Lesson 13: Using Matrix Operations for Encryption

Student Outcomes

- Students study and practice the properties of matrix multiplication.
- Students understand the role of the multiplicative identity matrix.

Lesson Notes

Data encryption has become a necessity with the rise of sensitive data being stored and transmitted via computers. The methods included in this section are not secure enough to use for applications such as Internet banking, but they result in codes that are not easy to break and provide a good introduction to the ideas of encryption. Interested students can research RSA public-key encryption, which relies on the fact that factoring extremely large numbers is a very difficult and slow process. Students interested in the history of data encryption can research the Cherokee and Choctaw Code Talkers from World War I and the Navajo Code Talkers from World War II.

This lesson reinforces concepts of matrix multiplication, matrix inverses, and the identity matrix in the context of encoding and decoding strings of characters using multiplication by either an encoding matrix or its inverse decoding matrix. This lesson aligns with **N-VM.C.6** (Use matrices to represent and manipulate data), **N-VM.C.8** (Add, subtract, and multiply matrices of appropriate dimensions), and **N-VM.C.10** (Understand that the zero and identity matrices play a role in matrix addition and multiplication similar to the role of 0 and 1 in the real numbers. The determinant of a square matrix is nonzero if and only if the matrix has a multiplicative inverse.)

The activity in Exercise 2 requires that six stations be set up in advance around the classroom as the messages have been encoded four times. At each station, post the specified decoding matrix:

Station 1:

$$D_1 = \begin{bmatrix} -1 & -1 \\ 1 & \frac{1}{2} \end{bmatrix}$$

Station 2:

$$D_2 = \begin{bmatrix} \frac{1}{6} & 0 \\ 0 & \frac{1}{3} \end{bmatrix}$$

Station 3:

$$D_3 = \begin{bmatrix} \frac{1}{3} & -\frac{1}{3} \\ -\frac{1}{3} & \frac{4}{3} \end{bmatrix}$$

Station 4:

$$D_4 = \begin{bmatrix} \frac{1}{2} & -\frac{1}{2} \\ -\frac{3}{2} & \frac{5}{2} \end{bmatrix}$$

Station 5:

$$D_5 = \begin{bmatrix} -1 & 1 \\ 0 & 1 \end{bmatrix}$$

Station 6:

$$D_6 = \begin{bmatrix} 2 & -1 \\ -3 & 2 \end{bmatrix}$$

Divide students into at least six groups numbered 1–6, assign each group their coded message, and start them at their numbered station. Groups will apply the decoding matrix to their message and then move to the next station. After applying four decoding matrices, the original message will be revealed. Each group will decode 20 characters of the original message, combining the results into the full quote from the entire class.

Classwork

Opening (7 minutes)

The phrase "The crow flies at midnight" appears to have first occurred in Ian Fleming's James Bond novel *From Russia with Love*. It has since become a coded message in spy movies and television shows.

Opening

A common way to send coded messages is to assign each letter of the alphabet to a number 1–26 and send the message as a string of integers. For example, if we encode the message "THE CROW FLIES AT MIDNIGHT" according to the chart below, we get the string of numbers

$$20, 8, 5, 0, 3, 18, 15, 23, 0, 6, 12, 9, 5, 19, 0, 1, 20, 0, 13, 9, 4, 14, 9, 7, 8, 20.$$

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13

N	O	P	Q	R	S	T	U	V	W	X	Y	Z	SPACE
14	15	16	17	18	19	20	21	22	23	24	25	26	0

However, codes such as these are easily broken using an analysis of the frequency of numbers that appear in the coded messages.

We can instead encode a message using matrix multiplication. If a matrix E has an inverse, then we can encode a message as follows.

- **First, convert the characters of the message to integers between 1 and 26 using the chart above.**
- **If the encoding matrix E is an $n \times n$ matrix, then break up the numerical message into n rows of the same length. If needed, add extra zeros to make the rows the same length.**
- **Place the rows into a matrix M.**
- **Compute the product EM to encode the message.**
- **The message is sent as the numbers in the rows of the matrix EM.**

Example (10 minutes)

- A common way to send coded messages is to assign each letter of the alphabet to a number 1–26 and send the message as a string of integers. For example, if we encode the message "THE CROW FLIES AT MIDNIGHT" according to the chart below, we get the string of numbers

$$20, 8, 5, 0, 3, 18, 15, 23, 0, 6, 12, 9, 5, 19, 0, 1, 20, 0, 13, 9, 4, 14, 9, 7, 8, 20.$$

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13

N	O	P	Q	R	S	T	U	V	W	X	Y	Z	SPACE
14	15	16	17	18	19	20	21	22	23	24	25	26	0

However, codes such as these are easily broken using an analysis of the frequency of numbers that appear in the coded messages. For example if the coded phrase is $20, 8, 5, 0, 3, 18, 15, 23, 0, 6, 12, 9, 5, 19, 0, 1, 20, 0, 13, 9, 4, 14, 9, 7, 8, 20$, we can see that there are three of the letters assigned to the integer 20, so we may want to try putting a common letter in for the number 20 like S, T, or E. If we assume the word *the* is used to start the phrase since we have three letters then a space, that would lead us to think that maybe the number 5 is E, and so on.

- We can instead encode a message using matrix multiplication. If a matrix E has an inverse, then we can encode a message as follows.
- First, convert the characters of the message to integers between 1 and 26 using the chart above.
- If the encoding matrix E is an $n \times n$ matrix, then break up the numerical message into n rows of the same length. If needed, add extra zeros to make the rows the same length. For example if we want to use an encoding matrix that is 2×2, we would write the message in two rows of equal length, filling in zero for the last number if the number of letters was odd. If the encoding matrix is 3×3, the message would be written in three equal rows adding zeros as necessary.
- Place the rows into a matrix M.
- Compute the product EM to encode the message.
- The message is sent as the numbers in the rows of the matrix EM.
- Using the matrix $E = \begin{bmatrix} 2 & 1 \\ 3 & 1 \end{bmatrix}$, we encode our message as follows:

  $$4, 14, 9, 7, 8, 20.$$

- Since E is a 2×2 matrix, we need to break up our message into two rows.

  $$20, 8, 5, 0, 3, 18, 15, 23, 0, 6, 12, 9, 5,$$
  $$19, 0, 1, 20, 0, 13, 9, 4, 14, 9, 7, 8, 20.$$

- Then we place the rows into a matrix M.

  $$M = \begin{bmatrix} 20 & 8 & 5 & 0 & 3 & 18 & 15 & 23 & 0 & 6 & 12 & 9 & 5 \\ 19 & 0 & 1 & 20 & 0 & 13 & 9 & 4 & 14 & 9 & 7 & 8 & 20 \end{bmatrix}.$$

Scaffolding:

- Students who are struggling can be given a simpler phrase such as "Be Happy" or "Dream Big."
- Have advanced learners find their own phrase of 30 characters or more and encode using a 3×3 matrix.

