N° 12,005 A.D. 1909

Date of Application, 21st May, 1909
Complete Specification Left, 22nd Nov., 1909—Accepted, 19th May, 1910

PROVISIONAL SPECIFICATION.

Apparatus for Forming and Transforming Cipher Messages for Telegraphic and other purposes.

We, RICHARD THOMAS NICHOLSON, of "The Mount", Loughton, in the County of Essex, Manager, and HARRY WILLIAM HIGHAM, of Glen Lyn, Sanderstead, in the County of Surrey, Assistant Manager, do hereby declare the nature of this invention to be as follows:—

This invention relates to the construction of cipher messages for telegraphic and other purposes by the sender and the deciphering of them by the receiver, and has for its object the provision of means whereby such can be carried out in a simple manner, the said means being compact in form and easy and of low cost to manufacture; further whereby a readily variable private and secret system can be carried out in coding and de-coding messages and also the coding can be consolidated and the cost reduced. It is customary in code books to use words up to 10 letters and each code-word has a corresponding number usually of 5 figures. We will take such conditions in describing our invention by way of example but it must be understood that it is not restricted to such conditions.

To carry our invention into effect, we arrange a series of slides, cylinders, bands, wheels, or other equivalent devices, adapted to be held by and adjusted in position in a suitable frame, in which two sets of windows, or apertures, or indicators, are provided. These slides, or other equivalent devices, are in pairs, one of the members of a pair carrying the vowels which ultimately enter into the composition of the code word to be telegraphed, and the other bearing the consonants which ultimately enter into the word to be telegraphed.

It is clear that by the combination of the consonants in the alphabet with the vowels in the alphabet, a sufficient number of pronounceable, bi-literal combinations, consisting of one consonant and one vowel, can be produced, to represent any two-figure combination, or to represent a combination consisting of even more than two figures.

Excluding the "Q" as a consonant and counting the "Y" as a vowel, there are nineteen consonants and six vowels available, so that the permutation of these nineteen consonants, singly, with these six vowels, singly, enables one hundred and fourteen pronounceable bi-literal syllables to be produced, when the consonants stands in the first place and the vowel in the second. Further, it is obvious that by transposing the vowel and the consonant, a further range of pronounceable combinations is produceable.

We place upon the aforesaid slides, cylinders, wheels, or bands, the characters of the alphabet, and we also place the digits either upon such slides, *etc.*, or upon some slide, *etc.*, working in conjunction therewith, in such a way that when a digit is made to appear at the digit window, opening or indicator, a letter will appear at the letter aperture, window or indicator. When the consonant slide, or other equivalent, has been actuated in this way, by setting up the first figure, the vowel slide is similarly actuated by setting up the second figure; or *vice versâ*.

[*Price 8d.*]

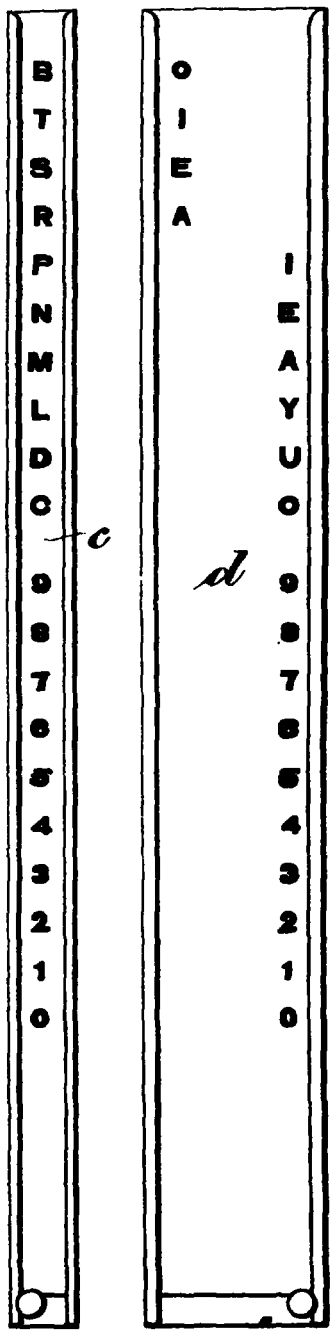

Fig: 3.

