CURSO DE PROFUNDIZACIÓN

MATRICES DISTRIBUIDAS

Maria Trinidad Pimentel Villegas
Instituto Tecnologico Superior del Sur de Guanajuato, ITSUR
maria.pv@surguanajuato.tecnm.mx
maria.pimentel@cimat.mx
https://www.facebook.com/trini.pimentel.3

SESIÓN 1

Sesión	Tema	Fecha	Horas
1	**Programación con Python** **Aplicaciones de Algebra lineal con Python**	13 de junio	3

Subtemas:

1. Operaciones con matrices
2. Codificación y decodificación de mensajes – Programación simple con Excel
3. Aplicaciones con el uso de matrices y sistemas de ecuaciones
4. Python para análisis de datos
    a. Construcción de programas
    b. Listas
    c. Decisiones
    d. Ciclos
    e. Funciones definidas por el usuario.
    f. Aplicaciones

SESIÓN 2

Sesión	Tema	Fecha	Horas
2	***Introducción a Sistemas Distribuidos y Sistemas de Computación***	**20 de junio**	**3**

Subtemas:

1. Sistemas distribuidos
2. Matrices dispersas
3. Optimización de código
4. Ejemplos de optimización de código con algebra lineal y multiplicación de matrices
5. Aplicaciones de optimización de código.

SESIÓN 3

Sesión	Tema	Fecha	Horas
3	***Programación en Paralelo***	**27 de junio**	**3**

Subtemas:

1. Teoría de la computación en paralelo
2. Paralelismo vs. Concurrencia
3. Sincronización
4. Modelos de programación en paralelo
5. Memoria compartida
6. Multiprocesamiento
7. Multihilos

SESIÓN 4

Sesión	Tema	Fecha	Horas
4	***Procesamiento de imágenes y señales.*** ***Imágenes en blanco y negro y escala de grises***	4 de julio	3

Subtemas:

1. Imágenes digitales teoría preliminar
2. Histogramas y estadísticos de imágenes
3. Imágenes binarias
4. Filtros morfológicos
5. Aristas y contornos
6. Filtros

SESIÓN 5

Sesión	Tema	Fecha	Horas
5	***Procesamiento de imágenes y señales.*** ***Imágenes en color***	**Viernes 26 de junio**	**3**

Subtemas:

1. Imágenes en color
2. Espacios de colorimetría
3. Filtros para imágenes en color
4. Interpolación de pixeles

APROBACIÓN DEL CURSO

50% Asistencia
30% Participación
20% Tareas

COMPLEMENTO - CURSO DE MATRICES DISTRIBUIDAS

APLICACIONES DE MATRICES CON PYTHON

SESIÓN 1 - Maria Trinidad Pimentel Villegas
Instituto Tecnologico Superior del Sur de Guanajuato, ITSUR
maria.pv@surguanajuato.tecnm.mx
maria.pimentel@cimat.mx

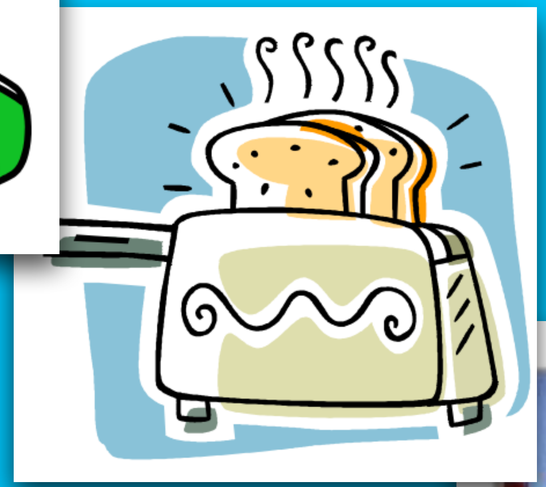
APLICACIONES DIVERSAS

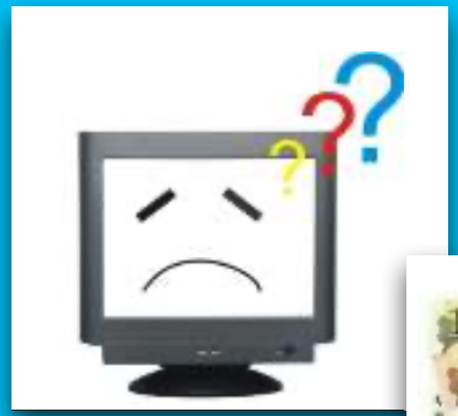
INVERSA DE UNA MATRIZ

Dada una matriz cuadrada **A**, si existe otra matriz **B** del mismo orden que verifique:

$$A \cdot B = B \cdot A = I$$ (I = matriz identidad).

Se dice que **B** es la matriz **inversa** de **A** y se representa por A^{-1}.





Supongamos que tenemos un sistema de n ecuaciones lineales con n incógnitas. Podemos representar el sistema de forma matricial como

$$Ax = b$$

donde

- La matriz A es de dimensión nxn y contiene en cada fila los coeficientes de las incógnitas de cada ecuación.
- La matriz x es de dimensión $nx1$ (una columna) y contiene las n incógnitas del sistema.
- La matriz b es de dimensión $nx1$ y contiene los términos independientes de las ecuaciones.

Si el sistema tiene una única solución (es compatible determinado), entonces la matriz A es **regular** (determinante distinto de 0) y, por tanto, **existe** su matriz inversa A^{-1}.

Entonces, podemos multiplicar toda la ecuación por la inversa de A^{-1}:

$$\begin{aligned} A^{-1} \cdot Ax &= A^{-1} \cdot b \\ x &= A^{-1} \cdot b \end{aligned}$$

Es decir, si la matriz A es regular, entonces la matriz columna resultante del producto matricial $A^{-1} \cdot b$ contiene la **solución** del sistema $Ax = b$.

