

Universidad Autónoma de Baja California

Ingeniero en Electrónica

Apuntes

Aplicación del Caos en la Ingeniería

Dra. Liliana Cardoza Avendaño

Dr. César Cruz Hernández

Dra. Rosa Martha López Gutiérrez

ÍNDICE

<i>TEMA</i>	<i>PÁG.</i>
1.0 CRIPTOGRAFÍA	3
1.1 Introducción	3
1.2 Significado	3
1.3 Objetivos	5
1.4 Origen	6
1.5 Algoritmo	16
1.6 Observaciones	19
1.7 Referencias	19
2.0 SINCRONIZACIÓN	20
2.1 Definición	20
2.2 Significado	20
2.3 Antecedentes históricos	20
2.4 Ejemplos de sincronización	24
2.5 Aplicaciones de la sincronización	31
2.6 Observaciones	32
2.7 Referencias	33
3.0 GENERACION DE CAOS	34
3.1 Introducción	34
3.2 Significado	34
3.3 Definición	35
3.4 Atractores	36
3.5 Fractal	38
3.6 Sistemas caóticos	42
3.7 Antecedentes históricos	49
3.8 Observaciones	54
3.9 Referencias	54

4.0 CIRCUITO DE CHUA	55
4.1 Introducción	55
4.2 Generador caótico	56
4.3 Simulación del circuito de Chua mediante el programa Simnon ver. 1.0	58
4.4 Implementación física y resultados experimentales del circuito de Chua	67
4.5 Simulación de la sincronización de dos circuitos de Chua mediante el programa Simnon ver. 1.0	78
4.6 Implementación física y resultados experimentales de la sincronización de dos circuitos de Chua	81
4.7 Simulación del encriptado de una onda senoidal a diferentes amplitudes y frecuencias por el método de enmascaramiento aditivo caótico	83
4.8 Encriptado de un mensaje de voz por medio del programa MatLab	93

5. APLICACIONES: Laseres EDFA (Erbium Doped Fiber Amplifier)

1.0 CRIPTOGRAFÍA

1.1 INTRODUCCIÓN

Con la proliferación de computadoras y de sistemas de comunicación, los usuarios de este tipo de servicios demandan que se les provea de seguridad en sus transmisiones, con el propósito de proteger su información confidencial. Es así que surge la criptografía desde tiempos antiguos, con la finalidad de alterar el mensaje confidencial de modo que sea incompresible a toda persona distinta al destinatario.

Por **cifrado**, se entiende un proceso de conversión de información a una forma disfrazada para enviarla a través de canales potencialmente inseguros. El proceso inverso se denomina **descifrado**. El uso de técnicas de cifrado permite que información valiosa pueda ser protegida contra organizaciones criminales, hackers o espías de potencias militares extranjeras.



Fig. 1.1.1 La privacidad y seguridad de la información confidencial durante la transmisión es de vital importancia.

Es obvio que la criptografía es usada generalmente como una herramienta militar. Sin embargo, en una sociedad con gran intercambio de información el valor de la criptografía aumenta día a día en áreas como privacidad, pagos electrónicos y control de acceso. De esta forma el campo de la criptografía se ha ampliado desde las clásicas técnicas de cifrado hasta áreas como autenticación, integración y transferencia de datos [1].

1.2 SIGNIFICADO

La **criptografía** proviene de los vocablos griegos **kryptos**, "ocultar", y **grafos**, "escribir", literalmente "*escritura oculta*". Una definición correcta de criptografía es la siguiente: *arte o ciencia de cifrar y descifrar información utilizando técnicas matemáticas que hagan posible el intercambio de mensajes de manera que sólo puedan ser leídos por las personas a quienes van dirigidos.*

Con mayor precisión, cuando se habla de esta área de conocimiento como ciencia se debería hablar de **criptología**, que engloba tanto las técnicas de cifrado, la criptografía propiamente dicha, como sus técnicas complementarias: el **criptoanálisis**, que estudia los métodos que se utilizan para romper textos cifrados con objeto de recuperar la información original en ausencia de la clave.

Según explica *Jorge Ramíó Aguirre* en su libro “Seguridad Informática y Criptografía” [2] la criptografía es:

“Rama inicial de las Matemáticas y en la actualidad de la Informática y la Telemática, que hace uso de métodos y técnicas con el objeto principal de cifrar y/o proteger un mensaje o archivo por medio de un algoritmo, usando una o más claves. Esto da lugar a diferentes tipos de sistemas de cifra que permiten asegurar estos cuatro aspectos de la seguridad informática: la confidencialidad, la integridad, la disponibilidad y el no repudio de emisor y receptor.”

Los cuatro aspectos de la seguridad informática se describen a continuación:

- ◆ Confidencialidad.- Se refiere a mantener en secreto el contenido de la información de grupos no autorizados.
- ◆ Integridad.- Se refiere a la detección de la alteración de datos no autorizada.
- ◆ Disponibilidad.- Se refiere a la identificación de otros entes o al origen de los datos.
- ◆ No repudio.- Se refiere a la prevención de un ente de denegar compromisos previos o acciones.

1.3 OBJETIVOS

La finalidad de la criptografía es, en primer lugar, garantizar el secreto en la comunicación entre dos entes y, en segundo lugar, asegurar que la información que se envía es auténtica en un doble sentido: que el remitente sea realmente quien dice ser y que el contenido del mensaje enviado, habitualmente denominado **criptograma**, no haya sido modificado en su tránsito.

En la actualidad, la criptografía no sólo se utiliza para comunicar información de forma segura ocultando su contenido a posibles fisgones. Una de las ramas de la criptografía que más ha revolucionado el panorama actual de las tecnologías informáticas es el de

la firma digital: tecnología que busca asociar al emisor de un mensaje con su contenido de forma que aquel no pueda posteriormente repudiarlo.

1.4 ORÍGENES [3]

Desde el principio de la historia intercambiar mensajes cifrados ha jugado un papel destacado. Tanto en la milicia, diplomacia y el espionaje, constituyen la mejor defensa de las comunicaciones y datos que se transmiten, por cualquier canal. Esto es debido a la necesidad de que algunos de los mensajes solo sean conocidos por aquellas personas a las que van dirigidos y no puedan ser interpretados por nadie más que por ellos. Cada civilización, a su manera, ha desarrollado y utilizado códigos secretos para mantener incomprensibles textos que, de alguna manera, comprometían su permanencia.

3500 A.C. - Los Sumerios

Los sumerios desarrollaron la escritura cuneiforme y los egipcios desarrollaron la escritura jeroglífica. La escritura Cuneiforme sumeria es la más vieja lengua escrita conocida de la historia humana y no fue descifrado hasta el siglo XIX. La forma más tempranamente conocida viene de Uruk, quien tomó la forma de “palabra-grabado” dibujados con una aguja en las tabletas de la arcilla húmeda. Cada palabra-grabado representó un objeto. Las “palabra-grabado” de Uruk se convirtieron en la nueva escritura ahora llamada cuneiforme. Los grabados se convirtieron gradualmente en “ideogramas”, un objeto que también significaba 'una idea'.

Entonces vinieron los “fonogramas” que representaban

sonidos así como el significado de un dibujo. Los jeroglíficos son diferentes a los cuneiformes sumerios debido a que son mucho más confusos. Los pensamientos de los jeroglíficos egipcios eran religiosos e históricos, pero los progresos recientes podrían señalar a un propósito económico para la escritura.



Fig. 1.4.1 Tablilla sumeria con escritura cuneiforme

1900 A.C. - Jeroglíficos Egipcios

El primer antecedente conocido sobre Criptografía.

Acerca de los jeroglíficos: Desde los griegos significaba “escritura sagrada”, esta es un lenguaje en dibujos que se usaba casi siempre para decorar templos y monumentos. Podía ser escrito con una pluma y tinta sobre papiros, pintado o grabado sobre piedra. Era cuidadosamente dibujado los signos lo

mas exacto posible. Los jeroglíficos se usaron para

escribir el lenguaje antiguo egipcio. En un principio los signos jeroglíficos eran usados para mantener recuerdos de las posesiones de los reyes. Los escribas podían fácilmente hacer estas historias dibujando una vaca o un bote seguido de un número. Sin embargo si el lenguaje llegaba a ser mas complejo se requerían más dibujos. Con el tiempo el lenguaje consistía en más de 750 signos diferentes.



Fig. 1.4.2 Jeroglíficos egipcios

1500 A.C. - Mesopotamia

Una tableta de 3" x 2" Mesopotámica contenía una formula encriptada para construir piezas de cerámica. Signos cuneiformes se utilizaban en la silaba menos común usados al final de silabas para intentar ocultar secretos de fórmulas. Acerca de la escritura Cuneiforme: pictogramas, o dibujos representando cosas reales, eran las bases para la escritura cuneiforme. Los inicios de los pictogramas

asemejaban los objetos representados, pero debido al uso repetido empezaron a lucir simples, incluso abstractas. Estas marcas con el tiempo llegaron a ser acuñadas y podían comunicar sonidos o conceptos abstractos.



Fig. 1.4.3 Tablilla de escritura mesopotámica

500 - 600 A.C. – Cifrado ATBASH

Los escribas hebreos acentuado en el libro de Jeremías emplearon el alfabeto inverso simplemente sustituyendo la cifra conocida como ATBASH. El cifrado ATBASH es un código hebreo el cual sustituye la primer letra del alfabeto por la ultima y la segunda letra por la penúltima y así sucesivamente. Este cifrado es uno de los pocos usados en el lenguaje hebreo. La cifra por si misma es muy similar al cifrado de sustitución. El cifrado de sustitución es donde cada letra del alfabeto representa otra letra. En este caso el cifrado ATBASH sustituye la primer letra por la ultima, la segunda por la penúltima y así sucesivamente. ATBASH tiene este nombre del hecho de en el cifrado la A se vuelve T, la B se vuelve Sh etcétera, por lo tanto ATBSh-ATBASH.

Hebrew Alphabet				Hebrew Letter	Final Form	Name	Transliteration
א		aleph	' (silent)	ל		lamed	l
ב, בּ		bet, vet	b, v	מ	ם	mem	m
ג		gimel	g	נ	ן	nun	n
ד		dalet	d	ס		samekh	s
ה		he	h	ע		ayin	' (silent)
ו		vav	v	פ, פּ	ף	pe, fe	p, f
ז		zayin	z	צ	ץ	tsade	ts
ח		khet	h	ק		qof	q
ט		tet	t	ר		resh	r
י		yod	y	שׁ, שׂ		shin, sin	sh, s
כ, כּ	ך	kaf, khaf	k, kh	ת		tav	t

Fig. 1.4.4 Alfabeto hebreo

486 A.C. – Escitala Griega

Los antiguos griegos inventaron la “Escitala”, una especie de bastón envuelto con estrechas tiras de piel o pergamino. El mensaje se escribía longitudinalmente en la tira envuelta, después la tira se removía quedando un mensaje incomprensible el cual se pasaba al mensajero. Solo si el receptor tenía un tubo del mismo



Fig. 1.4.5 Escitala, utilizada durante la Guerra entre Esparta y Atenas

diámetro sería capaz de leer el mensaje. Los antiguos griegos y espartanos en particular, emplearon la escitala para el cifrado en comunicaciones durante las campañas militares.

50 - 60 A.C. – Julio César

Este tipo de encriptado es una de los más simples y extensamente aplicado por sus técnicas conocidas de encriptado. Cada letra del texto es reemplazada por una letra sobre un determinado desplazamiento numérico del alfabeto. Por ejemplo, un desplazamiento de 4 movería la A a E, B a F, etc. Por ejemplo:

Letra original	A	B	C	D	E	F	G	H	...	R	S	T	U	V	W	X	Y	Z
Letra Codificada	D	E	F	G	H	I	J	K	...	U	V	W	X	Y	Z	A	B	C

El Cifrado César fue llamado Julio César, quien uso éste con un desplazamiento de tres para proteger mensajes de tipo militar.



Fig. 1.4.6 El cifrado de Julio César fue empleado por este personaje durante sus campañas militares

1000 – Análisis de Frecuencia

El Análisis de Frecuencia conduce a técnicas para el descifrado monoalfabetico por sustitución: mas probablemente motivado debido al análisis de textos del Corán. Sus orígenes han sido sugeridos como el estudio cercano del Qur'an primero dado a conocer al Árábigo, el cual tiene una frecuencia de letras característica. Fue extendido y fue tan extensamente usado por los europeos durante el Renacimiento que fueron inventados varios temas por los criptógrafos dedicados. Estos incluían homófonos, sustitución poli alfabética y esquemas del mismo. El análisis de frecuencia se basa en el hecho de que en cualquier lenguaje, letras y combinación de letras ocurren en diferentes variaciones de frecuencia. En el lenguaje ingles por ejemplo, la letra E es la mas común, mientras que la X es la mas rara, mientras que en el castellano es la A.

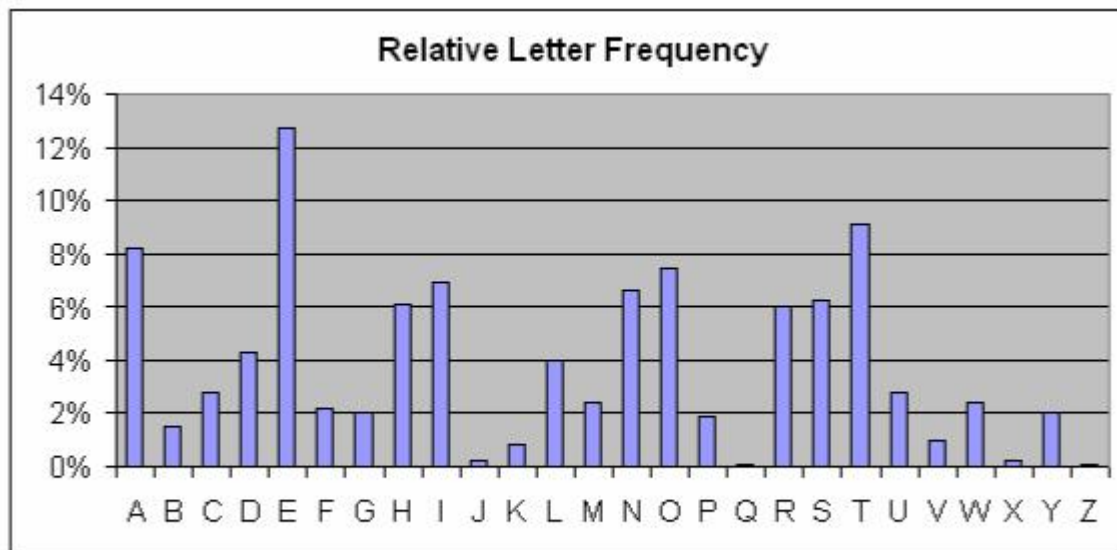


Fig. 1.4.7 Frecuencia de las letras en el lenguaje ingles

1466 - Leon Alberti

Leon Alberti inventó el disco cifrado y la clave criptográfica. El disco de cifrado de Alberti era polialfabético, significando que un nuevo alfabeto podía ser creado cada vez que girara el disco. Este tipo de disco fue el único método de uso de este tipo de cifrado hasta el siglo XVI. Alberti pensó que este cifrado era irrompible. Esta afirmación se baso en sus



Fig. 1.4.8 Disco de cifrado de Leon Alberti

investigaciones en análisis de frecuencia, el cual es el método mas efectivo de descifrado de criptogramas monoalfabéticos. Proporcionando suficiente texto cifrado, se puede usar la frecuencia de las letras en referencia de una distribución normal para encontrar el desplazamiento y resolver el criptograma. Este sistema falló al resolver los criptogramas polialfabéticos. El siguiente ejemplo muestra el funcionamiento del disco para diferentes claves dadas:

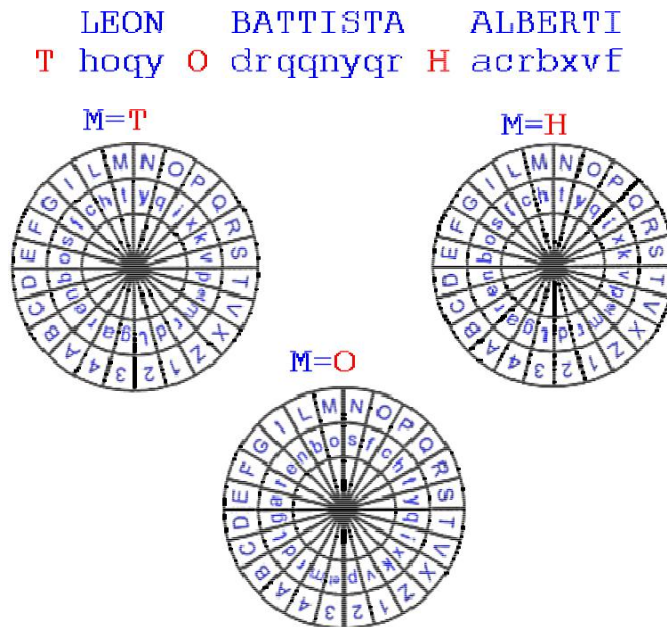


Fig. 1.4.9 Ejemplo de encriptado mediante el disco inventado por Leon Battista Alberti

1587 - Vigenere Cipher

Otro método de sustitución polialfabética es el conocido como tablero de Vigenere, consiste en una tabla formada por el alfabeto llano seguido por 26 alfabetos cifrados, consiguiéndose cada uno de ellos comenzando en la siguiente letra que el anterior. Para cifrar un mensaje con el tablero de Vigenere y la clave HIELO, por ejemplo, lo primero es repetir la clave sobre el texto llano tantas veces como sea necesario, hasta que cada letra del mensaje quede asociada con una letra de la clave. Para cifrar cada letra, buscamos la línea del tablero de Vigenere identificada por la letra de la clave y en esa línea buscamos la cifra correspondiente a la letra del texto llano.

	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. 1.4.10 Tablero de Vigenere

De esta forma un ejemplo de encriptado empleando el tablero de Vigenere se muestra a continuación:

Texto llano: LLEGARAN REFUERZOS POR MAR EL DÍA SIETE

Clave: HIELOHIE LOHIELOHI ELO HIE LO HIE LOHIE

Texto cifrado: STIROYIR CSMCICNVA TZF TIV PZ KQE DWLBI

1626 - Luis XIV, El Gran Cifrado

Una cifrado de nomenclatura desarrollada por Bonaventure Rossignols. Cada número se colocaba por una silaba francesa en vez de las letras simples. El gran cifrado se empleó para encriptar los mensajes más secretos del Rey Luis XIV. De hecho la identidad del Hombre de la Mascara de Hierro se protegió por el gran cifrado. El gran cifrado no se rompió hasta que el comandante Etienne Bazeries fue capaz de tomar los números que se tenían

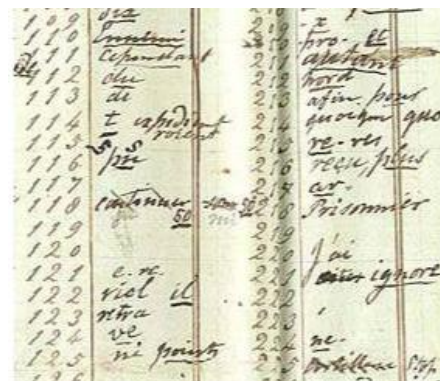


Fig. 1.4.11 El Gran Cifrado

frecuentemente para descifrar una palabra común.

1753 – La Invención del Telégrafo

El Telégrafo mostró que las señales generadas electrostáticamente pueden representarse como letras del alfabeto, las cuales pueden ser enviadas a distancia lejana a través de cables que empezaban a cubrir la Tierra. El telégrafo original usaba 26 cables; uno para cada letra del alfabeto.



Fig. 1.4.12 Telégrafo

1845 – Código Morse

Samuel Morse creó el código Morse: El código Morse representa letras, números y signos de puntuación por medio de señales codificadas enviadas intermitentemente. Este fue el principio de la comunicación digital. Esta usa estados (on y off) compuestas por cinco símbolos dit('), dah(-), short gap (entre letras), medium gap (entre palabras) y long gap (entre enunciados). El código Morse es diferente del telégrafo en el hecho de que envía códigos para cada letra por un simple cable mientras que el telégrafo emplea un cable para cada letra. En 1863 se creó la forma Europea del código Morse.

