Available online at www.sciencedirect.com
SCIENCE DIRECT®
ELSEVIER
Advances in Applied Mathematics 34 (2005) 697–708
ADVANCES IN Applied Mathematics
www.elsevier.com/locate/yaama

Lewis Carroll's ciphers: The literary connections

Francine F. Abeles *

Department of Mathematics & Computer Science, Kean University, Union, NJ 07083, USA

Received 11 May 2004; accepted 15 June 2004

Abstract

Charles L. Dodgson, who lectured on mathematics at Christ Church in Oxford University, constructed ciphers that were state of the art in his time. In poems and letters he demonstrated a great talent for creating acrostics and anagrams. In this paper I describe the ciphers closely and argue that their creation was intertwined with his word game inventions.

Keywords: Carroll; Dodgson; Baynes; Cryptography; Cipher; Beaufort; Variant Beaufort; Vigenère; Logarithm

1. Introduction

As the mathematical lecturer at Christ Church, Oxford, Charles L. Dodgson (Lewis Carroll, 1832–1898) taught the mathematical subjects students needed to pass the three examinations required for a bachelor's degree. For the second of these examinations, moderations, students who did not select the honours course in mathematics (passmen) were required to know topics in algebra, algebraical (analytic) geometry, trigonometry, and the contents of the first six books of Euclid's *Elements*, which, after 1871, became a primary focus of his instruction. Until then, he also taught subjects required in the honours course: algebra, geometry including conic sections, analytic geometry, and differential calculus.

During this period, from 1855 to 1871, Dodgson published five books and pamphlets on Euclid's geometry, a pamphlet on trigonometry, a book on analytic geometry and one

* Fax: 908 737 3717.
E-mail address: fabeles@kean.edu.

0196-8858/$ – see front matter
doi:10.1016/j.aam.2004.06.006

on linear algebra, as well as three pamphlets on voting theory. He wrote these political pamphlets as an outcome of his considerable involvement with college and university local affairs. But even during this busy time, the teaching duties and professional publications were not enough to satisfy his literary appetite and he wrote the two "Alice" books that made him famous as a novelist.

Throughout his life Dodgson maintained a strong interest in word games, particularly anagrams and acrostics. An anagram creates new words from existing words by changing the order of the letters and word divisions. He followed the 19th century preference for making the anagram descriptive of its subject. Examples are three anagrams of the Liberal Party leader, William Ewart Gladstone: "A wild man will go at trees," "Wild agitator! Means well," "Wilt tear down *all* images?" His anagram for Florence Nightingale is, "Flit on, cheering angel" [6].

An acrostic is a puzzle or a poem in which the first letter of each line spells a word, a name or a phrase. A double acrostic utilizes the last letters of the lines too. Dodgson was an acrostic master. Some of his best are the poem at the end of *Through the Looking Glass* which spells the name of Alice Pleasance Liddell; the dedication (poem) to *The Hunting of the Snark* which not only spells the name, Gertrude Chataway, but also the first word of each stanza suggests the sound of the letter in the name; and the poem appearing at the beginning of *Sylvie and Bruno Concluded* where he uses the *third* letter of each line, rather than the first letter, to spell the name, Enid Stevens. Perhaps his best acrostic is a fifteen stanza connected poem, "A Double Acrostic," composed in 1867 and published in *Phantasmagoria*, to which he did not give a solution. Its third stanza is often quoted:

Yet what are all such gaieties to me
Whose thoughts are full of indices and surds?
$x^2 + 7x + 3$
$= 11/3$ [6].

