Feb. 19, 1924. 1,484,477

A. G. DAMM

APPARATUS FOR CIPHERING AND DECIPHERING CODE EXPRESSIONS

Filed March 25, 1922 3 Sheets-Sheet 1

Fig. 1.

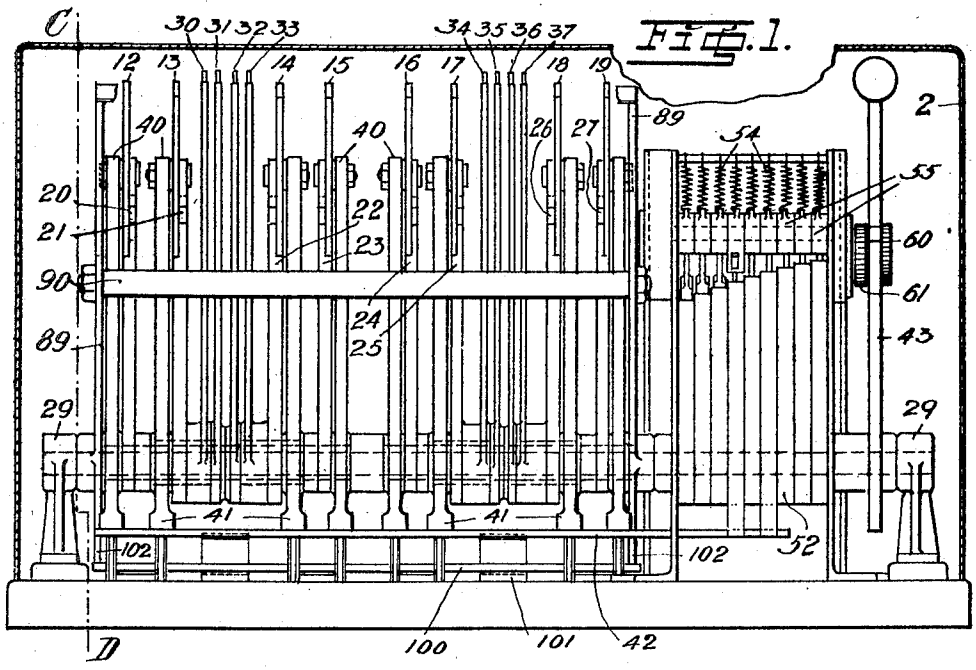
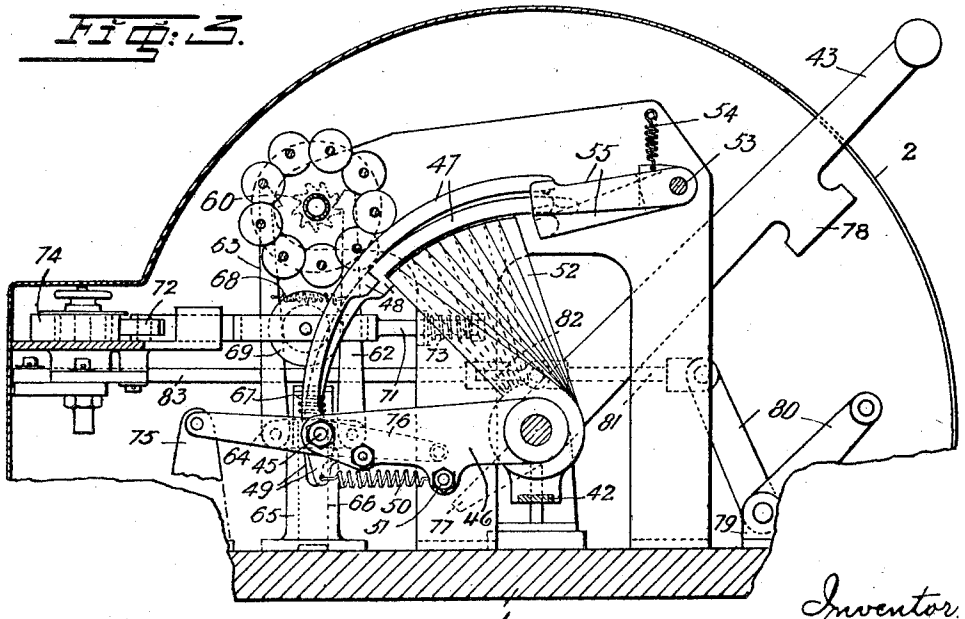


Fig. 2.



Inventor.
Arvid G. Damm,
By Kenny & Kenny
Attys.

