N° 23,204 A.D. 1913

(Under International Convention)

Date claimed for Patent under Patents and Designs Act, 1907, being date of first Foreign Application (in France), 23rd Oct, 1912

Date of Application (in the United Kingdom), 14th Oct, 1913

At the expiration of twelve months from the date of the first Foreign Application, the provision of Section 91 (3) (a) of the Patents and Designs Act, 1907, as to inspection of Specification, became operative

Accepted, 9th Apr, 1914

COMPLETE SPECIFICATION

Improvements in Devices for Cypheiing and Decypheiing Messages and the like

I, GLORGES LUCIGNE, of 19, rue de la Duse, Marseille, Bouches-du-Rhone, in the Republic of France, Civil Engineer, do hereby declare the nature of this invention and in what manner the same is to be performed to be particularly described and ascertained in and by the following statement —

This invention has for its subject a portible apparatus, capible of being easily carried in the pocket, and adapted to convert any message written in clear language into a cryptographic message and *vice versa* The use of the apparatus about to be described assures the absolute secrecy of correspondence exchanged by letters or by telegrams (ordinary telegrams or radio-telegrams)

It is already known to use cryptographic apparatus having 10 sliders each with the letters of the alphabet in normal order on one part, and in irregular order on the other part, and to arrange these sliders side by side in grooves on a board, the lower parts of the sliders being moved to bring the desired letters of a word into line under a slot, whereby the upper parts are caused to show different letters in line under another slot The upper parts of the sliders have been provided with numerals, the arrangement of which forms the key to the transposition The device according to the present invention differs from this, in that a greatly increased interchangeability is secured by dividing each slider into two parts, an upper and a lower part arranging the letters of the alphabet in various orders on the lower parts as well as the upper parts of the sliders, and making all of the lower sliders interchangeable as well as all of the upper sliders With this construction it is rendered absolutely impossible by mere guess work to decypher any code message as will be seen from the following description

The accompanying drawing shows by way of example, a form of construction of the apparatus

Figure 1 is a face view, the sliders being in the position which they occupy when the apparatus is not in use

Figure 2 shows the apparatus with the sliders arranged for a particular cryptographic transposition.

[*Price* 8*d.*]

Figure 3 is an end view of the apparatus

As will be seen in the drawings, the apparatus essentially consists of a base board in which are cut guide grooves of suitable form, in the drawing (Figure 3) these grooves are of a dove-tailed section, but obviously they may be of any other convenient section Sliders 2 are provided adapted to fit and move in these guides The number of grooves (and consequently the number of sliders) can naturally be varied, in the example illustrated ten grooves are provided adapted to receive ten upper movable sliders and ten lower movable sliders This number has been chosen because for telegraphy the assemblage of ten letters having no apparent sense but capable of being pronounced, is counted as a single word

These sliders, independent each from the others, are strictly identical in their dimensions so as to be perfectly interchangeable, they can be inserted indifferently each into the place of any of the others, and in any order, into the grooves of the board in which they can slide with slight friction

The sliders of each set are numbered from zero to nine On each slider are written one above another, but in a different order for each slider, all the letters of the alphabet

It will be seen that when all the sliders are in place, the numbers written on the ends thereof form, when read from left to right, a number of ten digits characteristic of the arrangement of the sliders relatively to one another For convenience of description the name 'MATRICULA' is given to these numbers For each arrangement or order of the sliders of the upper set there corresponds an upper matricula (for example the number 6978152430, for the position in Figure 2) and in the same manner that for each arrangement of the lower sliders there corresponds a lower matricula (1407963825 in Figure 2)

The sliders of each of the upper and lower sets can be placed relatively to one another in the board, in a very large number of different orders, in fact, the number of these arrangements obtained by varying the order of the sliders relatively to one another, is given by the known formula or permutations, whose application gives in the present case —

$$P_{10}=10\times9\times8\times7\times6\times5\times4\times3\times2\times1=3,628,800$$

There are therefore 3 628,800 different upper matriculæ and 3,628,800 lower matriculæ Moreover these matriculæ can be combined each with each, the number of combinations is then —

$$3,628,800^2=13,168,189,440,000$$

Plates 3 and 3¹ are fixed on the sides of the board so as to extend the one over the upper set of sliders, and the other across the lower set Each plate is slotted longitudinally for use as explained hereinafter, for the formation and reading of the cryptograms For the convenience of the description the name of "reader will be given to these slotted plates

