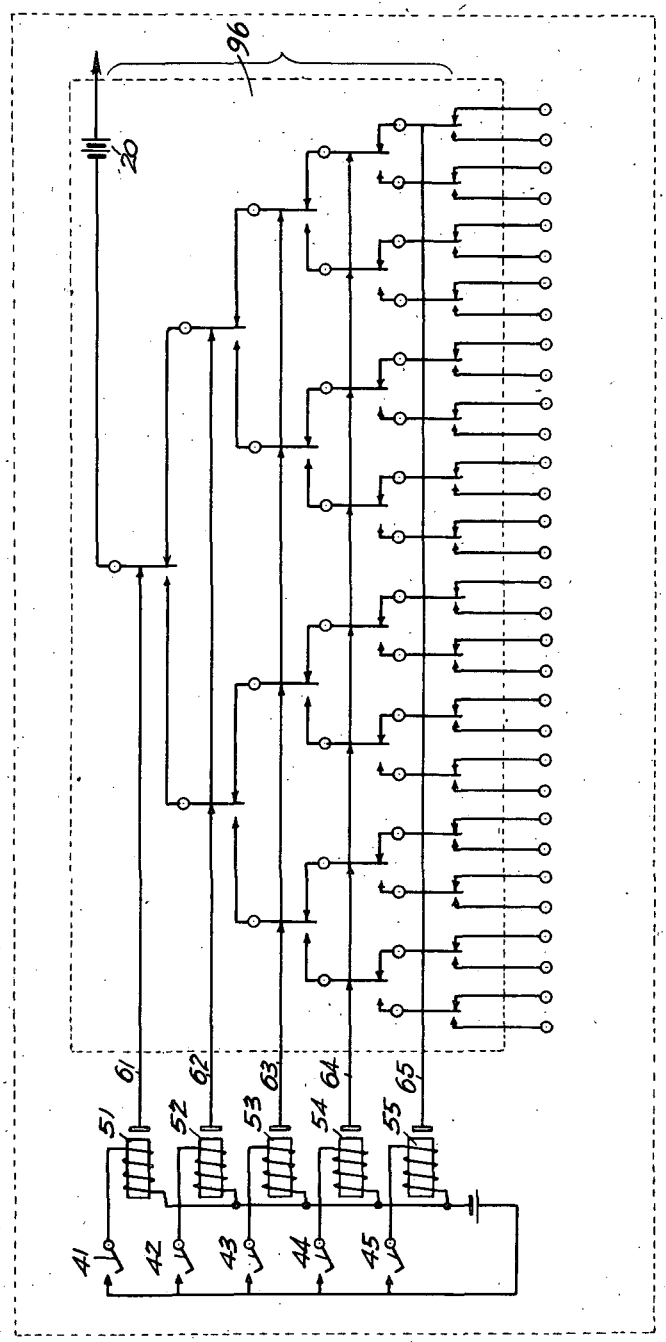


FIG. 4.

INVENTOR
WILLIAM F. FRIEDMAN
BY John J. Horan, Charles A. Howe
ATTORNEYS

Patented July 18, 1939 2,166,137

UNITED STATES PATENT OFFICE

2,166,137

ELECTRICAL SWITCHING MECHANISM

William F. Friedman, Washington, D. C., and Frank B. Rowlett, East Falls Church, Va.

Application August 19, 1935, Serial No. 36,868

10 Claims. (Cl. 200—17)

(Granted under the act of March 3, 1883, as amended April 30, 1928; 370 O. G. 757)

The invention described herein may be manufactured and used by or for the Government for governmental purposes, without the payment to us of any royalty thereon.

This invention relates to a switching mechanism and proposes a mechanism of this character for automatically establishing and/or varying circuit connections in a random order.

As distinguished from the idea of performing switching operations in an orderly sequence, the present invention contemplates an opposite function and provides means to vary the circuit connections in an irregular, aperiodic or fortuitous manner. The invention contemplates an operation which affords opportunity for the laws of probability to function in establishing the variation in circuit connections, rather than an operation controlled by the usual laws of direct cause and effect. An object of this invention is to provide a means of selecting from a plurality of available electrical circuits a single circuit at random, which electrical circuit will be operative for a period of time, the length of which depends upon one or several variable factors.

Another object of this invention is to provide apparatus for varying the speed of rotating bodies by means of a friction drive mechanism working in conjunction with cam wheels of irregular outline and operatively coordinated with a differential gearing system for the purpose of opening and closing electrical circuits for varying periods of time.

A further object of the invention is to provide a device in the nature of a fortuitously-operated device for selecting from a large assortment of punched cards, a random sample.

A further object of the invention is to provide a device in the nature of a scrambling device for arranging in a purely random sequence, a large number of punched cards originally arranged according to a definite sequence, such as an alphabetical or numerical sequence. For example, in the well-known card-sorting machines employed in accounting or statistical work, the function of the machine is to arrange a large number of punched cards in a sequential order, such as alphabetical or numerical. In certain types of operations with punched cards it is often necessary to disarrange the cards so as to destroy the original sequential order and bring the cards into a purely random order. However, once a large number of cards has been sequentially arranged, any attempts to destroy the arrangement by shuffling the cards would be extremely tedious and many cards would be damaged. In the present invention, the device if operated in connection with an ordinary card-sorting machine, would permit of placing a sequentially-ordered batch of cards in the machine and taking out of it a purely fortuitously-ordered batch of cards.

In order that the invention and its mode of application may be readily understood, there is disclosed in the accompanying drawing and in the detailed following description thereof, one form or embodiment of the invention.

In the drawing, the single figure shows in schematic form an apparatus for carrying out the invention.

Referring to the drawing, 1 is a gear, driven by any prime mover such as a motor M; gear 1 meshes with the two gears 2 and 2', having different numbers of teeth. Gear 2 is fixed to shaft 3 and drives the worm gear 4, which in turn, through the train of gears 5, 6, 7, drives shaft 8, on which is mounted cam 9 of irregular outline. Roller 10 rides on the periphery of cam 9 and serves to move lever 11, through a succession of angles which are determined by the depressions and elevations of cam 9. The free end of lever 11 is connected by a pin 12 to a collar 13 which is free to slide up and down on shaft 3 but is independent of the latter in its rotation. The upper end of collar 13 presses against disk 14, which is also mounted on shaft 3 but, by a slot and bar arrangement, is driven by shaft 3. Spring 15 serves to keep the assembly 12, 13, and 14 in place on the shaft 3 and also to cause the roller 10 to follow the outline of cam 9. Disk 14, by frictional effect, drives wheel 16, keyed to shaft 17 so that as shaft 3 turns disk 14 turns and slides up and down against the face of wheel 16, causing shaft 17 to rotate at continuously varying speeds as the roller 10 rides on the periphery of cam 9. Inherent in the mechanism here disclosed and as the result of such a friction drive a slipping action is produced, which action is aided by the sliding movement of disks 13 and 13' on the face of wheels 16 and 16', respectively. The cams 9 and 9' as well as the system of gearing previously described, contribute an important part to this slipping action and consequent lost motion whereby the switching operation is performed in an irregular, aperiodic or fortuitous manner. This constitutes an important object of the invention all as fully set forth in the specification and shown in the drawing. On the shaft 17 is mounted the commutator generally designated as 18 and a contact wheel 19, provided with a plurality of contacts 20, connected in a random manner to the commutator rings 21, 22,

23, 24, 25. Resting against the commutator rings are collectors 26, which are connected to conductors 27 leading to individual circuits, which circuits may include any conventional means or instrumentalities suggested, schematically as at 33 for utilizing the randomizing function of the present invention.

The action of the members 2 to 17 inclusive is the same as that of the members 2' to 17'. Shaft 17' rotates switch arm 30, carrying brush 31 which sweeps over the contacts 20 as it rotates. The commutator assembly which essentially comprises commutator 18 and its associated parts, including contact wheel 19, may be regarded as one component of a switching device, while switch arm 30 carrying brush 31 may be regarded as the other component of said switching device. Brush 31 is connected to the common return conductor 32 for the circuits R_1, R_2, R_3, R_4, R_5 to which conductors 27 lead. Since wheel 19 and brush arm 30 rotate in different directions and at constantly varying speeds, the circuits R_1, R_2, R_3, R_4 and R_5 are selected in the order of the contacts 20 on wheel 19, but each circuit is operative for a different interval of time.

