Vigenère Cipher

In a Caesar cipher, each letter of the alphabet is shifted along some number of places; for example, in a Caesar cipher of shift 3, A would become D, B would become E, Y would become B and so on. The Vigenère cipher consists of several Caesar ciphers in sequence with different shift values.

To encrypt, a table of alphabets can be used, termed a *tabula recta*, *Vigenère square*, or *Vigenère table*. It consists of the alphabet written out 26 times in different rows, each alphabet shifted cyclically to the left compared to the previous alphabet, corresponding to the 26 possible Caesar ciphers. At different points in the encryption process, the cipher uses a different alphabet from one of the rows. The alphabet used at each point depends on a repeating keyword.

For example, suppose that the plaintext to be encrypted is:

```
ATTACKATDAWN
```

The person sending the message chooses a keyword and repeats it until it matches the length of the plaintext, for example, the keyword "LEMON":

```
LEMONLEMONLE
```

Each row starts with a key letter. The remainder of the row holds the letters A to Z (in shifted order). Although there are 26 key rows shown, you will only use as many keys (different alphabets) as there are unique letters in the key string, here just 5 keys, {L, E, M, O, N}. For successive letters of the message, we are going to take successive letters of the key string, and encipher each message letter using its corresponding key row. Choose the next letter of the key, go along that row to find the column heading that matches the message character; the letter at the intersection of [key-row, msg-col] is the enciphered letter.

For example, the first letter of the plaintext, A, is paired with L, the first letter of the key. So use row L and column A of the Vigenère square, namely L. Similarly, for the second letter of the plaintext, the second letter of the key is used; the letter at row E and column T is X. The rest of the plaintext is enciphered in a similar fashion:

Plaintext: ATTACKATDAWN
Key: LEMONLEMONLE
Ciphertext: LXFOPVEFRNHR

Decryption is performed by going to the row in the table corresponding to the key, finding the position of the ciphertext letter in this row, and then using the column's label as the plaintext. For example, in row L (from *L*EMON), the ciphertext L appears in column A, which is the first plaintext letter. Next we go to row E (from L*E*MON), locate the ciphertext X which is found in column T, thus T is the second plaintext letter.

(This text is from Wikipedia)

Name _____ **Date**_____

Chapter 7: Combining Caesar Ciphers
(Text pages 56–57)

1. Encrypt using a Vigenère cipher with keyword DOG.

keyword:																								
plaintext:	h	i	d	d	e	n		t	r	e	a	s	u	r	e									
ciphertext:																								

2. Encrypt using a Vigenère cipher with keyword CAT.

M	e	e	t		m	e		t	o	n	i	g	h	t		a	t							

m	i	d	n	i	g	h	t																	

Return to Text

3. Decrypt using a Vigenère cipher with keyword CAT.

Q	K,		U	W	T		P	J	E	K	G		S	A	C	L	E		Y	E		F	G	E	M?

4. Decrypt using a Vigenère cipher with keyword LIE.

L		T	M	P		K	E	Y		B	V	L	D	I	W		P	E	W	N	A	L	G		

E	C	W	Y	Y	L		X	S	M		A	Z	Z	P	O		E	L	T	T	I		E	P	I

E	Z	Y	E	P		M	D		X	Y	E	B	M	Y	O		S	Y		Q	X	D			

A	L	Z	M	W.																				

—Mark Twain

Name _____ **Date**_____

(Text page 58)

5. Use the Vigenère square—not a cipher wheel—to finish encrypting:

D	O	G		D	O	G	D	O	G		D	O	G	D	O	G	D	O	G	D	O				
t	o	p		s	e	c	r	e	t		i	n	f	o	r	m	a	t	i	o	n				
W	C																								

6. Use the Vigenère square to decrypt the following. (Keyword: BLUE)

X	S	C	G	I		X	Y	X	I	Z	X		H	P		J	I	Y		M	T	E	I		

C	P	M	X?																						

