PATENT SPECIFICATION (11) 1303001

1303001

DRAWINGS ATTACHED

(21) Application No. 2358/71 (22) Filed 18 Jan. 1971

(31) Convention Application No. 524 (32) Filed 16 Jan. 1970 in

(33) Sweden (SW)

(44) Complete Specification published 17 Jan. 1973

(51) International Classification G09C 1/06

(52) Index at acceptance G5X 30

(54) CIPHERING APPARATUS

(71) We, A B TRANSVERTEX, a Swedish Company, of Fittja Industriomrade, Norsborg, Sweden, do hereby declare the invention for which we pray that a patent may be granted to us, and the method by which it is to be performed, to be particularly described in and by the following statement:—

A cipher of usual type has as its object the concealment of plain text which has been enciphered. The plain text is accessible only to the enciphering operator, and to the deciphering operator who has available the ciphering key valid for the cipher in question. An unauthorized person being on the possession of a cipher text and wanting to know its content, has illegally to get into his possession either the plain text corresponding to the cipher text, or the key used by the ciphering operator, or said person must by help of the cipher reconstruct this key. The reconstructruction of a cipher key, of course, is facilitated to a high degree if one has access both to the cipher and to the plain text corresponding thereto.

At password signalling, for example between two radio stations, an unauthorized listener gets access to the cipher as well as to the plain text. This constitutes an unavoidable weakness of ciphers of this kind and, therefore, the resistance to cryptanalysis of the cipher must be extremely high. In the apparatus according to the present invention, however, said weakness has been compensated for by the utilization of another fundamental property of ciphers for password signalling. A password signal need not be deciphered by the receiver.

The present invention consists in ciphering apparatus, particularly for password signalling, which includes at least two units, each comprising a setting mechanism adapted for stepwise movement, and a plurality of counters, each setting position of the setting mechanism being correlated to a counter, the units being interconnected to form an endless series by transmitting means between the counters of one unit and the setting mechanism of the following unit, said transmitting means after primary setting of the respective setting mechanisms of the units being capable of advancing the respective setting mechanism that number of steps which is determined by the counter that is correlated to the setting position prevailing at the moment of the setting mechanism of the preceding unit of the series. Hereby the apparatus is given such properties that the password signal (cipher) cannot be deciphered with the apparatus.

It is apparent that a cipher, the nature of which does not allow for deciphering even with the knowledge of the key applied renders extreme difficulties to the attempt of reconstructing the key in question.

In the cipher system of the apparatus to be described the outer key setting is determined by the text in clear, which consists of the clock stroke (the time when the password signal is ciphered) and two letters of some of the call signals of the stations communicating with each other. Since the point of time at which the password signal is produced is decisive for the appearance of the cipher, two or more password signals exchanged between the same correspondents, but at different points of time, differ from each other by their appearance. The settings of the apparatus are advanced irregularly, such that each setting directly or indirectly actuates all other settings, in such a manner, that the slightest change of a setting from an initial setting to another setting brings about a thorough change of the final position of all settings and a corresponding change of the cipher.

Example	I	II
Text in clear	AAAA	AAAB
Cipher	DGYD	KKPB

The accompanying drawings show by way of example two different embodiments of the invention. Figure 1 shows a purely mech-

anical ciphering apparatus according to the present invention.

Figure 2 shows, in a section taken on line II—II of Figure 1, how latches in the apparatus actuate a wheel provided with a stop dog, and how a wheel in the apparatus is caused to advance another wheel.

Figure 3 shows in a perspective view a wheel provided with balls for use in the apparatus of Figure 1.

Figure 4 is a section taken on line IV—IV of Figure 1, and Figure 5 shows a wiring diagram of a further embodiment of the invention operating electronically.

In the apparatus shown in Figure 1, four setting wheels 19—22 and four actuating wheels 2—5 are arranged on an axle 32. Each of the setting wheels 19—22 is adapted to be set in any one of twenty six equally spaced annular positions 40 (Figure 3), with the angle $\alpha=360°/26$ between the angular positions. A total of twenty six balls, pins or like adjustable lifting members 18 are so arranged on the setting wheels 19—22 in six rings 41 that there always is one ball in each angular position. The balls can be displaced axially within the same angular position 40 from one ring 41 to another ring in the way desired.

The balls in every ring 41 are sensed by a latch 12—17, the other end of which coacts with one of the actuating wheels, each of which includes six portions of axial distribution, and each portion comprises a stop dog or like stop members 6—11. Each ball ring on the setting wheel coacts directly or via a latch with an actuating wheel portion provided with a stop dog. The latches are pivotally mounted on an axle 34.