In the drawing, specific mechanical principles are shown for effecting the movements of the various parts of the apparatus. However, these are shown only for the purpose of demonstration of the principles incorporated in this invention, and it is pointed out that any other mechanical means for varying the angular velocity of the commutator 18 rotating with contact disk 19 and the contact arm 30, either separately or conjointly, will effect the result desired. It is also pointed out that, while five commutator rings are depicted in the drawing, any number may be used, and that the number of contacts on the face of the disk 19 may be equal to the number of contact rings or greater by any practicable number. It will also be noted that cams 9 and 9' are intended to be detachable and interchangeable, means being shown in the drawing to facilitate removal for that purpose, or to permit substitution of other cams of different shape.

Changes, modifications and equivalent arrangements are contemplated within the scope of the invention as defined by the appended claims.

We claim:

1. In a mechanism of the character described, a pair of rotating bodies associated for operative movement relative to one another; friction drives having a slipping action and arranged to actuate said bodies in a discrete time relation; and means including a system of differential gearing and cams of irregular contours operatively coordinated with said gearing and with each of said drives individually to aid the slipping action and to effect aperiodic movement of said bodies relative to one another.

2. A mechanism of the character described for controlling the operation of an electrical system, comprising a rotatable commutator provided with contact elements and a rotatable switching device operable with said elements for establishing a plurality of circuit connections; and means to effect a random operation of said system comprising variable driving units for operating said commutator and said switching device asynchronously, and means for differentially controlling the operation of the units.

3. A combination according to claim 2, in which the last named means includes cams of irregular contours individually operable with said units.

4. A combination according to claim 2, in which the last named means includes cams of different irregular contours.

5. A switching mechanism comprising in combination, a rotatable commutator provided with contact elements and a rotatable conductor operable with said elements for establishing a plurality of circuit connections; independently variable friction drives for operating said commutator and said conductor respectively; and means including differential gearing, and cams of irregular contours operatively coordinated with said gearing and individually with each of said drives to vary the circuit connections aperiodically.

6. A randomizing switching mechanism of the character described, comprising a rotatable commutator provided with a plurality of contact elements and a rotatable conductor operable with said elements for establishing a plurality of circuit connections; and means for continuously and irregularly changing the relative speed of said commutator and said conductor to vary the circuit connections aperiodically, said means including a friction drive operative with the commutator and conductor individually, cams of irregular contours operatively coordinated with each drive, and gearing for actuating the cams differentially.

7. A mechanism for controlling the operation of an electrical system, comprising relatively rotatable switching devices provided with cooperating contact elements for establishing a plurality of circuit connections; and means for continuously and aperiodically varying the relative speed of rotation of said switching devices, said means comprising change speed drives individually operative with said switching devices, interchangeable cams of different irregular contours operative with said drives, and a differential gearing system for operating the cams and drives in opposing relation.

8. A mechanism of the character described, comprising switching components movable relative to each other and provided with contacts for establishing a plurality of circuit connections; and means including continuously slipping drive elements and cams of irregular contours operative with each component for continuously and irregularly varying the timing of the contacts in a random manner.

9. A switching device comprising components provided with electrical contacts, said components being rotatable with respect to each other for establishing a plurality of circuit connections; a friction drive mechanism for each of said components, and including means for separately and differentially operating said mechanisms to vary the timing of the circuit connections in a random manner.

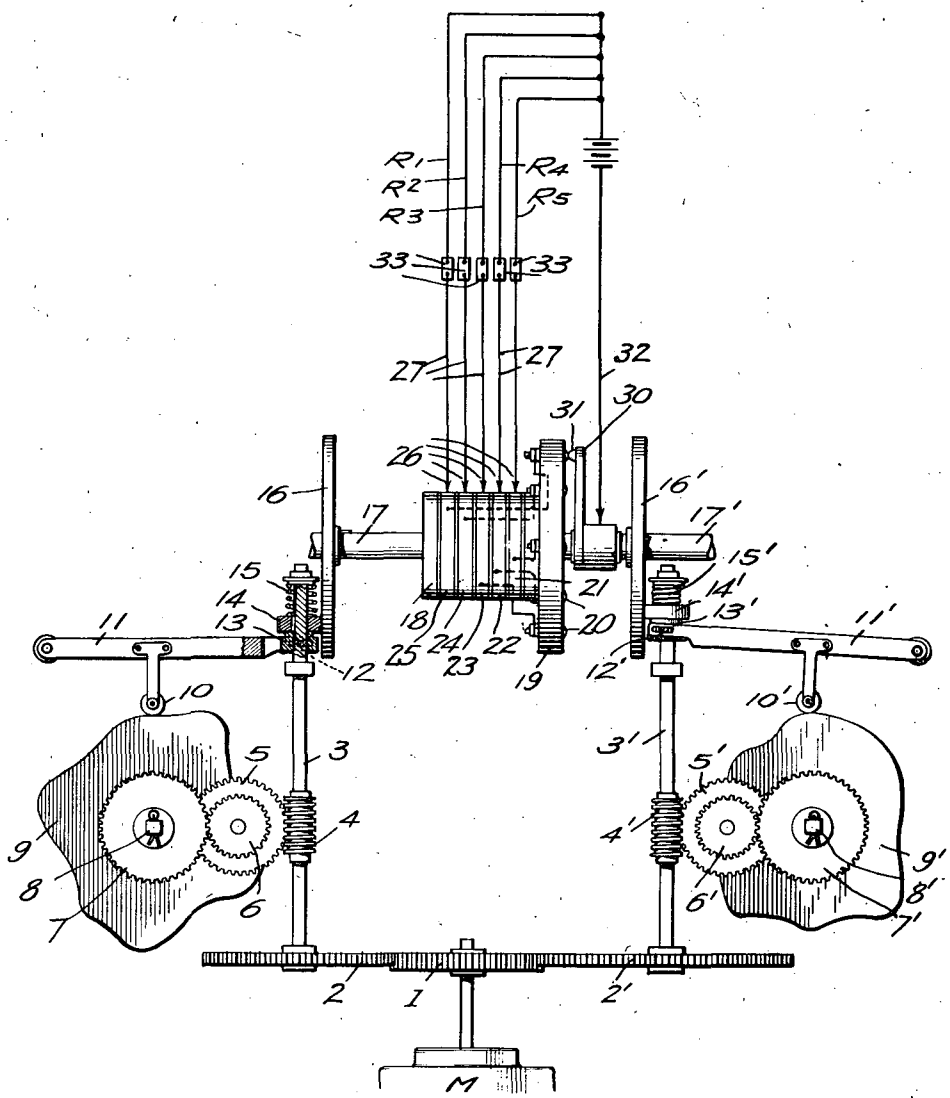
10. A switching mechanism, comprising relatively movable components provided with contacts for establishing a plurality of different circuit connections; means for varying the circuit connections, comprising frictional drive mechanisms operable variably with said components; and means for changing the rate of movement of said mechanisms to assist in randomizing the circuit controlling operation of the contacts.

WILLIAM F. FRIEDMAN.
FRANK B. ROWLETT.

July 18, 1939. W. F. FRIEDMAN ET AL 2,166,137

ELECTRICAL SWITCHING MECHANISM

Filed Aug. 19, 1935



INVENTORS
WILLIAM F. FRIEDMAN
FRANK B. ROWLETT
BY Robert V. Laughlin
Charles A. Howe
ATTORNEYS

Patented Jan. 28, 1936 2,028,772

UNITED STATES PATENT OFFICE

2,028,772

CRYPTOGRAPHIC SYSTEM

William F. Friedman, Washington, D. C., and George A. Graham, Fort Monmouth, Oceanport, N. J.