While a faculty member of Christ Church and after his retirement from teaching in 1881, he incorporated his literary interests into mathematical subjects by fixing his attention on mathematical topics well outside the standard Oxford curriculum. One of these, cryptology, is directly tied to word games, particularly anagrams and acrostics. Both anagrams and acrostics hide information. Anagrams are probably closer in spirit to ciphers than acrostics because the defining ingredient of an anagram is transposition, the changing of the order of a letter, which also defines a transposition cipher system. Currently, the general solution for transposition systems is known as multiple anagramming. Obscuring word divisions is common to both anagrams and ciphers. Acrostics also have the cryptic quality of concealment and Dodgson often hid the names of child friends in them. The use of certain letters to spell out the desired words in an acrostic loosely corresponds to the use of "key" letters or a "keyword" which can specify a cipher alphabet, or the rearrangement of letters in a transposition.

Dodgson derived his pseudonym, Lewis Carroll, as an anagram from a mix of simple cipher techniques, particularly the use of foreign alphabets. Using the Latin form Ludovic of his middle name Lutwidge, then unlatinizing Ludovic to Louis he transposed it to Lewis. Next by first latinizing Charles to Carolus, then unlatinizing it he obtained Carroll.

Dodgson's work on ciphers is not well known. In this paper I discuss his five cipher systems, all of which are substitution systems, in the context of what was known about ciphers during his lifetime and the uses he made of them. From the mid 15th century until the invention of the telegraph, systems of secret code were known as nomenclators, a hybrid of code and cipher. The basic unit of a code system is a word, while that of a cipher is a letter. Generally, cipher systems are of two types: transposition which changes the original letter's order, and substitution (of a letter by another letter or symbol) which changes the original letter's form or value. Dodgson created only substitution systems [7].

2. The Key-Vowel cipher [11]

In 1858, fifteen years after the first electric telegraph opened in England on the Great Western Railway from Paddington west to Slough, Dodgson created the first of his cipher systems, a subset of a simplified (and less secure) form of the Vigenère cipher, a periodic polyalphabetic substitution cipher invented by Blaise de Vigenère in 1585 that arguably was the best known cipher system before the 20th century.

Instead of utilizing the twenty-six available alphabets, just five are used, those lines beginning with Y, Z, A, B, C in Table 1. These are made to correspond with the *key-vowels* A, E, I, O, U. A keyword is required to encode a message using the Vigenère cipher. This word is repeated over the entire message to be enciphered (plaintext). The intersection of the row headed by a letter in the keyword and the column headed by the corresponding letter of the plaintext produces the cipherletter. This encipherment scheme is represented as Key + Plain = Cipher ($K + P = C$).

In this next example, Dodgson chose the keyword, IMAGINE. Using the vowels in the keyword to index the rows, and the letters of the plaintext, COME DIRECTLY to index the columns, we locate the letters of the ciphertext.

Keyword	I	M	A	G	I	N	E	I	M	A	G	I	N	E	I	M	A	G	I	N	E			
Plaintext	C		O		M		E	D		I		R		E	C		T		L		Y		
Ciphertext	C		M		M		D	D		G		R		D	C		R		L		X		

Dodgson padded the ciphertext by adding random letters (nulls). Then knowing that the first vowel of the keyword, "I," is the third vowel in the alphabet, and the second vowel of the keyword, "E," is the second vowel, he completed the ciphertext by placing three

Table 1

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
E	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
I	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	W	Z
O	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
U	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B

random letters at the beginning, and two at the end of the ciphertext in order to obscure word divisions, producing:

L A T C H M E M S D D F G E R X D C O R D L M X D N.

Dodgson believed his cipher system was simple enough to memorize, and unbreakable as long as the keyword was kept secret. But how secure is the keyword? It should be short because the general strategy is to slide the plaintext along the ciphertext (assuming both are available) to locate possible matches while at the same time observing the repetitions of pattern that will reveal the length of the keyword. However, recovering the plaintext from the ciphertext alone was practically impossible in his day.

3. The Matrix cipher [10]

Three days later, Dodgson created what he considered to be a much better cipher, still simple enough to memorize and he believed, unbreakable provided the keyword was not known, but also one he claimed would not permit the discovery of the keyword even if the plaintext were available. Using the letters of the Latin alphabet arranged as a 5×5 matrix he enciphered the word SEND using GROUND as the keyword by mapping from the alphabet to the group $G = Z_5 \times Z_5$.