7. Use either the cipher-wheel method or the Vigenère-square method to decrypt the following quotations from author Mark Twain.

   a. Keyword: SELF

S		T	P	W	K	S	Y		H	S	R	Y	T	L		F	P								

H	G	Q	Q	T	J	X	L	G	D	I		H	N	L	L	Z	Z	L		L	T	X			

G	A	Y		F	H	T	C	T	N	E	W.														

   b. Keyword: READ

S	I		C	D	I	I	F	X	C		E	B	R	L	X		R	H	R	H	I	Q	X		

L	E	D	C	X	H		E	F	S	K	V.		P	S	U		P	R	C		D	L	V		

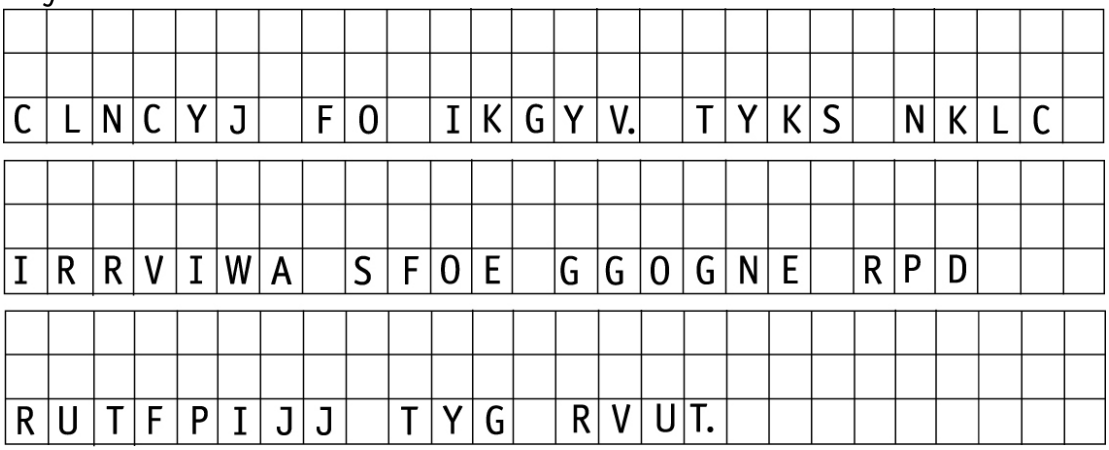
S	F		D		D	M	S	S	I	M	N	W.													

Name _____ **Date**_____

(Text page 59)

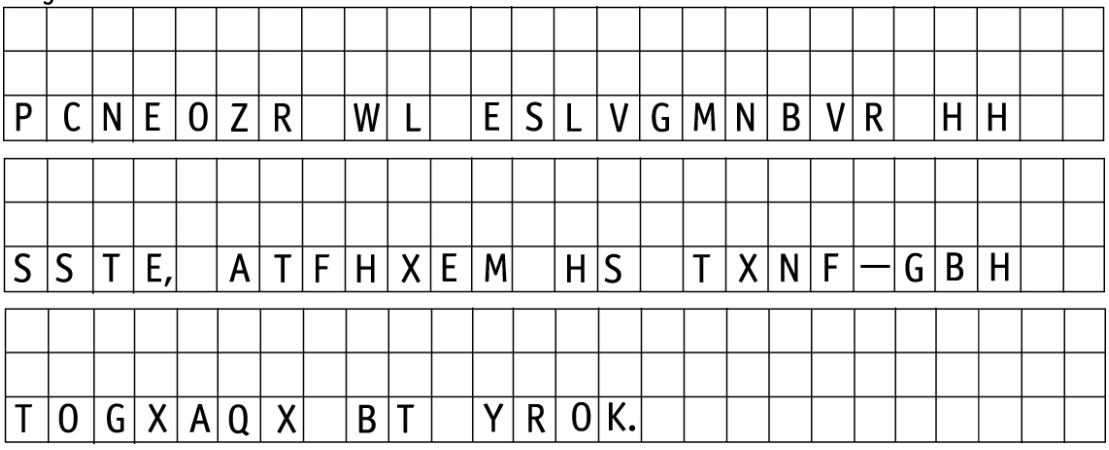
8. Use either the cipher-wheel method or the Vigenère-square method to decrypt the following quotes from Mark Twain.