Application January 23, 1932, Serial No. 588,344

34 Claims. (Cl. 35—4)

(Granted under the act of March 3, 1883, as amended April 30, 1928; 370 O. G. 757)

The invention described herein may be manufactured and used by or for the Government for governmental purposes, without the payment to us of any royalty thereon.

This invention relates to cryptographic systems and an object of the invention is to provide a cryptograph for enciphering and deciphering messages automatically, rapidly and by a method which, being absolutely aperiodic, renders the cryptograms unsolvable without the key.

A further object of this invention is the provision of a cryptograph controlled by means coordinated with a cipher-key transmitter through which is passed a key tape which serves as the keying element in the encipherment or decipherment of messages.

A further object of this invention is the provision of a cryptograph, which, although employing for its keying element a plural-unit-code of the Baudot type (a code of thirty-two permutations), nevertheless produces cryptograms the characters of which are restricted to the twenty-six letters of the alphabet. In this respect the cryptograph excludes the usual six extra Baudot characters, the transmission of which occasions much difficulty in ordinary telegraphy by the Morse alphabet. The way in which these six extra characters are eliminated constitutes one of the unique and important features of our invention.

A further object of this invention is to provide a cryptograph adapted to function either independently as a self-contained cryptographic unit, or in conjunction with an independent typewriter having a standard typewriter keyboard. In the first case, the cryptograph makes no permanent record of the message, but merely produces visual signals; in the second case, the cryptograph makes possible the production of a written record of the message.

A further object of this invention is the provision of a cryptograph functioning at the transmitting end of a communication system as a means for directly controlling a telegraph transmitter keyboard, so that the intelligence to be transmitted is automatically enciphered before transmission; and similarly, at the receiving end, a corresponding cryptograph functions as a means for indirectly controlling an ordinary typewriter so that the intelligence received in cryptographic form is deciphered before being typed by the typewriter.

By way of an introductory statement to our invention, it may be said that in practically all the portable mechanical, electrical, or mechano-electrical cryptographic devices or systems heretofore devised, the cryptographing and decryptographing of messages is entirely controlled by elements all embodied within the mechanism itself; that is, the basic or invariable elements concerned in the cryptographic treatment, as well as the keying, or variable elements for controlling and cryptographic treatment are integral parts of the device or apparatus. In contradistinction to this situation, in our invention, only the basic, or invariable elements concerned in the cryptographic treatment are integral parts of the mechanism, the keying, or variable elements being wholly independent of the mechanism itself, and consist of an extraneous factor which when properly associated with the mechanism controls the basic or invariable elements of the mechanism in cryptographing and decryptographing messages.

In the accompanying drawings:

Fig. 1 is a diagrammatic illustration of a mechanism embodying the invention;

Fig. 2 is a view in side elevation showing part of the commutator or connection changing device;

Fig. 3. shows that part of the commutator which carries the ratchet mechanism and also includes an illustration of the wheel stepping magnet and pawl;

Fig. 4 shows a section of the commutator carrying an arrangement of pins on its rim;

Fig. 5 is a view in side elevation showing a detail of the commutator drive and tensioning motor; and

Fig. 6 is a plan view partly in section of the commutator drive and automatic control therefor.

It is believed that an explanation of the schematic representation of our invention will form the best basis for its understanding, and therefore reference will be made more particularly to Figure 1. In this figure, 1 represents the keyboard of the cryptograph, the arrangement of the twenty-six keys thereof being that of the standard typewriter keyboard except that only twenty-six keys corresponding to the twenty-six letters of the alphabet are included. Each key of the keyboard operates an electrical contact, as shown schematically for the Q and W keys. In addition, our keyboard is provided with a universal bar which is actuated with each depression of any key. Keyboards of this type are well known in the art and require no further description.

The cipher wheel or commutator is shown at 2 in Figure 1. It may be made of bakelite or similar material, and serves as a commutator or connection changing device for carrying fifty-

two brush-type contacts arranged in two rings or sets of twenty-six each, one set being placed on the obverse face 3, of the wheel 2, the other set being similarly placed on the reverse face 5, of the wheel. The twenty-six contacts on each face are arranged equidistantly from one another in a circle adjacent to the periphery of the face, the contacts on the obverse face being connected to those on the reverse face by means of flexible, insulated conductors which pass through the interior of the wheel, as shown schematically and by way of example in Figure 1, for two pairs of contacts. The cipher wheel or commutator is fixed upon the shaft 7, which serves as an axis about which the wheel may rotate. The contacts of the obverse face 3, of the cipher wheel press against ball-bearing type contacts arranged on the fixed plate 4; the contacts of the reverse face 5, of the cipher wheel press against ball-bearing type contacts arranged on the fixed plate 6. The fixed plates 4 and 6 each contain twenty-six contacts arranged equidistantly in a circle. The cipher wheel rotates between these fixed plates 4 and 6 so that each contact on the obverse face 3, of the cipher wheel presents itself in turn to each contact on plate 4, and each contact on the reverse face 5, of the cipher wheel presents itself in turn to each contact on plate 6, as the said wheel rotates. The contacts of plate 6 are respectively connected by conductors to the contacts of the keyboard 1; the contacts of plate 4 are respectively connected by conductors to a bank of twenty-six electrical elements which may be small lamps, relays, or solenoids, only two of which are shown as at 10. For the sake of simplicity of explanation, it will be assumed that the electrical elements in this bank are lamps. As shown in Figure 1, when the key Q is depressed, assuming the cipher wheel to be in the position indicated in the figure, a circuit is established as follows: From positive pole of battery 11 through conductor 12, closed contact at the Q key, conductor 13, contact 14 on fixed plate 6, contact 15 on cipher wheel 2, conductor 16, contact 17 of cipher wheel 2, contact 18 of plate 4, conductor 19, through lamp 20, conductor 21 to negative of battery 11. Lamp 20 has a translucent glass window before it, on which a letter is painted, say the letter W. Hence, depression of the key Q on the keyboard gives the cipher resultant W, under the conditions specified.

Suppose that the key W of the keyboard is depressed, instead of Q. By following the path set up for the electrical current, it will be seen that the Q lamp will be lighted. Thus, reciprocity is established between the keys on the keyboard and the lamps so that if, for example, Q=W, in enciphering, W=Q in deciphering. The same reciprocal relationship can be established throughout the alphabet by connecting the flexible conductors in the interior of the cipher wheel in an appropriate manner to paired contacts on the obverse and reverse faces of the cipher wheel.

If the cipher wheel were stationary, the relationship between the key depressed and the lamp illuminated, that is, the equivalence between plain-text and cipher letters, would be fixed for each wiring of the interior of the cipher wheel. But the cipher wheel is rotatable and hence this relationship is subject to variation. As thus far described our cipher wheel is by no means novel in the art, similar wheels being well known in other cryptographs. Our cipher wheel is, however, novel in respect to certain features connected with the way in which the relationship between plain-text and cipher letters is varied and controlled, and these features will now be presented.

The rim or tire of our cipher wheel 2, is provided with 130 pins arranged in five superimposed bands each band consisting of 26 equidistantly-spaced pins. These pins, which are operable independently, are preferably arranged in groups of fives transversely of the rim face, and are positioned for permutative operation in accordance with the permutations of a plural unit code such as the 5-unit or Baudot code. To explain what is meant, we may say that according to the Baudot code, the permutation of elements for the letter A, for example, is represented thus:

1 2 3 4 5
+ + − − −.

For our purposes we will let the + sign indicate that a pin is to be positioned for positive operation, the − sign, that it is to be left in its inoperative or inactive position. In Figure 2 there is shown a view in side elevation of a section of the rim of the cipher wheel or commutator, with the pins now being described. The pins indicated by dotted lines in Fig. 4 represent pins which have been left depressed in their inactive positions; the pins indicated by whole lines represent pins which have been elevated into their active positions. The permutations represented in Figure 4 correspond to the Baudot signals for the letters Y, Z and A. The order of the letters in Figure 4, is, of course, only illustrative, since all the pins can be arranged in active or inactive positions to correspond with any sequence of signals of the Baudot code, and hence this sequence may be varied at will.

