No. 879,667. PATENTED FEB. 18, 1908.

H. C. NEWTON & A. G. M. MICHELL.

CIPHER SYSTEM.

APPLICATION FILED AUG. 30, 1907.

2 SHEETS—SHEET 1.

Fig. 1.

00	BA	20	CA	40	BO	60	FE	80	ZY	0	HO
01	RA	21	XE	41	ZI	61	WO	81	KI	1	SE
02	BE	22	XA	42	NE	62	XI	82	DY	2	SA
03	FA	23	PA	43	RO	63	DE	83	CY	3	HE
04	GO	24	VA	44	KO	64	MI	84	GU	4	SI
05	ZA	25	JA	45	KU	65	JO	85	VY	5	SO
06	JI	26	GA	46	GE	66	VU	86	PO	6	HU
07	NA	27	LO	47	PU	67	VI	87	NI	7	HY
08	GE	28	MA	48	RU	68	FY	88	MU	8	HA
09	RE	29	ME	49	JE	69	XU	89	NU	9	SU
10	KA	30	TA	50	FO	70	BY	90	LU	-	SY
11	WE	31	WA	51	BU	71	ZU	91	KY		
12	PE	32	TE	52	BI	72	MY	92	TI		
13	LE	33	DI	53	WU	73	NY	93	XY		
14	DA	34	XO	54	VE	74	LI	94	CU		
15	ZO	35	TU	55	ZE	75	PY	95	TY		
16	VO	36	DU	56	WI	76	LY	96	FU		
17	LA	37	RI	57	GI	77	JY	97	GY		
18	KE	38	CO	58	FI	78	CI	98	WY		
19	DO	39	PI	59	JU	79	RY	99	NO		

Fig. 2

BA	00	BE	02	BI	52	BO	40	BU	51	BY	70
CA	20	CE	08	CI	78	CO	38	CU	94	CY	83
DA	14	DE	63	DI	33	DO	19	DU	36	DY	82
FA	03	FE	60	FI	58	FO	50	FU	96	FY	68
GA	26	GE	46	GI	57	GO	04	GU	84	GY	97
HA	8	HE	3			HO	0	HU	6	HY	7
JA	25	JE	49	JI	06	JO	65	JU	59	JY	77
KA	10	KE	18	KI	81	KO	44	KU	45	KY	91
LA	17	LE	13	LI	74	LO	27	LU	90	LY	76
MA	28	ME	29	MI	64			MU	88	MY	72
NA	07	NE	42	NI	87	NO	99	NU	89	NY	73
PA	23	PE	12	PI	39	PO	86	PU	47	PY	75
RA	01	RE	09	RI	37	RO	43	RU	48	RY	79
SA	2	SE	1	SI	4	SO	5	SU	9	SY	-
TA	30	TE	32	TI	92			TU	35	TY	95
VA	24	VE	54	VI	67	VO	16	VU	66	VY	85
WA	31	WE	11	WI	56	WO	61	WU	53	WY	98
XA	22	XE	21	XI	62	XO	34	XU	69	XY	93
ZA	05	ZE	55	ZI	41	ZO	15	ZU	71	ZY	80

Witnesses;
C. D. Kesler
H. B. Kesler

Inventors
Henry C. Newton
Anthony A. M. Michell
By
James L. Norris.
Atty.

No. 879,667. PATENTED FEB. 18, 1908.

H. C. NEWTON & A. G. M. MICHELL.

CIPHER SYSTEM.

APPLICATION FILED AUG. 30, 1907.

2 SHEETS—SHEET 2.

Fig. 3.

	00	32	64	96
1	01	33	65	97
12	02	34	66	98
123	03	35	67	99
1234	04	36	68	
12345	05	37	69	
1235	06	38	70	
124	07	39	71	
1245	08	40	72	
125	09	41	73	
13	10	42	74	
134	11	43	75	
1345	12	44	76	
135	13	45	77	
14	14	46	78	
145	15	47	79	
15	16	48	80	
2	17	49	81	
23	18	50	82	
234	19	51	83	
2345	20	52	84	
235	21	53	85	
24	22	54	86	
245	23	55	87	
25	24	56	88	
3	25	57	89	
34	26	58	90	
345	27	59	91	
35	28	60	92	
4	29	61	93	
45	30	62	94	
5	31	63	95	

Witnesses:
C. D. Kesler
J. B. Kesler

Inventors
Henry C. Newton
Anthony G. M. Michell
By
James L. Norris.
Atty.

UNITED STATES PATENT OFFICE.

HENRY CLEMENT NEWTON, OF KEW, NEAR MELBOURNE, AND ANTHONY GEORGE MALDON MICHELL, OF MELBOURNE, VICTORIA, AUSTRALIA.

CIPHER SYSTEM.

No. 879,667. Specification of Letters Patent. Patented Feb. 18, 1908.

Application filed August 30, 1907. Serial No. 390,763.

