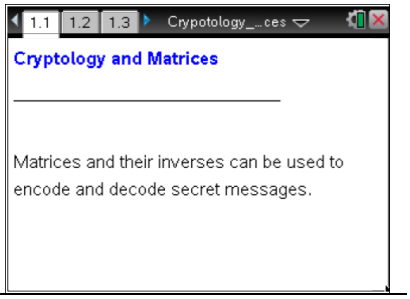
Cryptology and Matrices
Student Activity

Name _____

Class _____

Open the TI-Nspire document *Cryptology_and_Matrices.tns.*

In this activity, you will use matrices and their inverses to encode and decode messages.



Cryptology is the science of developing secret codes and using those codes for encrypting and decrypting data.[1] In June of 1929, an article written by Lester S. Hill appeared in the American Mathematical Monthly. This was the first article that linked the fields of algebra and cryptology.[2]

Today, governments use sophisticated methods of coding and decoding messages. One type of code, which is extremely difficult to break, makes use of a large matrix to encode a message. The receiver of the message decodes it using the inverse of the matrix. This first matrix is called the encoding matrix and its inverse is called the decoding matrix.[3]

In this activity, we will use a simple method for encoding a message by first assigning a numeral to each letter of the alphabet. We will represent the letter A with the numeral 1 and continue to the letter Z which will be assigned the numeral 26. We will also assign the numeral 0 to a space in the message.

For example, using the chart to the right, the word

SYSTEM

can be written using numerals as

19 25 19 20 5 13

and then recorded in a matrix as

$$\begin{bmatrix} 19 & 25 \\ 19 & 20 \\ 5 & 13 \end{bmatrix}.$$

_ = 0	**I** = 9	**R** = 18
A = 1	**J** = 10	**S** = 19
B = 2	**K** = 11	**T** = 20
C = 3	**L** = 12	**U** = 21
D = 4	**M** = 13	**V** = 22
E = 5	**N** = 14	**W** = 23
F = 6	**O** = 15	**X** = 24
G = 7	**P** = 16	**Y** = 25
H = 8	**Q** = 17	**Z** = 26

[1] http://www.answers.com/topic/cryptology

[2] http://www.glassblower.info/cryptosystems-journal/HILL29.HTM

[3] http://aix1.uottawa.ca/~jkhoury/cryptography.htm

Move to page 1.2.

Press ctrl ▶ and ctrl ◀ to navigate through the lesson.

1. To protect this message as it is transmitted, it is *encoded* by multiplying the message matrix by an encoding matrix, such as $\begin{bmatrix} 4 & 3 \\ 2 & 2 \end{bmatrix}$.

   a. Enter the following information into the matrices on Page 1.2. Press tab to move from one entry to the next.

   $$\begin{bmatrix} 19 & 25 \\ 19 & 20 \\ 5 & 13 \end{bmatrix} \cdot \begin{bmatrix} 4 & 3 \\ 2 & 2 \end{bmatrix}$$

   b. Press enter to find the product and fill in the spaces provided below.

   $$\begin{bmatrix} 19 & 25 \\ 19 & 20 \\ 5 & 13 \end{bmatrix} \cdot \begin{bmatrix} 4 & 3 \\ 2 & 2 \end{bmatrix} = \begin{bmatrix} \square & \square \\ \square & \square \\ \square & \square \end{bmatrix}$$

   c. Fill in the numerals for the new message:

   _____ _____ _____ _____ _____ _____.

The receiver of this message can retrieve the original message by *decoding* it by using the *inverse* of the coding matrix.

The **inverse** of a 2 X 2 matrix $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, provided $\det(A) \neq 0$, is $A^{-1} = \frac{1}{\det(A)} \cdot \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$.

2. What is the decoding matrix (the inverse of the encoding matrix)?

   (Recall that $\det\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right) = ad - bc$.)

   Fill in the information below.

   $$\begin{bmatrix} 4 & 3 \\ 2 & 2 \end{bmatrix}^{-1} = \frac{1}{\square} \cdot \begin{bmatrix} \square & \square \\ \square & \square \end{bmatrix} = \begin{bmatrix} \square & \square \\ \square & \square \end{bmatrix}$$

Move to page 1.3.

3. Test the decoding matrix to verify that these matrices are inverses. (When you multiply a matrix by its inverse, in either direction, their product will be the identity matrix.) Type the appropriate entries into the matrix given on Page 1.3. Change the order of the multiplication to verify that the two matrices are inverses, and record both of the results below.

$$\begin{bmatrix} \square & \square \\ \square & \square \end{bmatrix} \cdot \begin{bmatrix} \square & \square \\ \square & \square \end{bmatrix} = \begin{bmatrix} \square & \square \\ \square & \square \end{bmatrix}$$

$$\begin{bmatrix} \square & \square \\ \square & \square \end{bmatrix} \cdot \begin{bmatrix} \square & \square \\ \square & \square \end{bmatrix} = \begin{bmatrix} \square & \square \\ \square & \square \end{bmatrix}$$

Move to page 1.4.

4. a. Multiply the encoded message by the decoding matrix. Record the results below.

$$\begin{bmatrix} \square & \square \\ \square & \square \\ \square & \square \end{bmatrix} \cdot \begin{bmatrix} \square & \square \\ \square & \square \end{bmatrix} = \begin{bmatrix} \square & \square \\ \square & \square \\ \square & \square \end{bmatrix}$$

   b. Use the chart given at the beginning of the worksheet to see if the decoded message is the same as the original one.

5. Decode the message **18 27 51 81 37 58 60 100 18 27 85 137 59 93 51 79**, which was encoded with encoding matrix $\begin{bmatrix} 2 & 3 \\ 3 & 5 \end{bmatrix}$.

   - For this example, you will enter your own matrices into your TI-Nspire. The first matrix will have 8 rows and 2 columns. The second matrix will have 2 rows and 2 columns.
   - Press ctrl doc ▾ **> Add Calculator**.
   - Select **MENU > Matrix & Vector > Create > Matrix**, and choose a matrix with 8 rows and 2 columns. Press OK or enter.
   - Press the right arrow (▶) twice to move outside the matrix.
   - Insert a multiplication symbol to the right of the 8 X 2 matrix.
   - Repeat the process for entering a matrix and choose a matrix with 2 rows and 2 columns.

- Enter the data for the encoded message into the first matrix and the data for the decoding matrix into the second.
- Press tab to move from one entry to the next. (Be sure that you are multiplying the given message by the decoding matrix, which is the inverse of the encoding message.)
- Press enter to find the product.

a. What is the decoding matrix (the inverse of the encoding matrix)? $\begin{bmatrix} \square & \square \\ \square & \square \end{bmatrix}$

b. What is the matrix that has been decoded? $\begin{bmatrix} \square & \square \\ \square & \square \\ \square & \square \\ \square & \square \\ \square & \square \\ \square & \square \\ \square & \square \\ \square & \square \end{bmatrix}$

c. To help you decode the message, write out the numerals from the decoded message.

_____ _____ _____ _____ _____ _____ _____ _____ _____ _____ _____

_____ _____ _____ _____ _____

d. What does the message say? (Be sure to use the chart at the beginning of this activity to decipher the results.)