This invention relates to cryptographic apparatus for auto-
matically enciphering and deciphering messages.

An object of the invention is the provision of a crypto-
graph with a keyboard for high-speed manual operation, a bank of indicat-
ing 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 con-
stantly 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.

The fundamental cryptographic principle of the present invention is as follows: Keyboard operation is cyclic in character and is performed with a cadence similar to that in teletype operation. During each cycle of keyboard operation, hereinafter referred to as the operating cycle, the successive alphabets of a complete set of 26 or more mixed cipher alphabets are presented in a fixed sequence, for potential employment in encipherment or decipherment. Only one of these cipher alphabets, however, is selected during each operating cycle and the selection is varied in successive operating cycles according to a very long cipher key established by means to be described.

Broadly speaking, the foregoing cryptographic operation is accomplished practically as follows: The operating cycle is divided up into 26 equal time-intervals by means of the distributor 4, and a letter may be enciphered (or deciphered) within any one of these intervals by means of the rotor 3 which is operatively coordinated with the

8

keyboard 1 and bank of indicating devices 2 associated with the rotor 3.
A specific time-interval is selected within each operating cycle by means
of the translator 6 which is associated with the distributor 4 and the
switchboard 7. The time-interval that will be selected in each case
varies with successive operating cycles according to a key which is
produced by the cam-wheel cipher-key mechanism 5. Each interval will
yield a different result for the same letter.

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
Z 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 record-
ing 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

4

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/is connected to X on the
face
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 seg-
ments 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 ele-
ments 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. Dis-
tributor 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.

5

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 pro-
jecting 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 prefer-
ably 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

6

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 banch mark so as to correspond
to a cipher key, this initial alignment will recur only after 100 x
99 x 97 x 91 x 89 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

7

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 switchboard 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 keyboard 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

9

on the other side of the switchboard, thence along one of the conductors
68 so 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 constant

10

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 98 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 translator 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

