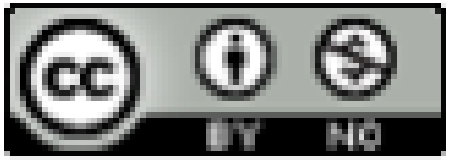
Presentado en eXIDO18 (2018)

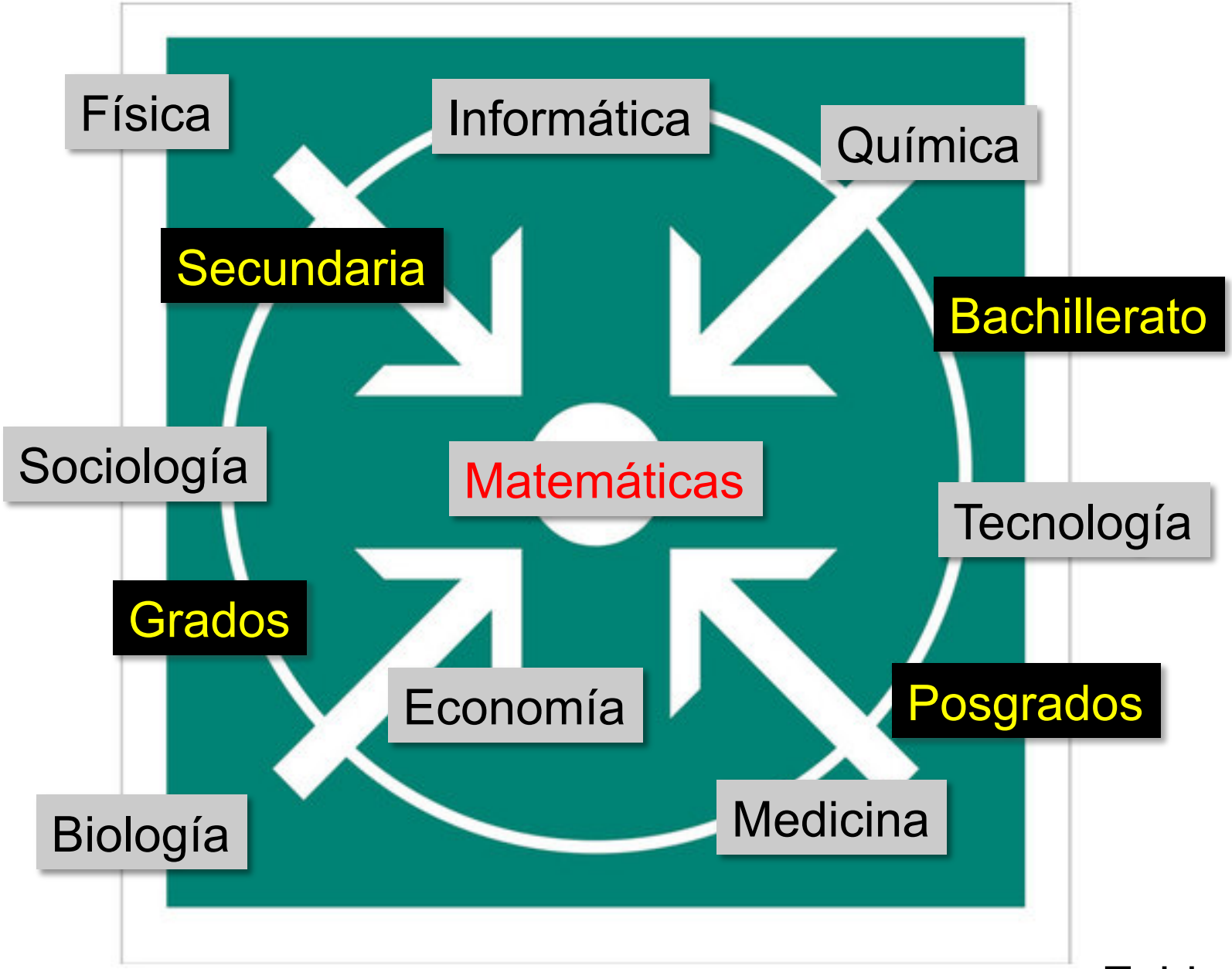


Agradecimientos

- Al C.A. de la UNED y a su director el Prof. Andrés Medina
- A Antonio Costa
- A los compañeros con los que trabajo
- A Miguelón

Miguel; me acuerdo de ti,
después del sol y del polvo,
antes de la misma luna,
tumba de un sueño amoroso.

Miguel Hernández

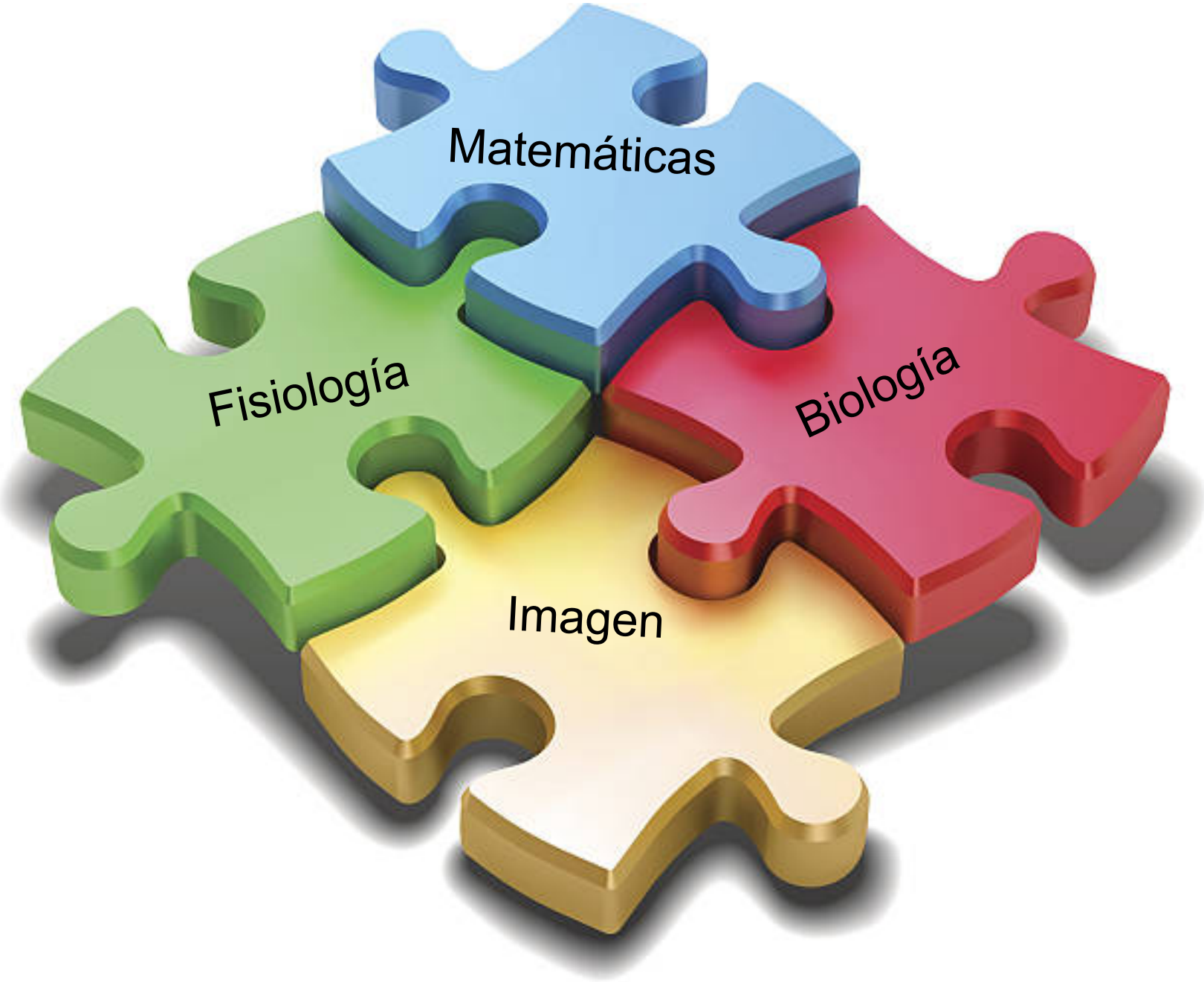

Física
Informática
Química
Secundaria
Bachillerato
Sociología
Matemáticas
Tecnología
Grados
Economía
Posgrados
Biología
Medicina

Exido ‘18


FOR TEN YEARS ONE WOMAN
NEVER STOPPED SEARCHING FOR THE
MOST WANTED MAN IN HISTORY
ZERO DARK THIRTY
FROM THE ACADEMY AWARD-WINNING WRITER AND DIRECTOR OF
THE HURT LOCKER
NAR LA GUERRA
UNA MAGISTRAL INTERPRETACIÓN DE BENEDICT CUMBERBATCH.
EXCEPCIONAL.
★★★★★
★★★★★
THE IMITATION GAME
BENEDICT CUMBERBATCH
KEIRA KNIGHTLEY
(DESCIFRANDO ENIGMA)
DESCIFRA EL SECRETO
QUE CAMBIARÁ EL DESTINO DEL MUNDO
Julio Verne
LA JANGADA
A message from deep space.
Who will be the first to go?
A journey to the heart of the universe.
CONTACT
ENIGMA
una película de MICHAEL APTED
DOUGRAY SCOTT
KATE WINSLET
JEREMY NORTHAM
SAFF
Intermedia
SOGEPAQ
www.plus.es/enigma

FOR TEN YEARS ONE WOMAN
NEVER STOPPED SEARCHING FOR THE
MOST WANTED MAN IN HISTORY

FROM THE ACADEMY AWARD®-WINNING WRITER AND DIRECTOR OF
THE HURT LOCKER


Matemáticas
Fisiología
Biología
Imagen

Criptografía, sistemas dinámicos e imagen: otras formas de encriptar/cifrar mensajes

JC Antoranz
Ciencias-UNED

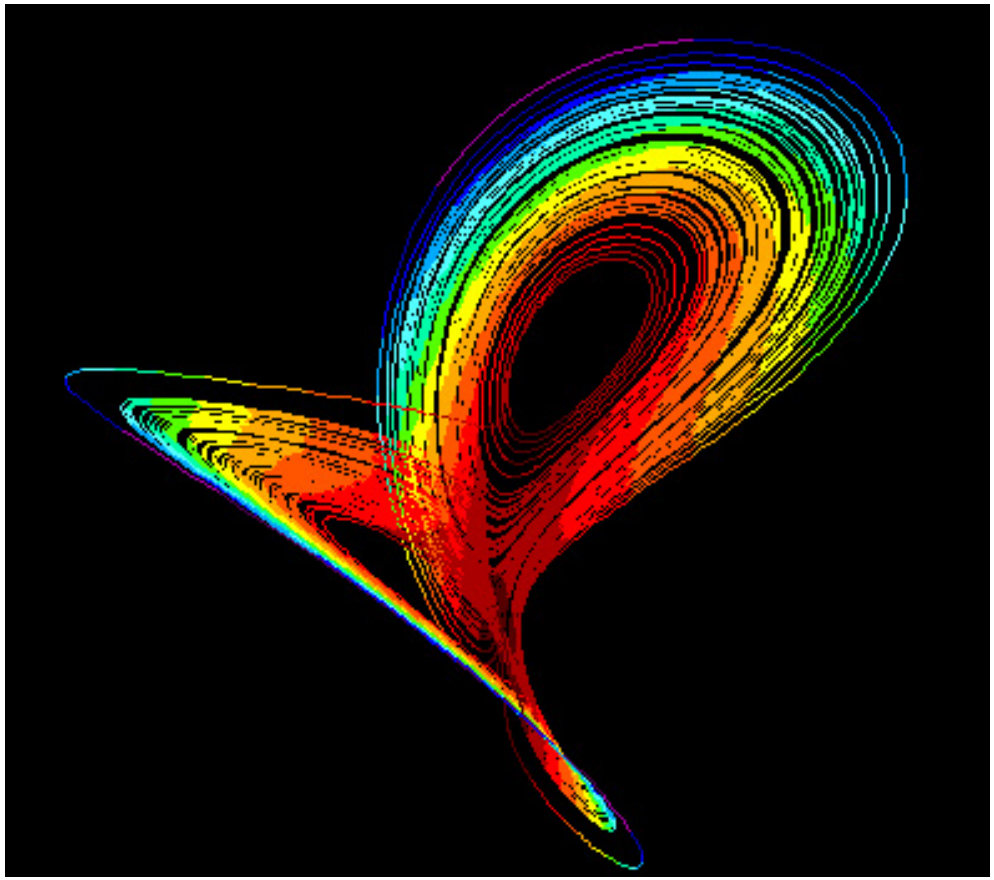
Laboratorio de Medida Avanzada por Imagen
Dpto. Física Matemática y de Fluidos
UNED

Doyne Farmer

"Nonlinear was a word that you only encountered in the back of the book. A physics student would take a math course and the last chapter would be on nonlinear equations. you would usually skip that, and, if you didn't, all they would do is take these nonlinear equations and reduce them to linear equations, so you just get approximate solutions anyway. It was just an exercise in frustration"

http://www.dewtronics.com/tutorials/roulette/eudaemons/eudaemons.html

Atractor de Lorenz: Washington, 29-12-79



Predictability:
Does the flap of a Butterfly's wings in Brazil set off a tornado in Texas?
E. Lorenz, Ame. Asoc. Advancement of Science., 1972.

