PATENT SPECIFICATION

DRAWINGS ATTACHED

Inventors: PER-ERIK AHLMAN and VIGO WALDEMAR **LINDSTEIN**

1,010,223

1,010,223

Date of Application and filing Complete Specification Aug. 14, 1962.

No. 31203/62.

Complete Specification Published Nov. 17, 1965.

Index at acceptance:—G5 X30

Int. Cl.:—G 09 c

COMPLETE SPECIFICATION

Improvements in and relating to Cryptographic Machines

We, AB TRANSVERTEX, a Swedish Body Corporate, of 15 Sigfridsvagen, Hagersten, 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:—

The purpose of the present invention is to rationalize and simplify the production of cryptograms, which usually are produced more or less manually and with a great number of previously arranged tables and series of keys. The disadvantage of this and similar cryptographic systems is, among others, that the series of keys cannot be produced "on the spot" at the same time as the ciphering operation.

These disadvantages are eliminated by the present invention without diminishing in practice the security against solving the cipher produced. The machine according to the invention comprises a plurality of pin wheels settable relatively to each other and having pins each settable to one active and one passive position the said wheels, at the ciphering or deciphering operation respectively being arranged to be rotated, while connected together, one or more steps simultaneously, characterized in that at each stepping operation of the pin wheels the active pins are sensed by arms corresponding in number to that of the pin wheels, the said arms cooperating with indicators which, in dependence upon the setting of the pins, occupy one or the other two positions only, thereby providing two rows of indications, one corresponding to the active pins and the other to the passive pins, and further characterized in that the machine is provided with a carrier for a plurality of disordered alphabets, and a member having an ordered alphabet, said carrier and said member being movable in relation to each other for selection of one of said disordered alphabets in dependence on the indication given by said indicators.

As the ciphering ultimately is based upon an arbitrary choice from a number of disordered alphabets, which may be varied from one day to another, the series of keys for two different days may be considered as not related to one another.

An embodiment of the invention will be described in detail by way of example with reference to the accompanying drawings.

In the drawings:

Figure 1 shows the machine as seen from above with the casing partially cut away.

Figure 2 shows a vertical section of the machine.

Figure 3 shows the machine as seen from behind and with the casing removed.

Figure 4 shows a lateral view of the machine with the casing partially cut away for the purpose of showing a detail of the feeding device.

Figure 5 shows an enlarged view of an alphabet holder.

Figure 6 shows an alphabet ribbon.

A base plate 1 has two end plates 3 and 4 fixed thereto. Between these end plates there is mounted a shaft 2, upon which five pin wheels 5, 6, 7, 8 and 9, with 19, 21, 23, 25 and 26 equidistant pins 15 respectively, are rotatably mounted. Each of these five pin wheels is disconnectably connected (by means of a catch or the like for shifting relatively to each other before the beginning of the ciphering or deciphering) with five gear wheels 10, 11, 12, 13 and 14, one for each pin wheel and having 19, 21, 23, 25 and 26 teeth respectively, *i.e.* one tooth for every pin carried by the corresponding pin wheel. The pins 15 are axially displaceable and the pin wheels have about their circumference

[*Price* 4*s.* 6*d.*]

recesses 16 provided with characters (letters or the like) for each initial setting and corresponding to the respective pins. These pins 15 will, in dependence upon their axial setting, actuate (active pins) or not actuate (passive pins) arms 17 for movement in a counter-clockwise direction, as seen in Figure 2. These arms have at their upper end a plate 18, which is provided with a digit. The plate associated with the pin wheel 5 is provided with the digit 1, the plate associated with the pin wheel 6 is provided with the digit 2 and so on. These digits may be read in an upper row 20 or a lower row 21 of windows in a casing 19. The arms 17 are rotatably mounted on a shaft 22 and are actuated by springs 48, in a clockwise direction. Each of the five gear wheels 10—14 engages one of gear wheels 23—27, fixed on the shaft 22 and all of which have the same number of teeth so that at each rotation of the shaft 22 through an angle corresponding to one tooth division all pin wheels 5—9 also rotate one division, because these gear wheels are coupled to the pin wheels during operation. At one end of the shaft 22 (Figure 1) a ratchet wheel 27^1 is fixedly attached, which has the same tooth pitch as the gear wheels 23—27. Close to this ratchet wheel a handle 28 is rotatably mounted, which handle is provided with a ratchet 29 pivotally mounted on an axle journal 31 and actuated by a spring 30 into engagement with the ratchet wheel 27^1. Each time the handle 28 is pressed down, the shaft 22 is rotated through an angle corresponding to a tooth division. (Limiting stop members for the movement of the handle 28 and the shaft 22, as well as the returning spring, are not shown). It is apparent that the same relative position of the pin wheels will not be reached until $19 \times 21 \times 23 \times 25 \times 26$ movements have taken place. Thus this number of digit arrangements is obtained before their sequence is repeated. On an extension of the base plate, beyond the device as described for the driving of the pin wheels, which is covered by the casing 19, there are provided holders 32, into which loose ribbons or the like 33 may be inserted, which ribbons have reciprocal cipher (*i.e.* disordered) alphabets printed thereon. Each holder is marked with a digit character 34 (Figure 1). Finaly a rod 35, fixed by means of brackets 36 and 37, carries a displaceable slide 38 provided with a window 39 and an ordered alphabet and an ear 41 for setting the slide.

