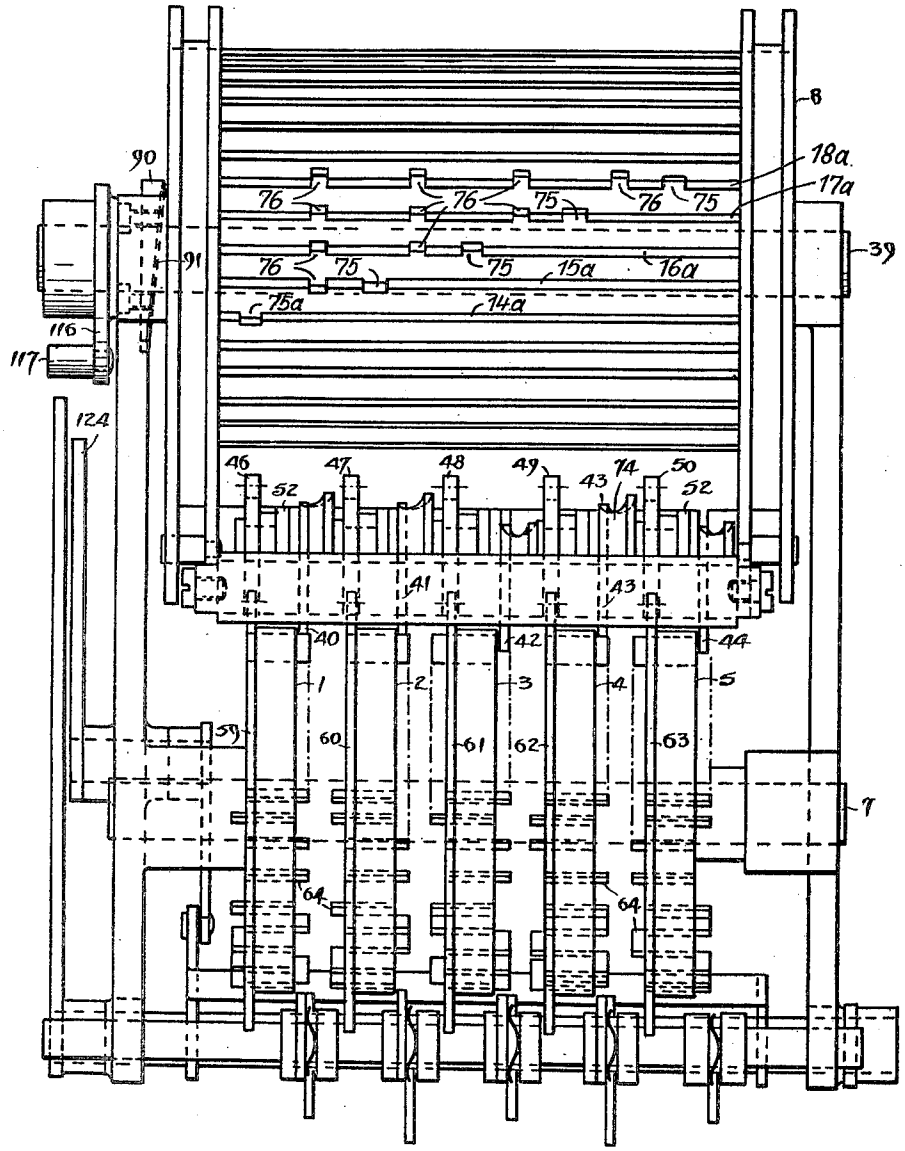
Oct. 31, 1961 S. NYBERG 3,006,081

ENCODING KEYING DEVICE

Filed June 8, 1959



INVENTOR

STURE NYBERG

BY Albert C. Johnston

ATTORNEY

United States Patent Office 3,006,081 Patented Oct. 31, 1961

3,006,081

ENCODING KEYING DEVICE

Sture Nyberg, Zug, Switzerland, assignor to Anstalt Europäische Handelsgesellschaft, Vaduz, Liechtenstein

Filed June 8, 1959, Ser. No. 818,765
Claims priority, application Switzerland June 7, 1958
1 Claim. (Cl. 35—3)

The present invention relates to keying devices for cryptographic apparatus.