MP.2

- Explain how matrix M represents "THE CROW FLIES AT MIDNIGHT."
  - *Each letter and space in the phrase was assigned an integer value, and these numbers represent the letters in the phrase.*
- We encode the message into matrix C by multiplying $E \cdot M$.

  $$C = E \cdot M = \begin{bmatrix} 2 & 1 \\ 3 & 1 \end{bmatrix} \begin{bmatrix} 20 & 8 & 5 & 0 & 3 & 18 & 15 & 23 & 0 & 6 & 12 & 9 & 5 \\ 19 & 0 & 1 & 20 & 0 & 13 & 9 & 4 & 14 & 9 & 7 & 8 & 20 \end{bmatrix}$$
  $$C = \begin{bmatrix} 59 & 16 & 11 & 20 & 6 & 49 & 39 & 50 & 14 & 21 & 31 & 26 & 30 \\ 79 & 24 & 16 & 20 & 9 & 67 & 54 & 73 & 14 & 27 & 43 & 35 & 35 \end{bmatrix}$$

- Thus, the coded message that we send is

  $$59, 16, 11, 20, 6, 49, 39, 50, 14, 21, 31, 26, 30, 79, 24, 16, 20, 9, 67, 54, 73, 14, 27, 43, 35, 35.$$

  If this coded message is intercepted, then it cannot easily be decoded unless the recipient knows how it was originally encoded.

Be sure to work through this discussion and emphasize that the way to decode a message is to multiply by the inverse of the encoding message.

MP.4

- Using what you know about how the message was encoded, as well as matrix multiplication, describe how you would decode this message.
  - *We need to know a decoding matrix D.*
- How can we find that matrix?
  - *The decoding matrix is the inverse of the encoding matrix, so $D = E^{-1}$.*
- What is the decoding matrix?
  - $D = E^{-1} = \begin{bmatrix} 2 & 1 \\ 3 & 1 \end{bmatrix}^{-1} = \frac{1}{2-3}\begin{bmatrix} 1 & -1 \\ -3 & 2 \end{bmatrix} = \begin{bmatrix} -1 & 1 \\ 3 & -2 \end{bmatrix}$.
- Decode this message!
  - $D \cdot C = \begin{bmatrix} -1 & 1 \\ 3 & -2 \end{bmatrix}\begin{bmatrix} 59 & 16 & 11 & 20 & 6 & 49 & 39 & 50 & 14 & 21 & 31 & 26 & 30 \\ 79 & 24 & 16 & 20 & 9 & 67 & 54 & 73 & 14 & 27 & 43 & 35 & 35 \end{bmatrix}$
    $= \begin{bmatrix} 20 & 8 & 5 & 0 & 3 & 18 & 15 & 23 & 0 & 6 & 12 & 9 & 5 \\ 19 & 0 & 1 & 20 & 0 & 13 & 9 & 4 & 14 & 9 & 7 & 8 & 20 \end{bmatrix}$.

    As expected, this is the matrix M that stored our original message "THE CROW FLIES AT MIDNIGHT."
- Why does this process work?
  - *The coded message stored in matrix C is the product of matrices E and M, so $C = E \cdot M$. We then decode the message stored in matrix C by multiplying by matrix D. Since matrices D and E are inverses, we have*

    $$D \cdot (E \cdot M) = (D \cdot E) \cdot M = I \cdot M = M.$$

    So, encoding and then decoding will return the original message in matrix M.
- Explain to your neighbor what you learned about how to encode and decode messages. Teachers should use this as an informal way to check for understanding.

Exercise 1 (7 minutes)

The encoded phrase in this exercise is "ARCHIMEDES." Archimedes (c. 287–212 BCE, Greece) is regarded as the greatest mathematician of his age and one of the greatest of all time. He developed and applied an early form of integral calculus to derive correct formulas for the area of a circle, volume of a sphere, and area under a parabola. He also found accurate approximations of irrational numbers such as $\sqrt{3}$ and π. However, during his lifetime he was known more for his inventions such as the Archimedean screw, compound pulleys, and weapons such as the Claw of Archimedes used to protect Syracuse in times of war.

The original message is stored in matrix $M = \begin{bmatrix} 1 & 18 & 3 & 8 \\ 9 & 13 & 5 & 4 \\ 5 & 19 & 0 & 0 \end{bmatrix}$, and the matrix used to encode the message is $E = \begin{bmatrix} 1 & 2 & 3 \\ 0 & 2 & 1 \\ 1 & 1 & 1 \end{bmatrix}$. This exercise introduces students to using a larger matrix to perform the encoding and decoding and requires that students practice matrix multiplication with non-integer matrix entries. Additionally, because students have not learned a method for finding the inverse of a 3×3 matrix, they must demonstrate understanding of the meaning of a matrix inverse in order to decode this matrix.

Exercises

1. You have received an encoded message: $34, 101, 13, 16, 23, 45, 10, 8, 15, 50, 8, 12$. You know that the message was encoded using matrix $E = \begin{bmatrix} 1 & 2 & 3 \\ 0 & 2 & 1 \\ 1 & 1 & 1 \end{bmatrix}$.

   a. Store your message in a matrix C. What are the dimensions of C?

