April 29, 1958 B. C. W. HAGELIN 2,832,826

CIPHERING MEANS

Filed Oct. 16, 1953 2 Sheets-Sheet 1

FIG. 4.

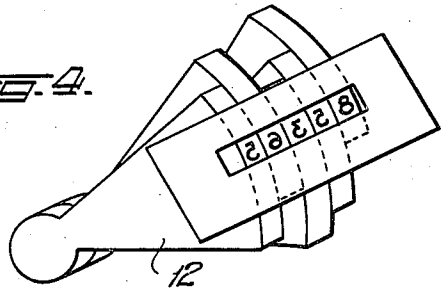


FIG. 1.

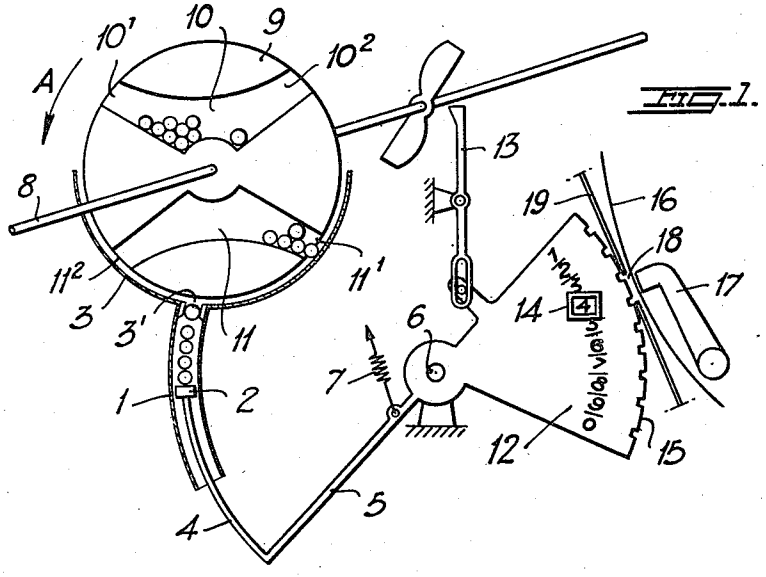


FIG. 2.

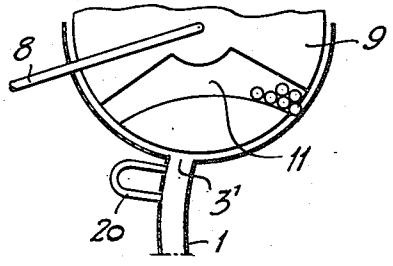
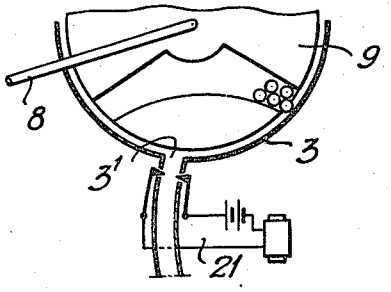


FIG. 3.



INVENTOR:
B. C. W. HAGELIN
BY: Morse & Hall
ATTORNEYS.

April 29, 1958 B. C. W. HAGELIN 2,832,826

CIPHERING MEANS

Filed Oct. 16, 1953 2 Sheets-Sheet 2

FIG. 5.

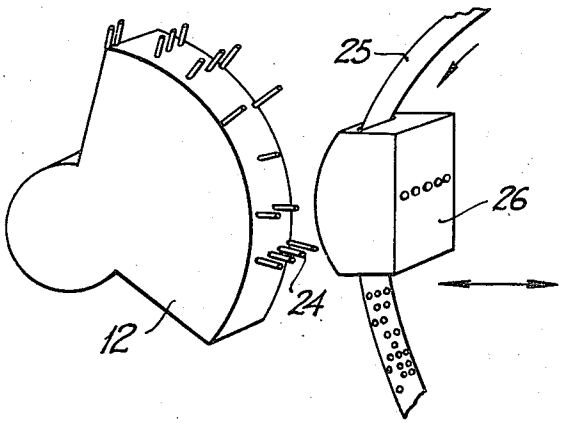


FIG. 6.

