



Teacher-to-Teacher

Video Series
for Secondary Educators

TITLE: Codes – Hiding Information With Matrices

PRIMARY SUBJECT AREAS: Mathematics

GRADE LEVELS: 11-12

OVERVIEW: In this lesson, everyday uses of codes will be explored, as well as the role codes have played and still play in national security. Then, students will learn how to use matrices and matrix equations to encode and decode information.

APPROXIMATE DURATION: 2 fifty minute class periods, 4 fifty minute lessons

LOUISIANA CONTENT STANDARDS:

<http://www/DOE/assessment/standards/MATH.pdf>

Algebra

A-1-H demonstrating the ability to translate real-world situations (e.g., distance versus time relationships, population growth, growth functions for diseases, growth of minimum wage, auto insurance tables) into algebraic expressions, equations, and inequalities and vice versa

A-4-H solving algebraic equations and inequalities using a variety of techniques with the appropriate tools (e.g., hand-held manipulatives, graphing calculator, symbolic manipulator, or pencil and paper)

Discrete Math

D-9-H using discrete math to model real-life situations (e.g., fair games or elections, map coloring)

GLEs Addressed

Grade 9

- 9. Model real-life situations using linear expressions, equations, and inequalities (A-1-H) (D-2-H) (P-5-H)
- 16. Interpret and solve systems of linear equations using graphing, substitution, elimination, with and without technology, and matrices using technology (A-4-H)

Grade 10

- 25. Use discrete math to model real life situations (e.g., fair games, elections) (D-9-H)

EDUCATIONAL TECHNOLOGY GUIDELINES:

<http://www/DOE/LCET/curric/k12stand.pdf>

Technology Research Tools

- Demonstrate knowledge and skills of Internet use and other resources consistent with acceptable use policies including the legal consequences of plagiarism and the need for authenticity in student work through and understanding of copyright issues.

Social, Ethical, and Human Issues

- Demonstrate and advocate legal and ethical behaviors among peers, family, and community regarding the use of technology and information.

Technology Productivity Tools

- Refine knowledge and enhance skills in keyboarding, word processing, desktop publishing, spreadsheets, databases, multimedia, and telecommunications in preparing and presenting classroom projects.

INTERDISCIPLINARY CONNECTIONS:

Social Studies

History

OBJECTIVES:

1. The student will be able to encode information using transposition ciphers.
2. The student will be able to decode information using transposition ciphers.
3. The student will be able to create their own 2 x 2 code matrices, each with a determinant of one.
4. The student will be able to encode information by multiplying matrices (Hill method).
5. The student will be able to decode information by solving matrix equations (Hill method).
6. The student will be able to explain connections between history and mathematics for a portfolio entry.

LESSON MATERIALS AND RESOURCES:

Matrices and the Graphing Calculator (Student and Teacher)

Transposition Ciphers – Teacher Notes

Hill Codes – Teacher

TECHNOLOGY TOOLS AND MATERIALS:

graphing calculators

computers

BACKGROUND INFORMATION:

Previous experiences in stating the dimensions of a matrix and finding the inverse of a 2x2 matrix are a definite plus. It is also helpful if students already know how to enter matrices into a graphing calculator.

LESSON PROCEDURES:

Day One

1. Give a brief history of codes and the role they have played and still play in national security. *Codes Galore* and *For All Practical Purposes* are excellent resources.
2. Discuss everyday uses of codes (house alarms, ATMs, Zip codes, ISBN, UPC, etc).
3. Assist students in encoding information using matrices of various dimensions.
4. Have the students encode enough messages to feel comfortable with the procedure.
5. Ask students to decode information given the dimensions and matrix rule.
6. Allow students to encode their own messages, swap it with a partner for decoding, and check the results.
7. Discuss the limitations of transposition ciphers.

Day Two

1. Introduce the Hill method of encoding information using matrix equations, first by hand and then using the graphing calculator.
2. Students may need a brief review on finding the determinant and inverse of 2x2 matrices.
3. Again, have the students encode enough messages to feel comfortable with the procedure.