On each of the setting wheels 21 and 20 are arranged a number ring 24 and 25, respectively, for the time number, and a letter ring 28 and 29, respectively, with a disordered alphabet. On the setting wheel 19 are provided two letter rings, one including an ordered alphabet and one a disordered alphabet 26 and 30, respectively. The setting wheel 22 is associated with letter rings 27, 31 arranged on the right-hand end of the axle 32, which letter rings via cogwheels 36, 37, axle 24' and cogwheels 38, 39 are so connected to the setting wheel 22 that upon rotation of the letter rings 27, 31 the setting wheel 22 rotates as much as the letter rings. The letter ring 27 includes an ordered alphabet, and the letter ring 31 includes a disordered alphabet.

The initial setting is made by setting the setting wheels 19 and 22 by means of the ordered alphabets 26 and 27 to the desired station signal, and the setting wheels 21 and 20 by means of the letter ring 24 and 25 to the time number. The password comprises two two-digit groups which are read on the disordered alphabets 28—31 of the setting wheels after a pre-determined number of movements in clockwise and counter-clockwise direction of the handle 1 between angular positions determined by a stop member 42 (Fig. 4) and an arm 43 on the axle 32.

The actuating wheels 2—5 are so arranged on the axle 32 that they follow with the handle 1 upon its turning in clockwise direction, due to the friction against the axle 32 on which the handle 1 is mounted (the ball 44 is pressed by a spring 45 against the axle 32). The angle through which the wheel 5, for example, is allowed to follow with the axle, is determined by the stop dogs 6—11 and a group of latches 12—17. The three remaining actuating wheels 2—4 include corresponding stop dogs and groups of latches of their own. In each group of latches only one latch is actuated by a ball, in such a way, that the other end of the latch enters the action range of its stop dog.

The setting wheels 19—22 are so arranged on the axle 32 that they stand still when the handle 1 is being turned. One of the stop dogs on each of the four actuating wheels stops against four of the twentyfour latches. Each actuating wheel is associated with a feedhook 23 operating against a feed disc 33 which is divided into twentysix portions (Fig. 2) and rigidly connected with a setting wheel. Upon rotation of an actuating wheel by the axle 32 in clockwise direction, the feed hook 23 follows along and fetches an equal number of steps on the feed disc 33 of the associated setting wheel. In this way the wheeels work in pairs, so that, for example, the feed hook of the actuating wheel 5 coacts with the feed disc of the setting wheel 21. Other such wheel pairs are 4,20—3,19—and 2,22 respectively.

In the next step of the operation the handle 1 is turned in the counterclockwise direction. Thereby, due to the friction against the axle, the actuating wheel follows along, and the feed hook 23 takes along the setting wheel as many steps as the stop dogs at the preceding operation step were allowed to move before they were stopped by the latches.

Owing to the advancing movement of the setting wheels, four new balls actuate four of the twentyfour latches advanced in their action range or that of the stop dogs.

At the subsequent turning in clockwise direction, these latches are sensed, and the feed hooks 23 fetch as many steps on the setting wheels as the stop dogs have to turn until they meet the latches.

During the next operation step, the handle 1 is turned in the counterclockwise direction, and the setting wheels are advanced to a new position. Consequently four new balls 18 actuate the latches.

The apparatus, thus, is based on the principle that the feeding parts of the

apparatus all the time influence the conditions (setting of the setting wheel) which are prejudical for the feeding during the next following operation step. For imparting to all wheels the same irregular feeding, the wheels have been coupled together to a ring through the transmitting axle 24'. The actuating wheel 2, thus, advances the setting wheel 22. A sufficient number of turns of the handle 1 brings about the effect that the initial settings made by the setting wheels for every password exchange actuate the feed of all setting wheels.

Although on Fig. 1 the setting and actuating wheels have been shown being arranged on a common axle 32, an embodiment (not shown on the drawings) has also proved to be practical where the wheels are arranged on parallel axles uniformly distributed along a circle, and on each axle are mounted the actuating wheel of one unit and the setting wheel of a subsequent unit, the axle of the handle being disposed in the centre of the circle. The setting wheels as well as the actuating wheels, their relative movements and the driving of the entire apparatus, of course, may be subjected to electronic control, i.e. they may be replaced by electronic elements and couplings.

