This invention deals with cryptographic machinery for automatically enciphering and deciphering messages. The 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 four figures. Fig. 1 is a diagramatic representation of the parts of the mechanism together with certain circuit arrangements. Fig. 2 is a diagramatic representation of means for imparting uniqueness to messages even when the latter are enciphered by the same keying sequence. Fig. 3 is a diagramatic representation of the electrical circuits applicable to the system shown in Fig. 2. Fig. 4 shows an alternative scheme for one of the basic elements of the mechanism shown in Fig. 1.

This invention deals with cryptographic machines and has for its object the production of a machine of simple design but of great cryptographic security.

The invention is described in connection with three figures. Fig. 1 is a diagrammatic representation of the parts of the mechanism together with certain circuit arrangements. Fig. 2 shows an alternative scheme for one of the basic elements of the mechanism shown in Fig. 1.

In Fig. 1 the principal elements consist of a keyboard 1, a bank of indicating devices 2, a rotatable 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 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, the keyboard 1 and bank of indicating devices 2. 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-intefval 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 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 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 stators 13 and 14. The rotor is made of bakelite or similar insulating material and consists of two ~~halves~~, a left-hand ~~half~~ and a right-hand ~~half each 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 ~~half~~ to those of the right ~~half~~, in a manner which is reciprocal in pairs. That is, if A on the left ~~half~~ is connected to X on the right ~~half~~, then X on the left ~~half~~ is connected to A on the right ~~half~~. Thus, with 13 paired contacts reciprocity in the enciphering-deciphering relationship is obtained without special switching arrangements therefor, ~~as in the case of certain other cryptographs employing rotating cipher commutators~~.

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 ~~with~~ 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 keyboard 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 ~~any number of these~~ a number of cams inserted in 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 keyboard 1, if these wheels are initially aligned at a bench mark so as to correspond to a cipher key, this initial alignment will ~~reappear~~ 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 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 ~~equivalent to~~ corresponding to keying characters and hereinafter referred to as keying characters.

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 ~~characters~~ combinations 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 ~~characters~~ combinations 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 ~~character~~ combination 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 energised. 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 cource 20, conductor 75, main relay 8, conductor 76, armature 77 nd 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 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 keyboard 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 contact 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 current 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 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, 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 imparted to it by means to be described. The periphery of each rotor 3a to 3e bears a collar 115 in which 26 gear teeth have

been cut so as to engage with gear wheels 113 and 114 which are mounted on shaft 12, the latter now corresponding to shaft 12 of Fig. 1. Gear wheels 113 and 114 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 113 and 114 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 113 or wheel 114 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 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 through 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 83, 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 85, 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 85, contact 116 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 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 connectors at switchboard 7.

(2) The composition of the rotors, that is their internal wirings; 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 113 and 114.

messages

It becomes obvious that even if two/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 113 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 113 and 114 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 113 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 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.