   There are 12 numbers in the coded message, and it was encoded using a 3×3 matrix. Thus, the matrix C needs to have three rows. That means C has four columns, so C is a 3×4 matrix.

   b. You have forgotten whether the proper decoding matrix is matrix X, Y, or Z as shown below. Determine which of these is the correct matrix to use to decode this message.

$$X = \begin{bmatrix} -\frac{1}{3} & -\frac{1}{3} & \frac{4}{3} \\ -\frac{1}{3} & \frac{2}{3} & \frac{1}{3} \\ -\frac{2}{3} & \frac{1}{3} & -\frac{2}{3} \end{bmatrix}, Y = \begin{bmatrix} -\frac{1}{3} & -\frac{1}{3} & \frac{4}{3} \\ -\frac{1}{3} & \frac{2}{3} & -\frac{1}{3} \\ \frac{2}{3} & -\frac{1}{3} & \frac{2}{3} \end{bmatrix}, Z = \begin{bmatrix} -\frac{1}{3} & -\frac{1}{3} & \frac{4}{3} \\ -\frac{1}{3} & \frac{2}{3} & \frac{1}{3} \\ \frac{2}{3} & -\frac{1}{3} & -\frac{2}{3} \end{bmatrix}$$

Matrices used to encode and decode messages must be inverses of each other. Thus, the correct decoding matrix is the matrix D so that $D \cdot E = I$. We can find the correct decoding matrix by multiplying $X \cdot E$, $Y \cdot E$, and $Z \cdot E$.

$$X \cdot E = \begin{bmatrix} -\frac{1}{3} & -\frac{1}{3} & \frac{4}{3} \\ -\frac{1}{3} & \frac{2}{3} & \frac{1}{3} \\ -\frac{2}{3} & \frac{1}{3} & -\frac{2}{3} \end{bmatrix} \cdot \begin{bmatrix} 1 & 2 & 3 \\ 0 & 2 & 1 \\ 1 & 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -\frac{4}{3} & -\frac{4}{3} & -\frac{7}{3} \end{bmatrix}$$

$$Y \cdot E = \begin{bmatrix} -\frac{1}{3} & -\frac{1}{3} & \frac{4}{3} \\ -\frac{1}{3} & \frac{2}{3} & -\frac{1}{3} \\ \frac{2}{3} & -\frac{1}{3} & \frac{2}{3} \end{bmatrix} \cdot \begin{bmatrix} 1 & 2 & 3 \\ 0 & 2 & 1 \\ 1 & 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ -\frac{2}{3} & \frac{1}{3} & -\frac{2}{3} \\ \frac{4}{3} & \frac{4}{3} & \frac{7}{3} \end{bmatrix}$$

$$Z \cdot E = \begin{bmatrix} -\frac{1}{3} & -\frac{1}{3} & \frac{4}{3} \\ -\frac{1}{3} & \frac{2}{3} & \frac{1}{3} \\ \frac{2}{3} & -\frac{1}{3} & -\frac{2}{3} \end{bmatrix} \cdot \begin{bmatrix} 1 & 2 & 3 \\ 0 & 2 & 1 \\ 1 & 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Since $Z \cdot E = I$, we know that Z is the decoding matrix we need.

Scaffolding:

- Students may need to be reminded that the matrices we use to encode and decode a message are inverses.
- Students may also need to be reminded of the property that defines inverse matrices: A and B are inverse matrices if $A \cdot B = I$.

c. Decode the message.

Using matrix Z to decode, we have

$$M = Z \cdot C = \begin{bmatrix} -\frac{1}{3} & -\frac{1}{3} & \frac{4}{3} \\ -\frac{1}{3} & \frac{2}{3} & \frac{1}{3} \\ \frac{2}{3} & -\frac{1}{3} & -\frac{2}{3} \end{bmatrix} \cdot \begin{bmatrix} 34 & 101 & 13 & 16 \\ 23 & 45 & 10 & 8 \\ 15 & 50 & 8 & 12 \end{bmatrix}$$

$$= \begin{bmatrix} -\frac{34}{3} - \frac{23}{3} + \frac{60}{3} & -\frac{101}{3} - \frac{45}{3} + \frac{200}{3} & -\frac{13}{3} - \frac{10}{3} + \frac{32}{3} & -\frac{16}{3} - \frac{8}{3} + \frac{48}{3} \\ -\frac{34}{3} + \frac{46}{3} + \frac{15}{3} & -\frac{101}{3} + \frac{90}{3} + \frac{50}{3} & -\frac{13}{3} + \frac{20}{3} + \frac{8}{3} & -\frac{16}{3} + \frac{16}{3} + \frac{12}{3} \\ \frac{68}{3} - \frac{23}{3} - \frac{30}{3} & \frac{202}{3} - \frac{90}{3} - \frac{100}{3} & \frac{26}{3} - \frac{10}{3} - \frac{16}{3} & \frac{32}{3} - \frac{8}{3} - \frac{24}{3} \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 18 & 3 & 8 \\ 9 & 13 & 5 & 4 \\ 5 & 4 & 0 & 0 \end{bmatrix}.$$

The decoded message is "ARCHIMEDES."

Exercises 2–3 (15 minutes)

In this exercise, groups of students decode separate parts of a message that have been encoded four times; as groups complete the decoding of their portion of the message, have them record it in a location that all students can see—either on the white board or projected through a document camera, for example. The decoded messages will together spell out a famous quote by Albert Einstein: "Do not worry about your difficulties in mathematics. I can assure you that mine are still greater." You may substitute a different quote if you would like, perhaps a school motto. Carefully encode each of six portions of a quote stored in matrices M_1 to M_6 using encoding matrices E_1 to E_6 as follows.

$$C_1 = E_1 \cdot E_2 \cdot E_3 \cdot E_4 \cdot M_1$$
$$C_2 = E_2 \cdot E_3 \cdot E_4 \cdot E_5 \cdot M_2$$
$$C_3 = E_3 \cdot E_4 \cdot E_5 \cdot E_6 \cdot M_3$$
$$C_4 = E_4 \cdot E_5 \cdot E_6 \cdot E_1 \cdot M_4$$
$$C_5 = E_5 \cdot E_6 \cdot E_1 \cdot E_2 \cdot M_5$$
$$C_6 = E_6 \cdot E_1 \cdot E_2 \cdot E_3 \cdot M_6$$

Scaffolding:

For struggling students, select a shorter quote, or encode it in fewer than four steps.

