Basic Encryption and Decryption through Matrices

Table of Contents

Multiplication of Matrices

Before learning how to encrypt with matrices, we first must understand how a matrix works and how it can be calculated. A matrix is an arrangement of a collection of numbers represented though rows and columns. When the numbers are arranged vertically, it forms columns. When the numbers are arranged horizontally, it forms rows. To show the size of a matrix, it is shown with mxn (where *m* represents the number of rows and *n* represents the number of columns). An example of a 2x2 matrix would be: $\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$. An example of a 2x3 matrix would be: $\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}$.

To determine if two matrices can be multiplied, we use the size of the two matrices. While doing this, we change the variables for the second size to (nxp) to make it less confusing. So, the equation would look like this: $(mxn)(nxp) = (mxp)$. The reason why n is used in both sizes is because the number must be same for the matrix to multiply. An example of a matrix size that could be multiplied is $(2x3)(3x1)$. An example of a matrix size that cannot be multiplied is $(3x2)(1x3)$. The product of the equation is (mxp) because when you multiply the matrix the m from the first matrix size and the p from the second matrix is used to determine the size of the product matrix. So, using the prior example, the product matrix size for this: $(2x3)(3x1)$ is $(2x1)$.

To multiply two matrices, we use the dot product. The dot product is the summation of all products of each corresponding entry. Basically, multiply every row of the first matrix with every column of the second matrix. To show how this works, we are going to multiply a $(2x2)$ with a $(2x2)$. Since we are multiplying a $(2x2)$ with a $(2x2)$, the product matrix size is $(2x2)$.

Equation: $\begin{pmatrix} 1 & 2 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} 3 & 1 \\ 2 & -2 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$

The first step is to find the top left number is solving the dot product of row 1 and column 1.

So, a would be $(1)(3) + (2)(2) = 7$.

The next step is the find the top right number by solving the dot product of row 1 and column 2.

So, b would be $(1)(1) + (2)(-2) = -3$.

To find the bottom left number, you would do the dot product of row 2 and column 1.

$c = (0)(3) + (-1)(2) = -2$.

To find the bottom right number, you would do the dot product of row 2 and column 1.

$d = (0)(1) + (-1)(-2) = 2$.

The equation is going to be: $\begin{pmatrix} 1 & 2 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} 3 & 1 \\ 2 & -2 \end{pmatrix} = \begin{pmatrix} (1)(3) + (2)(2) & (1)(1) + (2)(-2) \\ (0)(3) + (-1)(2) & (0)(1) + (-1)(-2) \end{pmatrix}$

$= \begin{pmatrix} 7 & -3 \\ -2 & 2 \end{pmatrix}$

To show how this works with matrices that aren't the same size, we will use a $(2x3)$ matrix and a $(3x1)$ matrix. Our product matrix size would be $(2x1)$.

The two matrices we will use are $\begin{pmatrix} 1 & 0 & 4 \\ -2 & 1 & -3 \end{pmatrix}$ and $\begin{pmatrix} 1 \\ 0 \\ 2 \end{pmatrix}$.

So the equation is $\begin{pmatrix} 1 & 0 & 4 \\ -2 & 1 & -3 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \\ 2 \end{pmatrix} = \begin{pmatrix} ? \\ ? \end{pmatrix}$.

Dot Product: $\begin{pmatrix} (1)(1) + (0)(0) + (4)(2) \\ (-2)(1) + (1)(0) + (-3)(2) \end{pmatrix} = \begin{pmatrix} 9 \\ -8 \end{pmatrix}$

Our answer for the problem $\begin{pmatrix}1 & 0 & 4\\ -2 & 1 & -3\end{pmatrix}\begin{pmatrix}1\\ 0\\ 2\end{pmatrix}$ is $\begin{pmatrix}9\\ -8\end{pmatrix}$.

Encryption with Matrices

For this, we will only use characters from the English alphabet and no other characters. To encrypt words and phrases with matrices, we first need to assign letter to a number. To show a simple encryption, we will assign letters to its corresponding rank on the alphabet. We also include a 0 for any spaces. Because we only using the value of the characters, it doesn't matter for the characters to be capitalized or not.