Random vs Caótico

- Random
  - Se desconoce la causa y sólo tenemos conocimiento de magnitudes estadísticas
- Caótico
  - Sistemas deterministas donde las interacciones, aún conocidas, son tan complicadas que no puede predecirse el comportamiento del sistema
  - Sistemas deterministas no lineales

El modelo de Lorenz

$$dx/dt = \sigma(x - y)$$

$$dy/dt = rx - y - xz$$

$$dz/dt = xy - bz$$

σ es el Número de Prandtl y *r* es el número de Rayleigh.

Lorenz, E. N. (1963). «Deterministic nonperiodic flow». J. Atmos. Sci. 20 p. 130-141.

Comportamiento de SD no lineales

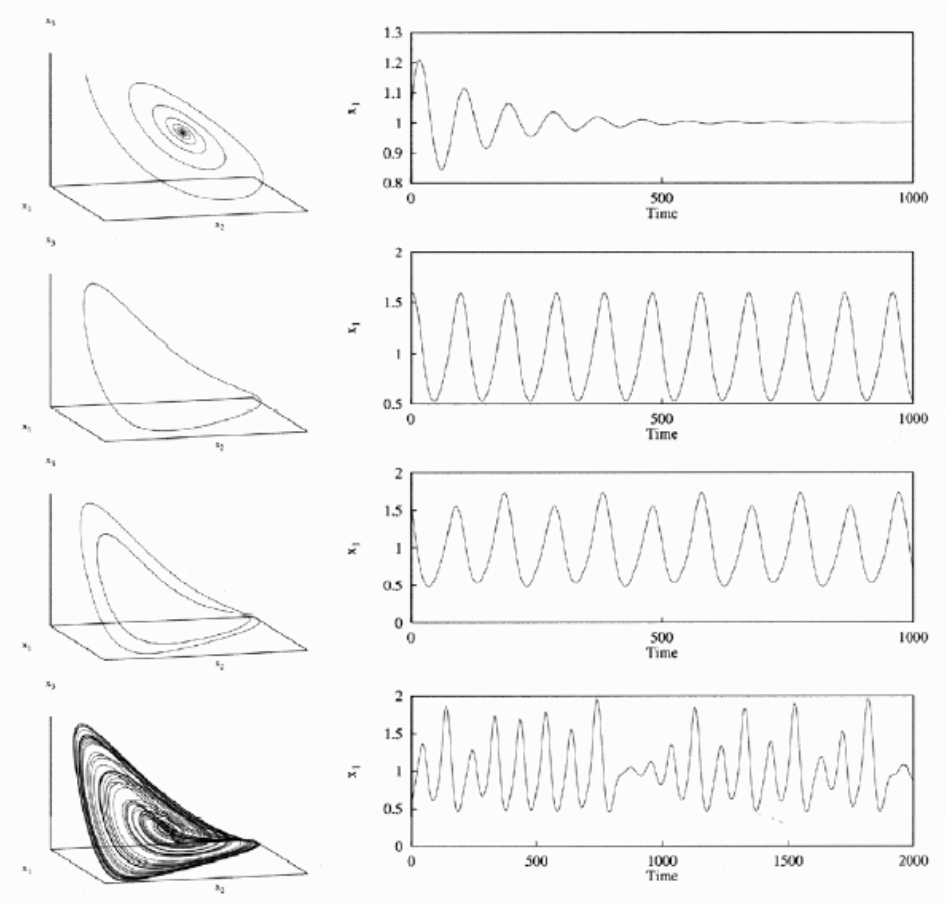
(a) Fixed points

(b) Simple periodic orbits

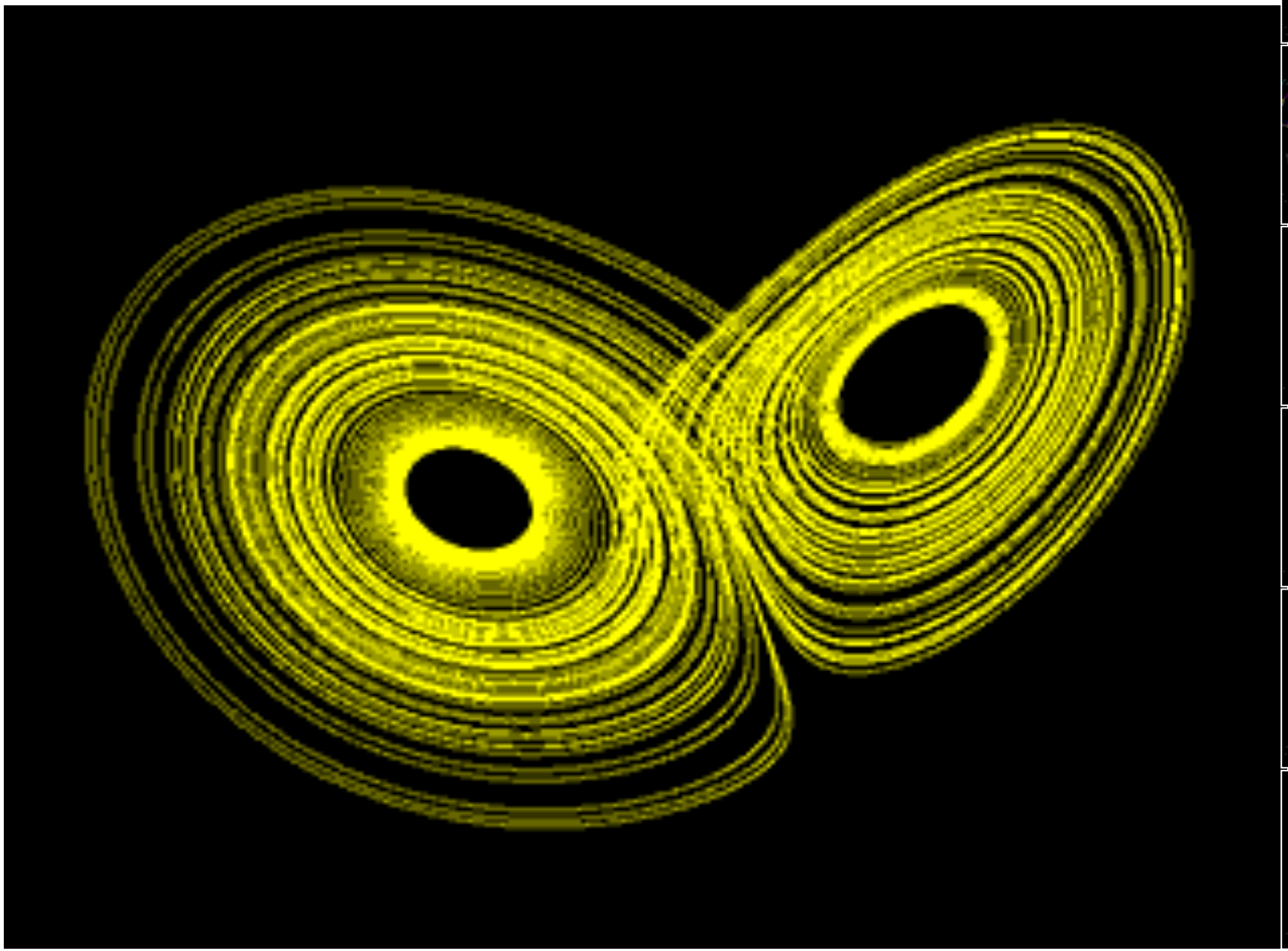
(c) Period-n orbit

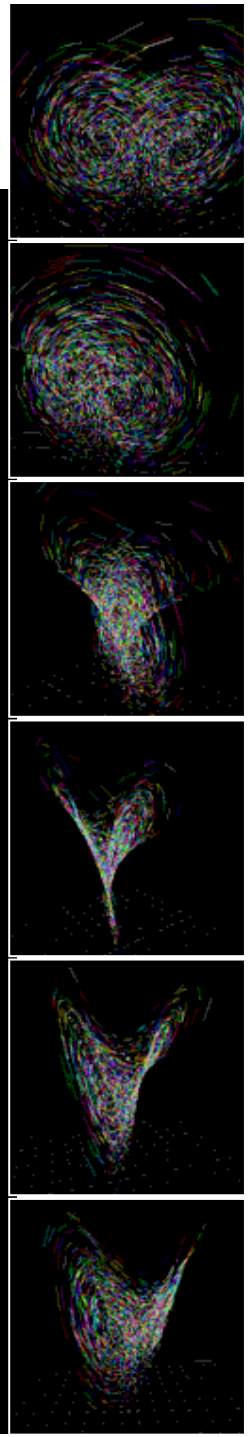
Quasi-periodic

(d) Chaos

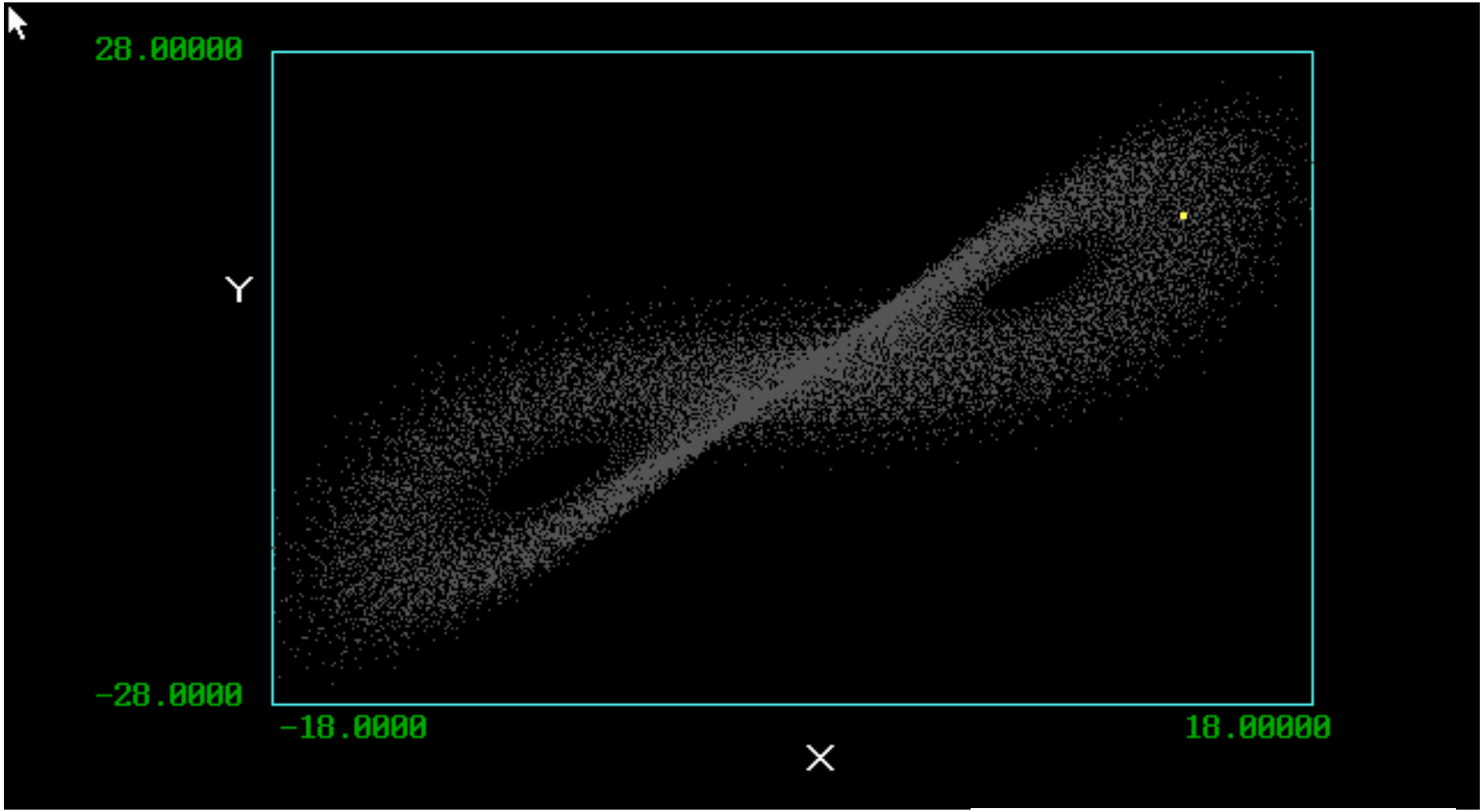


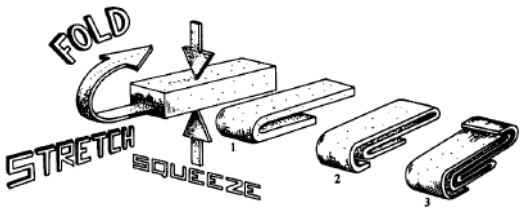
El atractor de Lorenz



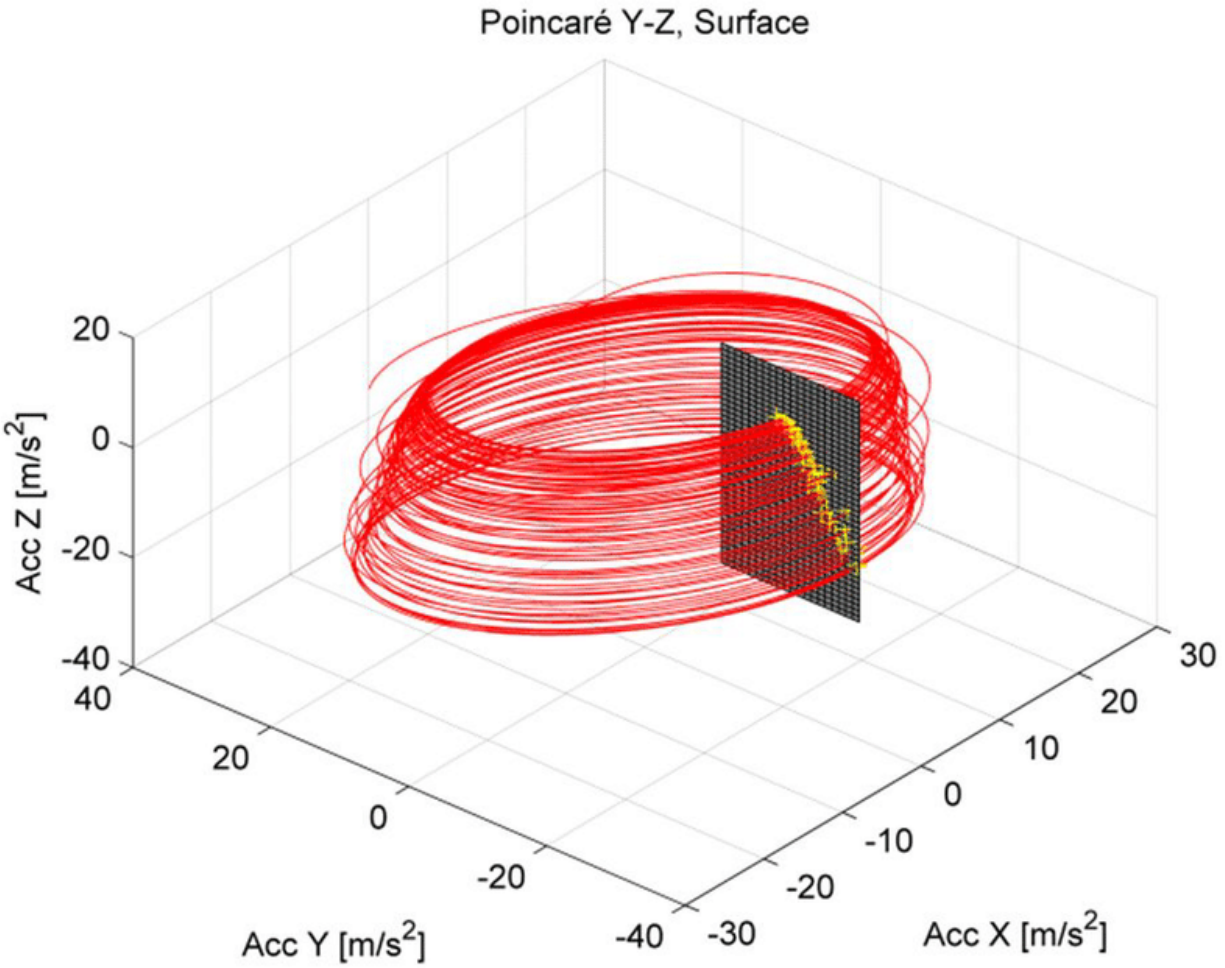