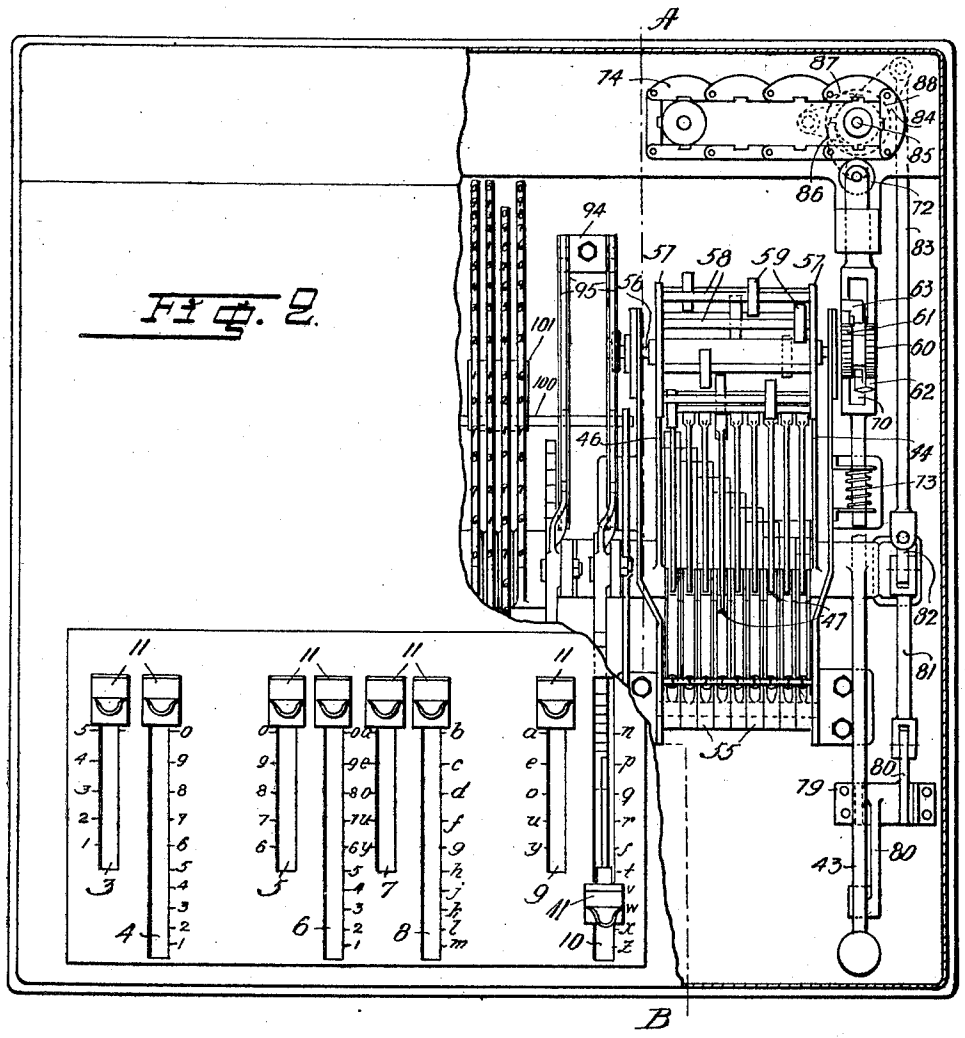
Feb. 19, 1924. 1,484,477

A. G. DAMM

APPARATUS FOR CIPHERING AND DECIPHERING CODE EXPRESSIONS

Filed March 25, 1922 3 Sheets-Sheet 2

FIG. 2.



Inventor
David G. Damm,
By Henry Orth & Co
Atty.

Feb. 19, 1924. 1,484,477

A. G. DAMM

APPARATUS FOR CIPHERING AND DECIPHERING CODE EXPRESSIONS

Filed March 25, 1922 3 Sheets-Sheet 3

Fig. 4.

