This invention relates to cryptographs and has for its object the provision of means for automatically and con involvely changing the cipher equivalents representing plain-text connecters so as to prevent any periodicity in this relationship.

Another ordect of the invention is the improvement of existing cryptographs employing a series of juxtaposed, rotatable, connection— changing mechanisms which provide an enormous number of alternative paths for the passage of an electric current corresponding to a message character, from the transmitting contacts of the keyboard to the indicating elements of the recording mechanism.

A further object is o provide means for the irregular and permutative displacements of the members of a set of circuit changing mechanisms so as to elicinate any predictable factors in the movements of the circuit changing mechanisms with the result that unauthorized persons, even though they may possess identical cryptographs, will be unable to decipher messages so enciphered.

The invention is explained in connection with he accompanying drawings, in which:

Fig. 1 is a diagrammatic view of a mechanism embodying the invention, employing one tape-transmitter;

Figs. 2 and I show diagrammatically the interacting relation of a plurality of tape-transmitters .

In Fig. 1, which is merely diagrammatic, there are shown the following elements all of which are well-known in the art applicable to modern cryptographs: The numeral 1 generally designates a standard typewriter

keyboard provided with a set of keys for closing a set of contacts corresponding to the 26 letters of the alphabet; the memeral 2 generally designates a recording or indicating device which may take the form of a set of magnets of a printing mechanism, or a bank of glow lamps to indicate by illumination of superimposed lettering the equivalents resulting from encipherment or decipherment; 3 generally designates a set of juxtaposed, rotatable circuit changers constructed in the form of cipher wheels or disks, mountable upon a common shaft and arranged to rotate relative to one another and to fixed end disks, in order to provide a large series of variable paths for the passa s of electric currents representing message characters, the exact path in each instance being determined by the relative rotatory positions of the whole set of cipher wheels and end disks at that instant. The essence of my invention consists in the addition of a set of cipher-wheel stepping mechanisms, generally designated by the numberal 4, which may be controlled by one or more tape-transmitters of the usual type employed in Baudot systems of printing telegraphy. In Fig. 1 only one such tape-transmitter is shown as at 5. In Fig. 2 two such transmitters are shown in interaction as at 5 and 5°; and in Fig. 3 three transmitters are shown in interaction as at 5, 5' and 5".

In cryptographs of this general character the principal reliance for cryptographic security is placed upon keeping secret the initial conditions as regards the relative positions and the arrangement of the cipher wheels at the beginning of the cryptographic operations. These initial conditions constitute the "key", and the latter usually consists of two parts. First, the specific horizontal permutation of the cipher

wheels upon the shaft, that is, the order of the wheels from left to right or right to left between the stationary disks must be indicated. Each cipher wheel consists of two rings of 26 contacts, one ring on the obverse face, the other on the reverse face; the contacts of the obverse face are connected, by insulated conductors passing through the wheel, to those of the reverse face in an entirely random manner. The cipher wheels bear identifying designations and are interchangeable as regards the order in which they may be inserted into their positions upon the shaft, and it is usual to agree upon a key which indicates that order. For example, in a cryptograph constructed for five cipher wheels, the key 4-1-5-2-5 may mean that cipher wheel number 4 is placed in the first position next to the left stationary disk, cipher wheel murbar 1, in the e cond position, and so on. The cipher wheels may be inserted on the shaft in a right side up or up side down position. Since the wirings within the respective wheels are different, it is obvious that each of the 10x8x6x4x2 or 3840 different permutations of the five wheels are available. Each such permutation will produce different cipher results from every other permutation because the complete path through the whole set of wheels is established by the juxtaposition of five separate paths, one in each wheel, The sequence or arrangement of the individual ciphe: wisels upon the shaft will hereafter be called the permutative key. The second part of the key is the specific alignment of identifying marks on the peripheries of the cipher wheels after they have been inserted on the shaft according to the permutative key. The periphery of each wheel bears a series of 26 identifying characters corresponding to the 26 stopping positions of the wheel as it is displaced by rotation on the shaft. The initial rotatory positions of the five cipher wheels relative to one another and to the stationary

end disks, as designated by the horisontal sequence of the identifying characters on their peripheries as aligned on a "bench mark" on the end disks, will be reavter be called the rotatory key. In cryptographs of the type under consideration the permutative key remains fixed, as a rule, throughout the encipherment of a message or a series of messages; the initial rotatory key usually changes from message to message.