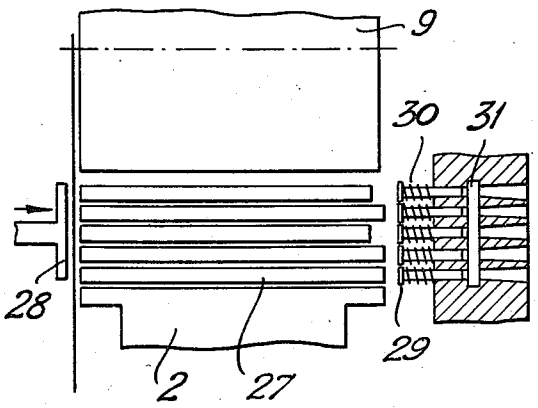
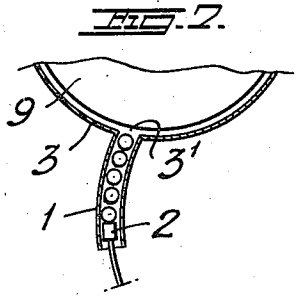


FIG. 7.



INVENTOR:
B. C. W. HAGELIN
By: Morse & Hall
ATTORNEYS.

United States Patent Office

2,832,826

Patented Apr. 29, 1958

2,832,826

CIPHERING MEANS

Boris Caesar Wilhelm Hagelin, Zug, Switzerland

Application October 16, 1953, Serial No. 386,570

6 Claims. (Cl. 178—22)

Ciphering devices which produce an irregular displacement are known in various forms. Most of such devices are so constructed that they produce a given series of transpositions which can be reconstructed by another correspondingly set similar device. This is necessary in order that the receiver of the communication can reconstruct the series of transpositions forming the basis of the cipher in order that he may decipher the code message.

Fundamentally these devices produce a conveniently long succession of characters determined mathematically in advance and it is sufficient for the partners to know how the devices act and what is their starting position.

The known devices referred to, due to their construction, suffer from the common drawback that the text ciphered thereby in many cases can be deciphered in a relatively short time by modern electronic calculating machines. This fact is easily understood because all such devices effect a mathematical development which can be partly reconstructed by an expert acquainted with the elements thereof. They are thus in a wide sense not ciphering instruments but only confusing devices. A completely safe ciphering can only be produced when the transposition of the separate characters or their replacement by others is effected in an entirely arbitrary manner. An example of such an arbitrary fixing of a series of transpositions of characters is given by a playing dice.

As the series of transpositions thus fixed is not positively predetermined it cannot be reconstructed by knowing the starting position. Cipher tables are therefore used which are written or printed on the basis of an arbitrary transposition of numerals or letters and these tables are available to the partners. A great disadvantage, however, in this connection, is that the partners must possess the complete tables.

The present invention is concerned with a device which affords the possibility of making cipher text tables or stamping perforated cipher strips relatively rapidly, mere accident forming the basis of the transposition.

Several embodiments of the invention are illustrated in the accompanying drawing, in which,

Figure 1 is a substantially diagrammatic view of an example of the invention, a rotary drum and associated outlet device being shown in section. Figure 2 is a section of the lower portion of a modified drum and outlet device. Figure 3 is a similar section as that shown in Figure 2 of the rotary drum with a still modified outlet device. Figure 4 is a perspective view of a set of selecting devices belonging to a system like that shown in Figure 1. Figure 5 is a modified, selecting mechanism. Figure 6 is an elevation, partly in section, of a still modified selecting mechanism. Figure 7 is a section at right angles to Figure 6 of the plunger system thereof.

In the embodiment shown in Fig. 1, the reference numeral **1** indicates an arcuate tube which serves as a cylinder for a reciprocable piston and for this reason in the following description is referred to as a cylinder. At the upper end of the cylinder **1** is mounted a hopper

3 which forms a part of a cylindrical wall having a horizontal axis. The opening in the hopper leading to the cylinder is indicated by **3'**. The piston **2** is rigidly connected through the medium of an arcuate rod **4** with an arm **5** which can turn about an axis **6** which is coincident with the centre of curvature of the cylinder **1**. A spring **7** attached to the arm **5** serves to press the piston **2** in the cylinder **1** towards the opening **3'**.