The apparatus is used in the following manner —

The two correspondents agree upon two matriculæ, one the lower and the other the upper, these being kept secret, for example as indicated in Figure 2, 6978152430 may be adopted as the upper matricula and 1407963825 as the lower matricula

When one of the correspondents wishes to send to the other a secret message he arranges the sliders in the order as shown in Figure 2, so as to form the two matriculæ agreed upon, then, by moving the sliders in their guides he causes the word to be transmitted to appear in the slot of the upper reader 3, for example the word "INVIOLABLE" as on the drawing

The sliders of the lower set being in contact with those of the upper set, as in the figure, the sender reads in the slot of the lower reader 3¹, the cryptogram to be transmitted, *viz* "ISLYUCEQZI" The person receiving the message

thus cyphered, and desiring to translate it, has only to dispose the sliders of his apparatus in the same manner as the sender, that is to say so as to obtain the two matriculæ agreed upon, and then to cause to appear in the slot of the lower reader 3¹ the cyphered words given in the telegram Then he will instantly read in clear language in the slot of the upper reader 3 the words of the message of his correspondent

It will be seen that it is sufficient to change the lower matricula in order completely to modify the cryptogram Thus, in the example proposed, if, instead of the lower matricula agreed upon (1407963825), the lower sliders had been disposed to form for example the matricula 5823960174, the cryptogram of the word 'INVIOLABLE" would have become 'EWFOUCYLVU"

The inviolability of the secrecy of the correspondence thus transmitted is practically absolute Except for an indiscretion making known the matriculæ agreed upon, there is no doubt that it would be quite impossible to decypher a secret dispatch transmitted by means of this apparatus, in view of the very large number of matriculæ that it is possible to obtain by the permutations, all matriculæ other than those agreed upon between the two correspondents give unintelligible transcriptions

The cryptographic system, resulting from the application of this apparatus gives rise to insurmountable difficulties in any attempt at de-cyphering without it The same letter is often replaced, in the cryptogram, by different letters or, *vice versa*, the same letter A for example, in the cryptogram, corresponds sometimes to an E, sometimes to an I, sometimes to an U, *etc* of the clear message

Having now particularly described and ascertained the nature of my said invention and in what manner the same is to be performed, I declare that what I claim is —

1 In a device of the type described for cyphering and de-cyphering words and messages, the construction wherein the sliders are arranged in two sets, an upper and a lower set, the sliders of each set being interchangeable in position in that set, while for any particular arrangement of the one set of sliders a word set thereon to appear through a slot in the reading plate will give a cryptographic word in the reading plate of the other set, which can be de-cyphered only by someone knowing the correct order of the sliders and thus enabled to set the cryptographic word on one set thereof so as to reproduce the original word under the reading plate on the adjacent set of sliders, substantially as described

2 In a device as claimed in Claim 1, the construction wherein the sliders of each set bear numbers thereon, so that their order for cyphering and de-cyphering in any case can be determined by a given order of the numbers which can be kept secret, substantially as described

3 The apparatus for use in cyphering and de-cyphering words and messages, constructed and adapted to be used substantially as described with reference to the accompanying drawings

Dated this 14th day of October, 1913

For the Applicant:
GILL & ELLIS,
Chartered Patent Agents,
55/56, Chancery Lane, London, W C

Redhill Printed for His Majesty's Stationery Office, by Love & Malcomson, Ltd —1914.