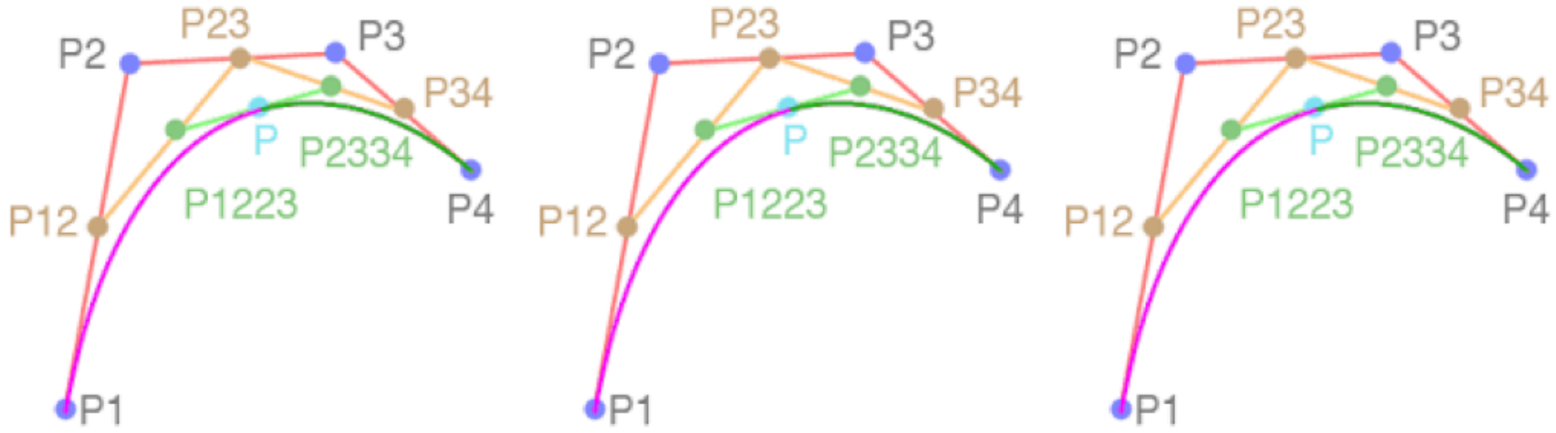
1

Patito computers fabrica tres modelos de computadoras personales: *cañon*, *clon*, y *lenta-pero-segura*. Para armar una computadora modelo *cañon* necesita 12 horas de ensamblado, 2.5 para probarla, y 2 más para instalar sus programas. Para una *clon* requiere 10 horas de ensamblado, 2 para probarla, y 2 para instalar programas. Y por último, para una *lenta-pero-segura* requiere 6 para ensamblado, 1.5 para probarla, y 1.5 para instalar programas. Si la fábrica dispone en horas por mes de 556 para ensamble, 120 para pruebas, y 103 horas para instalación de programas, ¿cuántas computadoras se pueden producir por mes?

2

La granja Thomson tiene 500 hectareas de terreno destinados al cultivo de maiz y frijol, el costo de cultivar cada semilla (incluyendo semillas y mano de obra) es de $42 y $30 por hectarea. El señor Thomson dispone de $18 600 para cultivar. Si desea utilizar toda la tierra destinada a estos cultivos y todo el presupuesto correspondiente, ¿Cuántas hectareas debe plantar de cada cultivo?.

3



Determine la función cuadrática que pasa por los puntos

P(1, 4), Q(−1, 2), y R(2, 3).

4

Un negociante internacional necesita, en promedio, cantidades fijas de yenes japoneses, francos franceses, y marcos alemanes para cada uno de sus viajes de negocios. Este año viajó tres veces. La primera vez cambió un total de $434 a la siguiente paridad: 100 yenes, 1.5 francos y 1.2 marcos por dolar. La segunda vez, cambió un total de $406 con las siguientes tasas: 100 yenes, 1.2 francos, y 1.5 marcos por dolar. La tercera vez cambió $434 en total, a $125 yenes, 1.2 francos, y 1.2 marcos por dolar. ¿Qué cantidades de yenes, francos y marcos compró cada vez?

5

Tres productos químicos X, Y y Z, utilizados en los laboratorios de la Escuela Politécnica Superior de la Universidad de Huelva, tienen los siguientes porcentajes de Fe, Zn y Cu:

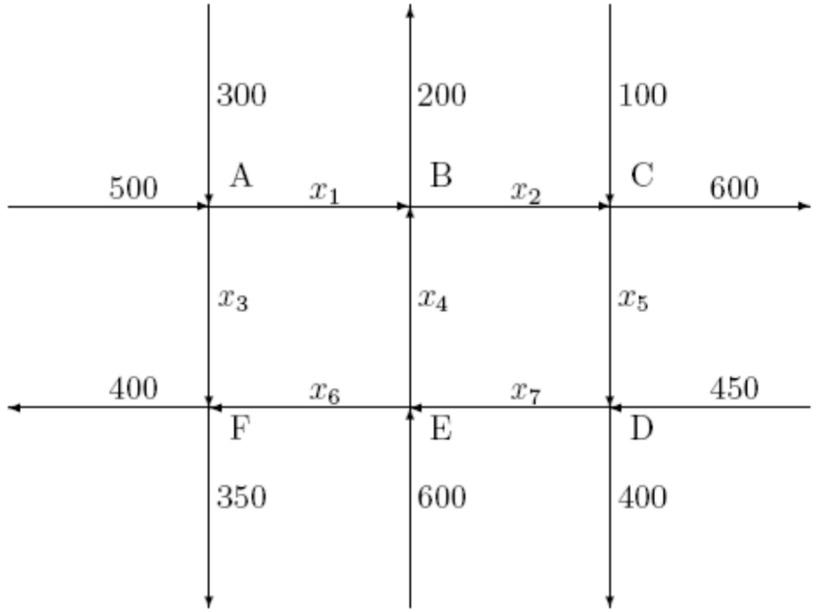
	Fe	Zn	Cu
X	50	30	20
Y	40	30	30
Z	30	70	0

¿Cuánto de cada producto debe combinarse para obtener un nuevo producto que contenga 44% de Fe, 38% de Zn y 18% de Cu?

6

Cruceros puntos Arco Iris cobra $8 por adulto y $4 por niño por un boleto de viaje redondo. Los registros muestran que cierto fin de semana, 1000 personas abordaron el crucero el sábado y 800 el domingo. Los ingresos totales del sábado fueron de $6400 y $4800 el domingo. Utilice la inversa para encontrar ¿Cuántos adultos y niños abordaron el crucero esos días?.

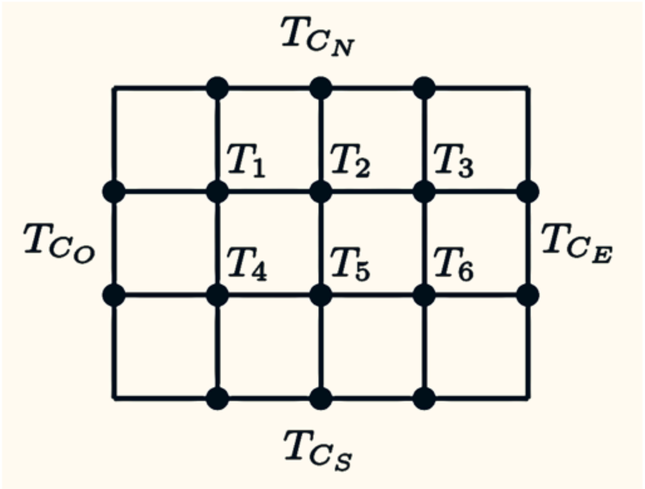
Para analizar el flujo de tráfico de una importante ciudad española como puede ser Barcelor consideremos la siguiente red de calles de una dirección:



Los números indican la cantidad de coches/hora que pasan por ese punto. Las variable $x_1, x_2, \ldots, x_7$, representan el número de coches/hora que pasan de la intersección A a la B, d la B a la C, etc. Suponiendo que en las calles está prohibido aparcar, ¿qué valores tomarán la variables $x_1, x_2, \ldots, x_7$ en los siguientes casos?