The machine is operated in the following manner (for ciphering as well as for deciphering): The initial setting of the pin wheels as agreed between the dispatcher and the receiver is set manually. The lowest one of the two digit combinations appearing in either of the two rows of windows 20 and 21 is read (for instance the number "13" in Figure 1, composed of the digits "1" and "3"), and the slide 38 is set in such a way that its window 39 frames that ribbon 33, whose holder is marked with the number 13. The letter to be ciphered (or deciphered) is sought in the alphabet 40, and the corresponding letter is read on the ribbon. Thereafter the handle 28 is pressed down, whereby the pin wheels are rotated one division and the plates 18 are set in new positions: the lowest number is read and the slide 38 is set at the corresponding holder.

The ciphering and deciphering may be performed according to two almost similar principles:

1. The machine is for instance provided, as shown in Figure 1, with sixteen reciprocal discarded cipher alphabets, which suitably are placed by lot in the holders 32 for each day. The holders 32 are marked: 0, 1, 2, 3, 4, 5, 12, 13, 14, 15, 23, 24, 25, 34, 35 and 45.

2. The machine may also be provided with an extended base plate and twenty six holders 32 for twenty six reciprocal disordered alphabets. The holders 32 are then marked: 0, 1, 2, 3, 4, 5, 12, 13, 14, 15, 23, 24, 25, 34, 35, 45, 123, 124, 125, 134, 135, 145, 234, 235, 245 and 345. To begin with, the numbers in the row 20 of windows are read as long as it contains at most three digits. As soon as this row 20 of windows contains a number having more than three digits, one reads instead the numbers in the row 21 of windows, until this row contains a number of more than three digits, whereafter one again reads the row 20 and so on.

As ciphering and deciphering are performed in exactly the same manner, the great advantage of seeking the letters of the plain text or the cipher letters respectively in an ordered alphabet is immediately realized.

Modifications of details of the machine described above are possible without departing from the scope of the invention as defined in the appended claims. Thus instead of displacing the window 39 past the holders 32, the window may have a fixed position and the holders mounted on a rotatable drum, and the machine may be arranged for automatically turning the drum in order to set the desired alphabet, corresponding to the lowest number appearing in the windows 20, 21, in the window 39, as said before.

WHAT WE CLAIM IS:—

1. A cryptographic machine with a plurality of pin wheels settable relatively to reach other and having pins each settable to one active and one passive position the said wheels, at the ciphering or deciphering operation respectively being arranged to be rotated, while connected together, one or more steps simultaneously, characterized in that at each stepping operation of the pin wheels the active pins are sensed by arms corresponding in number to that of the pin wheels, the said

arms cooperating with indicators which, in dependence upon the setting of the pins, occupy one or the other of two positions only, thereby providing two rows of indications, one corresponding to the active pins and the other to the passive pins, and further characterized in that the machine is provided with a carrier for a plurality of disordered alphabets, and a member having an ordered alphabet, said carrier and said member being movable in relation to each other for selection of one of said disordered alphabets in dependence on the indication given by said indicators.

2. A cryptographic machine according to claim 1, wherein markings are provided on said disordered alphabets, said markings each corresponding to a certain indication given by each one or other of the row of indications.

3. A cryptographic machine according to claim 1 or claim 2, characterized in that the machine is provided with a housing having two rows of openings therein, in one of which indicators of active pin position are visible and the other of which indicators corresponding with inactive pin positions are visible.