A F L Q W
B G M R X
C H N S Y
D I O T Z
E K P V $*$

Numbering the rows and columns of the matrix 0 to 4, each letter maps into its column, row pair, e.g., "B" $\to (0, 1)$, "V" $\to (3, 4)$. To encipher "S" $= (3, 2)$ with the keyletter "G" $= (1, 1)$, subtract the keyletter from the plainletter obtaining the cipherletter $(2, 1)$. Continuing, we obtain,

Keyletter	Plainletter	Cipherletter
"G" $= (1, 1)$	"S" $= (3, 2)$	$(2, 1)$
"R" $= (3, 1)$	"E" $= (0, 4)$	$(2, 3)$
"O" $= (2, 3)$	"N" $= (2, 2)$	$(0, 4)$
"U" $= (3, 4)$	"D" $= (0, 3)$	$(2, 2)$

Dodgson wrote this encipherment as 21.23.04.24. The scheme can be represented as Cipher = Plain − Key ($C = P - K$).

To protect the cipher he inserted a pair of parenthesized numbers at the beginning, the first a random number and the second number denoting the *current* position of the keyletter in the encipherment process, e.g., in the encipherment above, (7.11) indicates the eleventh

letter in the repeat of GROUND, i.e., "N." And by inserting a second pair of parenthesized numbers, the first a random number; the second indicating the position of the letter in the keyword, e.g., (1.2) he enabled the encipherment to proceed with an alteration in the repeat of the keyword. Here (7.11)(1.2) means use "R" as the next keyletter rather than "D". Since the weakness of any cipher system that uses a keyword is the periodicity of that word, by addressing this vulnerability he guaranteed his cipher would be unbreakable practically.

He also inserted nulls at the beginning and at the end of the ciphertext to obscure word divisions by following the parenthesized pairs with a letter whose encipherment gives the number of these nulls. In his example, (1.2)Q instructs us to encipher "Q" by "R" giving $(0, 4)$ meaning that no nulls appear at the beginning of the ciphertext, and four nulls are placed at the end. Finally, he asserted that by purposely misspelling words (omitting or adding letters), the recovery of the keyword from the plaintext would be impossible.

His complete encipherment of SEND, beginning with the third letter of the keyword GROUND, and including one null at the beginning and one at the end of the message, as well as several added letters, is:

$$(2.3)(\mathrm{V})10.14.20.00.00.01.33.40.42.40.01.20.23.02$$

This is the first cipher that uses a nonstandard arithmetic, and it is the first cipher system based on a mathematical group. Moreover, it incorporates encipherment instructions within the ciphertext itself, i.e., data and instructions, foreshadowing the notion of a stored program that would come almost a century later. Dodgson did not publish either of these first two ciphers. (They appear only as diary entries.) He made no use of them and did not take up the subject again for another ten years.

4. The Alphabet cipher [3]

In 1868 Dodgson reinvented the complete simplified form of the Vigenère cipher and called it the Alphabet cipher. He made similar claims for it as he did for the ciphers he had created ten years earlier, i.e., the ciphertext cannot be deciphered unless the keyword is known even if the alphabet table (Fig. 1) is available. If the table is unavailable, it can be written again, making this an easily memorized system too. However, Dodgson made no attempt to protect the cipher, not even obscuring word divisions. He used the cipher primarily in letters to child friends.

The next example is one he gave to encipher the message, MEET ME ON TUESDAY EVENING using the keyword, VIGILANCE. Referring to Fig. 1, when the keyword is repeated over the message, the intersection of the row (alternatively, column) headed by a letter in the keyword and the column (alternatively, row) headed by the corresponding letter of the plaintext produces the cipherletter. We see that the ciphertext is produced by Key + Plain = Cipher $(K + P = C)$.