The function of the pins on the rim of the cipher wheel is to control the commutator transmitter shown within the dotted line block designated as at 22 in Figure 1, which consists essentially of a set of 5 contact-levers movable between paired left and right contacts. Formally, these contact-levers are held against the left contact, by the action of respective retractile springs, but when a pin on the rim of the cipher wheel is in its active or operative position, as in the case of pin 48 in Fig. 1, and can therefore present itself to the contact-lever with which it is associated, it presses against the contact-lever and causes it to make contact at the right. Pins in their inactive positions do not, of course, act upon these contact-levers, allowing the latter to remain against their respective left-hand contacts. The function of the paired contacts controlled by the respective contact-levers of the commutator transmitter will be explained presently.

A portion of the cipher wheel near the edge of the reverse face 5, is formed to carry a ratchet wheel, shown in Figure 3. This ratchet wheel contains twenty-six equidistantly-spaced teeth, only five of which are shown in Figure 3, one tooth being designated as 23. It is likewise designated 23 in Figure 1. Associated with the ratchet wheel is the pawl shown at 24, Figures 1 and 3. The ratchet wheel and pawl, together with electro-magnet 25 and its armature 41, Figures 1 and 3, determine the stop position of the cipher wheel in its rotation on the shaft 7, under the drive of coiled spring 8, which is wound or maintained under a desired tension by a motor M.

Referring to Fig. 5, the spring 8 may be conveniently housed in a barrel 47, fixed on the shaft 7 for integral movement therewith and with said cipher wheel, which is also keyed or otherwise

secured to the shaft 7. A worm wheel 48 having a hollow hub 49 is journaled for rotation on shaft 7 and functions through associated instrumentalities to actuate tensioning spring 8, one end of said spring being secured to the worm wheel at 50 (see Fig. 6) and the other end of the spring being fixed to the shaft at 51. As before stated spring 8 is maintained under tension by motor M (see Fig. 6), which is coupled to drive the worm wheel by means of worm gear 52.

As will be seen by reference to Fig. 6, the circuit for the motor, which keeps coiled spring 8 under tension, is closed or opened according to the degree of tension which it is desired to maintain upon the said spring; that is, after the spring is sufficiently tensioned, the circuit is interrupted to stop the motor and is only started again by closing the circuit when the tension has been decreased below a predetermined minimum. For the purpose of controlling this action, the circuit arrangement in operative connection with the motor, comprises leads 53 and 54, including a voltage source 55. The motor shaft is operatively coupled to the worm gear 52 by means of a slide coupling comprising components 56 and 57. When the motor operates to put tension upon the spring 8, component 57 of the slide coupling is gradually moved away from its component member 56 due to the resistance of said spring 8. Thus the worm wheel 48 tends to move the worm gear as indicated by the arrow and progresses the entire shaft 58 from the slide coupling to the right (see Fig. 6) against the action of spring 59. Sleeve 60 which is rigidly secured to shaft 58, is operative through the adjustable L-shaped arm 61 with spring contact member 62, said member being adapted to ride on insulated block 63, conveniently mounted on bearing 64, in which shaft 58 is journaled. Block 63 is provided with a notch or groove 65, into which the projection 66 of spring contact member 62 will drop and break the contact at 67 to open the circuit and stop the motor M. During this period of operation, it should be noted that the drive shaft 7 is held from rotation, normally, by the armature 41 of magnet 25.

While a spring motor driving mechanism for the cipher wheel is here disclosed by way of example, it is understood that other methods are contemplated such as motor and clutch, or a stepping magnet arrangement, or other suitable means that will impart movement to the cipher wheel in accordance with the principles of the invention.

The movement of the cipher wheel is preferably step-by-step, or at intervals which will be explained subsequently in discussing the way in which the whole system functions.

The cipher-key transmitter 26, Figure 1, is a slightly modified Baudot code transmitter such as is employed with printing telegraph equipment of known commercial types. Its general features need not be explained, similar transmitters being well known in the art. It is sufficient to say here that a tape containing perforations permuted in accordance with the Baudot code is passed through this transmitter, setting up a series of five contacts inside the transmitter in accordance with the Baudot code. The transmitter is, of course, also provided with a tape-stepping magnet 27, the function of which is to step the tape forward at proper intervals. The principal difference between the transmitter as used in standard printing telegraph equipment and as used in our invention consists in the way in which the left and right paired contacts of the normal Baudot tape transmitter are interconnected. In the normally-wired transmitter the five contact-levers and their ten associated, paired contacts are members of a set of five separate or independent circuits; in the transmitter as modified for our purposes the five contact-levers and their ten associated paired contacts are conductivity-determining members of a series circuit, as explained in the next paragraph.

The cipher-key transmitter 26, is associated and functions jointly with the commutator transmitter 22, to control the angular displacements of the cipher wheel or commutator in the following manner. Note relay 28, which is energized by current from battery 29, through a path which begins at conductor 30 and includes only ten of the twenty contacts and all the contact-levers of commutator transmitter 22, and key-tape transmitter 26, and is completed along conductor 31. Note also the illustrative set-up of contacts and contact-levers at 22 and 26 in Figure 1, in which a specific case is presented. It is assumed there that the arrangement of operative pins on the cipher wheel which are at that moment presenting themselves to the contact-levers of the cipher-wheel transmitter 22, corresponds to the Baudot permutation for letter Z. At the same moment the character on the key tape and the permutation of contacts set-up within the cipher-key transmitter 26, also corresponds to the letter Z. Note that in view of the manner in which the twenty contacts and the ten contact-levers of 22 and 26 are interconnected, the circuit from battery 29 through relay 28 is completed only when the whole set of electrical connections established at the cipher-key transmitter 26, coincides with the whole set of connections established at the commutator transmitter 22, Hence, if Z is set up in cipher-key transmitter 26, relay 28 will operate only when Z is set up in the commutator transmitter 22. Similarly if any other letter, say X, is set up in the cipher-key transmitter 26, relay 28 will operate only when X is set up in the commutator transmitter 22. The complete path of the current when such coincidence of connections in transmitters 22 and 26 is established is as follows:

From positive of battery 29 along conductor 30, through all the contact-levers and the ten associated closed contacts of transmitters 26 and 22, conductor 31 to back contact 32, of armature 33, winding of relay 28, conductor 34, to negative of battery 29. It is obvious that since the armature 33 and back contact 32 of relay 28 form parts of the circuit for energizing relay 28, as soon as the relay has received an impulse and armature 33 is attracted, the circuit for energizing relay 28 is broken at contact 32. Since armature 33 is under tension of a retractile spring, if not prevented from being pulled back into its normal position on release of relay 28, armature 33 would reestablish contact at 32 and would set up a chattering. But the mechanical arrangements are such that when armature 33 is first drawn up by relay 28 it passes by and is immediately engaged by lever 35 and held from returning to its retracted position where it can reestablish contact at 32, until lever 35 is displaced by mechanical action to be described later. Armature 33 of relay 28 also controls the magnet 25, already referred to, which, in turn, controls the rotation of the cipher wheel 2, in the following manner:

The motor-tensioned coiled spring 8, tends to rotate the cipher wheel in the direction indicated

by the arrow, say to the right. The circuit for the motor which keeps coiled spring 8 under tension is closed or opened depending upon the tension of the spring; that is, after the spring has sufficient tension, the motor is stopped and is only started again after this tension has decreased below a certain minimum. The rotation of the cipher wheel is step-by-step, controlled by the magnet 25, and the ratchet referred to above. Assume the contact-levers in transmitters 22 and 26 set up to different permutations so that relay 28 is not energized and hence contact 36 is closed. A current starts from positive of battery 37 through conductor 38, closed contact 36, conductor 39, back contact 40, armature 41, conductor 42, winding of magnet 25, conductor 43, to negative of battery 37. A momentary impulse passes through magnet 25 and causes armature 41 to be attracted, breaking the circuit at back contact 40, whereupon armature 41, under action of its spring, returns and again closes the circuit at 40. However, the mechanical arrangement is such that the momentary attraction of armature 41 releases the pawl 24, associated with the ratchet on the cipher wheel and thus allows the cipher wheel, driven by coiled spring 8, to advance one step. Thus, the cipher wheel continues to move, one step at a time, so long as back contact 36 of relay 28 remains closed. When, however, the permutation of contacts set up in the commutator transmitter becomes the same as that set up in the cipher-key transmitter, thus causing the completion of the circuit through relay 28 as already described, and thus, when contact 36 is opened, under the action of relay 28, and is held open by lever 35 as described above, magnet 25 cannot operate to withdraw armature 41; hence the pawl 24 cannot be released, whereupon the cipher wheel cannot advance any further. As stated before, the first impulse through relay 28 causes armature 33 to be attracted, to pass by lever 35, which then engages the armature. Thus contact 36 remains open as long as lever 35 engages and holds it. It is only within this period, when the cipher wheel is stationary, that the keyboard 1, can be manipulated, the mechanical arrangement being such that the keys of the keyboard are locked except when the cipher wheel is stationary.