   a. Keyword: CAR



   b. Keyword: TWAIN

   c. Keyword: NOT

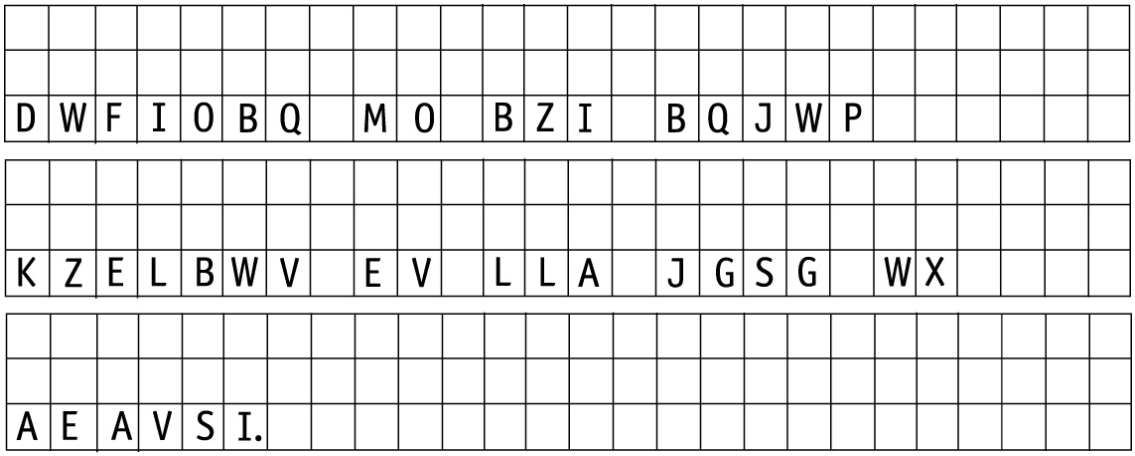


Name _____ **Date**_____

(Text page 60)

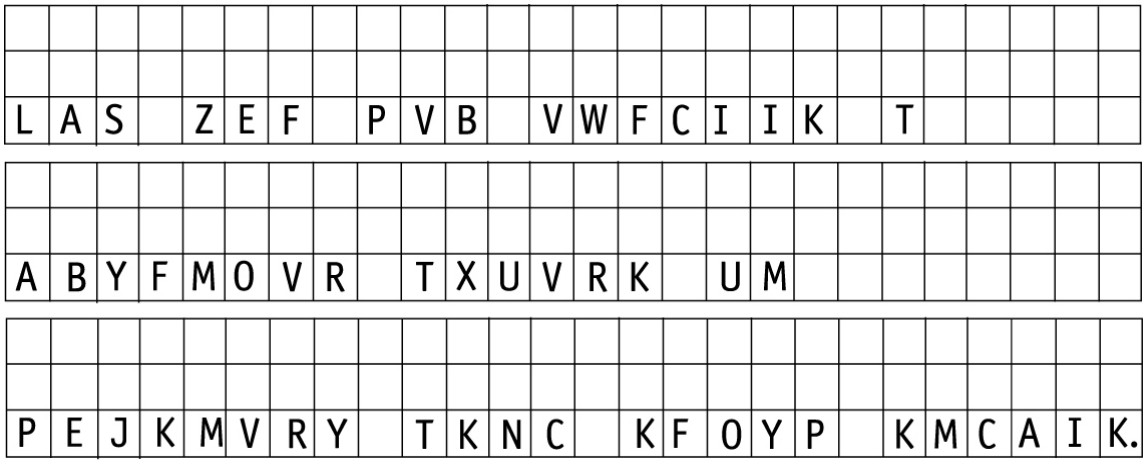
9. Use either the cipher-wheel method or the Vigenère-square method to decrypt the following quotations.