A	.-	M	--	Y	-.--	6	-....
B	-...	N	-.	Z	--..	7	--...
C	-.-.	O	---	Ä	.-.-	8	---..
D	-..	P	.--.	Ö	---.	9	----.
E	.	Q	--.-	Ü	..--	.	.-.-.-
F	..-.	R	.-.	Ch	----	,	--..--
G	--.	S	...	0	-----	?	..--..
H		T	-	1	.----	!	.._..
I	..	U	..-	2	..---	:	---...
J	.---	V	...-	3	...--	“	.-.-.-
K	-.-	W	.-.-	4	-	‘	.-----
L	.-..	X	-.-.-	5		=	-...-

Fig. 1.4.13 Código Morse

1883 - Auguste Kerckhoff

Auguste Kerckhoff es mejor conocido por una serie de dos ensayos que publicó en 1883 en el Periódico de Ciencia Militar. Estos artículos examinaban el estado del arte en la criptografía militar e incluía muchas piezas de recomendaciones y reglas generales, incluyendo sus seis famosos principios de diseño de cifrado práctico. El mejor conocido es el segundo de sus seis principios, conocido como la Ley de Kerckhoff's. Esta ley establece que: "No hay secreto en el Algoritmo – Todo esta en la clave".

1917 – Telegrama Zimmerman

El telegrama Zimmerman daba instrucciones al embajador alemán en México para proponer a este país una alianza en caso de que estallara la guerra entre los Estados Unidos y Alemania, con la promesa de que México recuperaría Texas, Nuevo México y California. Mas aun, sugería al presidente Carranza la posibilidad de una alianza con Japón para atacar a los Estados Unidos. Zimmerman tuvo que cifrar su telegrama porque era consiente de que los aliados interceptaban todas sus comunicaciones trasatlánticas. En efecto, el telegrama fue interceptado por lo británicos quienes consiguieron descifrarlo completamente, prueba de la supremacía de los criptoanalistas aliados durante la Primera Guerra Mundial.

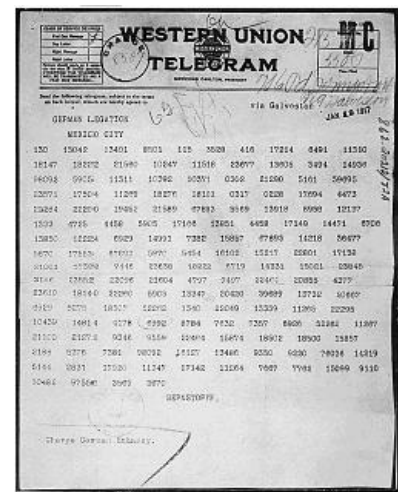


Fig. 1.4.14 Telegrama Zimmerman

1918 – Cifrado ADFGVX

El cifrado ADFGVX alemán fue el primer cifrado usado por la Armada Alemana durante la Primera Guerra Mundial. Este usaba un cifrado de transposición fraccionaria la cual combino una raíz Polybius modificada con una columna sencilla de transposición usada para codificar 36 letras de alfabeto (26 letras mas 10 dígitos).

1918 – La máquina Enigma

La solución al fracaso en la seguridad de las comunicaciones alemanas durante la Primera Guerra Mundial fue el Enigma, la maquina de cifrado de mensajes mas

avanzada hasta la llegada de la computadora y la cual supuso un punto de inflexión en la historia de la criptografía.

La máquina Enigma fue inventada por Arthur Scherbius, ingeniero alemán. Básicamente, Enigma era una maquina electromecánica que constaba de los siguientes elementos:

- ◆ Un teclado de 26 letras, similar al de una maquina de escribir.
- ◆ Un tablero luminoso, formado por 26 bombillas, una para cada letra.
- ◆ Una unidad de modificadores o rotores, discos circulares con 26 contactos. Cada uno de estos discos estaba conectado al siguiente mediante un complejo cableado.
- ◆ Un clavijero, situado en la parte frontal, de 26 clavijas, cada una de las cuales correspondía a una letra.
- ◆ Un reflector.

La rotación del modificador es la característica esencial de la maquina Enigma. Cada vez que se pulsa una letra en el teclado, el primer modificador gira un espacio. El segundo disco modificador permanece inmóvil hasta que el primero realiza una revolución completa, y así sucesivamente con el resto de los modificadores que haya. La corriente eléctrica que transmite el cableado hace que encienda en el tablero luminoso la bombilla correspondiente a la letra ya cifrada.

A pesar de la complejidad interna de la maquina, su manejo era muy sencillo: una vez que el operador dispone la configuración inicial, tecleaba el texto a cifrar y cada vez que una tecla era pulsada se

iluminaba su letra equivalente en el texto cifrado. Entonces se apuntan las letras que se iban iluminando y se transmitía el mensaje. La inclusión del reflector permitió que el cifrado y descifrado fueran simétricos, es decir, que la misma clave que se utilizaba para cifrar sirviese para descifrar.

El desciframiento de la Enigma por parte de los aliados supuso un esfuerzo colectivo sin precedentes en la historia. Los criptoanalistas luchaban a diario desde la media noche en que los operadores alemanes cambiaban a la nueva clave del día, los descifradores empezaban de cero.



Fig. 1.4 15 Máquina Enigma

1937 - 1945 La Segunda Guerra Mundial

Las dificultades de los Estados Unidos en la campaña del Pacífico ante los criptoanalistas japoneses los llevó a utilizar la lengua navaja como código seguro. Esta lengua no estaba escrita y por tanto sería casi imposible de descifrar para el enemigo. Además, las comunicaciones presentaban la ventaja de ser mucho más rápidas. Cifrar un mensaje escrito, radiarlo en Morse, transcribirlo y volver a descifrarlo en el punto de recepción a menudo llevaba una hora o más. Los navajos, sin embargo, entregaban sus mensajes en minutos. En 1968 el código navajo fue desclasificado y a partir de 1982, los Estados Unidos declararon el 14 de agosto como el Día nacional de los mensajeros de código navajo, justo homenaje a uno de los poquísimos códigos de la historia que nunca fue descifrado.



Fig. 1.4.16 Indios Navajos operando radio portátil

1.5 ALGORITMOS

El algoritmo es una descripción explícita de cómo un procedimiento debe ser efectuado o un problema debe ser resuelto. La eficiencia de un algoritmo puede ser medida como el número de pasos elementales que lleva para solucionar un problema.

Las dos técnicas más básicas de *cifrado* en la **criptografía clásica** son:

- ⊕ **Sustitución.**- Supone el cambio de significado de los elementos básicos del mensaje: las letras, los dígitos o los símbolos
- ⊕ **Transposición.**- Supone una reordenación de los elementos básicos del mensaje.

La gran mayoría de las *cifras* clásicas son combinaciones de estas dos operaciones básicas.

En la **criptografía moderna** existen dos grandes grupos de *cifras*: los algoritmos que utilizan una única *clave* tanto en el proceso de *cifrado* como en el de *descifrado* y los que utilizan una *clave* para *cifrar* mensajes y una *clave* distinta para *descifrarlos*. Los

primeros se denominan **cifras simétricas** o de **clave simétrica** y son la base de los algoritmos de cifrado clásico. Los segundos se denominan **cifras asimétricas**, de **clave asimétrica**. También son conocidos como de **clave privada** y **clave pública** respectivamente y forman el núcleo de las técnicas de cifrado modernas [4].

Criptografía de clave secreta

Se incluyen en esta familia el conjunto de algoritmos diseñados para cifrar un mensaje utilizando una única clave conocida por los dos interlocutores, de manera que el documento cifrado sólo pueda descifrarse conociendo dicha clave secreta. Algunas de las características más destacadas de este tipo de algoritmos son las siguientes:

- A partir del mensaje cifrado no se puede obtener el mensaje original ni la clave que se ha utilizando, aunque se conozcan todos los detalles del algoritmo criptográfico utilizado.
- Se utiliza la misma clave para cifrar el mensaje original que para descifrar el mensaje codificado.
- Emisor y receptor deben haber acordado una clave común por medio de un canal de comunicación confidencial antes de poder intercambiar información confidencial por un canal de comunicación inseguro.

Los algoritmos simétricos más conocidos son: **DES, 3DES, RC2, RC4, RC5, IDEA, Blowfish y AES**.

El más estudiado y probablemente el más ampliamente utilizado es DES (Data Encryption Standard). Sin embargo, debido al poder computacional, la versión básica de DES ya no pudo ser considerada suficientemente segura. Un cifrado más poderoso es el AES (Advanced Encryption Standard), el cual reemplazara al DES [5].

Criptografía de clave pública

Esta categoría incluye un conjunto de algoritmos criptográficos que utilizan dos claves distintas para cifrar y para descifrar el mensaje. Ambas claves tienen una relación matemática entre sí, pero la seguridad de esta técnica se basa en que el conocimiento de una de las claves no permite descubrir cuál es la otra clave.

Cada usuario cuenta con una pareja de claves, una la mantiene en secreto y se denomina clave privada y otra la distribuye libremente y se denomina clave pública. En este caso los algoritmos asimétricos garantizan que el mensaje original sólo puede volver a recuperarse utilizando la clave privada del destinatario.

Algunas de las características más destacadas de este tipo de algoritmos son las siguientes:

- Se utilizan una pareja de claves denominadas clave pública y clave privada, pero a partir de la clave pública no es posible descubrir la clave privada.
- A partir del mensaje cifrado no se puede obtener el mensaje original, aunque se conozcan todos los detalles del algoritmo criptográfico utilizado y aunque se conozca la clave pública utilizada para cifrarlo.
- Emisor y receptor no requieren establecer ningún acuerdo sobre la clave a utilizar. El emisor se limita a obtener una copia de la clave pública del receptor, lo cual se puede realizar, en principio, por cualquier medio de comunicación aunque sea inseguro.

A diferencia de los algoritmos de clave secreta, los métodos asimétricos son muy recientes. El algoritmo **RSA** es el más utilizado en la actualidad.

La seguridad del algoritmo RSA reside en la dificultad que supone la factorización de un número compuesto por factores primos muy grandes. Si un criptoanalista fuera capaz de encontrar los factores primos sería capaz también de determinar la clave privada y, por lo tanto, descifrar el mensaje. Sin embargo el problema de factorización se considera imposible de resolver en la práctica, y cuanto más grande sean los números utilizados, es decir las longitudes de las claves, mayor dificultad se alcanza.

Los algoritmos asimétricos se pueden utilizar para cifrado de documentos secretos o para firma electrónica tanto de documentos privados como públicos.

1.6 OBSERVACIONES

Un problema particularmente importante ha sido la exportación de criptografía y de software y hardware criptográfico. Debido a la importancia del criptoanálisis durante la Segunda Guerra Mundial y a la expectativa de que la criptografía continuaría siendo importante para la seguridad nacional muchos gobiernos occidentales han regulado estrictamente la exportación de criptografía.

En la sociedad actual se hace necesaria la seguridad en las comunicaciones, y como principal exponente en Internet, ya que este método de comunicación es cada vez mas utilizado en universidades, empresas, particulares. Con lo cual cabe pensar que el tema que hemos tratado será uno de los claros exponentes a tener muy en cuenta en la informática, sobretodo a la velocidad que se implementan nuevas tecnologías, las cuales permiten el envío de información valiosa y confidencial que puede comprometer a los interlocutores en caso de que sea interceptada por otras personas.

En la actualidad, el campo de aplicaron de la criptografía se ha ampliado, pero, ¿son estos nuevos métodos realmente seguros? Alguna ocasión Edgar Allan Poe dijo: “es dudoso que el genero humano logre crear un enigma que el mismo ingenio humano no resuelva”

1.7 REFERENCIAS

- [1] www.cryptographyworld.com
- [2] “*Seguridad Informática y Criptografía*”, Jorge Ramío Aguirre Ed. International Thompson Publishing
- [3] www.xramp.com/resources/cryptography-history
- [4] http://www.wikilearning.com/curso_de_seguridad_informatica_en_diapositivas-wkc-3584.htm
- [5] www.ssh.com/support/cryptography

2.0 SINCRONIZACIÓN

2.1 DEFINICIÓN

Propiedad que presentan algunos objetos de naturaleza distinta a manifestar un ritmo informe de coexistencia, generalmente distinto a su ritmo individual y necesariamente en presencia de una conexión o de un medio físico de acoplamiento, el cual, en la mayoría de los casos es extremadamente débil [1].

Una definición dada por Pikovsky en su libro Sincronización [2] es la siguiente: “Ajuste de ritmos de objetos oscilantes debido a sus débiles interacciones”.

2.2 SIGNIFICADO

Sus orígenes provienen de las palabras en griego **chronos** (tiempo) y **syn** (lo mismo, común, coincidencia).

Este termino, así como las palabras “Sincronización” y “sincronizado”, se refieren a una inmensa variedad de fenómenos que ocurren al mismo tiempo, en casi todas las ramas de las ciencias naturales, ingeniería y la vida cotidiana; fenómenos que aparentan ser algo diferentes pero sin embargo obedecen a las mismas leyes universales.

2.3 ANTECEDENTES HISTÓRICOS

El investigador Christiaan Huygens fue probablemente el primer científico que observó y describió el fenómeno de la sincronización en el siglo XII. El descubrió que una pareja de péndulos de reloj que colgaban de un soporte común se sincronizaban, esto es, sus oscilaciones coincidían perfectamente. Este descubrimiento fue hecho durante una serie de pruebas cuya intención era determinar la longitud de los péndulos. De hecho, la invención y diseño de los relojes de péndulo fue uno de los más importantes logros de Huygens [3].



Fig. 2.3.1 Christiaan Huygens

Tras su invención, Huygens continuó sus esfuerzos para incrementar la precisión y estabilidad de tales relojes. El puso especial atención en la construcción de relojes convenientes para el uso en barcos en mar abierto. En sus memorias, Huygens de forma breve, pero extremadamente precisa, describió sus observaciones de sincronización de la siguiente manera:

Es de bastante valor notar que cuando se suspenden dos relojes bien contruidos de dos ganchos incrustados en la misma viga de madera, el movimiento de cada péndulo en oscilaciones opuestas fue tan concordante que nunca retrocedieron en lo mas mínimo uno de otro y el sonido de ellos se escuchaba simultáneamente.

Además, si esta concordancia se desequilibraba

por alguna interferencia, se restablecía por si mismo en un corto tiempo. Por largo tiempo estuve asombrado de este resultado inesperado, pero tras una cuidadosa examinación finalmente encontré que la causa de esto era debido al movimiento de la viga, aun cuando esto es difícilmente perceptible. La causa es que la oscilación de los péndulos, en proporción a sus pesos, transmite algún movimiento a los relojes. Este movimiento impuesto en la viga, necesariamente tiene el efecto de hacer que los péndulos lleguen al estado de oscilaciones exactamente contrarias si sucedió que se movieron de otra manera en un inicio y finalmente el movimiento de la viga cesa completamente.

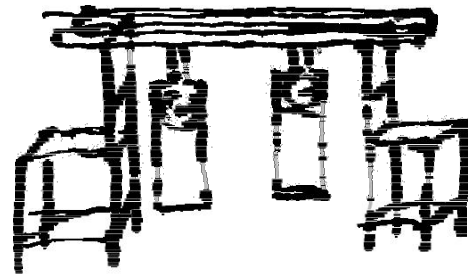


Fig. 2.3.2 Dibujo original de Christiaan Huygens ilustrando su observación de la sincronización de péndulos de reloj

De esta forma, Huygens no solo había dado una descripción exacta, sino también una brillante explicación de este efecto de sincronización mutua; él entendió correctamente que la conformidad de los ritmos de ambos relojes había sido causada por un movimiento imperceptible de la viga. En la tecnología moderna esto significa que los relojes fueron sincronizados en anti-fase debido al acoplamiento a través de la viga.

En la mitad del siglo XIX, en su tratado, La teoría del Sonido, William Strutt (Lord Rayleigh) describió el interesante fenómeno de la sincronización en sistemas acústicos como sigue:

Cuando dos tubos de órgano del mismo tono se colocan juntos, complicaciones sobrevienen las cuales frecuentemente dan problema en la práctica. En casos extremos los tubos casi reducen uno al otro al silencio. Aun cuando la influencia mutua es más moderada, podría ir más allá como para provocar que los tubos vayan al unísono a pesar de pequeñas e inevitables diferencias.



Fig. 2.3.3 John William Strutt, Lord Rayleigh



Fig. 2.3.4 En los tubos de órgano se observa la sincronización

Así, Rayleigh no solo observó la sincronización mutua cuando dos tubos distintos pero similares comenzaban a sonar al unísono, sino también el efecto de oscilación muerta cuando el acoplamiento resulta en la supresión de oscilaciones de sistemas en interacción.

Una nueva etapa en la investigación de sincronización se relacionó al desarrollo de la ingeniería eléctrica y de radio. En 1920 W. H. Eccles y J. H. Vincent confirmaron su descubrimiento de la propiedad de sincronización de un generador tríodo, un simple diseño eléctrico basado en un tubo vacío que producía una corriente eléctrica alterna periódicamente. La frecuencia de esta oscilación de corriente esta determinada por los parámetros de los elementos del esquema. En sus experimentos Eccles y Vincent acoplaron dos generadores los cuales tenían leves diferencias de frecuencia y demostraron que el acoplamiento forzaba al sistema a vibrar con una frecuencia común.

Pocos años después Edgard Appleton y Baltasar van der Pol replicaron y extendieron los experimentos de Eccles y Vincent e hicieron el primer paso en el estudio teórico de este efecto. Considerando el caso más simple, demostraron que la frecuencia de un generador puede ser sincronizada por una señal externa débil con leve diferencia de frecuencia. Estos estudios fueron de gran importancia práctica porque los generadores de triodo fueron los elementos básicos de los sistemas de comunicación por radio. El fenómeno de sincronización fue empleado para estabilizar la frecuencia de generadores poderosos con la ayuda de otro débil pero muy preciso.



Fig. 2.3.5 Sir Edward Victor Appleton

Por otro lado, la sincronización en sistemas vivientes ha sido conocida por siglos. En 1729, Jean-Jacques Dortous de



Fig. 2.3.6 Jean-Jacques Dortous de Mairan

Mairan notó que las hojas de la planta de frijol se movía hacia arriba y hacia debajo de acuerdo con el cambio de día a noche. Habiendo hecho esta observación, de Mairan

puso la planta en un cuarto oscuro y encontró que el movimiento de las hojas continuaba aun sin variaciones en la iluminación del medio. De Marian de esta forma había observado los ciclos circadianos que presentan los seres vivos.



Fig. 2.3.7 Sincronización observada en hojas de frijol

Como este último ejemplo histórico, el físico Engelbert Kaempfer tras su viaje a Siam, hoy Tailandia, en 1680 escribió:

Las larvas de luciérnaga... representan otro espectáculo, el cual ocurre en algunos árboles, como una nube ardiente, todo un enjambre de estos insectos toma posesión de un árbol y se extienden sobre sus ramas, a veces ocultan todas su luz y un momento después la hacen aparecer de nuevo con regularidad y exactitud casi perfecta.



Fig. 2.3.7 Sincronización observada en luciérnagas

Desde 1920 muchos fenómenos de sincronización han sido observados y reportados en la literatura. Más importante es la aclaración gradual de esos efectos los cuales a primera vista no tienen nada en común, sin embargo obedecen a algunas leyes universales.

Una gran cantidad de investigación llevada a cabo por matemáticos, ingenieros, físicos y científicos de otros campos ha llevado al desarrollo de un entendimiento de la conformidad de sonidos de tubos de órgano o de las no ocasionales canciones de grillos con el objetivo de poder ser descritos por una teoría unificada.

2.4 EJEMPLOS DE SINCRONIZACIÓN

Sincronización de las canciones de los grillos

Los grillos de pino es una especie común en los jardines de la mayoría de los Estados Unidos. Estos insectos pueden sincronizar sus chirridos respondiendo al chirrido precedido de sus vecinos. La canción del grillo es una secuencia larga y continua de chirridos producidos cuando el macho eleva sus alas delanteras y las frota. Cada chirrido consiste de 2 a 11 pulsos que corresponde al cierre de sus alas. El ritmo del chirrido es altamente regular en coros y usualmente ocurre así

para los grillos solitarios.



Fig. 2.4.1 Sincronización en los grillos de pino

Así, un grillo es capaz de ajustar su canción a otra como la suya rápidamente. Ya sea por alargamiento o acortamiento de su propio chirrido en la respuesta al chirrido anterior, el insecto puede alcanzar sincronía en dos ciclos según las observaciones realizadas.

Sincronización en las luciérnagas

La explicación al fenómeno visto por Kaempfer surgió a mediados de los 60's mediante un experimento realizado por el biólogo John Back y su esposa Elizabeth, tomaron muestras de luciérnagas a orillas del río Bangkok, y al llevarlas al cuarto oscuro del hotel, se dieron cuenta, de que al empezar a luminar una luciérnaga, respondieron a esta intensidad en pares y después en tríos.