8

Un aspecto importante del estudio de la Transferencia de Calor es determinar la temperatura en *estado estable* de una placa delgada cuando se conocen las temperaturas alrededor de la placa. Suponga que la placa de la siguiente figura representa una sección transversal perpendicular a la placa.



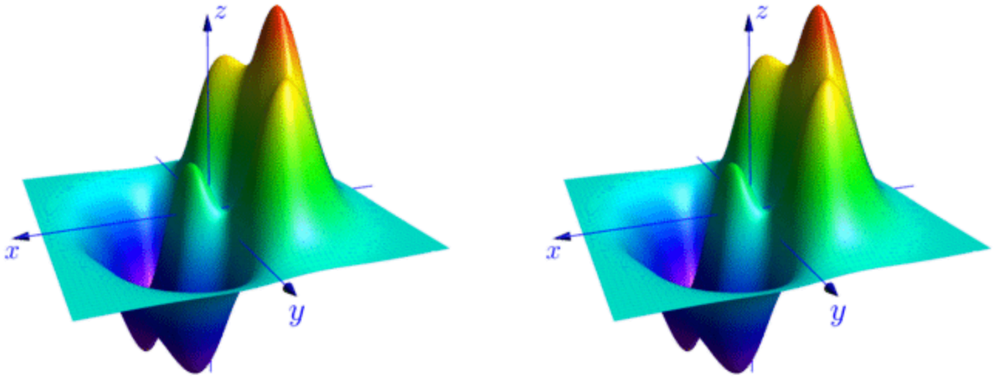
Sean T_1, T_2, T_3, T_4, T_5, y T_6 las temperaturas interiores de los nodos de la red. La temperatura en un nodo es aproximadamente igual al promedio de las temperaturas de los cuatro nodos más cercanos arriba, abajo, a la derecha, y a la izquierda.

Así, por ejemplo

$T_1 = (T_{C_N} + T_2 + T_4 + T_{C_O})/4$. Determine las temperaturas T_1 a T_6 sabiendo que

$T_{C_N} = 25^o, T_{C_E} = 37^o, T_{C_S} = 10^o, T_{C_O} = 31^o$

Reporte solo el valor de T_2.



Conociendo la solución general a una ED:

$$y(t) = C_1\, e^{t} + C_2\, e^{-t} + C_3\, e^{3\,t}$$

Determine en orden los valores de las constantes C_1, C_2, y C_3 para que se cumpla:

$$y(0) = 0,\ y'(0) = -1,\ y''(0) = -2$$

THE BLACK FRIDAY PUZZLE

HTTPS://WWW.COUNTBAYESIE.COM/BLOG/2015/11/21/THE-BLACK-FRIDAY-PUZZLE-UNDERSTANDING-MARKOV-CHAINS —- 2015

THE BLACK FRIDAY PUZZLE

You are the Senior Data Scientist for Bayes Books, a very successful chain of nearly identical bookstores. Living in a post-Amazon age, Bayes Books has diversified their collection and organized their stores into 5 main sections: Books, Children's Books, Puzzles, Toys, and Music. The most important problem for the store is optimizing the number of Sales Associates in each section. Past research has shown that 1 employee for every 100 customers in a section is the ideal amount to minimize salary cost and optimize sales.

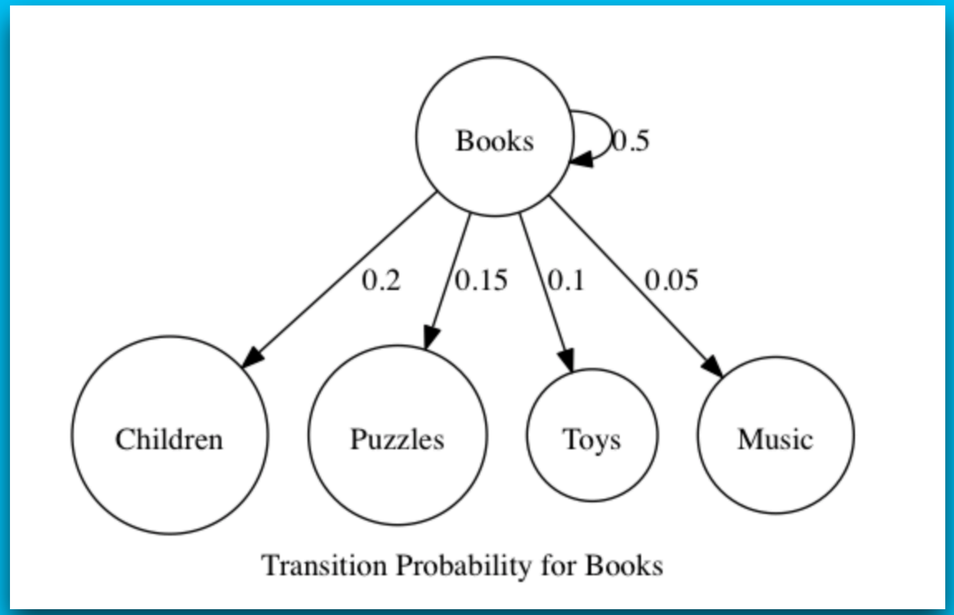
Under normal circumstances customers flow through the store in a very predictable pattern, given the average number of customers it is easy to figure out how many Sales Associates to put in each section. But on Black Friday all that changes! The customers, consumed with a mystic passion for reduced prices behave in very hard to understand patterns, jumping from section to section erratically!

