Hill cipher

Here is where our presentation begins

Name:

ندى عبد الغنى سعيد عثمان

ID:

20012095

Section: 1

There are two types of symmetric cipher

Transposition Cipher

In the transposition technique, there is no replacement occurs instead their positions are changed or reordering of the position of plain text is done to produce cipher text.
For Example, ABCDE ⟹ BADEC

Substitution Cipher

In Substitution Cipher each letter of the plaintext is replaced by some other letter, number, or symbol to produce cipher text.

There are different types of Substitution Cipher such as: Caesar Cipher, Monoalphabetic Cipher, Playfair Cipher, One-time pad cipher and **Hill Cipher**

Hill Cipher

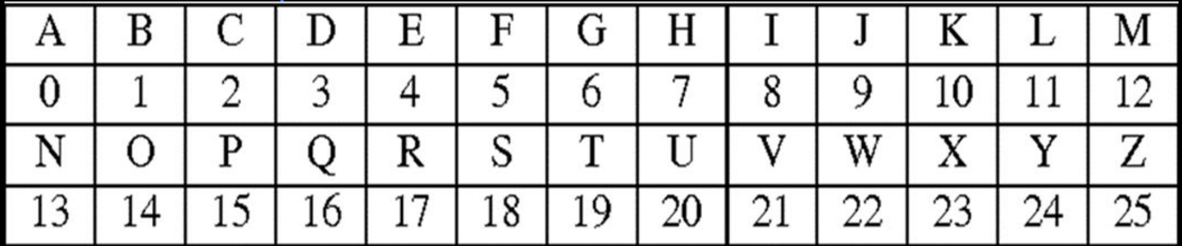
- mathematician Laster Hill developed This technique in 1929.
- It is a polyalphabetic substitution cipher.
- Hill cipher based on linear algebra. It uses matrix multiplication, matrix inverses, and modulo-arithmetic rules. It is a more mathematical cipher compared to others.
- Inputs of this technique are a keyword and plain text. The keyword is in a matrix form.

How the Hill cipher works?

The Hill cipher works by viewing a group of letters as a vector, and encryption is done by matrix multiplication. While this cipher can work on blocks of letters of any length, we'll describe it as working on pairs of letters, or digraphs.

First Way : Encryption

-Replace each character of the plain text with a number. As the given table.



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

-Create 2x2 or 3x3 key matrix.

-Make a group of plain text. each pair of plain text multiplied with the key matrix

-The new matrix values modules with 26.

-After module 26, the matrix values are replaced with characters using the table. that generated the final cipher text.

In other side, Way to solve Decryption:

-Assign a number to each character of the cipher text. As the given table we mentioned before.
-Find the inverse of the key matrix.
-Make a group of cipher text. each pair of cipher text multiplied with the inverse key matrix
-The new matrix values modules with 26.
-After module 26, the matrix values are replaced with characters using the table. that generated the original text.

Example: Input : Plaintext: ACT
Key: GYBNQKURP
Output : Ciphertext: POH

- 1st Encryption

We have to encrypt the message ‘ACT’ (n=3).The key is ‘GYBNQKURP’ which can be written as the nxn matrix:

$$\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix}$$

The message ‘ACT’ is written as vector:

$$\begin{bmatrix} 0 \\ 2 \\ 19 \end{bmatrix}$$

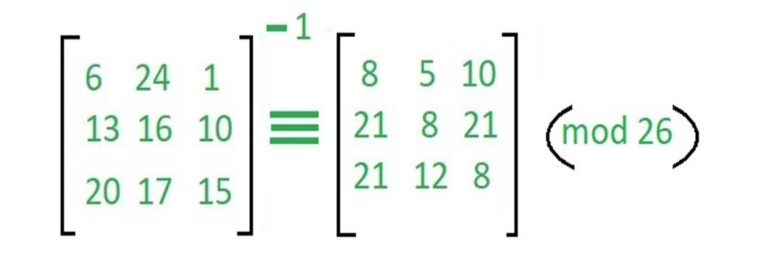
The enciphered vector is given as:

$$\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix} \begin{bmatrix} 0 \\ 2 \\ 19 \end{bmatrix} = \begin{bmatrix} 67 \\ 222 \\ 319 \end{bmatrix} \equiv \begin{bmatrix} 15 \\ 14 \\ 7 \end{bmatrix} \pmod{26}$$

which corresponds to ciphertext of ‘POH’.

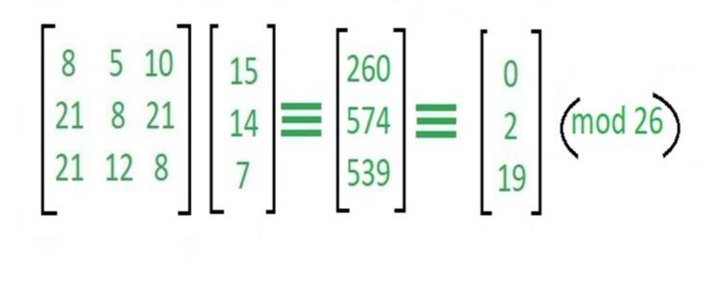
- 2nd Decryption

To decrypt the message, we turn the ciphertext back into a vector, then simply multiply by the inverse matrix of the key matrix (IFKVIVVMI in letters).The inverse of the matrix used in the previous example is:



$$\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix}^{-1} \equiv \begin{bmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{bmatrix} \pmod{26}$$

For the previous Ciphertext ‘POH’:



$$\begin{bmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{bmatrix} \begin{bmatrix} 15 \\ 14 \\ 7 \end{bmatrix} \equiv \begin{bmatrix} 260 \\ 574 \\ 539 \end{bmatrix} \equiv \begin{bmatrix} 0 \\ 2 \\ 19 \end{bmatrix} \pmod{26}$$

which gives us back ‘ACT’.
Assume that all the alphabets are in upper case.
Below is the implementation of the above idea for n=3.