An embodiment of the apparatus operating electronically is shown in Fig. 5. In this apparatus every wheel set 2, 19—3, 20—4, 21 and 5, 22, respectively, is replaced by electronic units 51, 61, 71 and 81, respectively, of identical relative construction. Each of the units comprises a shifting register 52, 62, 72 and 82, respectively, each of which in a suitable way is assembled of a series of twenty six bistable rockers. To each shifting register is associated a lamp row 53, 63, 73 and 83, respectively. The primary setting of time and station signal is effected by means of switches 54, 64, 74 and 84, respectively. The shifting registers having one step poled are advanced stepwise by closing the respective switch 54, 64, 74 and 84. In the lamp rows controlled by the respective shifting register only one lamp is lighted, due to the pole shifting register, and by operating the respective switch the lighted position can be moved. To the left side of the lamp row 53 there are time indications, and to the right side there is the unordered alphabet. At the primary setting of the unit 51 the lighted position is stepped ahead to the desired hour number (which is 04 in the example shown in Fig. 5, i.e. the lamp is lighted at 04) by the switch 54. In the same way the primary setting is made with the remaining shifting registers 62, 72 and 82. The lamp row 63 indicates minutes, and the lamp rows 73 and 83 together indicate the two-digit group for the station signal. Subsequent to completed primary setting, this setting is to be written in cipher, which is carried out by closing a switch 91 common to all units a predetermined number of times, which at the apparatus according to Fig. 1 corresponds to the turning of the handle 1 a definite number of times. At each closing of the switch 91, the shifting registers 52, 62, 72 and 82 are advanced according to the example in Fig. 5 as many steps as indicated by the counters 106, 110, 113 and 120 selected by the poled shifting registers. During the advancing of the shifting registers no new counters must be selected and, therefore, all counters are blocked upon the closing of switch 91. When, however, the switch 91 is opened again, it is possible for the poled shifting registers to select again four counters, in analogy with the first turning of the handle, which counters at the next closing of the switch 91 effect the advancing of the shifting registers 52, 62, 72 and 82. The function of the counters 101—124 is corresponded at the apparatus according to Fig. 1 by the function of the stop dogs 6—11.

Subsequent to pressing the switch 91 a predetermined number of times, the four lighted positions in the lamp rows 53, 63, 73 and 83 respectively, have been moved a number of steps, and the letters in the unordered alphabets which can be read adjacent the lighted positions, represent the password.

WHAT WE CLAIM IS:—

1. Ciphering apparatus, particularly for password signalling, which includes at least two units, each comprising a setting mechanism adapted for stepwise movement, and a plurality of counters, each setting position of the setting mechanism being correlated to a counter, the units being interconnected to form an endless series by transmitting means between the counters of one unit and the setting mechanism of the following unit, said transmitting means after primary setting of the respective setting mechanisms of the units being capable of advancing the respective setting mechanism that number of steps which is determined by the counter that is correlated to the setting position prevailing at the moment of the setting mechanism of the preceding unit of the series.

2. Apparatus according to claim 1, wherein for each unit the setting mechanism is a setting wheel provided with balls, pins or like adjustable lifting members and adapted to be advanced by steps in the rotation direction, and the counters include stop dogs or like stop members at a rotatable actuating wheel, wherein each setting step of the setting wheel directly or *via* latches is correlated to a stop member in the unit, and wherein the transmitting means comprise carrier members between the actuating wheel in one unit and the setting wheel in a subsequent unit, the members comprised in the apparatus being connected so to each other and to a handle

rotatable in both directions, that upon rotation in one direction all setting wheels stand still and all actuating wheels are turned through an angle determined by the stop members, and that upon rotation in the opposite direction the setting wheels are turned by the carrier members through the same angle as the actuating wheels were turned in the preceding operational step.

3. Apparatus according to Claim 1 or 2, having four setting mechanisms and setting wheels, wherein two of the setting mechanisms and setting wheels are correlated to a number series with time numbers and a letter series with an unordered alphabet, and the two remaining setting mechanisms and setting wheels are each correlated to a letter series with an ordered alphabet and a letter series with an unordered alphabet.

4. Apparatus according to Claim 2 or 3, wherein all wheels are arranged on a common axle and the handle is in a positive drive connection with the axle and wherein the actuating wheels by friction are taken along by the axle to their angles of rotation determined by the lifting members of the setting wheels.

5. Apparatus according to Claim 2 or 3, wherein the wheels are arranged on parallel axles uniformly distributed along a circle, and on each axle are mounted the actuating wheel of one unit and the setting wheel of a subsequent unit, the axle of the handle being disposed in the centre of the circle.