More particularly, this invention is applicable to keying devices for cryptographic apparatus of the known type which comprises a series of keying members each of which is cyclically movable step by step through a limited number of equidistant positions, and each of which carries a plurality of control elements which are selectively settable thereon to an active or an inactive position. These known keying devices further may comprise a series of sensing means, one for each keying member, for sensing whether said keying member occupying one of its said limited number of positions, presents at a fixed sensing station a control element in active position. Moreover, the devices here considered comprise a set of cyclically operable actuating means for moving the said keying members each under the control of such of the said sensing means as are associated with one or more of the other keying members, said actuating means being adapted to move the respective keying members through a number of steps depending on whether an active control element is presented at the respective sensing station or stations by said one or more other keying members.

Still more particularly, the said keying members may take the shape of individually stepwise rotatable key wheels carrying near their periphery a plurality of control pins each of which is axially shiftable between an active position in which it projects from its respective key wheel, and an inactive retracted position. The sensing means then may consist of cam levers each cooperating with one of the key wheels so as to assume an active position when the pin presented by that wheel at a certain fixed sensing station is in active position, and a different or inactive position when it is not. The said actuating means may take the shape of a rotatable drum carrying on its periphery a series of axially shiftable bars each featuring one or more radially projecting lugs. These lugs may be of two kinds: Those of the first kind are shaped and positioned for cooperation each with an inclined face on one of the said cam levers whenever that cam lever is in its active position while the lug is carried past that inclined face in the course of the rotation of the drum, whereby any bars which happen to have such lugs cooperating with any cam levers in active position are shifted axially from their basic or inactive position into a displaced or active position. The lugs of the second kind are shaped and positioned on the respective bars in such a manner that, whenever the respective bar is in its said "displaced" position, each of these lugs of the second kind engages one individually rotatable intermediate gearwheel. Each intermediate gearwheel is in constant mesh with another gearwheel and each of these other gearwheels is fixed to one of the key wheels. Of course, each of these other gearwheels may be integral with the respective key wheel rather than fixed to it. Thereby, as the drum is rotated, each lug of the second kind of any bar having previously been shifted to its displaced or active position on the drum, temporarily engages its corresponding intermediate gearwheel and causes the respective key wheel to rotate through a predetermined number of steps.

Obviously, the number of teeth of the gearwheel fixed to, or integral with, each key wheel should be equal to, or an integer multiple of, the limited number of equi-

distant angular positions which that key wheel can assume in the course of one of its revolutions, and the angular spacing of the control pins on the key wheel should be equal to, or an integer multiple of, the number of the said equidistant angular positions of the key wheel. Preferably, the said limited number of angular positions which can be assumed by the key wheel should be a prime number.

A keying device of this kind has been fully described and claimed in United States Patent No. 2,765,364 granted to Boris Caesar Wilhelm Hagelin on October 2, 1956. It is easily recognisable that keying devices of this kind offer the possibility of obtaining a great variety of sequences of ever varying combinations of angular positions of the several key wheels.

However, the present invention is also applicable to keying devices in which the keying members, sensing means and actuating means are of a different nature such as keying members in the shape of electric commutators, sensing means in the shape of electric circuits controlled by such commutators, and actuating means in the shape of electromagnetic pawl actuators for the said commutators.

In keying devices of the type broadly outlined above, it has been usual to provide keying members having each as high a prime number as possible of positions through which it is movable, and it also has been usual to have each keying member moved by one step each time the device is actuated. Thereby, a comparatively long repetition cycle was obtained since that cycle comprised a number of actuations which was equal to the product of the prime numbers used.

With electric keying apparatus of the kind just outlined, a somewhat different arrangement has been usual in that the rotary commutators have been actuated in the manner of counter wheels, i.e. a first commutator has been advanced one step each time the device is actuated and each time it has completed one revolution it causes a second commutator to be advanced one step; each time that second commutator has completed one revolution, it causes a third commutator to be advanced one step, and so on until the last commutator provided has completed one revolution. The repetition cycle in that case as well is equal to the product of the numbers of steps which the several wheels require for completing one revolution.

Development in the analysis of cryptograms since the second world war has been such, however, that a control system in which the keying members are stepped forward in a regular or linear mode can no longer be considered as safe since under certain conditions the knowledge of comparatively few data suffices to calculate the whole program according to which the keying members have been moved in ciphering the text. Therefore, one has replaced the system in which the keying members are advanced regularly, by systems comprising an irregular advancement of the several keying members, as evidenced by the aforemention United States Patent No. 2,765,364 to B. C. W. Hagelin. With such irregular programs, it is also possible to obtain the most varied key sequences, but it is difficult in certain cases to calculate the length of the minimum repetition cycle after which all keying members will have reverted to their starting position. Analyses have shown that depending on the setting of such a keying mechanism the repetition cycle may be considerably shortened, which fact is very undesirable because it facilitates unauthorized deciphering.