Name:

ياسمين علاء أبوشادى

ID:

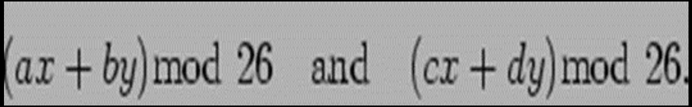
20012213

Section: 3

Second Way :

-Our key consists of four numbers which we call a, b, c, and d. These numbers must be chosen so that the quantity ad-bc is relatively prime to the length of the alphabet (26 in our case, so ad-bc cannot be even or a multiple of 13).

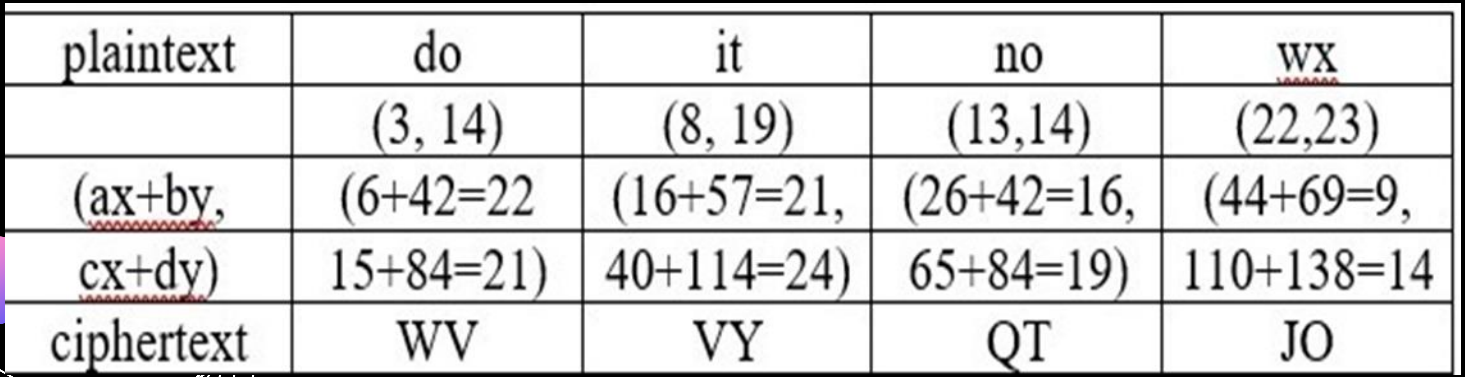
-To encrypt a pair of letters, we look up their numeric equivalents as usual. Suppose these numbers are x and y. Then the corresponding letters in the ciphertext are given by



$$(ax + by) \bmod 26 \quad \text{and} \quad (cx + dy) \bmod 26.$$

Example:

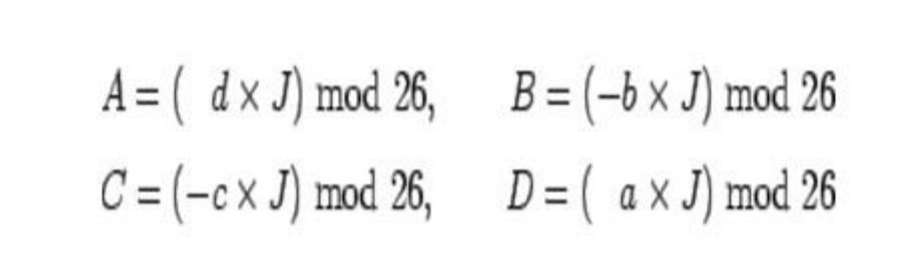
let's encipher the phrase do it now using a Hill Cipher with the key a=2, b=3, c=5, and d=6. Since $ad-bc=-3=23 (\mbox{mod} 26)$, this is a valid key. To encode, we break our text up into pairs, and since there are an odd number of letters, we add x to the end.



plaintext	do	it	no	wx
	(3, 14)	(8, 19)	(13,14)	(22,23)
(ax+by,	(6+42=22	(16+57=21,	(26+42=16,	(44+69=9,
cx+dy)	15+84=21)	40+114=24)	65+84=19)	110+138=14
ciphertext	WV	VY	QT	JO

In another side: To find A, B, C, and D, we first find the multiplicative inverse of ad-bc and denote it by J.

-Then:

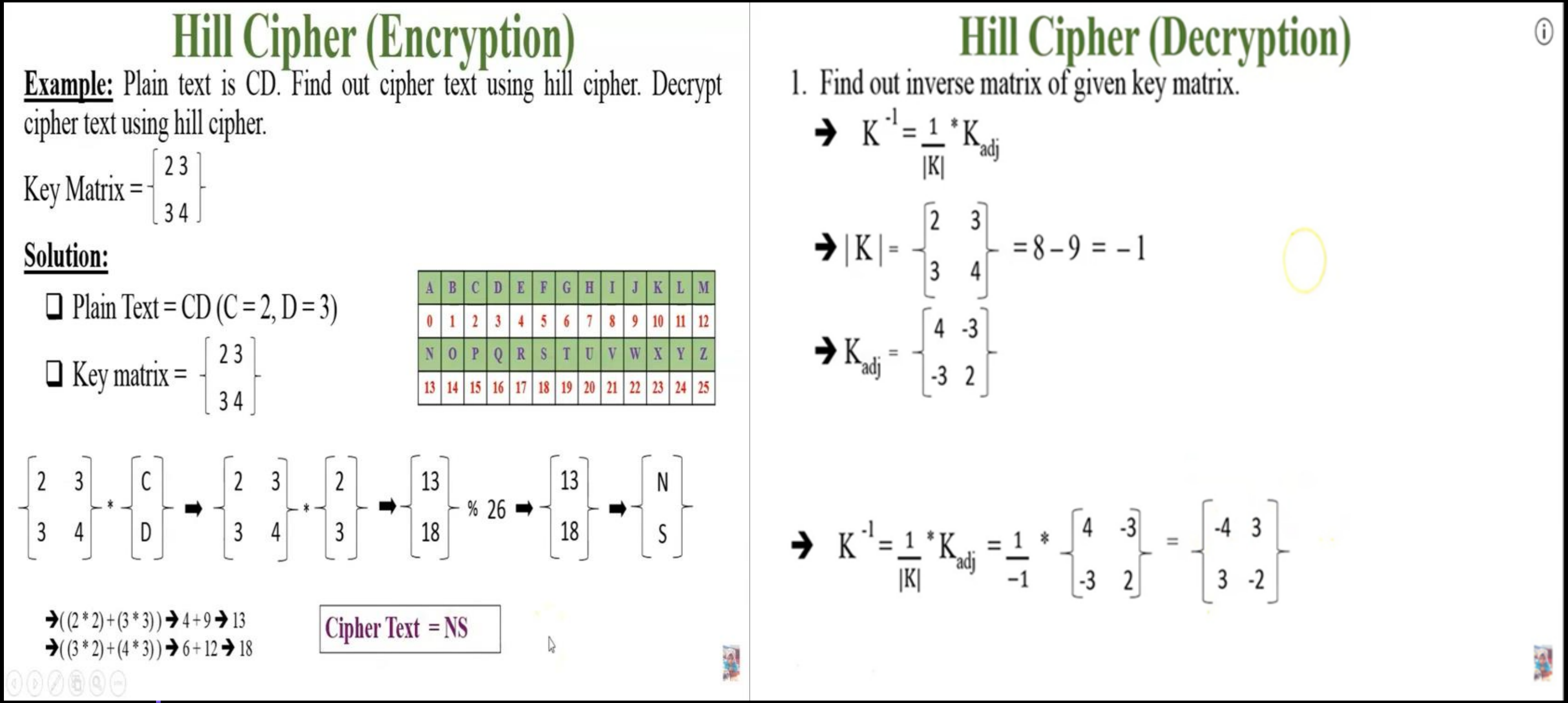


$$A = (\ \ d \times J) \bmod 26, \qquad B = (-b \times J) \bmod 26$$

$$C = (-c \times J) \bmod 26, \qquad D = (\ \ a \times J) \bmod 26$$

Extra Examples:

1.



Hill Cipher (Encryption)

Example: Plain text is CD. Find out cipher text using hill cipher. Decrypt cipher text using hill cipher.

Key Matrix = $\begin{bmatrix}2\,3\\3\,4\end{bmatrix}$

Solution:

❑ Plain Text = CD (C = 2, D = 3)

❑ Key matrix = $\begin{bmatrix}2\,3\\3\,4\end{bmatrix}$

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

$$\begin{bmatrix}2&3\\3&4\end{bmatrix} * \begin{bmatrix}C\\D\end{bmatrix} \Rightarrow \begin{bmatrix}2&3\\3&4\end{bmatrix} * \begin{bmatrix}2\\3\end{bmatrix} \Rightarrow \begin{bmatrix}13\\18\end{bmatrix} \% \, 26 \Rightarrow \begin{bmatrix}13\\18\end{bmatrix} \Rightarrow \begin{bmatrix}N\\S\end{bmatrix}$$

$\rightarrow ((2*2)+(3*3)) \rightarrow 4+9 \rightarrow 13$

$\rightarrow ((3*2)+(4*3)) \rightarrow 6+12 \rightarrow 18$

Cipher Text = NS

Hill Cipher (Decryption)

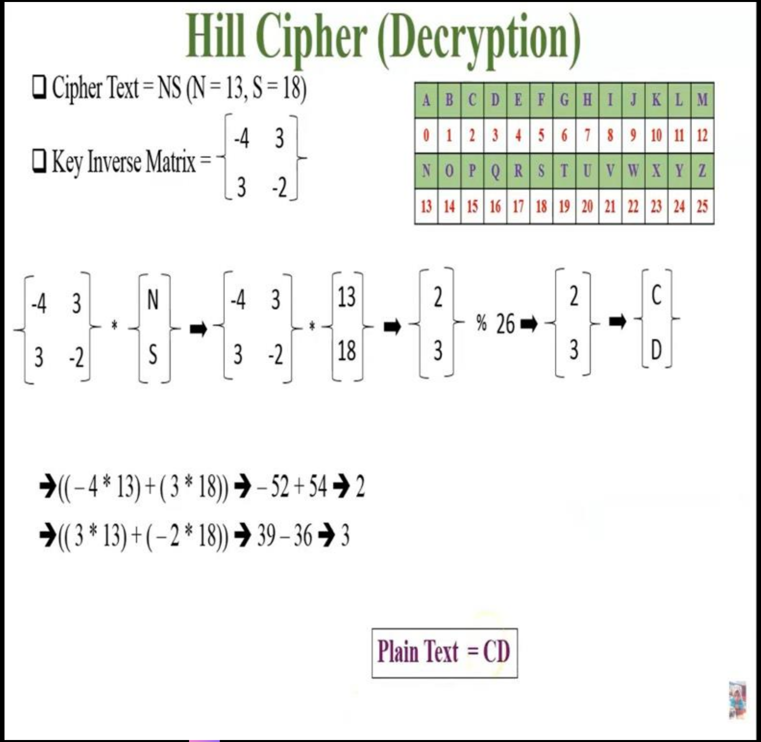
1. Find out inverse matrix of given key matrix.

$\rightarrow$ $K^{-1} = \frac{1}{|K|} * K_{adj}$

$\rightarrow$ $|K| = \begin{bmatrix}2&3\\3&4\end{bmatrix} = 8-9 = -1$

$\rightarrow$ $K_{adj} = \begin{bmatrix}4&-3\\-3&2\end{bmatrix}$

$\rightarrow$ $K^{-1} = \frac{1}{|K|} * K_{adj} = \frac{1}{-1} * \begin{bmatrix}4&-3\\-3&2\end{bmatrix} = \begin{bmatrix}-4&3\\3&-2\end{bmatrix}$



Hill Cipher (Decryption)

- □ Cipher Text = NS (N = 13, S = 18)
- □ Key Inverse Matrix = $\begin{bmatrix}-4 & 3\\ 3 & -2\end{bmatrix}$