Atractor de Lorenz: Estirar, comprimir y doblar



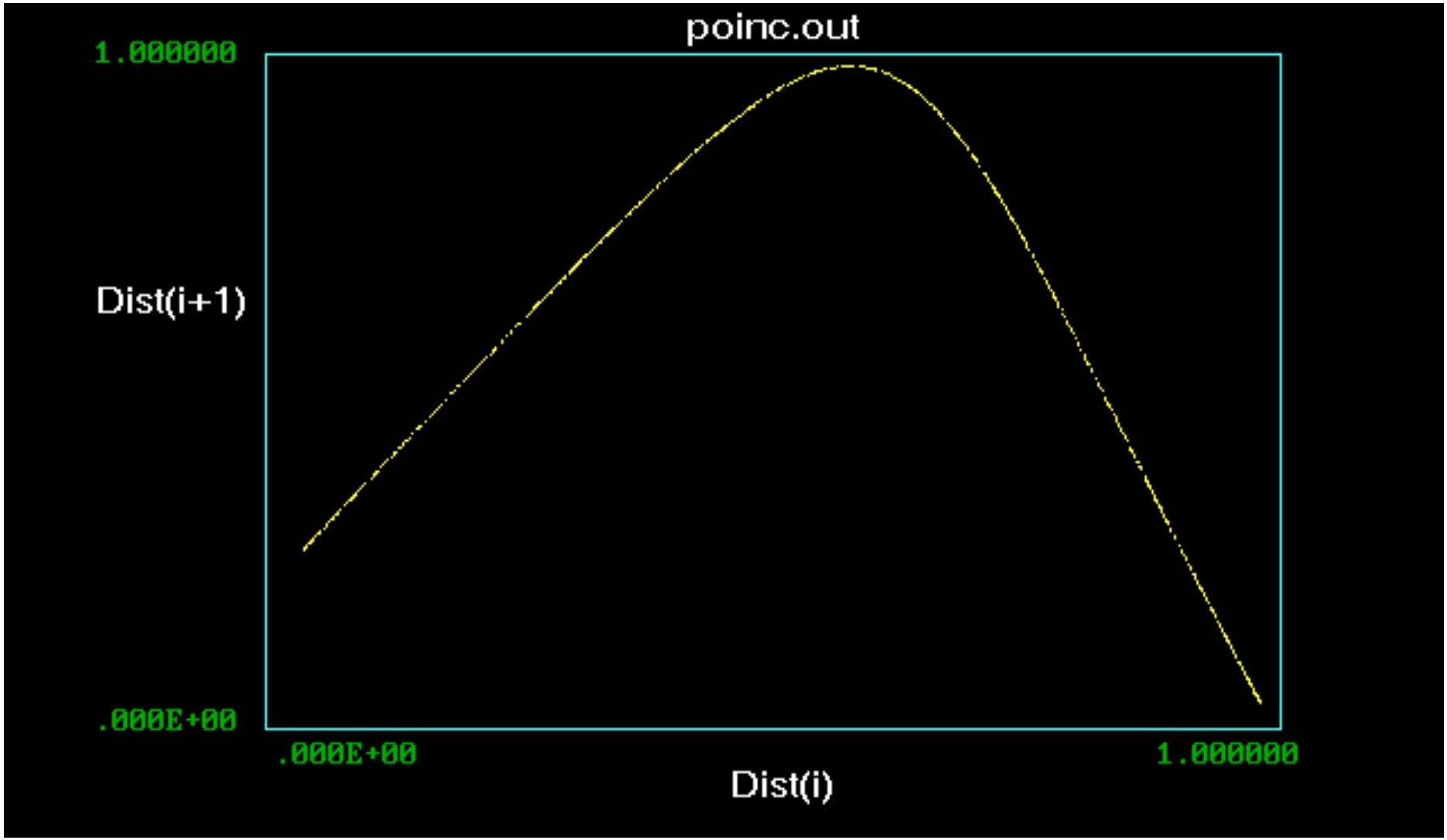


Sección de Poincaré



https://www.researchgate.net/

Aplicación de retorno



Aplicación unidimensional

$$x_{n+1} = r x_n (1 - x_n)$$

$$0 \leq x_n \leq 1$$

$$0 \leq r \leq 1$$

Divergencia de las trayectorias

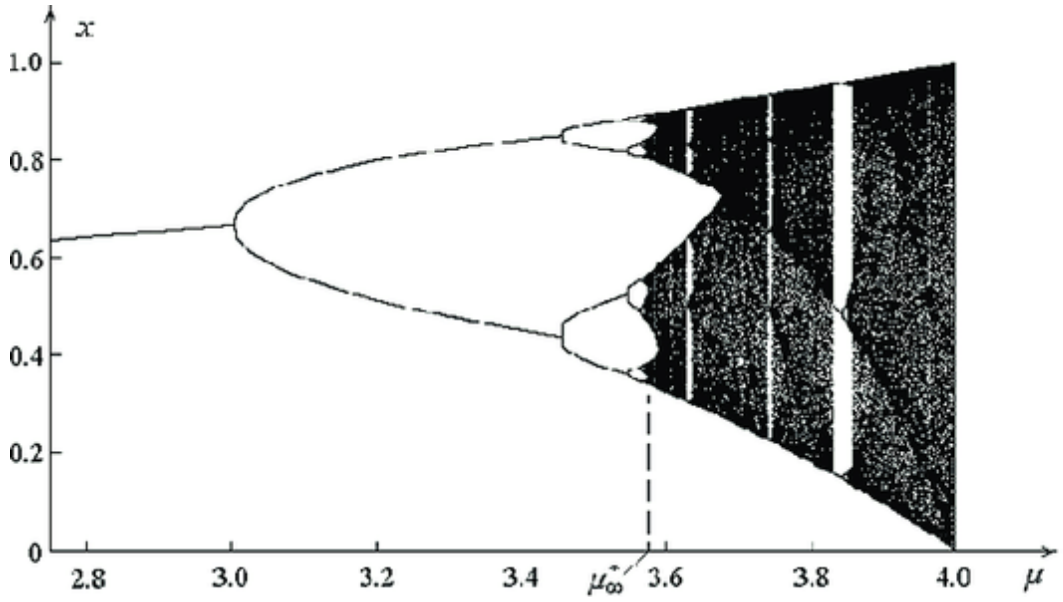
t	x_t^a	x_t^b	$\lvert x_t^a - x_t^b \rvert$
0	0.987654321	0.987654320	0.000000001
1	0.048773053	0.048773057	0.000000004
2	0.185576969	0.185576983	0.000000014
3	0.604552629	0.604552665	0.000000035
4	0.956274991	0.956274961	0.000000030
5	0.167252531	0.167252639	0.000000108
6	0.557116488	0.557116776	0.000000288
7	0.986950827	0.986950696	0.000000132
8	0.051515568	0.051516080	0.000000512
9	0.195446856	0.195448694	0.000001839
10	0.628989529	0.628994009	0.000004480
11	0.933446806	0.933442183	0.000004623
12	0.248495467	0.248511497	0.000016030
13	0.746981880	0.747014131	0.000032252