6. Apparatus according to any one of Claims 2 to 5, wherein the carrier members comprise a feed disc disposed on the setting wheels and a feed hook disposed on the actuating wheels, which hook upon rotation of the handle in the first direction follows the actuating wheel and on the feed disc of the setting wheel standing still advances a number of steps corresponding to the rotation of the actuating wheel, and thereafter upon rotation of the handle in the opposite direction advances the setting wheel a number of steps corresponding to the rotation of the actuating wheel in the preceding operational step.

7. Apparatus as claimed in Claim 1, wherein each setting mechanism is an electronic shifting register.

8. Ciphering apparatus substantially as described with reference to any of the accompanying drawings.

MARKS & CLERK
Chartered Patent Agents,
57 & 58 Lincoln's Inn Fields,
London, WC2A 3LS.
Agents for the Applicant(s).

Printed for Her Majesty's Stationery Office, by the Courier Press, Leamington Spa, 1973.
Published by The Patent Office, 25 Southampton Buildings, London, WC2A 1AY, from which copies may be obtained.

1,303,001
2 SHEETS

COMPLETE SPECIFICATION

This drawing is a reproduction of the Original on a reduced scale.

SHEET 1

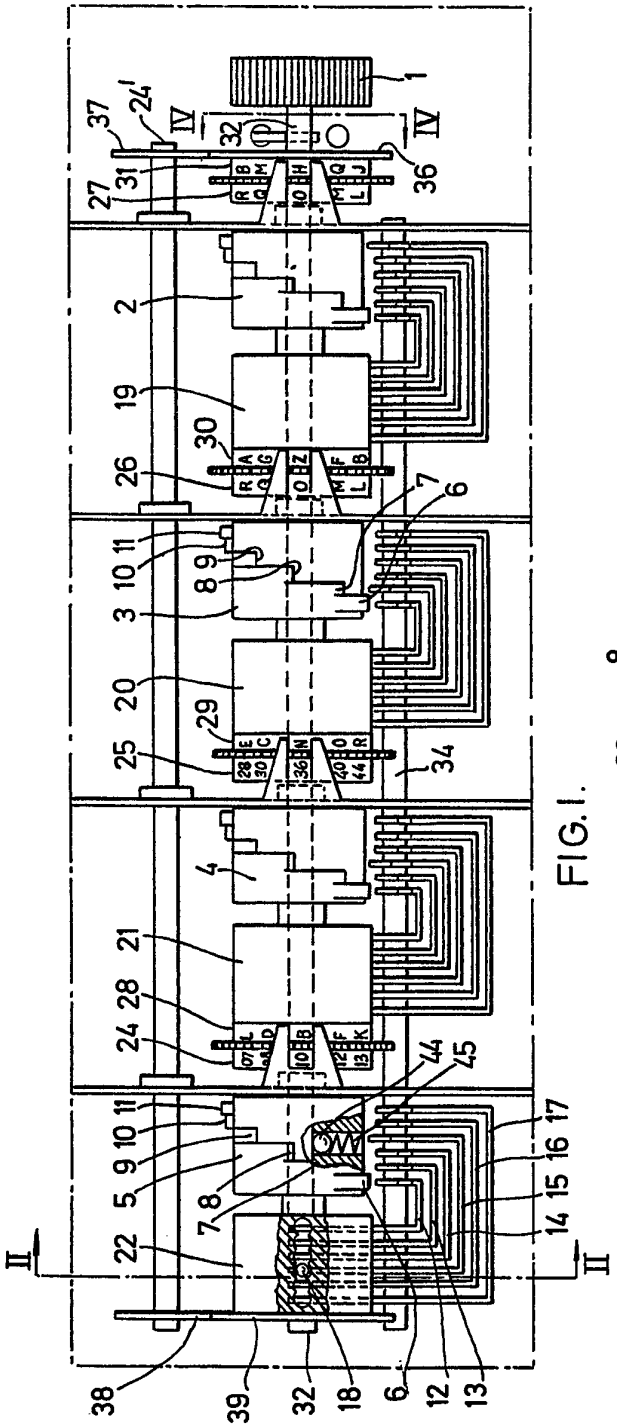

FIG. 1.

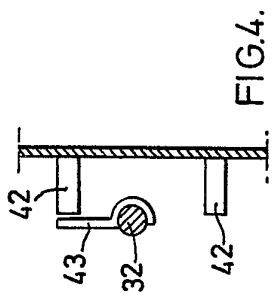

FIG. 4.