Now in all cryptographs based upon the use of rotetable cipher wheels of the type referred to above, and arranged as indicated, means are embodied within the cryptograph for automatically changing the rotatory positions of the cipher wheels during the course of enciphering or deciphering a message; these bears are always of such a nature as to make these changes of a definite and predetermined character. For example, in Hebern, U.S. Patent So. 1,683,072, the fixed character of the successive rotatory movements of the cipher wheels is explained in quite a detailed manner, and the same is true as recards similar cryptographs produced abroad. The progression of the cipher wheels in these cases is cimilar to that of indicating meters or counting mechanisms, which are basically regular or periodic in their action. This regularity or periodicity of motion produces predictable relationships between the plain-text claracters and the eigher characters for any given initial rotatory key. Thus, should the cryptograph and cipher messayes fall into the hands of manthorised parties, the latter can place themselves in a mostion to decipher the messages largely as a result of the predetermined nature of the successive rotatory displacements of the cipher wheels. even though the initial keys may not be known.

The basic feature of my invertion is the elimination of this predictable factor and the provision of a medianism for displacing the cipher

wheels in an entirely irregular, speriodic manner. This is accomplished by means of the wheel-stepping mechanisms shown as at 4, and operated in the present embodiment by individual magnets which are controlled by the single tape transmitter 5 of Fig. 1, or by two or more tape transmitters as shown in Figs. 2 and 3. In this description I show a cryptograph with a set of five rotatable cipher wheels and a transmitter using a plural unit code based upon the permutations of two elements through five positions, but it is obvious that the invention is applicable to a cryptograph using a fewer or a greater number of cipher wheels and a plural-unit code of a different type than the well-known Emudot five-unit code.

maps transmitter 5 in Fig. 1 is of the type well known in printing telegraphy, but only one of the usual two bus bars are connected to current source in this case. The transmitter is operated by a tape bearing a series of perforations permuted in accordance with the Baudot code. The perforations in the tape control the action of the five contact members 6-10, which, in turn, through the circuit including power source 35, and conductors 21 to 32, inclusive control the action of the five magnets, 11, 12, 15, 14, 15, as a set of elements operable in a permutative manner, as will be shown subsequently.

The magnets 11 to 15, with their associated stepping mechanisms, which may be of the ratchet and pawl type, control, permutatively, the displacement, in step-wise manner, of the individual cipher wheels 16 to 20, and thus continuously vary, in an irregular, aperiodic manner, the rotatory positions of the five cipher wheels in encipherment or decipherment. It is assumed naturally that correspondents must be equipped with similar cryptographs and similar cipher wheels, wired identically, and that the correspondents are provided with identical key tapes for controlling the movements

of the cipher wheels. The exact initial permutative and rotatory key and the initial point of action of the key tape must also be the same between correspondents, and can be predetermined by agreement.

The working arrangement may be such that on the back stroke of any key of the keyboard, a contact 34, controlled by a universal bar on the keyboard is closed, and the circuit from power source 35, for operating the tape step-forward magnet 36, is closed. The next character on the tape is brought into play, the cipher-wheel magnets, il to 15, are operated and the cipher wheels are set to a new position for the encipherment (or decipherment) of the next character of the message.