$E_1 = \begin{bmatrix} 1 & 2 \\ -2 & -2 \end{bmatrix}$; $E_2 = \begin{bmatrix} 6 & 0 \\ 0 & 3 \end{bmatrix}$; $E_3 = \begin{bmatrix} 4 & 1 \\ 1 & 1 \end{bmatrix}$; $E_4 = \begin{bmatrix} 5 & 1 \\ 3 & 1 \end{bmatrix}$; $E_5 = \begin{bmatrix} -1 & 1 \\ 0 & 1 \end{bmatrix}$; $E_6 = \begin{bmatrix} 2 & 1 \\ 3 & 2 \end{bmatrix}$

Divide the class into at least six groups of two or three students, numbered 1–6, assigning multiple groups to the same number as needed. Set up six stations around the room in a circular arrangement. Have each group start at the station with the same number as the group—Group 1 starts at Station 1, Group 2 starts at Station 2, etc. At each station, the groups apply the posted decoding matrix to their encoded message shown below, and then they progress to the next station, with groups at Station 6 proceeding to Station 1. It will require four decoding steps with different matrices (such as D_2, D_3, D_4 and D_5) to uncover a group's portion of the original message.

At each station, post the matrix listed below.

Station 1: $D_1 = \begin{bmatrix} -1 & -1 \\ 1 & \frac{1}{2} \end{bmatrix}$

Station 2: $D_2 = \begin{bmatrix} \frac{1}{6} & 0 \\ 0 & \frac{1}{3} \end{bmatrix}$

Station 3: $D_3 = \begin{bmatrix} \frac{1}{3} & -\frac{1}{3} \\ -\frac{1}{3} & \frac{4}{3} \end{bmatrix}$

Station 4: $D_4 = \begin{bmatrix} \frac{1}{2} & -\frac{1}{2} \\ -\frac{3}{2} & \frac{5}{2} \end{bmatrix}$

Station 5: $D_5 = \begin{bmatrix} -1 & 1 \\ 0 & 1 \end{bmatrix}$

Station 6: $D_6 = \begin{bmatrix} 2 & -1 \\ -3 & 2 \end{bmatrix}$

2. **You have been assigned a group number. The message your group receives is listed below. This message is TOP SECRET! It is of such importance that it has been encoded four times.**

Your group's portion of the coded message is listed below.

Group 1:

$1500, 3840, 0, 3444, 3420, 4350, 0, 4824, 3672, 3474, -2592, -6660, 0, -5976, -5940, -7560, 0, -8388, -6372, -6048$

Group 2:

$2424, 3024, -138, 396, -558, -1890, -1752, 1512, -2946, 1458, 438, 540, -24, 72, -90, -324, -300, 270, -510, 270$

Group 3:

$489, 1420, 606, 355, 1151, 33, 1002, 829, 99, 1121, 180, 520, 222, 130, 422, 12, 366, 304, 36, 410$

Group 4:

$-18, 10, -18, 44, -54, 42, -6, -74, -98, -124, 0, 10, -12, 46, -26, 42, -4, -36, -60, -82$

Group 5:

$-120, 0, -78, -54, -84, -30, 0, -6, -108, -30, -120, 114, 42, 0, -12, 42, 0, 36, 0, 0$

Group 6:

$126, 120, 60, 162, 84, 120, 192, 42, 84, 192, -18, -360, -90, -324, 0, -18, -216, -36, -90, -324$

a. **Store your message in a matrix C with two rows. How many columns does matrix C have?**

(Sample responses are provided for Group 1.) Our message is stored in a matrix with ten columns:

$C = \begin{bmatrix} 1500 & 3840 & 0 & 3444 & 3420 & 4350 & 0 & 4824 & 3672 & 3474 \\ -2592 & -6660 & 0 & -5976 & -5940 & -7560 & 0 & -8388 & -6372 & -6048 \end{bmatrix}$.

b. Begin at the station of your group number, and apply the decoding matrix at this first station.

$$D_1 = \begin{bmatrix} -1 & -1 \\ 1 & \frac{1}{2} \end{bmatrix}$$

$$D_1 \cdot C = \begin{bmatrix} -1 & -1 \\ 1 & \frac{1}{2} \end{bmatrix} \cdot \begin{bmatrix} 1500 & 3840 & 0 & 3444 & 3420 & 4350 & 0 & 4824 & 3672 & 3474 \\ -2592 & -6660 & 0 & -5976 & -5940 & -7560 & 0 & -8388 & -6372 & -6048 \end{bmatrix}$$

$$= \begin{bmatrix} 1092 & 2820 & 0 & 2352 & 2520 & 3210 & 0 & 3564 & 2700 & 2574 \\ 204 & 510 & 0 & 456 & 450 & 570 & 0 & 630 & 486 & 450 \end{bmatrix}$$

c. Proceed to the next station in numerical order; if you are at Station 6, proceed to Station 1. Apply the decoding matrix at this second station.

$$D_2 = \begin{bmatrix} \frac{1}{6} & 0 \\ 0 & \frac{1}{3} \end{bmatrix}$$

$$D_2 \cdot D_1 \cdot C = \begin{bmatrix} \frac{1}{6} & 0 \\ 0 & \frac{1}{3} \end{bmatrix} \cdot \begin{bmatrix} 1092 & 2820 & 0 & 2352 & 2520 & 3210 & 0 & 3564 & 2700 & 2574 \\ 204 & 510 & 0 & 456 & 450 & 570 & 0 & 630 & 486 & 450 \end{bmatrix}$$

$$= \begin{bmatrix} 182 & 470 & 0 & 422 & 420 & 535 & 0 & 594 & 450 & 429 \\ 68 & 170 & 0 & 152 & 150 & 150 & 0 & 210 & 162 & 150 \end{bmatrix}$$

d. Proceed to the next station in numerical order; if you are at Station 6, proceed to Station 1. Apply the decoding matrix at this third station.