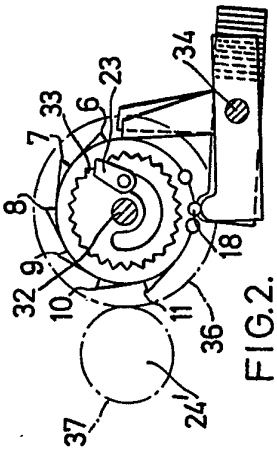

FIG. 2.

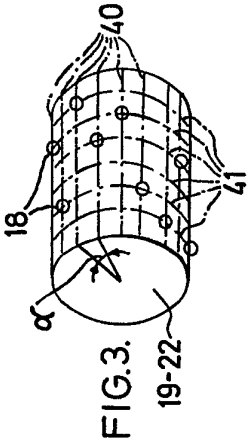

FIG. 3.

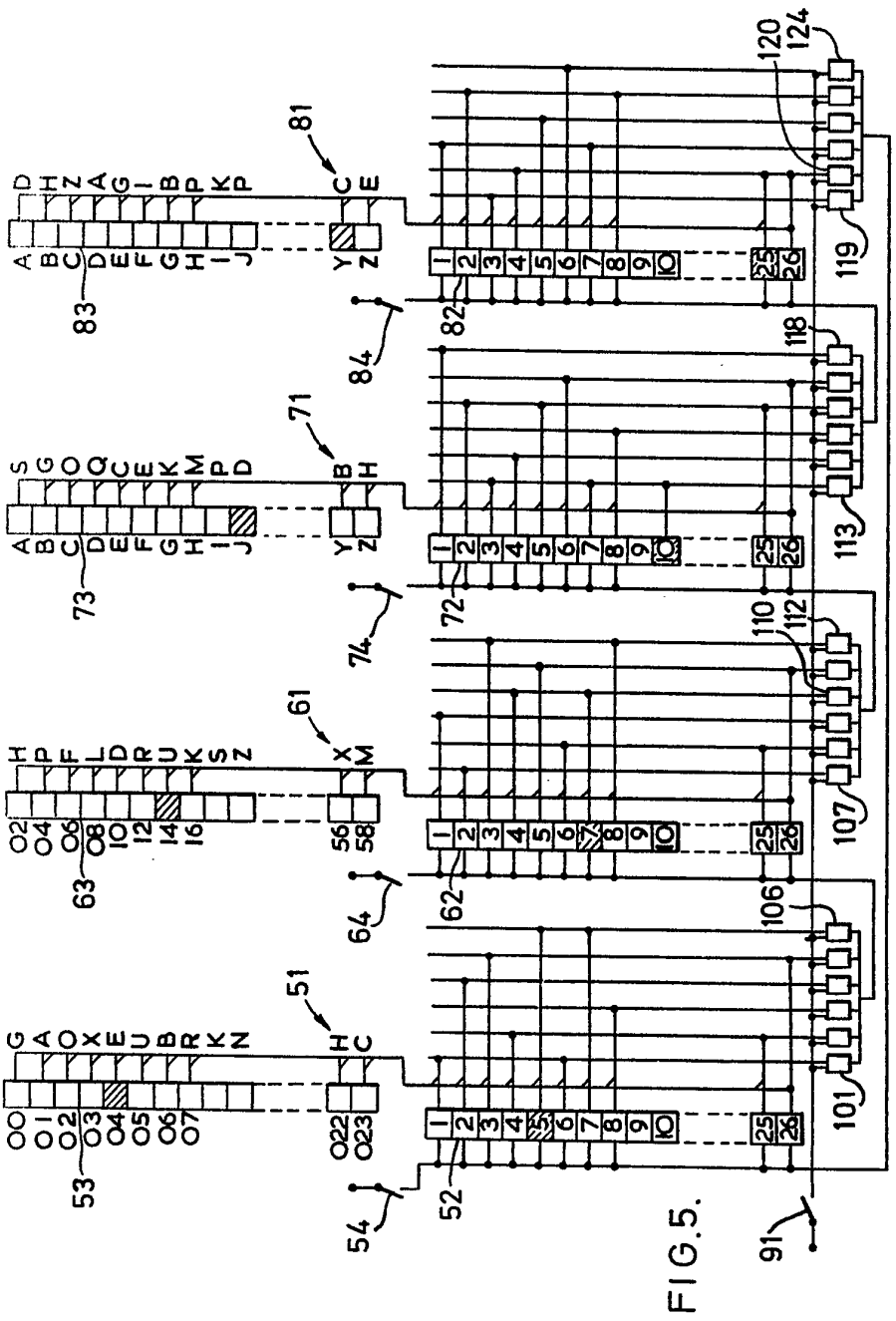

FIG.5.