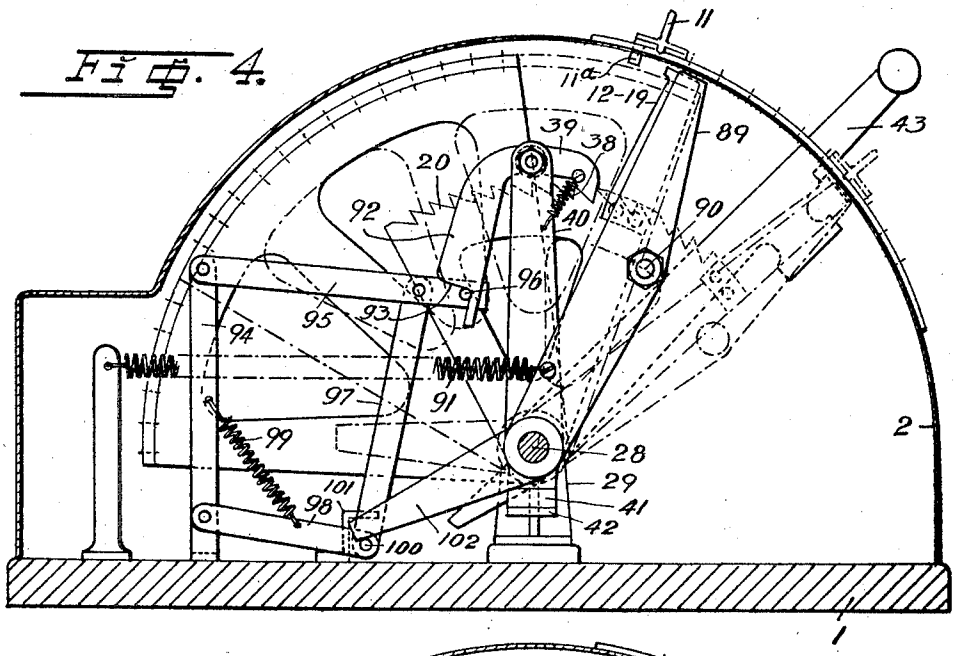
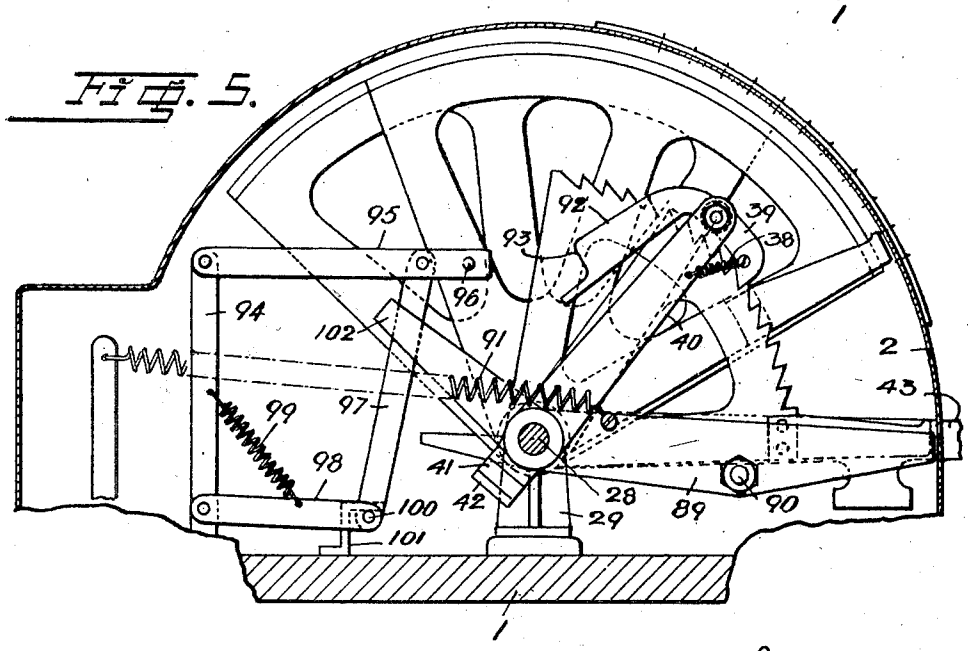


Fig. 5.



Inventor.
Arvid G. Damm.
By Henry Orth & Co Atty.

Patented Feb. 19, 1924. 1,484,477

UNITED STATES PATENT OFFICE.

ARVID GERHARD DAMM, OF RONNINGE, SWEDEN.

APPARATUS FOR CIPHERING AND DECIPHERING CODE EXPRESSIONS.

Application filed March 25, 1922. Serial No. 546,836.

To all whom it may concern:

Be it known that I, ARVID GERHARD DAMM, a citizen of the Kingdom of Sweden, residing at Ronninge, Sweden, have invented new and useful Improvements in Apparatus for Ciphering and Deciphering Code Expressions, of which the following is a specification.

In commercial telegraphic correspondence code books are extensively used, by means of which commercial denominations, embracing one or several words or even complete phrases, may be rendered by one single abbreviated group of signs, usually comprising 4-6 letters or figures. The object of the codes published is to reduce the cost of telegrams. As a means of safeguarding the secrecy of messages such codes are of no real practical value, being always available in the open market for the translation of such telegrams into plain language. Even the use of a private code, which is kept secret, always implies a considerable risk, as the code must soon become known to a number of persons, and besides may be lost, stolen or copied, for instance photographically, this often not being known to the correspondents until a considerable number of telegrams have been despatched. The numerous simple methods of a subsequent ciphering of the code expressions, hitherto applied in order to avoid such risks, have rarely proved satisfactory, a real security having been obtained only by continuously changing the principle of ciphering, a procedure which at all events implies loss of time and frequent mistakes and errors.