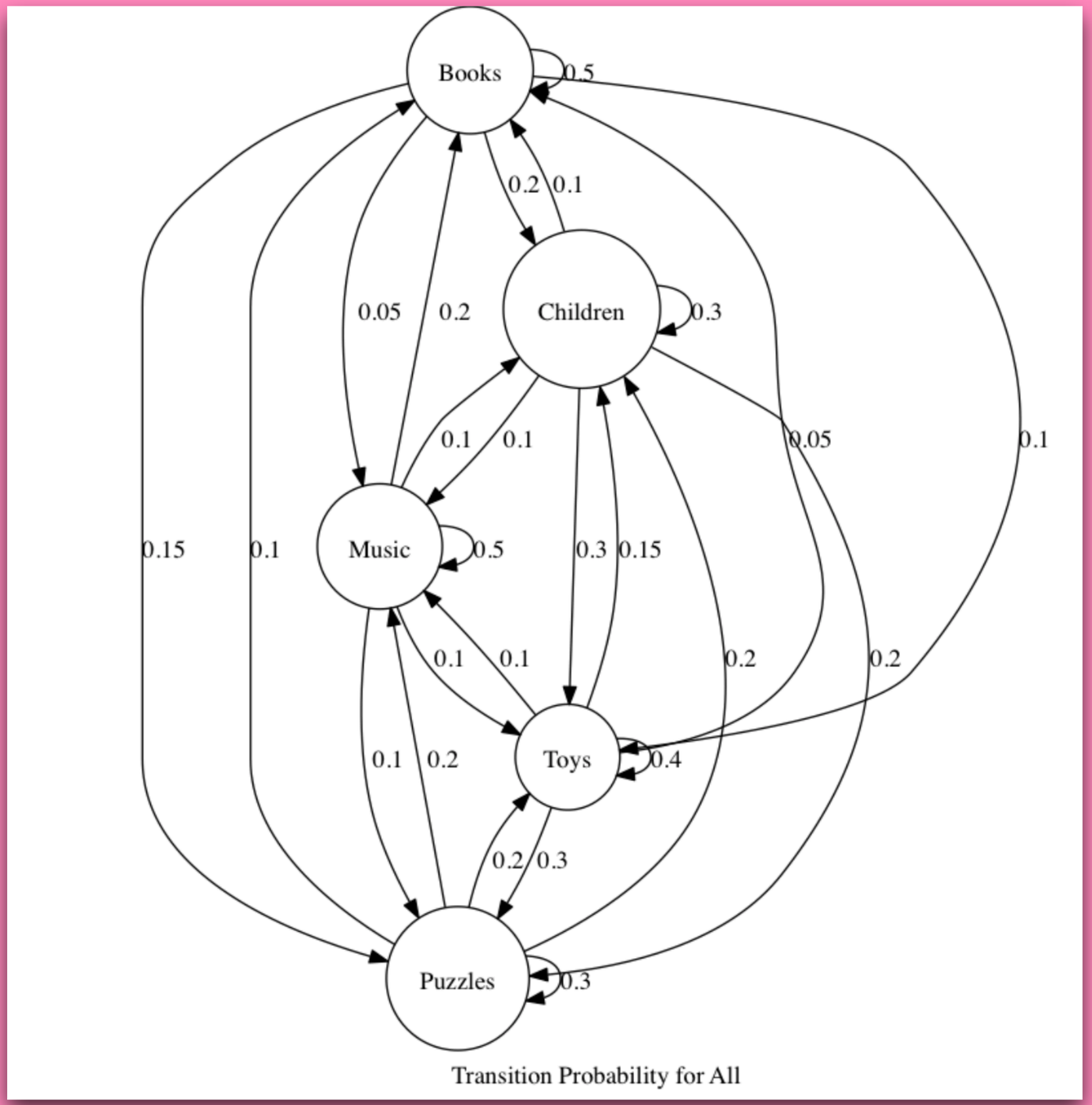
Your responsibility is to determine the ideal number of Sales Associates per section. Immediately you task your Junior Data Scientists with compiling data from past Black Fridays in an attempt to solve this problem. The good news is they developed a deep learning algorithm to predict the total number of customers in the store a given time. Unfortunately, the rest of the analysis looks grim; customers seem to move from section to section at random! Sometimes they will remain in Books for 20 minutes then all of a sudden rush across the store to Music, only to run back to Books a minute later!

The only thing that the Junior Data Scientists can give you is the probability that each customer moves to a given section each minute. For example:

If a customer is in Books, there's a 50% chance they'll stay there, a 20% chance they'll go to Children's Books, a 15% they'll move to Puzzles, 10% chance they'll move to Toys and a 5% chance they'll move to Music.

We can visualize this as a graph of customer movement.





Transition Probability for All

Yikes! The only thing this image helps with is letting us know that this is a pretty crazy problem! We can represent this data is a much easier by putting it in a table.

from ->	Books	Children's	Puzzles	Toys	Music
Books	0.5	0.1	0.1	0.05	0.2
Children's	0.2	0.3	0.2	0.15	0.1
Puzzles	0.15	0.2	0.3	0.3	0.1
Toys	0.1	0.3	0.2	0.4	0.1
Music	0.05	0.1	0.2	0.1	0.5

Transition graph in table form

MARKOV CHAIN

The problem we've outlined so far is formally called a Markov Chain. The key things that make this a Markov Chain are that each person transitions from each state probabilistically *and* the only state that matters is where the person currently is.

Normally there might be a relationship between starting in Books, moving to Children's Books and then going to Toys. Because of the Black Friday frenzy customers move only based on where they currently are, running back and forth across the store multiple times is a possible behavior.

To put it more poetically: In a Markov Chain the future is uncertain, and all that matters for tomorrow is where you are today.

EXPECTED NUMBER OF SALES ASSOCIATES

We want to know how many Sales Associates to put in each area. As always when dealing with a hard probability problem it's always best to start with a simplification; study how it behaves and add complexity from there.

Let's say there are 100 people in Books right now (and nobody anywhere else). We're assuming that our movements are all happening in 1-minute chunks. That is with the tick of each minute people move based on the table above. To keep this simple, we only care about the expected people in Books.

$$n_{books\_t}$$

number of people in books at time *t*

$$p_{x \to books}$$

probability of transitions from *x* to Books

EXPECTED NUMBER OF SALES ASSOCIATES

For our first time step all we care about is how many people are expected to stay in Books

$$E[n_{books\_1}] = p_{books \to books} \cdot n_{books\_0} = 0.5 \cdot 100 = 50$$

That was easy, but as soon as we take our next step it gets much more complicated. Now we have to consider how many people are going to come back to Books from other states!

$$E[n_{books\_2}] = p_{books \to books} \cdot n_{books\_1} + p_{children \to books} \cdot n_{children\_1} + p_{puzzles \to books} \cdot n_{puzzles\_1} \cdots$$

If you had some free time you could feasibly calculate that by hand, but step 3 is even worse that that! For step 3 we additionally have to recalculate the populations of each area of the store which is an identical process to the one for Books!

LINEAR ALGEBRA TO THE RESCUE!