One expedient to that situation has been found in causing the irregular program to affect part only of the keying members of the device while the remainder of these members continued to be advanced in a regular manner, e.g. one step only on each actuation of the device. Thus, on one hand, detection of the internal operation and

mechanism of the device has been rendered difficult while on the other hand, a minimum length of the repetition cycle is safeguarded.

Unavoidably, however, the length of the repetition cycle is reduced from the absolute possible maximum since not all of the keying members fully contribute to the lengthening of the period.

The need for a control programme which comprises an irregular sequence of advancement step numbers of the keying members and which provides the longest possible mathematically calculable period has led to the present invention.

The main object of this invention is to provide a keying device in which each keying member is imparted with an irregular sequence of step numbers but in which the repetition period is calculable and a minimum length of that repetion period is safeguarded.

In the accompanying drawing, one embodiment of the invention is schematically represented and will now be explained by way of example. Since this embodiment is substantially an improvement on the keying device shown and described in the aforesaid United States Patent No. 2,765,364, granted October 2, 1956, to Boris C. W. Hagelin, FIGS. 1, 3, 4 and 7 to 10 of that patent and their description, inasmuch as they relate to the keying device itself, should be considered an integral part of the present specification and should be referred to.

The accompanying drawing, like the said patent, discloses a keying mechanism comprising five individually rotatable key wheels, **1**, **2**, **3**, **4**, **5** mounted on a fixed shaft **7**, each bearing a number of pins **64** which project longitudinally either to the right or to the left parallel to the shaft **7**. The peripheral edges of the wheels **1** through **5** are milled to form spur gears **59** through **63**, respectively. The number of pins **64** in each key wheel **1**, **2**, **3**, **4**, **5** is the same as the number of teeth in the corresponding gears **59** through **63**; these numbers should have no common denominators and preferably be primes.

Key wheels **1** through **5** face a slide bar drum **8** mounted on a parallel shaft **39**. Drum **8** is radially slotted at its periphery to slidably mount a number of slide bars, numbered 9 through 38 in the patent. Shaft **39** is connected to an operating mechanism such as a crank **117**.

Between key wheels **1** through **5** and slide bar drum **8** is a shaft **45**, not illustrated, on which are pivoted five guide arms **40** through **44** which are independently movable. Each guide arm **40** through **44** has a forwardly projecting lug **73**, not illustrated, which cooperates with the pins **64** of key wheels **1** through **5** under certain conditions, and an oblique surface **74**, shown clearly in FIG. 5 of the patent, which cooperates with slide bars 9 through 38. Means fully described in the patent are provided for locking guide arms **40** through **44**.

Adjacent the guide arms **40** through **44** are five intermediate gear wheels or pinions **46** through **50** which are independently journaled at **51**, not illustrated, on fixed brackets or angle arms **52**, each pinion corresponding to a key wheel.

Each of the said slide bars is provided with at least two projections or lugs. One kind of lug **75** is short and acts as a driving tooth on one of the intermediate pinions or wheels **46** through **50**. A second kind of projection or lug **76** is employed on each slide bar. Lugs **76** are designed to contact oblique guide surfaces **74** of those guide arms **40** through **44** which are in active position and cause selected slide bars to slide to the left as drum **8** rotates. Guide arms **40** through **44** may be regarded as having active or inactive positions with respect to the slide bars depending upon whether or not the guide arms are pivoted toward drum **8** to a position where cam surfaces **74** can act on lugs **76**. Of course, only those slide bars will be moved to the left which have lugs **76** positioned to be acted upon by those guide arms **40** through **44** which are in active position. As drum **8** turns all those slide bars which have been moved to the left by

the action of active cam surfaces **74** are returned to the right undisplaced position by an obliterating bar **90** which has an active cam surface **91**.

According to the patent, in contradistinction to the present invention, a plurality of slide bars (9 through 14) have lugs **75** in the same relative position and each will rotate intermediate gear wheel **46** when moved to the left into active position by those guide arms **40** through **44**, respectively, which are rotated into active position toward drum **8** by the action of pins **64** of key wheels **1** through **5** upon projecting lugs **73**, not illustrated.