Above the hopper **3** a smooth drum **9** rotates about the axis **8** in the direction of the arrow. The lower part of the drum is concentrically embraced by the hopper **3**. The drum **9** contains a number of sector-like chambers of which two, indicated by **10** and **11**, are shown. These chambers each have two openings 10^1, 10^2 and 11^1, 11^2 at the periphery of the drum. Each chamber contains a number of balls, usually ten, which can pass to and fro through the openings in the chamber. During the rotation of the drum the openings 10^1, 10^2 and 11^1, 11^2 in succession communicate with the hopper 3^1 so that the balls from the chamber can pass into the cylinder **1** above the piston **2**.

Each time such a communication is established the piston **2** is held in its lowest position by an operating lever **13** which is moved over a cam disc **12** rigidly connected with the arm **5**.

It will be observed that the hopper opening 3^1 as well as the balls are so dimensioned that most balls in a chamber can flow freely out of the chamber through the opening 3^1, while one or more of the balls in the chamber are so large that they cannot pass through the opening 3^1. Thus, balls will continue to pass through the chamber into the cylinder **1** until a ball of larger dimensions reaches the opening 3^1 and closes it. The drum **9** which preferably rotates stepwise, but which can be moved continuously, turns further after a short interval of time. At the same moment the piston **2** is released and, under the action of the spring **7**, moves upwards again until it is stopped thereby, so that the balls in the cylinder can no longer be moved upwards as occurs when the uppermost ball remains pressed against the wall of the drum **9**. The final position of the piston is thus determined by the number of balls above the piston in the cylinder **1**.

Through an opening **14** provided in the side of the sector-shaped cam disc **12** a numeral corresponding to this position of the piston can be read off on a series of numerals on the sector **12** or the corresponding figure of a row of type **15** on the periphery of the sector can be printed on a paper strip **16** by means of the hammer **17**, since the hammer through an opening **18** in a plate **19** covering the periphery of the sector strikes the type exactly opposite this opening.

During the continued rotation of the drum **9** as soon as the rear opening in the chamber, i.e. the opening 11^2 of chamber **11** in the position shown, comes directly above the opening 3^1 of the hopper, due to the action of the spring **7** the piston system is moved in a clockwise direction so that all the balls in the cylinder **1** above the piston are again returned to the chamber, whereupon the instrument is again in starting position.

When the succeeding opening in the chamber, the opening 10^1 of chamber **10** in the example illustrated, comes directly over the hopper opening 3^1 the same process as above described is repeated. It is clear that by the rotation of the drum **9** the balls will become mixed so that it is a matter of pure chance whether more or fewer balls pass into the cylinder **1**.

In Fig. 2 a modification of the above described construction is illustrated in which the hopper opening 3^1 and the balls are not calibrated. Instead of calibrating them a magnet **20** is arranged at the upper end of the

cylinder **1** to attract a ball of magnetic material when it passes into the cylinder. Most of the balls will be of non-magnetic material while only a few of the balls will be magnetic. In other respects this arrangement operates in the manner already described, a magnetic ball at 3^1 preventing further inlet of balls into the cylinder.

In a third construction according to Figure 3 there is provided adjacent the hopper 3^1 a contact device, the balls being of insulating material and particular balls of conducting material. As soon as one of these conducting balls enters 3^1 printing of the number is effected by an electrical system. It is assumed that in the position of rest the piston **2** is located at the upper end and is displaced by the weight of the balls entering the cylinder. A control system will at the conclusion of a period move the piston upwards again in order to force the balls back into the rotating body. In this case it is not necessary that the entry of further balls after the specific ball should be prevented. If care is taken to ensure that the printing of the number is effected very rapidly, the entry of further balls and the rotation of the sector **12** caused thereby may have no effect on the position of the sector in printing.

Generally the action of the device depends on the fact that a number of balls are located in the chamber and that at least one special ball is present thereunder which is unavoidably identifiable in passing the point 3^1 and thereby influencing the device in a given manner. It is necessary that the distinguishing characteristics of the special and the neutral balls are such that they can be distinguished clearly for the release of the device or for the printing, but the characteristic of the specific ball or balls should have no influence on the mixing of the balls during the rotation of the drum so as to obtain as high a probability of chance as possible.