11

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, 13, 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, 3a,
3b, 3c, 3d, and 3e. 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 im-
parted to it by means to be described. The periphery of each rotor
3a to 3e 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 3a to 3e, 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 3a and 3e, 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 differ-
ent rotors 3a to 3e. 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 3a to 3e are to be set to a key, by aligning the letters on their peripheries at a bench march. 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 3a - e to the bank of solenoids 2 are shown diagrammatically in Fig. 3. In this figure stators 13 and 14, and rotors 3a to 3e correspond to the similarly designated stators and rotors of Fig. 2. The internal wirings of rotors 3a, 3b, 3c, and 3d are not reciprocal in pairs, as is the case with the single rotor 3 of Fig. 1, but are all random connections. The rotor 3e 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 3e serves as a means for reversing a current coming into the set of rotors from a contact in stator 13, passing through rotors 3a, 3b, 3c, 3d, and sending it back through rotors 3d, 3c, 3b, 3a 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 a 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
85, contact 112, lever 10, conductor 84) to a contact 115 in stator 13,
thence through the rotors and back to another contact 115 in stator 13
thence along conductor 86, lever 11, contact 113, solenoid "ς", back
to battery 18. Solenoid "ς" is actuated and the cipher resultant of
E is ς. 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 ς key of the keyboard it will be seen that the follow-
ing reciprocal deciphering circuit is established :   Battery 18, conductor
85, contact 114, lever 11, conductor 85, contact 115 in stator 13, through
and back through the rotors to contact 115, conductor 84, lever 10,
contact 111, solenoid "E" , back to battery. Thus, the plain-text re-