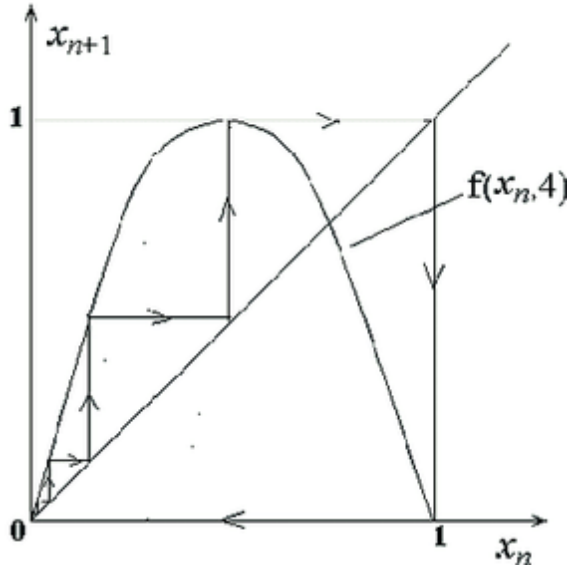
t	x_t^a	x_t^b	$\lvert x_t^a - x_t^b \rvert$
14	0.755999804	0.755936076	0.000063729
15	0.737856401	0.737986901	0.000130500
16	0.773697331	0.773448940	0.000248390
17	0.700359085	0.700902708	0.000543623
18	0.839424949	0.838552408	0.000872541
19	0.539162817	0.541529069	0.002366252
20	0.993865095	0.993101346	0.000763749
21	0.024389072	0.027404252	0.003015180
22	0.095176980	0.106613035	0.011436055
23	0.344473289	0.380986782	0.036513494
24	0.903245768	0.943343416	0.040097648
25	0.349571401	0.213786462	0.135784940
26	0.909484947	0.672327242	0.237157705
27	0.329288313	0.881213286	0.551924973

Sistemas caóticos son:

- Deterministas
- Muy sensibles a las condiciones iniciales
- No tienen memoria
- No son “complejos”

Diagrama de bifurcación





https://www.researchgate.net/

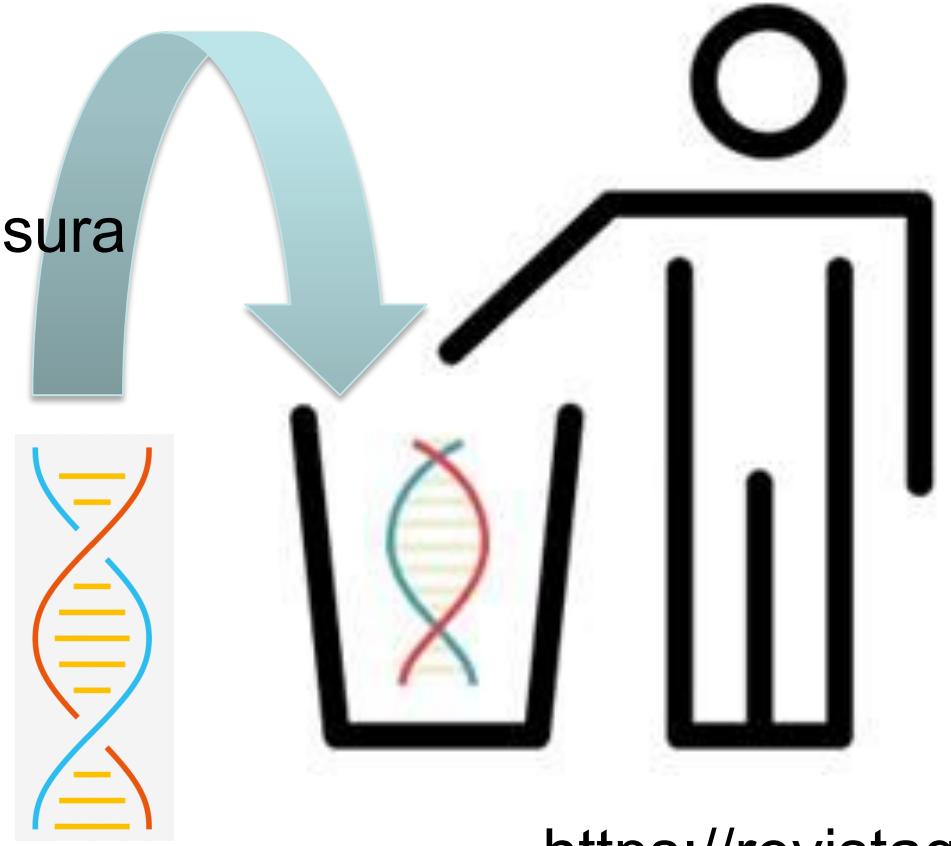
http://cogsci.ucd.ie/Connectionism/Labs/logistic/logistic.html

BIOLOGÍA

ADN basura

ADN basura es ADN que no codifica proteínas.

85% basura

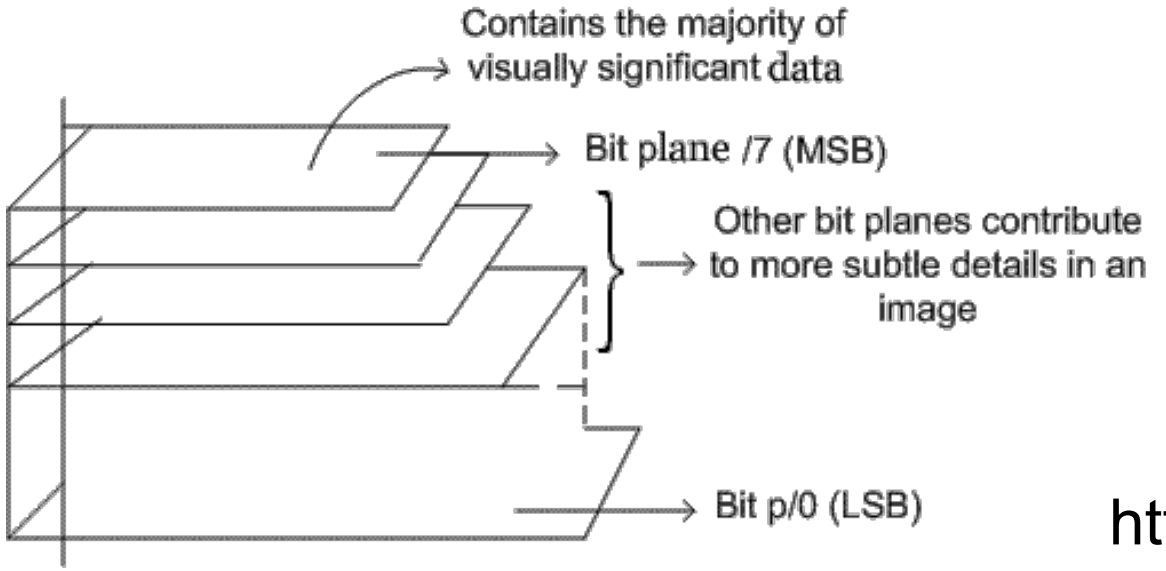


https://revistageneticamedica.com/

INFORMÁTICA

Bit Plane, ¿Qué es eso?

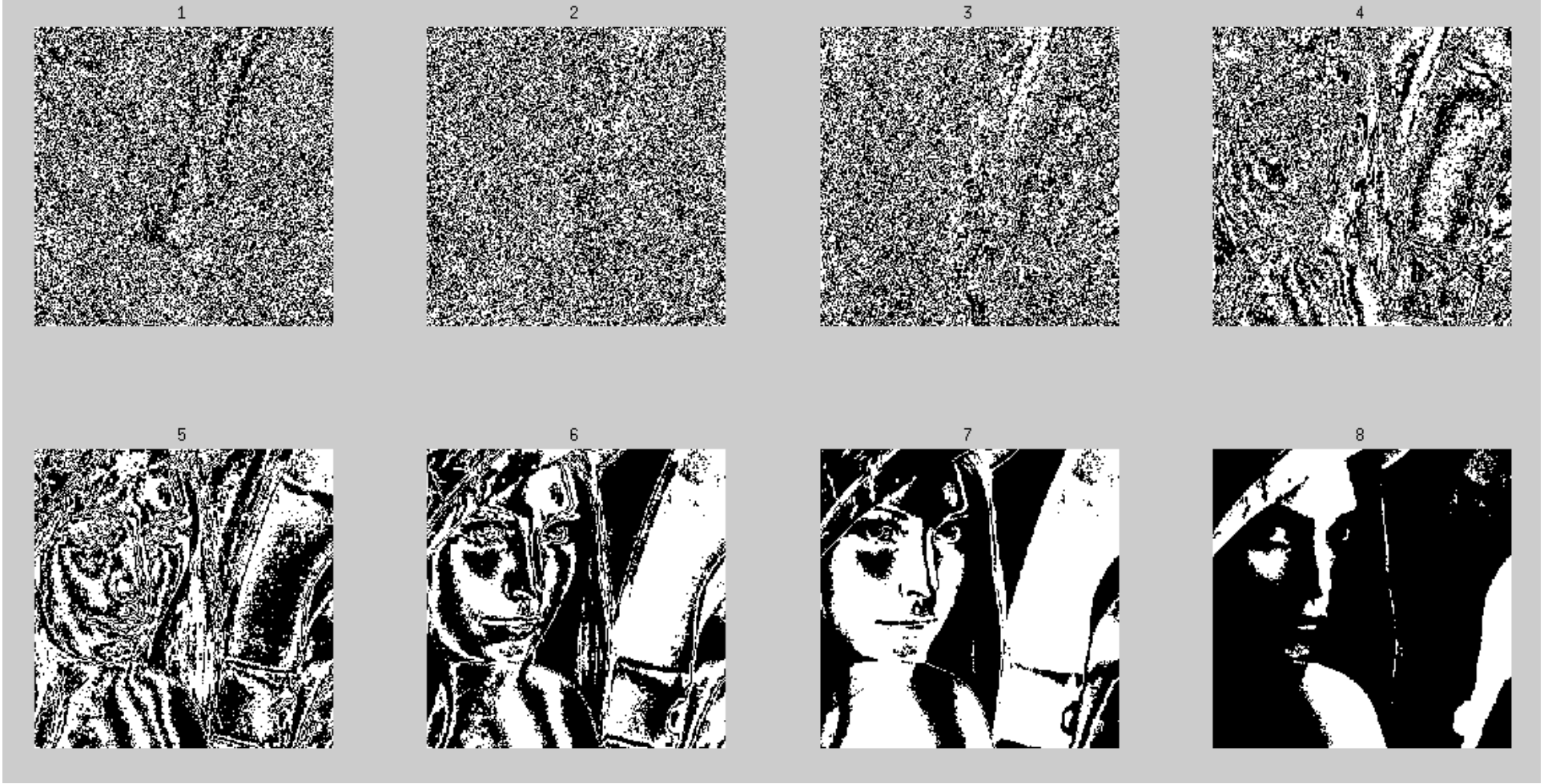
- Una imagen esté compuesta de lonchas de información o bit-planes, cero es el plano menos (LSB) y (MSB) el más significativo.
  - El i-plane es la capa i-ésima de la imagen



