INITIATE Lesson Plan: *Cryptography - Matrices*

Lesson plan at a glance...

Name	Cryptography using Matrices
Course	Algebra/Pre-calculus
Suggested grade	11th to 12th
Prerequisites	Basic knowledge of Matrix Operations.
Time	**Preparation:** 3 minutes **Instruction:** 75 minutes
Standards	*TPS:* (+) N.VM.8: Add, subtract, and multiply matrices of appropriate dimensions.

In this lesson plan…

- **Lesson Overview**
- **Materials and Equipment**
- **Preparation Tasks**
- **The Lesson**
- **Learning Objectives and Standards**
- **Additional Information and Resources**

Lesson Overview

With smart vehicles communicating with one another, there arises a need to make this communication secure. This is needed to prevent cars from being attacked by hackers and prevent passenger lives while driving on the road. While secure communication is needed by all smart vehicles, its most importance for vehicles carrying people with disabilities. From old age cryptographic techniques (such as Caesar's cipher) we have moved on to more complicated techniques such as RSA, AES and using matrices to for securing communication.

This lesson provides activities on cryptography such as Caesar's cipher and Cryptography using Matrices. Caesar's cipher is a shift or substitution cipher that replaces each character in the phrase with another character a fixed number of positions down the alphabet. With computers becoming more powerful such ciphers and methods can easily be broken and have become obsolete. Newer and more complicated methods have evolved, such as cryptography using matrices which changes the alphabets to numbers and use several matrix operations to encode the messages sent. This lesson provides engaging activities using both these methods for teaching standards related to matrices.

Driving Questions

Overarching Driving Questions for Bowsher Wide Project:

- How will autonomous vehicles affect the differently abled people of our society?

Lesson Specific Question:

- How can we make smart cars safer and more convenient for people with disabilities in the society?

Materials and Equipment

- □ For the student:
  - ○ *Required:*
    - ■ Tablet/Chromebook
    - ■ Calculator
    - ■ Pencil
    - ■ Scratch Paper
  - ○ *Optional:*
    - ■ *A handout for matrix multiplication*

Preparation Tasks

	• Check if the chromebook is sufficiently charged • Check if calculator is working • Check if everyone has scratch papers and pencils to work	3 minutes

The Lesson

Warm-up Activity	10 minutes
Activity 1: Caesar’s Cipher	20 minutes
Activity 2: Cryptography using matrices	25 minutes
Activity 3: Algorithm Writing	15 minutes
Wrap-up: Conclusions and Inferences	5 minutes

Warm-up Activity: Information Gathering and Brainstorming (10 minutes)

Activity:
The lesson starts off with the following question:

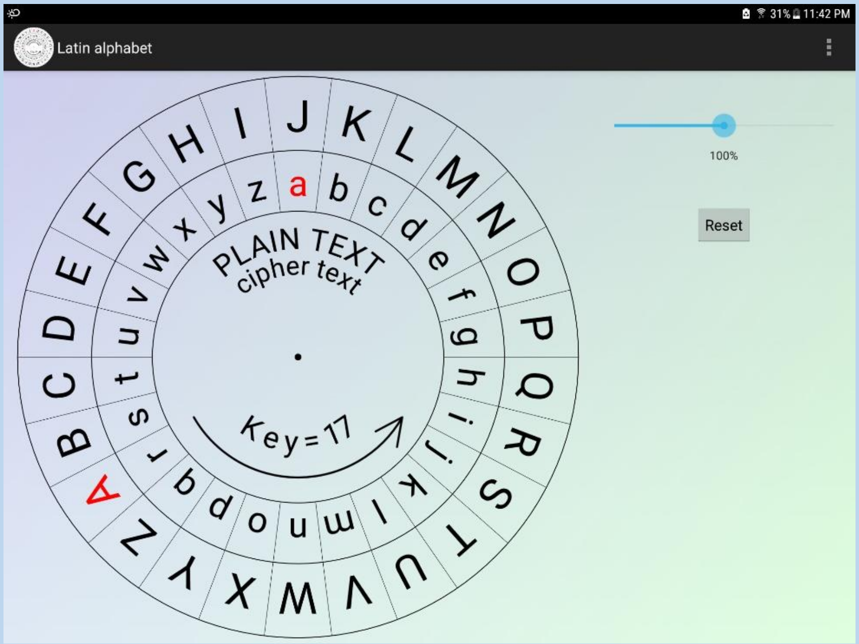
- How and why do you think smart cars communicate? - https://www.youtube.com/watch?v=44Oo-LGWjcg (CARJAM TV, 2015)
- How safe do you think is this communication?
  - Demo of a conversation between 2 people speaking a native language. This shows if only the sender and receiver know the language no one would be able to know the message sent.
- What do you understand by cryptography?
- Do you know any basic cryptographic methods?