4. A cryptographic machine with n pin wheels representing the digits 1 . . n and settable relatively to each other and having pins settable each to one active and one passive position, the said wheels, at the ciphering or deciphering operation respectively, being arranged to be rotated, while connected together, one or more steps simultaneously, characterized in that at each stepping operation of the pin wheels the active pins are sensed by arms corresponding in number to that of the pin wheels, the said arms cooperating with indicators which, in dependence upon the setting of the pins, occupy one or other of two positions only, thereby providing two rows of indications, one correspond to the active pins and the other to the passive pins, and further characterized in that the machine is provided with a carrier bearing $\frac{(2)^n}{2}$ disordered alphabets, and a member having an ordered alphabet, said carrier and said member being movable in relation to each other for selection of a disordered alphabet corresponding to a number composed of said digits and presented in one of said rows.

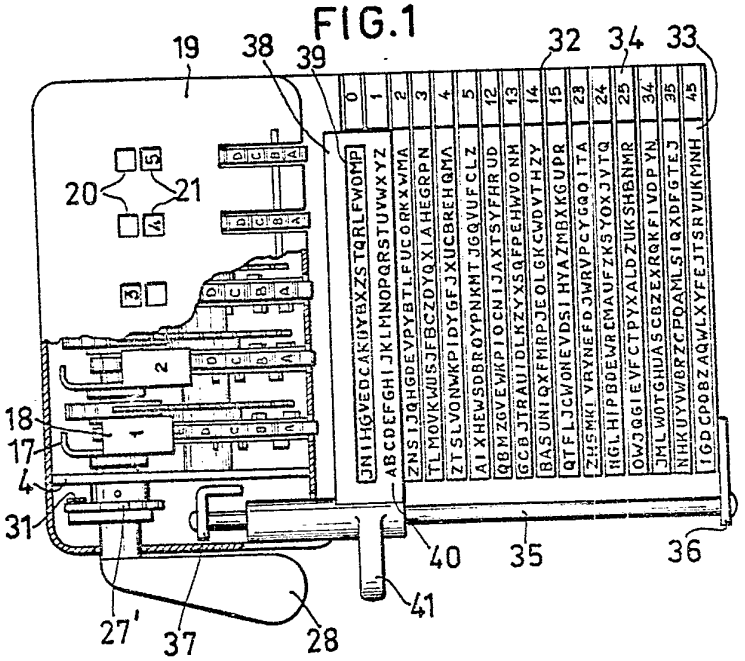
5. A cryptographic machine according to claim 4, characterized in that the disordered alphabet selected corresponds to the smaller of the two numbers composed of said digits.

6. A cryptographic machine substantially as hereinbefore described with reference to and as illustrated in the accompanying drawings.

AB TRANSVERTEX
Per: Boult, Wade & Tennant,
112, Hatton Garden, London E.C.1.
Chartered Patent Agents.

Leamington Spa: Printed for Her Majesty's Stationery Office by the Courier Press.—1965.
Published at The Patent Office, 25, Southampton Buildings, London, W.C.2, from which copies may be obtained.

FIG.1



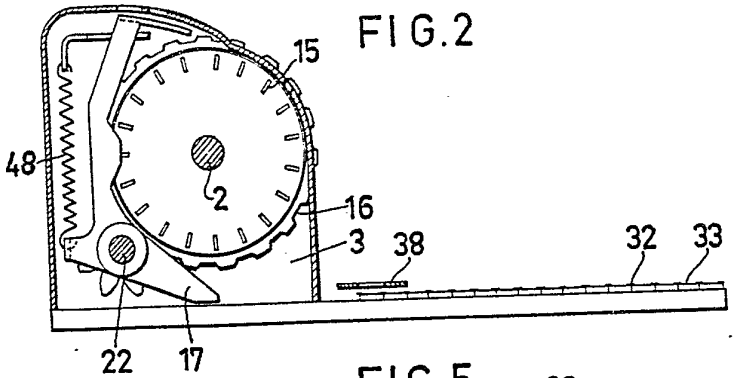
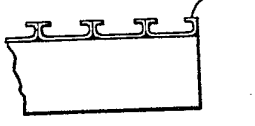


