Application of Matrices in Cryptography

Evelyn Mateo Hernandez
CS 131
Fall 2022

What are matrices?

- A matrix is a set of numbers in a fixed number of rows and columns
- The numbers in a matrix represent data or mathematical equations
- Each number in a matrix is called an element or an entry
- A matrix with m rows and n columns is called a m x n matrix

$$\begin{bmatrix} 1 & 4 \\ 2 & 5 \\ 3 & 6 \end{bmatrix}$$

3 x 2 matrix

Example

1.) What size is A?
2.) What is the third column of A?
3.) What is the second row of A?

$$\text{Let } A = \begin{bmatrix} 1 & 1 & 1 & 3 \\ 2 & 0 & 4 & 6 \\ 1 & 1 & 3 & 7 \end{bmatrix}$$

Matrix Arithmetic: Matrix Addition

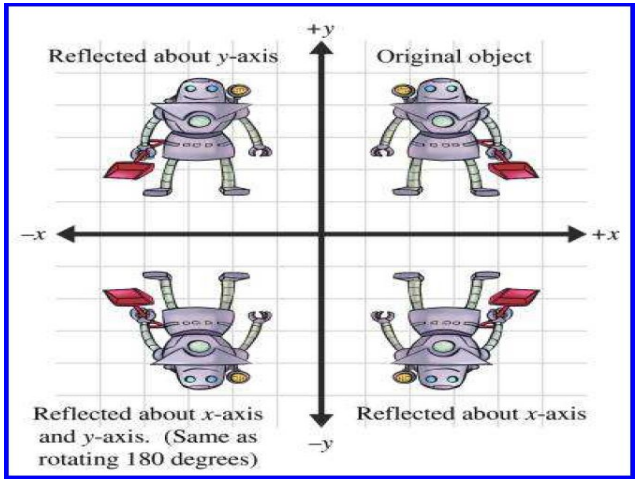
- We can get the sum of two matrices of the same size by adding elements in the corresponding positions.
- Two matrices of different sizes cannot be added, as they don’t have the same dimensions and they will not both have entries in some of their positions.

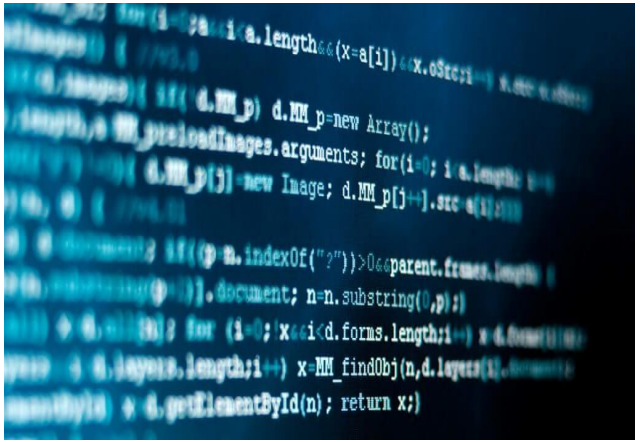
Matrix Addition Example

$$\mathbf{A} = \begin{bmatrix} 5 & 2 \\ 0 & 1 \\ 1 & 9 \end{bmatrix} \text{ and } \mathbf{B} = \begin{bmatrix} 2 & 3 \\ 4 & 1 \\ 0 & 2 \end{bmatrix} = \begin{bmatrix} 7 & 5 \\ 4 & 2 \\ 1 & 11 \end{bmatrix}$$

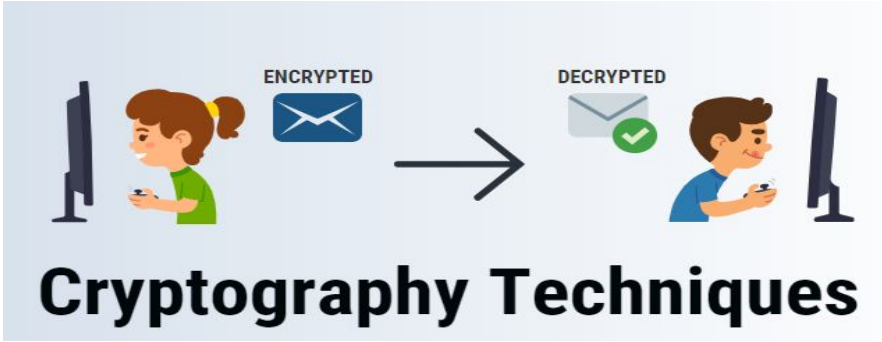
Application of Matrices

- Computer Graphics
- Optics
- Cryptography
- Economics
- Robotics and Animation
- Wireless communication
- Signal Processing





Cryptography



- Cryptography: secure communication techniques in which data is encrypted and secures information in computer systems.
- Ensures integrity of data in transit and data at rest
- Cryptography was used in the military during times of war to encode messages before being sent and the recipient would decode the message in order to keep information safe
- During world war II, cryptography had a huge impact on the outcome of the war
- Cryptography is also used to ensure safe online shopping, bank transactions, computer passwords, communication networks, chip based payment cards, military communications, etc.