Activity 1: Caesar's Cipher (20 minutes)

Problem Statement: Julius Caesar made this cipher to exchange messages of military importance. It is also known as shift or substitution cipher. If they were to be used for secure communication, how would they function?
Suggestion: Divide the class in groups of 2. Each group will have one Chromebook.

Part 1: Encoding (2 mins)
Question: If the plaintext message to be sent is JULIUS CAESAR, find the cipher text if the key is +17.
Solution:

Use the app on the Chromebook 'Caesar Cipher Disk' and move the outer wheel to the right so that the key becomes +17.



Map each character of JULIUS CAESAR on the outer wheel to that on the inner wheel. It will come out to be **ZKBYKI SQUIQH**.

J + 17 = Z, U + 17 = K, L + 17 = B, I + 17 = Y, S + 17 = I, C + 17 = S, A + 17 = Q, E + 17 = U, R + 17 = H

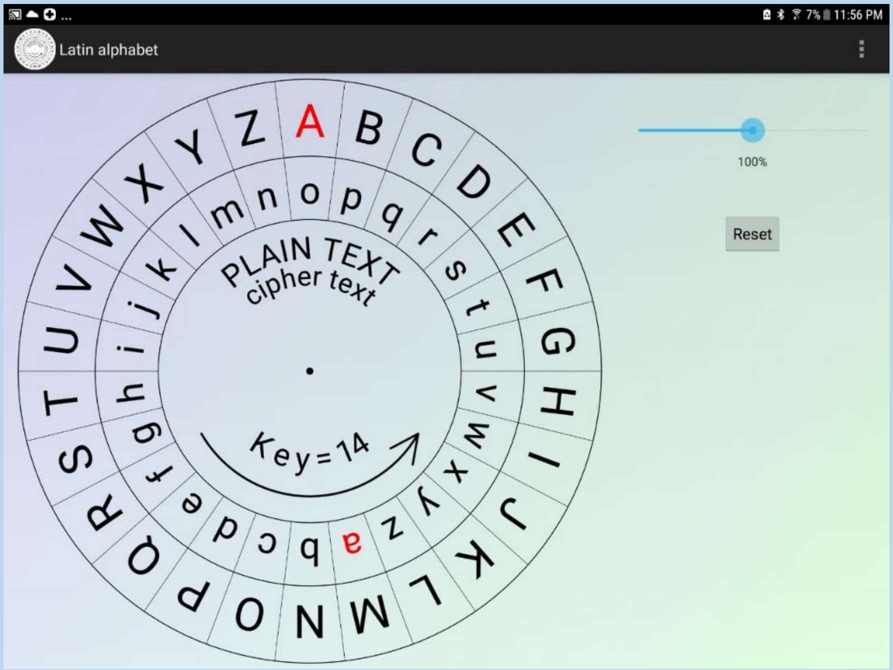
Part 2: Decoding (5 mins)

Question: If the Cipher text is ‘uc wbwhwohs’, find out the key and the original plaintext. (Hint: The key is between 11 - 16)

Solution:

Use the app on the Chromebook ‘Caesar Cipher Disk’ and move the outer wheel to the right and try out several keys to find the correct key and plaintext.