$$D_3 = \begin{bmatrix} \frac{1}{3} & -\frac{1}{3} \\ -\frac{1}{3} & \frac{4}{3} \end{bmatrix}$$

$$D_3 \cdot D_2 \cdot D_1 \cdot C = \begin{bmatrix} \frac{1}{3} & -\frac{1}{3} \\ -\frac{1}{3} & \frac{4}{3} \end{bmatrix} \cdot \begin{bmatrix} 182 & 470 & 0 & 422 & 420 & 535 & 0 & 594 & 450 & 429 \\ 68 & 170 & 0 & 152 & 150 & 150 & 0 & 210 & 162 & 150 \end{bmatrix}$$

$$= \begin{bmatrix} 38 & 100 & 0 & 90 & 90 & 115 & 0 & 128 & 96 & 93 \\ 30 & 70 & 0 & 62 & 60 & 75 & 0 & 82 & 66 & 57 \end{bmatrix}$$

e. Proceed to the next station in numerical order; if you are at Station 6, proceed to Station 1. Apply the decoding matrix at this fourth station.

$$D_4 = \begin{bmatrix} \frac{1}{2} & -\frac{1}{2} \\ -\frac{3}{2} & \frac{5}{2} \end{bmatrix}$$

$$D_4 \cdot D_3 \cdot D_2 \cdot D_1 \cdot C = \begin{bmatrix} \frac{1}{2} & -\frac{1}{2} \\ -\frac{3}{2} & \frac{5}{2} \end{bmatrix} \cdot \begin{bmatrix} 38 & 100 & 0 & 90 & 90 & 115 & 0 & 128 & 96 & 93 \\ 30 & 70 & 0 & 62 & 60 & 75 & 0 & 82 & 66 & 57 \end{bmatrix}$$

$$= \begin{bmatrix} 4 & 15 & 0 & 14 & 15 & 20 & 0 & 23 & 15 & 18 \\ 18 & 25 & 0 & 20 & 15 & 15 & 0 & 13 & 21 & 3 \end{bmatrix}$$

f. Decode your message.

The numerical message is 4, 15, 0, 14, 15, 20, 0, 23, 15, 18, 18, 25, 0, 20, 15, 15, 0, 13, 21, 3, *which represents the characters "DO NOT WORRY TOO MUCH."*

3. Sydnie was in Group 1 and tried to decode her message by calculating the matrix $(D_1 \cdot D_2 \cdot D_3 \cdot D_4)$ and then multiplying $(D_1 \cdot D_2 \cdot D_3 \cdot D_4) \cdot C$. This produced the matrix

$$M = \begin{bmatrix} \frac{10526}{3} & \frac{27020}{3} & 0 & \frac{24242}{3} & 8030 & \frac{30655}{3} & 0 & 11336 & 8616 & 8171 \\ -1455 & -3735 & 0 & -3351 & -3330 & -\frac{8475}{2} & 0 & -4701 & -3573 & -\frac{6177}{2} \end{bmatrix}.$$

a. How did she know that she made a mistake?

If Sydnie had properly decoded her message, all entries in the matrix M would be integers between 0 and 26.

b. Matrix C was encoded using matrices E_1, E_2, E_3 and E_4, where D_1 decodes a message encoded by E_1, D_2 decodes a message encoded by E_2 and so on. What is the relationship between matrices E_1 and D_1, between E_2 and D_2, etc.?

Matrices E_1 and D_1 are inverse matrices, as are E_2 and D_2, E_3, and D_3 and so on.

c. The matrix that Sydnie received was encoded by $C = E_1 \cdot E_2 \cdot E_3 \cdot E_4 \cdot M$. Explain to Sydnie how the decoding process works to recover the original matrix M, and devise a correct method for decoding using multiplication by a single decoding matrix.

Since $C = E_1 \cdot E_2 \cdot E_3 \cdot E_4 \cdot M$, we can recover the original matrix M by multiplying both sides of this equation by the proper decoding matrix at each step, remembering that $D_1 \cdot E_1 = I$, $D_2 \cdot E_2 = I$, etc.

$$\begin{aligned} C &= E_1 \cdot E_2 \cdot E_3 \cdot E_4 \cdot M \\ D_1 \cdot C &= D_1 \cdot (E_1 \cdot E_2 \cdot E_3 \cdot E_4 \cdot M) \\ &= (D_1 \cdot E_1) \cdot (E_2 \cdot E_3 \cdot E_4 \cdot M) \\ &= I \cdot (E_2 \cdot E_3 \cdot E_4 \cdot M) \\ &= (E_2 \cdot E_3 \cdot E_4 \cdot M) \\ D_2 \cdot D_1 \cdot C &= D_2 \cdot (E_2 \cdot E_3 \cdot E_4 \cdot M) \\ &= (D_2 \cdot E_2) \cdot (E_3 \cdot E_4 \cdot M) \\ &= I \cdot (E_3 \cdot E_4 \cdot M) \\ &= (E_2 \cdot E_3 \cdot E_4 \cdot M) \\ D_3 \cdot D_2 \cdot D_1 \cdot C &= D_3 \cdot (E_3 \cdot E_4 \cdot M) \\ &= (D_3 \cdot E_3) \cdot (E_4 \cdot M) \\ &= I \cdot (E_4 \cdot M) \\ &= E_4 \cdot M \\ D_4 \cdot D_3 \cdot D_2 \cdot D_1 \cdot C &= D_4 \cdot (E_4 \cdot M) \\ &= (D_4 \cdot E_4) \cdot M \\ &= I \cdot M \\ &= M. \end{aligned}$$

Since matrix multiplication is associative, this means that $M = (D_4 \cdot D_3 \cdot D_2 \cdot D_1) \cdot C$.

d. Apply the method you devised in part (c) to your group's message to verify that it works.

$$(D_4 \cdot D_3 \cdot D_2 \cdot D_1) = \begin{bmatrix} \frac{1}{2} & -\frac{1}{2} \\ -\frac{3}{2} & \frac{5}{2} \end{bmatrix} \cdot \begin{bmatrix} \frac{1}{3} & -\frac{1}{3} \\ -\frac{1}{3} & \frac{4}{3} \end{bmatrix} \cdot \begin{bmatrix} \frac{1}{6} & 0 \\ 0 & \frac{1}{3} \end{bmatrix} \cdot \begin{bmatrix} -1 & -1 \\ 1 & \frac{1}{2} \end{bmatrix}$$
$$= \begin{bmatrix} \frac{1}{3} & -\frac{5}{6} \\ -\frac{4}{3} & \frac{23}{6} \end{bmatrix} \cdot \begin{bmatrix} -\frac{1}{6} & -\frac{1}{6} \\ \frac{1}{3} & \frac{1}{6} \end{bmatrix} = \begin{bmatrix} -\frac{1}{3} & -\frac{7}{36} \\ \frac{3}{2} & \frac{31}{36} \end{bmatrix}$$