Al observar esto, pensaron que las luciérnagas respondían a los haces de luz de las otras, y para comprobar esta hipótesis, después realizaron estudios en el laboratorio, donde simulaban el haz de luz de una luciérnaga, y observaron que al incidir sobre una luciérnaga el haz simulado, esta respondía al mismo tiempo (ritmo), de la misma manera y consistencia. A su vez, observaron que el tamaño y dirección del cambio

depende del estímulo del ciclo que es recibido.

Por lo que se concluyó: En una congregación de luciérnagas, cada una está continuamente enviando y recibiendo señales, cambiando los ritmos de otras y siendo cambiados por ellas alternadamente. Cada luciérnaga contiene un oscilador, un pequeño metrónomo, el cual ajusta la sincronización automáticamente en respuesta a los haces de luz de las otras luciérnagas.



Fig. 2.4.2 Sincronización en las luciérnagas

Ritmos circadianos

El comportamiento de humanos y de animales se caracteriza por un ciclo preciso de 24hrs de descanso y actividad. Este ciclo, llamado ciclo circadiano, representa la adaptación fundamental de los organismos a los estímulos del ambiente. El termino "**circadiano**" viene del latin *circa*, "alrededor de", y *diem*, "día", por lo que el significado literal es "alrededor de un día". Este ciclo del comportamiento se acompaña por una oscilación diaria en la secreción hormonal, temperatura base del cuerpo y otras importantes funciones fisiológicas.

Esta bien establecido el hecho de que la ausencia de un ciclo de luz-oscuridad provoca que el periodo del ritmo circadiano se desvíe de las 24hrs. Bajo condiciones normales, el ciclo se obtiene por las variaciones diarias de la iluminación.

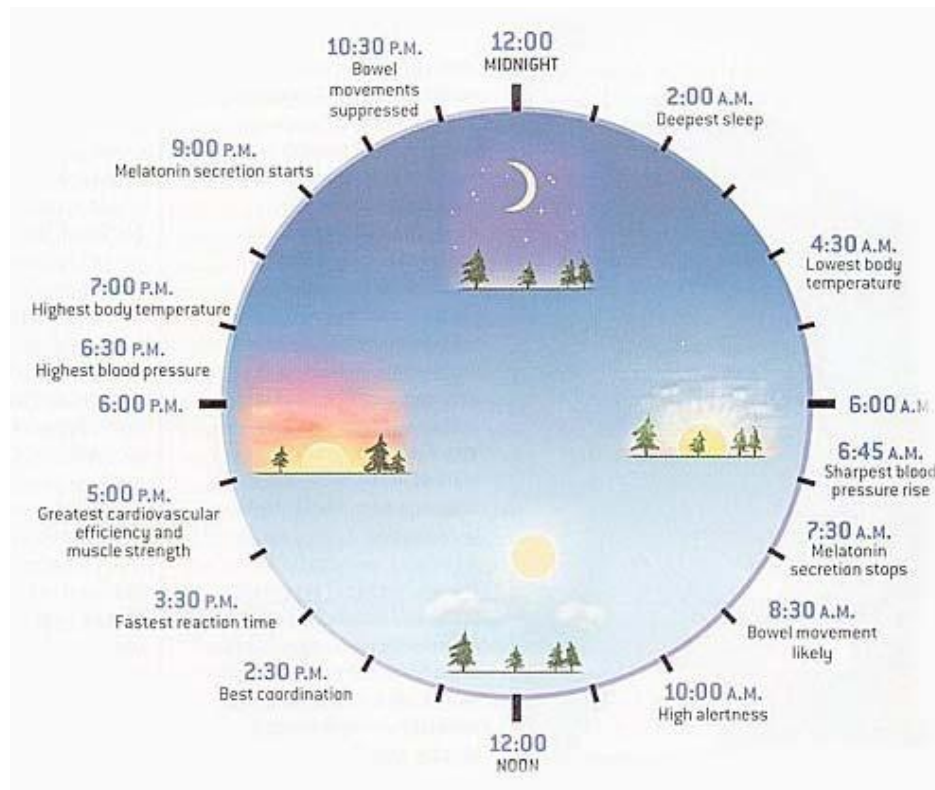


Fig. 2.4.3 El reloj circadiano afecta los ritmos diarios de muchos procesos psicológicos. El diagrama describe los patrones circadianos típicos de alguien que se levanta temprano en la mañana, come su almuerzo al mediodía y duerme en la noche. Aunque los ritmos circadianos tienden a ser sincronizados con los ciclos de luz-oscuridad existen otros factores como son temperatura, estrés y ejercicio que también pueden influir en los tiempos [4].

En experimentos en los cuales se aísla al sujeto del ciclo normal de luz-oscuridad y se priva de cualquier otra señal se observa que existe un reloj auto-sostenido que controla el ritmo. Todas las evidencias disponibles indican que hay un marcapasos principal en los mamíferos llamado núcleo "Suprachiasmatic" del hipotálamo. Este núcleo recibe información obtenida de las células de la retina.

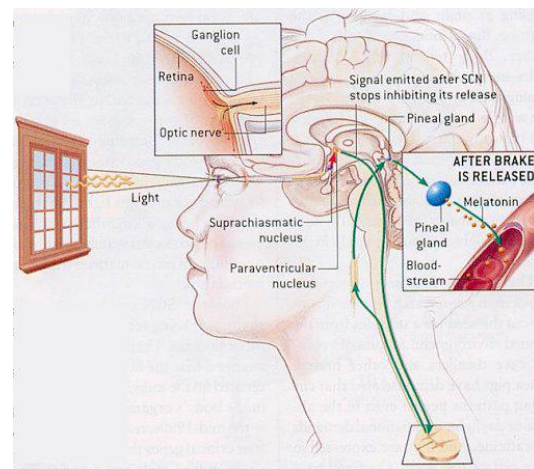


Fig. 2.4.4 El núcleo "Suprachiasmatic" del hipotálamo funciona como un marcapasos del ritmo circadiano

El ciclo menstrual

El ciclo menstrual puede ser estimado como una oscilación ruidosa de la concentración de varias hormonas. El periodo de oscilación es de alrededor de 28 días pero puede fluctuar considerablemente.

Un reporte presentado de un estudio detallado de ciclos menstruales de 135 mujeres con edades entre 17-22 años, todas residentes de un dormitorio en un colegio de mujeres mostraron un incremento en la sincronía en el inicio del ciclo durante el año académico. Esto confirmó la

influencia de grupos sociales en algunos aspectos del ciclo menstrual, demostrando que las influencias de tales grupos balancean el sistema endocrino. En particular, se demostró que la dispersión del inicio de las menstruaciones con diferentes grupos de "amigos cercanos" con el grupo bajo investigación decrece durante el año académico. El estudio indica la existencia en los humanos de algunos procesos fisiológicos interpersonales los cuales afectan el ciclo menstrual.



Fig. 2.4.5 El ciclo menstrual tiende a sincronizarse en grupos

cercanos de mujeres a través de las feromonas

El ritmo en los aplausos

En nuestro comportamiento social podemos detectar momentos de sincronía, por ejemplo, cuando una obra de teatro a llegado a su fin, justo cuando el telón se empieza a bajar se escucha un silencio momentáneo cuando de repente una persona empieza a aplaudir, unos instantes después se escuchan mas aplausos y después de unos segundos todos los espectadores están golpeando



Fig. 2.4.5 Sincronización en los aplausos de la gente

sus palmas. Cuando esto sucede, se puede escuchar claramente como poco a poco el

sonido de los aplausos se va sincronizando gradualmente hasta escuchar a toda una multitud aplaudir en sincronía.

En un experimento realizado recientemente, se grabaron varias presentaciones de opera. Se midió la intensidad de ruido global usando un micrófono colocado en el techo del teatro, y los sonidos de los aplausos individuales se promediaron mediante un micrófono oculto en las proximidades de un espectador. Se observó que el inicio de la sincronía del aplauso individual esta precedida por el doble del periodo de los aplausos del grupo. Una explicación aceptable es que en velocidades lentas los individuos son capaces de mantener un ritmo muy estable de si mismos (esto significa que cada oscilador se vuelve menos ruidoso debido a la reducción en las variaciones de la frecuencia) y la dispersión de frecuencias decrementa. Ambos factores, la reducción de ruido y la reducción de la desintonización generan la transición a la sincronización. Interesantemente, la reducción de la frecuencia apunta a una sincronía inducida como un acto voluntario de los individuos. Tal comportamiento colectivo es más típico para culturas homogéneas.

Correr y respirar en mamíferos

Se ha investigado la sincronización entre la respiración y el movimiento al correr en los mamíferos. El amarre de fase entre el miembro y la respiración ha sido grabada durante el correr de las liebres en las ruedas de juego y durante el movimiento de perros, caballos y humanos. Se encontró que en altas velocidades, el correr de las especies cuadrúpedas normalmente sincroniza los ciclos de movimiento y respiración en una relación constante 1:1. Los corredores humanos emplean varios patrones de amarre de fase



Fig. 2.4.6 Sincronización en los ciclos de movimiento y respiración

aunque la relación 2:1 parece ser la mas favorable. Queda poco claro si la sincronización entre respiración y actividades de movimiento se incrementa en **presentaciones** o si solo es una consecuencia fisiológica irrelevante de una propiedad general de acoplamiento de osciladores.

Migración de los animales

Otro fenómeno síncrono, es la migración, la cual se produce por mecanismos neurofisiológicos adquiridos por un largo proceso de selección natural, que se transmite hereditaria e instintivamente.

Las aves, al igual que otros animales, poseen dos "relojes biológicos" que determinan complejas funciones diarias y anuales, respectivamente. El reloj biológico diario responde a los ciclos diarios de luz y temperatura. El reloj anual actúa sobre el sistema hormonal y les anuncia, por ejemplo, el momento indicado para mudar plumaje, migrar, reproducirse. Estos mecanismos hacen que se den los



Fig. 2.4.7 La migración de las aves es un fenómeno síncrono.

cambios fisiológicos necesarios que los prepara para migrar en el momento indicado.

Algunas especies de aves viajan de noche. Otras lo hacen solo de día porque dependen de las corrientes de aire caliente, o termales, para trasladarse. Y hay algunas aves migratorias que viajan sin parar o haciendo muy pocas paradas hasta llegar a su destino.

El puente Millenium

Una de las sincronías más conocidas ocurrió en Londres, cuando fue inaugurado, el 10 de junio del 2000, el Millenium Bridge, el nuevo puente construido por Norman Foster. Sus 690 toneladas de acero se pusieron a temblar en el momento que cruzaron por encima de este puente los primeros centenares de londinenses. El puente registró



Fig. 2.4.8 Puente Millenium, Londres, Inglaterra

vibraciones en forma de "S" que llegaron a alcanzar desviaciones de 20 centímetros. Una explicación a este suceso la da Strogatz en su libro Sync [5], *"al caminar, creamos pequeñas fuerzas laterales con cada paso, alternativamente a la izquierda y a la derecha; estas fuerzas son pequeñas y, como normalmente no hay coordinación entre los peatones, ocurren al azar y se contrarrestan; pero al comenzar a caminar al mismo tiempo todos los asistentes, las fuerzas laterales se sumaron y se concentraron de forma sincrónica"*.

Investigaciones de los ingenieros de la constructora encontraron que en un puente largo y flexible como lo era el Millenium Bridge y con una multitud encima, *“hay posibilidades de que un grupo suficiente de gente camine en sincronía por accidente mas allá del umbral de fuerzas que el puente pueda aguantar”*.

Sincronización en mecánica celeste

La sincronización desempeña un papel importante en mecánica celeste donde explica el amarre de periodos de revolución entre planetas y satélites. Por ejemplo: la relación entre números enteros entre las velocidades angulares promedio de rotación y traslación de cuerpos celestes.

Uno de los aspectos más notorios de este hecho es que la Luna como la Tierra tienen la misma velocidad angular promedio en sus movimientos de rotación y traslación (resonancia del tipo 1:1), por lo tanto, la luna siempre muestra el mismo lado de su superficie hacia la Tierra.

La Sincronización entre la órbita de la Luna y su giro es explicado de la siguiente manera, suponiendo que la Luna sigue una órbita circular alrededor de la tierra. El tamaño de este círculo es determinado por un balance de dos fuerzas: la fuerza de gravedad que ejerce la Tierra sobre la Luna y la fuerza centrífuga del movimiento de la Luna, la cuál tiende a hacer un vuelo alrededor de la Tierra. Las dos fuerzas, la gravitacional y la centrífuga se balancean una a la otra



Fig.2.4.9 Sincronización entre la Tierra y la Luna

perfectamente en el centro de la Luna. Sobre el lado cercano de la Luna, la gravedad es más fuerte; sobre el lado lejano, la fuerza centrífuga es más fuerte. Este desbalance crea dos pequeños bombeos en la Luna, uno en el lado cercano y otro en el lado lejano. El mismo acontecimiento ocurre en la Tierra debido a la fuerza que ejerce la Luna, causando las mareas en el océano.

2.5 APLICACIONES DE LA SINCRONIZACIÓN

Marcapasos

Una aplicación importante en medicina es el marcapasos, los cuáles envían pulsos eléctricos dentro de áreas específicas del corazón dictando a los músculos una frecuencia necesaria de contracción (entre 60-70 por minuto). Básicamente el marcapasos es un circuito eléctrico oscilatorio, equivalente a un capacitor en paralelo con una resistencia (el capacitor es un dispositivo que almacena voltaje, y tiene un rol relacionado a las membranas de la célula; una resistencia provee de una

camino para la corriente de la célula, análogamente llamado canal de salida en la membrana). Una constante entrada de corriente causa que el capacitor se cargue, incrementando su voltaje constantemente.

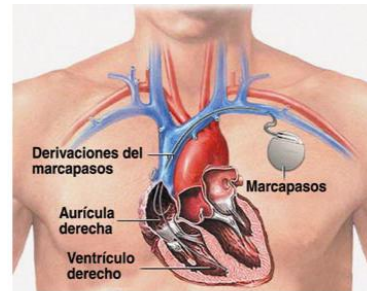


Fig. 2.5.1 La sincronía aplicada en la medicina a través del marcapasos

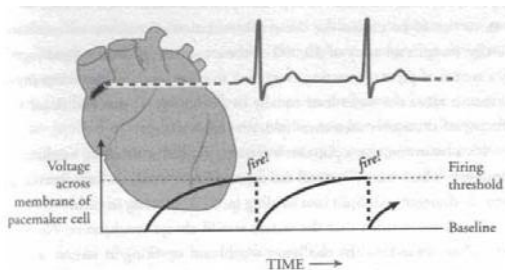


Fig. 2.5.2 Respuesta del marcapasos en el tiempo

Mientras tanto, así como en los rizados de voltaje, la cantidad de corriente de subida a través de la resistencia incrementa, entonces el tiempo de incremento disminuye lentamente. Cuando el voltaje llega a su valor máximo (umbral) el capacitor se descarga, y el voltaje cae instantáneamente a cero (este comportamiento simula el pulso del marcapasos y consecuentemente su regreso al inicio). Entonces el voltaje comienza a subir de nuevo, y el ciclo empieza de nuevo. Pero existe un ligero problema, al introducir el pulso: las oscilaciones que están cerca del umbral están golpeadas cerca del oscilador pulsante, pero los que están cerca de la línea del fondo (cero) son golpeados más lejos de la fase. En otras palabras, un pulso simple tiene efectos sincronizados para algunas oscilaciones y efectos desincronizados para otros.

Sincronización de generadores eléctricos

El fenómeno de sincronización en los generadores eléctricos se lleva a cabo a través de una carga común, la cual manejan estos generadores, y ésta misma actúa como un factor sincronizante.

Sincronización de Oscilaciones eléctricas y electromagnéticas

La sincronización de oscilaciones eléctricas y electromagnéticas en electrónica y radio física también ha traído grandes aportaciones debido sus campos de aplicación:

- ◆ Redes neuronales.
- ◆ Incremento en la potencia de los láseres.
- ◆ Control de oscilaciones en reacciones químicas.
- ◆ Telefonía digital, video y audio digital donde flujos de datos muestreados se manipulan
- ◆ Estabilización del pulso erróneo de corazones de animales enfermos.
- ◆ ***Codificación de mensajes electrónicos para comunicación segura***

2.6 OBSERVACIONES

En estos y otros numerosos casos, la sincronización representa un papel fundamental ya que establece alguna relación especial entre sistemas o mecanismos acoplados.

Sin exageración alguna, la propiedad de sincronización esta presente tanto en el macrocosmo como en el microcosmos, de hecho, es motivo de profundas discusiones filosóficas, ya que ofrece una oposición optimista de la armonía del universo en contra de la posición que ofrece la entropía.

En nuestros días, dicha propiedad es ampliamente empleada en tecnología, ya sea en dispositivos eléctricos, de radio, maquinas vibratorias,... donde las frecuencias a las cuales operan de manera independiente dichos sistemas, difieren en la mayoría de los casos, unas de otras

2.7 REFERENCIAS

- [1] Sincronización de Osciladores de Lorenz por formas Hamiltonianas, Cornelio Posadas Castillo, Tesis Maestría en Ciencias CICESE.
- [1] Evaluación y medición de un experimento en un caso de sincronización, Carlos Casio, Tesis Maestría en Ciencias CICESE.
- [2] Synchronization, Arkady Pikovsky, Cambridge University
- [3] <http://www.scienceandsociety.co.uk/results.asp?image=10239953>
- [4] The body clock guide to better health, Michael Smolensky and Lynn Lamberg
- [5] Sync, Steven Strogatz, Ed New York
- Synchronization in Science and Technology, I.I. Blekhman

3.0 CAOS

3.1 INTRODUCCIÓN

A principios de siglo, los físicos especulaban con que su materia de estudio se estaba acabando, pronto no habría aspectos físicos relevantes que pudieran descubrirse. En efecto, sólo les faltaba por resolver tres problemas:

- ◆ La órbita irregular de Mercurio
- ◆ La discrepancia entre la teoría y la cantidad de energía liberada por un agujero negro
- ◆ El efecto de un tercer cuerpo en el movimiento de otros dos

Resultó que la naturaleza es bastante más sutil de lo que imaginaron y el intento de completar la información respecto al primer caso condujo a la *teoría de la relatividad*; el segundo hizo aparecer la *teoría cuántica*; y del tercero surgió la **teoría del caos**. Cada una de estas teorías con misterios que resolver.

La teoría del Caos es una disciplina que ha aparecido hace unos años a partir del intento de establecer leyes físicas para la predicción del tiempo atmosférico y que está encontrando amplia aplicación en muchos campos de la ciencia, en los movimientos llamados caóticos, como los movimientos de las partículas en un fluido, la estabilidad del medio interno (homeostasis), etc.

Si bien es cierto que la Teoría del Caos no niega el mérito de la ciencia clásica, propone un nuevo modo de estudiar la realidad. Así, las leyes del caos ofrecen una explicación para la mayoría de los fenómenos naturales, desde el origen del universo a la propagación de un incendio o a la evolución de una sociedad.

3.2 SIGNIFICADO [1]

En la mitología griega, el Caos o Khaos es el estado primitivo de existencia del que surgieron los primeros dioses. En griego es Χάος o Χάεος, que significa 'vacío que ocupa un hueco', y procede del verbo χαίνω, 'abrirse de par en par', y éste del indoeuropeo **ghen-*, **ghn-*. También se le llamaba Aêr (Αἴρ, 'aire').

3.3 DEFINICIÓN

El **caos** es un comportamiento impredecible que surge en un sistema determinista debido a la gran sensibilidad a las condiciones iniciales que presenta. El caos surge en un sistema dinámico si dos puntos arbitrarios iniciales y cercanos divergen exponencialmente tal que su comportamiento futuro es eventualmente impredecible.

El término Caos se refiere a una interconexión subyacente que se manifiesta en acontecimientos aparentemente aleatorios [2]

El caos es impredecible, pero determinable. O dicho de otro modo, el caos no es aleatorio, tiene un orden subyacente [7]

La gran sensibilidad a las condiciones iniciales se observa en: "*El efecto mariposa*".

A saber: "Si hoy agita una mariposa sus alas en Barcelona, con su aleteo puede producir un huracán en Tokio el mes que viene."

Este concepto es el que se conoce como "*Dependencia sensitiva de las condiciones iniciales*" que es determinante y básico para comprender este mundo tan maravilloso, tan caótico y regular a la vez.

Los **sistemas dinámicos**, son sistemas que varían con el paso del tiempo, tales como la teoría maltusiana de población y recursos, la meteorología, los seísmos, los movimientos que efectúa un chorro de café humeante al entrar en contacto con la leche de un taza (mecánica de fluidos), el giro impredecible de una noria de agua cuando su caudal es inusitadamente acelerado, la gran mancha de Júpiter, las fluctuaciones económicas de los precios, etc.