Upon investigation one will find that the key is -14. So, move the inner wheel 14 places to the left side and map the characters in ‘uc wbwhwohs’ to the outer wheel. It will come out to be ‘go initiate’


7% 11:56 PM
Latin alphabet
100%
Reset
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
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
PLAIN TEXT
cipher text
Key=14

u – 14 = g, c – 14 = o, w – 14 = i, b – 14 = n, h – 14 = t, o – 14 = a, s – 14 = e

Part 3: Encoding and Decoding (10 mins)

Question: Each group think of a unique word and encode it using a key of their choice. Exchange the encoded message with the next group and try to decode it.

Solution:

Use the app on the Chromebook ‘Caesar Cipher Disk’ and move the outer wheel to the right and try out several keys to find the correct key and plaintext.

Checkpoint:
If run out of time, move to the wrap up activity. The questions will have similar answers

Cryptography using Matrices Theory: (20 minutes)

- At first each character is assigned a specific number, such as A is 1, B is 2,.. , Z is 26, and space is 27.
- Let *A* be the sender of the message and *B* be the receiver of message.
- *A* selects a message and assigns numbers to each character.
- Example: Message = GO FOR IT

G O * F O R * I T
7 16 27 6 16 19 27 9 21

- *A* then create a vector (n x 1 matrix) of three numbers each.

$$\begin{bmatrix}7\\16\\27\end{bmatrix}\begin{bmatrix}6\\16\\19\end{bmatrix}\begin{bmatrix}27\\9\\21\end{bmatrix}$$

- It creates a message matrix by combining the vectors.

$$\begin{bmatrix}7 & 6 & 27\\16 & 16 & 9\\27 & 19 & 21\end{bmatrix}$$

- Then select an encoding matrix

$$\begin{bmatrix}1 & 0 & 1\\4 & 4 & 3\\-4 & -3 & -3\end{bmatrix}$$

- Multiply the encoding matrix with the message matrix.

$$\begin{bmatrix}1 & 0 & 1\\4 & 4 & 3\\-4 & -3 & -3\end{bmatrix}\begin{bmatrix}7 & 6 & 27\\16 & 16 & 9\\27 & 19 & 21\end{bmatrix}=\begin{bmatrix}34 & 25 & 48\\173 & 145 & 207\\-157 & -129 & -198\end{bmatrix}$$

- The encoded matrix is then converted to an encoded message and sent to *B*.

Encoded Message: 34 173 -157 25 145 -129 48 127 -198

- On receiving the encoded message, *B* converts it into a vector of three numbers each.

$$\begin{bmatrix}34\\173\\-157\end{bmatrix}\begin{bmatrix}25\\145\\-129\end{bmatrix}\begin{bmatrix}48\\127\\-198\end{bmatrix}$$

- *B* then converts the vectors into encoded message matrix.

$$\begin{bmatrix}34 & 25 & 48\\173 & 145 & 207\\-157 & -129 & -198\end{bmatrix}$$

- B then uses the decoding matrix, which is the inverse of the encoding matrix.

$$\begin{bmatrix}-3 & -3 & -4\\0 & 1 & 1\\4 & 3 & 4\end{bmatrix}$$

- Multiply the decoding matrix with the encoded message matrix.

$$\begin{bmatrix}-3 & -3 & -4\\0 & 1 & 1\\4 & 3 & 4\end{bmatrix}\begin{bmatrix}34 & 25 & 48\\173 & 145 & 207\\-157 & -129 & -198\end{bmatrix}=\begin{bmatrix}7 & 6 & 27\\16 & 16 & 9\\27 & 19 & 21\end{bmatrix}$$

- The decoded matrix is then converted to a decoded message using the same technique.

Decoded Message: 7 16 27 6 16 19 27 9 21
Message: GO FOR IT

Activity 2: Cryptography using Matrices (25 minutes)

Problem Statement: Divide the class among 4 groups with 3 teachers.

Teacher 1 = Think of a four-letter word, and encrypt it using the Encoding Matrix to find the encoded message matrix.

Teacher 2 = Using the decoding matrix and encoded message matrix find the decoded matrix.

Teacher 3 = Map the numbers to alphabets and find the original word.