The enciphering-deciphering circuits will now be set forth in detail. Let us assume that the cryptograph is to encipher a message. A switch control mechanism 65, carrying a series of 52 movemble contact members similar to the four shown at 37, 37'. 38 and 38'. all mounted on the same base, is set to "enciphering". This brings contact member 37 against contact 40, contact member 37' against contact 42, contact member 38 against contact 44, and contact member 38' against contact 45. Suppose key "A" on the keyboard is depressed. A current from power source 46 flows along conductors 47, 48, through closed contact 49, conductor 41, contact member 57*, contact 42, to 51, which is one of the contacts on the contacts on the left-end fixed disk; the current then continues along a signag path through the cipher wheels, emerging at 52, which is one of the contacts on the right-end fixed disk, thence along conductor 5%, contact 44, contact member 38, conductor 45, through lamp or indicator"Y", conductor 54, back to the other pole of power source 46. Lamp or indicator "Y" is energised and the cipher equivalent of "A" is "Y", for the particular setting of the cipher wheels shown in the figure. For

a different setting of the cipher wheels, depression of "A" would yield some other letter. If the cipher wheels are displaced each time key "A" is depressed, the respective cipher equivalents will be causally different, and will vary in a completely aperiodic manner so long as the displacements of the cipher wheels are aperiodic, as would be the case in my invention with a key tape consisting of a random sequence of Baudot perforations. The arrangement at the keyboard is such that on the release of any key a universal bar closes the circuit for operating the tape stepping mechanism as explained above, thus causing the particular Baudot character then at the key-tape transmitter to actuate the five magnets 11 to 15, and thus set up a new rotatory arrangement of the cipher wheels 16 to 20.

the control device 65 for bringing the cripto raph to the deciphering condition is set so as to bring contact member 37 against contact 55, contact member 37° against contact 56, contact member 38° against contact 57, and contact member 38° against contact 58. The cipher wheels 10-20 are assumed to be at exactly the same rotatory position they were in when "A" was enciphered and produced cipher "Y". Now depress key "Y" on the keyboard. A current from power source 46 flows along conductors 47, 59, closed contact 60 at "Y", conductor 61, contact member 38°, contact 58, conductor 62, contact 44, conductor 53, contact 52, thence through the cipher wheels, emerging at contact 51, thence along conductor 50, contact 42, conductor 63, contact 56, contact member 37, conductor 59, thence through through through lawp or indicator "A", conductors 64, 54 back to the other pole of nower source 46. Thus lamp or indicator "A" is actuated and cipher "Y" reproduces plain text "A".

The reciprocal relationship between all the plain text and cipher letters is accomplished in the same way; only four of the 52 contact members shown at 37, 37°, 38 and 38° are indicated in the drawing, but they are all mounted upon one base and are moved into their enciphering or decipherin; position by the single control 65 which moves them as a set to the right or to the left for enciphering or deciphering, respectively.

All 26 upper right-hand contacts on this moveable plate, similar to those at 40 and 44, are wired to the 26 contacts on the right-end fixed disk;

all 26 lower right-hand contacts of the moveable place, similar to those at 42 and 45, are wired to the 26 contacts on the left-end fixed disk.

This arrangement for effecting reciprocity in inciphering and deciphering is, however, not a part of my invention. This method and others for so-complishing the same purpose are known in cryptographs of this type.

The affect of various keying arrangements with the cryptograph of my invention will now be shown and will be taken up individually.

First, let us assume that the permutative key of cipher wheels and the key tape remain: the same for a series of messages. The key tape may be started at the same initial point for all messages or at different initial points for different messages. Assuming the former case, diversity of cipher resultants for identical plain-text messages may be brought about by different initial rotatory positions of the five cipher wheels. For example, a message beginning "Proceed at once", enciphered with the initial rotatory key "White", will yield a different cipher text from that enciphered with the initial rotatory key "Write". Thus, since there are available, with a set of five cipher wheels, 265 different initial rotatory keys, the potentialities of the cryptograph in this respect are apparent.