Day Three

1. Give the students an encoded message.
2. Let the students work together to devise a plan for decoding the information.
3. Each group should share its plan with the class and the class should provide feedback.
4. Ask for a volunteer to come to the front of the class to set up and solve the matrix equation in order to decode the message. Again, this can be done by hand or with a graphing calculator.
5. Allow students to encode information for the class to decode.
6. Discuss the limitations of Hill codes.

Day Four

1. Allow groups to use the Internet to explore the role codes have played and still play in national security.
2. For homework, each student will prepare a brief report of the group findings for his math portfolio.

ASSESSMENT PROCEDURES:

Informational Assessment

1. The teacher watches for the “deer in the headlights” look.
2. The teacher walks around to check on the progress of individual students and groups.

Formal Assessment

1. The teacher will place transposition ciphers and Hill codes on matrix quizzes and exams.

2. The teacher will grade the student portfolio entry describing a code not covered in class or on the role codes have played at some particular point in history.

ACCOMMODATIONS/MODIFICATIONS:

1. Students with physical handicaps may need a partner to enter the matrices into the graphing calculator.
2. Students with visual handicaps may need an enlarged copy of a numbered alphabet list.

REPRODUCIBLE MATERIALS:

Matrices and the Graphing Calculator (Casio and Texas Instruments)

Transposition Ciphers – Teacher Notes (Encoding and Decoding)

Hill Codes – Teacher Notes (Encoding and Decoding)

EXPLORATIONS AND EXTENSIONS:

1. Modular numbers and their links to ISBN codes, bank codes, airline tickets, UPC codes, money orders, and error detection
2. ZIP codes
3. Linear codes
4. Public-Key cryptography
5. Huffman codes

LESSON DEVELOPMENT RESOURCES:

Froelich, D., Froelich, G., & Malkevitch, J. (1993). Codes Galore. Lexington: COMAP.

Froelich, G., & Malkevitch, J. (1993). Loads Of Codes. Lexington: COMAP.

Meyer, W. (Ed.). (1997). Principles and Practice of Mathematics. New York: Springer.

Steen, L.A. (Ed.). (1997). For All Practical Purposes. New York: W.H. Freeman and Company.

REFLECTIONS:

Most of my students grew bored with the business applications of matrices. Codes provided a fun tie into history and the use of matrix equations. Make sure that you, the teacher, are comfortable with entering matrices and performing operations with them using the graphing calculator. Since you can't be in ten places at the same time to debug calculator problems, let the students work in groups and help each other.

CONTACT INFORMATION:

Carol Price

Robert E. Lee High School

cprice@ebrpss.k12.la.us

Matrices and the Graphing Calculator

Casio 9850Ga Plus

Entering Data into Matrices

- Use the right arrow key to get to the matrix icon (**MAT**)
- Press **EXE** to enter the matrix mode
- Press the right arrow key to enter the dimensions
- Press **EXE** after the correct dimensions have been entered
- Enter the first number and press **EXE** to enter each succeeding number
- Press **EXIT** to enter the second matrix

Computing With Matrices

- Press **MENU**
- Use the left arrow key to get to the **RUN** icon
- Press **OPTN** and **F2**
- Press **F1 ALPHA A SHIFT x⁻¹ X F1 ALPHA B**
The screen will show: $\text{Mat A}^{-1} \times \text{Mat B}$
- Press **EXE**

TI 83+

Entering Data into Matrices

- Press **2nd x⁻¹**
- Use the right arrow key to highlight the word **EDIT** and press **ENTER**
- Use the right arrow key to enter the dimensions
- Repeat the first three steps to enter the second matrix, but make sure to arrow down to matrix B

Computing With Matrices

- Press **2nd QUIT** to return to the blank screen
- Press **2nd x⁻¹ ENTER x⁻¹ X 2nd x⁻¹ 2 ENTER**
The screen will show: $[A]^{-1} * [B]$
- Press **ENTER**

Transposition Ciphers – Teacher Notes

Transposition ciphers provide a fun avenue for reviewing matrix dimensions. Like all ciphers, the intent is to hide information. The letters of the original message are not altered, but the order in which they are arranged is changed.