Suppose now a key is depressed. The cipher resultant will be determined by the position of the cipher wheel at this time, because the circuit established through the cipher wheel depends upon the exact relative position of this wheel with respect to fixed plates 4 and 6. When a key is depressed, the cipher resultant is shown by the illuminated lamp; the latter continues to be illuminated so long as the key is held down.

We return now to relay 28 and its other armature 46. The latter controls the operation of the tape-stepping magnet 27 of the cipher-key transmitter 26, in the following manner: The tape-stepping magnet 27 is actuated by battery 44, but the circuit is normally open at contact 45. When relay 28 is energized, however, armature 46 is attracted and contact 45 is momentarily closed, allowing tape-stepping magnet 27 to function. This causes the key tape to step forward to the next position. It will remain in that position until the next time relay 28 is energized.

There now remains to be described only how lever 35 is controlled: The keyboard is provided with a universal bar, operable by every key. When a key is depressed and then released, the universal bar, near the close of its upward swing on return to normal position, actuates the lever 35, and causes it to be withdrawn from its engagement with armature 33. The latter immediately returns to its normal, retracted position, allowing contacts to be reestablished at 32 and 36. In the meantime the tape-stepping magnet having been actuated as described above, one of two things can happen as regards the set-up of connections in cipher-key transmitter 26: either a new set of connections between contact-levers and paired contacts has been established, or, by chance, if two similar characters occur in sequence on the tape, the same set of connections as before has been established. These two cases are described in turn:

(1) If a new set of connections in cipher-key transmitter 26 has been established, say a set corresponding to the Baudot signal for X, the set of connections no longer matches that set-up in the commutator transmitter 22, which, as we have seen, corresponded in the preceding case to the letter Z. Consequently, immediately upon closing of contact at 36 under action of the universal bar, the circuit for energizing magnet 25 is closed, allowing the cipher wheel to step forward. It will continue to do so until that set-up of pins on the rim of the cipher wheel corresponding to letter X presents itself to the contact-levers of the commutator transmitter 22, whereupon relay 28 is energized, contact at 36 is broken, magnet 25 deenergized, and the cycle has been completed.

(2) If, by chance, the next character on the key tape is the same as before (Z again), relay 28 is immediately energized, since the commutator transmitter is still set up for permutation Z. Magnet 25 does not function and the cipher wheel is held in place. Two letters are therefore enciphered at the same position of the cipher wheel. Of course, if the key tape now consists of a series of Z's, the cipher wheel will remain in fixed position during the encipherment of a corresponding number of letters.

It is obvious that the permutations of perforations on the key tape as well as the permutations of operative pins on the rim of the cipher wheel must be restricted to two sets of 26 similar permutations, otherwise there would be times when the cipher wheel would continue to revolve indefinitely and no encipherment or decipherment could take place. This is true for the reason that in order to bring the cipher wheel to rest it is essential that a permutation of pins on its rim exactly coincide with that permutation which happens to be set up at the cipher-key transmitter at that moment. This restriction to two sets of similar permutations does not, however, reduce the cryptographic security of the system in any degree whatsoever.

In addition, attention is especially called to the way in which a serious disadvantage of other cryptographs employing the Baudot code for cryptographic purposes is obviated in our system. In order to explain what is meant it is necessary to enter into a brief discussion of Baudot transmission from the practical, economic point of view. For this purpose reference is made to U. S. Patent No. 1,416,765, issued May 23, 1922, to G. S. Vernam, lines 12 to 81 of the specification.

In the patent to which reference has just been made, a special mechanism was devised to suppress the six extra characters which cause all these difficulties; and while accomplishing the object intended, the mechanism is quite complicated and has in addition the further disadvantage that the method selected to accomplish the

suppression of the six extra characters results in increasing the number of characters to be transmitted by as much as 10 to 30 per cent. In our invention, both these disadvantages have been eliminated in the simplest manner possible, viz., by arrangements which necessitate only 26 of the 32 Baudot permutations for cryptographic purposes. So far as cryptographic technique is concerned, basically our arrangements for eliminating the six extra characters ordinarily introduced by the use of the Baudot code for cryptographic purposes differ from those described in the patent referred to above in the following respect. In the cryptographic system underlying the latter method the cipher resultants in the cryptographic process are the resultants of electrical interaction between a set of signaling elements in the Baudot code set up by a message character and a set of signaling elements in the same code set up by a key character; these resultants can not be restricted to but 26 of the 32 possible Baudot permutations because of this interaction. In our cryptographic system the cipher resultants in the cryptographic process are not at all the resultants of electrical interaction between two sets of signaling elements in the Baudot code; the signaling element representing the message character is not at all in the Baudot code and does not interact directly with the signaling elements representing the key character, nor is the cipher resultant represented by signaling elements in the Baudot code. The role the Baudot code plays in our system is, so far as signaling elements are concerned, only an indirect one, and that is why in our system the restriction of cipher characters to a set of only 26 is rendered easy, without any apparatus specifically introduced to suppress the six extra characters.

It is obvious that instead of having the cryptograph function to produce visual signals of the type indicated in the foregoing description, it is possible to provide at 10, Figure 1, a set of 26 electro-magnets instead of a set of 26 lamps, which magnets would act through proper plungers or armatures directly upon the keyboard of a typewriter with which they are associated, so as to cause the typewriter to print the letters of the cipher message, in the case of enciphering, and the letters of the plain-text message, in the case of deciphering.

Again, these magnets, instead of being associated with the keyboard of an ordinary typewriter, might be associated with the keyboard of an automatic telegraph transmitter keyboard, and thus, in the case of enciphering, bring about the transmission of signals corresponding to enciphered letters. At the receiving end of this system, the received signals would act directly upon the keyboard of the cryptograph, and the latter would cause the received cryptographed signals to be deciphered and, if the cryptograph at the receiving end is associated with a typewriter as described in the preceding paragraph, the cryptograph would cause a written record to be made of the deciphered message.

It is also obvious that the mechanism which we have provided permits of variations in cryptographic resultants other than those introduced by changing the key tape. One of these sources of variations lies in the possibility of changing the permutations of operative and inoperative pins on the rim of the cipher wheel. Another source lies in the changing of connections between the keyboard contacts and the contacts of plate 6, Figure 1; or between the contacts of plate 4 and the signaling elements in bank 10. Another source lies in constructing the cipher wheel in two sections, an upper and lower, so that the two sections can be positioned or juxtaposed at any one of twenty-six different points of coincidence with respect to each other, thus varying the cipher resultants. Another source lies in the changing of connections between the contacts on the obverse and reverse faces of the cipher wheel. Finally, an important source of variation lies in the changing of the connections between the homologous contacts of the cipher-key transmitter 26, and the commutator transmitter 22. All these sources of variation existing within the mechanism itself are subsidiary, however, to the principal source inherent in constant change of key tapes, and it may be said that so long as a given key tape is coextensive in number of characters with that of the intelligence to be enciphered, so that no two messages are ever enciphered by the same key tape or portion thereof, and so long as these key tapes consist of unintelligible, entirely randomized sequences of characters, the messages enciphered according to such a system are absolutely indecipherable without actual possession of the key tapes employed in their encipherment or a knowledge of the sequence of the characters on such key tapes.