Solution:

Let us assume the word is ‘SHOW’.

Teacher 1:

Step 1: Assigning numbers to alphabets:

S = 19, H = 8, O = 15, W = 22

Step 2: Creating two 2x1 vectors:

$$\begin{bmatrix} 19 \\ 8 \end{bmatrix} \begin{bmatrix} 15 \\ 22 \end{bmatrix}$$

Step 3: Combining to form a 2x2 message matrix:

$$\begin{bmatrix} 19 & 15 \\ 8 & 22 \end{bmatrix}$$

Step 4: Selecting an encoding matrix. For example:

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

Step 5: Multiply the encoding matrix with the message matrix

$$\begin{bmatrix} 3 & 5 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} 19 & 15 \\ 8 & 22 \end{bmatrix} = \begin{bmatrix} 97 & 35 \\ 155 & 59 \end{bmatrix}$$

Encoded Message matrix = $\begin{bmatrix} \mathbf{97} & \mathbf{35} \\ \mathbf{155} & \mathbf{59} \end{bmatrix}$

Teacher 2:

Step 1: The Decoding matrix is inverse of Encoding matrix:

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

Step 2: Multiplying the decoding matrix with the encoded message matrix:

$$\begin{bmatrix} 2 & -5 \\ -1 & 3 \end{bmatrix} \begin{bmatrix} 97 & 35 \\ 155 & 59 \end{bmatrix} = \begin{bmatrix} 19 & 15 \\ 8 & 22 \end{bmatrix}$$

Decoded Message matrix = $\begin{bmatrix} \mathbf{19} & \mathbf{15} \\ \mathbf{8} & \mathbf{22} \end{bmatrix}$

Teacher 3:

Step 1:

Decoded message = 19 8 15 22

Step 2:

19 = S, 8 = H, 15 = O, 22 = W

Decoded word = SHOW

Teaching Tips:
The teachers can use any online portal, such as Google Classrooms, Blackboard, etc. for students to submit their answers.

Activity 3: Algorithm Writing (15 minutes)

Problem Statement: Given that there are 3x3 encoding and decoding matrices. Write an algorithm for encoding and decoding using matrices. Divide the class into 2 groups. Group 1 will consider a message to be sent and write an algorithm to encode the message using the encoding matrix. Group 2 will consider that an encoded message is received and write an algorithm to decode the message using the decoding matrix.
NOTE: Write the algorithm steps as short sentences with step numbers. The minimum number of steps in the algorithm should be 5, maximum can be 10.
Suggestion: You can draw a flowchart, if you are comfortable.

Solution:

Group 1: Encoding

1. Map letters of the message to numbers and make a sequence of numbers.
2. Convert the sequence of numbers into vectors of size 3 (3x1 matrix).
3. Join the vectors to form the message matrix.
4. Multiply the encoding matrix to the message matrix.
5. The encoded message matrix is then converted to a sequence of numbers and transmitted.

Group 2: Decoding

1. The sequence of encoded numbers is converted to vectors of size 3.
2. Join the vectors to form the encoded matrix.
3. Multiply the encoded matrix with the decoding matrix.
4. The product is converted in to sequence of numbers.
5. This sequence is mapped back to alphabets and the message is obtained.

Teaching Tips:
The teachers can use any online portal, such as Google Classrooms, Blackboard, etc. for students to submit their answers.

Wrap-up: Conclusions and Inferences (5 minutes)

Activity:

- Can you think of a way to make this technique more complex?
- Have you ever been a victim of a cyber-attack?
- Are complex cryptography techniques enough to prevent cyber-attacks on AVs? Why?

Assessment:
Collect students' reflections. Assess for thoughtful, complete responses and experimental understanding. The students'

interest in STEM.

Learning Objectives and Standards

Learning Objectives	**Standards**
LO1: Students will be able to analyze a problem and suggest possible solutions.	*Computer Science* CCSS.MATH.PRACTICE.MP1: Make sense of problems and persevere in solving them.
LO2: Students will be able to see the relationship between two sets of data.	*TPS:* (+) N.VM.8: Add, subtract, and multiply matrices of appropriate dimensions.
LO3: Students will be able to verbalize a plan (an algorithm) for the whole process.	
LO5: Students will be able to see the mathematics behind everyday things.	