To change the order of the letters, write the original message in matrix form. The dimensions of the matrix are selected by the encoder. Unless the message is extremely long, generally two or three rows will suffice, as will three to five columns. In order to make the code difficult for enemies to decode, make sure the message is spread out over at least three matrices. The letter *q* is used as a filler when the message does not fill the last matrix.

Next, choose a key that describes how to read the columns. Lastly, write the coded text according to the key.

Encoding Information

Original Message: Studying codes is fun.

Step 1: Choose the dimensions of the matrices. For this example we will use 2x4 matrices.

Step 2: Write the original message in matrix form.

$$\begin{bmatrix} s & t & u & d \\ y & i & n & g \end{bmatrix} \begin{bmatrix} c & o & d & e \\ s & i & s & f \end{bmatrix} \begin{bmatrix} u & n & q & q \\ q & q & q & q \end{bmatrix}$$

Step 3: Choose a key for how to read the columns. For this example we will use the key C: 1 3 2 4.

Step 4: Write the encoded message.

Encoded Message: s y c s u q u n d s q q t i o i n q d g e f q q

Let's try to encode another message.

Original Message: The invasion begins on Wednesday at sunrise.

Step 1: Choose the dimensions of the matrices. This time we will use 3x5 matrices. and the key – C: 2 5 3 4 1.

Step 2: Write the original message in matrix form.

$$\begin{bmatrix} t & h & e & i & n \\ v & a & s & i & o \\ n & b & e & g & i \end{bmatrix} \begin{bmatrix} n & s & o & n & w \\ e & d & n & e & s \\ d & a & y & a & t \end{bmatrix} \begin{bmatrix} s & u & n & r & i \\ s & e & q & q & q \\ q & q & q & q & q \end{bmatrix}$$

Step 3: Choose a key for how to read the columns. The key for this example will be C: 2 5 3 4 1.

Step 4: Write the encoded message.

Encoded Message: habsdaueqnoiwstiqqeseonynqqiignearqqtvnnedssq

Decoding Information

In order to decode a transposition cipher, the decoder must know the matrix dimensions of the message and the key for how to read the columns. These two components must be sent either before or after the coded message is sent.

Coded Message: h w t g q q o o o h q q n m r n t q o e k i q q

2x4 matrices & key C: 3 4 1 2

Step 1: Determine the number of matrices used to hold the original message. Since there are 24 letters in the coded message and each matrix holds 8 letters, there will be 3 matrices.

Step 2: Fill in the 2x4 matrices using the key.

$$\begin{bmatrix} n & o & h & o \\ m & e & w & o \end{bmatrix} \begin{bmatrix} r & k & t & o \\ n & i & g & h \end{bmatrix} \begin{bmatrix} t & q & q & q \\ q & q & q & q \end{bmatrix}$$

Step 3: Write the original message by reading the rows of each matrix.

Decoded Message: no homework tonight

Try to decode the next message.

Coded Message: teltodorqeiescsowqhwbenemoqrlatotrqq

3x4 matrices & key C: 1 3 2 4

Step 1: Determine the number of matrices used to hold the original message. Since there are 31 letters in the coded message and each matrix holds 12 letters, there will be 3 matrices.

Step 2: Fill in the 3x4 matrices using the key.

$$\begin{bmatrix} t & h & e & r \\ e & w & i & l \\ l & b & e & a \end{bmatrix} \begin{bmatrix} t & e & s & t \\ o & n & c & o \\ d & e & s & t \end{bmatrix} \begin{bmatrix} o & m & o & r \\ r & o & w & q \\ q & q & q & q \end{bmatrix}$$

Step 3: Write the original message by reading the rows of each matrix.

Decoded Message: There will be a test on codes tomorrow.

Hill Codes

One of the earliest attempts to use mathematics to hide information was developed by Lester Hill. Mr. Hill developed a code system that used matrix multiplication as a means of hiding information.

$$\mathbf{Matrix\ A\ x\ Matrix\ B\ =\ Matrix\ C}$$

Matrix A is the square code matrix chosen by the encoder.

Matrix B is the original message in numerical form.

Matrix C is the encoded message.

Encoding Information

Original Message: Let the good times roll!