While in the mechanism shown in the prior patent, thirty slide bars (9 through 38) are provided, the number and position of the lugs **75** and **76** of which differ from one slide bar to the other somewhat at random, as exemplified in FIG. 6 of that patent, the embodiment of the invention which will now be described features only one non-slidable bar **14***a* and four slide bars numbered **15***a*, **16***a*, **17***a*, **18***a*, respectively, in their place on drum **8**. The non-slidable bar **14***a* is provided with only one lug **75***a* which in any case acts as a driving tooth on the intermediate wheel **46**. The first slide bar **15***a* is provided with one lug **75** which acts as a driving tooth on intermediate wheel **47** when the slide bar is in its displaced position, and with a single lug **76** in such position that bar **15***a* is displaced to the left on rotation of drum **8** whenever guide arm **40** has been shifted to its active position by an active pin on key wheel **1**. The second slide bar **16***a* again has one lug **75** of the first kind, which cooperates with intermediate wheel **48** when the slide bar is its displaced or active position, and with two lugs **76** in such positions, respectively, that bar **16***a* is displaced to the left when guide arms **40** or **41**, or both, are in active position. Similarly, slide bar **17***a* has one lug **75** of the first kind adapted to cooperate with intermediate wheel **49**, and three lugs **76** whereby slide bar **17***a* is shifted to the left whenever any one or more of guide arms **40**, **41** and **42** is or are active. Finally, a single lug **75** on slide bar **18***a* is positioned for cooperating with intermediate wheel **50** when that bar is active, and four lugs **76** for shifting the bar **18***a* into active position whenever any one or more of the four guide arms **40**, **41**, **42** and **43** is or are active.

Therefore, whenever drum **8** effects one full turn and if the pin **64** on key wheel **1** which is in position for cooperation with guide arm **40** is in active condition and therefore has moved the latter into active position as well, the four lugs **76** of slide bars **15***a*, **16***a*, **17***a* and **18***a* which cooperate with guide arm **40** will displace these slide bars to the left. Thereby, the lugs **75** of all four slide bars will engage intermediate wheels **47**, **48**, **49** and **50**, respectively, and cause them to advance key wheels **2**, **3**, **4** and **5** each by one step. Also, lug **75***a* of non-slidable bar **14***a* will engage intermediate wheel **46** and advance key wheel **1** by one step as well.

If, however, the relevant pin **64** on key wheel **1** is not one in active condition, guide arm **40** will not become active to engage lugs **76** of any of the slide bars. On the other hand, it may be that an active pin **64** on key wheel **2** has carried guide arm **41** into active position, in which case it will engage lugs **76** of slide bars **16***a*, **17***a* and **18***a*, thus causing the lugs **75** of these bars to engage intermediate wheels **48**, **49** and **50** and thereby to rotate key wheels **3**, **4**, and **5** by one step. If guide arm **41** is inactive as well, due to the absence of an active pin **64** on key wheel **2**, but if there is such an active pin on key wheel **3** having cooperated with guide arm **42** to make the latter active, rotation of the drum **8** will cause that guide arm **42** to engage lugs **76** on the two slide bars **17***a* and **18***a*, thus causing key wheels **4** and **5** to be rotated by one step, and finally, if the pin **64** facing the respective guide arm is not active on any of key wheels **1** to **3**, there may be an active pin **64** on key wheel **4** to actuate guide arm **43** whereby slide bar **18***a* will be shifted to active position for rotating key

wheel 5 by one step. It will be noted that in any case key wheel 1 is advanced one step by lug 75*a* of the non-slidable bar 14*a*. In the later part of each turn, all the slide bars 15*a* through 18*a* are reset to their original position on drum 8.

It is now evident that key wheel 1 will have completed one revolution after P_1 revolutions of the drum 8, if P_1 is the number of teeth of key wheel 1. Key wheel 2 is advanced one step only if wheel 1 is in such an angular position as to cause an active pin 64 to carry guide arm 40 towards the drum 8; the number of revolutions of the drum 8 required for causing key wheels 1 and 2 to revert both to their starting position is $P_1 \cdot P_2$, if P_2 is the number of teeth on key wheel 2. The number n_1 of active pins 64 on wheel 1 must have no common denominator with P_2 and must be greater than zero and different from P_2. If $P_2=P_1$, this requires that $1 \leqq n_1 < P_1$, which is always easy to ascertain by examination of key wheel 1 and the setting of pins 64 on it, without referring to key wheel 2.