Es en los sistemas dinámicos donde podemos usar el término "caos" y donde una variación mínima de las condiciones iniciales supone un comportamiento totalmente distinto del esperado por parte del sistema. Es decir, que un sistema podrá ser caótico cuando su comportamiento sea impredecible.

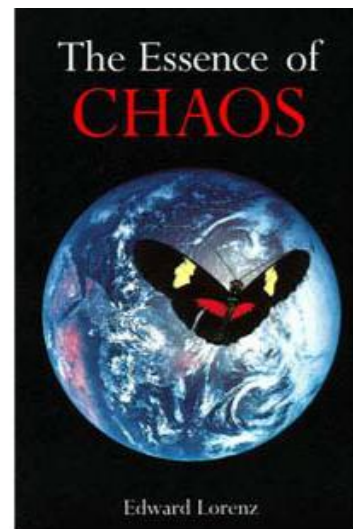


Fig. 3.3.1 E. Lorenz acuñó el término *efecto mariposa* para indicar aquellas situaciones en las que una pequeña causa puede multiplicarse de tal modo que acabe produciendo un resultado catastrófico.

El caos es determinista al estudiar uno de estos sistemas, si se trata en su globalidad. No podrá predecir el estado futuro del mismo pero sí modelar su comportamiento general. Estos sistemas pueden comportarse de diferentes formas, pero muchos de ellos tras suficientes iteraciones (repetición de un cálculo simple) de las funciones que los determinan su función tiende a estabilizarse en uno o más valores. Este conjunto de valores para los cuales la función $f(x)$ se estabiliza cuando el número de iteraciones tiende a infinito, se denomina "*atractor*".

Características de los sistemas caóticos:

- ◆ Deterministas.- Siguen unas reglas que pueden resumirse en una serie de funciones.
- ◆ Sensibles.- A las condiciones iniciales ya que un cambio mínimo en sus datos iniciales puede provocar un resultado totalmente inesperado
- ◆ Simples.- No en cuanto a su comportamiento sino en cuanto a las funciones que los determinan

3.4 ATRACTORES

El concepto *atractor* va ligado al de los "*sistemas dinámicos*". Para caracterizar un sistema dinámico, contamos con variables dinámicas (por ejemplo, posición y velocidad), y variables estáticas, estas últimas son los parámetros o constantes. Un **espacio de estados**, es una representación gráfica cartesiana, donde cada eje es una variable dinámica. Cada punto es una instantánea del estado, y la línea descrita por esa sucesión de puntos, se denomina *trayectoria*. Dicha trayectoria es arrastrada hacia una región del espacio de estados llamada **atractor**, que no es sino la manifestación de los parámetros fijos y de las ecuaciones que determinan los valores de las variables dinámicas.

Los sistemas dinámicos pueden comportarse de diferentes formas, y su función tiende a estabilizarse en uno o más valores. Este conjunto de valores para los cuales la función $f(x)$ se estabiliza cuando el número de iteraciones tiende a infinito (∞), se denomina "**atractor**". De esta forma el atractor aparece al representar la evolución del sistema dinámico en el denominado *espacio de fases*.

En realidad, un atractor puede tener tantos ejes como se quiera, el problema es graficarlo. Si se elige un gráfico en tres dimensiones, este puede estudiarse mejor si se lo corta en "rebanadas". Dichos cortes o secciones, se denominan *secciones de Poincaré*.

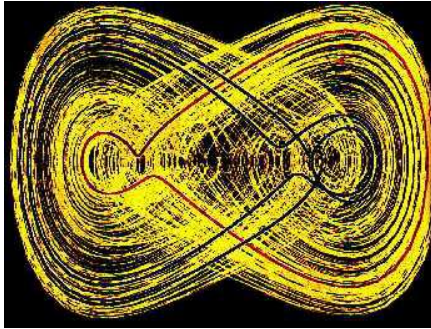


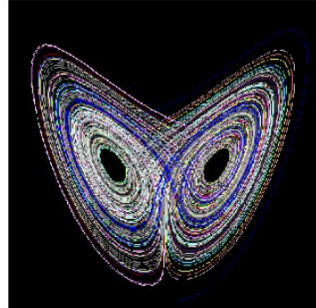
Fig. 3.4.1 Atractor caótico
En rojo la órbita de periodo uno y en azul la órbita de periodo dos

El atractor consta de múltiples órbitas periódicas. El atractor de la Fig. 3.4.1 representa un sistema cuya velocidad y posición cambian a lo largo de una sola dirección. Un eje representa la posición, el otro la velocidad.

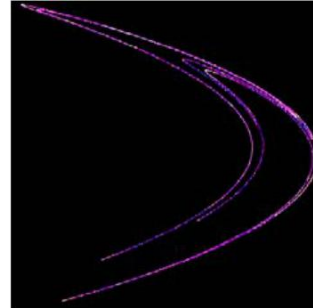
Los atractores pueden ser multidimensionales, pues los sistemas pueden tener muchas variables, que equivalen a otras tantas dimensiones en el espacio de estados: por ejemplo, posiciones y velocidades

que varíen en tres dimensiones.

Como atractores conocidos tenemos el de Lorenz, Hénon, KAM, Pickover y muchos otros. La representación visual de un atractor se puede ver en los siguientes ejemplos:



Lorenz (3D)



Henon



Ikeda (2D)



Ushiki (2D)

Fig. 3.4.2 Representación visual de diferentes atractores

La idea de un atractor es que partiendo de un sistema dinámico cuyo movimiento y actividad resulta azaroso no repitiéndose 2 valores seguidos iguales, resulta que pasado cierto tiempo se estabiliza en ciertos valores independientemente de su funcionamiento primario.

Tanto los puntos fijos como los ciclos límite son atractores, pero la dinámica caótica se caracteriza por un tercer tipo de atractor, que F. Takens y D. Ruelle en 1971 bautizaron con el sugerente nombre de "**atractor extraño**", cuya peculiaridad es el poseer una dimensión fractal [6].

La sección de Poincaré consiste en dar al atractor un corte por un plano (Fig. 3.4.3), visualizando lo que queda interceptado por dicho plano. Haciendo "zooms", adecuadamente, de la sección de Poincaré se pone de manifiesto la compleja estructura fractal del atractor.[6]

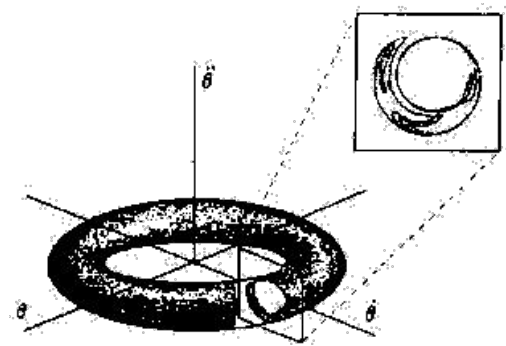


Fig. 3.4.3 La sección de Poincaré pone de manifiesto la estructura fractal del atractor

3.5 FRACTAL

Pensar en un objeto que tenga, por ejemplo, más de dos dimensiones pero menos de tres, es algo que escapa a la intuición sensible. Así nació, en un plano meramente teórico, el concepto de *dimensión fractal*.

El término "**fractal**" fue acuñado por Mandelbrot, el cual, reacio a los rigorismos matemáticos, define los objetos fractales como los que poseen la cualidad de "autosemejanza" o "simetría de escalas". Significa esta propiedad, que el objeto en cuestión ofrece el mismo aspecto observado a distintas escalas; es decir: una parte de él es semejante al total. Quizá el paradigma de fractal sea el que ha sido calificado de

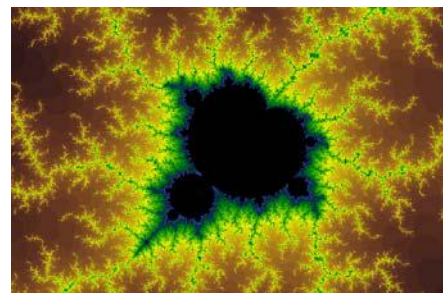


Fig. 3.5.1 Conjunto de Mandelbrot, ejemplo de objeto fractal

"objeto más complejo de la Matemática" y que lleva el nombre de su descubridor: el conjunto de Mandelbrot.

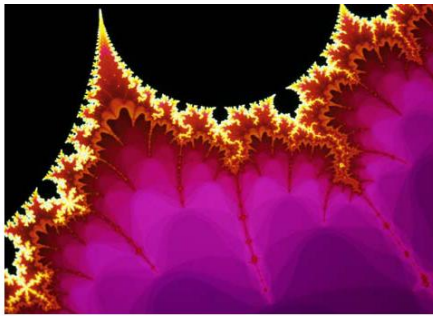


Fig. 3.5.2 Conjunto de Mandelbrot realizando un "zoom"

Este conjunto es generado por ordenador mediante un proceso iterativo. Realizando varios "zooms" consecutivos reaparecen una y otra vez réplicas semejantes, pero no idénticas, al total [6].

Benoit Mandelbrot (Fig. 3.5.3) un matemático el cual trabajaba en el área de investigación de la IBM en EU estaba estudiando la fluctuación en el precio del algodón. No importa como se analizaran los datos de los precios del algodón, los resultados no se ajustaban a la distribución normal. Mandelbrot finalmente obtuvo todos los datos disponibles de los precios del algodón, desde el año 1900. Cuando analizó los datos en los ordenadores de IBM, observó un hecho asombroso:



Fig. 3.5.3 Benoit Mandelbrot. Según Mandelbrot la geometría fractal representa la transición del orden al caos.

Los números que producen aberraciones desde el punto de vista de la distribución normal producen simetría desde el punto de vista de la escala. Cada cambio de precio particular era aleatorio e impredecible. Pero la secuencia de los cambios era escala: las curvas para los cambios del precio diario y perfectamente.

independiente de la mensual encajaban

Increíblemente, analizados de la forma de Mandelbrot, el grado de variación había permanecido constante a través del tumultuoso periodo de sesenta años que pasaba por dos Guerras Mundiales y una depresión.

Mandelbrot no sólo analizó los precios del algodón, sino muchos otros fenómenos también. En uno de ellos, se preguntaba por la longitud de una línea costera. Un mapa de una línea de costa muestra muchos entrantes. Sin embargo, al medir la longitud de

una línea costera en un mapa perderemos los entrantes que son demasiado pequeños para mostrarse en el mapa. De igual modo, caminando a lo largo de la costa perdemos los microscópicos entrantes que hay entre los granos de arena. No importa lo mucho que se amplíe una línea costera, siempre habrá más entrantes visibles si la ampliamos más.



Fig. 3.5.4 El problema del cálculo de la longitud de una línea costera

Para ver si un punto es parte del conjunto de Mandelbrot, la ecuación es simple: $z = z^2 + c$, simplemente toma un número complejo z , elévalo al cuadrado, y súmalo al número original. Eleve al cuadrado el resultado, y súmalo al número original. Repite esto hasta el infinito, y si los números que obtienes tienden a infinito, no es parte del conjunto de Mandelbrot [4]. Si se mantienen por debajo de un cierto nivel, es parte del conjunto de Mandelbrot.

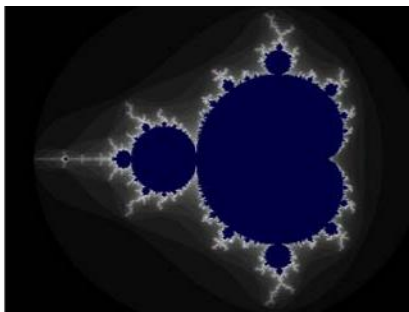


Fig. 3.5.5 Conjunto de Mandelbrot

El conjunto de Mandelbrot es la sección más interna del dibujo, y cada distinta sombra gris representa lo alejado que está ese punto en particular (Fig. 3.5.5). Una característica interesante del conjunto de Mandelbrot es que los montículos circulares encajan con el gráfico de bifurcación. El fractal de Mandelbrot tiene la misma auto-similitud vista en las otras ecuaciones. De hecho, ampliando en profundidad lo suficiente un fractal de Mandelbrot finalmente aparecerá una réplica exacta del conjunto de Mandelbrot, perfecto en cada detalle.

Lo que ha despertado particularmente el interés de los matemáticos es que el conjunto de Mandelbrot es como un muestrario de la infinita variedad de conjuntos de Julia.

Así, el conjunto de Mandelbrot encierra la gran paradoja de que la cantidad de información necesaria para describirlo es infinita, pero no así la información necesaria para generarlo, que cabe en unas pocas líneas de código de ordenador.

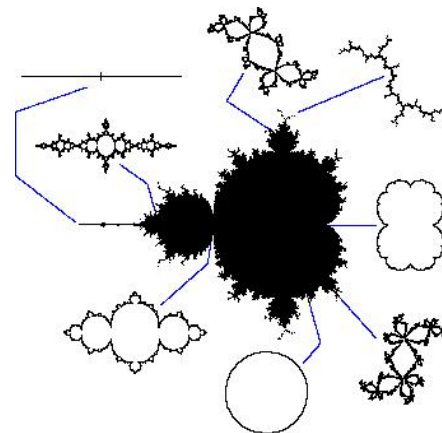


Fig. 3.5.6 El conjunto de Mandelbrot es un muestrario de los conjuntos de Julia

Peitgen y Richter (Bremen, RFA) fueron quienes lograron las representaciones más espectaculares del Conjunto de Mandelbrot coloreando transiciones de fase (Fig. 3.5.7) [10] Las "cuencas" corresponden a atractores (una característica típica de fenómenos "caóticos"). Los límites entre cuencas ponen en evidencia que la frontera entre "la calma y la catástrofe" es más complicada de todo lo que se puede imaginar, contrariamente a las proyecciones ingenieros.

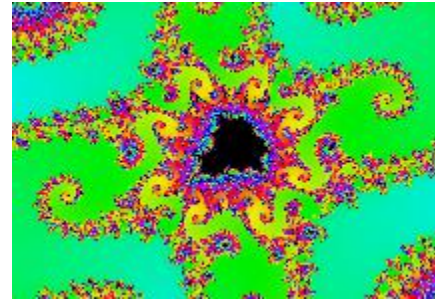


Fig. 3.5.7 Conjunto de Mandelbrot
habituales (anteriores) de los

La curva de Koch

Un matemático, Helge von Koch, creó la curva de Koch, imagina un triángulo equilátero. En el tercio central de cada lado, añade otro triángulo equilátero. Sigue añadiendo nuevos triángulos en la parte central de cada lado, y el resultado es una curva de Koch (Fig. 3.5.8). Una ampliación de la curva de Koch tendría el mismo aspecto que el original. Es otra figura auto-similar.

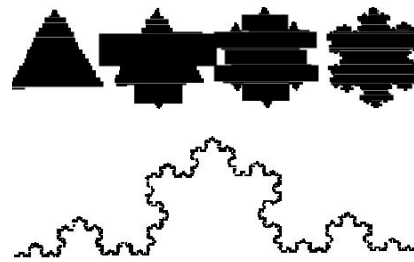


Fig. 3.5.8 La curva de Koch

La curva de Koch nos brinda una interesante paradoja. Cada vez que añadimos nuevos triángulos a la figura, la longitud de la línea se hace mayor. Sin embargo, el área interior a la curva de Koch permanece menor que el área de un círculo dibujado alrededor del triángulo original. Esencialmente, es *una línea de longitud infinita que rodea un área finita*.

Diferencia entre caos y fractal

No son sinónimos y tienen comportamientos distintos, a pesar de compartir una formulación sencilla y que ciertos fenómenos caóticos tengan una estructura fractal (atractor) [3].

Caos	Fractal
Dependencia sensitiva de las condiciones iniciales	Recursividad infinita
Impredecible	Autosemejanza, invariablemente de la escala
Definido por ecuaciones deterministas	Muchos fractales no son caóticos

Aplicaciones de los fractales actualmente

Michael Barnsley, con el invento del "juego del caos" descubrió que se pueden generar todos los fractales con reglas muy sencillas y creó un método inverso: cómo extraer la fórmula a partir del dibujo ("Teorema del collage") y demostró que el azar no juega ningún papel real. Y las investigaciones muestran que todos los fractales parecen terminar en el conjunto de Mandelbrot, confirmándose el principio de universalidad.

Las estructuras fractales se han revelado en muchas áreas del mundo real, además de en la mente de los matemáticos. Las ramificaciones de los vasos sanguíneos, las ramas de un árbol, la estructura interna de los pulmones, los gráficos de datos del mercado de valores, y muchos otros sistemas del mundo real tienen todos algo en común: son todos auto-similares

De esta forma, **fractal** ha llegado a significar cualquier imagen que muestre el atributo de la auto-similitud. El diagrama de bifurcación de la ecuación de poblaciones es fractal. El Atractor de Lorenz es fractal. La curva de Koch es fractal. [9]

3.6 SISTEMAS CAÓTICOS

Durante mucho tiempo, los científicos encontraron muchas dificultades para obtener publicaciones de sus trabajos sobre el caos. Dado que no habían mostrado aún relevancia en situaciones del mundo real, la mayoría de los científicos no pensaban que los resultados de los experimentos en el caos fuesen importantes. Como resultado, incluso aunque el caos es un fenómeno matemático, la mayoría de las investigaciones en el caos se hicieron por personas de otras áreas como la meteorología y la ecología. El campo del caos creció rápidamente como un pasatiempo para los científicos que trabajaban en problemas que tal vez tenían algo que ver con él.

Más tarde, un científico llamado Mitchell Feigenbaum estaba mirando de nuevo el diagrama de bifurcación de la ecuación de poblaciones. Miraba la velocidad a la que llegaban las bifurcaciones. Descubrió que aparecían a una tasa constante. La calculó como 4,669. En otras palabras, descubrió la escala exacta a la que eran auto-similares. Haz el diagrama 4,669 veces menor, y aparece igual a la siguiente región de bifurcaciones. Decidió mirar otras ecuaciones para ver si era posible determinar factores de escala también para ellas. Para su total sorpresa, el factor de escala era exactamente el mismo. No solo esta compleja ecuación mostraba regularidad, la regularidad era exactamente la misma con una ecuación mucho más simple. Hizo el intento con muchas otras funciones, y todas ellas produjeron el mismo factor de escala, 4,669.

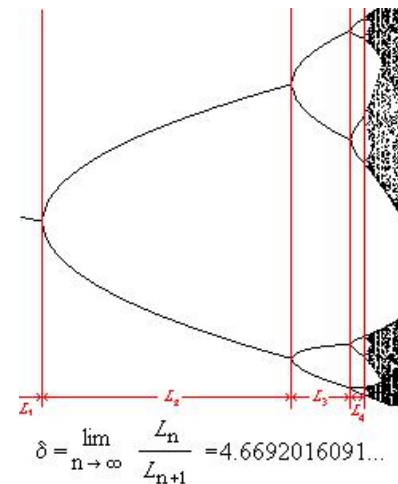


Fig. 3.6.1 La constante universal de Feigenbaum

Este fue un descubrimiento revolucionario. Había encontrado que una clase entera de funciones matemáticas se comportaban del mismo modo predecible. Esta generalización ayudaría a otros científicos a analizar fácilmente ecuaciones caóticas. La generalización dio a los científicos las primeras herramientas para analizar un sistema caótico. Ahora simplemente podían usar una ecuación simple para predecir el resultado de una ecuación más compleja.

La ecología y la predicción de las poblaciones biológicas

La ecuación que define las poblaciones biológicas sería simple si la población sólo creciera de forma indefinida, pero los efectos de los predadores y un suministro de alimento limitado hacen esta ecuación incorrecta. La ecuación más simple que tiene esto en cuenta es la siguiente:

$$\text{Población del año siguiente} = r * \text{población de este año} * (1 - \text{población de este año})$$

En esta ecuación, la población es un número entre 0 y 1, donde 1 representa el máximo de población posible y el 0 la extinción, r es la tasa de crecimiento. La pregunta era, ¿Cómo afectan estos parámetros a la ecuación? La respuesta obvia es que una mayor tasa de crecimiento implica que un aumento en la población, mientras que una menor tasa de crecimiento decrementará el número. Esta tendencia es cierta para algunas tasas de crecimiento,



Fig. 3.6.2 La interacción depredador presa presenta un comportamiento caótico

pero no para todas ellas.