FIG_3_

FIG_1_

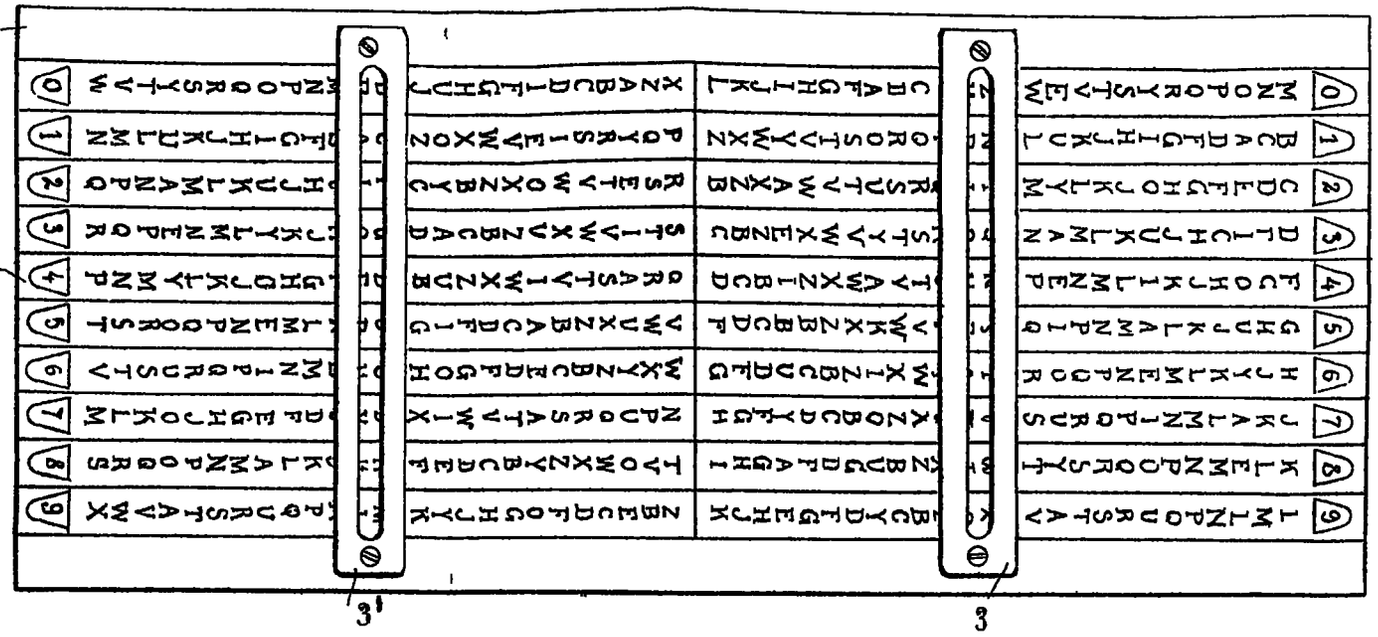
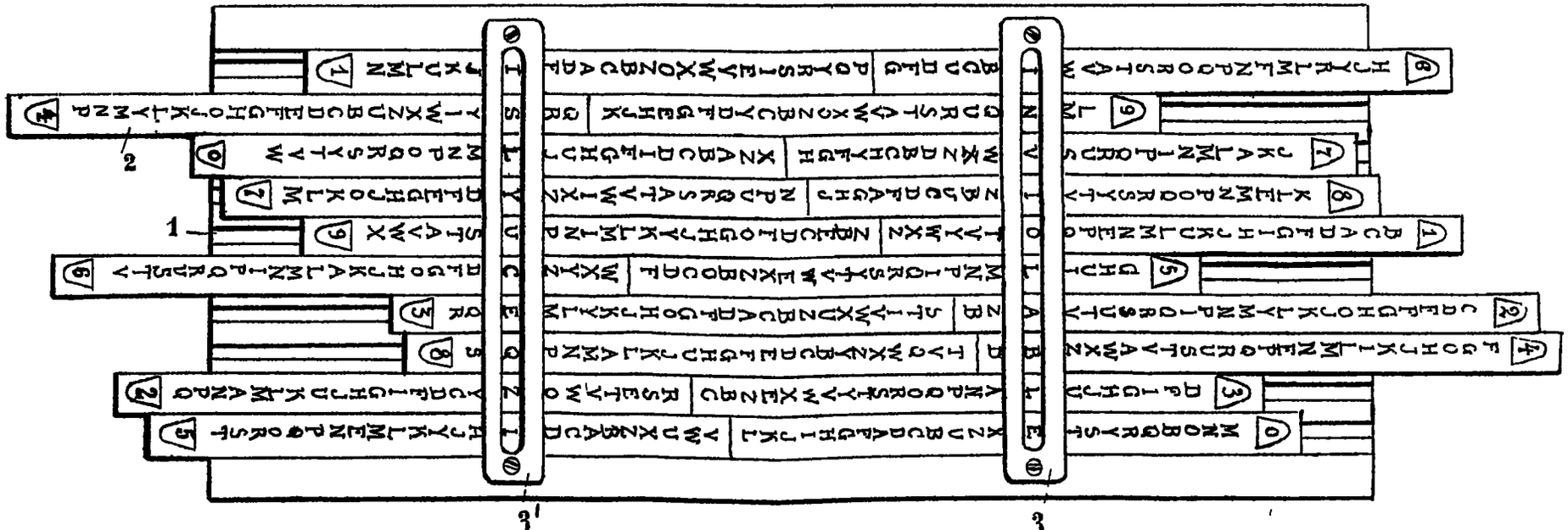


FIG_2_



British № 23,204

Fugagne