http://nptel.ac.in/

Lena

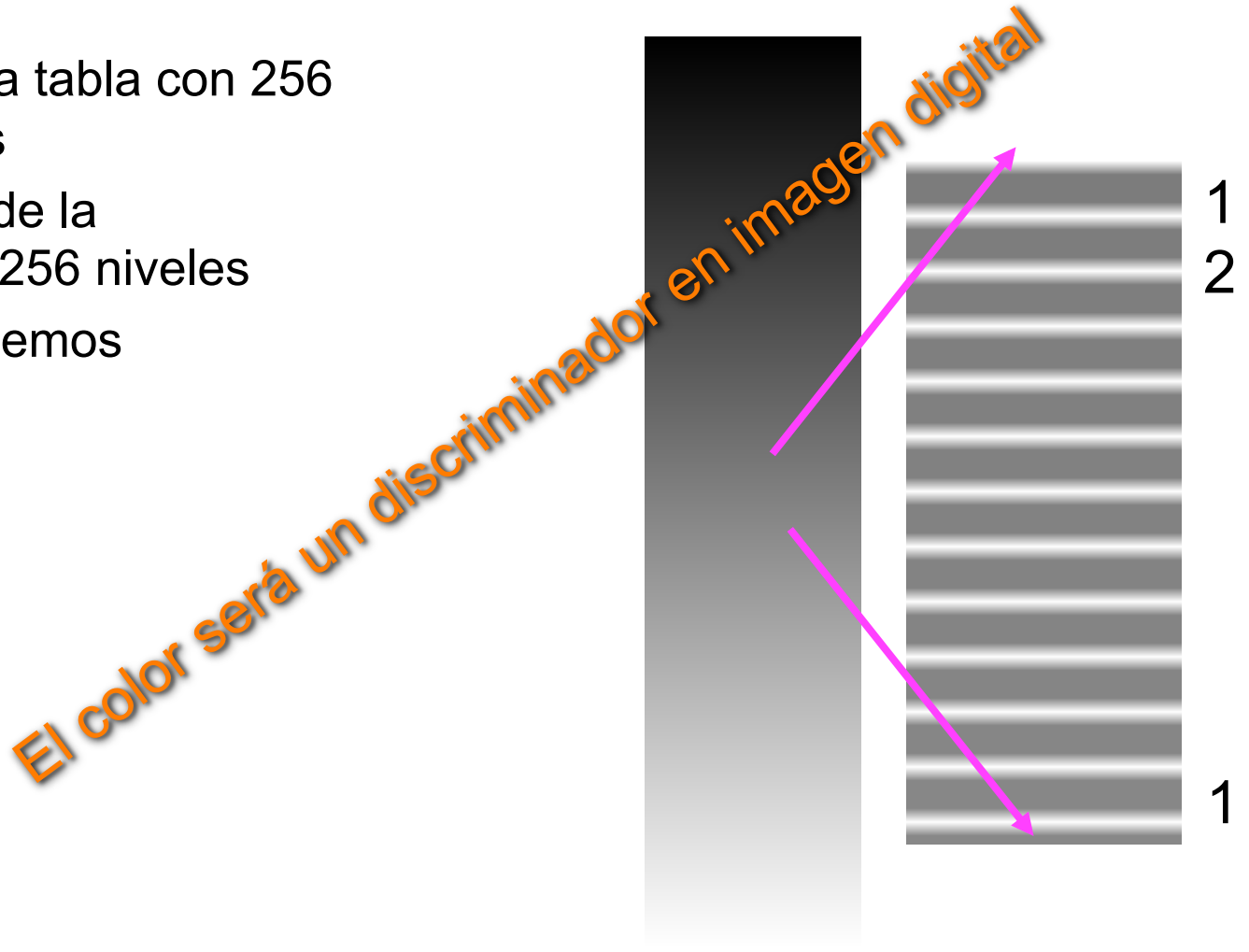
Bitplanes



https://github.com/mdegis/Image-Processing

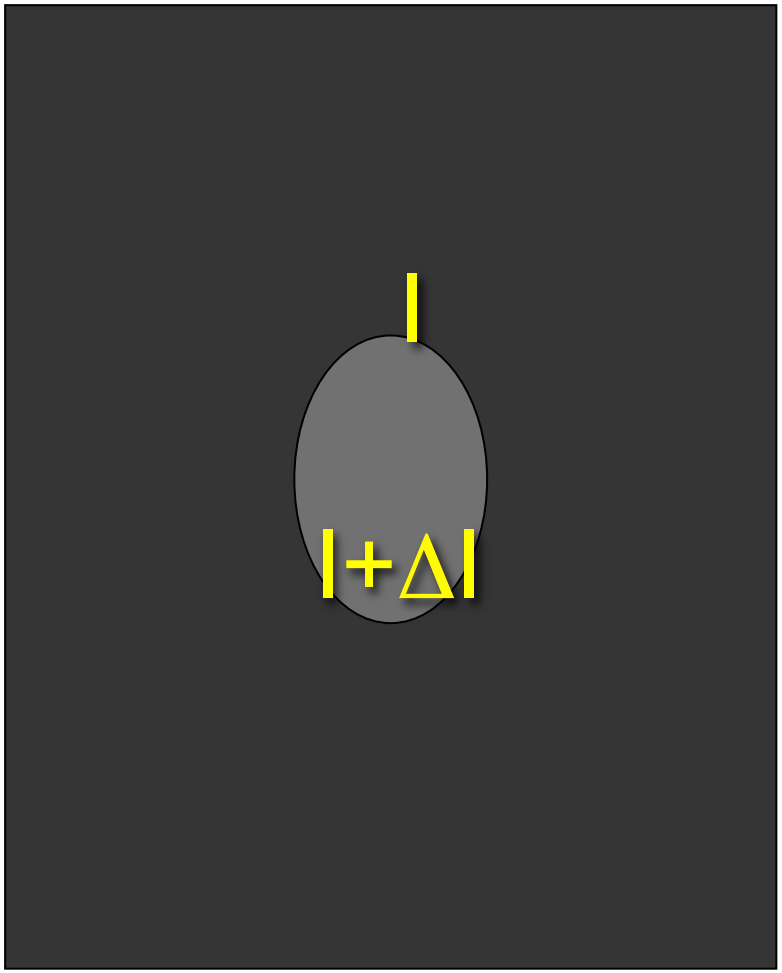
Niveles de gris

- Imagen de una tabla con 256 niveles de gris
- Cuantización de la intensidad en 256 niveles
- ¿Cuántos podemos distinguir?

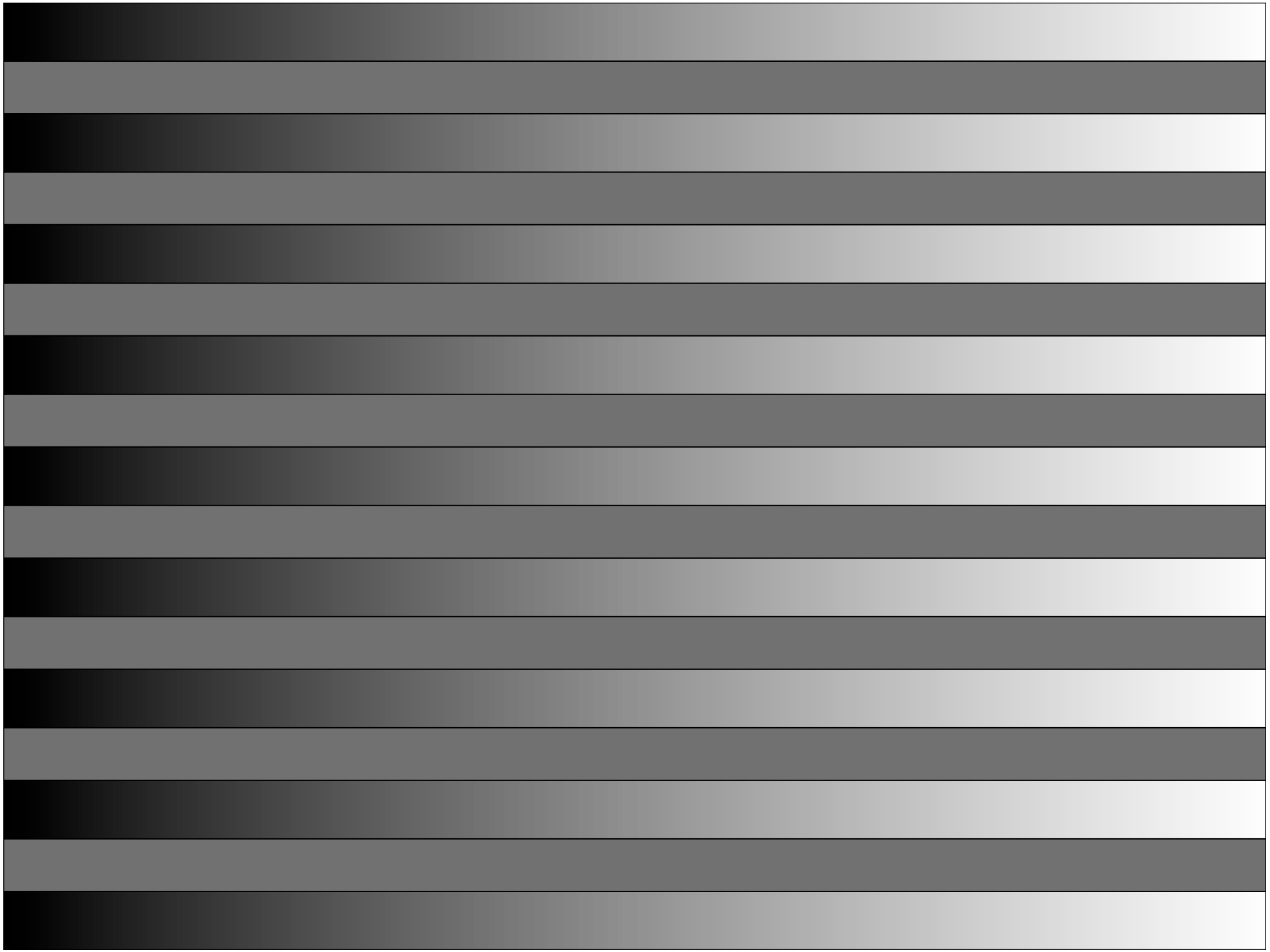


Contraste

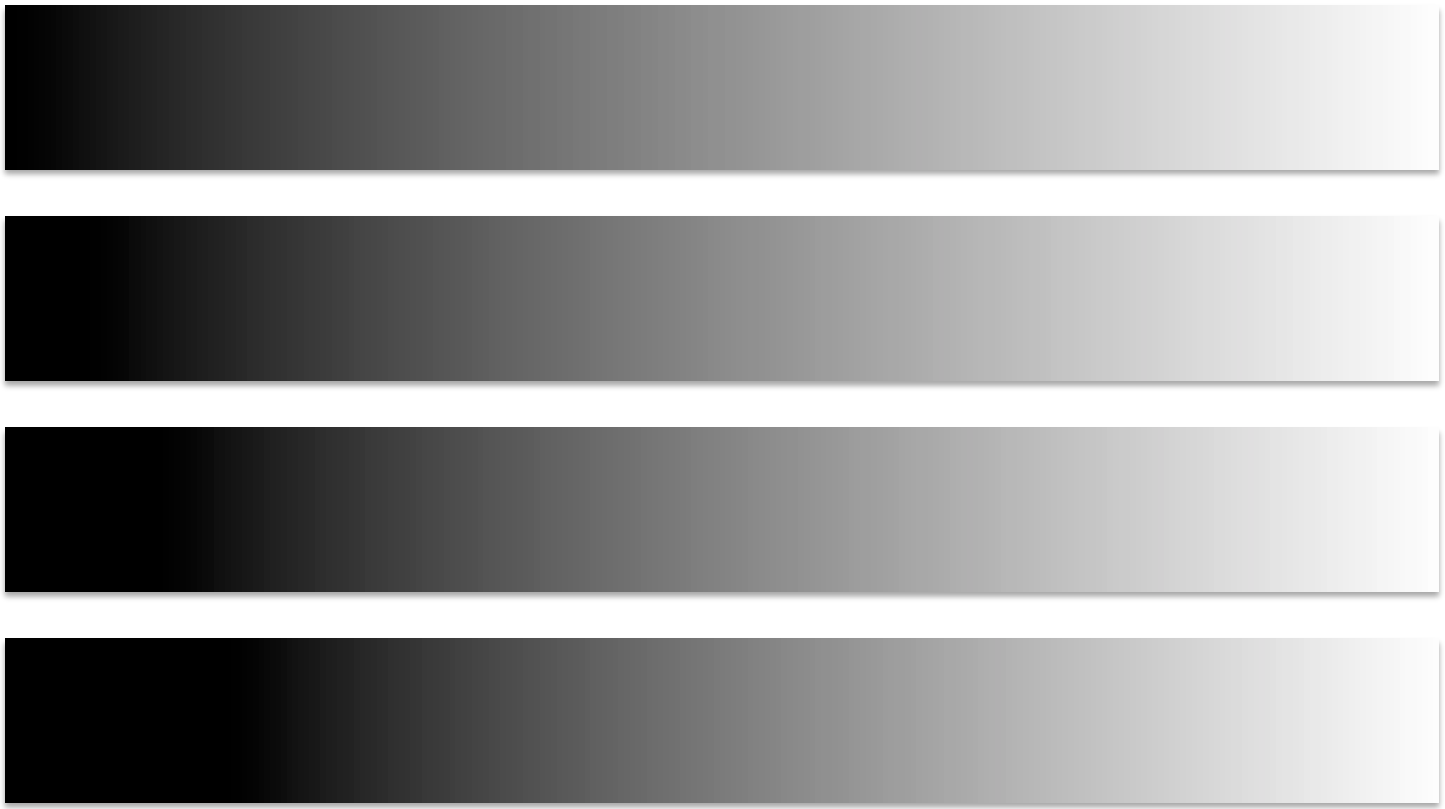
- Contraste (absoluto, relativo) = $\Delta I / I$
- Nuestra percepción se adapta en un rango de diez potencias de diez
  - Equivalente entre 1 cm y la distancia Tierra-Luna
- Percepción no lineal
  - Discriminamos mejor las intensidades altas
- Fracción de Weber (2%)
  - Relación cuantitativa entre la magnitud de un estímulo físico y cómo éste es percibido