Un biólogo, Robert May, decidió ver qué sucedía con las ecuaciones cuando cambiaba el valor de la tasa de crecimiento. A valores bajos de tasa de crecimiento, la población se establecería en un único número. Por ejemplo, si la tasa de crecimiento es 2.7, la población se establecerá en 0.6292. Cuando se incrementa la tasa de crecimiento, la población final se incrementaría también. Entonces, sucedió algo extraño. Tan pronto como la tasa de crecimiento pasaba de 3,

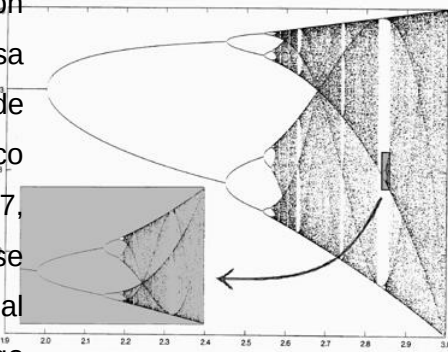


Fig. 3.6.3 Diagrama de bifurcación para la ecuación de poblaciones

la línea se rompía en dos. En lugar de establecerse en una única población, saltaría entre dos poblaciones distintas. Tendría un valor para un año, otro para el siguiente, repitiendo el ciclo para siempre. Incrementar la tasa de crecimiento un poco más provocó que saltara entre cuatro valores distintos. Cuando el parámetro crecía aún más, la línea se bifurcaba de nuevo. Las bifurcaciones llegaban más y más rápidamente hasta que de pronto, aparecía el caos. Pasada una cierta tasa de crecimiento, se hacía imposible predecir el comportamiento de la ecuación. Sin embargo, bajo una inspección

más detallada, es posible ver líneas claras. Mirando más de cerca, estas líneas revelan pequeñas ventanas de orden, donde la ecuación va a través de las bifurcaciones de nuevo antes de volver al caos. Esta auto-similitud, el hecho de que el gráfico tenga una copia exacta de sí mismo oculta en su interior, viene a ser un aspecto importante del caos.

El goteo de un grifo

Científicos de la UC Santa Cruz encontraron caos en el goteo del agua de un grifo. Tomando datos de un grifo que gotea y tomando datos de los periodos de tiempo, descubrieron que a cierta velocidad de flujo, el goteo no tenía lugar en tiempos iguales. Cuando realizaron los gráficos de los datos, descubrieron que el goteo en efecto seguía un patrón.



Fig. 3.6.4 El goteo de un grifo presenta un comportamiento caótico

El corazón humano

El corazón humano también sigue un patrón caótico. El tiempo entre latidos no se mantiene constante; depende de la actividad que la persona está realizando, entre otras cosas. Bajo ciertas condiciones, el latido puede acelerarse. Bajo condiciones distintas, el corazón late de forma errática. Podría incluso llamarse latido caótico. Estas pequeñas alteraciones son una señal de salud del corazón, una muestra del vigor del sistema caótico, que es flexible a los cambios. El caos permite al corazón un abanico de comportamientos (grados de libertad) que le permiten volver a su ritmo normal después de un cambio.

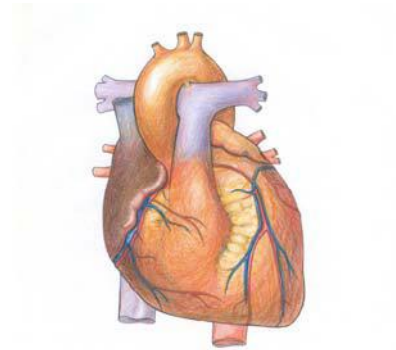


Fig. 3.6.5 El corazón sigue un patrón caótico

El análisis del latido puede ayudar a los investigadores médicos a encontrar formas de colocar un latido anormal de nuevo en un estado seguro, en lugar del caos incontrolado (Fig. 3.6.6).

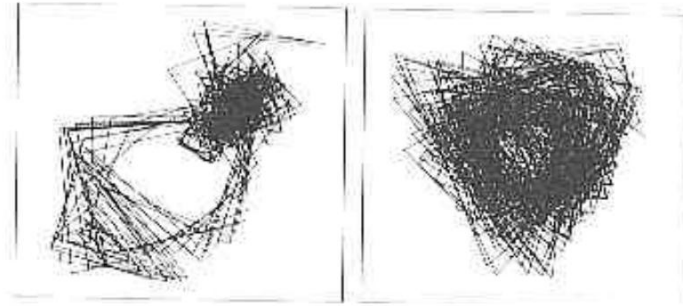


Fig.3.6.6 a) Gráfico que muestra un comportamiento de un corazón sano b) Gráfico de un corazón enfermo, que con el más pequeño cambio se pararía.

El helecho

Los investigadores descubrieron un conjunto simple de tres ecuaciones que dibujaba un helecho. Esto inició una nueva idea, tal vez el ADN no codificaba exactamente el crecimiento de las hojas, sino una fórmula que controlaba su distribución. El ADN, incluso aunque mantiene una sorprendente cantidad de datos, no puede mantener todos los datos necesarios para determinar dónde va cada célula del ser humano. Sin embargo, usando fórmulas fractales para controlar como crear nuevas fibras nerviosas y vasos sanguíneos, el ADN tiene información más que suficiente. Se ha especulado que el cerebro mismo podría estar organizado de alguna forma de acuerdo con las leyes del caos.

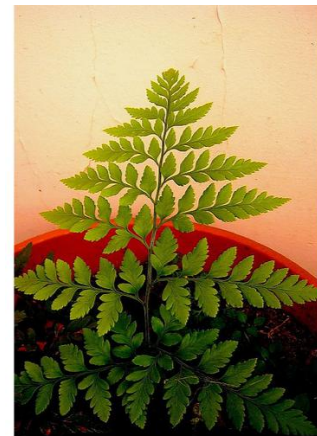


Fig. 3.6.7 Mediante simples ecuaciones se puede dibujar un helecho

El bosque

Un bosque, puede llegar a ser muy flexible y adaptable debido a su rica red de rizados retroalimentadores que interactúan con el medio constantemente. Algunos bosques, incluso, se han ajustado a cambios drásticos. Pero cuando este sistema caótico se desestabiliza (porque empezamos a talar bosques, por ejemplo), la conducta no lineal puede hacer que su dinámica



Fig. 3.6.8 El bosque es un sistema caótico

cambie abruptamente o que incluso se colapse. Ya tenemos el ejemplo de tierras sobre las que hace años hubo ricos bosques que creaban su propio microclima y ellos mismos hacían que las condiciones les fueran favorables, sin embargo, ahora no se puede plantar ni una sola planta ahí. Cortar un árbol puede significar que el bosque se quede con un árbol menos. Cortar diez árboles también. Pero cortar mil árboles puede no significar que el bosque se quede con mil menos, sino que a partir de ahí se extingan todos. Los procesos naturales de la Tierra son indivisibles y constituyen un holismo capaz de mantenerse y alimentarse, al menos que en el sistema caótico intervenga algún factor que lo desestabilice.

Vórtices

Cuando el agua hierve, el líquido del fondo asciende, y el de arriba baja, formándose una competición caótica. Se dice que el agua ejerce sus máximos *grados de libertad*. Se ha descubierto que al calentar el agua por debajo del punto de ebullición ésta se autoordena en un modelo de *vórtices* geométricos. Para suceder esto, primero se ha de llegar a un punto de bifurcación, que es donde el sistema se transforma. Cada uno de los vórtices este caso de forma hexagonal, Fig. 3.6.9) se enlaza a otras vórtices, así se amplifica el sistema, *retroalimentándose* a vórtice es "atractor extraño con pocos grados de libertad".

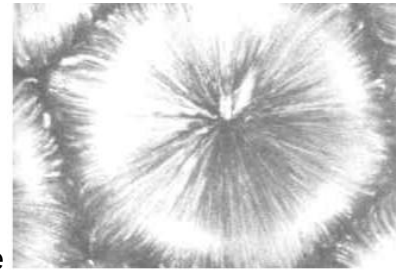


Fig. 3.6.9 Los vórtices presentan un autoordenamiento que entonces se forman (en fluctuaciones formando más sí mismo. Una definición de



Fig. 3.6.10 La retroalimentación en un sistema caótico

El sistema micrófono-altavoz

Otra fase de la retroalimentación consiste en la amplificación de los efectos. Ejemplo: cuando colocamos el micrófono demasiado cerca del altavoz: los pequeños sonidos ambientales son captados por el micro, salen amplificados por el altavoz, vuelven a ser captados por el micro y vuelven a salir todavía más amplificados.

Reacciones químicas Belousov-Zhabotinski

En la figura 3.6.11 se observa una simulación tridimensional de la reacción de Belousov-Zhabotinski. Las zonas más claras indican una mayor concentración de uno de los reactivos. Partiendo de una mezcla homogénea de sustancias químicas, el sistema se autoorganiza dando lugar a ondas macroscópicas, observables a simple vista, que surgen del comportamiento caótico molecular.

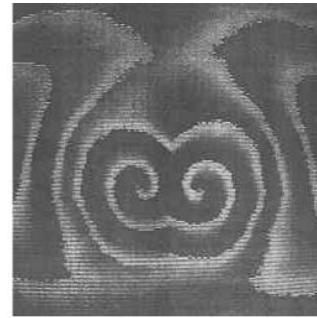


Fig. 3.6.11
Autoorganización al
mezclar reactivos

Las colonias de hormigas

Su comportamiento global sorprende, si contamos el número de individuos activos, a lo largo del tiempo, comprobaremos que el número fluctúa con una periodicidad de unos 25 minutos. Cada cierto tiempo ningún elemento está activo. Ese ciclo de actividad podría ser sólo un reflejo de sincronización, sin embargo la actividad individual es totalmente aperiódica, caótica, sin ningún tipo de regularidad intrínseca. Al aumentar el número de individuos aparece un comportamiento colectivo hasta que, para cierta densidad de hormigas, comienzan a aparecer oscilaciones regulares. Si artificialmente cambiamos la densidad de las hormigas la colonia redefine sus fronteras, para volver a la densidad



Fig. 3.6.12 La
autoorganización de las
colonias de hormigas

óptima para mantenerlas autoorganizadas. En esa densidad crítica el sistema se comporta como un todo, a medio camino entre el orden y el caos.

Los mercados financieros

Son entornos caóticos, donde pequeñas variaciones iniciales producen grandes cambios en los movimientos de los precios finales.

En este sentido, lo que interesa es conocer si existe algún atractor, es decir, si existen algunas pautas o fórmulas que nos permitan determinar el estado final al



Fig. 3.6.13 Los mercados
financieros son sistemas caóticos

que son atraídas las cotizaciones. En realidad todas las teorías de análisis (fundamental, chartismo, onda de Elliot), son los primeros pasos en la búsqueda de un atractor que permita conocer, con antelación, el estado final de las cotizaciones [8].

Más ejemplos de sistemas en los que puede aparecer un comportamiento caótico [11]

Otros ejemplos de sistemas caóticos incluyen la atmósfera terrestre, el Sistema Solar, las placas tectónicas, los fluidos en régimen turbulento y los crecimientos de población. Algunos otros sistemas que presentan comportamiento caótico son:

- ◆ Mecánica celeste (3 cuerpos)
- ◆ Fluidos
- ◆ Láseres y sistemas ópticos no lineales
- ◆ Sólidos
- ◆ Plasmas
- ◆ Aceleradores de partículas
- ◆ Reacciones químicas
- ◆ Dinámica de poblaciones
- ◆ Sistemas biológicos diversos
- ◆ Economía y sociología

El horizonte de las aplicaciones del caos

En el terreno de la biología y la medicina, la teoría del caos empieza a dar respuesta a problemas relacionados con la circulación sanguínea, introduciendo la idea de turbulencia como elemento que viene a romper la regularidad circulatoria y cardíaca. En el tratamiento de la epilepsia, las propuestas derivadas de esta concepción apuntan hacia el desarrollo de tratamientos que mediante la idea de la provocación del caos en determinadas zonas del cerebro generando turbulencias eléctricas en la actividad cerebral, pueden bloquear o impedir los ataques epilépticos.

Otro campo de interés para aplicar la teoría del caos es el de los fenómenos y procesos sociales. Así, el estudio del comportamiento errático, impredecible y caótico de la Bolsa, de los flujos financieros, así como el de los periodos de transición política, adquieren nuevas dimensiones para el análisis y la investigación económica, social y política

3.7 ANTECEDENTES HISTÓRICOS

Henry Poincaré

El problema de los tres cuerpos era más que nada astronómico: si se tienen dos cuerpos en el espacio, es fácil deducir las ecuaciones del movimiento: se moverán en elipses, por ejemplo. Pero si se tienen tres cuerpos, ya no hay manera de encontrar tales ecuaciones exactas, solamente aproximaciones válidas para un intervalo. Al salir de ese intervalo de validez, se deben hacer otras aproximaciones.



Fig. 3.7.1 Henry Poincaré

Henry Poincaré decidió atacar el problema de los tres cuerpos a finales del siglo XIX, con motivo de un concurso de Matemáticas organizado en Suecia. Al estudiarlo, encontró algo que le sorprendió: un sistema tan sencillo de plantear como el de los tres cuerpos podría dar un comportamiento extremadamente complicado, tanto que imposibilitaba hacer predicciones a largo plazo en el mismo.

Poincaré mismo lo expresa de esta manera:

*“Una pequeña causa que nos pasa desapercibida determina un considerable efecto que es imposible de ignorar, y entonces decimos que el efecto es debido al azar. Si conocemos exactamente las leyes de la Naturaleza y la situación del Universo en el momento inicial, podemos predecir exactamente la situación de este mismo Universo en un momento posterior. Pero aun si fuera el caso que las leyes de la Naturaleza no nos guardasen ningún secreto, todavía nosotros conoceríamos la situación inicial sólo **aproximadamente**. Si esto nos permitiera predecir la situación posterior con la **misma aproximación**, que es todo lo que necesitamos, podríamos afirmar que el fenómeno ha sido predicho, que es gobernado por leyes conocidas. Pero ésto no es siempre así; puede pasar que pequeñas diferencias en las condiciones iniciales produzcan grandes diferencias en el fenómeno final. Un pequeño error al principio produce un error enorme al final. La predicción se vuelve imposible, y tenemos un fenómeno fortuito”.*



Fig. 3.7.2 El problema de los 3 cuerpos fue atacado por Poincaré, haciendo así las primeras observaciones del caos.

Los físicos y demás científicos hicieron poco caso de este descubrimiento matemático (de hecho sólo los matemáticos continuaron trabajando en ello). Hasta el último cuarto del siglo XX donde, una vez apaciguada la llama de la Revolución de la Física, se observaron las consecuencias del descubrimiento de Poincaré y sobre todo por la ayuda de los ordenadores.

Edward Lorenz

El matemático Edward Lorenz usaba su ordenador Royal McBee para desentrañar la maraña matemática que él mismo había creado con sus doce ecuaciones para predecir el tiempo atmosférico en el Massachusetts Institute of Technology. Era el año 1960.

La predicción del tiempo se debía regir por ecuaciones, al igual que las órbitas de los planetas, satélites y galaxias, quizá más complicadas pero ecuaciones al fin y al cabo. Para ello escogió 12 funciones, unas establecían el vínculo entre velocidad y viento, otras entre presión y temperatura y así unas cuantas variables más. No le promovía un interés meramente físico sino también matemático.



Fig. 3.7.3 Edward Lorenz

Hojeando los rollos y rollos de papel con datos numéricos que escupía su impresora, Lorenz ideó un método para que el ordenador señalara cada minuto el paso de un día imprimiendo una hilera de números.

En 1961, Lorenz cansado de observar ese vaivén numérico salido de la impresora de su ordenador, intentó atajar partiendo de una sucesión anterior pero al traspasar los dígitos sólo tecleó 3 en vez de los 6 originales, esperando que el comportamiento no cambiara.

Los resultados obtenidos trajeron de cabeza a Lorenz pues no eran los esperados y revisó el software y hardware hasta darse cuenta finalmente, que el error lo cometió al truncar el valor inicial de la función cambiando el input de 0,506127 a 0,506.



Fig. 3.7.4 La dependencia sensitiva de las condiciones iniciales es una limitación fundamental comparable al Principio de Incertidumbre. En Caos tiene poco sentido la representación de orbitas en el espacio de fases. En la figura se pueden ver un atractor de Lorenz, pero ahora representado como orbital, es decir, ley de distribución de probabilidad.

Había dado con "el efecto mariposa". Este redondeo insignificante era el aleteo de la mariposa; y el comportamiento anómalo, o digamos inesperado, de la función del huracán que se produciría el próximo mes en Tokio.

A su descubrimiento lo llamó Lorenz "*Dependencia sensitiva de las condiciones iniciales*" (Fig. 3.7.4) y con ello creó la base de una nueva ciencia: el **Caos**.

Dependencia sensitiva de las condiciones iniciales significa que, partiendo de dos puntos del espacio de fases, las dos trayectorias correspondientes acaban por diverger, aunque los puntos en cuestión estén tan próximos como queramos. Estos dos puntos representan sendos conjuntos de condiciones iniciales, siendo las trayectorias la distinta evolución del sistema según sea el punto de partida.

Lorenz animado por su descubrimiento, decidió comenzar a experimentar con sus resultados en el campo de las corrientes de fluidos y sus 12 fórmulas se vieron reducidas a 3 simples ecuaciones no lineales. Lorenz representó gráficamente los resultados obtenidos con sus 3 ecuaciones en una gráfica tridimensional, asignando el valor obtenido de cada ecuación a una de las 3 dimensiones del plano euclídeo.

Al ver el gráfico resultante, llamado en adelante "*atractor de Lorenz*", Lorenz se encontró otra vez con el efecto mariposa, concretamente con sus alas.

La línea de la gráfica no se tocaba jamás, el desorden era total pues ningún punto se repetía ya que no había intersecciones, pero se vislumbró un nuevo tipo de "desorden ordenado": el caos.[3]

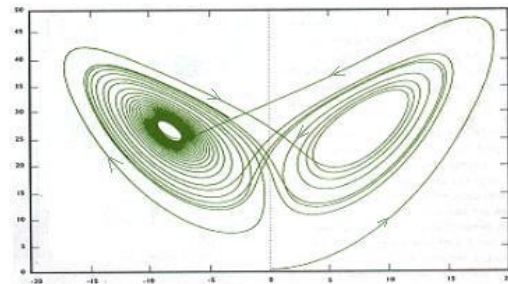


Fig. 3.7.5 Atractor de Lorenz es una figura geométrica similar a una mariposa

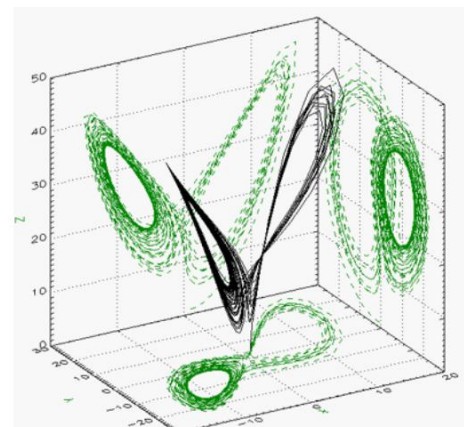


Fig. 3.7.6 Atractor de Lorenz en tres dimensiones

Ecuaciones de Lorenz

Edward Lorenz, utilizó el sistema de ecuaciones diferenciales de "Navier-Stokes" para modelar la evolución del estado de la atmósfera [5]:

$$\begin{aligned}\dot{x} &= \sigma(y - x) \\ \dot{y} &= rx - y - xz \\ \dot{z} &= xy - bz\end{aligned}$$

Donde:

x = razón de rotación del sistema

y = gradiente de temperatura

z = desviación de la temperatura respecto a su valor de equilibrio

σ = Número de Prandtl: [viscosidad] / [conductividad térmica]

r = número de Rayleigh (diferencia de temperatura entre la base y el tope del sistema) b = razón entre la longitud y altura del sistema

Lorenz observó dos cosas fundamentales que ocurrían en su ecuación:

- ✦ Cualquier diferencia en las condiciones iniciales antes de los cálculos, incluso infinitesimal, cambiaba de forma dramática los resultados.
- ✦ Tan sólo se podía predecir el sistema por cortos periodos de tiempo.

Llevando eso a la meteorología, suponía lo que se llamó efecto mariposa, hipersensibilidad a las condiciones iniciales.

A pesar de lo anterior lo impredecible del sistema, lejos de ser un comportamiento al azar, tenía una curiosa tendencia a evolucionar dentro de una zona muy concreta del espacio de fases, situando una especie de pseudocentro de gravedad de los comportamientos posibles.

Lorenz descubrió que su sistema contenía una dinámica extremadamente errática. Las soluciones oscilaban irregularmente sin llegar a repetirse, pero en una región acotada del espacio de fases. Vio que las trayectorias rondaban siempre alrededor de lo que ahora definimos como **atractor extraño**.