According to the international telegraphic service regulations a group of 5 arbitrary figures or else a pronounceable group of 10 letters is taxed as a unit. Conseqeuntly a figure cipher telegram containing for instance 20 figures is taxed as 4 units of 5 letters each, while the same telegram, if translated into pronounceable groups of letters, will be taxed only as 2 units of 10 letters each, and the tariff expense will in the latter case be 50% of that in the former. The object of this invention is to effect such a translation by mechanical operations of a kind to admit of a simultaneous and unequivocal ciphering and deciphering impenetrable to parties not concerned and of its immediate recording in type-print. This result, hitherto not obtainable by any known mechanical ciphering device, is made possible by the use of a special kind of letter groups comprising two signs, of which one is always a vowel and the other always a consonant, and by a special arrangement of the type-carrying members of the apparatus relatively to its members adjustable in accordance with the signs to be translated.

This relation is schematically shown by the following table:

A_1	B_1		C_1	D_1
→y→m	→y→z		1 1	6 1
u l	u x		2 2	7 2
o k	o w		3 3	8 3
e j	e v		4 4	9 4
a h	a t	Arrangement of types (Type wheels)	5 5	0 5
y g	y s		1 6	6 6
u f	u r		2 7	7 7
o d	o q		3 8	8 8
e c	e p		4 9	9 9
a b	a n		5 0	0 0
Enciphering.			Deciphering.	
→5→0	→0→0		a b	a n
4 9	9 9		→e c	→e p
3 8	8 8		o d	o→q
2 7	7 7		u f	u r
1 6	6 6	Scale of adjustment (Key board)	y g	y s
5	5		h	t
4	4		j	v
3	3		→k	w
2	2		l	x
1	1		m	z
A.	B.		C.	D.

According to the above two kinds of letter groups are used, consisting either of a vowel followed by a consonant or of a consonant followed by a vowel, in which any letter used must unequivocally correspond to one of the ten figures. As the use of ten vowels is not permitted in international telegraph correspondence, certain vowels would have to correspond to two figures, and consequently unequivocal deciphering would be impossible, if no possibility existed in each instance to determine the casual meaning of a vowel generally corresponding to two figures.

Such a possibility does, however, exist, twenty consonants telegraphically permitted being available as equivalents, which renders it possible always to translate a figure by two different consonants alternatively, so that one of these consonants is used when the vowel adjoined has one of its figure meanings, and the other consonant, when the vowel in question has its other meaning.

In the above table the letter groups used are of the type *ab*, in which *a* represents any one of five admissible vowels a, e, o, u, y and *b* any one of the twenty admissible consonants b, c, d, f, g, h, j, k, l, m, n, p, q, r, s, t, v, w, x, z.

The scale of adjustment (key-board) for the ciphering is represented in the table by the two double-figure columns A and B, and the adjustment for ciphering of a certain figure is supposed to be effected by the displacement of the indicators represented by arrows to the left of each column.

The type-carrying members for recording the cipher, consisting in reality of type-wheels, are represented in the table by the two double-letter columns A_1 and B_1, which are supposed to be movable in such a way, that a letter column is moved as many steps upward as the indicator is moved downwards relatively to the corresponding column of the scale of adjustment, so that the indicators represented by arrows to the left of each letter column A_1, B_1 are brought into a position to point out the cipher sign resulting. As shown by the table, the vowel columns A_1 and B_1 contain the same five vowels, repeated twice in the same order, while each of the consonant columns contains ten different consonants. The two vowel columns correspond to figure columns A and B, representing the type-carrying members, each of which contains five different figures, repeated twice in each column in the same sequence as in the columns containing the ten figures and corresponding to the two consonant columns.

Supposing a couple of digits 73 is to be ciphered, the indicators to the left of the double column B must be moved downwards, the left one by three steps and the right one by seven steps, which according to the above supposition effects an upward movement of the left column B_1 by three steps, the indicator then pointing at letter e, and of the right column B_1 by seven steps, the indicator then pointing at letter q, by which operation the letter group eq is obtained as an equivalent of the figure group 73.

Supposing a couple of digits 28 is to be ciphered, the corresponding operations of adjustment will have to be performed within columns A, resulting in corresponding movements of columns A_1 and in the cipher ek.