Keyword	V I G I L A N C E V I G I L A N C E
Plaintext	M E E T M E O N T U E S D A Y E V E
Ciphertext	H M K B X E B P X P M Y L L Y R X I

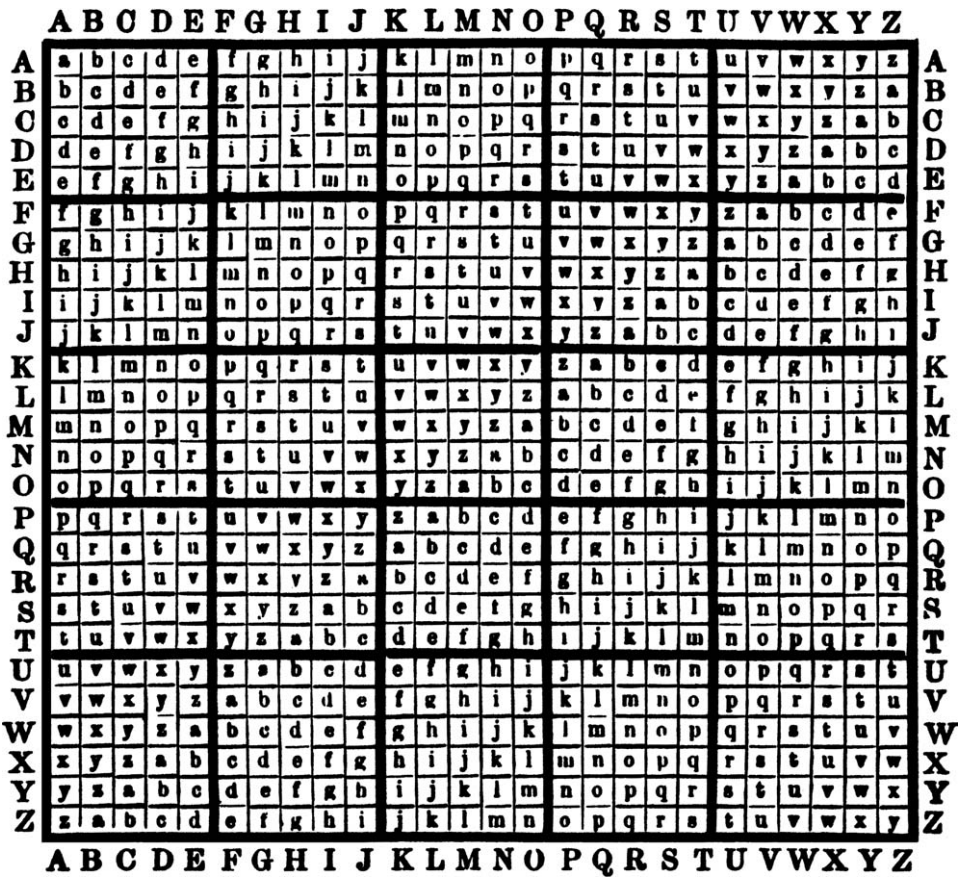

Fig. 1. The Alphabet cipher. Originally printed on a card measuring 7 and $1/8''$ by 4 and $15/16''$ with the tableau on the recto side and the explanation on the verso side. Undated and anonymous, it was probably completed in April 1868, almost certainly by Dodgson. Courtesy: Bodleian Library, Oxford University.

Note that the same plainletter can produce different cipherletters because the cipher alphabet is translated to the left of the plain alphabet the number of places determined by the keyletter. For example, when the letter "D" is repeatedly used to encode the entire plain alphabet, we observe that the cipherletter is three letters to the right of the plainletter ($C = P + 3$).