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

For this example, we will use a $(2x2)$ matrix multiplication to encrypt, so after every odd number of letters in a word at the end of a sentence, we will also include a 0. Our message is going to be "Basic Encryption" and will use the matrix $\begin{pmatrix}2 & 3\\ 1 & 2\end{pmatrix}$ to encrypt our message. I chose this matrix to encrypt our message because this matrix determinant, this will be explained later, will be 1 which will make it easier to understand how to decrypt.

Our first step is going to be translate all the letters into numbers:

B	**A**	**S**	**I**	**C**		**E**	**N**	**C**	**R**	**Y**	**P**	**T**	**I**	**O**	**N**
2	**1**	**19**	**9**	**3**	**0**	**5**	**14**	**3**	**18**	**25**	**16**	**20**	**9**	**15**	**14**

Our next step is to arrange each pair of letters as $(1x2)$ matrix so it can be multiplied to a $(2x2)$ matrix.

$$(2\ 1)\ (19\ 9)\ (3\ 0)\ (5\ 14)\ (3\ 18)\ (25\ 16)\ (20\ 9)\ (15\ 14)$$

After this, we multiply each $(1x2)$ matrix with our $(2x2)$ encryption matrix.

$$(2\ 1)\begin{pmatrix} 2 & 3 \\ 1 & 2 \end{pmatrix} = (2 \times 2 + 1 \times 1 \quad 2 \times 3 + 1 \times 2) = (5\ 8)$$

$$(19\ 9)\begin{pmatrix} 2 & 3 \\ 1 & 2 \end{pmatrix} = (47\ 75)$$

$$(3\ 0)\begin{pmatrix} 2 & 3 \\ 1 & 2 \end{pmatrix} = (6\ 9)$$

$$(5\ 14)\begin{pmatrix} 2 & 3 \\ 1 & 2 \end{pmatrix} = (24\ 43)$$

$$(3\ 18)\begin{pmatrix} 2 & 3 \\ 1 & 2 \end{pmatrix} = (24\ 45)$$

$$(25\ 16)\begin{pmatrix} 2 & 3 \\ 1 & 2 \end{pmatrix} = (66\ 107)$$

$$(20\ 9)\begin{pmatrix}2 & 3\\1 & 2\end{pmatrix} = (49\ 78)$$

$$(15\ 14)\begin{pmatrix}2 & 3\\1 & 2\end{pmatrix} = (44\ 73)$$

Then gather each number in the encrypted message and the encrypted message would be:

$$(5\ 8)(47\ 75)(6\ 9)(24\ 43)(24\ 45)(66\ 107)(49\ 78)(44\ 73)$$

5 8 47 75 6 9 24 43 24 45 66 107 49 78 44 73

Decryption using the Inverse of Matrices

In order to decrypt a message with matrices, we must use the inverse of the matrix we used to encrypt our message. When inversing a matrix, we use something called the determinant. The determinant is an integral part in inversing a matrix.

Inverse of a 2x2 Matrix

To calculate the determinant of a 2x2 matrix we use the formula $\det(A) = ad - bc$, where A refers to the matrix we are inversing. It is important to know that if the determinant is zero, there is no inverse.

For example, if $A = \begin{pmatrix}5 & -1\\4 & 3\end{pmatrix}$

$\det(A) = (5)(3) - (-1)(4) = 19$

To calculate the inverse of a matrix we do the following:

1. Switch the positions of elements *a* and *d*
2. Multiply -1 to element *b* and element *c*
3. Divide all elements by the determinant

Using the matrix example from above

$A = \begin{pmatrix} 5 & -1 \\ 4 & 3 \end{pmatrix}$

$\det(A) = 19$

$A = \begin{pmatrix} 5 & -1 \\ 4 & 3 \end{pmatrix} \rightarrow \begin{pmatrix} 3 & -1 \\ 4 & 5 \end{pmatrix} \rightarrow \begin{pmatrix} 3 & 1 \\ -4 & 5 \end{pmatrix} \rightarrow \frac{1}{19}\begin{pmatrix} 3 & 1 \\ -4 & 5 \end{pmatrix} \rightarrow \begin{pmatrix} 3/19 & 1/19 \\ -4/19 & 5/19 \end{pmatrix}$

$$A^{-1} = \begin{pmatrix} \frac{3}{19} & \frac{1}{19} \\ -\frac{4}{19} & \frac{5}{19} \end{pmatrix}$$