FIG.2

FIG.5



1010223 COMPLETE SPECIFICATION
2 SHEETS *This drawing is a reproduction of the Original on a reduced scale*
Sheets 1 & 2

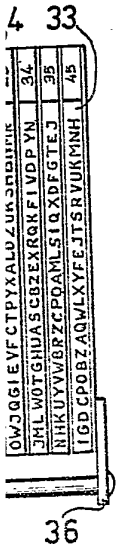


FIG.3

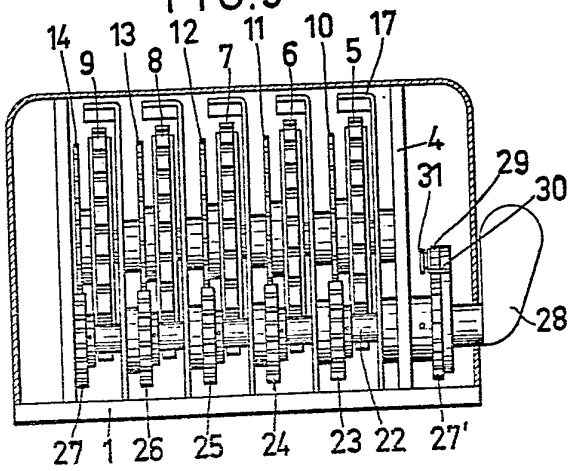
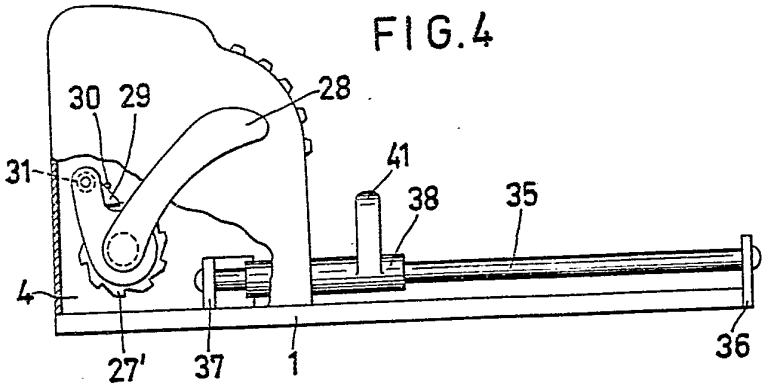


FIG.4



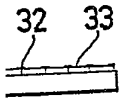
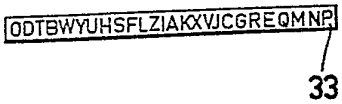


FIG.6



1010223 COMPLETE SPECIFICATION
2 SHEETS *This drawing is a reproduction of the Original on a reduced scale*
Sheets 1 & 2

FIG.1

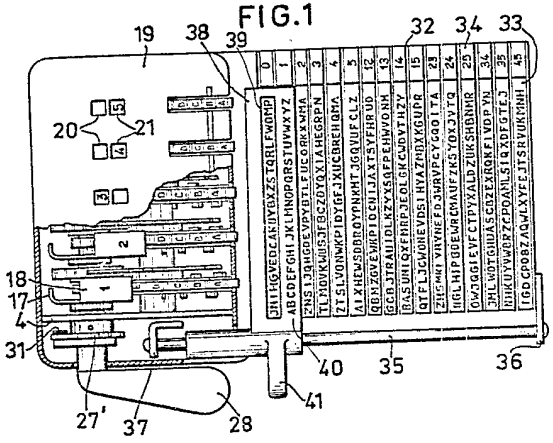


FIG.2

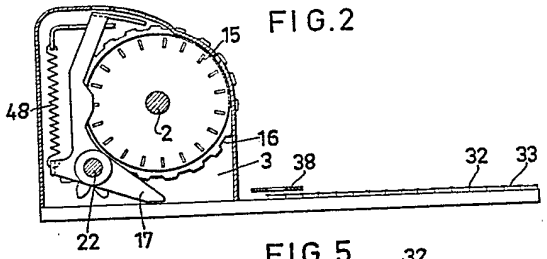


FIG.5

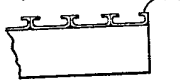


FIG.3

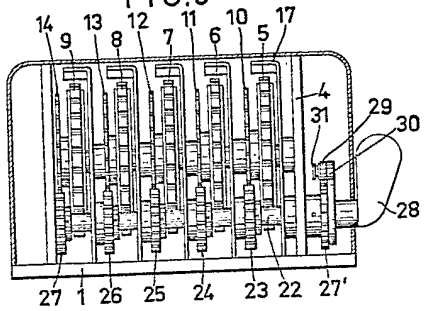


FIG.4

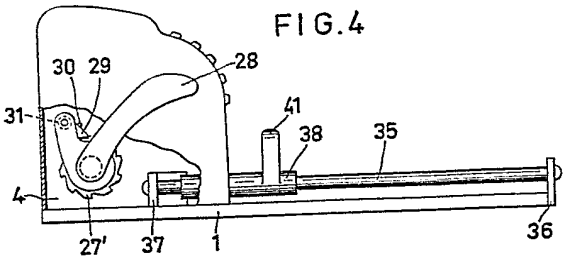


FIG.6