Additional Information and Resources

Project-based Learning Features

Feature	**Where does this occur in the lesson?**
Driving Question	The Driving Question can be seen at the very top after defining the Lesson Objective. In this lesson, we answered the question how to make autonomous vehicles safer. One way to make sure they are safe is to make the communication secure through cryptography. This lesson plan teaches some concepts of cybersecurity.
Investigation & Problem Solving	A Problem Statement is presented in the beginning of each Activity section. These problems are solved in the Activities using an Investigatory and problem-solving approach. The activities done in this lesson requires learning about two cryptography methods which are Caesar's cipher and Cryptography using matrices.
Technology Incorporation	The participants are using a Caesar's cipher disk app on their Chromebooks. We are also using google classroom to share the results.
Collaborative Opportunities	In the Activities designed, the people involved the lesson are discussing their results and sharing their ideas. They share their ideas and knowledge with each other, leading to Collaborative Learning Opportunities.
Assessment techniques	Assessment is done on whether the solutions to the problems are correct or not and the approach used is appropriate to the problem presented. The students should be able to solve problems in a better way and show sign of developing Computational Thinking skills.

Computational Thinking Concepts

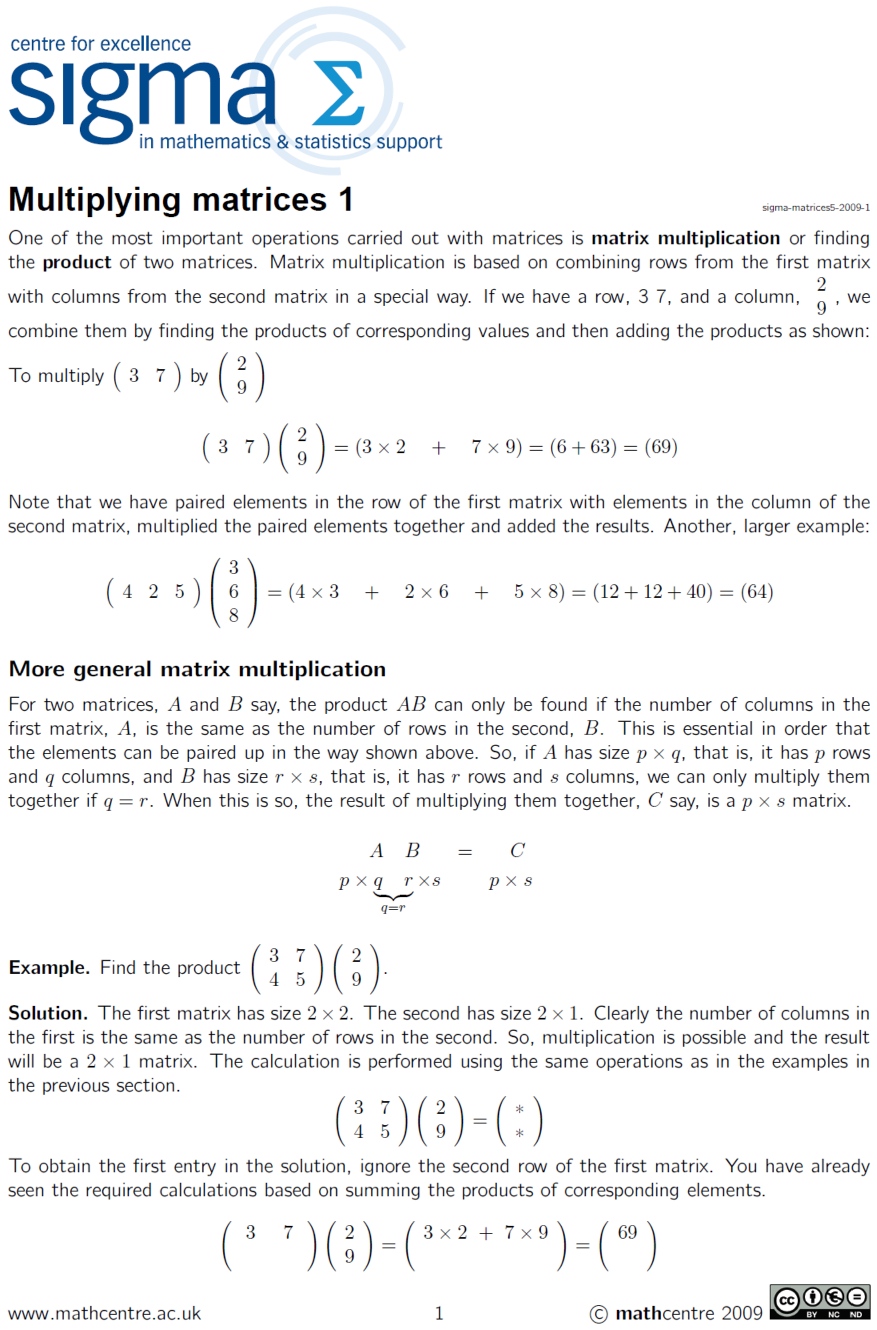
Concept	**Where does this occur in the lesson?**

