Cryptography on the Telegraph Lines

Standards Addressed: Computer Science: 5.IC.C.01 Math: 4.OA.C, 5.OA.B Science:S.4.3.3, S.4.3.4, S.4.4.5 Social Studies: ss.4.3.5, ss.4.4.8, ss8.4.6. ss8.6.5

Cryptography was used to guard the security of messages over telegraph lines. During the Civil War many types of ciphers were utilized for encrypting messages of great importance. Students will learn and utilize three different encryption methods which were commonly used in America during the late 1800s.

Objectives

- Students will understand that important messages were relayed publicly if they were protected with ciphers.
- Students will identify encryption and decryption.
- Students will utilize Caesar and Stager Ciphers.
- Students will solve ciphers with pattern analysis and critical thinking skills.
- Students will investigate how the Cipher Wheel, as an innovative tool, increased code security and decreased decrypting time.
- Students will collaborate with others to send secret messages.

Preparation

Print the following handouts for each student.

- *Caesar Cipher worksheet*
- *Cipher Wheel worksheet*
- *Stager's Cipher worksheet*

Read teacher preparation before beginning the lesson.

Download free Caesar Cipher Wheels from internet.

Construct Cipher Wheels with students.

Materials

- Caesar Cipher worksheet
- Cipher Wheel worksheet
- Stager's Cipher worksheet

Optional: Caesar Cipher Wheel

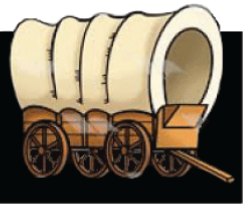
Directions

Lesson One: Caesar Cipher

Begin with a class dialog of telegraph communication in America from 1831 through the Civil War. Discussion questions may include:

- How did Americans communicate before telephones?
  - What were the timelines of these methods of communication?
- How did the first long-distance telegraph line built by Samuel Morse in 1844 change communication in America?
  - What are the benefits for business, government, and society?
- How was communication transmitted along telegraph lines?


National Historic Trails Interpretive Center
1501 N. Poplar St.
Casper, WY 82601
307-261-7700
blm_wy_trailscenter@blm.gov

- Was Morse code a secure method of transmitting confidential private messages? Why or why not?
- When could it be very important that information transmitted publicly is kept confidential?

Introduce the concept of **encryption** to the class. Discuss how messages could be transmitted confidentially by encoding the original text to say something else. Explain to the students that there are many methods to **encoding** messages, and that it is crucial for the recipient of the message to understand how to **decode** the message to understand its full meaning.

Write the first Caesar encoded message on the board and ask the class what it means.

Follow the steps in **Teacher's Notes** to explain the **cipher** and work together as a class to decode the message.

Practice with the *Caesar Cipher* worksheet.

(Expansion) In small groups, task the students to encode a message of their choice utilizing number substitution for text. Share the encrypted messages with other groups to decrypt.

Lesson Two: Cipher Wheel

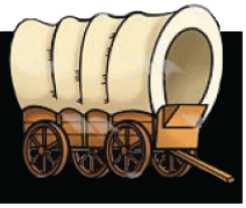
Continue from the Caesar Cipher lesson with an introductory discussion which may include the following questions:

- Why was decryption just as important as encryption for relaying the message?
- What would you do if your coded message was no longer confidential and safe?
- How could you improve the security of the ciphers?
- What type of tool could be invented which would assist you with the ciphers?

Explain to the class that innovations were created which increased the speed and complexity of the ciphers, making them easier to encode and decode but more difficult for others to break.

Introduce the cipher wheel to the class. You may utilize a paper wheel, an actual wheel you have purchased, or a virtual wheel from the internet. Demonstrate how the wheel





rotates to shift to differing Caesar codes. Explain the concept of a **key word.**

Demonstrate the first example from the *Cipher Wheel worksheet* with a **key word** of **BEE**. Refer to **Teacher's Notes** for guidance.

Practice the Cipher Wheel worksheet. Students may utilize a cipher wheel you have provided, or the table provided on the worksheet to decrypt the messages.

(8-12 Expansion) In small groups, ask the students to research different ciphers utilized by the Union and Confederate armies during the Civil War. Have groups identify one cipher to research further and prepare an example to teach the class.

Lesson Three: Stager's Cipher

Begin with a class dialog about the previous cipher learned by the class.