Thus in both these instances the first figure is rendered by letter e with a different signification in each instance.

By means of the table it will be shown, that the deciphering will give an unequivocal result. The reversed order of signs in the scale of adjustment and on the typewheels relatively to the columns for ciphering is clearly shown by columns C, D and C_1, D_1 respectively.

The deciphering operations will be as follows:

As shown by the arrows the indicators are adjusted for eq in columns D, which effects a corresponding movement of columns D_1 bringing the figures 73 into recording position, and for ek in columns C, which records 28 in C_1.

Whether the one or the other of the double columns A, B has to be used for ciphering or the one or the other C, D for deciphering, will be obvious on account of the fact, that a group of figures or of letters can be found only within one of those double columns.

If the ciphering operation is effected by ciphering the first figure according to the right and the second figure according to the left column of double columns A and B, letter-groups of the type ba instead of ab will be produced.

If the series of signs within A_1 B_1 C_1 and D_1 are cyclically arranged, for instance as types on the circumference of wheels, it is evident that their initial positions may be arbitrarily varied relatively to each other and to the scale of adjustment. Consequently, as every single operation of ciphering may be considered either as an independent individual operation or as a member of a continuous series of such operations, it is also evident that, when continuously ciphering, the relative initial positions can always be arbitrarily varied between two individual ciphering operations by the influence of some key-mechanism, for instance by relating to a member, representing a series of figures and movable in two different directions, according to the U. S. Patent No. 1,233,035.

In the accompanying drawings I have shown one embodiment of my invention. Fig. 1 shows a front elevation of the apparatus, the one side of the cover being removed. Fig. 2 is a view from above with part of the cover removed. Fig. 3 is a section on line A—B in Fig. 2. Fig. 4 is a section on line C—D in Fig. 1, and Fig. 5 the section last mentioned with some members in different positions. In Figs. 4 and 5 certain details are omitted in order to make the figures clearer.

In the drawings 1 indicates a bottom plate and 2 a cover formed with eight slots, 3, 4, 5, 6, 7, 8, 9 and 10 (Fig. 2), in each of which a slide 11 having a lug 11^a is movable. The sides of said slots are provided with uniformly divided scales, the divisions of which are marked with figures or letters, arranged in accordance with the columns A, B, C and D of the table mentioned above. Each of said indicator slides actuates a lever 12, 13, 14, 15, 16, 17, 18, 19 respectively (Figs. 1, 4 and 5) by the lug 11^a on each slide, each lever being fixed to a ratchet sector 20, 21, 22, 23, 24, 25, 26, 27 respectively. These sectors are swingably journalled on a shaft 28 mounted in bearings 29, another sector 30, 31, 32, 33, 34, 35, 36, 37 respectively being fixed to the hub of each ratchet sector. These

sectors are attached respectively one to each of the ratchet sectors, 30 to 13, 31 to 12, 33 to 22, 32 to 23, 34 to 17, 35 to 16, 37 to 18 and 39 to 19, 33, 22 for instance being coupled together by a tube, journalled on another tube coupling together 32 and 23 and journalled in its turn on the shaft 28. On the circumference of the sectors 30—37, denominated typesectors, types are arranged in accordance with the columns A_1, B_1, C_1 and D_1 of the table mentioned above, so that the type sector 30 corresponds to the right and the type sector 31 to the left column A_1, the type sector 32 to the right and 33 to the left column B_1, the type sector 34 to the right and 35 to the left column C_1, the type sector 36 to the right and 37 to the left column D_1.

Each ratchet sector is operated by a pawl 39, kept down by a spring 38 (Figs. 4 and 5), carried by the long arm of a lever 40, swingable on the shaft 28. Below the shaft 28 the levers 40 are provided with short arms 41, on which a bar 42 is fixed, rigidly connecting all levers 40 to each other. In starting position the ratchets engage the first tooth (farthest to the right in Figs. 4 and 5) of each ratchet sector. When one of the indicator slides 11, for instance the second one from the left in Fig. 2, is moved for instance to the seventh line of division of the corresponding scale, as indicated by dash lines in Fig. 4, the corresponding lever 13 and ratchet sector 21 partake of this movement, through which the pawl 39 is brought to engage the seventh tooth of the ratchet sector, counting from the right in Figure 4.