This pattern of calculation is exactly how Matrix Multiplication works! Specifically it would be the dot product of our Transition Matrix.

and a vector of our initial populations. To make this a bit more clear, we can represent our table of Transition Probabilities as a Matrix:

$$\begin{bmatrix} 0.5 & 0.1 & 0.1 & 0.05 & 0.2 \\ 0.2 & 0.3 & 0.2 & 0.15 & 0.1 \\ 0.15 & 0.2 & 0.3 & 0.3 & 0.1 \\ 0.1 & 0.3 & 0.2 & 0.4 & 0.1 \\ 0.05 & 0.1 & 0.2 & 0.1 & 0.5 \end{bmatrix}$$

Our simple model of 100 people in Books looks like this:

$$\begin{bmatrix} 100 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

LINEAR ALGEBRA TO THE RESCUE!

We calculate step 1 from before by taking the dot product of the Transition Matrix with our Vector representing our population at t=0

$$\begin{bmatrix} 0.5 & 0.1 & 0.1 & 0.05 & 0.2 \\ 0.2 & 0.3 & 0.2 & 0.15 & 0.1 \\ 0.15 & 0.2 & 0.3 & 0.3 & 0.1 \\ 0.1 & 0.3 & 0.2 & 0.4 & 0.1 \\ 0.05 & 0.1 & 0.2 & 0.1 & 0.5 \end{bmatrix} \cdot \begin{bmatrix} 100 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 50 \\ 20 \\ 15 \\ 10 \\ 5 \end{bmatrix}$$

To calculate step 2 we simply replace our original population vector with the new one:

$$\begin{bmatrix} 0.5 & 0.1 & 0.1 & 0.05 & 0.2 \\ 0.2 & 0.3 & 0.2 & 0.15 & 0.1 \\ 0.15 & 0.2 & 0.3 & 0.3 & 0.1 \\ 0.1 & 0.3 & 0.2 & 0.4 & 0.1 \\ 0.05 & 0.1 & 0.2 & 0.1 & 0.5 \end{bmatrix} \cdot \begin{bmatrix} 50 \\ 20 \\ 15 \\ 10 \\ 5 \end{bmatrix} = \begin{bmatrix} 30.0 \\ 21.0 \\ 19.5 \\ 18.5 \\ 11.0 \end{bmatrix}$$

And of course, step 3, which would have taken most of an evening to calculate by hand, is just the same thing repeated!

$$\begin{bmatrix} 0.5 & 0.1 & 0.1 & 0.05 & 0.2 \\ 0.2 & 0.3 & 0.2 & 0.15 & 0.1 \\ 0.15 & 0.2 & 0.3 & 0.3 & 0.1 \\ 0.1 & 0.3 & 0.2 & 0.4 & 0.1 \\ 0.05 & 0.1 & 0.2 & 0.1 & 0.5 \end{bmatrix} \cdot \begin{bmatrix} 30.0 \\ 21.0 \\ 19.5 \\ 18.5 \\ 11.0 \end{bmatrix} = \begin{bmatrix} 22.175 \\ 20.075 \\ 21.200 \\ 21.700 \\ 14.850 \\ \\ \end{bmatrix}$$

THE STATIONARY DISTRIBUTION!

WHAT HAPPENS IF WE KEEP ON DOING THIS? AFTER 30 STEPS OF THIS PROCESS...

HERE IS OUR POPULATION VECTOR:

$$\begin{bmatrix} 17.90006 \\ 18.86964 \\ 21.67067 \\ 22.77285 \\ 18.78677 \end{bmatrix}$$

And then after 1,000 steps???

HERE IS OUR POPULATION VECTOR:

$$\begin{bmatrix} 17.90006 \\ 18.86964 \\ 21.67067 \\ 22.77285 \\ 18.78677 \end{bmatrix}$$

And then after 1,000 steps???

$$\begin{bmatrix} 17.90006 \\ 18.86964 \\ 21.67067 \\ 22.77285 \\ 18.78677 \end{bmatrix}$$

REMARKABLE! THEY'RE IDENTICAL!

What if we started with a different initial population:

$$\begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 100 \end{bmatrix}$$ repeat 1000x

What if we started with a different initial population:

$$\begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 100 \end{bmatrix} \text{repeat 1000x} \begin{bmatrix} 17.90006 \\ 18.86964 \\ 21.67067 \\ 22.77285 \\ 18.78677 \end{bmatrix}$$

IT'S STILL THE SAME!

THE REMARKABLE THING ABOUT MARKOV CHAINS IS, AS LONG AS YOU CAN GET TO ANY STATE FROM ANY STATE IN A FINITE NUMBER OF STEPS, THE DISTRIBUTION OF THE POPULATION IN EACH STATE REMAINS THE SAME. THIS IS REFERRED TO AS THE STATIONARY DISTRIBUTION OF A MARKOV CHAIN.

PUTTING OUR ANSWER TOGETHER

Your team of Junior Data Scientists has put a bunch of data in a Deep Neural Net and determined that for a particular store there should be a pretty stable population of 6,000 people throughout Black Friday. If we look at our stable distribution as a percentage of the whole population we can just perform scalar multiplication and get our answer:

$$6,000 \cdot \begin{bmatrix} 0.1790006 \\ 0.1886964 \\ 0.2167067 \\ 0.2277285 \\ 0.1878677 \end{bmatrix} = \begin{bmatrix} 1074.003 \\ 1132.179 \\ 1300.240 \\ 1366.371 \\ 1127.206 \end{bmatrix}$$

PUTTING OUR ANSWER TOGETHER

$$6,000 \cdot \begin{bmatrix} 0.1790006 \\ 0.1886964 \\ 0.2167067 \\ 0.2277285 \\ 0.1878677 \end{bmatrix} = \begin{bmatrix} 1074.003 \\ 1132.179 \\ 1300.240 \\ 1366.371 \\ 1127.206 \end{bmatrix}$$

Given that we need 1 Sales Associate per 100 customers, rounding our answers, we should have 11 Sales Associates in Books, 11 in Children's, 13 in Puzzels, 14 in Toys and 11 in Music. Given the complexity we started with its amazing that just a little Linear Algebra gives us pretty quick and clear answer!