sultant of ς is E. In this manner a reciprocal enciphering-decipher-
ing 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 ψ (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
wirings; the relative order of rotors 3_a, 3_b, 3_c and 3_d 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 3_a to 3_e 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 permutative 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 arrange-
ments 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 signalling 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 letter 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 a contact 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 es-
tablishing 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 synchron-
ously 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 con-
trolled by the cam wheel mechanism through the intermediacy of said trans-
lator 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 s lected 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 striving the same sequentially and repetitively at a uniform angular velocity through all of their potential ciphering positions, each complete revolution of said a-lected 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 signal-
ing elements of said indicating mechanism; and means for varying said selec-
tion 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 opera-
tive 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 multi-
plicity 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 selec-
tion 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 connec-
tion 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 connec-
tion 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.
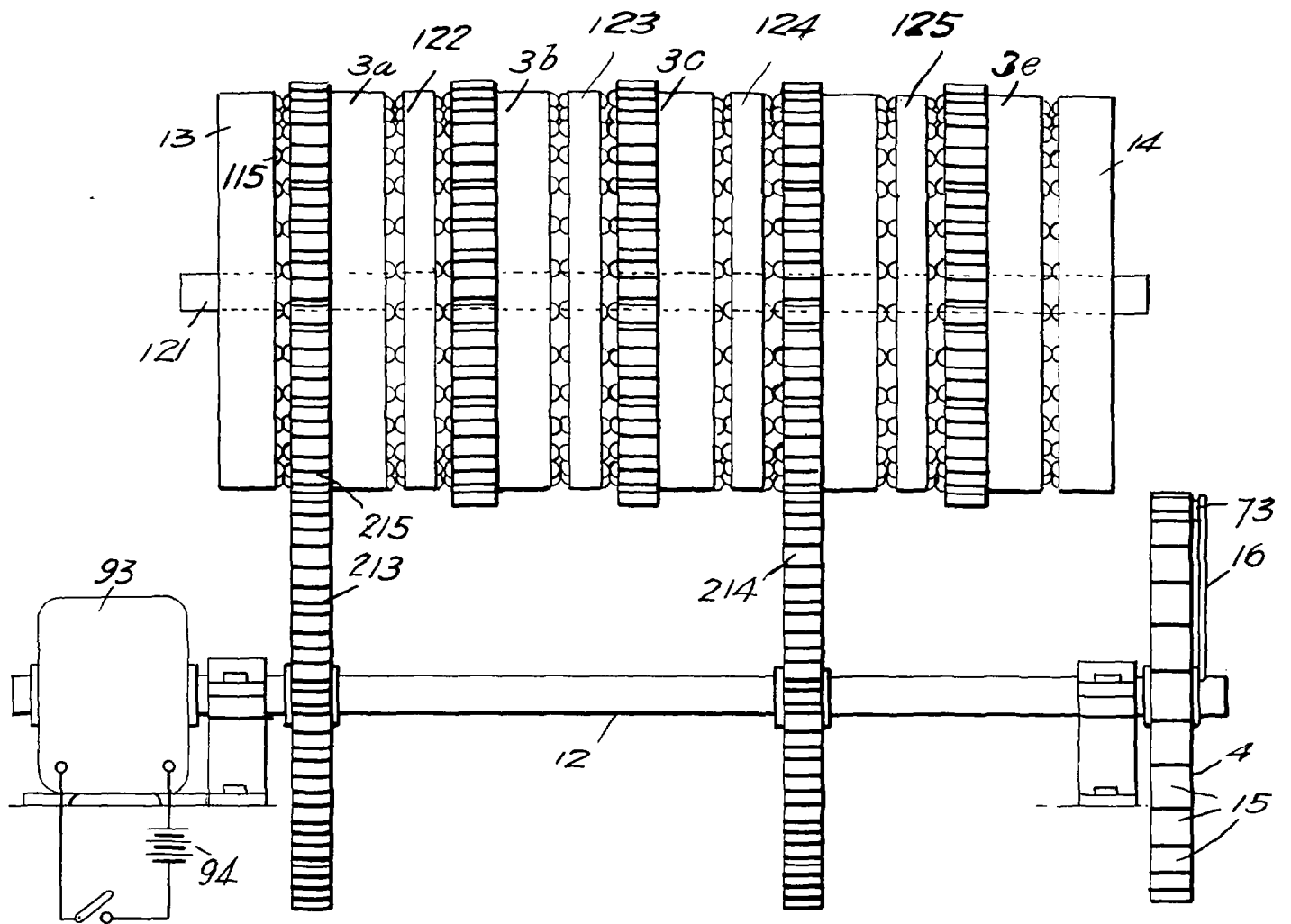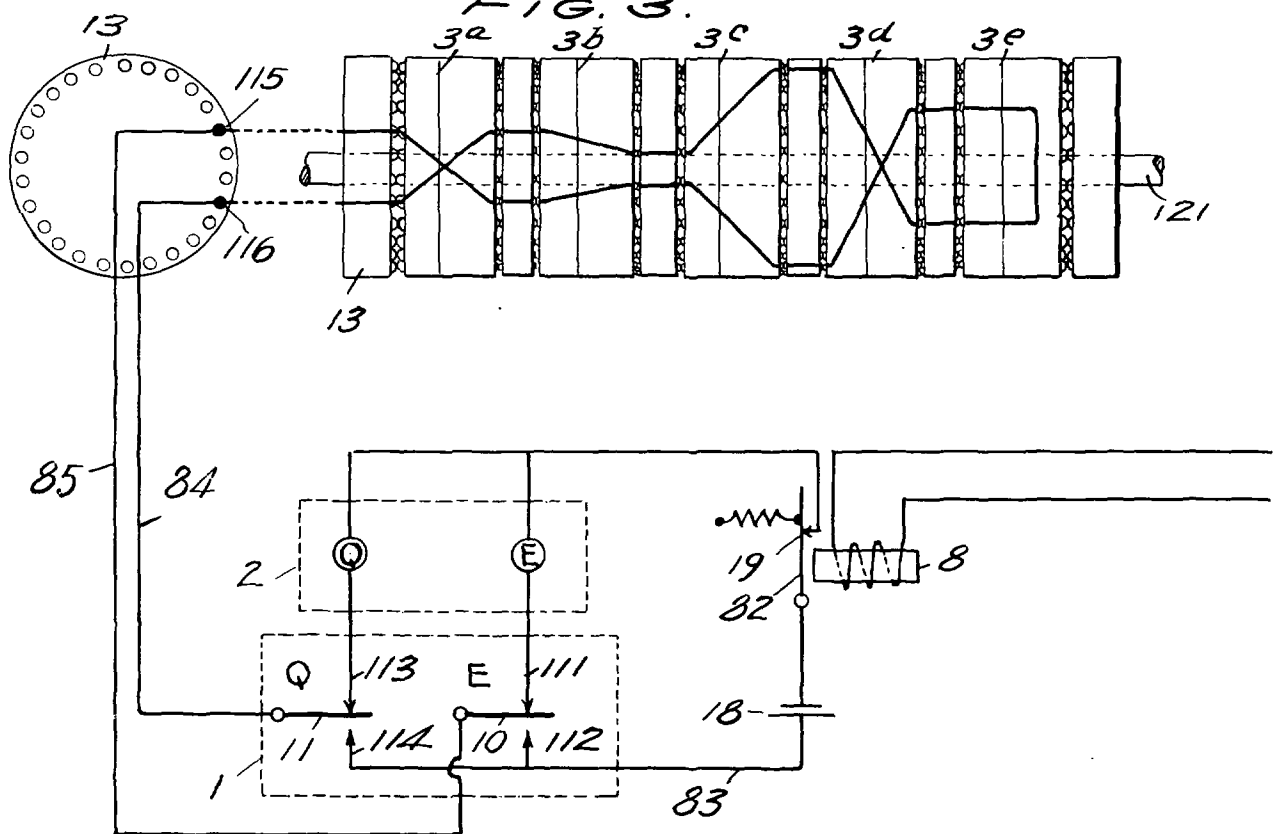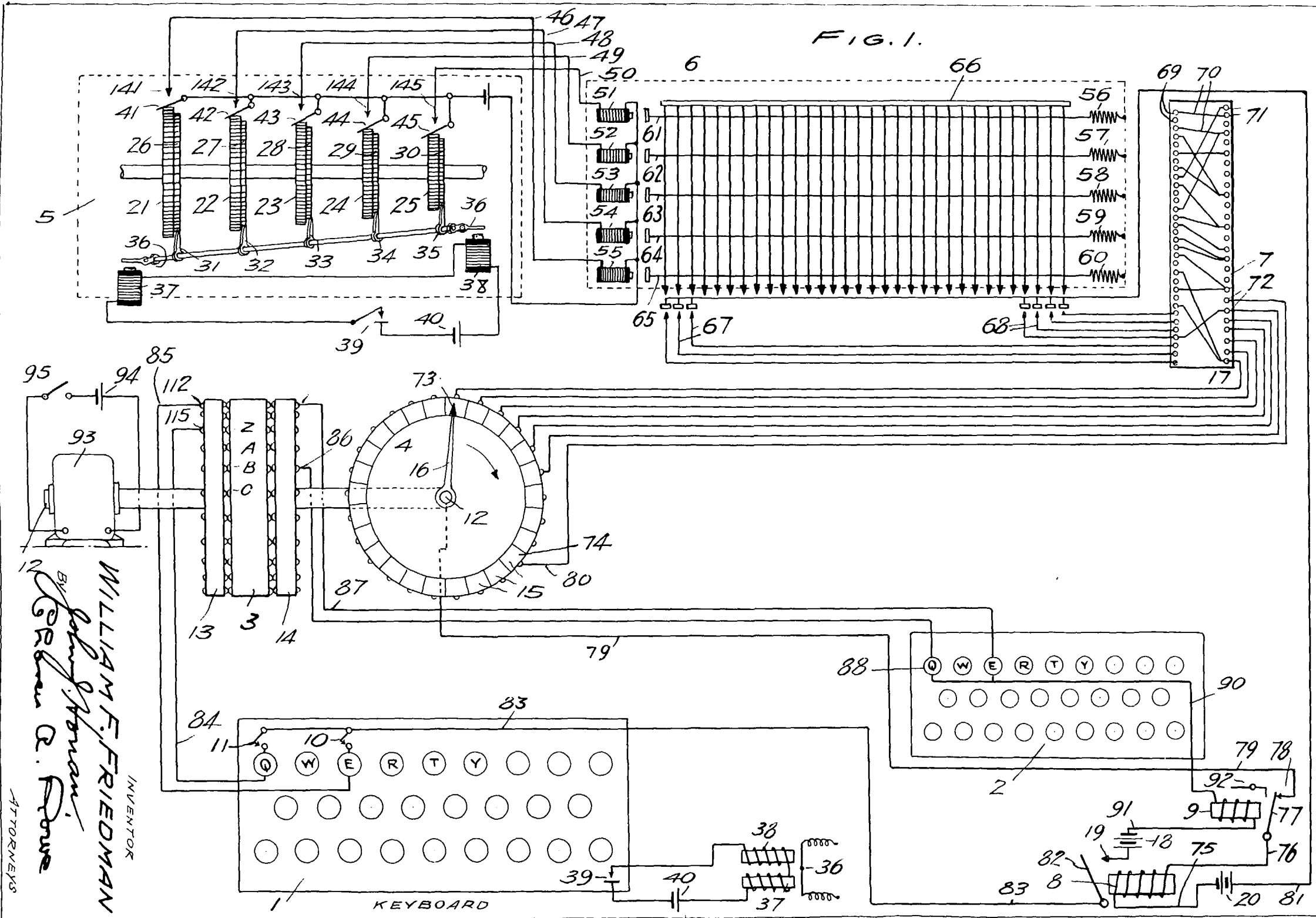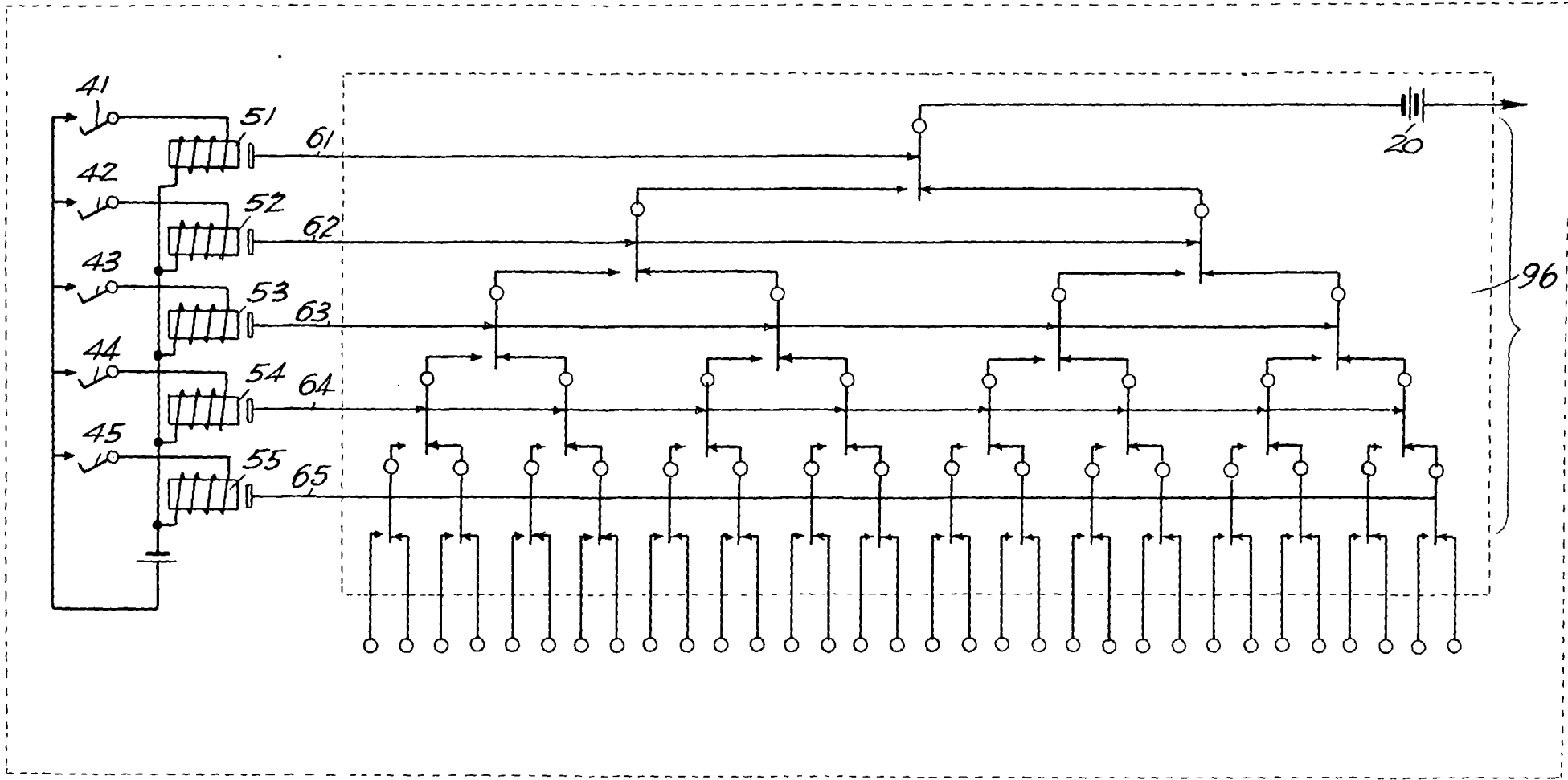
F I G. 2.

F I G. 3.

INVENTOR

WILLIAM F. FRIEDMAN

John J. Honan,

BY Charles a. Rowe

ATTORNEYS

F I G. 1.

WILLIAM F. FRIEDMAN
INVENTOR
By
John S. Freeman
Gödüs Q. Rowe
ATTORNEYS

KEYBOARD

FIG.4.

INVENTOR
WILLIAM F. FRIEDMAN
BY
ATTORNEYS