Now assume that the key tape is in the form of a continuous ring and can be started at different initial points. A messare enciphered with the same initial rotatory key can be enciphered in as many different forms as there are characters on the key tape; if it is 10,000 units in length, 10,000 versions of the same message can be produced by starting each message at a different initial point on the tape.

It goes without eaving that by using many different tapes, and changing the permutative key of the cipher wheels on the shaft, the cryptograph will afford an almost limitless diversity of cryptographic results.

All the foregoing variations are entirely speriodic in character, so that no cyclic phenomena such as are used in the analysis of the usual types of automatic cryptographs are available for solving as seages produced by the cryptograph of my invention.

Fig. 2 shows two tape-transmitters, 5 and 5°, jointly controlling the magnets 11 to 16, which are identical with similarly designated magnets of Fig. 1. In this arrangement two different cipher-key tapes in the form of continuous rings govern the operation of the tape transmitters. The tape passing through transmitter 5 brings the set of contact members 6, 7, 8, 9, and 10 against bus bar 66 or bus bar 67 in a permanentive manner; similarly, the tape passing through transmitter 5° brings the set of contact members 6°, 7°, 8°, 9°, and 10° against bus bar 66° or bus bar 67° in a permutative manner. The circuits are such that only when homologous contact members are in contact with opposite bur bars will current flow from power source 35 through the magnet controlled by this pair of homologous contact members. The tape stepping magnets 36 and 30° are controlled by a contact operated by the universal bar of the keyboard.

The object of such an arrangement wit, two interacting taps transmitters is to provide a very long resultant, or secondary cipher key by the interaction of two relatively short, primary keys. For example, suppose a circular caps containing 1000 characters is passed through tape transmitter 5, and another circular tape containing 999 characters is passed through tape transmitter 5. If the two tapes are started at given initial points and are moved forward synchronously by single steps, then these same initial points will not again present themselves simultaneously to the contact pins until a total of 999,000 steps have been made. Thus, two key tapes of 1000 and 999 characters produce a resultant key of 999,000 characters.

caused to interact to produce still longer resultant keys. For example, three tapes 1001, 1000, and 999 characters in length will produce by interaction a resultant key of 999,999,000 characters. Fig. 3 shows how three cipher-key tape transmitters would be interconnected to bring this about.

13'
Transmitters 5 and 5' interact to control relays 11', 12', 14', and 15'.

he arrectures 6'', 7'', 8'', 9'', and 10'', of the latter relays act in the same manner as do the contact members 6 to 10 and 6' to 10' of the tape transmitters 5 and 5', respectively. The interaction of the arrectures 6'' to 10'' with the contact members 6''' to 10''' of the third transmitter 5'', controls the operation of marmets 11 to 15, which serve the function indicated by identically numbered magnets of Figs. 1 and 2. The tape-satepping magnets 36, 36' and 36'' are all in the same circuit controlled by the universal bar of the keyboard, so that all three tapes are moved synchronously.

REF ID: A272912

By an extension of this manner of interconnecting tape transmitters and relays, it is possible to have a set of four, five, or more tape transmitters all interacting to control collectively the magnets of the cipherwheel stepping mechanisms.

It is one of the notable features of my invention that while employing all the permutations of the Baudot code, 32 in number, as keying characters, the final cryptogram is composed of only the usual 26 letters of the
ordinary alphabet. The six extra permutations (those other than the ones
representing the 26 letters of the alphabet), which, in systems using the
Baudot code as a basis for a cipher key, cause much difficulty, either in
their elimination by automatic means; or if the latter is not possible, in
their representation in written characters having standard equivalents in
the Morse code, have been automatically eliminated from the cryptograms,
since all the Baudot permutations have been excluded from direct interaction
with the message characters in my system.

This invention relates to cryptographs and has for its object the provision of means for submatically and continuously changing the eigher equivalents representing plain-text characters so as to prevent any periodicity in this relationship.