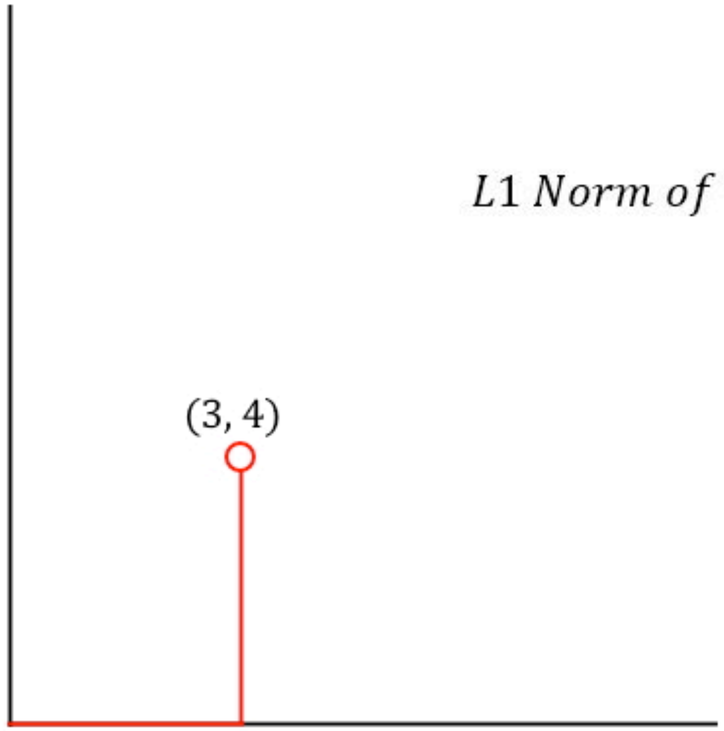
LOSS FUNCTION - FUNCIÓN DE PERDIDA

You must be quite familiar with how a model, say a Linear Regression model, fits a given data:

- You start with some arbitrary prediction function (a linear function for a Linear Regression Model)
- Use it on the independent features of the data to predict the output
- Calculate how far-off the predicted output is from the actual output
- Use these calculated values to optimize your prediction function using some strategy like Gradient Descent

A loss function is an application of the Vector Norm in Linear Algebra. The norm of a vector can simply be its magnitude. There are many types of vector norms

Manhattan Distance or L1 Norm

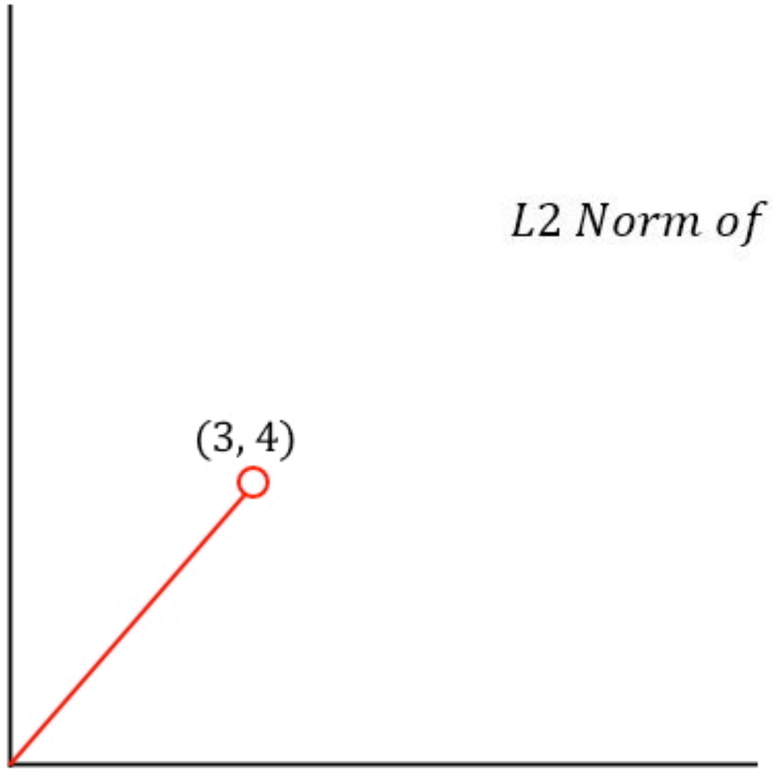


$$L1\ Norm\ of\ vector\ V = (v_1, v_2, \ldots, v_n)$$

$$||V||_1 = |v_1| + |v_2| + \cdots + |v_n|$$

L1 Norm: **Also known as the Manhattan Distance or Taxicab Norm. The L1 Norm is the distance you would travel if you went from the origin to the vector if the only permitted directions are parallel to the axes of the space.**

Euclidean Distance or L2 Norm



$$L2\ Norm\ of\ vector\ V = (v_1, v_2, \dots, v_n)$$

$$\left|\left|V\right|\right|_2 = \sqrt{v_1^2 + v_2^2 + \cdots + v_n^2}$$

L2 Norm: **Also known as the Euclidean Distance. L2 Norm is the shortest distance of the vector from the origin.**

This distance is calculated using the Pythagoras Theorem

TOTAL LOSS FOR THE PREDICTION

But how is the norm used to find the difference between the predicted values and the expected values? Let's say the predicted values are stored in a vector P and the expected values are stored in a vector E.

$$\text{Total loss} = P - E$$

CRIPTOGRAFÍA

CODIFICACIÓN Y DECODIFICACIÓN DE MENSAJES

CRIPTOGRAFÍA - DEFINICIÓN

- La criptografía de acuerdo con Williams (2002) es el proceso de codificar y decodificar mensajes. Esta palabra viene del griego *kriptos*, que significa “oculto”.
- El origen de esta técnica se encuentra en la Grecia Antigua.
- Hoy día existen técnicas sofisticadas para codificar y decodificar mensajes.
- Un tipo de código muy difícil de descifrar es el que maneja una matriz muy grande para codificar el mensaje.
- El receptor del mensaje lo decodifica usando la matriz decodificadora.

** CODIFICANDO UN MENSAJE **

SEA EL MENSAJE:

LISTOS PARA ATACAR

Y LA **MATRIZ CODIFICADORA** SEA

$$C = \begin{bmatrix} 3 & 6 & 2 \\ 2 & 3 & 1 \\ 3 & 1 & 1 \end{bmatrix}$$

A cada letra del alfabeto se la asigna un número (consideraremos 26 caracteres sin ningún caso especial). Por comodidad se asigna a cada letra con su posición en el alfabeto: A es 1, B es 2, y así sucesivamente.

A	1
B	2
C	3
D	4
E	5
F	6
G	7
H	8
I	9
J	10
K	11
L	12
M	13
N	14
O	15
P	16
Q	17
R	18
S	19
T	20
U	21
V	22
W	23
X	24
Y	25
Z	26
*	27

A cada letra del alfabeto se la asigna un número (consideraremos 26 caracteres sin ningún caso especial). Por comodidad se asigna a cada letra con su posición en el alfabeto: A es 1, B es 2, y así sucesivamente.