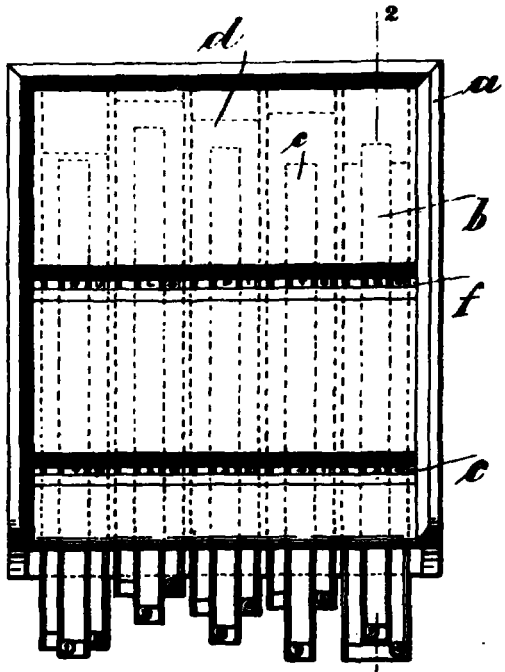

Fig: 1.

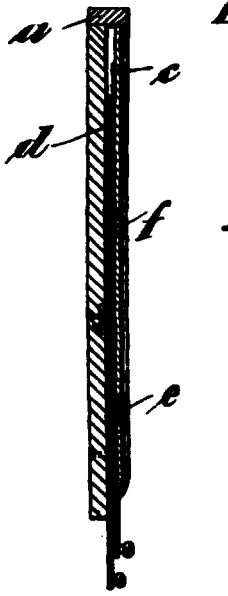

Fig: 2.

Fig: 4.

Malby & Sons, Photo-Litho.

The foregoing represents a general statement of the method in which a pronounceable syllable is made to represent any two successive digits whatsoever. We now proceed to describe more particularly a special application of the general principle of construction which has been described in the foregoing.

In the following description, reference is made only to slides, but any equivalent device may be adopted. Each of the compound slides consists of two parts, one part having ten different consonants arranged one under the other, and then the ten digits in a similar way below them, in such a fashion that when one of these digits appears at one of the windows, apertures or indicators, as the slide is moved, a corresponding consonant appears at the other window, aperture or indicator. The other part of the compound slide has a certain number of vowels, say 6—towards its right-hand edge, and toward the left-hand edge, say 4 vowels, the six on the one side and the four on the other making up the ten required to represent the ten digits. These vowels are arranged one under the other, but the column is broken where it changes from one side to the other of the said part. Beneath this column on this part, ten digits are arranged as a column, in such a way that when one of the digits appears at its window, aperture or indicator, the corresponding vowel appears at its window, aperture or indicator. The part having the ten consonants and ten digits all in one column, is disposed on the other part so that its column is disposed between the two broken parts of the column of the other part.

In this way, when any two digits are brought in succession to the digit window, aperture or indicator, there appears at the letter window, aperture or indicator, two letters, one of which is a vowel and the other a consonant, so that a pronounceable, bi-literal syllable is thus formed, the consonant representing the first digit of any required pair of digits, and the vowel representing the second digit of such pair. At the letter window, aperture or indicator, the vowel will, however, appear to the left or right of the consonant, according as the vowel is derived from the right-hand series of vowels or the left-hand series of vowels on the vowel slide described in the foregoing. If now five compound slides are arranged in the frame in series, a pronounceable word of ten letters, or five bi-literal syllables can be constructed, and a numerical equivalent of, say, ten digits. It is obvious that the number of digits, however, can be extended beyond these, inasmuch as by increasing the number of the consonants on the consonant slide, a consonant can be used to indicate a number higher than the number of any single digit. Similarly, it is obvious that by extending the vowel series, a number higher than that represented by any single digit can be represented. For the purpose of this description, however, it is sufficient to assume that no combination of numbers consisting of more than ten digits (that is to say, two numbers of five digits each) is required to be represented.

The method of using our invention is as follows:—

A code word is looked up in the code-book, representing a certain sentence or message, and its numerical reference of, say, five figures, is set up or reproduced on the apparatus, by moving the compound slides in succession, until the actual number appears at the figure window, aperture or indicator. A second message or word is then looked up, and its numerical reference in turn set up on the remaining slides, at the figure windows, and these two messages together will give a number of ten digits, at the figure windows, and ten letters, forming five pronounceable syllables, and one pronounceable and telegraphable word of ten letters, at the letter windows. In this way, not only can two messages be transmitted in one word, but it can be done without anyone being able to understand or decipher it, unless such person has knowledge of the arrangement of the slides and of the letters and figures thereon. On receipt of such [illegible] be decoded by the converse process to that already described.