Another object of the invention is the improvement of existing cryptographs employing a series of justaposed, notatable, connection-changing mechanisms which provide an enormous number of alternative paths for the pararge of an electric current corresponding to a measure character from the transmitting contacts of the keyboard to the indicating elements of the recording mechanism.

A further object is to provide means for the irregular and permutative cisplacements of the members of a set of circuit changing measuraless so as to climinate any predictable factors in the movements of the circuit changing mechanisms with the result that unauthorized per one, even though they may possess identical cryptograph, will be unable to decipher measures so encolabored.

The invention is end incommention with the necompanying drawings, on where the a chaptan matter view of a trope in writing on the property of the particular of the particular

In Figure 1, which is merely discrementic, there are shown the following elements all of which are well-known in the art applicable to modern crypto-graphs: 1(5) a stransic typewriter, keyboard provided with a set of keys.

Frq S. 2 and 3 reflect of these are a file after the presented of the provided with a set of keys.

for closing a set of contrate corresponding to the 26 letters of the spacecally designates The Victorian of calabet; 2 for recording or indicating device which may take the form of a set of any actual of a printing measurable, or a brank of glow large to inviente by illumination of properlatored lettering the equivelents regulting Trust constants and as lead flower, it; I is a set of just poses, not table circuit mourtable paragers points at as in the for sof eigher sheels or disher mounted upon a someon and the remark of the restrict restricted to one enother and to fixed end in the new street, provided in a purplet of veriable paths for the passage of in their marks to represent in the characters, the exact path in each that rate sein actor inc. by the relative rotatory positions of the whole set of them. The espence of my invention considered designator by the harm of it is sunglet in the resultion of () a set of disser-sheel stepping mechanisms, probability on or or type-transitter of the usual type exployed in ... of the or or printing telegraphy. In hig. I only one such tope-trans-Hence it is for the second to the small transmitters are shown in interwas 5, 5 and 5 " + stlm., the limit. 3 three transmitters are shown in interaction.

on the man of the general character the principal religace for any to make the placed upon adeping secret the initial conditions.

Adative the man recommendation of the clopher wheels at the beginning or the anyste required position. There initial conditions constitute the man anyste required positions. There initial conditions constitute the man anyste required positions of the parts. First, the specific horizontal

wheels from left to right or right to left between the stationary disks

Fact.

must be indicated. The cipher wheel consists of two rings of 26 contects, one must be indicated. The other

one on the obverse face, one on the reverse face; the contacts of the by insulated conductors bassing through the wheel, obverse face are connected to those of the reverse face in an entirely random

regards the order which they may and it is usual to agree upon a key which is become that order in thick they are to

be mounted upon the shaft for example, in a cryptograph constructed for five cipher wheels, the key 4-1-3-2-5 may meen that cipher wheel number 4 is placed in the first position next to the left stationary wisk, cipher wheel number 1, in the second position, and so on. The eigher wheels may be inserted on the shaft in a right side up or up wide down position. Since the wirings within the respective wheels are different, it is obvious that each of the 10x4x6x4x2 or are available. Each puch parmutation 3340 different permutations of the five wheels, will produce different cipher from every other permutation results because the complete path through the whole set of wheels is established by the juxtaposition of five separate paths, one in each wheel. The sequence or arrangement of the individual ciphor wheels upon the shaft will hereafter be called the permutative key. The second part of the key is the specific elignment of identifying marks on the peripheries of the cipher wheels after they have been inserted on the shaft according to the permutative key. The periphery of each wheel bears a series of 26 identifying characters corresponding

permutation of the cipher wheels upon the shaft, that is, the order of the wheels from left to right or right to left between the stationary disks