To all whom it may concern:

Be it known that we, HENRY CLEMENT NEWTON, a subject of the King of Great Britain, residing at "Kenilworth," Barry street, Kew, near Melbourne, in the State of Victoria, Australia, engineer, and ANTHONY GEORGE MALDON MICHELL, a subject of the King of Great Britain, residing at No. 413 Collins street, Melbourne aforesaid, engineer, have invented a Cipher System, of which the following is a specification.

This invention relates to cipher systems and the object thereof is the providing of a cipher-system for the transmission of telegraphic and similar messages, in which a check upon the correctness of transmission is contained intrinsically in the constituent parts of the message, this check being superimposed upon the ordinary meaning.

Code-meanings may be attached to the syllables in various ways known and practiced in code-telegraphy, but the system is preferably employed in connection with a code-book of phrases containing phrases associated with distinctive numbers, such code-books being well known and in common use.

In the drawings which form a part of this specification:—Figure 1 is a view illustrating the tabulation of the symbols employed in the system. Fig. 2 is a similar view of another tabulation of the symbols employed in the system, and Fig. 3 is a tabulation of the combinations involved in the method of checking employed in the system.

The code of symbols employed in the present system consists of biliteral syllables and numbers, the syllables and numbers being mutually representative of each other. Each biliteral syllable, hereinafter called simply a "syllable", consists of a consonant and a vowel, a syllable in which the consonant preedes the vowel is called a "normal" syllable, one in which the vowel precedes the consonant a "reversed" syllable. The normal and reversed syllables consisting of the same two letters are said to form a pair, and are represented indifferently by one and the same code-number. For this preferred application the system employs one hundred and eleven pairs of syllables and one hundred and ten numbers, namely all the two-figure numbers 00, 01, 02, . . . 99 together with all the single-figure numbers 0, 1, 2, . . . 9. Each of these numbers is represented indifferently by either one of a pair of syllables. One hundred and ten of the pairs of syllables are thus employed, the remaining pair is used to indicate a blank or missing number. The one hundred and eleven pairs of syllables may be selected from the one hundred and fourteen combinations of nineteen consonants with the six vowels a, e, i, o, u and y, and the syllables whether normal or reversed combine to form pronounceable groups. The selection of syllables which is preferably employed is set out in the table in Fig. 1, each normal syllable being placed opposite the number which it represents.

In coding a message from the code-book of phrases, the numbers associated with the phrases of the message are written or otherwise placed in succession, and are divided into groups each consisting of a definite number of digits, which for adaptation to prevalent telegraphic usuage is preferably ten, as we hereinafter assume. It will be apparent in the course of the description that the same system may be applied with groups of any other number of digits.

The groups of ten digits will not necessarily correspond with the phrases, and the whole series of digits may not be exactly divisible into groups of ten. In such cases the last group is still to be considered as having ten places, some at the beginning containing digits and the others at the end being blank.

The numerical groups are converted into literal groups by the division of each group of ten digits into five pairs of digits and by the substitution for each pair of digits or two-figure number of the normal syllable which it represents, as explained above and set out in Table 1. If the last group contains an odd number of digits, the last digit is written as a single digit, the preceding digits, if any, are written in pairs as in the other groups, and after the last digit a number of blank spaces is indicated equal to the quotient of the number of missing digits divided by two. The total number of pairs of digits, single digits and blank spaces in the last group is therefore five, and equal to the number of pairs of digits in each of the other groups, and each of them is replaced by the normal syllable which it represents, as shown in Table 1, each of the blanks being denoted by SY. Each of the groups of five normal syllables formed as above explained is hereinafter called a

"normal word." A group of five syllables whether normal or reversed is called simply a "word."

As an example of the method of forming the words as above explained, let it be supposed that the last fifteen figures of the message were

743120906539730

These are divided into two groups, the first containing five pairs of digits and the second two pairs of digits, one single digit and two blank spaces, thus:—

74 31 20 90 65 39 73 0 . . .

and the equivalent literal groups or "normal words" are according to Table 1

LI WA CA LU JO PI NY HO SY SY.

The provision of normal and reversed syllables each having the same numerical values enables a check upon the correctness of transmission of each word to be incorporated in it, this check being superimposed upon its code-meaning. Every word of the message consisting of five syllables may be transmitted in thirty-two different forms. This is shown in Table 3 which sets out in its first column thirty-one different selections of one or more of the digits from 1 to 5 inclusive, indicating thirty-one different combinations of normal and reversed syllables possible in a five-syllable word, or with the original normal word itself thirty-two forms of the word, all expressing the same code-meaning. Any particular arrangement of normal and reversed syllables corresponding to the numbers in the first column of Table 3 is thus associated with one of the numbers from 00 to 31 set out in the second column, and may be used to indicate such a number, hereinafter called the check-number, derived as by summation from the separate numbers which the syllables respectively represent.

The correspondence of the check-number expressed by the arrangement of syllables in the word as received, with the number derived by summation of the numbers represented by the separate syllables as received, constitutes a proof that the word has been correctly transmitted.