a. Keyword: WISE



—Thomas Jefferson

b. Keyword: STONE

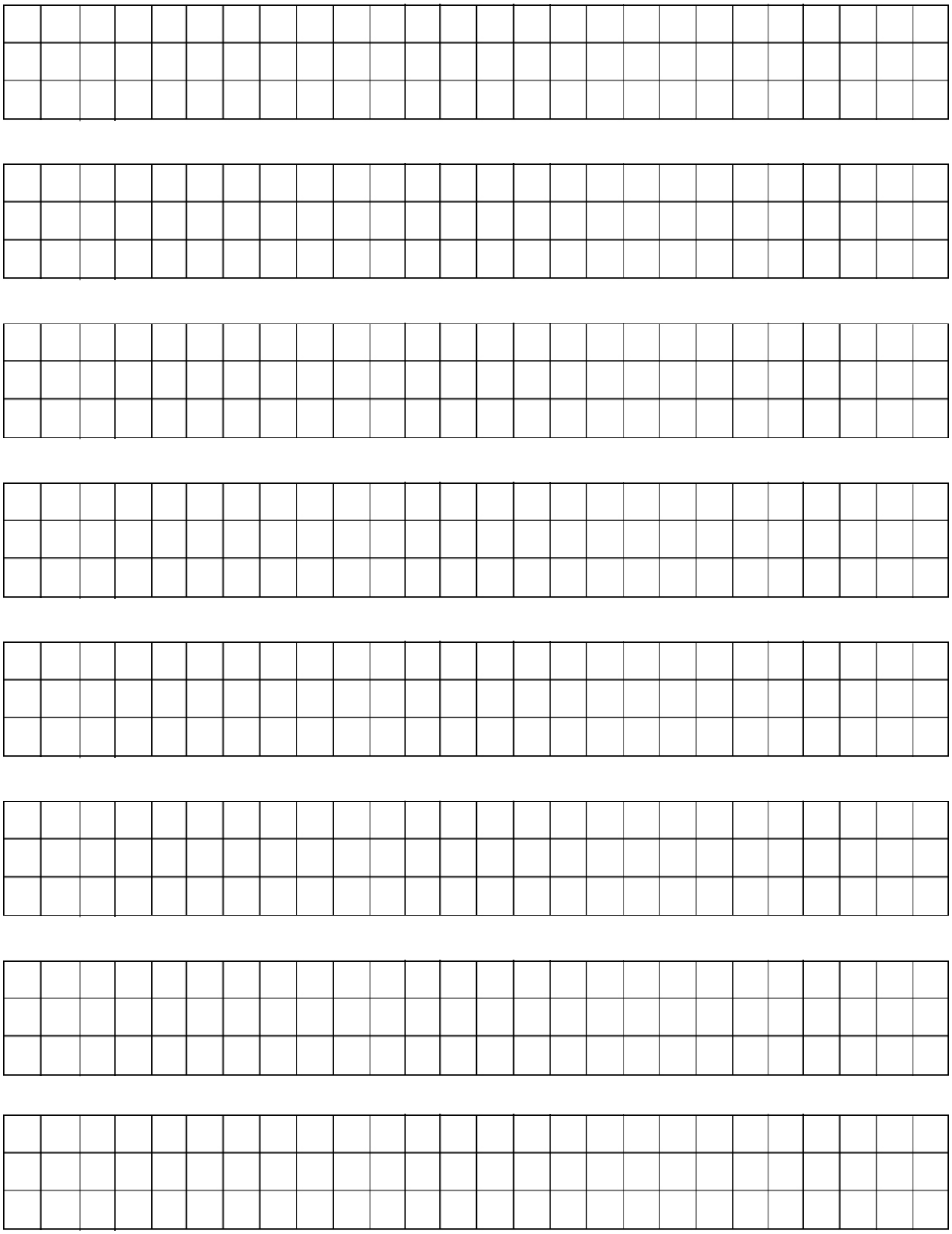


—Chinese Proverb

Name _____ **Date**_____

(Text page 60)