Each

must be indicated. The cipher wheels consists of two rings of 26 contacts, one rings the other

obverse face are connected to those of the reverse face; the contacts of the obverse face are connected to those of the reverse face in an entirely random

manner. The cipher theels bear identifying designations and are interchangeable

regards the order in which they may and it is usual to agree upon a key which is
become that order is which they are to

be mounted upon the shaft. For example, in a cryptograph constructed for five cipher wheels, the key /-1-3-2-5 may mean that cipher wheel number 4 is placed in the first position next to the left stationary wisk, cipher wheel number 1, in the second position, and so on. The eigher wheels may be inserted on the shaft in a right side up or up side down position. Since the wirings within the respective wheels are different, it is obvious that each of the 10x8x6xxx2 or are available. Each puch permutation 3340 different permutations of the five wheels, will produce different cipher from every other permutation results because the complete path through the whole set of wheels is established by the juxtaposition of five separate paths, one in each wheel. The sequence or arrangement of the indivioual ciphor wheels upon the shaft will hereafter be called the permutative key. The second part of the key is the specific alignment of identifying marks on the peripheries of the claher wheels after they have been inserted on the shaft according to the permutative key. The periphery of each wheel bears a series of 26 identifying characters corresponding

to the 26 stopping positions of the wheel as it is displaced by rotation on the shaft. The initial rotatory positions of the five cipher wheels relative to one another and to the stationary fend disks, as designated by the sequence of as aligned on a "benein mark" on the end disks, the identifying encreaters on their peripheries, will hereafter be called the rotatory key. In cryptographs of the type under consideration the permutrive key rearing fixed, as a rule, throughout the encipherment of a message or a series of messages; the initial rotatory key usually changes from message to message.

Now in all crypto raphs based upon the use of rotatable cipher wheels of

the type referred to above, and arranged as indicated, means are embodied than the or stormal for automatically charging the rotatory positions of during the course of enalthering or deciphering a message; these methic are always of such a nature at to make these changes of a definite and predetermined character. For example, in Hobern, U.S. Patent No. 1,683,072, the fixed character of the successive rotatory movements of the eigher wheels is explained in quite a detailed manner, and the same is true as regards similar The progression is the cipher wheels in these cases is similar to that il crypto raphs produced abroad. This invariability of motion produces predictable relationships between the plain-test characters and the cipher characters for ony liven initial permutative and rotatory key. Thus, should the cryptograph and cipher messages fall into the hands of unauthorized parties, the latter can place themselves in a position to decipher the messages largely as a result predetermined nature of the successive rotatory displacements of the

medicating meterder ecu. ting no handand, which we basically,

cipher wheels, even though the initial keys may not be known.

The basic feature of a invention in the elimination of this preciation factor and the province of a section of the cipher heals in which are a preciated as a preciate of the compliance by means of the cipher of entirely importate of the cipher. This is accomplished by means of the cipher attacking the calculation and a section of the cipher of the preciation as an including the control of the cipher of the control of the control of the cipher of

The true smitters of in right in of the type well known is printing to Light up, and only one of the usual too our bars are connected to current course in this case. The truesmitter is operated by a tape bearing a series of pure smallons permuted in accordance with the Brudot code. The perforations is the type control the action of the five control anothers 6-10, which, in turn, through the circuit including power source 35, and conductors 21 to 32, accordant control the action of the five regacts, 11, 12, 17, 14, 15, as a set of clements of the five regacts, 13, 14, 15, as a set of clements

The magnets 11 to 15, with their associated stepping mechanisms, which may be of the ratchet and pawl type, control, permutatively, the displacement, in steppwise manner, of the individual cipher wheels 16 to 20, and thus continuously very, in an irregular, aperiodic manner, the rotatory positions of the five cipher wheels in encipherment or decipherment. It is assumed naturally that correspondents where equipped with similar cryptographs and similar cipher wheels, wired identically, and that the correspondents are provided with identical key tapes for controlling the movements of the cipher whoels. The exact initial permutative and rotators key and the initial point of action of the key tape must also be the same between correspondents, and can be predetermined by agreement.

of the keyboard, a contact, 3/, controlled by a universal bar on the keyboard is closed, and the circuit from power source, 35, for operating the tape of the play, the cipher-wheel magnets, 11 to 15, are operated and the cipher wheels are set to a new position for the encipherment (or decipherment) of the next character of the meant character

The enciphering-deciphering director will now be set forth in detail.