Since the encryption matrix is a 2x2 matrix, we can find the inverse of the matrix

$BE = \begin{pmatrix} 2 & 3 \\ 1 & 2 \end{pmatrix}$, where EM means encryption matrix

$\det(BE) = (2)(2) - (3)(1) = 1$

$BE^{-1} = \begin{pmatrix} 2 & -3 \\ -1 & 2 \end{pmatrix}$

Now that we know the inverse of the encryption matrix, can be referred as the decryption matrix, we can multiply it with our encrypted message, and we should get our first message. Even if our determinant is 1, it is important to calculate it because it can affect our encrypted message.

Encrypted Message: **5 8 47 75 6 9 24 43 24 45 66 107 49 78 44 73**

Since our decryption matrix is a 2x2 matrix, we can arrange each pair of numbers as a 1x2 matrix. And multiply it by our decryption matrix. When sending the encrypted message, both sides need to know the original encryption matrix in order to decrypt the message. This is what make encryption and decryption difficult to break because for a hacker to attempt to break the encryption, they must find what was used to encrypt the message in the first place. This is also how banks and other websites keep your information safe, because they have encryption on a much larger scale, and only they know what the encryption key (encryption matrix in this case) is.

$$(5\ 8)\begin{pmatrix} 2 & -3 \\ -1 & 2 \end{pmatrix} = (2\ 1)$$

$$(47\ 75)\begin{pmatrix} 2 & -3 \\ -1 & 2 \end{pmatrix} = (19\ 9)$$

$$(6\ 9)\begin{pmatrix} 2 & -3 \\ -1 & 2 \end{pmatrix} = (3\ 0)$$

$$(24\ 43)\begin{pmatrix} 2 & -3 \\ -1 & 2 \end{pmatrix} = (5\ 14)$$

$$(24\ 45)\begin{pmatrix} 2 & -3 \\ -1 & 2 \end{pmatrix} = (3\ 18)$$

$$(66\ 107)\begin{pmatrix} 2 & -3 \\ -1 & 2 \end{pmatrix} = (25\ 16)$$

$$(49\ 78)\begin{pmatrix} 2 & -3 \\ -1 & 2 \end{pmatrix} = (20\ 9)$$

$$(44\ 73)\begin{pmatrix} 2 & -3 \\ -1 & 2 \end{pmatrix} = (15\ 14)$$

Decrypted Message: **2 1 19 9 3 0 5 14 3 18 25 16 20 9 15 14**

When you translate it back to letters, you get the message: **BASIC ENCRYPTION**

Encryption Practice

Message: ENCRYPT THIS

The $(2x2)$ encryption matrix: $\begin{pmatrix} 6 & 3 \\ 4 & 1 \end{pmatrix}$.

For practice encrypt this message. Solution for this is below

Decryption Practice

Encrypted Message: **73 4 183 3 319 25 140 20 212 20 234 9**

Encryption Matrix: $\begin{pmatrix} 7 & 1 \\ 9 & 0 \end{pmatrix}$

For practice encrypt this message. Solution for this is below

Encryption Practice Solution

Message translated into numbers: **5 14 3 18 25 16 20 0 20 8 9 19**

The $(1x2)$ matrix form of these are: (5 14) (3 18) (25 16) (20 0) (20 8) (9 19)

When multiplying each $(1x2)$ matrix with the encryption matrix, the matrices should come out to: $(86\ 29)(90\ 27)(214\ 91)(120\ 60)(152\ 68)(130\ 46)$

This means the encrypted message is: **86 29 90 27 214 91 120 60 152 68 130 46**

Decryption Practice Solution

The decryption matrix (inverse of encryption) should be: $\begin{pmatrix} 0 & \frac{1}{9} \\ 1 & -\frac{7}{9} \end{pmatrix}$ with determinant: -9

After multiplying the decryption matrix with the encrypted messages, the message (in number form) should be: **4 5 3 18 25 16 20 0 20 8 9 19**

The message translated from numbers to letter should be **decrypt this**