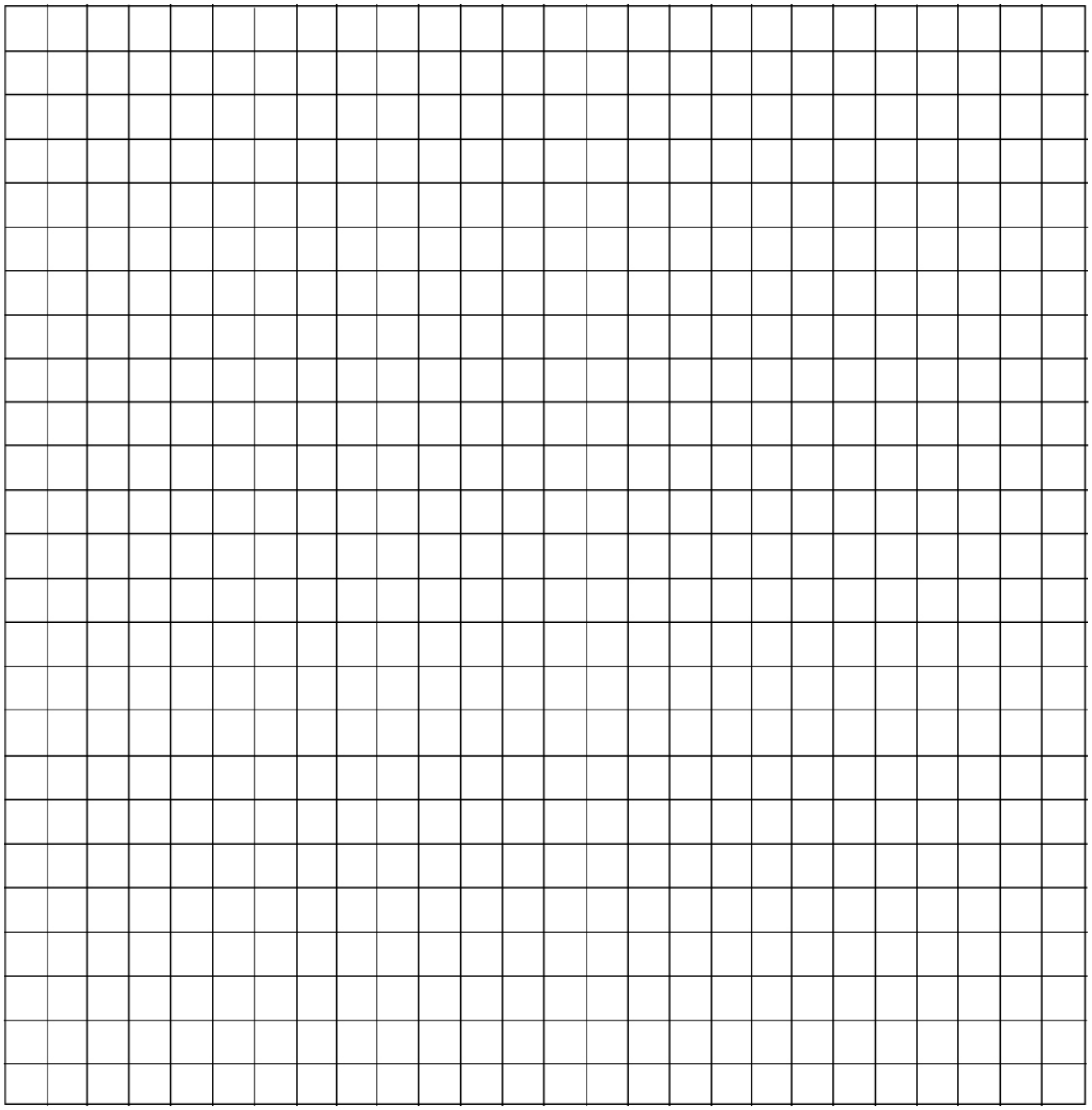
10. Find a quote from a famous person. Encrypt it using a Vigenère Cipher. Use it to play Cipher Tag.