The type sector joined to the ratchet sector in question is hereby turned a corresponding angle, so that its seventh type from the right in Fig. 4 reaches a position perpendicularly above the centre of the shaft 28, which position corresponds to that of a printing mechanism of a known kind (not shown in the drawings), by means of which a print of the type in question can be obtained on a paper band or the like. Before, however, said printing mechanism is brought into action, a further movement must be imparted to said type sector by means of its ratchet sector, the length of said movement being determined by two co-operating members, each representing an arbitrary series of figures If a device for imparting such a variable movement were not used, the pronounceable letter cipher obtained would become what is technically termed "elementary," that is, a couple of consecutive figures, for instance 35, would invariably be translated for instance by "up", while an additional and variable movement of the type sectors has the effect of rendering the ciphering result variable, so that said couple of figures will alternatively be translated for instance by "up", "ab", "iq" and so forth. It is well known that the variability of a cipher during a period of arbitrary length is of the greatest importance as regards its resistance to analytic decoding by outsiders. As shown in the drawings the devices for this purpose are as follows:

On the hub of a driving lever 43 an arm 44 is fixed, connected by an axle 45 (Fig. 3) to an arm 46 (Figs. 2 and 3), both members 43 and 46 swinging on shaft 28.

On the axle 45 nine arms 47 are swinging. The contour of these arms is circular and each is provided with a catch 48 and is extended on the other side of axle 45 as an arm 49, influenced by a spiral spring 50, attached to a rod 51, which connects the two arms 44 and 46. The catches 48 are adapted to actuate a fan-shaped member 52, which swings on the shaft 28 and consists of nine parts of the same shape and fixed together.

The nine parts of member 52 are displaced stepwise relatively to each other, each step corresponding to the division of the ratchet sectors, respectively to the distance between the types of the type-sectors. The curved arms 47 are, when in rest, kept in such a position by the springs 50, that when the driving lever 43 is turned down, all catches 48 pass the fan-shaped member 52 without actuating same, except one, which by the pressure of a key-member described below is kept down in spite of the action of its spring 50. The upper ends of the arms 47 are guided by slotted arms 55, swinging on an axle 53 and actuated by springs 54, which also serve to arrest the fan-shaped member 52 at the end of its movement. This latter member 52 is rigidly connected to the above-mentioned bar 42, which connects the shorter arms 41 of the levers 40 carrying the ratchets 39. The key-member referred to above consists in the embodiment shown of two disks 57, both fixed on an axle 56, the said discs 57 being connected by nine rods 58 (Fig. 2) placed at the same radial distance from the axle 56 and at the same peripherical distance from one another. Each of these rods 58 carries an adjustable roller 59, which, in a certain position of the disks 57, serves to keep one of the curved arms 47 pressed down (compare Fig. 3). The rollers 59 may be adjusted, relatively to each other and to the arms 47 influenced, in accordance with an arbitrary series of figures.

Supposing the key-member just described to be in such a position, that one of its rollers actuates an arm 47 corresponding to that part of the fan-shaped member 52, which in Fig. 3 is shown farthest to the right and which also is nearest to the guide arms 55 and farthest away from the catches 48, the turning downwards of the driving lever 43 will cause the arm 47 in question by its catch 48 to turn the member 52 an angle corresponding to one division of the ratchet sectors, the member 52 being at the end of

this movement arrested by the guiding arm 55 depressed by the arm 47 in question.

If the key-member occupies such a position, that one of its rollers 59 is keeping down the second arm 47 from the right in Fig. 2, the member 52 will be turned an angle corresponding to two divisions of the ratchet sectors and so forth. Thus, depending upon the occasional positions of the rollers 59 of the key-member, the ratchet sectors may, by the turning down of the driving lever 43, receive a turning movement corresponding to any number from one to nine of the divisions of the ratchet sectors, said movement of the driving lever 43 taking place after the indicators 11 have been adjusted.

In the embodiment shown the occasional position of the key-member is determined by the following arrangement (Figs. 2 and 3). On the axle 56 of the key-member two ratchet-wheels 60, 61 are fixed with their teeth pointing in opposite directions, each wheel having nine teeth. Each of these ratchet wheels 60, 61 can be engaged by a pawl 62, 63 respectively. These pawls are linked to a cross bar 64 placed on a sliding rod 66 perpendicularly movable in a stud 65 and pressed down by a spring 67. The pawls are attracted towards each other by a spring 68, and between them a roller 69 is placed, said roller being disposed in a slot 70 (Fig. 2) in a sliding rod 71. At one end this rod 71 carries another roller 72, a spiral spring 73 pressing the rod and said roller 72 against the links of a chain 74. As described in the U. S. Patent No. 1,233,035 this chain is composed of flat links and segment-shaped ones arranged in accordance with an arbitrary series of figures. When the roller 72 meets a flat link, the pawl 62 will engage the ratchet wheel 60, as shown in Fig. 3, whereas, when the roller 72 meets a segment link, the rod 71 is displaced to the right in Fig. 3, pawl 63 consequently engaging ratchet wheel 61. A knob on the sliding rod 66 enters into a groove in a lever 76. One end of said lever 76 turns on a journal in a support 75 and its other end is at the end of the downward movement of the driving lever 43 actuated by an arm 77 fixed thereto, this causing the sliding rod 66 to move upwards against the spring 67, so that either of the pawls 62 or 63 momentarily engaging its ratchet wheel can engage a new tooth of that ratchet wheel. When the driving lever 43 is then turned back into its idle position, the key-member will, on account of the downward action of spring 67 on the pawl-mechanism described, turn one step in one direction or the other, the direction depending upon the momentary position of the chain 74.