So,

$$(D_4 \cdot D_3 \cdot D_2 \cdot D_1) \cdot C$$
$$= \begin{bmatrix} -\frac{1}{3} & -\frac{7}{36} \\ \frac{3}{2} & \frac{31}{36} \end{bmatrix} \cdot \begin{bmatrix} 1500 & 3840 & 0 & 3444 & 3420 & 4350 & 0 & 4824 & 3672 & 3474 \\ -2592 & -6660 & 0 & -5976 & -5940 & -7560 & 0 & -8388 & -6372 & -6048 \end{bmatrix}$$
$$= \begin{bmatrix} 4 & 15 & 0 & 14 & 15 & 20 & 0 & 23 & 15 & 18 \\ 18 & 25 & 0 & 20 & 15 & 15 & 0 & 13 & 21 & 3 \end{bmatrix}.$$

This is the same decoded message that we found in Exercise 2, part (f).

Exercise 4 (optional, 8 minutes)

The encoded phrase in this exercise is "RAMANUJAN." Srinivasa Ramanujan (1887–1920) was a self-taught mathematician from India who made significant contributions to many branches of mathematics, particularly analysis and number theory, compiling thousands of mathematical results. Although he died young, he is widely considered to be one of the greatest mathematicians of his time.

The original message is stored in matrix $M = \begin{bmatrix} 18 & 1 & 13 \\ 1 & 14 & 21 \\ 10 & 1 & 14 \end{bmatrix}$, and the matrix used to encode the message is $E = \begin{bmatrix} 1 & 2 & 1 \\ -1 & 0 & 2 \\ 1 & 1 & -1 \end{bmatrix}$. In this optional exercise, students need to reason through the process of encoding and decoding to recover a missing entry in the decoding matrix when the encoding matrix is unknown. Use this exercise as an extension for students who have finished the previous exercises quickly.

4. **You received a coded message in the matrix $C = \begin{bmatrix} 30 & 30 & 69 \\ 2 & 1 & 15 \\ 9 & 14 & 20 \end{bmatrix}$. However, the matrix D that will decode this message has been corrupted, and you do not know the value of entry d_{12}. You know that all entries in matrix D are integers. Using x to represent this unknown entry, the decoding matrix D is given by $D = \begin{bmatrix} 2 & x & -4 \\ -1 & 2 & 3 \\ 1 & -1 & -2 \end{bmatrix}$. Decode the message in matrix C.**

Decoding the message requires that we multiply $D \cdot C$:

$$D \cdot C = \begin{bmatrix} 2 & x & -4 \\ -1 & 2 & 3 \\ 1 & -1 & -2 \end{bmatrix} \cdot \begin{bmatrix} 30 & 30 & 69 \\ 2 & 1 & 15 \\ 9 & 14 & 20 \end{bmatrix}$$
$$= \begin{bmatrix} 24 + 2k & 4 + x & 58 + 15x \\ 1 & 14 & 21 \\ 10 & 1 & 14 \end{bmatrix}.$$

Since we know all entries are integers and that the entries represent letters, we know that

$$0 \leq 24 + 2x \leq 26$$
$$0 \leq 4 + x \leq 26$$
$$0 \leq 58 + 15x \leq 26.$$

Solving these inequalities gives

$$-12 \leq x \leq 1$$
$$-4 \leq x \leq 22$$
$$-\frac{58}{15} \leq x \leq -\frac{32}{15}.$$

Because we know that x is an integer, the third inequality becomes $-3 \leq x \leq -3$, so we know that $x = 3$. Then the decoded message is

$$D \cdot C = \begin{bmatrix} 24 + 2(-3) & 4 + (-3) & 58 + 15(-3) \\ 1 & 14 & 21 \\ 10 & 1 & 14 \end{bmatrix};$$

thus,

$$D \cdot C = \begin{bmatrix} 18 & 1 & 13 \\ 1 & 14 & 21 \\ 10 & 1 & 14 \end{bmatrix},$$

and the decoded message is "RAMANUJAN."

Closing (3 minutes)

Ask students to write a brief answer to the question, "How do matrix inverses make encoding and decoding messages possible?" Then, have students share responses with a partner before sharing responses as a class.

- How do matrix inverses make encoding and decoding messages possible?
  - *If an $n \times n$ matrix E is invertible, then it can be used to encode a message. We store the message in a matrix M, where M has n rows, and then encode it by multiplying $E \cdot M$. To decode the message, we multiply $E^{-1} \cdot (E \cdot M) = (E^{-1} \cdot E) \cdot M = I \cdot M = M$.*

Exit Ticket (4 minutes)

The message encoded in the problem in the Exit Ticket is "HYPATIA." Hypatia (Hy-pay-shuh) of Alexandria (born between 350–370 CE, died 415 CE) is one of the earliest known female mathematicians. She was the head of the Neoplatonic School in Alexandria, Egypt, and the head of the Library of Alexandria. She was murdered in a religious conflict. None of her mathematical works have survived.

Name _____ Date _____

Lesson 13: Using Matrix Operations for Encryption

Exit Ticket

Morgan used matrix $E = \begin{bmatrix} 1 & -2 \\ -1 & 3 \end{bmatrix}$ to encode the name of her favorite mathematician in the message

$$-32, 7, 14, 1, 52, 2, -13, -1.$$

a. How can you tell whether or not her message can be decoded?

b. Decode the message, or explain why the original message cannot be recovered.

Exit Ticket Sample Solutions

Morgan used matrix $E = \begin{bmatrix} 1 & -2 \\ -1 & 3 \end{bmatrix}$ to encode the name of her favorite mathematician in the message

$$-32, 7, 14, 1, 52, 2, -13, -1.$$

a. How can you tell whether or not her message can be decoded?