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

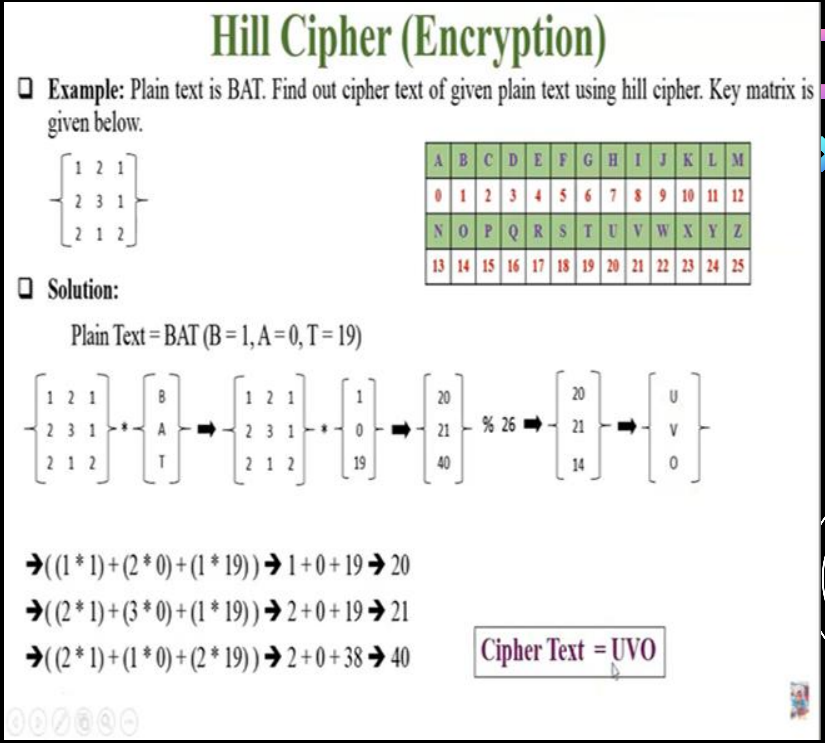
$$\begin{bmatrix}-4 & 3\\ 3 & -2\end{bmatrix} * \begin{bmatrix}N\\ S\end{bmatrix} \Rightarrow \begin{bmatrix}-4 & 3\\ 3 & -2\end{bmatrix} * \begin{bmatrix}13\\ 18\end{bmatrix} \Rightarrow \begin{bmatrix}2\\ 3\end{bmatrix} \% \ 26 \Rightarrow \begin{bmatrix}2\\ 3\end{bmatrix} \Rightarrow \begin{bmatrix}C\\ D\end{bmatrix}$$

$\rightarrow ((-4 * 13) + (3 * 18)) \rightarrow -52 + 54 \rightarrow 2$

$\rightarrow ((3 * 13) + (-2 * 18)) \rightarrow 39 - 36 \rightarrow 3$

Plain Text = CD

2.



Hill Cipher (Encryption)

- □ **Example:** Plain text is BAT. Find out cipher text of given plain text using hill cipher. Key matrix is given below.

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

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

- □ **Solution:**

Plain Text = BAT (B = 1, A = 0, T = 19)

$$\begin{bmatrix}1 & 2 & 1\\ 2 & 3 & 1\\ 2 & 1 & 2\end{bmatrix} * \begin{bmatrix}B\\ A\\ T\end{bmatrix} \Rightarrow \begin{bmatrix}1 & 2 & 1\\ 2 & 3 & 1\\ 2 & 1 & 2\end{bmatrix} * \begin{bmatrix}1\\ 0\\ 19\end{bmatrix} \Rightarrow \begin{bmatrix}20\\ 21\\ 40\end{bmatrix} \% \ 26 \Rightarrow \begin{bmatrix}20\\ 21\\ 14\end{bmatrix} \Rightarrow \begin{bmatrix}U\\ V\\ O\end{bmatrix}$$

$\rightarrow ((1 * 1) + (2 * 0) + (1 * 19)) \rightarrow 1 + 0 + 19 \rightarrow 20$

$\rightarrow ((2 * 1) + (3 * 0) + (1 * 19)) \rightarrow 2 + 0 + 19 \rightarrow 21$

$\rightarrow ((2 * 1) + (1 * 0) + (2 * 19)) \rightarrow 2 + 0 + 38 \rightarrow 40$

Cipher Text = UVO

Recap:

- Hill ciphers are an application of linear algebra to cryptology (the science of making and breaking codes and ciphers).
- Hill cipher is an encryption algorithm that works on matrix multiplication.
- Matrix must be non-singular.
- This algorithm involves matrix operations such as matrix multiplication, matrix inversion etc.
- Geometric image transformations involve applying various transformations, such as translation, rotation, scaling, shearing, and reflection, to images.

Name:

رحمة أحمد السيد

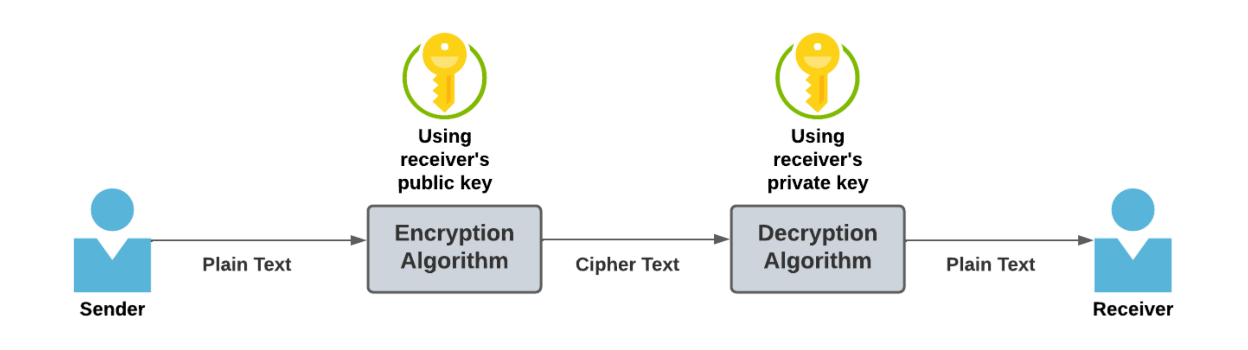
ID:

20010556

Section: 7

What is the relation between linear algebra and cryptography?

- ➢ Linear algebra is used in some cryptographic algorithms. Ex: for public-key generation, we use RSA encryption and elliptic curve encryption.
- ❑ **for RSA: operation of encryption and decryption can be expressed in terms of matrix multiplications and modular arithmetic.