Keyletter	D	D	D	D	D
	0	1	2	3	4
Plainletter	A	B	C	D	E
	3	4	5	6	7
Cipherletter	D	E	F	G	H

5. The Telegraph cipher [3]

In the same year, on 22 April, Dodgson invented another cipher that he would use in letters to communicate with child friends. Soon after he created it, he composed the piece, "Cipher-Poem," using the keyword, FOX. His system employed two sliding alphabets, one for keyletters, the key-alphabet; the other for the plaintext, the message-alphabet. Other then stating that the keyword (or key sentence) had to be kept secret, Dodgson made no claims about the security of the cipher, nor did he add embellishments that would obscure normal word divisions.

Key-alphabet	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Message-alphabet	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A

The method is this: find the keyletter on the key-alphabet, then slide the message-alphabet under it so that the letter of the plaintext appears under the keyletter. Then using the appropriate "A" on the message-alphabet as an index, the cipherletter appears on the key-alphabet above that "A". The result is a Beaufort enciphered message, named for the retired British Royal Navy Admiral Sir Francis Beaufort who had reinvented this cipher, first proposed by Giovanni Sestri (1710), probably in 1857 [4].

In this next example by Dodgson, the message, MEET ME AT SIX is enciphered using the keyword, WAR.

Keyword	W A R W A R W A R W A
Plaintext	M E E T M E A T S I X
Ciphertext	K W N D O N W H Z O D

We can use the Vigenère tableau (Fig. 1) to simulate the Beaufort encipherment. To encipher the plainletter "M" using the keyletter "W", we enter the table at row M, continuing in that row to the keyletter "W." The letter at the head of the W's column gives the cipherletter "K". We represent this encipherment as Cipher = Key − Plain ($C = K - P$). Note that like the Alphabet cipher, the same plainletter can produce a different cipherletter as the diagram below shows.

Keyletter	D D D D D
	0 1 2 3 4
Plainletter	A B C D E
	3 2 1 0 25
Cipherletter	D C B A Z

The cipher alphabet is a reversed alphabet and the cipherletter is three letters to the left of the plainletter ($C = P - 3$), e.g., $C = B - 3$ ($-2 = 1 - 3$).

The last of the main 19th century polyalphabetic ciphers is derived from the Beaufort and named the Variant Beaufort. Its encipherment is given by $C = P - K$. Comparing this encipherment scheme to the Vigenère *decipherment* process, $P = C - K$, we see that each

of these is the inverse of the other. Using the Vigenère tableau (Fig. 1) to simulate a Variant Beaufort encipherment, we observe that the Matrix cipher is a Variant Beaufort system.

It is entirely possible that Dodgson knew about Beaufort's work which was well known at the time, but he does not mention it. Dodgson communicated his own invention to George Ward Hunt, then Chancellor of the Exchequer, formerly First Lord of the Admiralty, at dinner on 24 April 1868. There is no record of a response.

Although Dodgson believed his ciphers to be unbreakable, this was not the case. In the 19th century, few people knew of the existence of the book, *Die Geheimschriften und die Dechiffrir-kunst*, published in Berlin in 1863 in which its author, Friedrich W. Kasiski, gave the first general solution to polyalphabetic ciphers with repeating keywords. His solution is based on the observation that if there is both a (true, not accidental) repetition of part of the key and of the plaintext, then there also is a repetition of part of the ciphertext. The length of the keyword can then be determined by analyzing the intervals between the repetitions. Knowing how long the keyword is gives the number of alphabets used in the encipherment which allows the letters of the enciphered message to be sorted into sets of cipherletters sorted by the first keyletter, by the second keyletter, and so on. Each of these sets constitutes a monoalphabetic substitution cipher which then can be more easily solved [8].

6. The *Memoria Technica* cipher [1]

Dodgson's final cipher system, one that he did not refer to as a cipher, but used it as one, is a variant of scheme created by Richard Grey in the 18th century as an *aide de memoire* for numerical data. Dodgson's interest in Grey's system was motivated by his own difficulty remembering dates. It evolved into an unusual method for not only remembering dates, but also the digits of π and e, and certain logarithms that would enable the user to obtain the logarithm of any number.