3.8 OBSERVACIONES

Siempre hemos estado obsesionados por el control, creemos que cuantas más técnicas creemos, más control tendremos sobre el mundo. Pero con cada tecnología nueva que introducimos se nos echan encima un montón de problemas, para cada uno de los cuales hemos de inventar nueva tecnología. Veamos el ejemplo del río: si tiramos una piedra el cauce no cambia, pero si tiramos una roca gigante la flexibilidad del sistema caótico no será suficiente. Es lo que ocurre en la Tierra: es un sistema caótico: siempre cambiante y adaptándose, pero si nos pasamos de la raya el sistema se puede romper. De hecho lo está haciendo y por eso tenemos problemas con la capa de ozono, el aumento de la temperatura global y el deshielo, problemas con los recursos como el petróleo, etc.

Aprender a vivir en el caos no significaría aprender a controlarlo, ni a predecirlo. Al contrario: hemos de enfocar la cuestión desde el punto de vista de que *nosotros también somos parte del caos*, no nos podemos considerar como elementos aparte. Desde esa perspectiva lo que podemos hacer es vivir de la creatividad del caos, sin intentar imponernos: si conseguimos realmente formar parte del sistema el concepto de sujeto y objeto desaparecerán, con lo cual el problema del control también.

3.9 REFERENCIAS

- [1] http://es.wikipedia.org/wiki/Caos_%28mitolog%C3%ADa%29
- [2] <http://usuarios.lycos.es/teoriacaos/>
- [3] <http://fractales.org/?q=node/63>
- [4] <http://www.iec.csic.es/gonzalo/caos/fracfaq.htm>
- [5] <http://www.geofisica.cl/English/pics5/FUM3.htm>
- [6] <http://www.didyf.unizar.es/info/jlsubias/IntrCaos.htm>
- [7] <http://platea.cnice.mecd.es/~jdelucas/teoriacaos.htm>
- [8] http://ciencias.huascaran.edu.pe/modulos/m_caos/actividad3.html
- [9] <http://www.astroseti.org/vernew.php?codigo=1256>
- [10] <http://www2.ing.puc.cl/~dcolle/publicaciones/caos/caos.htm>
- [11] <http://centros5.pntic.mec.es/ies.victoria.kent/Rincon-C/Curiosid/Rc-49/Rc-49.htm>

4.0 CIRCUITO DE CHUA

4.1 INTRODUCCIÓN

Desde que Pecora y Carroll reportaron el descubrimiento de la sincronización del caos en 1990, la sincronización de los sistemas caóticos ha recibido un gran interés entre los investigadores de diferentes campos de la ciencia. Una de las motivaciones para la sincronización es la posibilidad de enviar mensajes a través de sistemas caóticos para comunicaciones seguras. Tales sistemas sincronizados usualmente consisten en dos partes: Un generador de señales caóticas (sistema maestro) y un receptor (sistema esclavo). El sistema esclavo es a menudo un duplicado de una parte (o todo) del sistema maestro. Una señal caótica generada por el sistema maestro se puede utilizar como la entrada en el sistema esclavo para sincronizar las señales comunes de ambos sistemas. Después de la sincronización, mediante una modulación adecuada de la dinámica de transmisión caótica, el mensaje privado se oculta y envía a la dinámica del receptor. Bajo ciertas condiciones, uno puede recuperar el mensaje original al final del receptor. Diferentes aproximaciones para la construcción de sistemas caóticos son propuestas y se les está dando seguimiento. Sin embargo, la mayoría de los métodos son complicados y a menudo se dificulta su implementación electrónica.

El encriptado de datos empleando dinámica caótica se reporto en los años 90's como una nueva forma para el codificado de información que difiere de los métodos convencionales que emplean algoritmos numéricos como clave de encriptado. Por ello, la sincronización del caos juega un rol importante en las comunicaciones caóticas. En particular, varias técnicas, como son enmascaramiento caótico aditivo, conmutación caótica, modulación caótica de parámetros han sido elaboradas.

Para que pueda existir caos en un circuito eléctrico (sin entradas) construido con resistencias, inductores y capacitores, este debe contener:

- ⊕ Al menos un elemento no lineal
- ⊕ Mínimo un resistor localmente activo
- ⊕ Al menos tres elementos almacenadores de energía.

El circuito de Chua, mostrado en la figura 4.1.1, es el circuito eléctrico más simple que satisface este criterio.

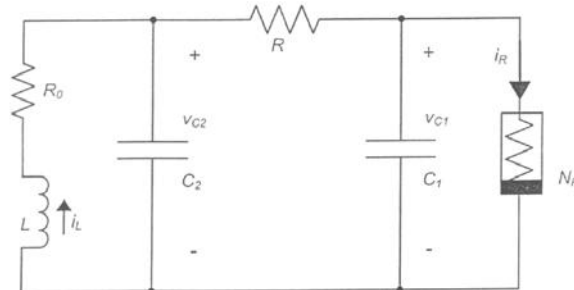


Fig. 4.1.1 Circuito de Chua, contiene un inductor L , dos capacitares C_1 y C_2 , una resistencia R , la resistencia interna del inductor R_0 y un resistor no lineal N_R (diodo chua)

4.2 GENERADOR CAÓTICO

En los sistemas de comunicación privada, emplearemos el circuito de Chua como generador caótico. El circuito de Chua es uno de los sistemas físicos para el cual la presencia de caos ha sido establecida experimentalmente, confirmada numéricamente y probada matemáticamente. Escogimos este circuito para nuestro estudio por el hecho de que ha sido investigado a fondo en la literatura y es de fácil implementación electrónica.

El circuito de Chua consta de solo cuatro elementos lineales (un resistor R , un inductor L , dos capacitares C_1 y C_2) y un elemento no lineal (el llamado diodo de Chua N_R). El circuito de Chua se muestra en la figura 4.2.1

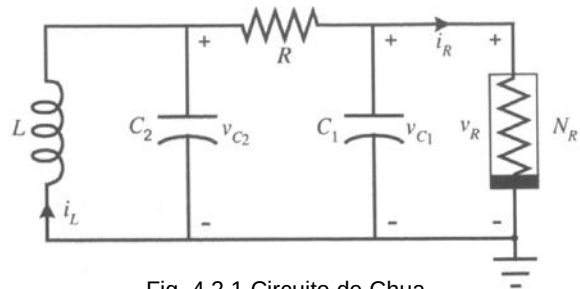


Fig. 4.2.1 Circuito de Chua

La resistencia no lineal N_R , también llamada diodo Chua, tiene una característica $v-i$ que es lineal por secciones, como se observa en la figura 4.2.2. Las tres zonas lineales confirman una función no lineal suave.

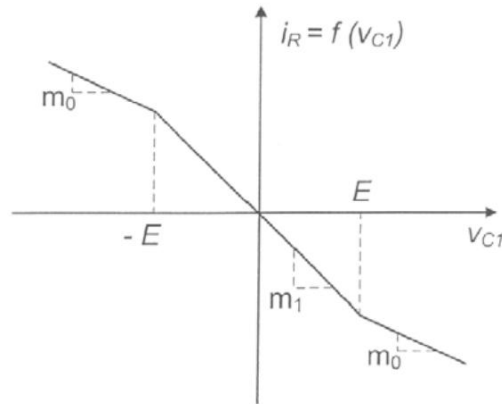


Fig. 4.2.2 Característica v-i de tres segmentos lineales de la resistencia no lineal N_R del circuito de Chua. Las regiones externas tienen pendiente m_0 ; la región interna tiene pendiente m_1 . Los puntos de quiebre se encuentran dados por $\pm E$

Empleando análisis de redes, se reducen las ecuaciones de estado, que modelan el comportamiento dinámico del circuito Chua:

$$\begin{aligned} \frac{dv_{C1}}{dt} &= \frac{1}{RC_1} (v_{C2} - v_{C1}) - \frac{1}{C_1} f(v_{C1}) \\ \frac{dv_{C2}}{dt} &= \frac{1}{RC_2} (v_{C1} - v_{C2}) - \frac{1}{C_2} i \\ \frac{di_L}{dt} &= -\frac{1}{L} v_{C2} - \frac{R_{OL}}{L} \end{aligned} \quad (1)$$

Donde:

$$f(v_{C1}) = m_1 v_{C1} + \frac{1}{2} (m_0 - m_1) (|v_{C1} + E| - |v_{C1} - E|) \quad (2)$$

Es la característica v-i del diodo Chua, donde m_0 es la pendiente de las regiones externas y m_1 es la pendiente del segmento interior. $\pm E$ es el voltaje del punto de quiebre en la curva de los segmentos lineales mostrada en la figura 4.2.2.

Modelo normalizado

Para realizar el análisis dinámico del circuito de Chua, en cualquiera de sus versiones, es de gran utilidad trabajar con un modelo matemático que tenga menor número de parámetros y al mismo tiempo, que describa la misma dinámica de los circuitos de Chua. Para este propósito, es posible transformar (1) y (2) en un conjunto de ecuaciones adimensionales (normalizadas) mediante el siguiente cambio de variables:

$$\begin{aligned}
 x_1 &= \frac{V_{C1}}{E} \\
 x_2 &= \frac{V_{C2}}{E} \\
 x_3 &= i \frac{R}{L} \\
 \gamma &= \frac{RC}{C} \frac{R}{L} \\
 \alpha &= \frac{C}{C_1} \frac{L}{R} \\
 \beta &= \frac{C_1}{R} \frac{L}{C} \\
 a &= Rm_0 \\
 b &= Rm_1
 \end{aligned}$$

Donde E representa el voltaje de ruptura de la parte no lineal del diodo Chua, el cual, se fijara en 1 para el resto del documento. Así, las ecuaciones adimensionales o normalizadas del circuito de Chua son:

$$\begin{aligned}
 \dot{x}_1 &= \alpha (x_2 - x_1 - f(x_1)) \\
 \dot{x}_2 &= x_1 - x_2 + x_3 \\
 \dot{x}_3 &= -\beta x_2 - \gamma x_3
 \end{aligned} \tag{3}$$

Donde $f(x_1)$ es la función no lineal y está definida por:

$$f(x_1) = b x_1 + \frac{1}{2}(a - b)(|x_1 + 1| - |x_1 - 1|) \tag{4}$$

4.3 SIMULACIÓN DEL CIRCUITO DE CHUA MEDIANTE EL PROGRAMA SIMNON VER. 1.0.

Para observar el comportamiento dinámico del circuito de Chua, se realizaron simulaciones numéricas, utilizando el modelo normalizado con valores de los parámetros:

$$\begin{aligned}
 a &= -87 \\
 b &= -7.5
 \end{aligned}$$

Y condiciones iniciales:

$$\begin{aligned}
 x_1 &= 0.1 \\
 x_2 &= 0.02 \\
 x_3 &= 0
 \end{aligned}$$

Estos valores aseguran la existencia de oscilaciones caóticas.

Simulación del circuito de Chua mediante el programa SIMNON ver. 1.0.

El programa elaborado en el programa SIMNOM se muestra a continuación:

CONTINUOUS SYSTEM

CHUA " Version: 1.0

" Abstract: w

" Description:

" Revision: 1.0

" Author: DelFin

" Created: 13/07/2006

" States, derivates and

time: STATE x y z

DER dx dy

dz TIME t

" Initializations:

x:0.1

y:0.02

z:0

" Equations: $f = b \cdot x + (1/2) \cdot (a -$

$b) \cdot (\text{ABS}(x+1) - \text{ABS}(x-1))$ $dx = \text{alfa} \cdot (y - x - f)$

$dy = x - y + z$

$dz = -\text{beta} \cdot y$

" Parameter

values: $a = -8/7$

$b = -5/7$

$\text{alfa} = 10$

$\text{beta} = 12.013$

END

Alfa y Beta (α , β) son los parámetros críticos, al mover este valor, varía el comportamiento del sistema.

Resultados obtenidos en la simulación numérica

1. Para los valores de parámetros en los que se tiene $\alpha=9$, $\beta=14.87$, $a=-8/7$, y $b=-5/7$ todos los puntos fijos son hiperbólicos. El flujo linealizado alrededor del origen tiene un valor propio real positivo, y un par de valores propios complejos conjugados con partes reales negativas.

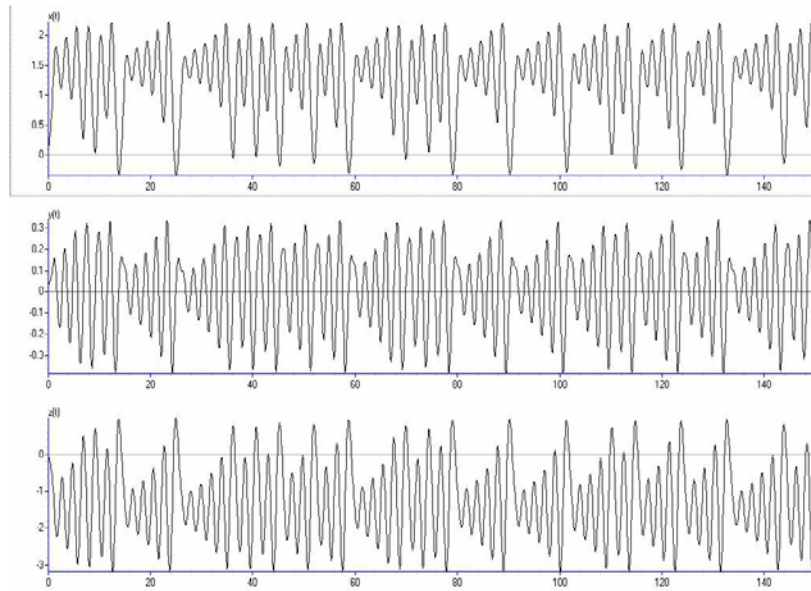


Fig. 4.3.1 Evolución temporal de x_1 x_2 x_3 para valores de $\alpha = 9$ y $\beta = 14.87$

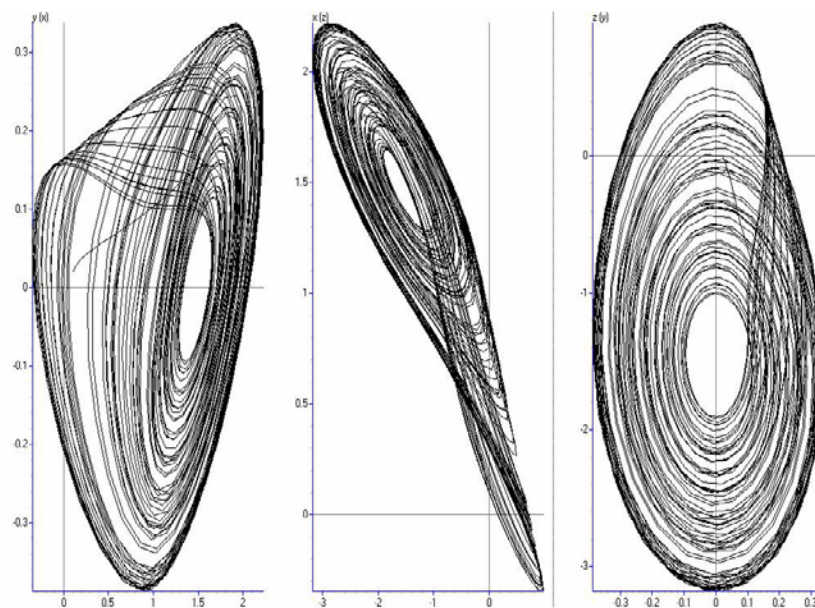


Fig. 4.3.2 Retrato de fase para $\alpha = 9$ y $\beta = 14.87$

2. Bifurcaciones con **periodo 1**, tomamos los valores de $\alpha = 8.8$ y $\beta = 16$.

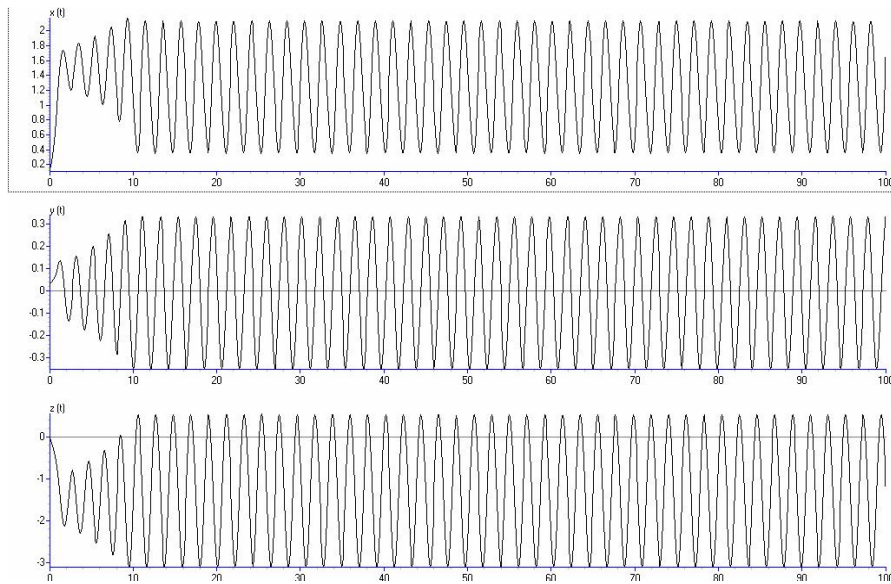


Fig. 4.3.3 Evolución temporal de x_1 x_2 x_3 para los valores de $\alpha = 8.8$ y $\beta = 16$

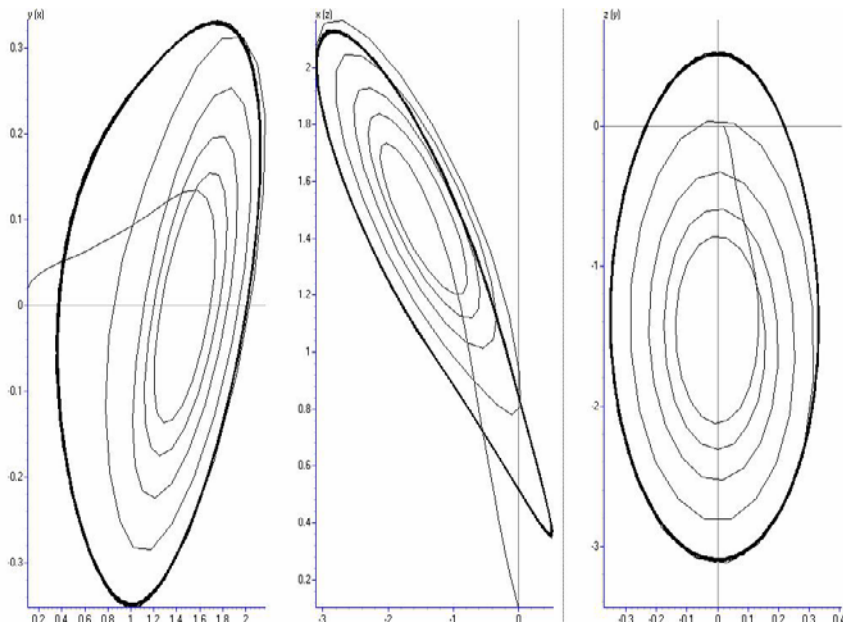


Fig. 4.3.4 Retrato de fase para los valores $\alpha = 8.8$ y $\beta = 16$

3. Bifurcaciones de **dos periodos** para los valores de $\alpha = 8.86$ y $\beta = 16$

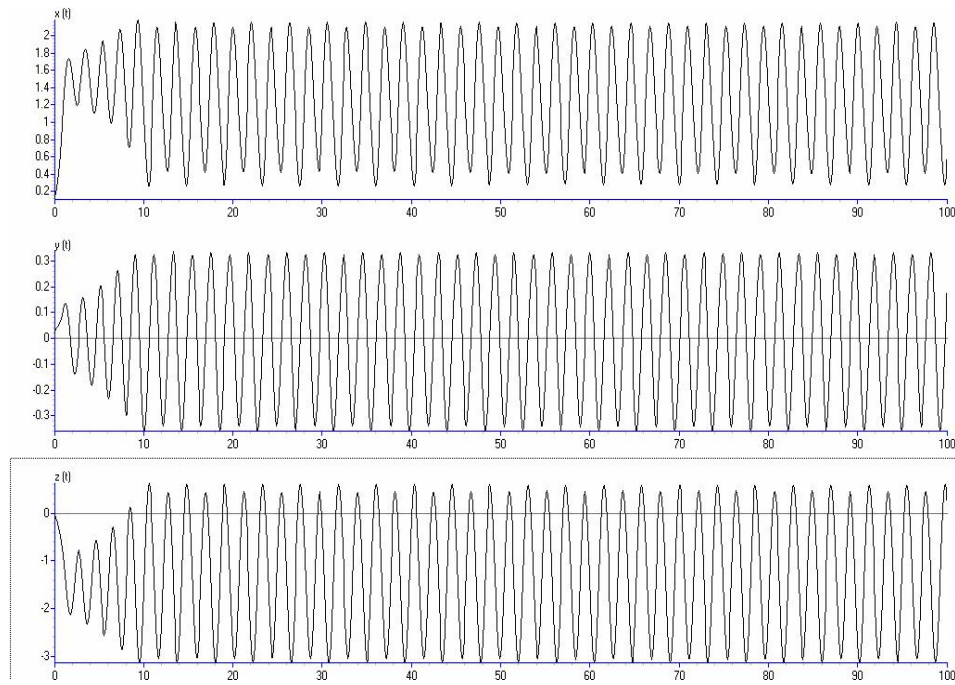


Fig. 4.3.5 Evolución temporal de x_1 x_2 x_3 para los valores de $\alpha = 8.86$ y $\beta = 16$