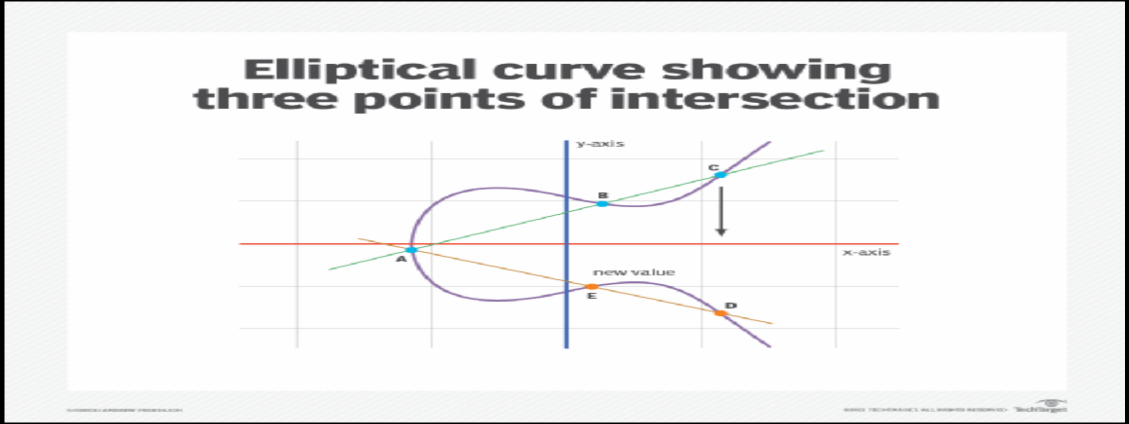


- **To generate the keys, two large prime numbers are selected, and their product is calculated to obtain a composite number, which is used as the modulus for the public and private keys. (with picture)**

  ciphertext c equation for example:

  c = m^e mod n

  **for elliptic curve:


Elliptical curve showing three points of intersection
y-axis
x-axis
A
B
C
D
E
new value
SOURCE: ANDREW FROEHLICH
©2021 TECHTARGET. ALL RIGHTS RESERVED. TechTarget

- This method relies on point addition, which expressed in terms of matrix multiplication, and scalar multiplication

- Linear algebra can be used to build pseudorandom number generators.
- Linear algebra concepts like vectors, matrices, and linear transforms are used in symmetric key ciphers like AES.

how eigenvalues can reveal information about a cipher's security?

- In some ciphers, the eigenvectors and eigenvalues of the transformation matrices can reveal linear dependencies or weaknesses in the cipher.
- For example, in the Square cipher, the cipher operates by multiplying the plaintext by a square matrix which can be ideal or non-ideal matrix.
- Essentially, repeating eigenvalues or dependent eigenvectors indicate that the transformation matrix is "less random" and has some linear structure that an attacker may be able to take advantage of.

Name:

علاء عبد المنعم الرفاعى

ID:

20010928

Section: 1

Modular arithmetic:

1. Modular arithmetic is a mathematical system that deals with arithmetic operations on remainders. It is used in various applications, including computer science, cryptography, and number theory. In computer science, it is used for hashing, random number generation, error detection and correction, cryptography, and timing analysis. In number theory, it is used to define congruence relations, prove theorems such as Fermat's Little Theorem and the Chinese Remainder Theorem, study Diophantine equations, and perform primality testing. Overall, modular arithmetic provides a simple and efficient way to perform arithmetic operations on large numbers and is a fundamental tool in mathematics and computer science.

Name:

يمنى عونى عبد المنعم صالح

ID:

20012237

Section: 1

Example on modular arithmetic:

The best way to explain it is if I used the clock as my example. The clock is a system of arithmetic for integers of 1 up to 12 and it is wrapped around 12. If I say it is 15 o'clock, you will know that I mean 3 pm. You got that by simply taking 12 out of 15 and you got 3. So the time of the clock is a 12 module and 15 = 3 (mod 12).

We use it in Matlab by using the expression: b=mod(a,m);

For example:

```
b= mod(15,12)

>> b = 3
```

Name:

رنا ياسر محمد خيرى بركات

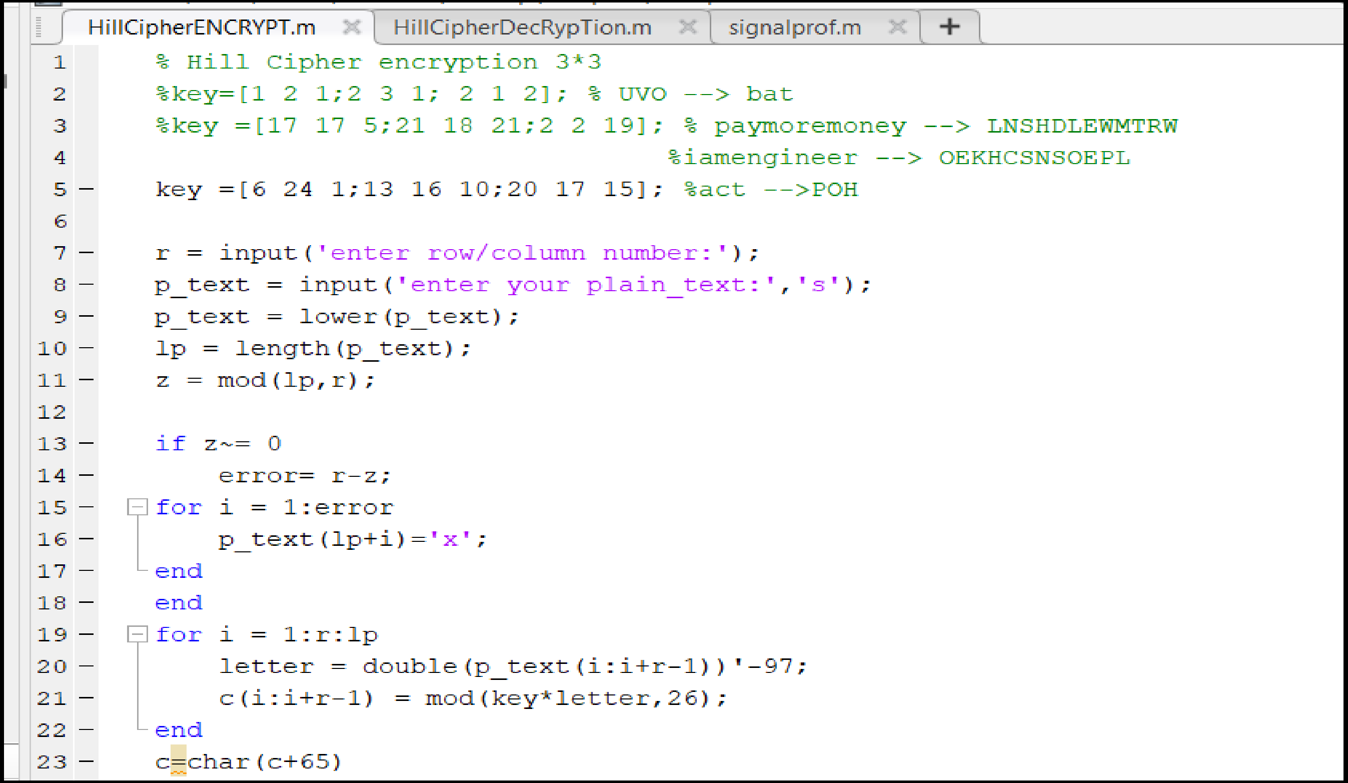
ID:

20010578

Section: 7

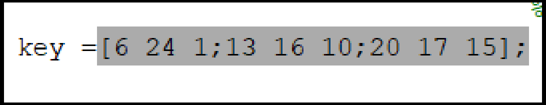
Encryption code:

Code:

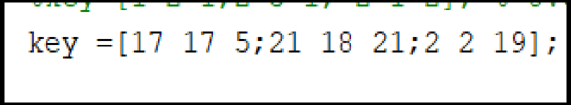


```
% Hill Cipher encryption 3*3
%key=[1 2 1;2 3 1; 2 1 2]; % UVO --> bat
%key =[17 17 5;21 18 21;2 2 19]; % paymoremoney --> LNSHDLEWMTRW
                                %iamengineer --> OEKHCSNSOEPL
key =[6 24 1;13 16 10;20 17 15]; %act -->POH

r = input('enter row/column number:');
p_text = input('enter your plain_text:','s');
p_text = lower(p_text);
lp = length(p_text);
z = mod(lp,r);

if z~= 0
    error= r-z;
for i = 1:error
    p_text(lp+i)='x';
end
end
for i = 1:r:lp
    letter = double(p_text(i:i+r-1))'-97;
    c(i:i+r-1) = mod(key*letter,26);
end
c=char(c+65)
```

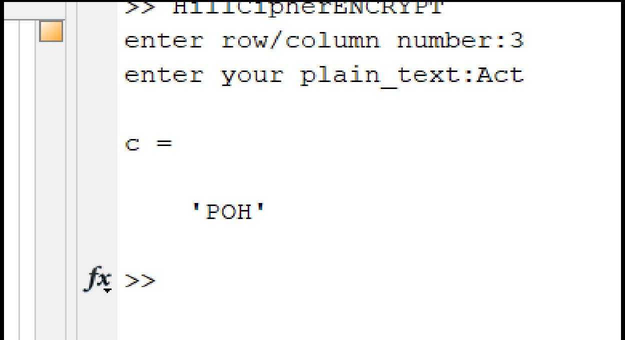
O/P: 1.



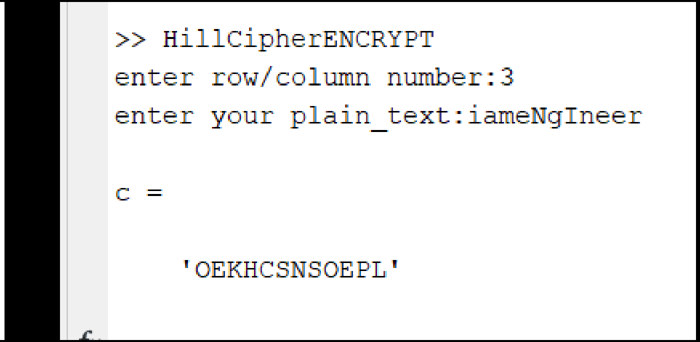
```
key =[6 24 1;13 16 10;20 17 15];
```



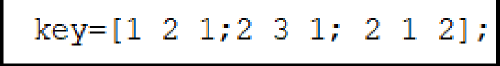
```
key =[17 17 5;21 18 21;2 2 19];
```



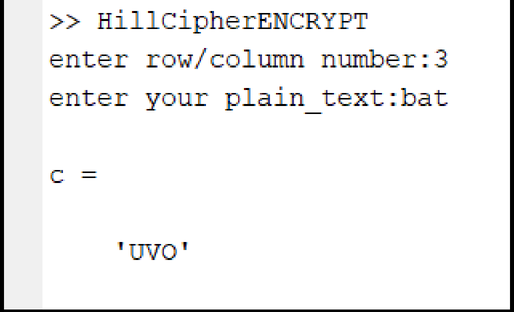
```
>> HillCipherENCRYPT
enter row/column number:3
enter your plain_text:Act

c =

    'POH'

>>
```



```
>> HillCipherENCRYPT
enter row/column number:3
enter your plain_text:iameNgIneer

c =

    'OEKHCSNSOEPL'
```



```
key=[1 2 1;2 3 1; 2 1 2];
```



```
>> HillCipherENCRYPT
enter row/column number:3
enter your plain_text:bat

c =

    'UVO'
```

Name:

هايدى محمد عادل حسين

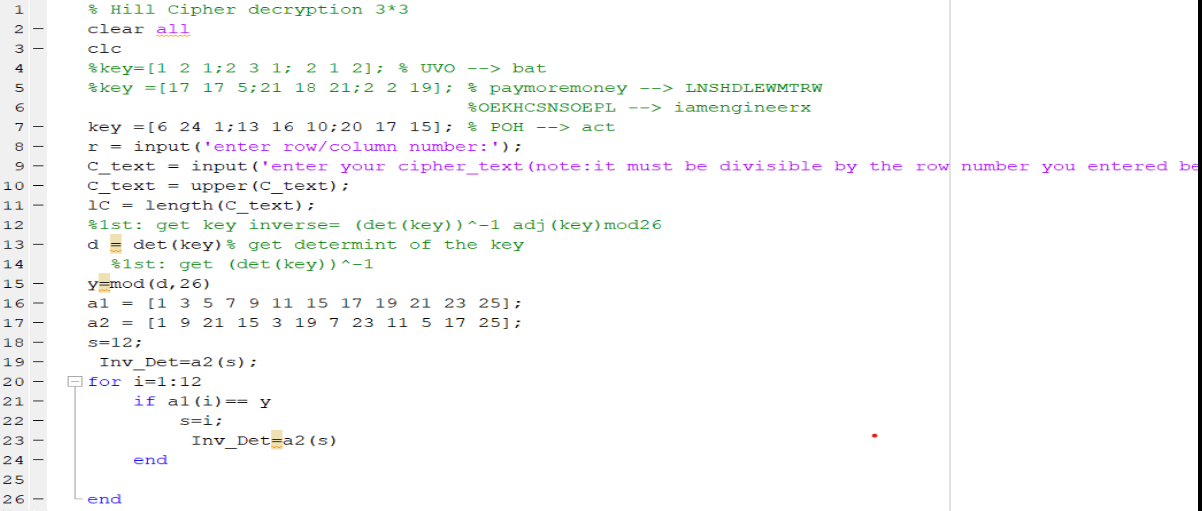
ID:

20012165

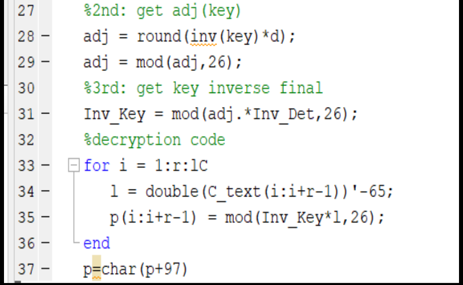
Section: 7

Decryption code:

Code:

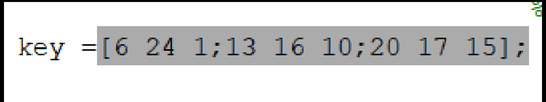


```
% Hill Cipher decryption 3*3
clear all
clc
%key=[1 2 1;2 3 1; 2 1 2]; % UVO --> bat
%key =[17 17 5;21 18 21;2 2 19]; % paymoremoney --> LNSHDLEWMTRW
                                  %OEKHCSNSOEPL --> iamengineerx
key =[6 24 1;13 16 10;20 17 15]; % POH --> act
r = input('enter row/column number:');
C_text = input('enter your cipher_text(note:it must be divisible by the row number you entered be
C_text = upper(C_text);
lC = length(C_text);
%1st: get key inverse= (det(key))^-1 adj(key)mod26
d = det(key)% get determint of the key
  %1st: get (det(key))^-1
y=mod(d,26)
a1 = [1 3 5 7 9 11 15 17 19 21 23 25];
a2 = [1 9 21 15 3 19 7 23 11 5 17 25];
s=12;
 Inv_Det=a2(s);
for i=1:12
    if a1(i)== y
        s=i;
         Inv_Det=a2(s)
    end

end
```

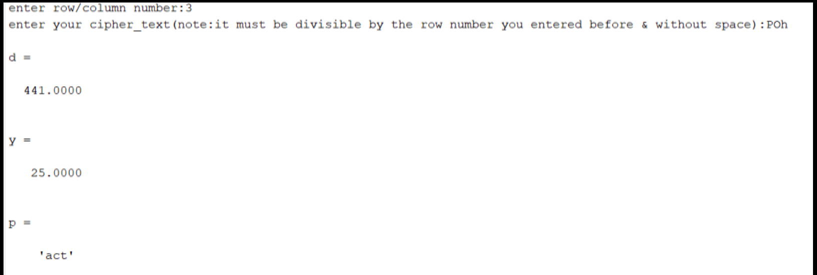


```
%2nd: get adj(key)
adj = round(inv(key)*d);
adj = mod(adj,26);
%3rd: get key inverse final
Inv_Key = mod(adj.*Inv_Det,26);
%decryption code
for i = 1:r:lC
   l = double(C_text(i:i+r-1))'-65;
   p(i:i+r-1) = mod(Inv_Key*l,26);
end
p=char(p+97)
```

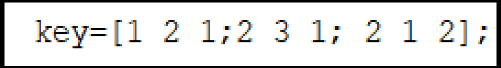
O/P:



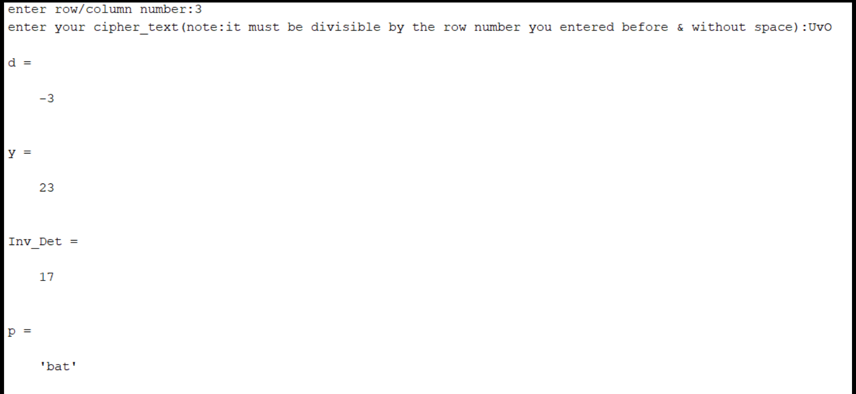
```
key =[6 24 1;13 16 10;20 17 15];
```