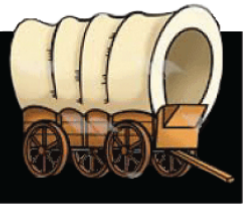
Guiding questions may be:

- What did you like about the Caesar ciphers? What did you dislike?
- How did the tool make it easier to decode the message?
- What are other methods you might use encode a message more complexly than the Caesar cipher?

Introduce the Stager's Cipher to students by utilizing hints from the **Teacher's Notes** and practice with the *Stager's Cipher worksheet*.

(Expansion) In small groups, have students encode an important fact the class has been studying. The encrypted facts will be shared with other groups to decode.





Key Vocabulary

Caesar cipher -a simple substitution encryption utilized by Julius Caesar where a plaintext letter is substituted with a letter which has been shifted down the alphabet.

cipher -a secret or camouflaged way of writing

cipher wheel -tool used to encode/decode messages with a simple substitution cipher

code books -secret books needed to decrypt a cipher

decode -translate a cipher into a message

decrypt -translate a cipher into a message

encode -convert a message into a cipher

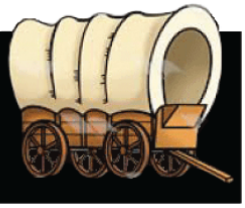
encrypt -convert a message into a cipher

indicators -decryption data used to solve a code

null word -extra words added that have no meaning in the message

Stager's cipher -a transposition cipher utilized during the Civil War which rearranges the order of words in a message.


National Historic Trails Interpretive Center
1501 N. Poplar St.
Casper, WY 82601
307-261-7700
blm_wy_trailscenter@blm.gov

Teacher's Notes

Caesar Cipher

History This cipher was first utilized by Julius Caesar (100 BC to 44BC) to keep his personal correspondence safe from unfriendly eyes. It has been used throughout the world with many alphabets since that time. During the Civil War both armies used this cipher to encrypt communication. However, it can easily be broken, letting important messages be deciphered by the enemy.

Encryption A Caesar cipher utilizes a simple substitution of letters to encode the message. Letters are shifted down the alphabet to remap the encoded letters. A common Caesar cipher has a shift of 3, meaning that plain text A maps to encoded text D, B maps to E, C maps to F, and so on and so forth. The end of the alphabet loops to the beginning in the encoded text. In a simple substitution cipher no letter may map to itself or to more than one letter.

Caesar Example

Encryption

1. The first step to encoding the communication is to write out the plain text message:

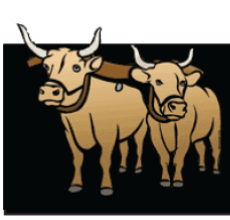
FRIDAY

2. If you know the shift, then fill in the coded letters in a chart. (Shift of 3)

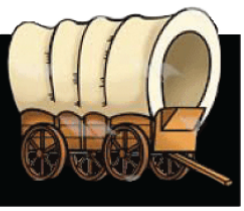
PLAIN	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
CODED	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

3. Next replace the plain text with the coded text.

FRIDAY ⟶ **IULGDB**




National Historic Trails Interpretive Center
1501 N. Poplar St.
Casper, WY 82601
307-261-7700
blm_wy_trailscenter@blm.gov

Decryption

1. Given the shift for the Caesar cipher, fill in the table with the encoded letters. (Shift of 3)

PLAIN	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
CODED	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

2. Replace the encoded letters to discover the first message sent by telegraph. Find the encoded letter on the chart and move upwards to find the plain text.

Message: **ZKDW JRG KDWK ZURXJKW**

WHAT GOD HATH WROUGHT

Breaking the Caesar Code with Numbers.

1. Replace the alphabet with the numbers 0-25. The number corresponding to a letter does not change.

PLAIN	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
CODED	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

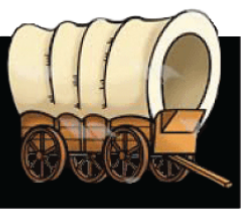
2. Given a shift of 4, add 4 to the plain text numbers.

PLAIN	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
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
Shift #	**4**	**4**	**4**	**4**	**4**	**4**	**4**	**4**	**4**	**4**	**4**	**4**	**4**	**4**	**4**	**4**	**4**	**4**	**4**	**4**	**4**	**4**	**4**	**4**	**4**	**4**
Total	4	5	6	7	8	9	10	11	12	13	14	15	16	16	18	19	20	21	22	23	24	25	26	27	28	29
CODED																										

3. The coded letter corresponds to the number total for each column. Refer to the chart with each letter coded to a number 0-25. Plain text A shifts by 4 (0+4= 4) and equals a E. Plain text J shifts by 4 (9+4=13) and equals an N. (With numbers 26 to 29 subtract 26 (letters in the alphabet) to find the coded letter. (This is called mod 26.) Fill in the chart.

