THE ALICE CIPHER

ASHLEY DALE
New Palestine, Indiana

Lewis Carroll loved ciphers. Between 1858 and 1868 he invented four and recorded them in his diary: two matrix ciphers and two polyalphabetic ciphers: the Telegraph Cipher and the Alphabet Cipher. He submitted the latter two for publication, and personally used them to write letters to his child friends.

It is possible to view Carroll's novel *Through the Looking-Glass and What Alice Found There* as Carroll's fifth cipher. The plot follows Alice across a chess board in her journey to become a queen, and Carroll helpfully provides a chess board with pieces placed on it and a list of chess moves at the beginning of the book. The story, board, list of moves, and Martin Gardner's annotations comprise the elements necessary to a cipher: a plaintext, a key, and a ciphertext.

Cipher Basics

A **plaintext** is the original message being sent. A classic, military-esque example would be "ATTACK AT DAWN." In order to prevent unintended recipients from reading this message, the plaintext is encrypted using a key which transforms the letters into something unreadable e.g. BUUBDLBUEBXO. In *Through the Looking-Glass,* the plaintext can be found in the starting chess board placed at the beginning of the book.

A **cipher key** is the method used to encode a plaintext and decode a ciphertext. In the simplest of substitution ciphers, the key is nothing more than a shift in the alphabet where A=B, B=C, C=D, and so on; resulting in a chart which looks like this:

ABCDEFGHIJKLMNOPQRSTUVWXYZ
BCDEFGHIJKLMNOPQRSTUVWXYZA

This cipher, known as the Caesar Cipher, is easy to both use and break. To add security to messages, steps are added to the key, and in more complicated ciphers, the key can consist of multiple steps involving key phrases, modular arithmetic, and so on.

In *Through the Looking-Glass,* the key may be found in the list of moves beneath the chess board and in Gardner's annotations. The first is the process which turns the chess board into a story. The second helps provide necessary knowledge of how to interpret the moves, i.e. what happens where and when. Together, the moves and annotations relate the story to the chess board; which is what a key does for a plaintext and a ciphertext.

Finally, the **ciphertext** in *Through the Looking Glass* is the story itself. While the story contains elements of chess in the characters and references, the actual plot only vaguely resembles a game of chess. This partly due to Carroll's artistic license with traditional chess rules, but this is also because Carroll translated the chess board into the Looking-Glass world. One example of this is when Alice-the-chess-pawn moves forward one square on the chess board, Alice-in-the-story crosses a stream.

Having identified the elements of a cipher in Carroll's novel, my goal was to combine it with elements of his other ciphers to create a new, Alice themed cipher.

Carroll's Ciphers

Carroll's formal ciphers, outlined in two papers published by Francine Ables and Stanley H. Lipson, consist of two polyalphabetic ciphers and two matrix ciphers.

The first of Carroll's polyalphabetic ciphers, which he named "The Alphabet Cipher," is a kind of Vigenère cipher, and uses the following table:

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

Polyalphabetic Cipher Table

To use a Vigenère cipher, a key word is used (e.g. ALICE) and is then repeated over the plaintext:

Key: A L I C E A L I C E A L
Plain: A T T A C K A T D A W N

To encrypt the first letter of the plaintext, an A, find the column for the key phrase letter 'A' in 'ALICE' on the top of the grid and the row for the plaintext letter A in 'ATTACK' on the left side of the grid. The intersection of the two 'A's is A, which means that the first letter of the ciphertext is 'A'.

The second letter of the plaintext is T. The second letter of the key phrase is L. The L column and T row intersect at E. Therefore, the second letter of the encrypted phrase is E.

The entire plaintext ATTACKATDAWN encoded with key word ALICE is AEBCGKLBFEWY.

To decipher, the letter of the key phrase becomes the column, the letter of the ciphertext becomes the intersection, and the plaintext is the letter of the row.

The second of Carroll's polyalphabetic ciphers, called "The Telegraph Cipher," is a kind of Beaufort Cipher. It uses the same table as a Vigenère Cipher, but is applied differently. Rather than starting from the top column and left row and finding the encrypted letter where the column and row intersect, a Beaufort cipher begins with the key letter as the top column, travels down the column until the plaintext letter is found, then travels left out of the row and is enciphered as the letter of the row. In short, it is the same process as the decryption of the previous cipher.

Using the same key phrase 'ALICE' and the same plaintext 'ATTACKATDAWN' with a Beaufort Cipher yields a ciphertext of AILXYKPLBWWC.