FISIOLOGÍA

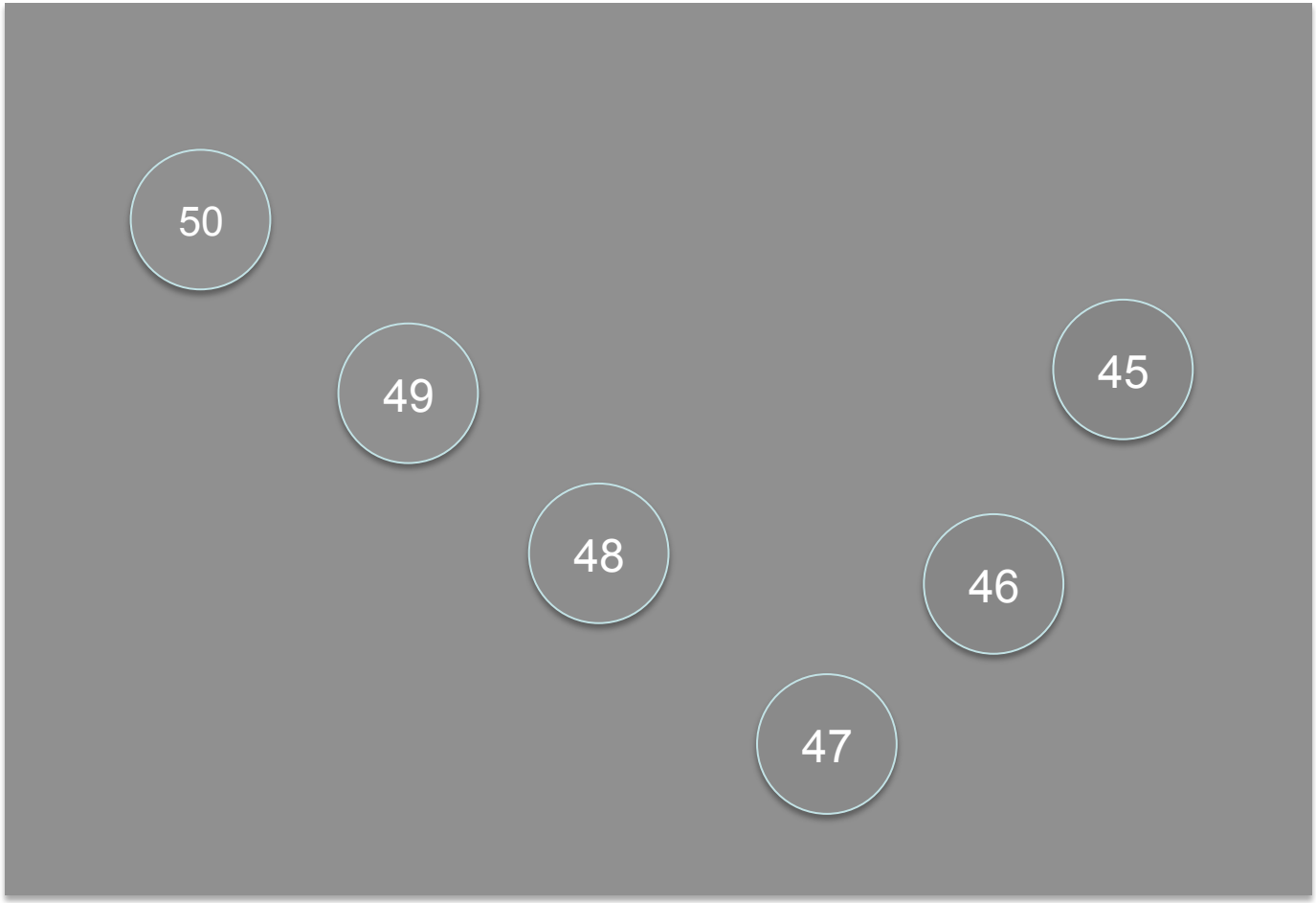


Nuestra percepción

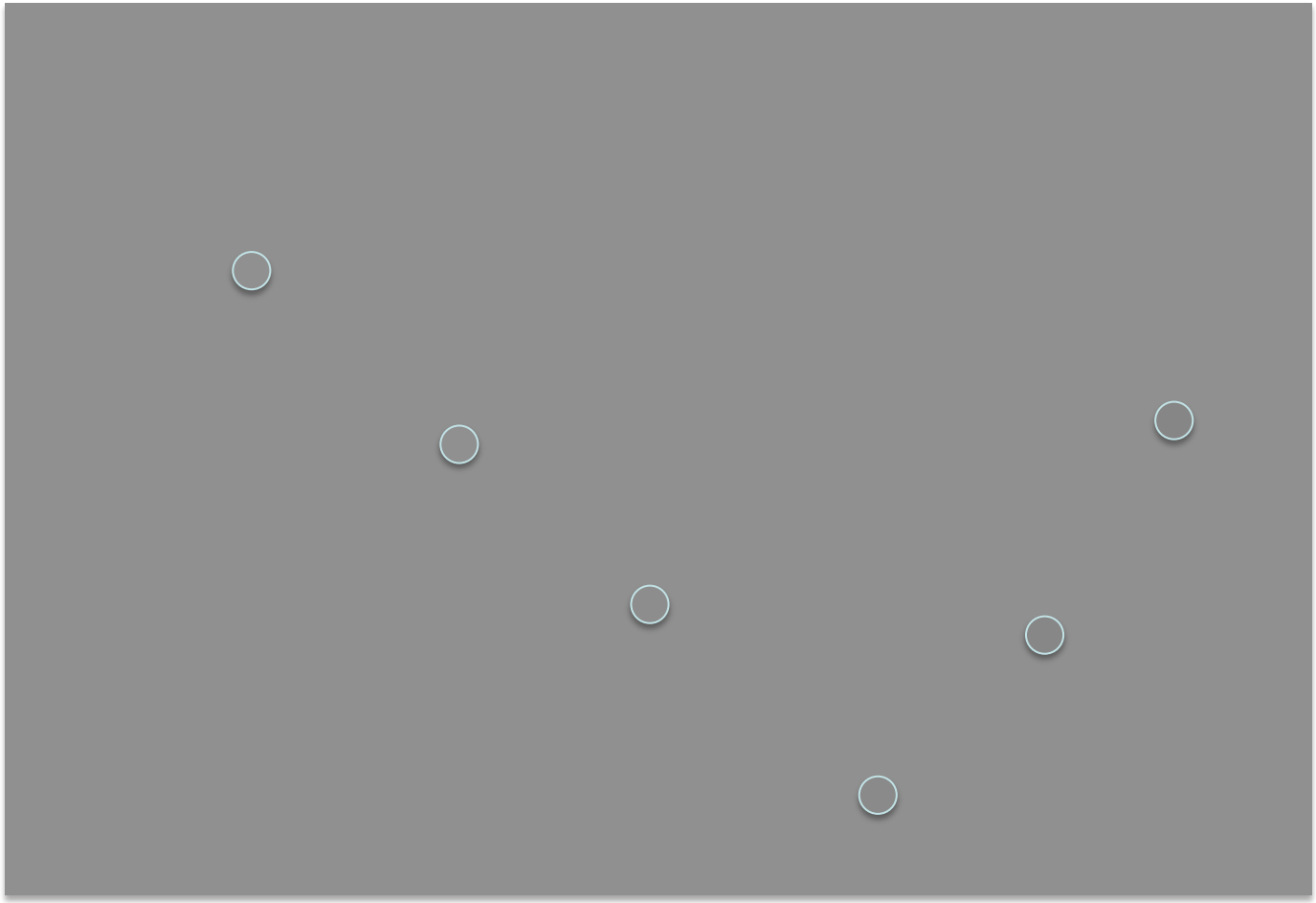


Nuestra percepción

Nuestra percepción



Nuestra percepción



Nuestra percepción

CRIPTOLOGÍA

Laboratorio de Medida Avanzada por Imagen
Dpto. Física Matemática y de Fluidos
UNED

Escítala espartana (400 a.C)

La Jangada (Julio Verne, 1881, Vol 2-XIII)

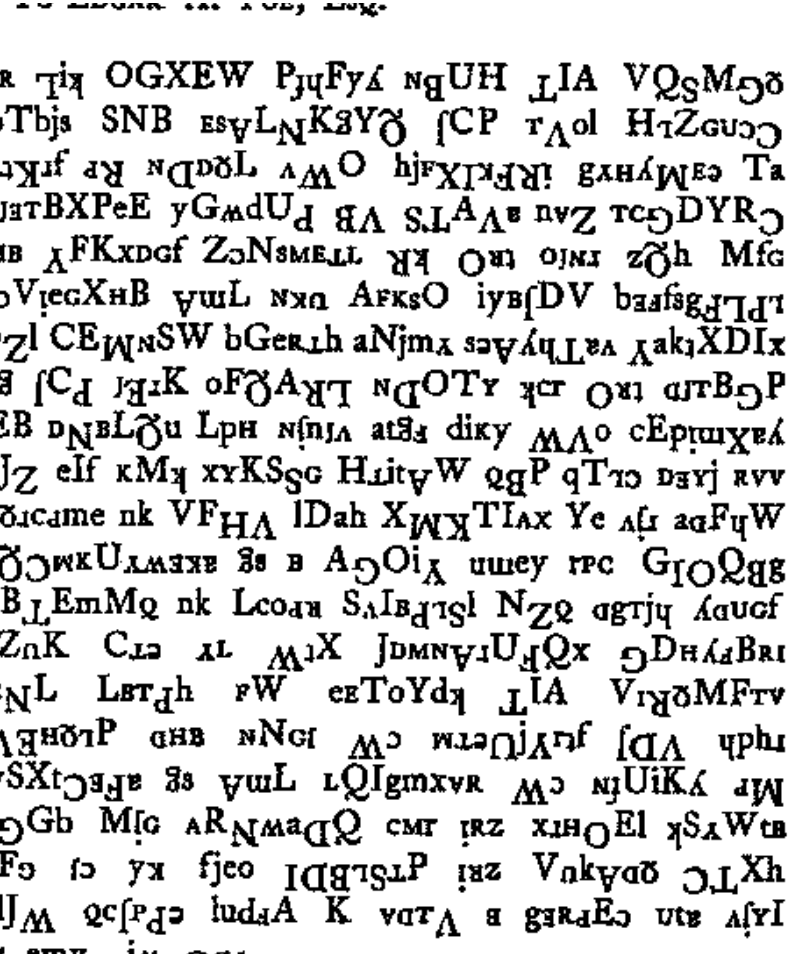
- XIII
- «*Phyjslyddqfdzxgasgzzqqehxgkxfndrxujugiocytdxvksbxhhuypohdvyrymhuh puydkjoxphetozsletnpmvffovpdpajxkyynojyggaymeqynfuqlnmvlyfgsuzmqizll bqgyugsqeubvnrcredgruzblrmxyuhqhpzdrrgcrokepqxufivvrplphontkvddqfhqs ntzhkknfepmqkyuuexkloqzgkyuumfvijdqdpzjqsykrplxhxqrymnklohkkotozvdks ppsuvjhd*.»