This chain is moved a distance corresponding to the length of one link by each downward movement of the driving lever 43. At the end of each such movement a protruding part 78 of said lever 43 actuates one of the arms of a double-armed lever 80, journalled in bearing 79, its other arm being pivoted to a bar 81, connected by a universal coupling 82 to a sliding rod 83, which is pivoted to a double-armed lever 84 (Fig. 2), swinging on the axle 85 of a ratchet wheel 88 fixed to a prism 86 driving the chain 74.

Said double-armed lever 84 carries a pawl 87 engaging the ratchet wheel 88. When the arm to the right in Fig. 3 of lever 80 is pressed down by the portion 78 of the driving lever 43 and the rod 83 is pushed to the right in Fig. 3, which movement corresponds to an upward movement in Fig. 2, the pawl 87 will turn the ratchet wheel 88 such an angle that the chain 74 moves the length of one link. When the driving lever 43 is turned upwards, a spring (not shown on the drawings) moves the sliding bar 83 so far downwards in Fig. 2 that the pawl 87 engages the next tooth of the ratchet wheel 88.

In order to return the ratchet- and type-sectors into their idle positions the following device is provided. On the shaft 28 are journalled two arms 89 (Figs. 1 and 5), rigidly connected to each other by a rod 90, which by a spring 91, is pressed against the ratchet sectors. When the driving lever 43 is turned upwards from the position shown in Fig. 5, the arms 44 and 46 (Figs. 2 and 3) turn to the left in Fig. 3, in which movement the bent arms 47 partake, one of these having, as described above, at an earlier moment turned the fan-shaped member 52 to the right in Fig. 3. This member 52, connected by the bar 42 to the double-armed levers 41, 40, which carry the pawls 39, will then be turned to the left in Fig. 3 by the spring 91, which forces all ratchet- and type-sectors back to their starting position. Each of the pawls 39 is provided with an arm 92 (Fig. 4), having at its lower end a recess 93, one side of which is slightly rounded. Said arm 92 enters between two parallel arms 95, rigidly connected to each other and pivotally connected to a fixed support 94, a pin 96 or the like being fixed in said arms.

By a link 97 the arms 95 are connected to an arm 98 pivotally connected to the support 94 and actuated by a spring 99 tending to lift the arm 98. All arms 98 are connected together by a rod 100, which also serves to connect the links 97 and the arms 98 and which, when lifted by the action of the spring 99, presses against a stop 101 secured to the base plate 1.

Before those ratchet sectors, the type-sectors of which have occasionally been adjust-

ed for enciphering or deciphering, come back into their position of rest, the arms 92 of their pawls 39 will engage the corresponding pins 96, thus, as the movement continues, disengaging the pawls 39 from their ratchet sectors 20. Just before these ratchet sectors, respectively the arms 89, reach their idle position (Fig. 4) a projection 102 of each arm 89 will force the rod 100 downwards, this movement being transmitted to the arms 95 and the pins 96 by means of the links 97. The pins 96 now engage the recesses 93 of the pawl-arms 92, which latter again engage the ratchet sectors 20.

When a group of figures, for instance 353567 is to be ciphered, the operations and their results are as follows, it being supposed that the initial positions and arrangement of the chain 74 and the revolving key member are as shown in Fig. 2, a roller 59 pressing down the fourth lever 47 from the left. According to said drawing the revolving key member represents, if rotating in the direction determined by a high link of the chain 74, a series of figures 6, 2, 5, 8, 4, 1, 7, 3, 9, each figure of which equals the number of steps of additional movement given to the sectors by means of the fan-shaped plate 52.

It should be noted that the slides during the first step of adjustment will not actuate the sectors, as is evident from Fig. 4.