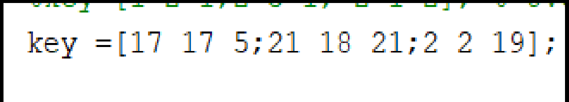
```
enter row/column number:3
enter your cipher_text(note:it must be divisible by the row number you entered before & without space):POh

d =

  441.0000


y =

   25.0000


p =

    'act'
```



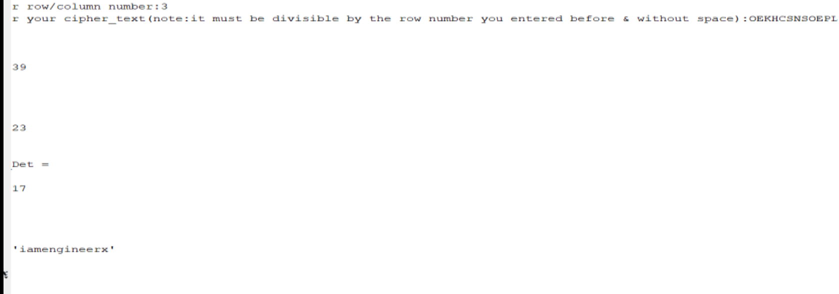
```
key=[1 2 1;2 3 1; 2 1 2];
```



```
enter row/column number:3
enter your cipher_text(note:it must be divisible by the row number you entered before & without space):UvO

d =

    -3


y =

    23


Inv_Det =

    17


p =

    'bat'
```



```
key =[17 17 5;21 18 21;2 2 19];
```



```
r row/column number:3
r your cipher_text(note:it must be divisible by the row number you entered before & without space):OEKHCSNSOEPL


39



23


Det =

17



'iamengineerx'
```

Name:

علاء عبد المنعم الرفاعى

ID:

20010928

Section: 1

Geometric Image Transformations

- Geometric image transformations involve applying various transformations to images, such as:

1. Translation
2. Rotation
3. Scaling
4. Shearing
5. Reflection

- To apply any of these transformations to an image, each pixel's coordinate (x, y) is transformed using matrix multiplication, where the corresponding transformation matrix is multiplied by the homogeneous coordinate vector (x, y, 1). The resulting transformed coordinates (xnew, ynew) can then be used to obtain the pixel values from the original image and construct the transformed image.

- These transformations can be represented and applied using transformation matrices in linear algebra. Let's explore how the transformation matrices associated with these transformations can be applied to images.

1. Translation

- Translation moves an image by shifting its position along the x and y axes.
- The translation matrix is a 3x3 matrix of the form:

$$\begin{bmatrix} 1 & 0 & tx \\ 0 & 1 & ty \\ 0 & 0 & 1 \end{bmatrix}$$

where (tx, ty) represents the amount of translation in the x and y directions, respectively. To apply this transformation to an image, each pixel coordinate (x, y) is multiplied by the translation matrix:

$$\begin{bmatrix} xnew \\ ynew \\ 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & tx \\ 0 & 1 & ty \\ 0 & 0 & 1 \end{bmatrix} * \begin{bmatrix} x \\ y \\ 1 \end{bmatrix}$$

2. Rotation

- Rotation rotates an image by a specified angle around a chosen center point.
- The rotation matrix is a 3x3 matrix of the form:

```
[cos(theta) -sin(theta) 0]
[sin(theta)  cos(theta) 0]
[    0           0          1]
```

where theta represents the angle of rotation in radians. To apply this transformation to an image, each pixel coordinate (x, y) is multiplied by the rotation matrix:

```
[xnew]    [cos(theta) -sin(theta) 0]    [x]
[ynew] = [sin(theta)  cos(theta) 0] * [y]
[ 1     ]    [    0           0          1]    [1]
```

Name:

منة الله أشرف حجاج عبد الجليل

ID: 20012001

Section: 1

3. Scaling

- Scaling resizes an image by multiplying its dimensions by scaling factors along the x and y axes.
- The scaling matrix is a 3x3 matrix of the form:

$$\begin{bmatrix} sx & 0 & 0 \\ 0 & sy & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

where sx and sy represent the scaling factors in the x and y directions, respectively. To apply this transformation to an image, each pixel coordinate (x, y) is multiplied by the scaling matrix:

$$\begin{bmatrix} xnew \\ ynew \\ 1 \end{bmatrix} = \begin{bmatrix} sx & 0 & 0 \\ 0 & sy & 0 \\ 0 & 0 & 1 \end{bmatrix} * \begin{bmatrix} x \\ y \\ 1 \end{bmatrix}$$

4. Shearing

- Shearing distorts an image by shifting points in a specific direction relative to an axis.
- There are different types of shearing, such as:
    a. horizontal shearing (along the x-axis)
    b. vertical shearing (along the y-axis)

  Here, we'll consider horizontal shearing. The shearing matrix for horizontal shearing is a 3x3 matrix of the form:

$$\begin{bmatrix} 1 & shx & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

  where shx represents the shearing factor along the x-axis. To apply this transformation to an image, each pixel coordinate (x, y) is multiplied by the shearing matrix:

$$\begin{bmatrix} xnew \\ ynew \\ 1 \end{bmatrix} = \begin{bmatrix} 1 & shx & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} * \begin{bmatrix} x \\ y \\ 1 \end{bmatrix}$$

5. Reflection

- Reflection flips an image horizontally or vertically. The reflection matrix depends on the axis of reflection. For example, to reflect an image horizontally, the reflection matrix is a 3x3 matrix of the form:

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

To reflect an image vertically, the reflection matrix is:

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

5. Reflection

- To apply the reflection transformation to an image, each pixel coordinate (x, y) is multiplied by the respective reflection matrix:

For horizontal reflection:

$$\begin{bmatrix} \text{xnew} \\ \text{ynew} \\ 1 \end{bmatrix} = \begin{bmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} * \begin{bmatrix} x \\ y \\ 1 \end{bmatrix}$$

For vertical reflection:

$$\begin{bmatrix} \text{xnew} \\ \text{ynew} \\ 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{bmatrix} * \begin{bmatrix} x \\ y \\ 1 \end{bmatrix}$$

In both cases, the reflection matrix alters the sign of either the x-coordinate (horizontal reflection) or the y-coordinate (vertical reflection), effectively flipping the image along the respective axis.

Thanks!