Algorithm Design	In Activity 2 and 3, the participants should be able to identify an algorithm or a series of steps to complete cryptography using matrices. They need to follow a certain number of steps in the logical order to obtain the desired results, and check whether the decrypted word matches the original word.
Decomposition	Activity 2 and 3 requires the students to decompose the problems into parts and solve each of the parts independently to get the result of the presented problem.

Administrative Details

Contact info:	www.utoledo.edu/research/initiate
Sources:	CARJAM TV. (2015). *How Vehicle-to-vehicle (V2V) Will Save Your Life / Self Driving Car Car2X CarToCar ADAS CARJAM TV HD*. https://www.youtube.com/watch?v=44Oo-LGWjcg MathCentre. (2009). *Multiplying matrices 1*. MathCentre. https://www.mathcentre.ac.uk/resources/uploaded/sigma-matrices5-2009-1.pdf
Date Written:	03/18/2020
Template adapted from:	https://edu.google.com/resources/programs/exploring-computational-thinking/

Appendix: Matrix Multiplication (MathCentre, 2009)



centre for excellence
sigma Σ
in mathematics & statistics support

Multiplying matrices 1

sigma-matrices5-2009-1

One of the most important operations carried out with matrices is **matrix multiplication** or finding the **product** of two matrices. Matrix multiplication is based on combining rows from the first matrix with columns from the second matrix in a special way. If we have a row, 3 7, and a column, $\begin{matrix} 2 \\ 9 \end{matrix}$, we combine them by finding the products of corresponding values and then adding the products as shown:

To multiply $\begin{pmatrix} 3 & 7 \end{pmatrix}$ by $\begin{pmatrix} 2 \\ 9 \end{pmatrix}$

$$\begin{pmatrix} 3 & 7 \end{pmatrix}\begin{pmatrix} 2 \\ 9 \end{pmatrix} = (3 \times 2 \quad + \quad 7 \times 9) = (6 + 63) = (69)$$

Note that we have paired elements in the row of the first matrix with elements in the column of the second matrix, multiplied the paired elements together and added the results. Another, larger example:

$$\begin{pmatrix} 4 & 2 & 5 \end{pmatrix}\begin{pmatrix} 3 \\ 6 \\ 8 \end{pmatrix} = (4 \times 3 \quad + \quad 2 \times 6 \quad + \quad 5 \times 8) = (12 + 12 + 40) = (64)$$

More general matrix multiplication

For two matrices, A and B say, the product AB can only be found if the number of columns in the first matrix, A, is the same as the number of rows in the second, B. This is essential in order that the elements can be paired up in the way shown above. So, if A has size $p \times q$, that is, it has p rows and q columns, and B has size $r \times s$, that is, it has r rows and s columns, we can only multiply them together if $q = r$. When this is so, the result of multiplying them together, C say, is a $p \times s$ matrix.

$$\underset{p \times q}{A} \; \underset{r \times s}{B} = \underset{p \times s}{C} \qquad p \times \underbrace{q \quad r}_{q=r} \times s$$

Example. Find the product $\begin{pmatrix} 3 & 7 \\ 4 & 5 \end{pmatrix}\begin{pmatrix} 2 \\ 9 \end{pmatrix}$.