When ciphering, which always comprises two figures, the adjustment for the second figure is first made, thus in this instance the first indicator from the left on 5, the second indicator from the left on 3, by which operation the type sector 31 is not turned, while the type sector 30 is turned seven steps. Then the driving lever 43 is pressed down, this movement bringing a high link of the chain 74 to bear against the roller 72 and turning, by the action of the sixth lever 47 from the right on the fan-shaped plate 52, the type sectors six steps. At the end of the downward movement of the driving lever the type sector 31 thus has been turned six steps while the type sector 30 has been turned thirteen steps. The types of these sectors being in printing position thus are y and k respectively, which letters will be recorded as k y. When returning the driving lever 43, the pawl 63 (Fig. 3) will turn the revolving key member so as to make a roller 59 press down the second lever 47 from the right in Fig. 2. The next adjustments of the indicators are the same. The downward movement of the driving lever, which brings a new high link into operative position, will move the sectors two steps, bringing into printing position u and c, recorded as c u.

The next adjustments will be: the third indicator from the left on 7 and the fourth on 6, turning the type sectors 33 and 32 three and four steps, respectively. As the additional movement caused by the downward movement of the driving lever 43 will be five steps the types o and p of the type sectors will come into printing position and will be recorded as p o.

Thus the figures 353567 will be ciphered as ky cu po.

In order to decipher this code word, the revolving key member and the key chain are placed in the same initial positions as used for the ciphering.

The adjustments will be: the sixth indicator from the left on k and the fifth indicator from the left on y, turning the type sectors 34 and 35 seven and four steps respectively. The additional movement imparted by the fan-shaped plate 52 will be six steps, bringing the types 3 and 5 respectively into printing position to be recorded as 35. When returning the driving lever, the pawl 63, (Fig. 3) will turn the revolving key member so as to make a roller 59 press down the second lever 47 from the right, in Fig. 2. The next adjustments will be: the sixth indicator from the left on c and the fifth indicator from the left on u, turning the type sectors one and three steps respectively. The additional movement of these sectors caused by the fan-shaped plate will be two steps, bringing the types 3 and 5 into printing position, recorded as 35. The movements of the driving lever have then brought a new high link of the chain and a roller of the revolving key member to press down the fifth lever 47 from the right or left into active position. The next adjustments will be: the eighth indicator from the left on p and the seventh indicator from the left on o, turning the type sectors 36 and 37 one and two steps respectively. The additional movement is five steps, thus bringing the type 6 of the type sector 36 and the type 7 of the type sector 37 into printing position, to be recorded as 67.

Thus the code word ky cu po has been deciphered into the original sequence of the figures 353567.

Having now described my invention I declare that what I claim is:—

In an apparatus for recording in type-print two-letter syllables, always composed of one vowel and one consonant and constituting cipher-equivalents of two-figure groups, and for the rendering in type-print two-figure groups, constituting cipher-equivalents of two-letter syllables of said kind, the combination of a scale of adjustment, one part of which, for the ciphering of two-figure groups, comprises four series of figures, two of these series containing ten different figures in arbitrary order and the other two series containing each five figures in arbitrary order, these figures being different in one series as compared to the other,

and the other part of which scale, for the ciphering of two-letter syllables, comprises four series of letters of which series two contain each ten different consonants in arbitrary order and the two other both contain the same arbitrary sequence of five vowels, and eight rotary type-wheels, four carrying letter-types and four figure-types, of which type-wheels those carrying letter-types are dependent, as to their movements, each on a member adjustable according to one of the four series of figures of the scale of adjustment, the arrangement of the letter-types being such, that the two type-wheels dependent each on a member adjustable according to the series of ten figures carry each ten consonant-types, for each wheel the same as are comprised in one of the series of ten consonants of the scale of adjustment, though in reversed order, and that the two type-wheels, which are dependent each on a member adjustable according to one of the series of five figures, carry the same five vowel-types repeated twice in the same sequence on each type-wheel and for each type-wheel in reversed order, as compared to that of one of the series of five vowels of the scale of adjustment, the four type-wheels carrying figure-types being dependent as to their movements each on a member adjustable according to the letter-series of the scale of adjustment, the arrangement of the figure-types being such that the two type-wheels, each of which is dependent on a member adjustable according to one of the series containing ten consonants, both carry the same figure-types, for each wheel in reversed order as compared to that of one of the ten-figure series of the scale of adjustment, and that the two type-wheels, each of which is dependent on a member adjustable according to one of the five-vowel series, carry each five different figures repeated twice in the same order on each wheel and for each wheel identical to those of one of the five figure series of the scale of adjustment, but arranged in reversed order.

In testimony whereof I have signed my name.

ARVID GERHARD DAMM.