To remember a date, Dodgson creates a single word, a line, a rhymed couplet or a short verse composed of rhymed couplets in which the *consonants* encoding the date are those (underlined) in words at the *end* of the line. He chose the end of the line so that the user would also remember the rhyme structure which is given at the end of lines so that the rhyme itself can be enlisted to remember the words containing the significant consonants.

As an example, to remember the date Cromwell was made Protector, 1653, Dodgson wrote the couplet:

Ambition was thy fault:
Thine own self to e<u>x</u>al<u>t</u>.

The integers: 6, 5, 3 (1 being understood) are encipered by the letters: "x", "l", "t", using the scheme below.

1	2	3	4	5	6	7	8	9	0
b	d	t	f	l	s	p	h	n	z
c	w	j	qu	v	x	m	k	g	r

Working with his physics colleague, Robert Edward Baynes (1849–1921), Dodgson created his version of *Memoria Technica* in 1875 to remember logarithms (mantissas only) using a method Baynes had constructed. Dodgson determined that just twenty-six logarithms had to be remembered to obtain the logarithm of any number correct to seven places without using tables: the 26 logs of the primes less than 20, the numbers between 101 and 109, and those between 1001 and 1009. (In [1, p. 222, line 8], insert "prime" before "numbers." On line 10, substitute "26" for "2^6".) For example, to remember the logarithm of $106 = 0.0253059$, with the leading 0 understood, he composed this verse,

Six months I have travelled unshaven,
That's exactly one half of a year:
I have changed from a dove to a raven –
But I will not be shaved, even here!

Using the scheme above, we have the encoding of 2 5 3 0 5 9 by d v t r v n.

Both Baynes and Dodgson were able to calculate logarithms and antilogarithms rapidly; Baynes in four minutes, Dodgson averaging between five and eight minutes. But Dodgson went further and was able to calculate the seventh root of 123454321, the value of π^π in fourteen minutes, the first eight digits of the tenth power of 237541 in thirteen minutes, and the thirteenth root of 87654327 in nine minutes. Except for the first, each result is correct to four or five decimal places. These rapid calculations were extraordinary computational feats at the time. Here is Dodgson's calculation of π^π using Baynes' method. Decimal points are omitted [5].

- Divide $\pi = 3141592653$ by its first digit, 3, whose logarithm (mantissa) is the first factor.
- Divide the result from the first step, 1047197551, by its first three digits to produce the third factor, the mantissa of the log of 104. (Omit division by the first two digits since this number is 10.)
- Divide the result from the previous step, 10069207, by its first four digits to produce the fourth factor, the mantissa of the log of 1006.
- For the fifth (last) factor, since logarithms of successive numbers between 10000 and 10010 differ by an average of .00004341, take the excess over 10000 of the result from the previous step, 1000914, (9.14) and multiply it by this average number, giving .0003967.
- Adding the fifth factor and from memory, the logarithms (seven place mantissas) of 1006, 104 and 3 which are .0025980, .0170333, .4771213, respectively, Dodgson obtained .4971493 as the logarithm of π. (Using mantissas given by an HP calculator, the value of π to seven places is .4971493.)

Dodgson obtained the antilogarithm of $\pi \log \pi$, 1.56183926943 (he used 3.1415900 as the value of π), using the inverse of Baynes' method and the mantissas of logarithms he had memorized.

- Subtract from the decimal part of 1.56183926943 the closest mantissa of the logarithm of a number between 1 and 10, .4771213, which is the log of 3. So the first factor is 3.
- Subtract from the difference in the first step, .0847180, the closest mantissa of the logarithm of a number between 10 and 20, .0791813, which is the log of 12. So the second factor is 12.
- Subtract from the difference in the second step, .0055367, the closest mantissa of the logarithm of a number between 100 and 110, .0043214, which is the log of 101. So the third factor is 101.
- Subtract from the difference in the third step, .0012153, the closest mantissa of the logarithm of a number between 1000 and 1010, .0008677, which is the log of 1002.
- Divide the difference in the fourth step, .0003476, by .00004341 which gives the excess of the fifth (last) factor over 10000. This excess is 8.007, so the fifth factor is 10008.
- Multiplying all the factors, 3, 12, 101, 1002, 10008, Dodgson inexplicably made an error and obtained 36.1008 as the final result. (An HP calculator gives 36.4619.)