To decode, the key phrase letter is the column, the ciphertext letter is the row, and the plaintext letter is the intersection.

Carroll's matrix ciphers use the following table:

	0	1	2	3	4
0	A	F	L	Q	W
1	B	G	M	R	X
2	C	H	N	S	Y
3	D	I	O	T	Z
4	E	K	P	V	*

Matrix Cipher Table

This matrix uses the Latin alphabet, which means that I and J are substituted for each other, as are V and U. The asterisk fills in the remaining space to create an even grid of 5x5. Each letter is assigned a two digit numerical value of (column, row) so that the letters of our key phrase become A=(00), L=(20), I=(13), C=(02), and E=(04): 00.20.13.02.04.

In the first of Carroll's matrix ciphers, the distance is measured between the key phrase letter and the plaintext letter, and that distance becomes the new ciphertext letter. For example, the first key phrase letter is A, the first plaintext letter is A, and A is 0 rows and 0 columns away from A, so the first letter/number of the ciphertext is A=00. The second key phrase letter is L. The second plaintext letter is T. T is 1 column and 3 rows away from L, so the second letter/number is I=13.

Using this method, the plaintext 'ATTACKATDAWN' with key phrase 'ALICE' is encoded as AILQQXQLBFWC or as 00.13.02.03.03.14.03.02.01.10.40.02.

To decode, use the letter of the key phrase, then add the distance (the double digit number in the ciphertext) and you have the plaintext letter again. So L is 0 columns away and 2 rows up from the N at the end of DAWN.

The second matrix cipher uses the same matrix table, but a different method of encryption. 'ALICE' is still equivalent to 00.20.13.02.04, but this time the plaintext is also converted into numerical terms using the same method: 00.33.33.11.02.14.00.33.03.00.40.22. To convert the plaintext to ciphertext using a key, the value of the key phrase letter is subtracted from the value of the plaintext letter:

00.33.33.11.02.14.00.33.03.00.40.22.
-00.20.13.02.04.00.20.13.02.04.00.20.
00.13.20.14.03.00.30.20.01.10.40.02.

To decode, the ciphertext is added to the key phrase; the reverse process.

It is important to note that the math taking place is modular, specifically mod4. I find it helpful to think of the graph as wrapping around, with the bottom edge meeting the top edge and the left edge meeting the right edge. When converting from letters to numbers, numbers to letters, or measuring the distance from one letter to another (in the first cipher), we always move *down* the column and across the row from *left to right*. When we run out of numbers, we start again at the *top* of the column and the *left side* of the row. This is the equivalent of adding: always going forward, top to bottom, left to right.

However, in the second matrix cipher, the numbers are subtracted. To subtract using the matrix, columns are traveled *bottom to top* and rows are traveled *right to left*. In short, we are going backwards on the graph. So to subtract 04 from 02, find 02 on the grid then travel 0 columns *left* and four rows *up*.

Application to *Through The Looking Glass*

The cipher used in *Through the Looking Glass* contains structural elements similar to all of Carroll's four ciphers. When compared to the two matrix ciphers, the chess board itself is easily recognizable as a kind of matrix, and instead of moving according to mod4 addition and subtraction, Carroll provides a series of chess moves to guide us around the board. When compared to the polyalphabetic ciphers, the chess board can serve as the table of shifted alphabets.

Using these recognizable elements, I created the following table:

	0	1	2	3	4	5	6	7
0	'Twas	Shoes	Days	As	The	As	I	Sent
1	Digs	Message	Gimble	Go	By	Ships	Slithy	To
2	Mimsy	Told	Cabbages	The	Fish	Wabe	Were	Wish
3	Summers	Did	Lie	Dreaming	Kings	Dreaming	Lion	A
4	All	Mome	They	Wonderland	Unicorn	Some	Borogroves	Bread
5	Seas	Gave	Outgrabe	Down	Brillig	White	Die	Fighting
6	Plum Cake	And	Gyre	In	Raths	Brown	Boiling	Wings
7	Evening	That	Gate	Sitting	Hot	Crown	Toves	Long

Alice Cipher Matrix

Rather than the 26x26 grid of the polyalphabetic cipher, or the 5x5 grid of the matrix cipher, I have used the 8x8 grid of the chess board Carroll provided at the beginning of the book, and labeled it using mod7.