Courte Contractor to encipher a message. A (dereg mechanism)

65 63, carrying a series of 52 moveable contact members similar to the four shown at 37, 37', 38 and 38', all mounted on the same base, is set to "enciphering". This brings contact member 37 against contact 40, contact member 37' against contact 42, contact member 33 against contact 44, and contact member 33' against contact 15. Suppose key "A" on the keyboard is depressed. A current from power source /26 flows along conductors 47, 43, through closed contact 49, conductor 41, contact member 37', contact 42, to 51, which is one of the contacts on the left-end fixed disk; the current then continues along a zigzag path through the cipher wheels, emerging at 52, which is one of the contacts on the right-end fixed disk, thence along conductor 53, contact 44, contact member 33, conductor 43, through lamp or inuicator "Y", conductor 5/, back to the other pole of power source 46. Lamp or indicator "Y" is energized and the cipher equivalent of "A" is "Y", for the particular setting of the cipher wheels shown in the figure. For a different setting of the cipher wheels, depression of "A" would yield some other letter. If the cipher wheels are displaced each time key "A" is depressed, the successive cipher equivalents will be different, and will vary in a completely aperiodic manner so long as the displacements of the cipher wheels are aperiodic, as would be the case in my invention with a key tape consisting of a random sequence of Baucot perforations. The arrangement at the keyboard is such that on the release of any key a universal bar closes the

causing the particular Baudot character then at the key-tape transmitter to actuate the five magneto 11015, and thus set up a new rotatory arrangement of the cipher wheels 1002).

Let up now reverse the operation and decipher. In this case the screwn is, for bringing the cryptograph to the decimering condition is set so as to brin controt lember 37 against contact 55, contact member 37' against contact 56, contact member 33 against contact 57, and contact member 33' against control 53. The cipher cheels 10-10 are assumed to be at emactly the same rotator, position this were in when "A" was enciphered and produced eigher "a". No see rear key "Y" on the leybours. A surrent from power source 26 Tion whose most meters (7.5), aloses contrated at """, conquetor 61, contact ember (1), contact 5: conductor 62, contact 1/, conductor 53, contact 52, thereof through the eigher wheels, emerging at contact 51, thence along conenetor 50, contact 12, concactor 63, contact 55, contact member 37, conductor), thence through lemp or indicator "A", conquetors 64, 54 back to the other pole of lower source /6. Thus lamp or indicator "A" is actuated and cipher "Y" reproduces plain text "Y".

The reciprocal relationship between all the plain text and eigher letters is accountished in the same way; only four of the 52 contact members shown at 37, 37', 33 and 33' are indicated in the drawing, but they are all mounted upon

one base and are moved into their enciphering or deciphering position by the critical single cores 65 which moves them in a set to the right or to the left for enciphering or deciphering, respectively. All 26 upper right-hand contacts on this moveable plate, similar to those at 40 and 44, are wired to the 26 contacts on the right-end fixed disk; all 26 lower right-hand contacts of the moveable place, similar to those at 42 and 45, are wired to the 26 contacts on the left-end fixed disk. This arrangement for effecting reciprocity in enciphering and deciphering is, however, not a part of my invention. This method and others for accomplishing the same purpose are known in cryptographs of this type.

The effect of various keying arrangements with the cryptograph of my invention will now be shown and will be taken up inciviously.