Name _____ **Date**_____

(Text page 60)

11. **Challenge.** Explore how to describe a Vigenère cipher using numbers. In Chapter 2, you worked with number messages. You described Caesar ciphers with arithmetic—by adding to encrypt and subtracting to decrypt. The Vigenère Cipher can be described with arithmetic too. Instead of writing the keyword repeatedly, change the letters of the keyword to numbers and write the numbers repeatedly. Then add to encrypt. For an example, see page 60 of the text. Encrypt and decrypt your own message with this method.



Name _____ **Date**_____

Chapter 8: Cracking Vigenère Ciphers When You Know the Key Length

(Text pages 72–73)

CLASS ACTIVITY. Finish Decrypting the Girls´ Message

Finish decrypting the Girls' Message (key length 4) on pages W36–W37. Your teacher will assign your group 3 or 4 lines of the message to work with.

1. **First wheel**. The letters for the first wheel are already decrypted. What letter was matched with **a**? _____

2. **Second wheel**
   a. Use the table on page 72 of the text to decide how to turn the second wheel. Then decrypt the letters with 2 underneath in your assigned lines.
   b. What letter did you match with **a**? _____

3. **Third wheel**
   a. Find the number of **A**s, **B**s, **C**s, etc. among the letters with 3 underneath. Record your data in the tables on page W38.
   b. Use the class data from 3a to decide how to turn the third wheel. Then decrypt the letters with 3 underneath in your assigned lines.
   c. What letter did you match with **a**? _____

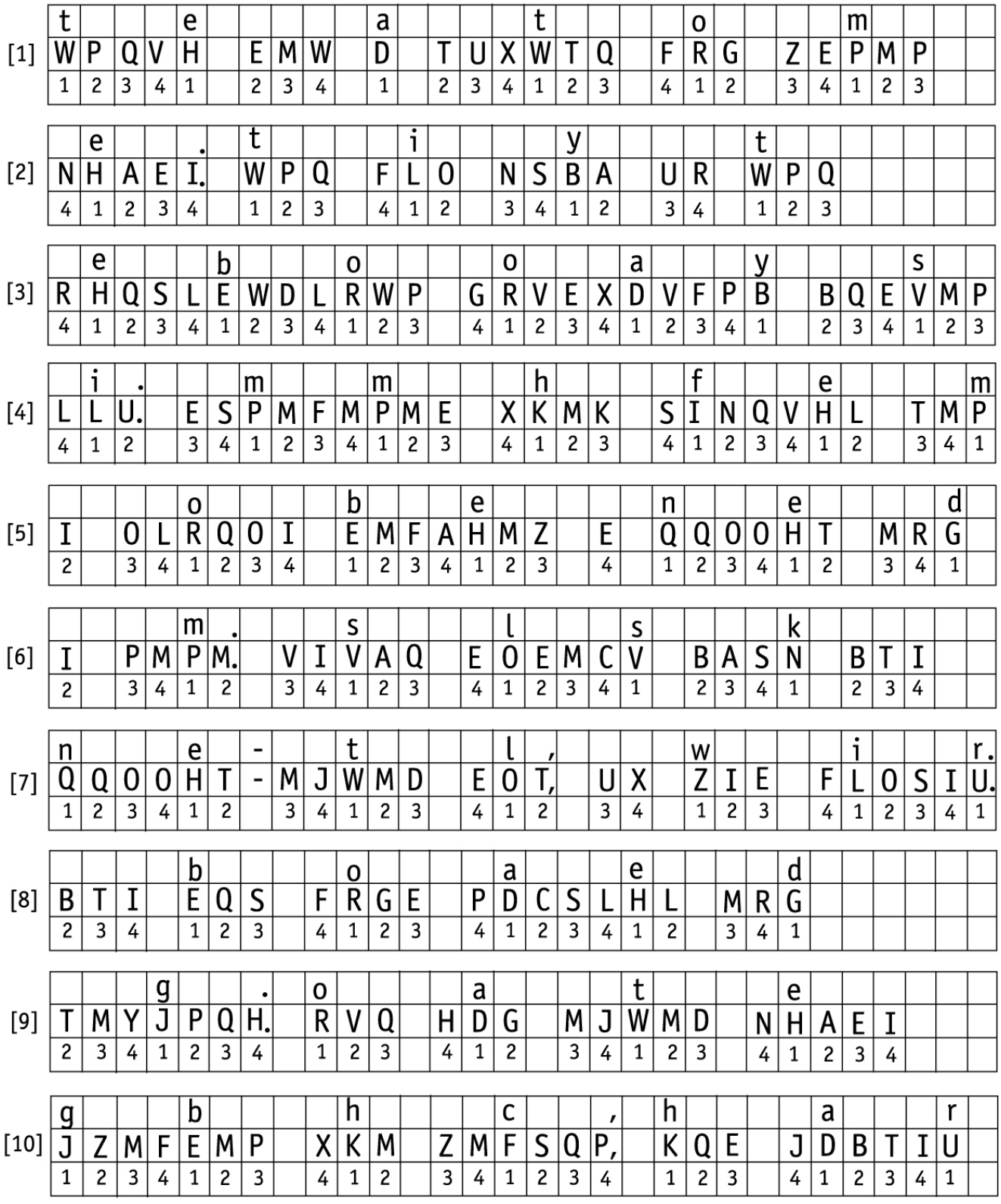
4. **Fourth wheel**
   a. Use the partly decrypted message to guess how to decrypt one of the letters with 4 underneath. Use this to figure out what the fourth wheel must be. Then decrypt the rest of your assigned lines.
   b. What letter did you match with **a**? _____