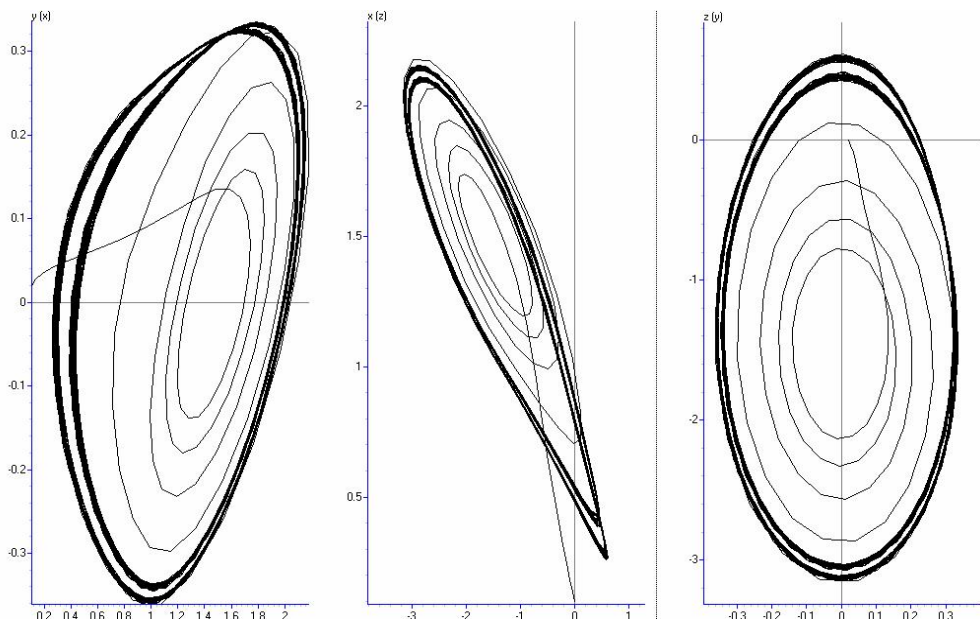


Fig. 4.3.6 Retrato de fase para los valores de $\alpha = 8.86$ y $\beta = 16$

4. Bifurcación de 4 periodos para los valores de $\alpha = 9.12$ y $\beta = 16$

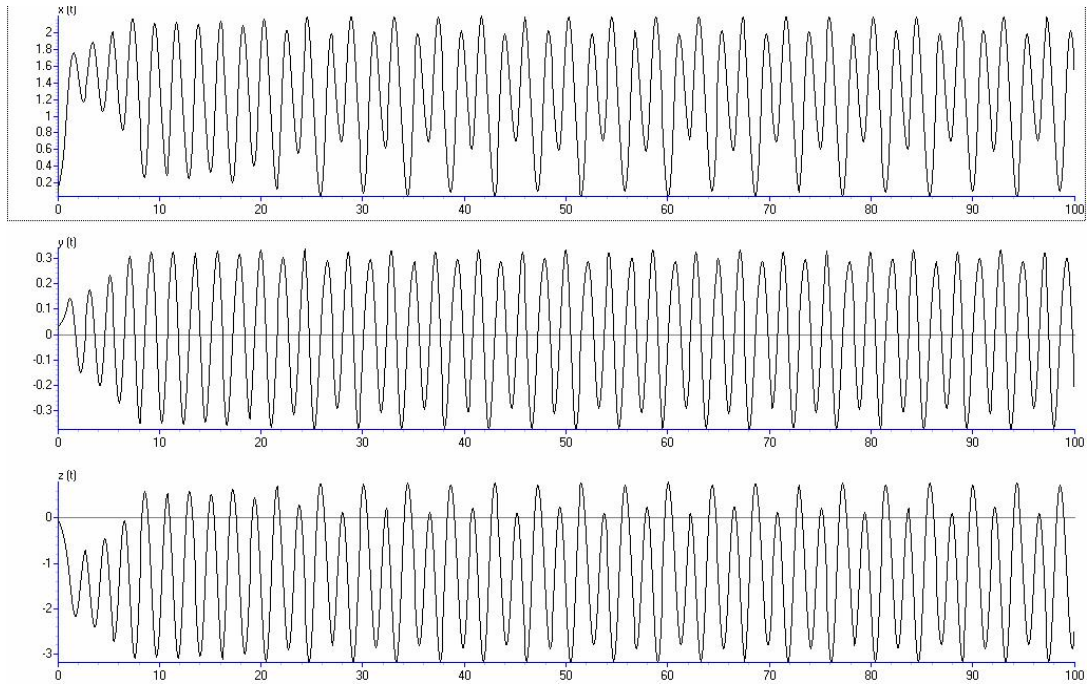


Fig. 4.3.7 Evolución temporal de x_1 x_2 x_3 para los valores de $\alpha = 9.12$ y $\beta = 16$

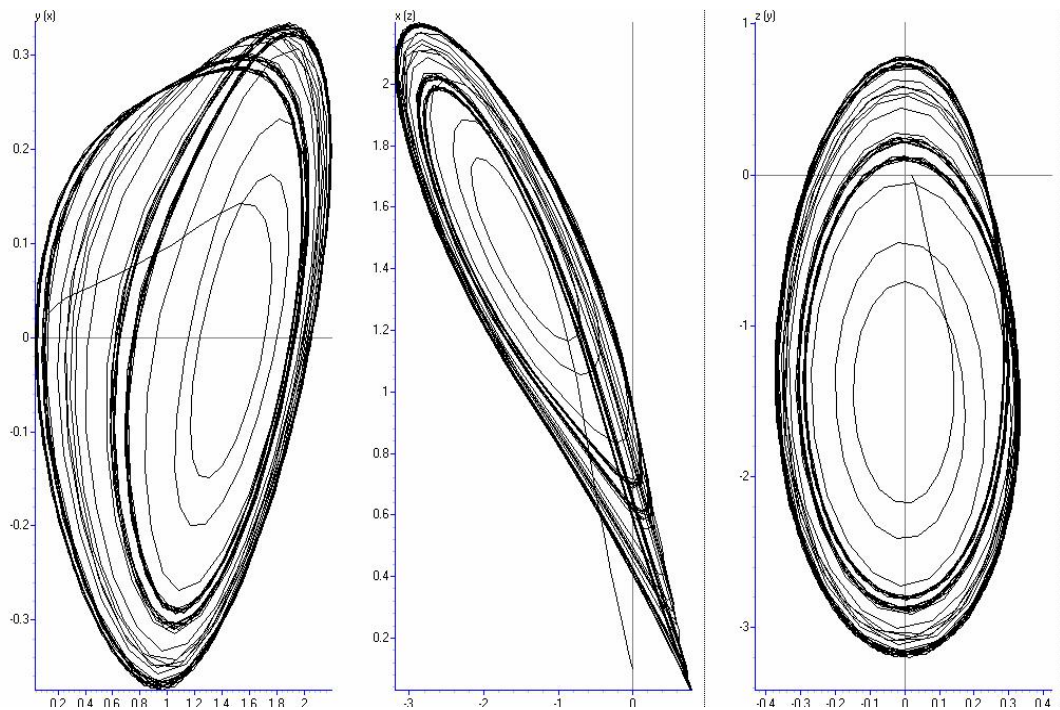


Fig. 4.3.8 Retrato de fase para los valores de $\alpha = 9.12$ y $\beta = 16$

5. Atractor de **espiral caótico** para los valores de $\alpha = 9.4$ y $\beta = 16$

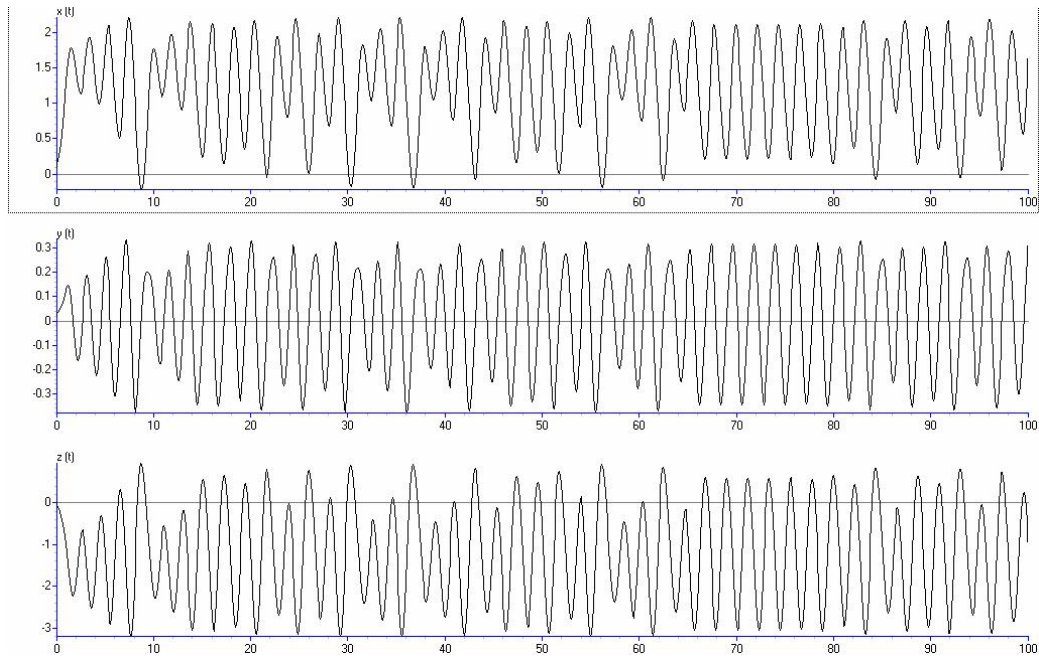


Fig. 4.3.9 Evolución temporal de x_1 x_2 x_3 para los valores de $\alpha = 9.4$ y $\beta = 16$

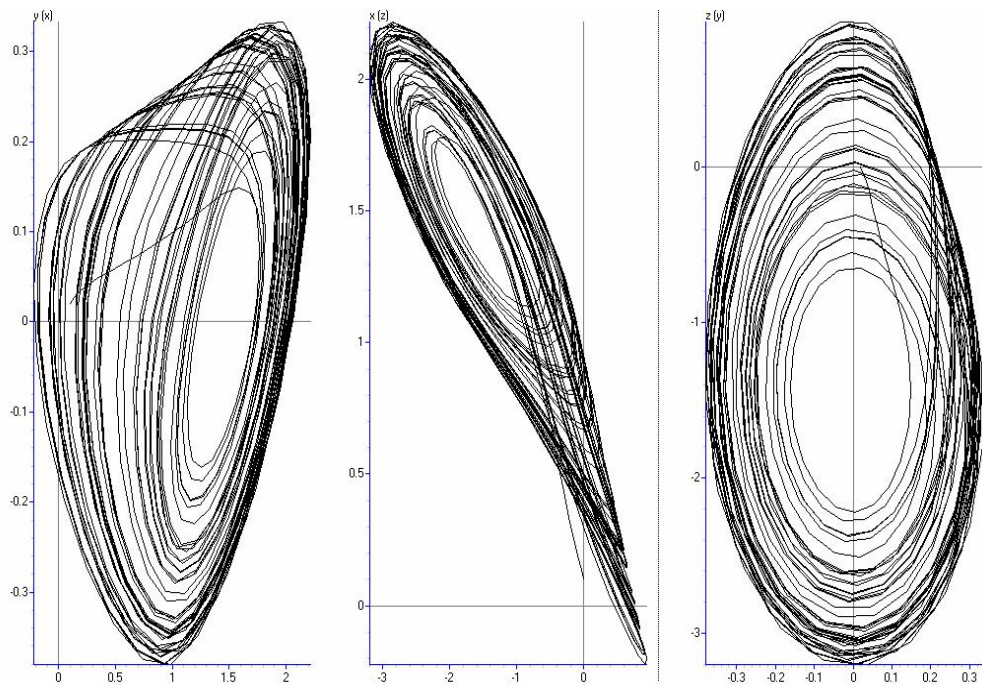


Fig. 4.3.10 Retrato de fase para los valores de $\alpha = 9.4$ y $\beta = 16$

6. Intermitencia presentada en el Circuito Chua para los valores de $\alpha = 4.295$ y $\beta = 5$

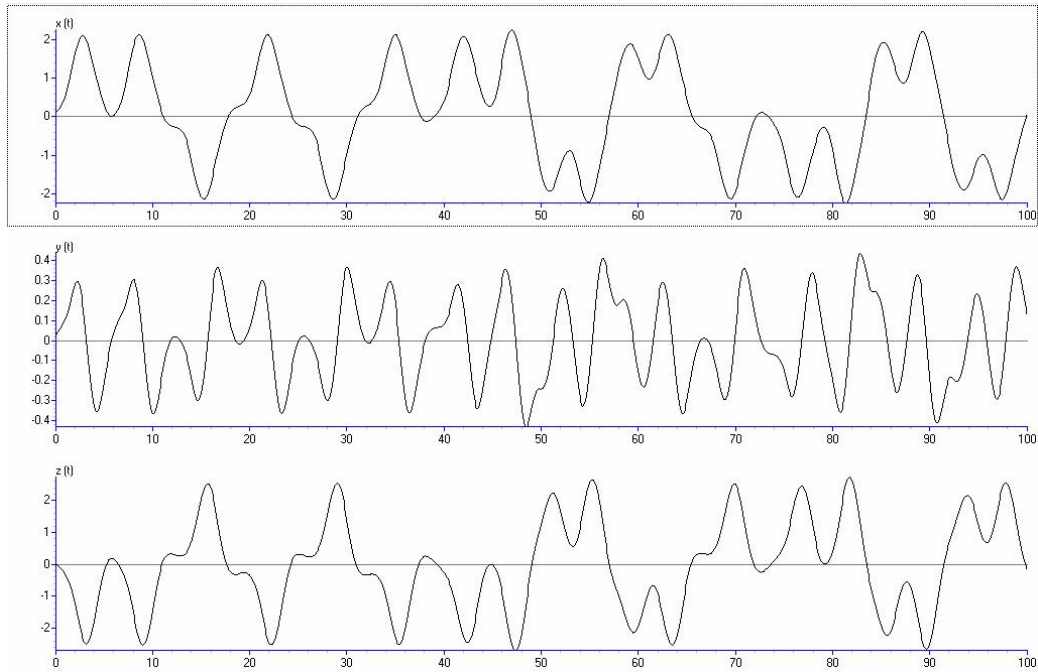


Fig. 4.3.11 Evolución temporal de x_1 x_2 x_3 para los valores de $\alpha = 4.295$ y $\beta = 5$

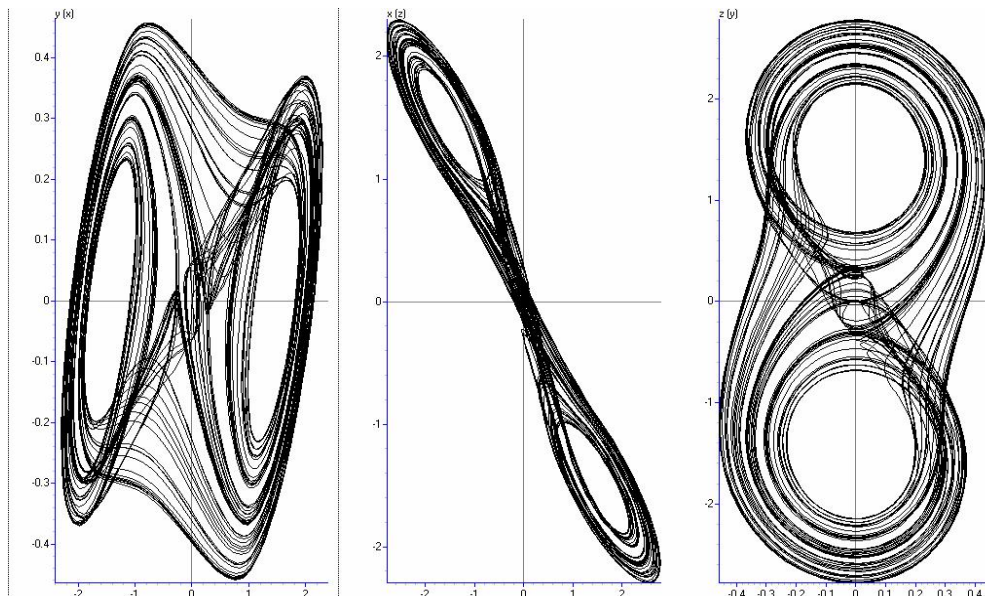


Fig. 4.3.12 Retrato de fase para los valores de $\alpha = 4.295$ y $\beta = 5$

7. Circuito de Chua generando un atractor caótico llamado **doble scroll**, para los valores de $\alpha = 10$ y $\beta = 14.87$

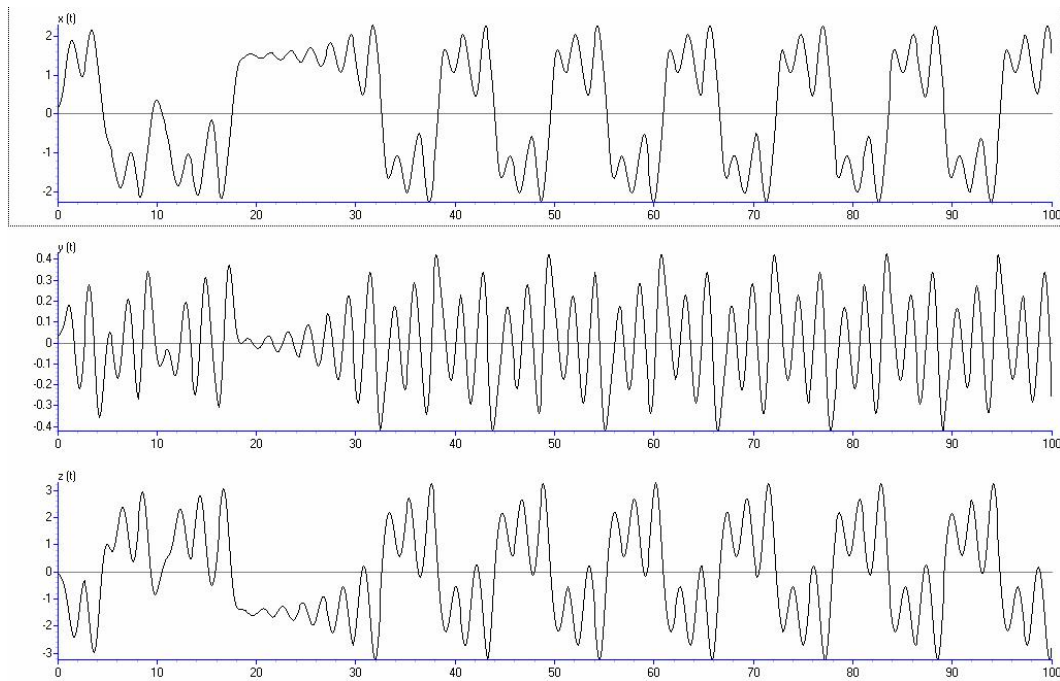


Fig. 4.3.13 Evolución temporal de los estados x_1 x_2 x_3 para los valores de $\alpha = 10$ y $\beta = 14.87$

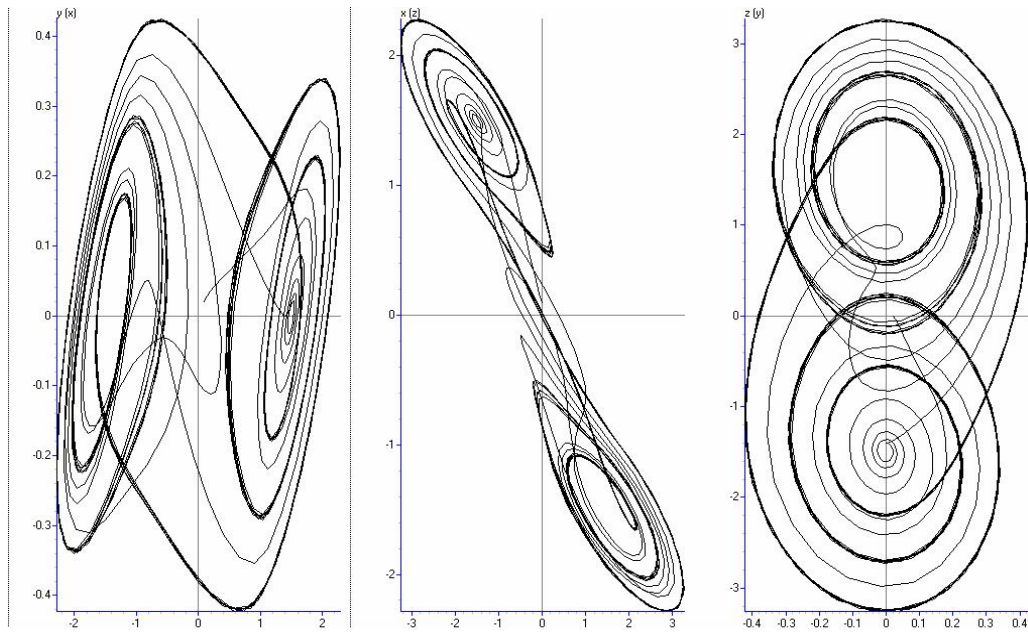


Fig. 4.3.14 Retrato de fase para los valores de $\alpha = 10$ y $\beta = 14.87$

En la figura 4.3.11 se muestra la evolución en el tiempo de los estados del circuito de Chua. Al observar la amplitud de la señal con respecto al tiempo, se puede apreciar la primera característica que presenta un sistema caótico; la forma de onda que exhibe no muestra ningún patrón o periodicidad visible, al menos en el tiempo de simulación empleado, que fue suficientemente grande. La siguiente característica, son los atractores extraños formados por las trayectorias caóticas de estos estados, los cuales se ilustran en la figura 4.3.12.