PLAIN	**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**
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	16	18	19	20	21	22	23	24	25
Shift #	**4**	**4**	**4**	**4**	**4**	**4**	**4**	**4**	**4**	**4**	**4**	**4**	**4**	**4**	**4**	**4**	**4**	**4**	**4**	**4**	**4**	**4**	**4**	**4**	**4**	**4**
Total	4	5	6	7	8	9	10	11	12	13	14	15	16	16	18	19	20	21	22	23	24	25	26	27	28	29
CODED	**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**


National Historic Trails Interpretive Center
1501 N. Poplar St.
Casper, WY 82601
307-261-7700
blm_wy_trailscenter@blm.gov

Teacher's Notes

Cipher Wheel

History The cipher wheel was a mechanical encryption device used by the Confederate Army during the Civil War to safeguard messages. Francis LeBarre, who was very good at creating objects with metal, created a device made of two rotating alphabet discs which could encode and decode Caesar messages. By aligning different letter combinations, the user could work quickly with the messages. The cipher wheel made encryption much more difficult to break. The Confederate Army utilized this method of encryption because it was more secure and more difficult to break with manual decryption techniques.

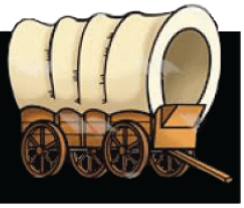
Encryption The cipher wheel method utilizes different combinations of Caesar ciphers to encrypt a message. A **code word** is needed for encryption. The wheel is turned to the first letter of the code word to decrypt the first word of the message, the second letter of the code word for the second word, and so on. This method of encryption could also be substituted for every letter of the message and not just shifting on every word, making it nearly impossible to decrypt with just the human mind (if you don't know the code word.)

Where to find cipher wheels? Cipher wheels with the roman alphabet are available for purchase through many online merchants. Free downloadable paper wheels are also available online.

Note: While it is fun for students to utilize the physical cipher wheel, some may find it frustrating. The letter alignment can be complicated, and misalignment leads to the incorrect encryption. Many students enjoyed trying the paper wheels, but shifted to utilizing the chart method, which didn't move every time they touched it.



National Historic Trails Interpretive Center
1501 N. Poplar St.
Casper, WY 82601
307-261-7700
blm_wy_trailscenter@blm.gov



Decryption

1. The first step to encoding the communication is to determine a **code word**. The code word will be **BEE.**

2. Second, align the wheel with the plain text A mapping to B. If using a chart, map the first shift to B.

PLAIN	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
1st	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
2nd																										
3rd																										

3. Write the word order above the coded text. Remember the word BEE has 3 letters.

1 2 3 1 2 3 1 2 3

OPUIJOH MW MQTSWWMFPI, UIF ASVH MXWIPJ TBZT, “M’Q TSWWMFPI.”

4. Decode words with the number 1 with the coded text of A mapping to B. (Use the chart or a cipher wheel.)

NOTHING MW MQTSWWMFPI, THE ASVH MXWIPJ SAYS, “M’Q TSWWMFPI.”

5. Move to the next letter of the code word. Fill in the chart or turn the cipher wheel. Notice that the code word BEE has a double letter, the pattern is the same for the 2 and 3. Look at the first column A. Do you see the code word?

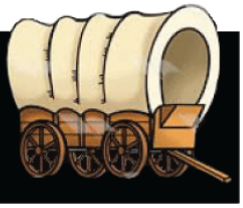
PLAIN	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1st	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
2nd	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
3rd	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D

6. Replace the coded letters for the 2 and 3 words. Discover this message by Audrey Hepburn.

NOTHING IS IMPOSSIBLE, THE WORD ITSELF SAYS, “I’M POSSIBLE.”

Encryption By now you should be able to encrypt a message using the cipher wheel. Remember to chose a code word first! To make it more difficult to break, shift the cipher wheel for every letter instead of every word.