We would have it understood that we are not limited in any way as to the [illegible] of compound slides, or as to the number of letters or digits used on the slides, but we find that the number given in the example gives a sufficient range of permutations to comply with ordinary commercial purposes.

In order that a record may be kept of the actual word constructed, by the device, the letters on the slides, cylinders, bands, wheels or other equivalent device may be formed as printing type and the device can be mounted together with inking means and operative mechanism in such a way that an impression of the word can be made on any suitable medium or equivalently the said slides, cylinders, bands or wheels can be geared to separate printing mechanism to produce the same result.

Dated this 21st day of May, 1909.

FELL & JAMES,
1, Queen Victoria Street, London, E.C.,
Agents for the Applicants.

COMPLETE SPECIFICATION.

Apparatus for Forming and Transforming Cipher Messages for Telegraphic and other purposes.

We, RICHARD THOMAS NICHOLSON, of "The Mount", Loughton, in the County of Essex, Manager, and HARRY WILLIAM HIGHAM, of Glen Lyn, Sanderstead, in the County of Surrey, Assistant Manager, 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 relates to the construction of cipher messages for telegraphic and other purposes by the sender and the deciphering of them by the receiver and has for its object the provision of improved means whereby such can be carried out in a simple manner, the said means being compact in form and easy and of low cost to manufacture; further whereby a readily variable private and secret system can be carried out in coding and de-coding messages and also the coding can be consolidated and the cost of telegraphing be thus reduced. It is customary in code books to use words up to ten letters and each code word has a corresponding number usually of five figures. We will take such conditions in describing our invention by way of example but it must be understood that it is not restricted to such conditions.

To carry our invention into effect, we arrange a series of slides, cylinders, bands, wheels, or other equivalent devices, adapted to be held by and adjusted in position in a suitable frame, in which two sets of windows, apertures, or indicators, are provided. These slides, or other equivalent devices, are in pairs, one of the members of a pair carrying the vowels which ultimately enter into the composition of the code word to be telegraphed, and the other bearing the consonants which ultimately enter into the word to be telegraphed.

It is clear that by the combination of the consonants in the alphabet with the vowels in the alphabet, a sufficient number of pronounceable, bi-literal combinations, consisting of one consonant and one vowel, can be produced, to represent any two-figure combination, or to represent a combination consisting of even more than two figures.

Excluding the "Q" as a consonant and counting the "Y" as a vowel, there are nineteen consonants and six vowels available, so that the permutation of these nineteen consonants, singly, with these six vowels, singly, enables one hundred and fourteen pronounceable bi-literal syllables to be produced, when the consonant stands in the first place and the vowel in the second. Further, it is obvious that by transposing the vowel and the consonant, a further range of pronounceable combinations is produceable.

We place upon the aforesaid slides, cylinders, wheels, or bands, the characters of the alphabet, and also digits in such a way that when a digit is made to appear at the digit window, aperture or indicator, a letter will appear at the letter window, aperture or indicator. When the consonant slide, or other equivalent, has been actuated in this way, by setting up the first figure, the vowel slide is then similarly actuated by setting up the second figure: or *vice versâ*.

The foregoing represents a general statement of the method in which a pronounceable syllable is made to represent any two successive digits whatsoever. We now proceed to describe more particularly a special application of the general principle of construction which has been described in the foregoing; and in order that the invention may be the better understood, we will describe it in relation to the accompanying drawing, reference being had to the letters and figures marked thereon.

Figure 1 is a front view of the device of flat form constructed in accordance with our invention.

Figure 2 is a sectional view of the same on the line 2—2 of Figure 1.

Figure 3 shows full size the two parts of the compound slide separated from each other.

Figure 4 is a transverse section of the vowel portion of the compound slide.

In the following description, reference is made only to slides, but any equivalent device may be adopted.

Upon a suitable frame *a* a series of compound slides *b* are arranged side by side with one another so that they can each be slid up or down within the frame *a* parallel to one another for the purpose of adjusting their position in said frame.