Ciphers

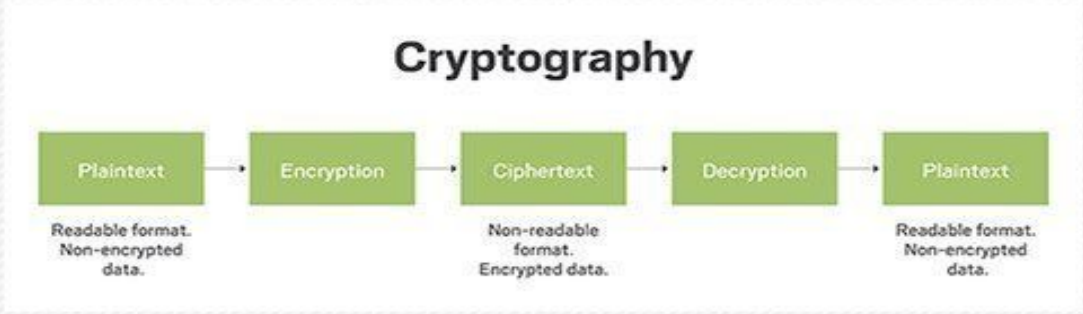
A cipher converts readable text (plaintext) to encrypted text (ciphertext) in which it can only be read by reversing the process (decryption).

Types of Ciphers:

- **Caesar Cipher (Substitution Cipher):** named after Julius Caesar, a substitution method in which each letter in a message are shifted by a fixed number of spaces which results in an encoding alphabet.
- **Transposition Ciphers:** Keeps letters the same but rearranges the order based on a specific algorithm.
- **Polygraphic Ciphers:** substitutes a letter for another and substitutes with two or more groups of letters.
- **Permutation Ciphers:** positions held by plaintext are shifted to a regular system so that the ciphertext forms a permutation of the plaintext.
- **Private Key Cryptography:** sender and receivers need to have a pre-shared key. Shared key is kept secret from other parties and will be used for encryption and decryption.
- **Public Key Cryptography:** includes two different keys, private and public, used for encryption and decryption. The sender will use the public key for encryption, while the private key is kept secret from the receiver.

More on Cryptography

- One method of encryption uses matrix multiplication and matrix inversion.
- The use of encryption has evolved into secure communication and in keeping private data secure.
- Modern cryptography involves mathematics, computer science, information security, digital signal processing, physics, etc.



Use of Matrices in Cryptography

Matrices are used to encode and decode messages

Procedure:

1.) The message is converted into a string of numbers by randomly assigning a number to each letter of the message
2.) The string of numbers is converted into a new set of numbers by multiplying the string to a square matrix that has an inverse. The new set of numbers represents the coded message.
3.) In order to decode the message, you must multiply the string of coded numbers and multiply it by the inverse of the matrix to get the original string of numbers
4.) Lastly, by connecting the numbers to their corresponding letters, your result will be the original message

Encoding a Message

We will use the table to encode the message:

ATTACK NOW

We will also use matrix A to encode the message

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

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
14	15	16	17	18	19	20	21	22	23	24	25	26

Space (-) is represented by the number 27

Procedure

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
14	15	16	17	18	19	20	21	22	23	24	25	26

1.) First, we will divide the letters in the message in groups of 2

AT TA CK -N OW

2.) Next, assign the numbers to the letters from the table, which will convert each pair of numbers into 2 x 1 matrices

$$\begin{bmatrix} A \\ T \end{bmatrix} = \begin{bmatrix} 1 \\ 20 \end{bmatrix} \quad \begin{bmatrix} T \\ A \end{bmatrix} = \begin{bmatrix} 20 \\ 1 \end{bmatrix} \quad \begin{bmatrix} C \\ K \end{bmatrix} = \begin{bmatrix} 3 \\ 11 \end{bmatrix}$$

$$\begin{bmatrix} - \\ N \end{bmatrix} = \begin{bmatrix} 27 \\ 14 \end{bmatrix} \quad \begin{bmatrix} O \\ W \end{bmatrix} = \begin{bmatrix} 15 \\ 23 \end{bmatrix}$$

Procedure Cont.