We claim:

1. In a cryptographic system adapted for use with a plural unit code transmitter; means comprising electrically operable elements for coordinating the transmitter with said system; and circuit means for interconnecting said elements for cryptographic purposes, said means comprising contact levers and paired contact points permutatively positioned and operative in series relation.

2. In a cryptograph, a keyboard comprising character elements in operative electrical connection with corresponding signaling elements; means comprising a commutator for varying the connections between the keyboard elements and said signaling elements; a commutator transmitter; a cipher-key transmitter; and means coordinated with said transmitters for effecting progressive operation of the commutator.

3. In a cryptograph, a keyboard comprising character elements in operative electrical connection with corresponding signaling elements; means comprising a commutator for varying the connections between the character elements and said signaling elements; a cipher-key transmitter mechanism; and means coordinating said mechanism with the commutator for effecting its progressive operation.

4. In a cryptograph, a keyboard comprising character elements in operative electrical connection with corresponding signaling elements; means comprising a commutator for varying the connections between the character elements and said signaling elements; a cipher-key transmitter mechanism; and means comprising a commutator transmitter coordinating said mechanism with the commutator for effecting its progressive operation.

5. In a cryptograph, a keyboard comprising character elements in operative electrical connection with a corresponding number of signaling elements; means comprising a commutator for varying the connections between the keyboard elements and said signaling elements; a commutator transmitter; a cipher-key transmitter; and circuit means coordinated with said

transmitters for effecting progressive operation of the commutator.

6. In a cryptograph, a keyboard comprising character elements in operative electrical connection with corresponding signaling elements; means comprising a commutator for varying the connections between the keyboard elements and said signaling elements; a commutator transmitter; a cipher-key transmitter; and circuit means coordinating both of said transmitters for jointly effecting progressive operation of the commutator.

7. In a cryptograph, a keyboard comprising character elements in operative electrical connection with corresponding signaling elements; means comprising a commutator for varying the connections between the keyboard elements and said signaling elements; a commutator transmitter; a cipher-key transmitter; and means coordinating said commutator and cipher-key transmitter through the commutator transmitter for effecting progressive operation of the commutator.

8. In a cryptograph, a keyboard comprising character elements in operative electrical connection with corresponding signaling elements; means comprising a commutator for varying the connections between the keyboard elements and said signaling elements; a commutator transmitter; a cipher-key transmitter mechanism; and means coordinated with both of said transmitters for effecting progressive operation of the commutator, said cipher-key transmitter mechanism being controlled by a keying element which is independent of the cryptograph.

9. In a cryptograph, a keyboard comprising character elements in operative electrical connection with corresponding signaling elements; means comprising a commutator for varying the connections between the keyboard elements and said signaling elements; a commutator transmitter; a cipher-key transmitter mechanism; and means coordinated with both of said transmitters for effecting progressive operation of the commutator, said cipher-key transmitter mechanism being controlled by a tape bearing perforations permuted in accordance with a plural unit code.

10. A cryptograph, comprising an electrical circuit and including a current source; a relay in said circuit; a set of contact levers and paired contact points, permutatively positioned and operative therewith in said circuit; a second set of contact levers and contact points associated in similarly operative relation with said circuit; and means for completing said circuit and energizing said relay only at such times as the entire series of connections established within the first set of contact levers and their associated contact points is identical with the entire series of connections established within the second set of contact levers and their associated contact points.

11. A cryptograph, comprising an electrical circuit and including a current source; a relay in said circuit; a set of contact levers and paired contact points, permutatively positioned and operative therewith in said circuit; a second set of contact levers and contact points associated in similarly operative relation with said circuit; and means for permutatively varying as a set each of the said sets of contact levers.

12. A cryptograph, comprising an electrical circuit and including a current source; a relay in said circuit; a set of contact levers and paired contact points, permutatively positioned and operative therewith in said circuit; a second set of contact levers and contact points associated in similarly operative relation with said circuit; and means for permutatively varying as a set each of the said sets of contact levers, the permutative variations being in accordance with the same plural unit code for both sets of contact levers.

13. A cryptograph, comprising an electrical circuit and including a current source; a relay in said circuit; a set of contact levers and paired contact points, permutatively positioned and operative therewith in said circuit; a second set of contact levers and contact points associated in similarly operative relation with said circuit; means for completing said circuit and energizing said relay only at such times as the entire series of connections established within the first set of contact levers and their associated contact points is identical with the entire series of connections established within the second set of contact levers and their associated contact points; and means for permutatively varying as a set each of the two sets of contact levers, the permutative variations being in accordance with the same plural unit code for both sets of contact levers.

14. A cryptograph, comprising an electrical circuit and including a current source; a relay in said circuit; a set of contact levers and paired contact points, permutatively positioned and operative therewith in said circuit; a second set of contact levers and contact points associated in similarly operative relation with said circuit; and means for permutatively varying as a set each of the said sets of contact levers, the permutative variations for one of said sets of levers being in accordance with one plural-unit code, those of the other of the two sets of levers being in accordance with a different plural-unit code.

15. A cryptograph, comprising an electrical circuit and including a current source; a relay in said circuit; a set of contact levers and paired contact points, permutatively positioned and operative therewith in said circuit; a second set of contact levers and contact points associated in similarly operative relation with said circuit; means for completing said circuit and energizing said relay only at such times as the entire series of connections established within the first set of contact levers and their associated contact points is identical with the entire series of connections established within the second set of contact levers and their associated contact points; and means for permutatively varying as a set each of the two sets of contact levers, the permutative variations for one of said sets of levers being in accordance with one plural-unit code; those of the other of the two sets of levers being in accordance with a different plural-unit code.

16. In a cryptograph, a connection changing vice comprising a rotatable drum, bearing a series of pins arranged in groups about its rim, the groups comprising each a plurality of units positioned transversely of said rim and corresponding in number of groups to a predetermined selection of characters; means for positioning the pins for independent operation in groups in accordance with the permutations of a plural-unit code; said drum also bearing on its obverse and reverse faces respectively a series of equidistantly spaced contact elements arranged in a ring adjacent to the periphery; and means for establishing fortuitous electrical connections between the contact elements of said faces.

17. In a cryptograph, a connection changing

device comprising a rotatable drum, bearing a series of pins arranged in spaced groups about its rim, the groups comprising each a plurality of units positioned transversely of said rim and corresponding in number of groups to a predetermined selection of characters; means for positioning the pins for independent operation in groups in accordance with the permutations of a plural-unit code; said drum also bearing on its obverse and reverse faces respectively a series of equidistantly spaced contact elements arranged in a ring adjacent to the periphery; and means for establishing fortuitous electrical connections reciprocally in pairs between the oppositely disposed contact elements of said faces.

18. A cryptograph, comprising an operatively associated electrical circuit and including a current source; a rotatable commutator bearing a series of pins arranged in groups about its rim and positioned for independent operation in accordance with the permutations of a plural-unit code, the groups comprising each a plurality of pins and said groups corresponding in number to a predetermined selection of characters; a transmitter controlled by said pins, said transmitter comprising a set of contact points and contact levers operative therewith in series circuit relation.

19. A cryptograph, comprising an operatively associated electrical circuit and including a current source; a rotatable commutator bearing a series of pins arranged in groups about its rim and positioned for independent operation in accordance with the permutations of a plural-unit code, the groups comprising each a plurality of pins and said groups corresponding in number to a predetermined selection of characters; a transmitter controlled by said pins, said transmitter comprising a set of contact points and contact levers operative therewith in series circuit relation; and means also controlled by said pins and permutatively operable with said transmitter to set up progressive steps in the continuity of said series circuit.

20. A cryptograph, comprising an operatively associated series electrical circuit and including a current source; a relay in said circuit; a rotatable commutator carrying a series of pins positioned in groups about its rim for independent operation in accordance with the permutations of a plural-unit code, the groups comprising each a plurality of pins and said groups corresponding in number to a predetermined selection of characters; a commutator transmitter controlled by said pins, said transmitter comprising a set of contact points and contact levers operative therewith in series circuit relation; means consisting of a cipher-key transmitter, said transmitter comprising a set of contact points and contact levers operative therewith in the same series circuit relation; and means jointly controlled by both of said transmitters for setting up progressive steps in the continuity of said series circuit for operating said relay.