Each of the compound slides *b* consists of two parts *c* and *d*, one part *c* having ten or more different consonants arranged one under the other, and then an equivalent number of digits or numerals in a similar way below them, in such a fashion that when one of these digits or numerals appears at one of the windows, apertures or indicators *e* formed in the frame *a*, as the part *c* is moved a corresponding consonant appears at the other window, aperture or indicator *f* formed higher up in the frame. The other part *d* of the compound slide *b* has a certain number of vowels, say 6 towards its right-hand edge, and towards the left-hand edge, say 4 vowels, the six on the one side and the four on the other making up the ten required to represent the ten digits. These vowels are arranged one under the other, but the column is broken where it changes from one side to the other of the said part. Beneath this column on this part *d*, ten digits are arranged as a column, in such a way that when one of the digits appears at its window, aperture or indicator *e*, the corresponding vowel appears at its window, aperture or indicator *f*. The part *c* having the ten consonants and ten digits all in one column, is superposed on the other part *d* so that the column of the part *c* is disposed between the two broken parts of the column on the other part *d*.

In this way, when any two digits of a combined slide are brought in succession to the digit window, aperture or indicator *e*, there appear at the letter window, aperture or indicator *f*, two letters, one of which is a vowel and the other a consonant, so that a pronounceable, bi-literal syllable is thus formed, the consonant representing the first digit of any required pair of digits, and the vowel representing the second digit of such pair. At the letter window, aperture or indicator *f* the vowel will, however, appear to the left or right of the consonant, according as the vowel is derived from the right-hand series of vowels or the left-hand series of vowels on the vowel slide *d*. If now five compound slides *b* are arranged in the frame in series as illustrated in the drawing, a pronounceable word of ten letters, or five bi-literal syllables can be constructed say RU, LO, PI, TE, BU, and a numerical equivalent of say ten digits 7320324134. It is obvious that the number of digits, however, can be

extended beyond these, inasmuch as by increasing the number of the consonants on the consonant slide, a consonant can be used to indicate a number higher than the number of any single digit. Similarly it is obvious that by extending the vowel series, a number higher than that represented by any single digit can be represented. For the purpose of this description, however, it is sufficient to assume that no combination of numbers consisting of more than ten digits, (that is to say, two numbers of five digits each) is required to be represented. In order to prevent the slides from moving too loosely in the frame springs are arranged at the back of each slide and adapted to exert pressure between the slide and the frame.

The method of using our invention is as follows:—

A code word is looked up in the code-book, representing a certain sentence or message, and its numerical reference of, say, five figures, is set up or reproduced on the apparatus by moving the compound slides in succession, until the actual number say 73203 appears at the figure window, aperture or indicator *e*. A second message or word is then looked up, and its numerical reference say 24134 in turn set up on the remaining slides, at the figure window *e*, and these two messages together will give a number of ten digits 7320324134, at the figure window *e*, and ten letters, forming five pronounceable syllables, and one pronounceable and telegraphable word of ten letters say "rulopitebu," at the letter window *f*. In this way, not only can two messages be transmitted in one word, but it can be done without anyone being able to understand or decipher it, unless such person has knowledge of the arrangement of the compound slides *b* and of the letters and figures thereon. On receipt of such word, it can be decoded by the converse process to that already described.

We would have it understood that we are not limited in any way as to the number of compound slides *b*, or as to the number of letters or digits used on the slides, but we find that the number given in the example gives a sufficient range of permutations to comply with ordinary commercial purposes.

We are aware that it has been proposed in check cipher systems, cryptographic instruments and the like to use a series of cylinders, wheels or bands relatively movable to one another and adapted to be adjusted in relation to two registering positions or marks, each cylinder, wheel or band carrying a series of syllables in columnar form and a corresponding series of numbers in columnar form so that each syllable has a corresponding number when the syllable and number are opposite the registering positions respectively, and we do not claim such devices broadly

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

1. Apparatus for forming and transforming cipher messages for telegraphic and other purposes consisting of a series of compound relatively movable elements adapted to be adjusted in relation to two registering positions or marks, each element consisting of two parts, one part carrying a series of consonants and a series of numbers in columnar form, and the other part carrying a series of vowels and a series of numbers in columnar form, the vowel column being broken; the two parts of the element being adapted to move relatively to one another and to have the consonant column disposed between the two parts of the vowel column, substantially as described.

2. Apparatus for forming and transforming cipher messages for telegraphic and other purposes consisting of a frame having two registering means transversely disposed at predetermined positions relative to one another, a series of compound elements adapted to move relatively to one another in said frame in a direction substantially normal to said registering means, each compound element having one part carrying a column of consonants and figures and another part having a column of vowels and figures, the vowel column being

British # 12,005

Nicholson + Higham

broken so that one part is one side of and the other part is the other side of the consonant column, substantially as described.