L	I	S	T	O	S	*	P	A	R	A	*	A	T	A	C	A	R
12	9	19	20	15	19	27	16	1	18	1	27	1	20	1	3	1	18

Como se usará una matriz de 3x3 para codificar el mensaje, divida el mensaje numerado en matrices columna de 3x1, de la siguiente manera

$$Mensaje = \begin{bmatrix} 12 & 20 & 27 & 18 & 1 & 3 \\ 9 & 15 & 16 & 1 & 20 & 1 \\ 19 & 19 & 1 & 27 & 1 & 18 \end{bmatrix}$$

Se escriben las matrices columna como columnas de matriz y se multiplican por la matriz codificadora, de la siguiente forma

(3x3)	(3x6)	(3x6)
Codificadora	Mensaje	Mensaje Codificado

$$\begin{bmatrix} 3 & 6 & 2 \\ 2 & 3 & 1 \\ 3 & 1 & 1 \end{bmatrix} \begin{bmatrix} 12 & 20 & 27 & 18 & 1 & 3 \\ 9 & 15 & 16 & 1 & 20 & 1 \\ 19 & 19 & 1 & 27 & 1 & 18 \end{bmatrix} = \begin{bmatrix} 128 & 188 & 179 & 114 & 125 & 51 \\ 70 & 104 & 103 & 66 & 63 & 27 \\ 64 & 94 & 98 & 82 & 24 & 28 \end{bmatrix}$$

Mensaje codificado

128,70,64,188,104,94,179,103,98,114,66,82,125,63,24,51,27,28

** DECODIFICANDO EL MENSAJE **

SEA EL MENSAJE CODIFICADO:

Mensaje codificado

128,70,64,188,104,94,179,103,98,114,66,82,125,63,24,51,27,28

Y LA **MATRIZ DECODIFICADORA** SEA

$$C^{-1} = \begin{bmatrix} -1 & 2 & 1 \\ -5 & 1.5 & -5 \\ 3.5 & -7.5 & 1.5 \end{bmatrix}$$

La decodificadora y el mensaje se multiplican

(3x3)			(3x6)						(3x6)					
Decodificadora			Mensaje codificado						Mensaje Original					
-1	2	1	128	188	179	114	125	51	12	20	27	18	1	3
-5	1.5	-5	70	104	103	66	63	27	9	15	16	1	20	1
3.5	-7.5	1.5	64	94	98	82	24	28	19	19	1	27	1	18

Las columnas de esta matriz producen el mensaje original:

L	I	S	T	O	S	*	P	A	R	A	*	A	T	A	C	A	R
12	9	19	20	15	19	27	16	1	18	1	27	1	20	1	3	1	18

RETO .... DESCIFRA EL SIGUIENTE MENSAJE

Mensaje codificado

129,69,54,150,86,98,58,31,33,203,102,49,73,38,23,70,42,50

$$C = \begin{bmatrix} 3 & 6 & 2 \\ 2 & 3 & 1 \\ 3 & 1 & 1 \end{bmatrix}$$

MENSAJE

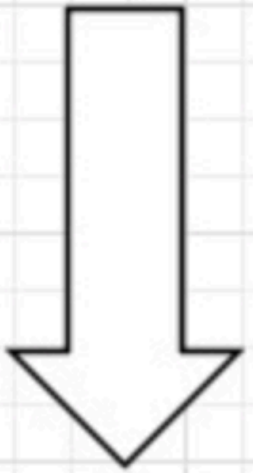
CIFRADO POR

TRANSPOSICIÓN

ESCRITURA INVERSA

Plain Text

H E L L O



Cipher Text

O L L E H

TIPOS DE TRANSPOSICIÓN

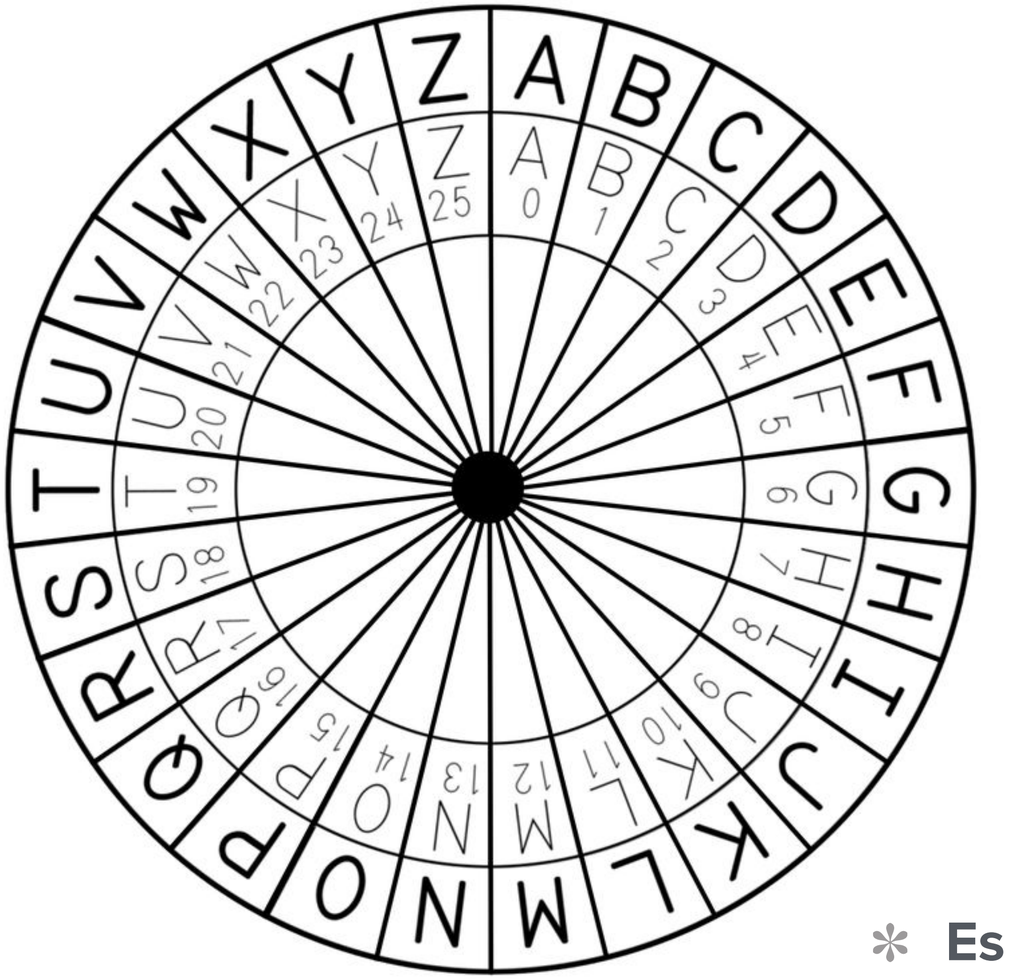
- Transposición por ruta
- Transposición china
- Escítala
- Permutación de grupos
- Permutación por series