3.) We will result with 2x1 matrices being expressed as the message

$$\begin{bmatrix} 1 \\ 20 \end{bmatrix} \begin{bmatrix} 20 \\ 1 \end{bmatrix} \begin{bmatrix} 3 \\ 11 \end{bmatrix} \begin{bmatrix} 27 \\ 14 \end{bmatrix} \begin{bmatrix} 15 \\ 23 \end{bmatrix}$$

4.) In order to encode, we have to multiply each matrix of the message by matrix A

$$\begin{bmatrix} 1 & 2 \\ 1 & 3 \end{bmatrix} \begin{bmatrix} 1 \\ 20 \end{bmatrix} = \begin{bmatrix} 41 \\ 61 \end{bmatrix} \qquad \begin{bmatrix} 1 & 2 \\ 1 & 3 \end{bmatrix} \begin{bmatrix} 20 \\ 1 \end{bmatrix} = \begin{bmatrix} 22 \\ 23 \end{bmatrix}$$

5.) We will get our coded message through multiplication of matrices

$$\begin{bmatrix} 41 \\ 61 \end{bmatrix} \begin{bmatrix} 22 \\ 23 \end{bmatrix} \begin{bmatrix} 25 \\ 36 \end{bmatrix} \begin{bmatrix} 55 \\ 69 \end{bmatrix} \begin{bmatrix} 61 \\ 84 \end{bmatrix}$$

Decoding a Message

Decode an encoded message using matrix A

$$\begin{bmatrix} 21 \\ 26 \end{bmatrix} \begin{bmatrix} 37 \\ 53 \end{bmatrix} \begin{bmatrix} 45 \\ 54 \end{bmatrix} \begin{bmatrix} 74 \\ 101 \end{bmatrix} \begin{bmatrix} 53 \\ 69 \end{bmatrix}$$

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

(Note that the message was encoded by multiplying by matrix A as shown in the previous example)

Procedure

1.) Use the inverse of matrix A to decode the message

$$A = \begin{bmatrix} 1 & 2 \\ 1 & 3 \end{bmatrix} \qquad A^{-1} = \begin{bmatrix} 3 & -2 \\ -1 & 1 \end{bmatrix}$$

2.) Now we multiply each matrix by the inverse of matrix A

$$\begin{bmatrix} 3 & -2 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} 21 \\ 26 \end{bmatrix} = \begin{bmatrix} 11 \\ 5 \end{bmatrix}$$

Procedure Cont.

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
14	15	16	17	18	19	20	21	22	23	24	25	26

2.) Result after multiplication:

$$\begin{bmatrix} 11 \\ 5 \end{bmatrix} \begin{bmatrix} 5 \\ 16 \end{bmatrix} \begin{bmatrix} 27 \\ 9 \end{bmatrix} \begin{bmatrix} 20 \\ 27 \end{bmatrix} \begin{bmatrix} 21 \\ 16 \end{bmatrix}$$

3.) Lastly, we will associate the numbers with the corresponding letters

$$\begin{bmatrix} K \\ E \end{bmatrix} \begin{bmatrix} E \\ P \end{bmatrix} \begin{bmatrix} - \\ I \end{bmatrix} \begin{bmatrix} T \\ - \end{bmatrix} \begin{bmatrix} U \\ P \end{bmatrix}$$

The message is: KEEP IT UP

Works Cited Page

- Rosen, Kenneth H. *Discrete Mathematics and its Applications*. 8th ed. McGraw-Hill, 2019.
- "Application of Matrices in Science, Commerce and Social Science Fields." *Vedantu*, https://www.vedantu.com/maths/application-of-matrices Accessed December 11, 2022.
- Sekhon, Rupinder, and Roberta Bloom. "2.5: Application of Matrices in Cryptography." *LibreTexts Mathematics*,https://math.libretexts.org/Bookshelves/Applied_Mathematics/Applied_Finite_Mathematics_(Sekhon_and_Bloom)/02%3A_Matrices/2.05%3A_Application_of_Matrices_in_Cryptography Accessed December 9, 2022.
- Liang Chua, Boon. "Harry Potter and the Cryptography with Matrices." https://files.eric.ed.gov/fulltext/EJ743766.pdf Accessed December 9, 2022.
- "Cryptography." *Wikipedia*, https://en.wikipedia.org/wiki/Cryptography
- https://www.techtarget.com/whatis/definition/ciphertext Accessed December 8, 2022.
- Olwenyi, Julius O, and Aby Tino Thomas, et al. "Cryptography in Modern World." *St Mary's University*, https://cdn.stmarytx.edu/wp-content/uploads/2020/10/Cryptography-in-Modern-World.pdf Accessed December 10, 2022.
- Argintaru, Daniel. "Data Encryption - Data at Rest vs In Transit vs In Use Options." *mimecast*, https://www.mimecast.com/blog/data-in-transit-vs-motion-vs-rest/ Accessed December 9, 2022.
- "Adding & Subtracting Matrices." *Khan Academy*, https://www.khanacademy.org/math/precalculus/x9e81a4f98389efdf:matrices/x9e81a4f98389efdf:adding-and-subtracting-matrices/a/adding-and-subtracting-matrices Accessed December 9, 2022.