21. In a mechanism of the character described, the combination of a commutator transmitter; a cipher-key transmitter; and a rotatable commutator bearing on its rim a series of pins arranged in sets, the sets corresponding in number to a predetermined selection of characters, said pins being positioned permutatively in groups of five in accordance with a selected set of permutations of a five-unit code.

22. In a mechanism of the character described, the combination of a commutator transmitter; a cipher-key transmitter; and a rotatable commutator bearing on its rim a series of pins arranged in sets, the sets corresponding in number to a predetermined selection of characters, said pins being positioned permutatively in groups of five in accordance with a selected set of permutations of a five-unit code to effect control of said commutator transmitter.

23. In a mechanism of the character described, the combination of a commutator transmitter; a cipher-key transmitter; and a rotatable commutator bearing on its rim a series of pins arranged in sets, the sets corresponding in number to a predetermined selection of characters, said pins being positioned permutatively in groups of five in accordance with a selected set of permutations of a five-unit code to effect control of said commutator transmitter; and means operative with said commutator transmitter for jointly controlling the progressive displacements of the commutator.

24. In a mechanism of the character described, the combination of a commutator transmitter; a cipher-key transmitter; and a rotatable commutator bearing on its rim a series of pins arranged in sets, the sets corresponding in number to a predetermined selection of characters, said pins being positioned permutatively in groups of five in accordance with a selected set of permutations of a five-unit code to effect control of said commutator transmitter; and means coordinated with a cipher-key transmitter mechanism and operative with said commutator transmitter for jointly controlling the progressive displacements of the commutator.

25. In a mechanism of the character described, the combination of a commutator transmitter; a cipher-key transmitter; and a rotatable commutator bearing on its rim a series of pins arranged in sets, the sets corresponding in number to a predetermined selection of characters, said pins being positioned permutatively in groups of five in accordance with a selected order of permutations of a five-unit code, and to the exclusion of undesired permutations of the said code.

26. In a mechanism of the character described, the combination of a commutator transmitter; a cipher-key transmitter; and a rotatable commutator bearing on its rim a series of pins arranged in sets, the sets corresponding in number to a predetermined selection of characters, said pins being positioned permutatively in groups of five in accordance with a selected order of permutations of a five-unit code, and to the exclusion of undesired permutations of the said code to effect control of said commutator transmitter; and means coordinated with said cipher-key transmitter mechanism and operable with said commutator transmitter for jointly controlling progressive displacements of the commutator.

27. In a mechanism of the character described, the combination of a commutator transmitter; a cipher-key transmitter; a rotatable commutator bearing on its rim a series of pins arranged in sets, the sets corresponding in number to a predetermined selection of characters, said pins being positioned permutatively in groups of five in accordance with a selected order of permutations of a five-unit code, and to the exclusion of undesired permutations of the said code to effect control of said commutator transmitter; means coordinated with said cipher-key transmitter and operable with said commutator transmitter for jointly controlling progressive displacements of the commutator; and circuit

means including an electro-magnetic relay for controlling said displacements.

28. In a mechanism of the character described, the combination of a commutator transmitter; a cipher-key transmitter; a rotatable commutator bearing on its rim a series of pins arranged in sets, the sets corresponding in number to a predetermined selection of characters, said pins being positioned permutatively in groups of five in accordance with a selected order of permutations of a five-unit code, and to the exclusion of undesired permutations of the said code to effect control of said commutator transmitter; means coordinated with said cipher-key transmitter and operable with said commutator transmitter for jointly controlling progressive displacements of the commutator; and circuit means including an electro-magnetic relay for controlling said displacements, the circuit means being under the joint control of both of said transmitters.

29. A mechanism of the character described, comprising a set of elements constituting a keyboard and a set of elements constituting a signaling bank, said sets of elements being electrically interrelated; a switching device for varying the electrical relation between the two sets of elements; means for angularly displacing the switching device in an aperiodic manner, the angular displacements being unequal.

30. A mechanism of the character described, comprising a set of elements constituting a keyboard, a set of elements constituting a signaling bank, and including electrical connections between said sets of elements; a switching device for varying the connections between the two sets of elements; means for angularly displacing the switching device in an aperiodic manner, the angular displacements being unequal, the inequality in angular displacements being determined by a series of ciphering characters constituting an external cipher key.

31. A mechanism of the character described, comprising a set of elements constituting a keyboard, a set of elements constituting a signaling bank, and including electrical connections between said sets of elements; a switching device for varying the connections between the two sets of elements; means for angularly displacing the switching device in an aperiodic manner, the angular displacements being unequal, the inequality in angular displacements being determined by an external key, said key comprising a non-repeating series of ciphering characters arranged in random, unintelligible order.

32. A mechanism of the character described, comprising a set of elements constituting a keyboard, a set of elements constituting a signaling bank, and including electrical connections between said sets of elements; a switching device for varying the connections between the two sets of elements; means for angularly displacing the switching device in an aperiodic manner, the angular displacements being unequal, the inequality in angular displacements being determined by an external key, said key comprising a nonrepeating series of ciphering characters arranged in random, unintelligible order, the said ciphering characters being employed successively to encipher successive characters of the message.

33. A cryptograph, comprising an operatively associated electrical circuit and including a current source; a rotatable commutator bearing a series of pins positioned for permutative operation in groups comprising each a set of five pins and said groups corresponding in number to a predetermined selection of characters; a cipher-key transmitter; a commutator transmitter controlled by said pins, said transmitter comprising a first set of contact levers and paired contact points electrically operative therewith, said levers being actuated by the permutatively positioned pins of said commutator, when electrically operated through said levers and five of said contact points, to set up a first set of five progressive steps in the continuity of an electrical path for the displacement of the commutator; means coordinated with said commutator transmitter for jointly controlling progressive displacements of the commutator, said means being controlled by said cipher-key transmitter; a second set of contact levers and paired contact points electrically operable therewith, said levers being actuated by said cipher-key transmitter, when circuits are completed through the contact levers of said cipher-key transmitter and five of the contact points, to set up a second set of five progressive steps in the continuity of an electrical path for the displacement of the commutator; means for rotating the commutator; means operative with said commutator to cause aperiodic interruption in its rotation; and means to start and stop the commutator.

34. In a cryptograph, the combination of a bank of twenty-six signaling elements in electrical circuit connection with a twenty-six element keyboard, said keyboard comprising a corresponding number of contacts for closing said circuit connections; a plural-unit code cipher-key transmitter coordinated with said keyboard to jointly control said signaling elements; means for changing the electrical paths between the keyboard elements and signaling elements, said means consisting of a commutator provided with a first set of twenty-six contacts equidistantly distributed on the obverse face of said wheel; a second and homologous set of twenty-six contacts equidistantly distributed on the reverse face of said wheel; conductors respectively connecting the contacts of one face with the contacts of the other face; twenty-six sets of pins mounted on the rim of said wheel and positioned for permutative operation according to the permutations of a five-unit code; a commutator transmitter comprising a first set of five contact levers electrically operable with ten paired contact points, said levers being actuated by the pins of said commutator, when electrically operated through said levers and five of said contact points, to set up a first set of five progressive steps in the continuity of an electrical circuit for the displacement of the commutator; a second and similar set of five contact levers electrically operable with ten paired contact points, said contact levers being actuated by the cipher-key transmitter, when operated through its contact levers and five of its ten associated contact points, to set up a second and similar set of five progressive steps in the continuity of the same electrical circuit for the displacement of the commutator; means dependent upon the continuity of said electrical circuit to effect displacements of the commutator until the first set of five progressive steps exactly matches the second set of five progressive steps in the continuity of said electrical circuit.

WILLIAM F. FRIEDMAN.
GEORGE A. GRAHAM.

Jan. 28, 1936. W. F. FRIEDMAN ET AL 2,028,772

CRYPTOGRAPHIC SYSTEM

Filed Jan. 23, 1932 2 Sheets-Sheet 2

FIG. 2.