5. What was the keyword? ____ ____ ____ ____

Name _____ **Date**_____

(Text page 70–73)

The Girls' Message



(continued)

Name _____ **Date**_____

(Text page 70–73)

[11]

			k					a				e					s			,	"j			e,	
B	A	S	N		P	U	Q	D	A	U	H	H	I	Z	H		V	I	U	H,	"M	M	E	W	H,
2	3	4	1		2	3	4	1	2	3	4	1	2	3	4		1	2	3	4	1	2	3	4	1

[12]

			s				y				e				i				u					
B	T	S	V	M		N	S	B	A		M	V	H		U	M	O	L	V	S		J	X	V		A	J
2	3	4	1	2		3	4	1	2		3	4	1		2	3	4	1	2	3		4	1	2		3	4

[13]

y		.			h					h					y					o	'				n			
B	W	G.		X	K	M	K		X	K	Q	Z	O		B	W	G		H	R	V'	F		O	Q	W	I	
1	2	3		4	1	2	3		4	1	2	3	4		1	2	3		4	1	2	3		4	1	2	3	

[14]

	h					m					w				h					e					n			
X	K	M		P	M	P	M		U	W		Z	W	D	X	K		U	A	V	H		B	T	E	Q		
4	1	2		3	4	1	2		3	4		1	2	3	4	1		2	3	4	1		2	3	4	1		

[15]

				n				e	."			s					r				e					d		
B	T	I		Q	Q	O	O	H	T."		V	I	V	A	Q		K	U	Q	Z	R	H	L		M	R	G	
2	3	4		1	2	3	4	1	2		3	4	1	2	3		4	1	2	3	4	1	2		3	4	1	

[16]

			d,	"		'	t					r					d.						o					
A	M	M	G,	"L	A	R'	W		E	A	V	U	G		P	E	G.		Q		W	R	R	E				
2	3	4	1		2	3	4	1		2	3	4	1	2		3	4	1		2		3	4	1	2				

[17]

		i					s					t					r	.				t						
I	L	L	K	T		M	V		E	A	V	W	P		Y	S	U	M.		N	Y	W		Q	R		M	
3	4	1	2	3		4	1		2	3	4	1	2		3	4	1	2		3	4	1		2	3		4	

[18]

t					t				i		',			h					o					s				
W	W	A	O		W	P	Q		H	L	U	Q,		X	K	M	K		A	R	C	X	H		V	B	A	T
1	2	3	4		1	2	3		4	1	2	3		4	1	2	3		4	1	2	3	4		1	2	3	4	