In 1878, Dodgson made several improvements to Baynes' method so that from a modern point of view it is an algorithm that a computer can execute.

Memoria Technica shares several characteristics with the previous four ciphers. First, all of them are schemes that are easily remembered. The first four use a keyword or a key sentence; *Memoria Technica* uses just keyletters. For example, the letters "s" and "x" are associated with the integer 6. If 6 is part of a number to be remembered, and if s is the keyletter, 6 is enciphered as "x". Similarly, 6 can be enciphered as "s" if "x" is chosen as the keyletter. Unlike the earlier ciphers where different cipherletters can result from the same plainletter, each integer can be enciphered in just one way, depending on the choice of keyletter. But for creating the *words* containing these consonants, the 2^n combinations of the consonants for an n digit number is certainly enough.

Like the Key-Vowel and Matrix ciphers, *Memoria Technica* has the embellishments of letters added, but these letters create the *real* words that are the ingredients of the verse. Unlike nulls, these are meaningful symbols that are essential to the purpose of the *Memoria Technica* cipher: remembering, not hiding the numerical plaintext. Just as nulls disguise a ciphertext, varying the placement of the lines in the verse that hold the consonants enciphering the integers is a form of disguise that conveys a sense of playfulness.

Curiously, the Key-Vowel cipher, where vowels encipher the plaintext and where random consonants are used to pad the ciphertext, can be considered an opposite of the *Memoria Technica* cipher which uses only consonants to encipher the numerical plaintext and then pads the rest of the ciphertext, i.e., the word, rhyme or verse, with nonrandom letters.

Dodgson used his *Memoria Technica* cipher in letters to friends, and as a tool for teaching memory aids to students in several local schools, an activity he began in the spring of 1887. In September 1891, he invented what he called a Nyctograph, a sixteen square cutout cardboard grid. He often wanted to make written notes at night when he was unable to sleep. To make this activity less difficult at a time when candles had to be lit to provide light, he created a scheme whereby he could remain in bed and write. It consisted of a "square alphabet" for writing letters, For example, he represented the letter "A" by its

right-hand side, and the letter "B" by its vertical line and dots standing for the semicircles. For writing numbers, he used an abbreviated form of his *Memoria Technica*, assigning just one of the consonants to each integer. He also used just "q" instead of "qu" for the encipherment of "4," thereby having only consonants in the table, a revision he had made earlier to be more consistent with a cipher system [6].

The cipher made an appearance in an unpublished piece, probably written in 1896–1897, that Dodgson intended as a chapter of an unfinished book on games and puzzles titled, "Other Mental Recreations." This piece, "Rule for Finding Easter-Day for any Date till A.D. 2499," is a version of Carl F. Gauss's rule published in 1800. Dodgson succeeded in simplifying the rule so that a result required about half a minute of mental calculation. He claimed that someone using his rule might forget the date being working on and so he offered his *Memoria Technica* cipher to remember that date. The rule employs a table (below) that Dodgson called the *ah*-Table [2].

No. of hundreds in date	15	16	17	18	19	20	21	22	23	24
Value of *a*	8	8	7	7	6	6	6	5	4	5
Value of *h*	2	2	3	4	5	5	6	0	1	1

He also used the cipher to remember the last four columns of the table where the values of *a* and *h* are enciphered in the third and fourth lines of:

List my song to!
'Tis as wrong to
Save a flea
As rob a bee [2].