National Historic Trails Interpretive Center
1501 N. Poplar St.
Casper, WY 82601
307-261-7700
blm_wy_trailscenter@blm.gov

Teacher's Notes

Stager's Cipher

History Anson Stager was tasked with developing the first telegraphic cipher used to protect government communications during the Civil War. He developed a simple but very effective "route" cipher which transposed words to encrypt communications. His cipher was adopted as the official cipher of the War Department and was never cracked by the Confederates.

Encryption Messages are written with an equal number of words in each line. Then words are copied up and down columns by various routes, sometimes adding **null words** (extra words) at the end of columns and substituting code words for important names and activities.

Stager's ciphers have **indicators** which tell the number of columns, and which page (in the code book) describe the **route** of the cipher. The routes are shown by a table, where only the ***top*** and ***bottom*** row numbers are significant. The numbers in these rows correlate to the column numbers and indicate which direction the text is entered into the column. Indicator numbers in the top row mean that the column should be filled from the top down. Indicator numbers in the bottom row mean that the column should be filled from the bottom up.

Code books contain word substitution lists which replace important names and activities in the message. These words are replaced before writing the message along the route.


National Historic Trails Interpretive Center
1501 N. Poplar St.
Casper, WY 82601
307-261-7700
blm_wy_trailscenter@blm.gov


Stager Example

Encryption

1. The first step to encoding the communication is to write out the plain text message:

Don't walk in the battleground tonight because an enemy was spotted.

2. The second step is to substitute important names and activities with their code words. Also, take out articles (a, the, etc.) that are not needed.

Code Book Substitutions
battleground ⟶ **cornfield**
enemy ⟶ **dog**

Don't walk in cornfield tonight because dog was spotted.

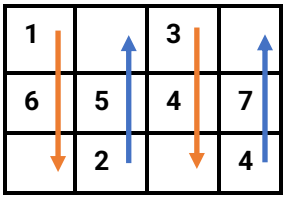
3. Next **null words** may be added to make messages more complex.

Don't walk in cornfield tonight because rabid dog was spotted.

4. Write the plain text message in a grid with the number of columns stated by the code book. In this case, four columns will be used. Write the words from left to right moving to the next row as needed. Fill in blank spots with **null words**.

DON'T	WALK	IN	CORNFIELD
TONIGHT	BECAUSE	RABID	DOG
WAS	SPOTTED	APPLE	TREE

5. Lastly, rearrange the words according to the route indicator. The number of columns for decryption equals the number in the indicator table. The top and bottom rows indicate the direction for placing the words in their columns. Indicator numbers on the top row mean the words go down the column. Indicator numbers on the bottom row mean the words go up the column. The middle rows are null numbers, ignore them.



The example is down 1, up 2, down 3, up 4.

Coded Message: DON'T TONIGHT WAS SPOTTED BECAUSE WALK IN RABID APPLE TREE DOG CORNFIELD

Decryption

Coded Message: DON'T TONIGHT WAS SPOTTED BECAUSE WALK IN RABID APPLE TREE DOG CORNFIELD

1		3	
6	5	4	7
	2		4

1. Fill in an empty table with the coded message. The route indicator tells you how many columns (same as indicator) and which direction to fill in the table.

DON'T	WALK	IN	CORNFIELD
TONIGHT	BECAUSE	RABID	DOG
WAS	SPOTTED	APPLE	TREE

NOTE: This example has columns in order 1,2,3,4, but columns may be out of order for more complexity. Also, divide the number of words by the number of columns to determine how many rows are needed in the table.

2. Write the coded message from right to left.

DON'T	WALK	IN	CORNFIELD
TONIGHT	BECAUSE	RABID	DOG
WAS	SPOTTED	APPLE	TREE

MESSAGE: DON'T WALK IN CORNFIELD TONIGHT BECAUSE RABID DOG WAS SPOTTED APPLE TREE

3. Replace coded text with code book substitutions.

Code Book Substitutions
battleground ⟶ **cornfield**
enemy ⟶ **dog**

MESSAGE: DON'T WALK IN **BATTLEGROUND** TONIGHT BECAUSE RABID **ENEMY** WAS SPOTTED APPLE TREE

4. Cancel null words. Fill in articles (if you want).

PLAIN TEXT MESSAGE: Don't walk in the battleground tonight because an enemy was spotted.


National Historic Trails Interpretive Center
1501 N. Poplar St.
Casper, WY 82601
307-261-7700
blm_wy_trailscenter@blm.gov