Step 1: Choose a square code matrix. If the decoder must break the code by hand, it is helpful to select a 2x2 matrix with a determinant of 1.

$$\text{Code Matrix: } \begin{bmatrix} 3 & 1 \\ 2 & 1 \end{bmatrix}$$

Step 2: Write the original message in 2x2 matrices.

$$\begin{bmatrix} l & e \\ t & t \end{bmatrix} \begin{bmatrix} h & e \\ g & o \end{bmatrix} \begin{bmatrix} o & d \\ t & i \end{bmatrix} \begin{bmatrix} m & e \\ s & r \end{bmatrix} \begin{bmatrix} o & l \\ l & q \end{bmatrix}$$

Step 3: Replace each letter with its numerical value (e.g., A = 1, B = 2, etc.) and write the result as one big matrix (2x10).

$$\text{Original Message: } \begin{bmatrix} 12 & 5 & 8 & 5 & 15 & 4 & 13 & 5 & 15 & 12 \\ 20 & 20 & 7 & 15 & 20 & 9 & 19 & 18 & 12 & 17 \end{bmatrix}$$

Step 4: Use matrix multiplication to encode the original message. This can be done by hand or with graphing calculators.

$$\mathbf{Code\ Matrix\ X\ Original\ Message\ =\ Encoded\ Message}$$

$$\begin{bmatrix} 3 & 1 \\ 2 & 1 \end{bmatrix} \begin{bmatrix} 12 & 5 & 8 & 5 & 15 & 4 & 13 & 5 & 15 & 12 \\ 20 & 20 & 7 & 15 & 20 & 9 & 19 & 18 & 12 & 17 \end{bmatrix} = \begin{bmatrix} 56 & 35 & 31 & 30 & 65 & 21 & 58 & 33 & 57 & 53 \\ 44 & 30 & 23 & 25 & 50 & 17 & 45 & 28 & 42 & 41 \end{bmatrix} = \text{Encoded Message}$$

Let's try to encode another message using the Hill method.

Original Message: Math is my favorite subject.

Step 1: Choose a square code matrix. Again, it is helpful to the decoder to create a matrix with a determinant of 1.

$$\text{Code Matrix: } \begin{bmatrix} 5 & 2 \\ 7 & 3 \end{bmatrix}$$

Step 2: Write the original message in matrix form.

$$\begin{bmatrix} m & a \\ t & h \end{bmatrix} \begin{bmatrix} i & s \\ m & y \end{bmatrix} \begin{bmatrix} f & a \\ v & o \end{bmatrix} \begin{bmatrix} r & i \\ t & e \end{bmatrix} \begin{bmatrix} s & u \\ b & j \end{bmatrix} \begin{bmatrix} e & c \\ t & q \end{bmatrix}$$

Step 3: Replace each letter with its numerical form (a = 1, b = 2, etc.) and write the result as one big matrix (2x12).

$$\text{Original Message: } \begin{bmatrix} 13 & 1 & 9 & 19 & 6 & 1 & 18 & 9 & 19 & 21 & 5 & 3 \\ 20 & 8 & 13 & 25 & 22 & 15 & 20 & 5 & 2 & 10 & 20 & 17 \end{bmatrix}$$

Step 4: Use matrix multiplication to encode the original message. This can be done by hand or with graphing calculators.

Code Matrix X Original Message = Encoded Message

$$\begin{bmatrix} 5 & 2 \\ 7 & 3 \end{bmatrix} \begin{bmatrix} 13 & 1 & 9 & 19 & 6 & 1 & 18 & 9 & 19 & 21 & 5 & 3 \\ 20 & 8 & 13 & 25 & 22 & 15 & 20 & 5 & 2 & 10 & 20 & 17 \end{bmatrix} = \begin{bmatrix} 105 & 21 & 71 & 145 & 74 & 35 & 130 & 55 & 99 & 125 & 65 & 49 \\ 151 & 31 & 102 & 208 & 108 & 52 & 186 & 78 & 139 & 177 & 95 & 72 \end{bmatrix}$$

Decoding Information

In order to decode a Hill message you must know the code matrix. Therefore, the code matrix should be sent either before or after the coded message is sent.