First, let us assume that the horizontal permutative of cipher wheels and the key tape remains the same for a series of messages. The key tape may be storted at the same initial point for all messages or at different initial points for different messages. Assuming the former case, diversity place—text of cipher resultants for identical messages may be brought about by different initial rotatory positions of the five cipher wheels. For example, a message beginning "Process at once", enclosered with the initial rotatory key "White", will yield a different cipher text from that enclosered with the initial rotatory key "write". Thus, since there are available, with a set of five cipher anects, 265 different initial rotatory keys, the potentialities of the crystoresh in this resuct are apparent.

Now assume that the key tape is in the form of a continuous ring and can be started at different initial points. A message enciphered with the same initial rotatory key can be enciphered in as many different forms as there are characters on the key tape: if it is 10,000 units in length, 10,000 versions of the same message can be produced by starting each message at a different initial point on the tape.

It goes without saying that by using many different tapes, and changing the horizontal permutative of the cipher wheels on the shaft, the cryptograph will afford an almost limitless diversity of cryptographic results.

All the foregoing variations are entirely aperiodic in character, so that no cyclic phenomena such as are used in the analysis of the usual types of automatic cryptographs are available for solving messages produced by the cryptograph of my invention.

Fig. 2 shows two tape-transmitters, 5 and 5', jointly controlling the magnets 11 to 15, which are identical with similarly designated magnets of Fig. 1. In this arrangement two different cipher-key tapes in the form of continuous rings govern the operation of the tape transmitters. The tape passing through transmitter 5 brings the set of contact members 6, 7, 6, 9, and 10 against bus bar 60 or bus bar 60 in a permutative manner; similarly, the tape passing through transmitter 5' brings the set of contact members 6', 7', 3', 9', and 10' against bus bar 60' or bus bar 60' in a permutative

in contact with opposite bus bars will current flow from power source 33 through the magnet controlled by this pair of homologous contact members. The tape controlled by this pair of homologous contact members. The tape stepping magnet: 36 and 36' are returned by a contact controlled by the universal bar of the meyboard.

The object of such an arrange until to provide a very long resultant.

or secondary eigher rep by the interestion of two relatively short, primary asym. For example, purpose a simular type containing 1000 characters is some a turning type true dither 5, and mother simular type containing 999 commoters is passed throw a type treasultter 51. If the two types are street, as even initial points and are moved forward synchronously by single that, as even a term of the such a factor of the such a factor initial points will not again present themselves.

The treatment in a safety that he such a 1999,000 attendance and the such as the such as

to interact to produce still longer resultant keys. For example, three tapes 1991, 1999, and 999 characters in length will produce by interaction a regulation key of 991,399,000 characters. Fig. 3 shows how three cipher-key tape translatters would be interconnected to bring this about. Transmitters 5 and 51 interact to control relays 111, 121, 131, 141, and 151. The armatures 68, 78

3", 9", and 10", of the latter relays act in the same manner as do the contact members 6 to 10 and 6' to 10' of the tape transmitters 5 and 5', respectively. The interaction of the armatures 6" to 10" with the contact members 6" to 10" of the third transmitter 5", controls the operation of magnets 11 to 15, which serve the function indicated by identically numbered magnets of Figs. 1 and 2. The tape-stepping magnets 36, 36' and 36" are all in the same circuit controlled by the universal bar of the keyboard, so that all three tapes are moved synchronously.

()

By an extension of this manner of interconnecting tape transmitters and relays, it is possible to have a set of four, five, or more tape transmitters all interacting to control collectively the magnets of the cipher-wheel stopping mechanisms.

It is one of the notable features of my invention that while employing all the permutations of the Baudot code, 32 is number, as keying characters, the final cryptogram is composed of only the usual 26 letters of the ordinary alphabet. The six extra permutations (those other than the ones representing the 26 letters of the alphabet), which, in systems using the Baudot code as a basis for a cipher key, cause much difficulty, either in their elimination by automatic means; or if the latter is not possible, in their representation in written characters having standard equivalents in the Morse code, have been sutomatically eliminated from the cryptograms, since all the Baudot permutations have been excluded from direct interaction with the message characters in my system.