The values of *a* and *h* (from the *Memoria Technica* table) are:

$$\begin{matrix} 6\,5\,4\,5 \\ s\ v\ f\ l \end{matrix} \quad \text{and} \quad \begin{matrix} 6\,0\,1\,1 \\ s\ r\ b\ b \end{matrix}$$

(The first four columns of the *ah*-Table are easily remembered from numerical patterns.)

Dodgson worked on his *Memoria Technica* cipher at the same time he was writing his famous poem, *The Hunting of the Snark*, composed entirely of 141 rhymed four line stanzas like those of his cipher. It appeared early in 1876. (Unlike the reception of his two "Alice" books, the reviews of "Snark" were not good.)

7. Conclusion

From the outset of his academic career Dodgson created ciphers, revising the last one in 1888. He based his constructions on the three cipher paradigms of his time: Vigenère, Beaufort, and Variant Beaufort. He continued to create anagrams, and acrostics well into the 1890s, employing variations inspired by his ciphers, such as varying the location of

the "key" letters in acrostic poems. Together these ciphers, anagrams, acrostics and poems represent one of the closest associations of his mathematical-literary interests.

After 1875 the nature of his cipher work changed. He created the first two ciphers, Key-Vowel and Matrix, to be suitable for military and diplomatic purposes, and from a practical viewpoint, they were unbreakable systems. The Alphabet and Telegraph ciphers appeared after the publication of *Alice in Wonderland*. These ciphers were simpler to use, well constructed and secure by the standards of his time for ordinary telegrams and mailed postcards. Twenty five years after Dodgson had created his first two ciphers, Auguste Kerckhoffs established the basic requirements for secure military ciphers transmitted by telegraph. These were: the system should be unbreakable in practice; the key should be easily remembered and changeable; the system should be simple, and not involve a long or difficult list of rules [9]. Dodgson's ciphers of 1858 and 1868 certainly meet these standards. The *Memoria Technica* cipher was his most literary cipher, but one that broke with secure ciphers. However, he used it in conjunction with his mathematical work more than any of his earlier cipher systems.

References

[1] F. Abeles, The Memoria Technica Cipher, Cryptologia xxvii (2003) 217–229.
[2] F. Abeles, The Mathematical Pamphlets of Charles Lutwidge Dodgson and Related Pieces, LCSNA–University Press of Virginia, New York–Charlottesville, 1994.
[3] F. Abeles, S.H. Lipson, Some Victorian periodic polyalphabetic ciphers, in: C.A. Deavours, et al. (Eds.), Selections from Cryptologia, Artech House, Norwood, MA, 1998, pp. 309–315.
[4] F. Beaufort, Cryptography. A System of Secret Writing by the late Admiral Sir Francis Beaufort, K.C.B., adapted for telegrams and postcards (Card), London, Edward Sanford, n.d.
[5] C.L. Dodgson, Packet 60, items 1, 2, 3. The Mathematical Manuscripts of Charles Lutwidge Dodgson, Morris L. Parrish Collection, Department of Rare Books and Special Collections, Princeton University Library, Princeton, NJ.
[6] J. Fisher (Ed.), The Magic of Lewis Carroll, Simon and Schuster, New York, 1973.
[7] D. Kahn, The Codebreakers, Macmillan, New York, 1967.
[8] F.W. Kasiski, Die Geheimschriften und die Dechiffrir-kunst, Mittler & Sohn, Berlin, 1863.
[9] A. Kerckhoffs, La Cryptographie Militaire, L. Baudoin & Cie, Paris, 1883.
[10] S.H. Lipson, F. Abeles, The Matrix Cipher of C.L. Dodgson, Cryptologia xiv (1990) 28–36.
[11] S.H. Lipson, F. Abeles, The Key-Vowel Cipher of Charles L. Dodgson, in: C.A. Deavours, et al. (Eds.), Selections from Cryptologia, Artech House, Norwood, MA, 1998, pp. 323–329.