Encoded Message

$$\begin{bmatrix} 55 & 5 & -11 & 7 & 48 & 55 & 2 & 12 & 25 & 34 \\ -90 & -2 & 23 & -5 & -77 & -87 & -3 & -17 & -36 & -51 \end{bmatrix}$$

$$\text{Code Matrix: } \begin{bmatrix} 3 & -1 \\ -5 & 2 \end{bmatrix}$$

Step 1: Set up the Hill matrix equation.

Code Matrix x Original Message = Encoded Message

$$\begin{bmatrix} 3 & -1 \\ -5 & 2 \end{bmatrix} X = \begin{bmatrix} 55 & 5 & -11 & 7 & 48 & 55 & 2 & 12 & 25 & 34 \\ -90 & -2 & 23 & -5 & -77 & -87 & -3 & -17 & -36 & -51 \end{bmatrix}$$

Step 2: Solve the matrix equation by multiplying both sides of the equation by the inverse of the Code Matrix.

Inverse of Code Matrix x Code Matrix x Original Message = Inverse of Code Matrix x Encoded Message

Multiplying a matrix by its inverse yields the identity matrix. Any matrix times its identity is that same matrix, so the above equation can be simplified to:

Original Message = Inverse of Code Matrix x Encoded Message

$$\text{Original Message} = \begin{bmatrix} 20 & 8 & 1 & 9 & 19 & 23 & 1 & 7 & 14 & 17 \\ 5 & 19 & 14 & 20 & 9 & 14 & 1 & 9 & 17 & 17 \end{bmatrix}$$

Step 3: Replace each number with the letter it represents and write each letter in 2x2 matrices.

$$\text{Original Message} = \begin{bmatrix} t & h \\ e & s \end{bmatrix} \begin{bmatrix} a & i \\ n & t \end{bmatrix} \begin{bmatrix} s & w \\ i & n \end{bmatrix} \begin{bmatrix} a & g \\ a & i \end{bmatrix} \begin{bmatrix} n & q \\ q & q \end{bmatrix}$$

Original Message = The Saints win again!

Try to crack the following Hill code.

$$\text{Encoded Message: } \begin{bmatrix} 10 & 35 & 56 & 7 & 41 & 45 & 47 & 41 \\ 17 & 55 & 93 & 13 & 63 & 75 & 79 & 70 \end{bmatrix}$$

$$\text{Code Matrix: } \begin{bmatrix} 2 & 1 \\ 3 & 2 \end{bmatrix}$$

Step 1: Set up the Hill matrix equation.

$$\text{Code Matrix} \times \text{Original Message} = \text{Encoded Message}$$

$$\begin{bmatrix} 2 & 1 \\ 3 & 2 \end{bmatrix} \times \begin{bmatrix} 10 & 35 & 56 & 7 & 41 & 45 & 47 & 41 \\ 17 & 55 & 93 & 13 & 63 & 75 & 79 & 70 \end{bmatrix}$$

Step 2: Solve the matrix equation by multiplying both sides of the equation by the inverse of the Code Matrix.

$$\text{Inverse of Code Matrix} \times \text{Code Matrix} \times \text{Original Message} = \text{Inverse of Code Matrix} \times \text{Encoded Message}$$

Multiplying a matrix by its inverse yields the identity matrix. Any matrix times its identity is that same matrix, so the above equation can be simplified to:

$$\text{Original Message} = \text{Inverse of Code Matrix} \times \text{Encoded Message}$$

$$\text{Original Message} = \begin{bmatrix} 3 & 15 & 19 & 1 & 19 & 15 & 15 & 12 \\ 4 & 5 & 18 & 5 & 3 & 15 & 17 & 17 \end{bmatrix}$$

Step 3: Replace each number with the letter it represents and write each letter in 2x2 matrices.

$$\text{Original Message} = \begin{bmatrix} c & o \\ d & e \end{bmatrix} \begin{bmatrix} s & a \\ r & e \end{bmatrix} \begin{bmatrix} s & o \\ c & o \end{bmatrix} \begin{bmatrix} o & l \\ q & q \end{bmatrix}$$

$$\text{Original Message} = \text{Codes are so cool!}$$