Also, rather than using a repeated or modified alphabet, I have chosen to fill my matrix with words used in various poems throughout the book. This is a reasonable choice because my matrix still contains the necessary information for a key phrase, plaintext, and ciphertext. Also, while decreasing the amount of safety offered by the anonymity of the alphabet, I have decreased the amount of time necessary to code/decode a ciphertext to something more suitable for a class period.

For my key phrase I have chosen the line 'THAT SUMMERS EVENING LONG A-GO', a slight variation on the second to last line of the White Knight's poem found in Chapter 8. For my plaintext I have chosen the sixth verse of the poem which ends the book:

In a Wonderland they lie,
Dreaming as the days go by,
Dreaming as the summers die:

To encode using Carroll's original algorithm (the list of chess moves) I have combined moves where the chess board remains static, and made the amended list of moves read as follows:

1. Alice meets R.Q.
2. R.Q. to K.R's 4th
3. Alice through Q's 3rd (*by railway*) to Q's 4th (*Tweedledum and Tweedledee*)
4. W.Q. to Q.B's 4th; Alice meets W.Q
5. W.Q. to Q.B's 5th (*becomes sheep*)
6. Alice to Q's 5th (*shop, river, shop*)
7. W.Q. to K. B's 8th (*leaves egg on shelf*)
8. Alice to Q's 6th (*Humpty Dumpty*)
9. W.Q. to Q.B's 8th (*flying from R. Kt.*)
10. Alice to Q's 7th (*forest*)
11. R. Kt. to K's 2nd (ch.)
12. W. Kt. takes R. Kt.; W. Kt. to K. B's 5th
13. Alice to Q's 8th (*coronation*)
14. R.Q. to K's sq. (*examination*); Alice becomes Queen; Queen's castle; Alice Castles (*feast*)
15. W.Q. to Q.R's 6th (*soup*)
16. Alice takes R.Q. & wins

When encoded using mod7 coordinates, the squares where each move ends read as follows:

36.73.34.24.23.33.50.32.20.31.41.53.30.40.03.65.

This is not strictly equivalent to the Beaufort and Vigenère ciphers because the algorithm also doubles as the key phrase. However, because the input-output of the system has the same straightforward characteristics of those two ciphers, actually using the list of chess moves to encode/decode feels fairly similar to using the Beaufort and Vigenère ciphers.

Carroll's matrix ciphers may be applied on the Alice Cipher Matrix without modification of either. The key phrase is encrypted as follows:

17.03.07.77.73.31.

Using Carroll's first matrix cipher to measure the distance between the key phrase and the plaintext yields the following ciphertext:

26.70.35.43.30.02.41.73.21.42.56.22.21.45.04.76.

Converted to words, the ciphertext reads as follows:

GYRE SENT TOWN KINGS AS MIMSY BY A GIMBLE FISH BROWN CABBAGES GIMBLE BRILLIG ALL WINGS

Using Carroll's second matrix cipher of key phrase-plaintext=ciphertext yields the following:

71.10.53.53.50.06.47.51.67.46.32.66.67.43.04.12.

Converted to words, the ciphertext reads:

TO SHOES DREAMING DREAMING AS PLUM-CAKE HOT SHIPS TOVES RATHS THE BOILING TOVES KINGS ALL TOLD

Any combination of words could be used in the matrix. Of course, the words themselves will give a connotation of the general subject of the plaintext, as demonstrated by the easily identifiable words "mimsy," "slithy," and "brillig" which denote work by or relating to Lewis Carroll.

References

Abeles, F. & Lipson, S. H. (1990). The Matrix Cipher of C. L. Dodgson. *Cryptologia, XIV (1),* 28-36.

Abeles, F. & Lipson, S. H. (1990). Some Victorian Periodic Polyalphabetic Ciphers. *Cryptologia, XIV (2),* 128-134.

Beaufort Cipher. (n.d.). In *Wikipedia.* Retrieved April 22, 2013 from http://en.wikipedia.org/wiki/Beaufort_cipher

Carroll, L. (2000). *The Annotated Alice: The Definitive Edition* (Gardner, M., Ed.). New York, NY: W.W. Norton & Company, Inc.

Modular Arithmetic. (n.d.). In *Wikipedia.* Retrieved April 22, 2013 from http://en.wikipedia.org/wiki/Modular_arithmetic

Vigenère Cipher. (n.d.). In *Wikipedia.* Retrieved April 22, 2013 from http://en.wikipedia.org/wiki/Vigenère_cipher