Solution. The first matrix has size 2×2. The second has size 2×1. Clearly the number of columns in the first is the same as the number of rows in the second. So, multiplication is possible and the result will be a 2×1 matrix. The calculation is performed using the same operations as in the examples in the previous section.

$$\begin{pmatrix} 3 & 7 \\ 4 & 5 \end{pmatrix}\begin{pmatrix} 2 \\ 9 \end{pmatrix} = \begin{pmatrix} * \\ * \end{pmatrix}$$

To obtain the first entry in the solution, ignore the second row of the first matrix. You have already seen the required calculations based on summing the products of corresponding elements.

$$\begin{pmatrix} 3 & 7 \\ & \end{pmatrix}\begin{pmatrix} 2 \\ 9 \end{pmatrix} = \begin{pmatrix} 3 \times 2 \; + \; 7 \times 9 \\ \end{pmatrix} = \begin{pmatrix} 69 \\ \end{pmatrix}$$

To obtain the second entry in the solution, ignore the first row of the first matrix.

$$\begin{pmatrix} & \\ 4 & 5 \end{pmatrix}\begin{pmatrix} 2 \\ 9 \end{pmatrix} = \begin{pmatrix} \\ 4\times 2\ +\ 5\times 9 \end{pmatrix} = \begin{pmatrix} \\ 53 \end{pmatrix}$$

Putting it all together

$$\begin{pmatrix} 3 & 7 \\ 4 & 5 \end{pmatrix}\begin{pmatrix} 2 \\ 9 \end{pmatrix} = \begin{pmatrix} 3\times 2\ +\ 7\times 9 \\ 4\times 2\ +\ 5\times 9 \end{pmatrix} = \begin{pmatrix} 69 \\ 53 \end{pmatrix}$$

Example. Find the product AB when $A = \begin{pmatrix} 2 & 4 \\ 5 & 3 \end{pmatrix}$ and $B = \begin{pmatrix} 3 & 6 \\ -1 & 9 \end{pmatrix}$.

Solution. The first matrix has size 2×2. The second matrix has size 2×2. Clearly the number of columns in the first is the same as the number of rows in the second. The multiplication can be performed and the result will be a 2×2 matrix.

$$AB = \begin{pmatrix} 2 & 4 \\ 5 & 3 \end{pmatrix}\begin{pmatrix} 3 & 6 \\ -1 & 9 \end{pmatrix} = \begin{pmatrix} 2\times 3+4\times(-1) & 2\times 6+4\times 9 \\ 5\times 3+3\times(-1) & 5\times 6+3\times 9 \end{pmatrix} = \begin{pmatrix} 2 & 48 \\ 12 & 57 \end{pmatrix}$$

Example. Find, if possible, $\begin{pmatrix} 2 \\ 5 \end{pmatrix}\begin{pmatrix} 3 & 6 \\ -1 & 9 \end{pmatrix}$.

Solution. The first matrix has size 2×1. The second matrix has size 2×2. This time, the number of columns in the first (1) is not the same as the number of rows in the second (2). It is not possible to multiply these matrices together.

Example. Find $\begin{pmatrix} 3 & 2 \\ 1 & 4 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}$.

Solution. The first matrix has size 2×2. The second matrix has size 2×1. Clearly the number of columns in the first is the same as the number of rows in the second. The multiplication can be performed and the result will be a 2×1 matrix.

$$\begin{pmatrix} 3 & 2 \\ 1 & 4 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 3x+2y \\ x+4y \end{pmatrix}$$

There are more examples of matrix multiplication in the next leaflet in this series.

Note that a video tutorial covering the content of this leaflet is available from **sigma**.