According to Figure 4 different complete selecting devices are arranged adjacent one another which operate independently of one another and only are driven in common.

As shown in Figure 5, the sector **12** can be provided with pins **24** which stamp out a system of perforations in a strip **25** passing through a block **26** moved against the sector **12**. A variant based on the same idea serves for the exclusive production of five-hole strips and is explained in conjunction with Figure 6.

In this embodiment the falling bodies consist of cylindrical rods of individual lengths. The rotating drum **9** is disposed longitudinally and the rods lie axially therein. The piston **2** in the lowest position permits only a total of five rods to fall in. The few special rods are of greater length and there are at least five of them. In the measuring cylinder **1** which is open at the side, after the dropping of the rods five of them are always present, 0 to a maximum of five being "normal" and the remainder "special," i. e. longer rods.

A plunger **28** pushes the rods which have dropped in to the right in the drawing against five stamps **29** which are held in position to the left by springs **30**. A paper strip is pushed forward step by step in the slot **31**. When the plunger **28** moves to the right the stamps **29** in front of the long rods perforate the strips but not those in front of the normal rods. The plunger thereupon returns and the piston **2** pushes the rods back into the rotating drum.

If in lieu of numerals, letters of the alphabet were used in preparing the tables, more balls would be required, a total, say, of 25 or 26 per chamber.

In all the embodiments illustrated means may be provided in order to set the drum in vibration or vibrate it positively for the purpose of ensuring greater mixture of the balls or other falling bodies.

I claim:

1. An apparatus of the class specified comprising in combination, a movable container, a set of bodies loosely placed therein some of which are different from the other, "normal," ones, the container having an outlet opening at least for said bodies, a measuring device having a measuring chamber for receiving bodies dropping from the container in given positions thereof, means in connection with said chamber for interrupting the entry of bodies therein upon arrival of a "different" body to the measuring chamber, a movable member in said chamber, means for automatically setting said member in a position determined by the number of "normal" bodies received by the measuring chamber before the arrival of said "different" body, and means under the control of said movable member for marking said number.

2. An apparatus of the class specified comprising in combination, a drum mounted to rotate about a horizontal axis, said drum having separate chambers and openings in its periphery leading to said chambers, a plurality of bodies loosely placed in each of said chambers, some of the bodies in each chamber being different from the other, "normal," ones, a stationary hopper concentrically surrounding the lower portion of the rotatable drum, a cylinder in communication with said hopper for receiving bodies dropping from the container into the hopper in given positions of the drum, feeler means in connection with the cylinder for allowing only "normal" bodies to enter the cylinder while cutting off the entry of further bodies to the cylinder upon the arrival of a "different" body to said feeler means, a piston mounted on said cylinder so as to form a movable bottom thereof, means for setting said piston to a position depending on the number of "normal" bodies as collected in the cylinder before the arrival of the "different" body to the feeler means, and means for registering said number under the control of the setting of the piston.

3. An apparatus as claimed in claim 2, in which the bodies contained in the chambers of the rotatable drum comprise calibrated balls, the inlet opening of the cylinder in communication with the hopper being correspondingly calibrated.

4. An apparatus as claimed in claim 2, in which said "different" bodies are of a magnetic material, while the "normal" bodies are of a non-magnetic material, the feeler means comprising a magnet provided adjacent the inlet of the cylinder for preventing the entry to the cylinder of said magnetic bodies.

5. An apparatus as claimed in claim 2, in which the bodies contained in the chambers of the drum comprise rods of various lengths extending in the axial direction of the drum, the feeler means being adapted to act on certain of these rods while leaving the remaining rods unaffected.

6. An apparatus as claimed in claim 2, in which means are provided for vibrating the drum in order to improve the mixing of the bodies.

References Cited in the file of this patent

UNITED STATES PATENTS

2,406,031	Parker	Aug. 20, 1946
2,412,301	Spencer	Dec. 10, 1946