Since the matrix E has determinant $\det(E) = 3 - 2 = 1$, we know that $\det(E) \neq 0$, so then a decoding matrix $D = E^{-1}$ exists.

b. Decode the message, or explain why the original message cannot be recovered.

First, we place the coded message into a 2×4 matrix C. Using $D = E^{-1} = \begin{bmatrix} 3 & 2 \\ 1 & 1 \end{bmatrix}$, we have

$$\begin{aligned} M &= D \cdot C \\ &= \begin{bmatrix} 3 & 2 \\ 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} -32 & 7 & 14 & 1 \\ 52 & 2 & -13 & -1 \end{bmatrix} \\ &= \begin{bmatrix} -96 + 104 & 21 + 4 & 42 - 26 & 3 - 2 \\ -32 + 52 & 7 + 2 & 14 - 13 & 1 - 1 \end{bmatrix} \\ &= \begin{bmatrix} 8 & 25 & 16 & 1 \\ 20 & 9 & 1 & 0 \end{bmatrix}. \end{aligned}$$

The decoded message is "HYPATIA."

Problem Set Sample Solutions

Problems 1–4 are optional as they are practice on skills previously taught and assessed. Problems 6–9 allow students to practice the use of matrix multiplication for coding and decoding messages.

1. Let $A = \begin{bmatrix} 1 & 3 \\ 2 & 5 \end{bmatrix}$, $B = \begin{bmatrix} -2 & 7 \\ 3 & -4 \end{bmatrix}$, $C = \begin{bmatrix} -5 & 3 \\ 2 & -1 \end{bmatrix}$, $Z = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$, and $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$. Evaluate the following.

a. $A + B$

$$\begin{bmatrix} -1 & 10 \\ 5 & 1 \end{bmatrix}$$

b. $B + A$

$$\begin{bmatrix} -1 & 10 \\ 5 & 1 \end{bmatrix}$$

c. $A + (B + C)$

$$\begin{bmatrix} -6 & 13 \\ 7 & 0 \end{bmatrix}$$

d. $(A + B) + C$

$$\begin{bmatrix} -6 & 13 \\ 7 & 0 \end{bmatrix}$$

e. $A + I$

$$\begin{bmatrix} 2 & 3 \\ 2 & 6 \end{bmatrix}$$

f. $A + Z$

$$\begin{bmatrix} 1 & 3 \\ 2 & 5 \end{bmatrix}$$

g. $A \cdot Z$

$$\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

h. $Z \cdot A$

$$\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

i. $I \cdot A$

$$\begin{bmatrix} 1 & 3 \\ 2 & 5 \end{bmatrix}$$

j. $A \cdot B$

$$\begin{bmatrix} 7 & -5 \\ 11 & -6 \end{bmatrix}$$

k. $B \cdot A$

$$\begin{bmatrix} 12 & 29 \\ -5 & -11 \end{bmatrix}$$

l. $A \cdot C$

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

m. $C \cdot A$

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

n. $A \cdot B + A \cdot C$

$$\begin{bmatrix} 8 & -5 \\ 11 & -5 \end{bmatrix}$$

o. $A \cdot (B + C)$

$$\begin{bmatrix} 8 & -5 \\ 11 & -5 \end{bmatrix}$$

p. $A \cdot B \cdot C$

$$\begin{bmatrix} -45 & 26 \\ -67 & 39 \end{bmatrix}$$

q. $C \cdot B \cdot A$

$$\begin{bmatrix} -75 & -178 \\ 29 & 69 \end{bmatrix}$$

r. $A \cdot C \cdot B$

$$\begin{bmatrix} -2 & 7 \\ 3 & -4 \end{bmatrix}$$

s. $\det(A)$

$$-1$$

t. $\det(B)$

$$-13$$

u. $\det(C)$

$$-1$$

v. $\det(Z)$

$$0$$

w. $\det(I)$

$$1$$

x. $\det(A \cdot B \cdot C)$

$$-13$$

y. $\det(C \cdot B \cdot A)$

-13

2. For any 2×2 matrix A and any real number k, show that if $kA = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$, then $k = 0$ or $A = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$.

Let $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$; then $kA = \begin{bmatrix} ka & kb \\ kc & kd \end{bmatrix}$. Suppose that $kA = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$.

Case 1: Suppose $k \neq 0$. Then $ka = 0, kb = 0, kc = 0$, and $kd = 0$; all imply that $a = b = c = d = 0$. Thus, if $k \neq 0$, then $A = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$.

Case 2: Suppose that $A \neq \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$. Then at least one of a, b, c and d is not zero, so $ka = 0, kb = 0, kc = 0$, and $kd = 0$ imply that $k = 0$.

Thus, if $kA = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$, then either $k = 0$ or $A = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$.

3. Claire claims that she multiplied $A = \begin{bmatrix} -3 & 2 \\ 0 & 4 \end{bmatrix}$ by another matrix X and obtained $\begin{bmatrix} -3 & 2 \\ 0 & 4 \end{bmatrix}$ as her result. What matrix did she multiply by? How do you know?

She multiplied A by the multiplicative identity matrix $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$. Since the product is a 2×2 matrix, we know that X is a 2×2 matrix of the form $= \begin{bmatrix} a & b \\ c & d \end{bmatrix}$. Multiplying $A \cdot X$ gives $A \cdot X = \begin{bmatrix} -3a + 2c & -3b + 2d \\ 0a + 4c & 0b + 4d \end{bmatrix}$. Since $A \cdot X = A$, we have the following system of equations:

$$\begin{aligned} -3a + 2c &= -3 \\ -3b + 2d &= 2 \\ 0a + 4c &= 0 \\ 0b + 4d &= 4. \end{aligned}$$

The third and fourth equations give $c = 0$ and $d = 1$, respectively, and substituting into the first two equations gives $-3a = -3$ and $-3b + 2 = 2$. Thus, $a = 1$ and $b = 0$, and the matrix X must be $X = I$.

4. Show that the only matrix B such that $A + B = A$ is the zero matrix.

Let $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ and $B = \begin{bmatrix} x & y \\ z & w \end{bmatrix}$; then we have $A + B = \begin{bmatrix} a + x & b + y \\ c + z & d + w \end{bmatrix}$, $a + x = a$, $b + y = b$, $c + z = c$, and $d + w = d$. In each case, solving for the elements of B, we find that $B = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$.