- XIX
- Et voici ce qu'il lut au milieu de ce profond silence :
- *Le véritable auteur du vol des diamants et de l'assassinat des soldats qui escor-taient le convoi, commis dans la nuit du vingt-deux janvier mil huit cent vingt-six, n'est donc pas Joam Dacosta, injustement condamné à mort ; c'est moi, le misérable employé de l'administration du district diamantin ; oui, moi seul, qui signe de mon vrai nom, Ortega.*

Criptografía

http://www.ecojoven.com/uno/03/poe.html

- Criptograma de Poe
- El escarabajo de oro
- Resolvió más de 100 criptogramas …



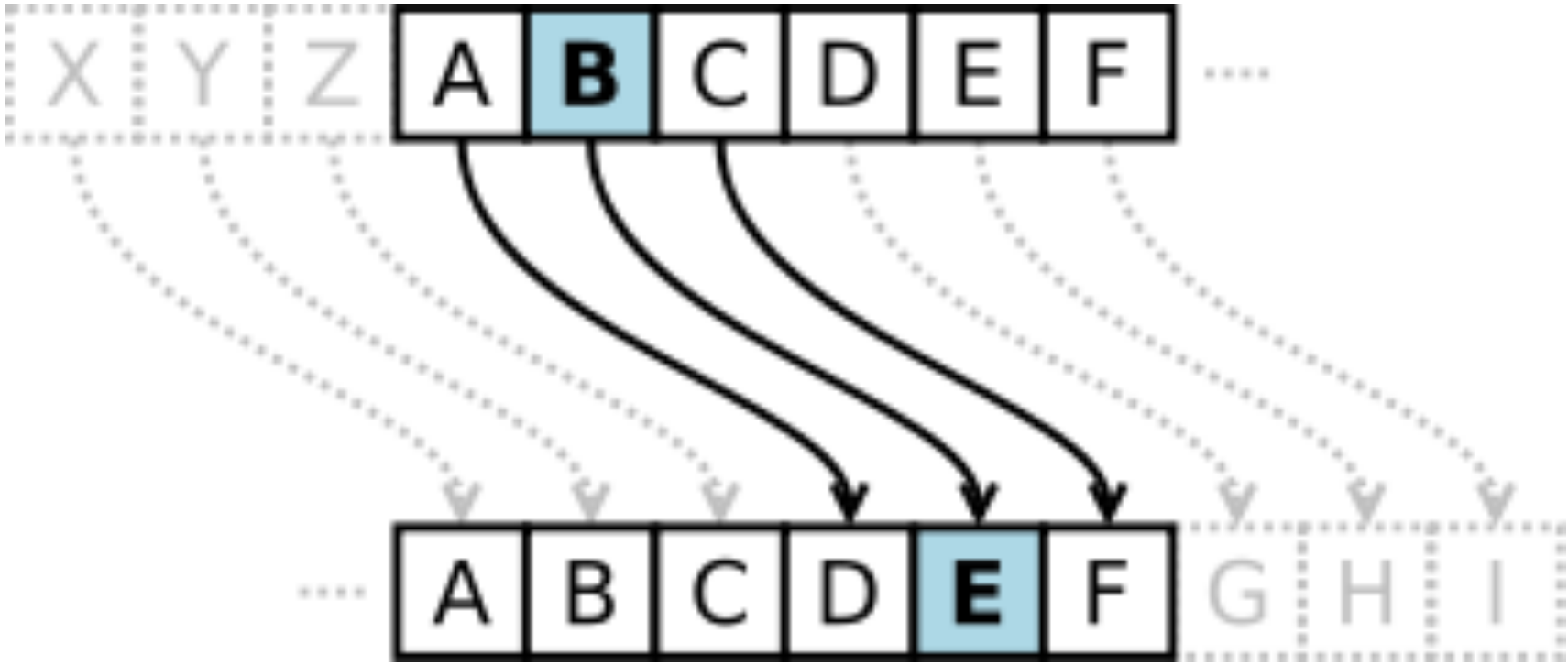
El cifrador de Polybios (siglo II a. C.)

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

Genbeta Dev Historia de la criptografia Metodo usado por los griegos

BBAECCABAEDDAA ADAEEA BCBDDCDDCDDBBDAA
ADAE CAAA ACDBBDCEDDCDBBDBAABABDAA
CBAEDDCDADCD DEDCAAADCD CECDDB CACDDC
BBDBBDAEBBCDDC

Método de César



Cifrados de sustitución polialfabeto

Mensaje P L A N
Clave S O L S
Cifrado I Z L F

Para facilitar las operaciones con este criptosistema, se dispone el llamado **cuadro de Vigenère**, que está formado por una matriz cuadrada de 27x27 en el caso de un alfabeto de 27 letras como el español. La primera fila de la matriz está formada por el alfabeto empezando por la letra A y acabando en la letra Z, la segunda por el alfabeto que empieza por la B y acaba en A, y así hasta la última fila, la 27ª, que empieza por las letras ZAB... y acaba con la letra Y.

	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

Fig- Tablero Vigènere para el alfabeto inglés

Algoritmo RSA. Algoritmo

Supongamos que Bob quiere enviar a Alicia un mensaje secreto que solo ella pueda leer.

Alicia envía a Bob una caja con una cerradura abierta, de la que solo Alicia tiene la llave. Bob recibe la caja, escribe el mensaje, lo pone en la caja y la cierra con su cerradura (ahora Bob no puede leer el mensaje). Bob envía la caja a Alicia y ella la abre con su llave. En este ejemplo, la caja con la cerradura es la «clave pública» de Alicia, y la llave de la cerradura es su «clave privada».

Distribución del texto en español

• E - 16,78%	R - 4,94%	Y - 1,54%	J - 0,30%	
• A - 11,96%	U - 4,80%	Q - 1,53%	Ñ - 0,29%	
• O - 8,69%	I - 4,15%	B - 0,92%	Z - 0,15%	
• L - 8,37%	T - 3,31%	H - 0,89%	X - 0,06%	
• S - 7,88%	C - 2,92%	G - 0,73%	K - 0,00%	
• N - 7,01%	P - 2,77%	F - 0,52%	W - 0,00%	
• D - 6,87%	M - 2,12%	V - 0,39%	-	

Código ASCII

Código ASCII

Binario	Dec	Hex	Representación	Binario	Dec	Hex	Representación	Binario	Dec	Hex	Representación
0010 0000	32	20	espacio ( )	0100 0000	64	40	@	0110 0000	96	60	`
0010 0001	33	21	!	0100 0001	65	41	A	0110 0001	97	61	a
0010 0010	34	22	"	0100 0010	66	42	B	0110 0010	98	62	b
0010 0011	35	23	#	0100 0011	67	43	C	0110 0011	99	63	c
0010 0100	36	24	$	0100 0100	68	44	D	0110 0100	100	64	d
0010 0101	37	25	%	0100 0101	69	45	E	0110 0101	101	65	e
0010 0110	38	26	&	0100 0110	70	46	F	0110 0110	102	66	f
0010 0111	39	27	'	0100 0111	71	47	G	0110 0111	103	67	g
0010 1000	40	28	(	0100 1000	72	48	H	0110 1000	104	68	h
0010 1001	41	29	)	0100 1001	73	49	I	0110 1001	105	69	i
0010 1010	42	2A	*	0100 1010	74	4A	J	0110 1010	106	6A	j
0010 1011	43	2B	+	0100 1011	75	4B	K	0110 1011	107	6B	k
0010 1100	44	2C	,	0100 1100	76	4C	L	0110 1100	108	6C	l
0010 1101	45	2D	-	0100 1101	77	4D	M	0110 1101	109	6D	m
0010 1110	46	2E	.	0100 1110	78	4E	N	0110 1110	110	6E	n
0010 1111	47	2F	/	0100 1111	79	4F	O	0110 1111	111	6F	o
0011 0000	48	30	0	0101 0000	80	50	P	0111 0000	112	70	p

Tiempo medio para la búsqueda exhaustiva de claves

Tamaño de clave (bits)	Número de claves alternativas	Tiempo necesario a 1 cifrado/μs	Tiempo necesario a 10^6 cifrado/μs
32	$2^{32} = 4{,}3 \times 10^9$	2^{31} μs = 35,8 minutos	2,15 milisegundos
56	$2^{56} = 7{,}2 \times 10^{16}$	2^{55} μs = 1.142 años	10,01 horas
128	$2^{128} = 3{,}4 \times 10^{38}$	21^{27} μs = 5,4 x 10^{24} años	5,4 x 10^{18} años
168	$2^{168} = 3{,}7 \times 10^{50}$	21^{67} μs = 5,9 x 10^{36} años	5,9 x 10^{30} años

http://www.matem.unam.mx/rajsbaum/cursos/web/presentacion_seguridad_1.pdf

Los seis principios de Kerckhoffs (1883)

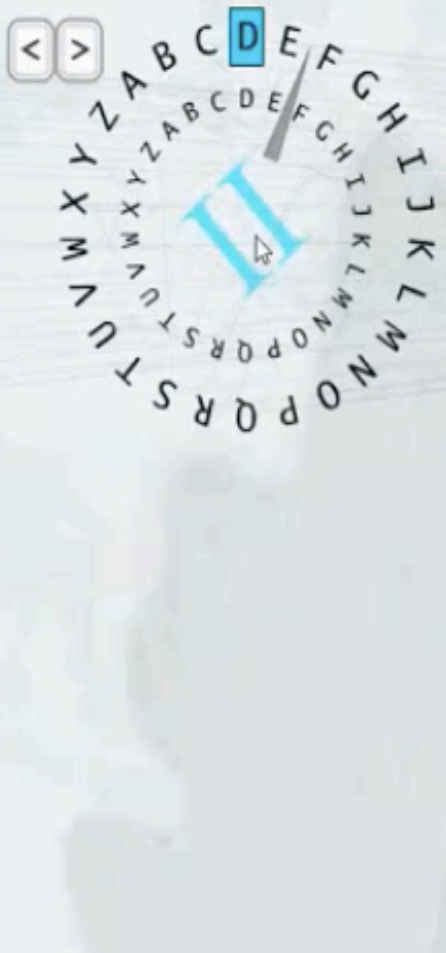
- Si el sistema no es teóricamente irrompible, al menos debe serlo en la práctica.
- La efectividad del sistema no debe depender de que su diseño permanezca en secreto.
- La clave debe ser fácilmente memorizable de manera que [illegible] recurrir a notas escritas.
- Los [illegible] dar resultados [illegible]
- El [illegible] le por una única [illegible]
- El sistema [illegible] ser fácil de utilizar.

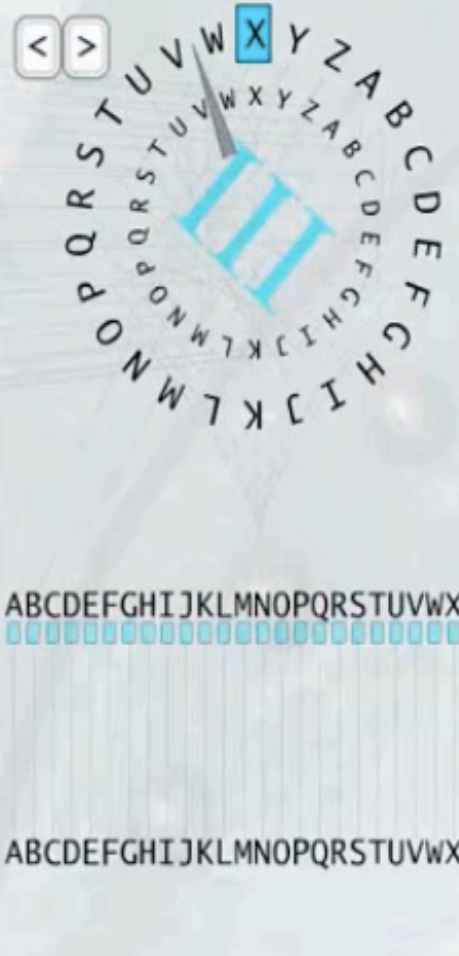
Y si ni siquiera de sabe que hay un mensaje secreto que se transmite?