With three key wheels, the repetition cycle works out as follows: Key wheel 1 controls both key wheel 2 and key wheel 3, key wheel 2 controls key wheel 3 but simultaneous displacement of slide bar 16*a* by key wheels 1 and 2 of course only causes key wheel 3 to rotate by one step. The repetition cycle period then is $P_1 \cdot P_2 \cdot P_3$ provided the total number of steps imparted to wheel 3 in each period $P_1 \cdot P_2$ has no common denominator with P_3, which condition is automatically fulfilled if all key wheels have the same number of teeth and if this number is a prime number. For more than three wheels, similar considerations will apply.

It can be seen that the repetition cycle on one hand is equal to its mathematical maximum and that it is substantially independent of any particular setting of the active pins 64 on the several key wheels. Thereby, a very great variety of keywheel position sequences can be produced which are absolutely independent of each other but which have the same repetition cycle length. Nevertheless, the sequence of keywheel positions in itself is irregular so that analytical treatment thereof on the basis of fragments thereof which may have been detected is rendered exceedingly difficult.

Transformation of the key wheel position sequence thus obtained into actual coding and decoding is possible by various means. It has been shown in the aforementioned United States Patent No. 2,765,364 how the key wheels themselves can be used to control a ciphering teletyper. Another arrangement can consist in a mechanism controlled in response to the position of the slide bars on the drum 8, in which case a number of additional slide bars having each a random number of lugs 76 of the second kind but no lug 75 of the first kind can be provided on said drum (see British Patent No. 455,333 to Boris Caesar Wilhelm Hagelin); the key wheels also may be constructed as electric commutators as already indicated.

A further modification may consist in providing one or more additional non-slidable bars on drum 8, each having, however, one lug of the type shown at 75*a* for each one of the intermediate wheels 46 through 50, whereby instead of having each key wheel rotated by either zero or one step according to the position of the slide bars, this rotation would be by either one or two steps, or by either two or three steps, etc., as the case may be.

It will be understood that reference to the said prior patent and its mechanical arrangement has been had for convenience only and should not be considered as limitative. For instance, electro-mechanical or even purely electronic devices operating on the same basic principle would come within the ambit of this invention.

I claim:

A keying device for coding and decoding apparatus of the type comprising a series of keying members each mounted for cyclical movement step by step through a limited number of positions in each cycle of its movement, a series of sensing means each located at a fixed sensing station adjacent to one of said keying members, a plurality of control elements each mounted on one of the said keying members and movable thereby so as to be presented thereby at the sensing station which is adjacent to the respective keying member each time said keying member occupies a definite one of its said positions in the course of its cyclical movement, each of said control elements being selectively settable to an active or an inactive condition, each said sensing means being activatable by the movement of any active one of said control elements on the respective keying member to the respective sensing station, and a multiplicity of actuating means mounted for joint cyclical movement and for individual setting to an active or inactive condition under the control of the said sensing means, each of said actuating means including control means for rendering the same active in each cycle of the said joint cyclical movement in response to the presence of sensing means activated as foresaid at the sensing station adjacent to at least one of said keying members, and upon being rendered active being operative to move another of said keying members through a predetermined number of steps of the cyclical movement of the other keying member, wherein said device comprises a further means mounted for movement with said actuating means but not under the control of any of said sensing means for, on each cycle of the joint cyclical movement of said actuating means, moving at least a first of the said keying members through a first invariable number of steps differing from zero and differing from the limited number of positions through which said first keying member is movable in each cycle of its cyclical movement, and wherein the respective one of the said actuating means which is operable to move as aforesaid the *n*th of said keying members, the term *n*th denoting any particular member other than said first keying member of at least two said keying members included in a sequence constittued by said series of keying members, comprises control means as aforesaid which are responsive as aforesaid to the sensing means activatable by each keying member in a group composed of those of said keying members, including said first keying member, which extend to and include the $(n-1)$th keying member of said sequence, so that in each cycle of said joint cyclical movement the *n*th of said keying members is moved through a second invariable number of steps in response to the presence of sensing means activated as aforesaid at the sensing station adjacent to any of the keying members of said group.

References Cited in the file of this patent

UNITED STATES PATENTS

2,765,364 Hagelin ---------- Oct. 2, 1956