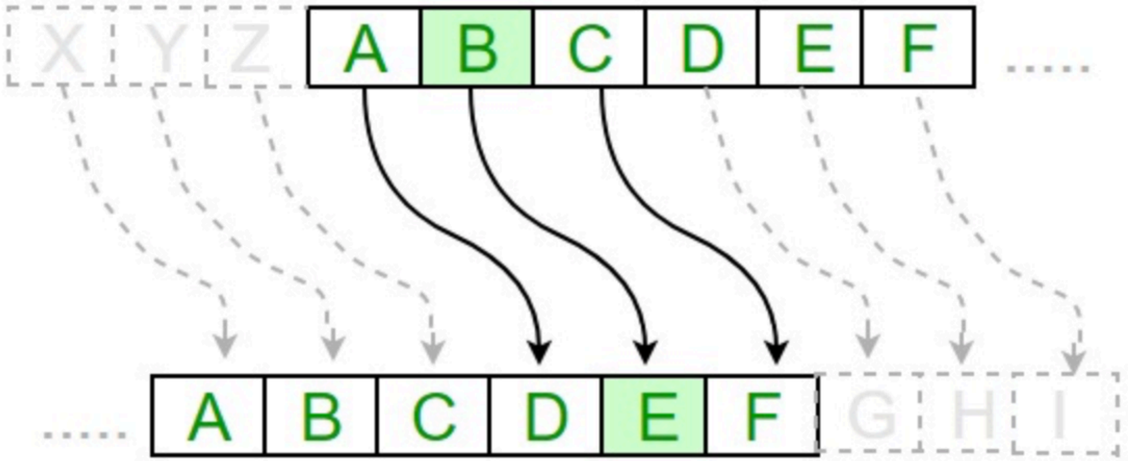
- Escritura Inversa
- Transposición columnar simple
- Transposición columnar doble
- Transposición interrumpida
- AMSCO

- Transposición indefinida
- Rejillas criptográficas
- Paralelo vertical
- Cifrado por riel

https://es.wikipedia.org/wiki/Cifrado_por_transposición

CIFRADO CESAR





- Es un tipo simple de cifrado por sustitución.
- Cada letra de un texto plano es sustituida por una letra con un número fijo de posiciones.

https://www.youtube.com/watch?v=l6jqKRXSShI

CIFRADO VIGNERE

Vignere Tableau

The tableau used for Vignere cipher is as shown below –

	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
A	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
B	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	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	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
N	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
O	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	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	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

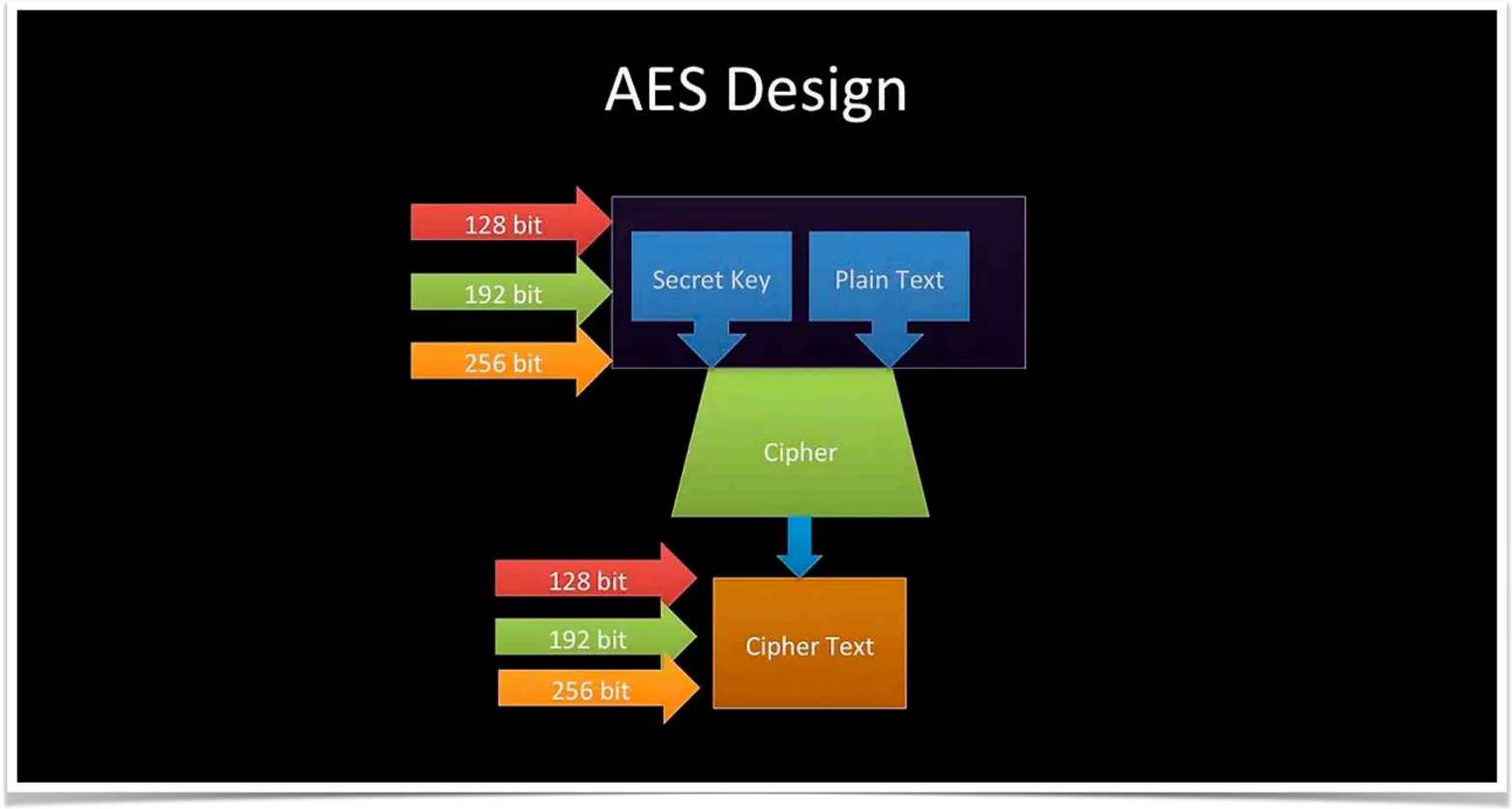
Es un cifrado basado en diferentes series de caracteres o letras del **cifrado César**

formando estos caracteres una tabla, llamada tabla de Vigenère, que se usa como clave.

El cifrado de Vigenère es un **cifrado de sustitución** simple polialfabético.

https://www.youtube.com/watch?v=SkJcmCaHqS0

CIFRADO AES-256 BITS



https://hardzone.es/tutoriales/rendimiento/cifrado-aes-256-bits-como-funciona/

GRACIAS POR SU ATENCIÓN