In the ordinary procedure of coding a message the summation above mentioned is practiced in the following manner. The five pairs of digits in a group are added as if each of them were a two-figure number, a single digit occurring in the last group of a message being treated for this purpose as if it were preceded by zero and also formed a two-figure number, and blanks being treated as zeros. The sum will in all cases be less than five hundred. If there are three digits in the sum the first is removed and the two-figure number formed by the remaining two digits is divided by thirty-two, and the remainder resulting from the division, being one of the numbers 00, 01, 02, . . . 31, is found among the check-numbers in the second column of Table 3. The syllables, if any, in the normal word whose places are indicated by the figures in the first column opposite to this check-number are to be reversed, the other syllables remaining normal. The code-word is then completed for transmission.

As an example of the method of completing the word for transmission let it be supposed that the last fifteen figures of the message were

743120906539730

giving the numerical and literal groups

74 31 20 90 65 39 73 0 . . .

LI WA CA LU JO PI NY HO SY SY

as explained.

The sums of the pairs of digits in the numerical groups are 280 and 112 respectively.

Removing the first figures in each case leaves the numbers 80 and 12; dividing these by 32 gives remainders 16 and 12 and from Table 3 it is found that the syllables to be reversed are 1 and 5 in the first word and 1, 3, 4, and 5 in the second.

The completed words are thus:—

ILWACALUOJ IPNYOHYSYS.

To save the labor of effecting the division by thirty-two all the two-figure numbers which will produce the same remainder are written in line with it in the table, forming the third, fourth and fifth columns thereof.

It will be observed on inspection of Table 2 that no syllables having a letter in common are represented by numbers differing by exactly thirty-two. Consequently the substitution of one letter for another in transmission must alter the remainder resulting from the division of the sum of the constituent numbers of a group by thirty-two, and will be detected by the check.

To check a message upon its receipt, the process above described is carried out in the reverse order. The two-figure number formed by the last two digits of the sum of the five numbers represented by the five syllables of the word is divided by thirty-two. The remainder after division is found in the second column of Table 3. The places of the reversed syllables of the word should be indicated in the first column and on the same line as this remainder. If this is not so the word has been incorrectly transmitted.

The removal of the first figure of the sum in the above process is a matter of convenience merely, and the same process of division by thirty-two may be applied to the sum as first obtained, the remainder being dealt with exactly as before. It is also evident that in place of the number thirty-two

any lesser number may be used as divisor, without affecting the principle of the system. All the 32 possible arrangements of normal and reversed syllables in a five syllable word would not in such cases be required, but only a number equal to the divisor employed. The divisor 32 however provides a more stringent check than any smaller number.

It will also appear from the foregoing explanation that syllables may have one set of numbers associated with them for the purposes of the check, and another set for the attachment of code meanings; or again, numbers may be associated with the syllables for the purposes of the check only, the meanings being attached in any other of the ways known or practiced in code-telegraphy or cipher-telegraphy.

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. In a cipher-system employing a number of syllables each consisting of one consonant and one vowel; the assignment to each pair of such syllables having the same consonant and vowel of a common numerical value; the distinction of the two syllables of each such pair as normal or reversed according as the consonant or vowel precedes; the combination or resolution of a message as a succession of such syllables either normal or reversed; the division of such message into sections each consisting of a definite number of such syllables; the assignment to each of such sections of a check number according to the succession of normal and reversed syllables; and the establishment of a correspondence between the check-number so assigned to such section and a totality of the numerical values assigned to its separate syllables all for the purposes set forth.

2. In a cipher-system employing a number of syllables each consisting of one consonant and one vowel; the assignment to each pair of such syllables, having the same consonant and vowel, of a common numerical value less than 100; the distinction of the two syllables of each such pair as normal or reversed according as the consonant or vowel precedes; the combination or resolution of a message as a succession of such syllables either normal or reversed; the division of such message into sections of five syllables each; the assignment to each such section of five syllables of a check number from 0 to 31 according to the order of succession of the normal and reversed syllables; and the establishment of an equivalence between the check-number so assigned to each section and the remainder obtained upon division by 32 of the sum, or last two figures of the sum, of the numerical values assigned to the separate syllables of the section all for the purposes set forth.

3. In a cipher-system, employing pronounceable words of five syllables consisting each of one consonant and one vowel; the assignment to each pair of syllables having the same consonant and vowel of a common numerical value less than 100; the distinction of the syllables of each such pair as normal or reversed, according as the consonant or vowel precedes; the assignment to such words of check-numbers from 0 to 31 according to the order of succession of normal and reversed syllables; and the establishment of an equivalence between the check-number so assigned to such word, and the remainder obtained upon division by 32 of the last two figures of the sum of the values assigned to the separate syllables of the word, all for the purposes set forth.

4. A cipher-system comprising a table of biliteral syllables and numbers, said syllables associated with said numbers, the numerical order of the numbers being independent of the alphabetical order of the syllables, and no two numbers associated with syllables having the same consonant or same vowel differing by 32 or by a multiple of 32.

In testimony whereof we have hereunto set our hands in the presence of two subscribing witnesses.

HENRY CLEMENT NEWTON.
ANTHONY GEORGE MALDON MICHELL.

Witnesses:
EDWARD WATERS,
EDWARD NEEDHAM WATERS.