Enigma

Geheim! **Sonder - Maschinenschlüssel BGT**

Datum	Walzenlage	Ringstellung	Steckerverbindungen	Grundstellung
31.	IV II I	F T R	HR AT IW SK UY DF GV LJ BO MX	vyj
30.	III V II	Y V P	OR KI JV CM ZN HU BF YC DS GP	cqr
29.	V IV I	O H R	UX JC PB BK TA ED ST DS LU FI	vhf





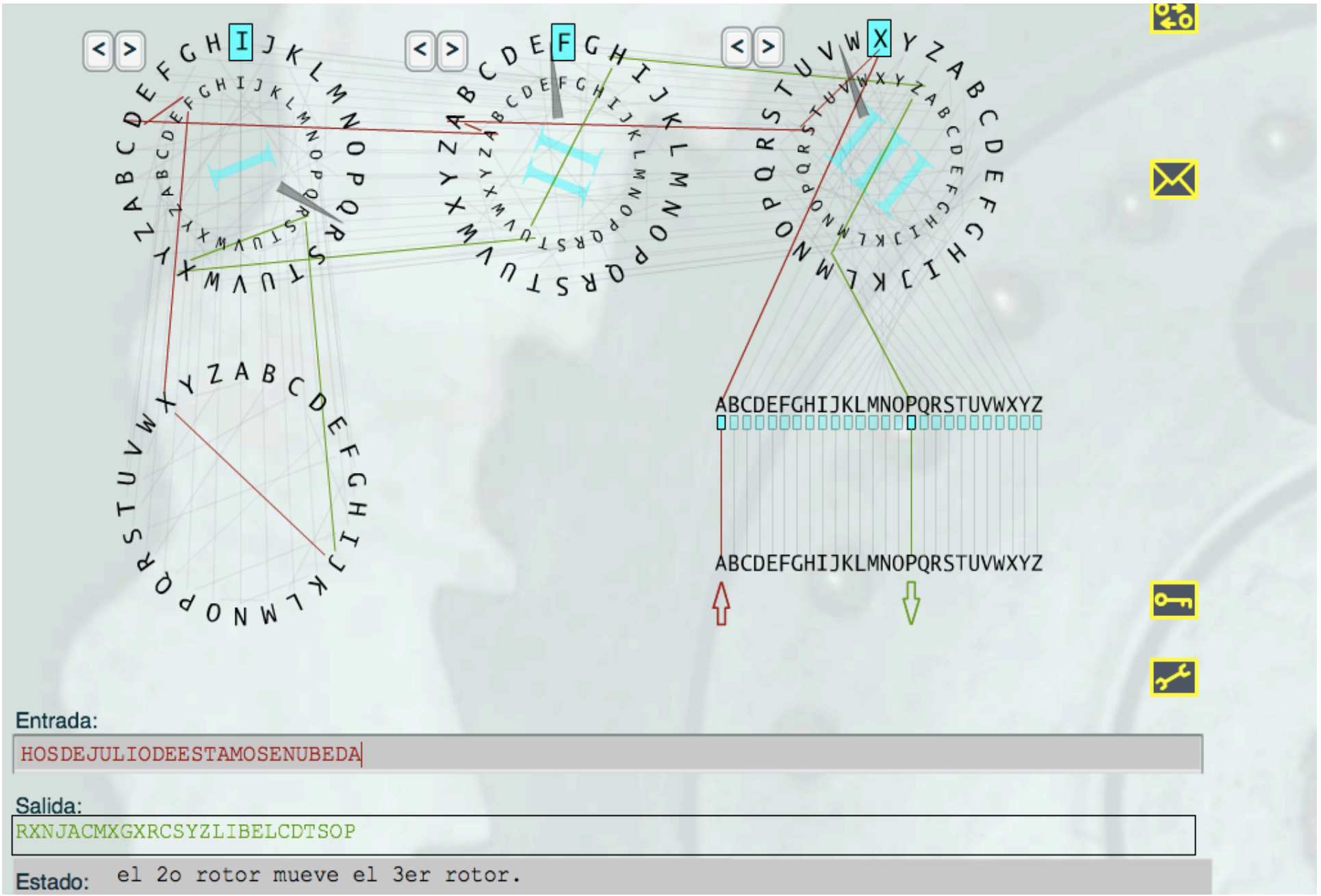
ABCDEFGHIJKLMNOPQRSTUVWXYZ

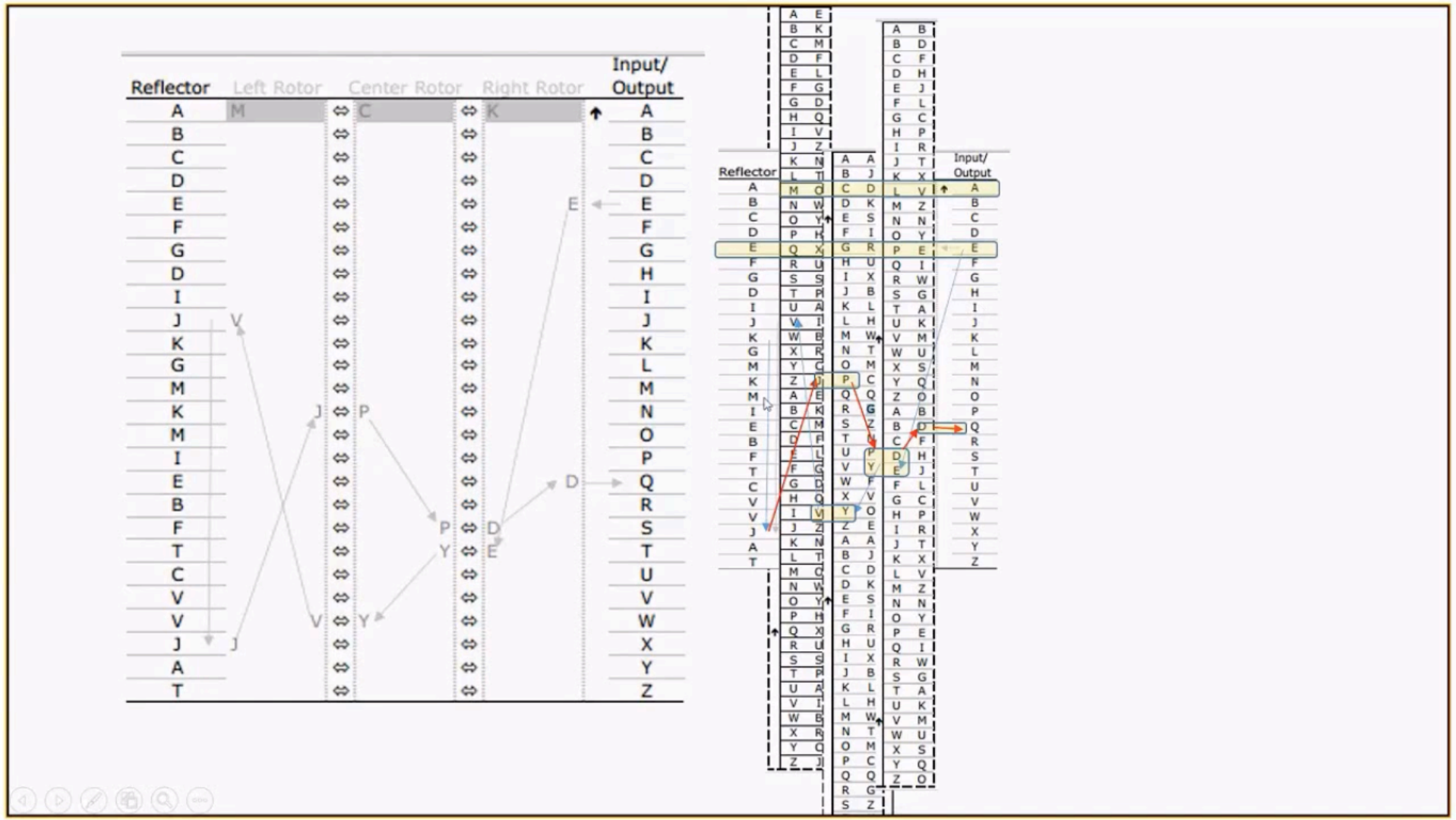
ABCDEFGHIJKLMNOPQRSTUVWXYZ

Entrada:

Salida:

Estado: Por favor, introduzca el texto en el campo de entrada.


I
F
X
ABCDEFGHIJKLMNOPQRSTUVWXYZ
ABCDEFGHIJKLMNOPQRSTUVWXYZ
Entrada:
HOSDEJULIODEESTAMOSENUBEDA
Salida:
RXNJACMXGXRCSYZLIBELCDTSOP
Estado: el 2o rotor mueve el 3er rotor.


Reflector
Left Rotor
Center Rotor
Right Rotor
Input/
Output
A B C D E F G D I J K G M K M I E B F T C V V J A T
M C K
V J P P D E Y V Y
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
Reflector
Input/
Output

ESTEGANOGRAFÍA

Esteganografía

- Del griego στεγανος *steganos*, "cubierto" u "oculto", y γραφος *graphos*, "escritura", es el estudio y aplicación de técnicas que permiten ocultar mensajes de modo que no se perciba su existencia.
- Ha sido utilizada por organizaciones criminales y terroristas
- Puede complementarse con la criptografía, dando un nivel de seguridad extra a la información
- Inserción en LSB
- Las técnicas de estegoanálisis, normalmente, sólo llegan a brindar nivel de probabilidad de existencia de un mensaje encubierto en un portador.

Ejemplo de inserción LSB

Prof. Ribagorda Garnacho

Laboratorio de Medida Avanzada por Imagen
Dpto. Física Matemática y de Fluidos
UNED

ALGORITMO

Secuencia

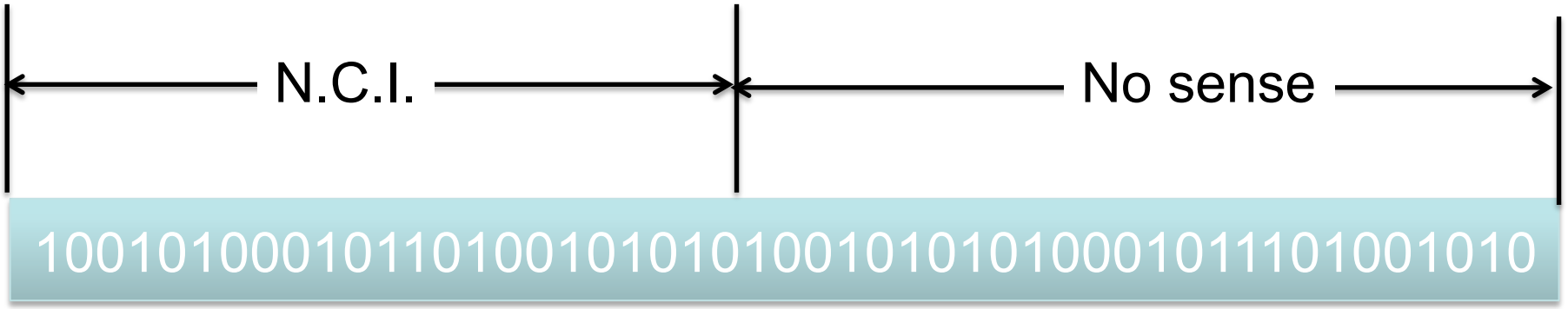
- Secuencia de orden
- Valor de r
- Valor de C.I.
- Número de iteraciones
- Longitud del bloque basura
- Data
- Bloque basura
- Data
- Bloque basura
- ...

Codificación

- Sistema caótico
- C.I.
- Inicialización X_0->X_D. X_1=X_D
- Do i=1,N
  - T_i=Int(27*X_i)
  - César de desplazamiento T_i
  - Codificación de carácter
- Vuelta al Do

Bloque basura

- Bloque basura
  - Nueva C.I.
  - Secuencia sin sentido



¿Dónde esconderlo?

- En una página web (banner)
  - http://www.uned-jaen-ubeda.es/index.php/noticia/leer/400
- ¿Vídeo en youtube?
  - https://www.youtube.com/watch?v=pZsuxZXN33g
- ¿Sonido?
- ¿Futuro? La nariz digital

CALIGRAFÍA PARA MÉDICOS

a = ~ j = ~ r = ~
b = ~ K = ~ s = ~
c = ~ l = ~ t = ~
d = ~ m = ~ u = ~
e = ^ n = ~ v = ~
f = ~ ñ = ~ W = ~~
g = ^ o = e X = +
h = ~ p = q Y = ~
i = ~ q = ~ Z = ~

e ~ ~ ~ ~

~ ~ ~ ~ ~ ~

EJEMPLO:

~ ~ q ~ ~ ~ ~

AMPICILINA