3. The arrangement and construction of an apparatus for forming and transforming cipher messages for telegraphic and other purposes, substantially as described and illustrated in the accompanying drawing.

Dated this 22nd day of November, 1909.

FELL & JAMES,
1, Queen Victoria Street, London, E.C.,
Agents for the Applicants.

Redhill: Printed for His Majesty's Stationery Office, by Love & Malcomson, Ltd.—1910.

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 Cyphering and Decyphering Messages and the like.

I, GEORGES LUGAGNE, of 19, rue de la Darse, Marseille, Bouches-du-Rhône, 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 portable apparatus, capable 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:—

$$P_{10} = 10 \times 9 \times 8 \times 7 \times 6 \times 5 \times 4 \times 3 \times 2 \times 1 = 3,628,800.$$

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 3^1 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 3^1, 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 3^1 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.

REF ID:A71811

FIG_3_

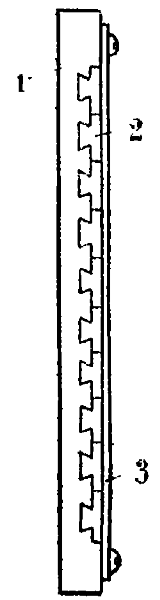

FIG_1_

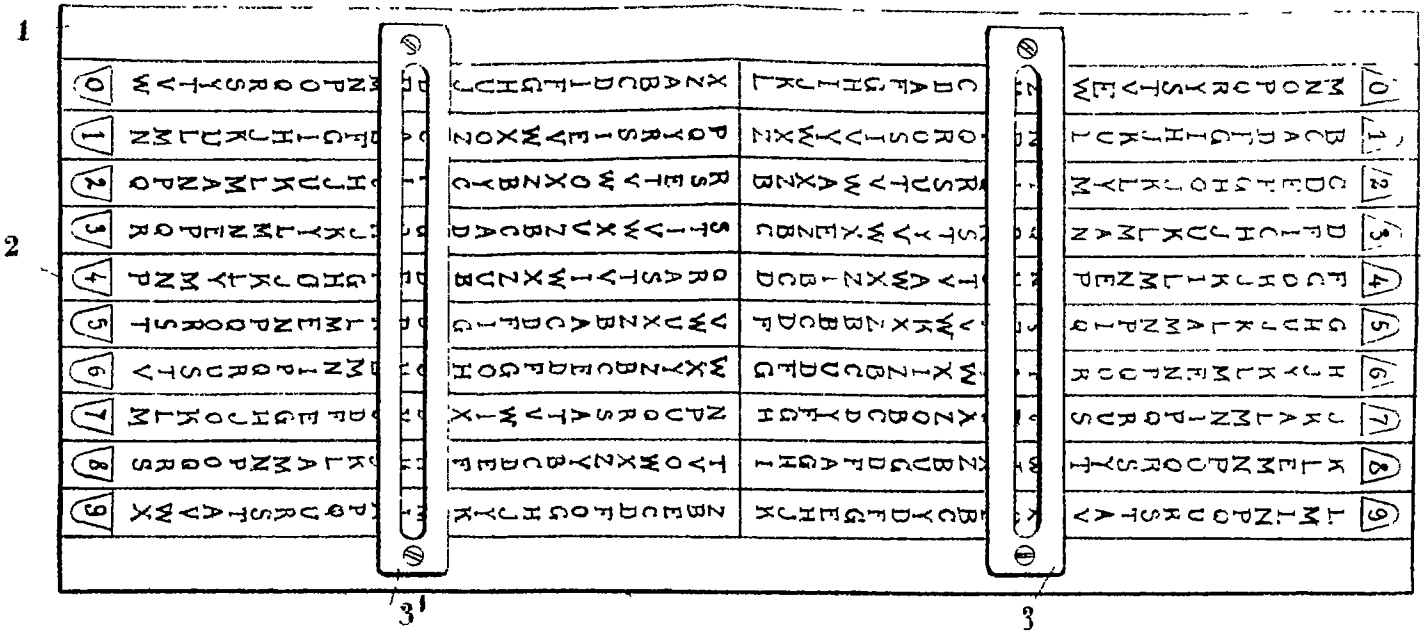

FIG_2_