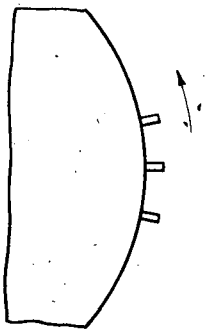


FIG. 3.

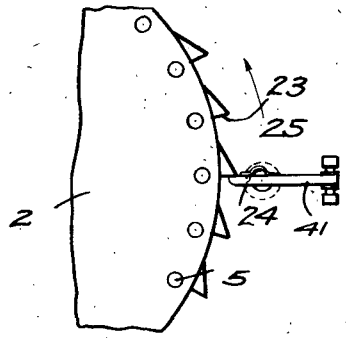


FIG. 4.

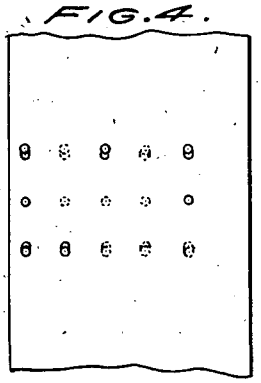
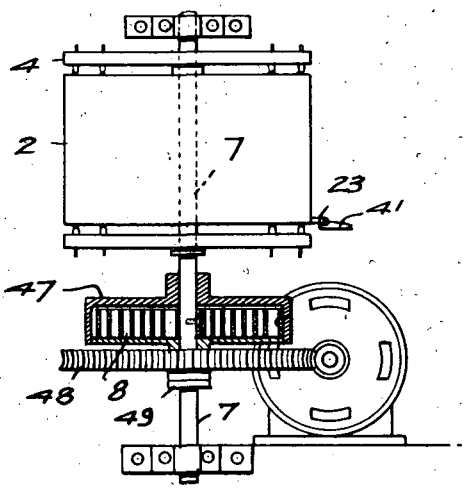


FIG. 5.



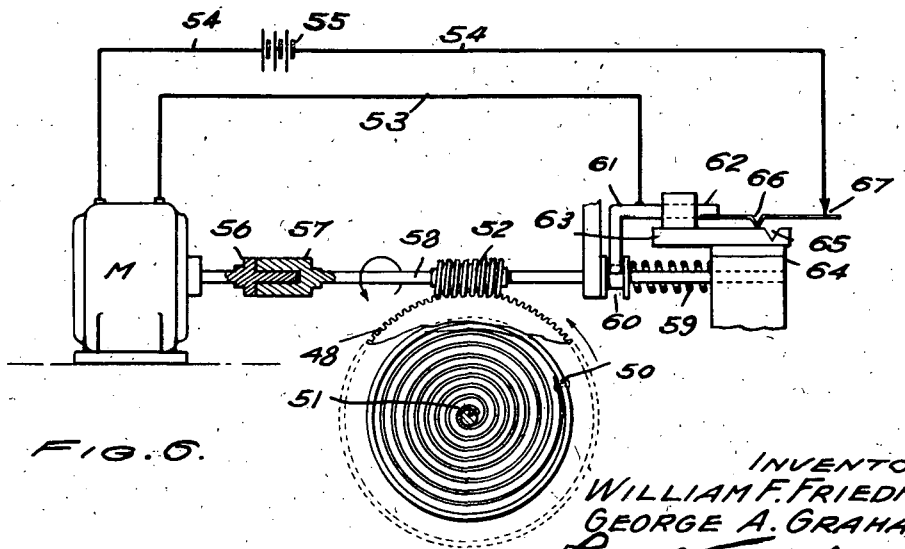


FIG. 6.

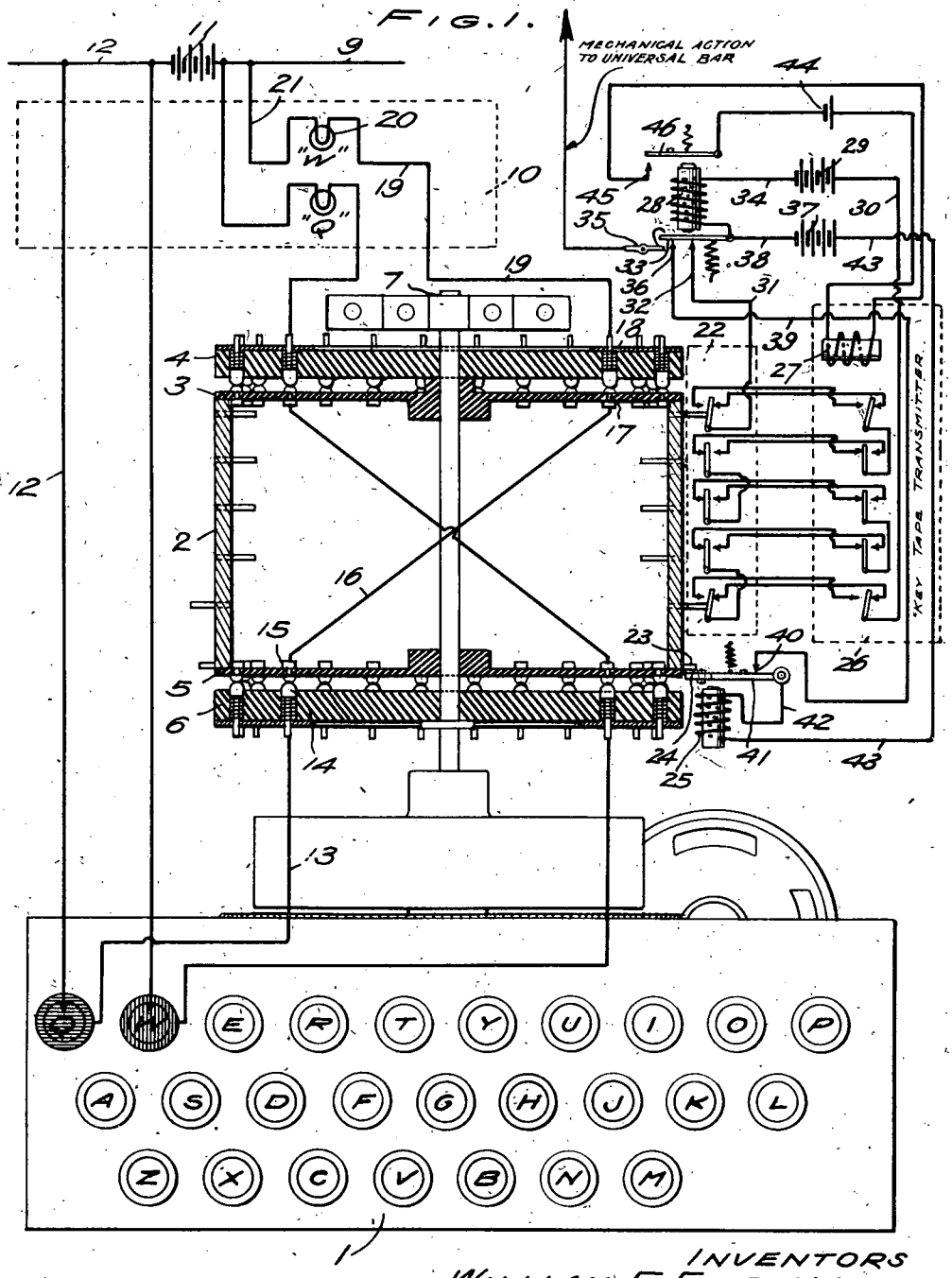
INVENTORS
WILLIAM F. FRIEDMAN
GEORGE A. GRAHAM
By Harris & Vandenberg
Charles A. Howe
ATTORNEYS

Jan. 28, 1936. W. F. FRIEDMAN ET AL 2,028,772

CRYPTOGRAPHIC SYSTEM

Filed Jan. 23, 1932 2 Sheets-Sheet 1

FIG. 1.



INVENTORS
WILLIAM F. FRIEDMAN
GEORGE A. GRAHAM
BY Francis H. Sandenwalder
Charles A. Howe
ATTORNEYS