[19]

d				g			.			o						i'					o				c				
G	W	U	R	J		Q	F.		W	R		N	M	V		L'	D	Q		G	R	T	X	I	F	B	Q	H	
1	2	3	4	1		2	3		4	1		2	3	4		1	2	3		4	1	2	3	4	1	2	3	4	

[20]

t					o				r		."																	
W	M	Z		H	R	T	X	E	U	A	."																	
1	2	3		4	1	2	3	4	1	2																		

Name _____ **Date**_____

(Text page 70–73)

Tables for the third wheel of the Girls' Message.

What line numbers are assigned to your group? _____

To save work, count the letters in your assigned lines only. Then combine data with your class to get a total.

Frequency in Your Assigned Lines

Wheel 3 letter	Tally (optional)	Number in your lines only
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		

Class Total

Wheel 3 letter	Number in entire message
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	**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	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	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	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	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	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	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	Z	Y	Z	A	B	C	D	E	F
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	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	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	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	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	U	J	K
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	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	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	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	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	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	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	U	V	W	X	Y	X	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
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	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	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	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	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	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

In Message		In English	
Letter	Rel. Freq. (%)	Letter	Rel. Freq. (%)
		e	12.7
		t	9.1
		a	8.2
		o	7.5
		i	7.0
		n	6.7
		s	6.3
		h	6.1
		r	6.0
		d	4.3
		l	4.0
		c	2.8
		u	2.8
		m	2.4
		w	2.4
		f	2.2
		g	2.0
		y	2.0
		p	1.9
		b	1.5
		v	1.0
		k	0.8
		j	0.2
		q	0.1
		x	0.1
		z	0.1

In Message		In English	
Letter	Rel. Freq. (%)	Letter	Rel. Freq. (%)
		e	12.7
		t	9.1
		a	8.2
		o	7.5
		i	7.0
		n	6.7
		s	6.3
		h	6.1
		r	6.0
		d	4.3
		l	4.0
		c	2.8
		u	2.8
		m	2.4
		w	2.4
		f	2.2
		g	2.0
		y	2.0
		p	1.9
		b	1.5
		v	1.0
		k	0.8
		j	0.2
		q	0.1
		x	0.1
		z	0.1

In Message		In English	
Letter	Rel. Freq. (%)	Letter	Rel. Freq. (%)
		e	12.7
		t	9.1
		a	8.2
		o	7.5
		i	7.0
		n	6.7
		s	6.3
		h	6.1
		r	6.0
		d	4.3
		l	4.0
		c	2.8
		u	2.8
		m	2.4
		w	2.4
		f	2.2
		g	2.0
		y	2.0
		p	1.9
		b	1.5
		v	1.0
		k	0.8
		j	0.2
		q	0.1
		x	0.1
		z	0.1

In Message		In English	
Letter	Rel. Freq. (%)	Letter	Rel. Freq. (%)
		e	12.7
		t	9.1
		a	8.2
		o	7.5
		i	7.0
		n	6.7
		s	6.3
		h	6.1
		r	6.0
		d	4.3
		l	4.0
		c	2.8
		u	2.8
		m	2.4
		w	2.4
		f	2.2
		g	2.0
		y	2.0
		p	1.9
		b	1.5
		v	1.0
		k	0.8
		j	0.2
		q	0.1
		x	0.1
		z	0.1

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	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	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	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	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	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	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	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	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

Wheel 2	Wheel 2 Frequency
M	17.5%
Q	10.5%
B	9.6%
T	7.9%
A	7.9%
W	7.0%
P	6.1%
V	5.3%
I	4.4%
E	4.4%
U	3.5%
L	3.5%
G	3.5%
O	1.8%
N	1.8%
C	1.8%
Z	0.9%
S	0.9%
K	0.9%
D	0.9%
Y	0.0%
X	0.0%
R	0.0%
J	0.0%
H	0.0%
F	0.0%
Total	1