5. A 2×2 matrix of the form $\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$ is a *diagonal* matrix. Daniel calculated

$$\begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix} \cdot \begin{bmatrix} 2 & 3 \\ 5 & -3 \end{bmatrix} = \begin{bmatrix} 4 & 6 \\ 10 & -6 \end{bmatrix}$$
$$\begin{bmatrix} 2 & 3 \\ 5 & -3 \end{bmatrix} \cdot \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix} = \begin{bmatrix} 4 & 6 \\ 10 & -6 \end{bmatrix}$$

and concluded that if X is a diagonal matrix and A is any other matrix, then $X \cdot A = A \cdot X$.

a. Is there anything wrong with Daniel's reasoning? Prove or disprove that if X is a diagonal 2×2 matrix, then $X \cdot A = A \cdot X$ for any other matrix A.

Yes, there is something wrong with Daniel's reasoning. A single example does not establish that a statement is true, and the example he calculated used a special case of a diagonal matrix in which the entries on the main diagonal are equal.

If $A = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$ and $X = \begin{bmatrix} 2 & 0 \\ 0 & 3 \end{bmatrix}$, then $X \cdot A = \begin{bmatrix} 2 & 4 \\ 9 & 12 \end{bmatrix}$ and $A \cdot X = \begin{bmatrix} 2 & 6 \\ 6 & 12 \end{bmatrix}$. Thus, it is not true that $X \cdot A = A \cdot X$ for all diagonal matrices X and all other matrices A.

b. For 3×3 matrices, Elda claims that only diagonal matrices of the form $X = \begin{bmatrix} c & 0 & 0 \\ 0 & c & 0 \\ 0 & 0 & c \end{bmatrix}$ satisfy $X \cdot A = A \cdot X$ for any other 3×3 matrix A. Is her claim correct?

Elda is correct since $X = \begin{bmatrix} c & 0 & 0 \\ 0 & c & 0 \\ 0 & 0 & c \end{bmatrix} = cI$. Then,

$$X \cdot A = cI \cdot A = c(I \cdot A) = cA = Ac = (A \cdot I)c = A \cdot (cI) = A \cdot X$$

for all matrices A.

6. Calvin encoded a message using $E = \begin{bmatrix} 2 & 2 \\ -1 & 3 \end{bmatrix}$, giving the coded message $4, 28, 42, 56, 2, -6, -1, 52$. Decode the message, or explain why the original message cannot be recovered.

Putting the message in a 2×4 matrix, we have $C = \begin{bmatrix} 4 & 28 & 42 & 56 \\ 2 & -6 & 1 & 52 \end{bmatrix}$. We can decode the message with $D = E^{-1} = \frac{1}{6-(-2)} \begin{bmatrix} 3 & -2 \\ 1 & 2 \end{bmatrix} = \begin{bmatrix} \frac{3}{8} & -\frac{2}{8} \\ \frac{1}{8} & \frac{2}{8} \end{bmatrix}$. Then the original message is found in message M:

$$M = D \cdot C = \begin{bmatrix} \frac{3}{8} & -\frac{2}{8} \\ \frac{1}{8} & \frac{2}{8} \end{bmatrix} \cdot \begin{bmatrix} 4 & 28 & 42 & 56 \\ 2 & -6 & -1 & 52 \end{bmatrix} = \begin{bmatrix} 1 & 12 & 16 & 8 \\ 1 & 2 & 5 & 20 \end{bmatrix}.$$

The original message is "ALPHABET."

7. Decode the message below using the matrix $D = \begin{bmatrix} 1 & 1 & -1 \\ -1 & 0 & 2 \\ 1 & 2 & 1 \end{bmatrix}$:

$$22, 17, 24, 9, -1, 14, -9, 34, 44, 64, 47, 77.$$

The decoded message is found by multiplying $\begin{bmatrix} 1 & 1 & -1 \\ -1 & 0 & 2 \\ 1 & 2 & 1 \end{bmatrix} \cdot \begin{bmatrix} 22 & 17 & 24 & 9 \\ -1 & 14 & -9 & 34 \\ 44 & 64 & 47 & 77 \end{bmatrix} = \begin{bmatrix} 3 & 18 & 25 & 16 \\ 20 & 15 & 7 & 18 \\ 1 & 16 & 8 & 25 \end{bmatrix}$. Then the message is "CRYPTOGRAPHY."

8. Brandon encoded his name with the matrix $E = \begin{bmatrix} 1 & 1 \\ 2 & 2 \end{bmatrix}$, producing the matrix $C = \begin{bmatrix} 6 & 33 & 15 & 14 \\ 12 & 66 & 30 & 28 \end{bmatrix}$. Decode the message, or explain why the original message cannot be recovered.

Brandon used a matrix that is not invertible. The original matrix cannot be recovered.

9. Janelle used the encoding matrix $E = \begin{bmatrix} 1 & 2 \\ 1 & -1 \end{bmatrix}$ to encode the message "FROG" by multiplying $C = \begin{bmatrix} 6 & 18 \\ 15 & 7 \end{bmatrix} \cdot \begin{bmatrix} 1 & 2 \\ 1 & -1 \end{bmatrix} = \begin{bmatrix} 24 & 30 \\ 22 & 37 \end{bmatrix}$. When Taylor decoded it, she computed $M = \begin{bmatrix} -1 & 2 \\ 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 24 & 30 \\ 22 & 37 \end{bmatrix} = \begin{bmatrix} 20 & 44 \\ 2 & -7 \end{bmatrix}$. What went wrong?

Janelle multiplied her matrices in the wrong order. When Janelle tried to decode the matrix $C = \begin{bmatrix} 24 & 30 \\ 22 & 37 \end{bmatrix}$ using the decoding matrix $D = \begin{bmatrix} 1 & 2 \\ 1 & -1 \end{bmatrix}^{-1}$, she ended up calculating

$$\begin{aligned} D \cdot C &= D \cdot M \cdot E \\ &= E^{-1} \cdot M \cdot E. \end{aligned}$$

Because matrix multiplication is not commutative, $E^{-1} \cdot M \cdot E \neq M$, Taylor was unable to recover the original message.