Es de gran provecho emplear técnicas de análisis de señales para determinar el comportamiento dinámico de los estados de un sistema caótico. La función de autocorrelación manifiesta en el tiempo, que tan parecida es una señal a si misma, es decir, cuantas componentes periódicas la constituyen. Para este caso, la señal que presente la autocorrelación más pequeña, indicará la que tiene mayor dinámica caótica.

4.4 IMPLEMENTACIÓN FÍSICA Y RESULTADOS EXPERIMENTALES DEL CIRCUITO DE CHUA.

El método más robusto y económico para realizar un circuito experimental de Chua se muestra en la figura 4.4.1. En esta estructura, la resistencia no lineal N_R llamada diodo de Chua, es implementada con dos amplificadores operacionales y seis resistencias lineales. Debido a su bajo costo y sencillez, el circuito de Chua se ha convertido en una opción para aplicaciones de señales caóticas donde se requiere el bajo costo y sencillez.

El circuito de Chua se puede realizar en una gran variedad de formas utilizando componentes electrónicos estándar o especiales. Dado que los elementos lineales (capacitores, resistencias e inductores) están disponibles como elementos de dos terminales, nuestro principal interés es con el circuito para construir el resistor no lineal N_R .

El objetivo es la construcción de un elemento resistivo de dos terminales con tres segmentos lineales en característica v-i como se muestra en la figura 4.2.2. Esto se puede hacer con el subcircuito etiquetado N_R de la figura 4.4.1. El resistor no lineal se forma por dos amplificadores operacionales U1A y U1B (con fuentes de alimentación de $\pm 12V$) y seis resistores lineales. El punto sobresaliente de la característica de v-i es que presenta tres regiones de pendiente negativa. Los puntos de inflexión entre las regiones lineales son proporcionales a los niveles de saturación de los op-amps. La figura muestra una implementación práctica de un circuito de chua utilizando un MC34084P de Analog Device, fuentes de alimentación de $\pm 12V$ y seis resistencias lineales para implementar la resistencia negativa N_R .

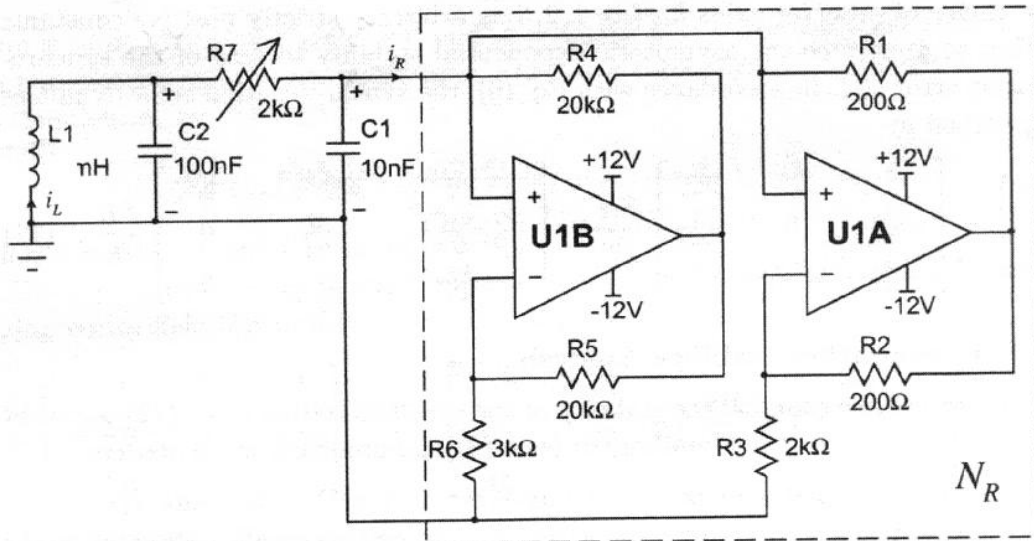


Fig. 4.4.1 Implementación electrónica del circuito de Chua

Las pendientes del resultado de la característica v-i se da por:

$$m_0 = -\frac{R_2}{R_1 R_3} + \frac{1}{R_4}$$

$$m_0 = -0.5 \frac{mA}{V}$$

$$m_1 = -\frac{R}{R_1 R_3} - \frac{R}{R_4 R_6}$$

$$m_1 = -0.833 \frac{mA}{V}$$

Los puntos de quiebre se determinan por los voltajes de saturación E_{sat} de los op-amps:

$$\pm B_P \approx 1.46V \text{ cuando } R_5 + R_6$$

$$, E_{sat} \approx 11.2V$$

Elementos utilizados para la construcción de dos circuitos de Chua.

- f 1 CI Amplificador Operacional TL084
- f 2 Bobinas de 18 mH
- f 2 Capacitores de 100 nF y 2 de 10 nF
- f 4 Resistencias de 220 Ω
- f 4 Resistencias de 2.2 k Ω
- f 4 Resistencias de 22 k Ω
- f 2 Resistencias de 3.3 k Ω
- f 2 Resistencias de 1.5 k Ω
- f 2 Potenciómetros de 500 Ω

Instrumentos que se utilizaron para la medición del circuito

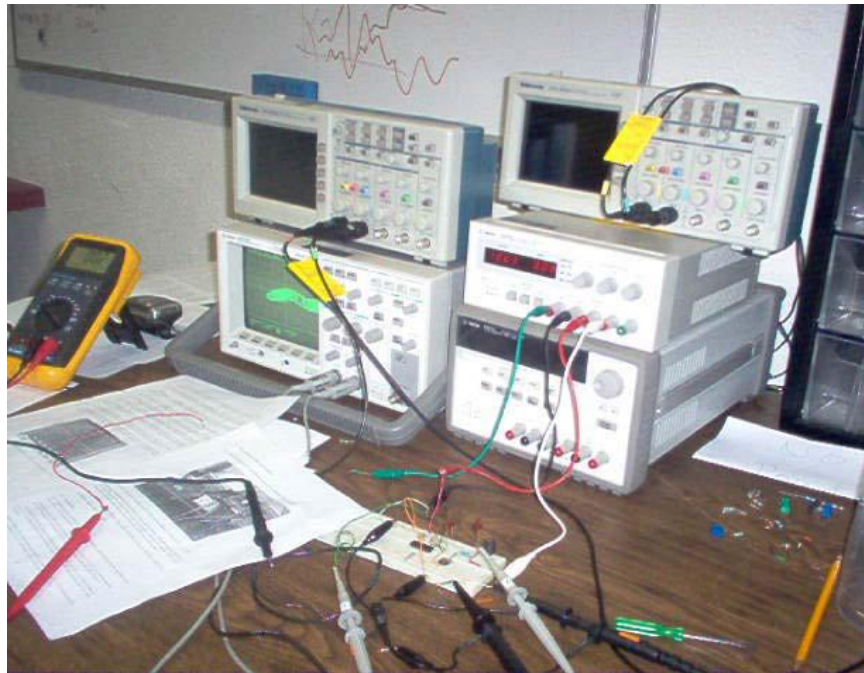


Fig. 4.4.2 Equipo empleado en la medición del circuito de Chua

- f **Osciloscopio AGILENT 54615B** de 500 MHz. Cuenta con dos canales, ancho de banda de 500 MHz $\pm$ 3 dB, Rango Dinámico $\pm$ 12 divisiones desde el centro de la pantalla resistencia de entrada 1 M Ω o 50 Ω , Capacitancia de entrada de 9 pF, Máxima entrada de voltaje de 250 V.
- f **Fuente de poder AGILENT E3630A**. Triple salida de corriente directa (0 – 6V, 2.5 A y $\pm$ 0.5 A)
- f **Multimetro digital WAVETEK 235**.

Resultados

A continuación se muestran los resultados experimentales que se obtuvieron en las mediciones que se hicieron al circuito que representa las ecuaciones de Chua. En estos resultados se muestra la dinámica que puede presentar el circuito de Chua antes de convertirse en caótico.

CIRCUITO CHUA

El circuito de Chua que se construyó se muestra en la figura 4.4.3, en este circuito $x_1(t)$ representa el voltaje del capacitor C1 mientras que $x_2(t)$ representa el voltaje en el capacitor C2.

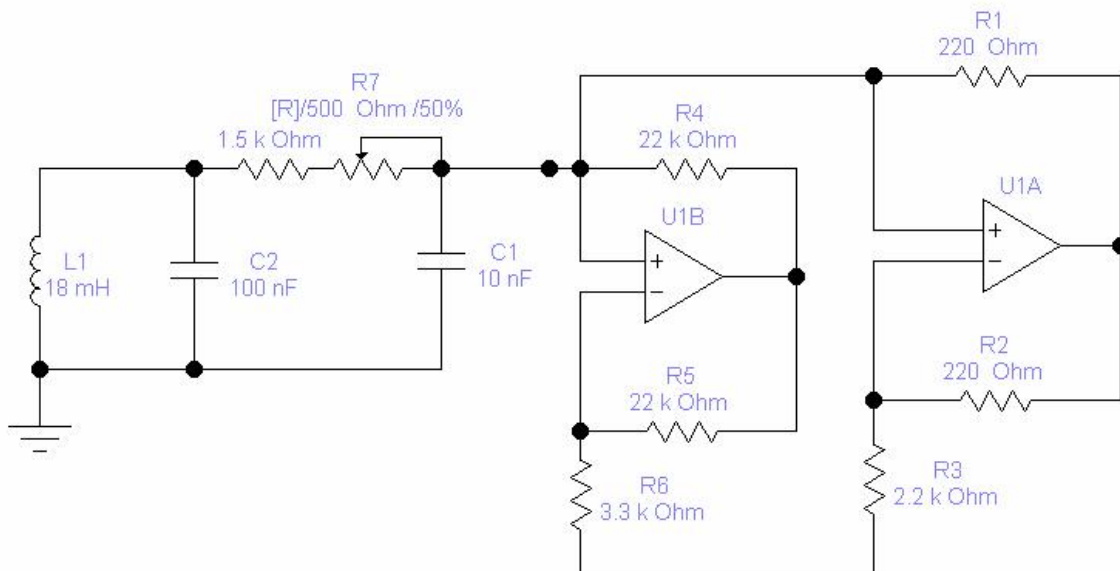


Fig. 4.4.3 Diagrama esquemático del circuito de Chua

1. En la figura 4.4.4 se muestra la grafica de x_1 contra el tiempo, en la figura 4.4.5 la grafica de x_2 contra el tiempo y en la figura 4.4.6 se muestra la bifurcación con *periodo 1*, con valores de $\alpha = 8.8$ y $\beta = 16$.

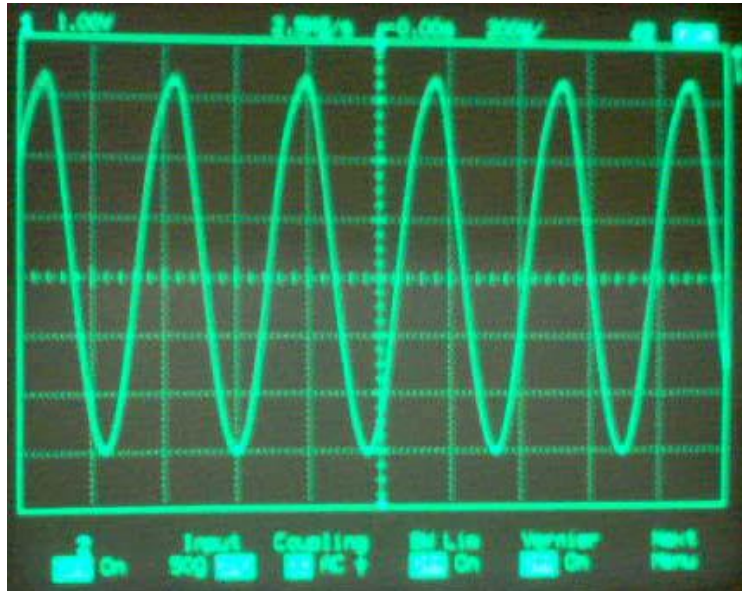


Fig. 4.4.4. Gráfica de $x_1(t)$

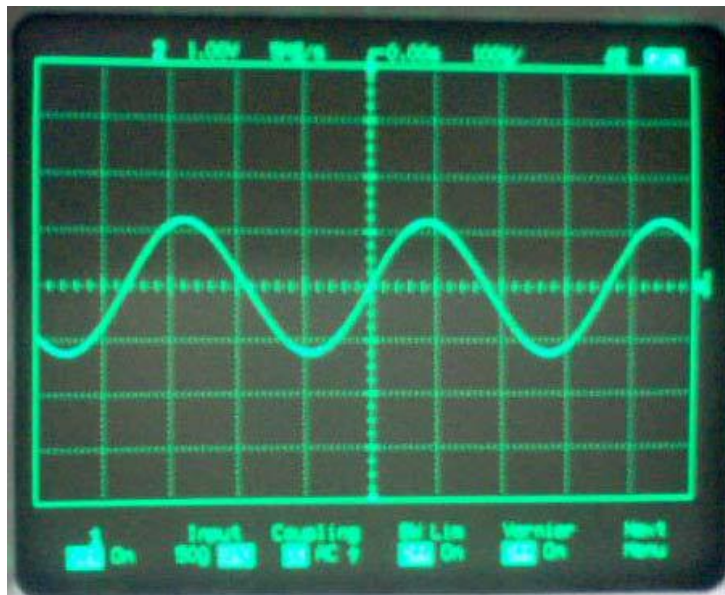


Fig. 4.4.5. Gráfica de $x_2(t)$

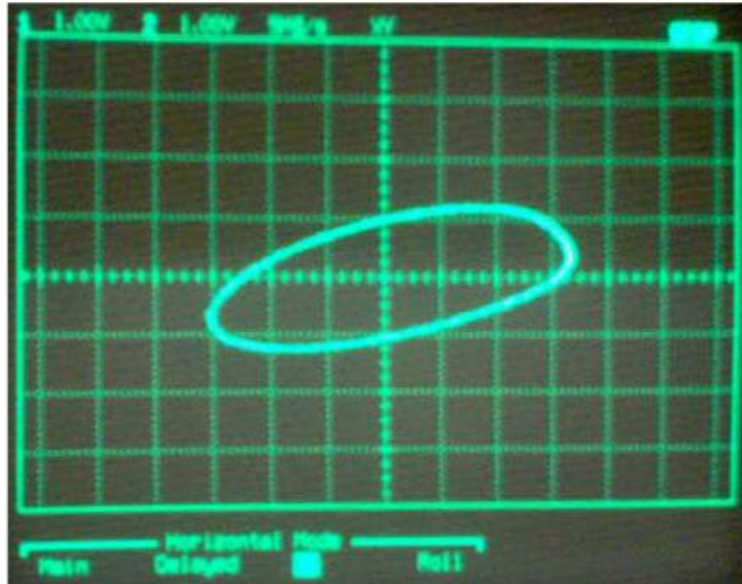


Fig. 4.4.6. Gráfica de periodo uno $x_1(t)$ vs $x_2(t)$

2. En la figura 4.4.7 se muestra la grafica de x_1 contra el tiempo, en la figura 4.4.8 se muestra x_2 y en la figura 4.4.9 se muestra la bifurcación con 2 *periodos*, con valores de $\alpha = 8.86$ y $\beta = 16$.

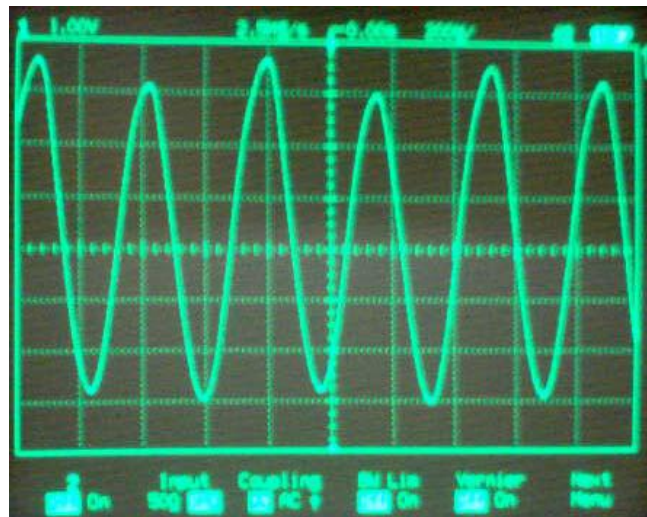


Fig. 4.4.7. Gráfica de $x_1(t)$

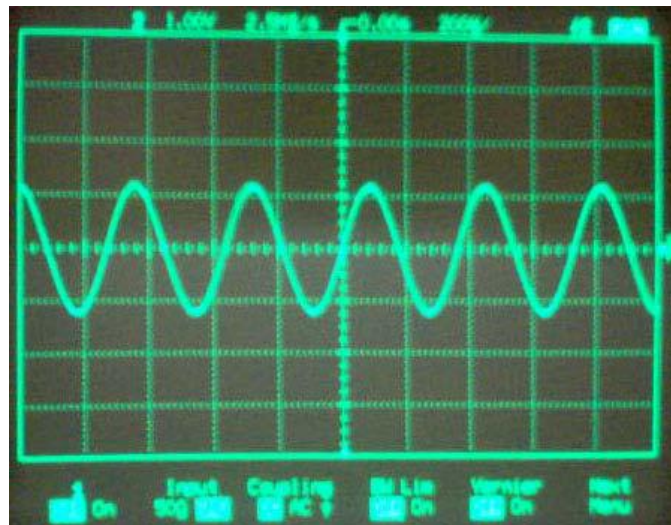


Fig. 4.4.8. Gráfica de $x_2(t)$

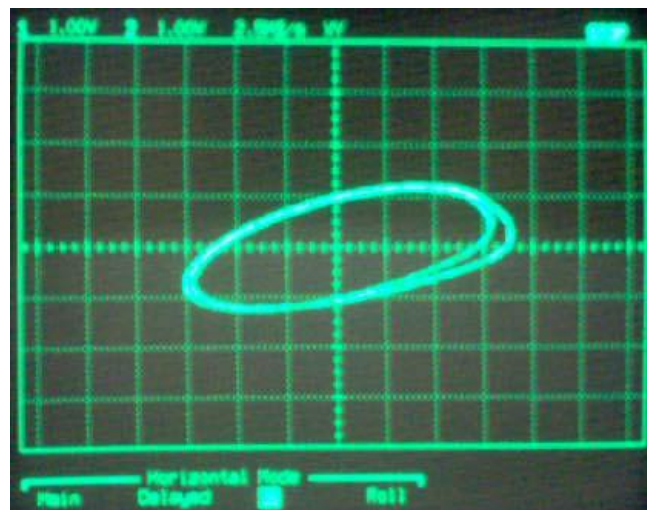


Fig. 4.4.9. Gráfica de dos periodos $x_1(t)$ vs $x_2(t)$

3. En la figura 4.4.10 se muestra un atractor de espiral caótico para los valores de $\alpha = 9.4$ y $\beta = 16$.

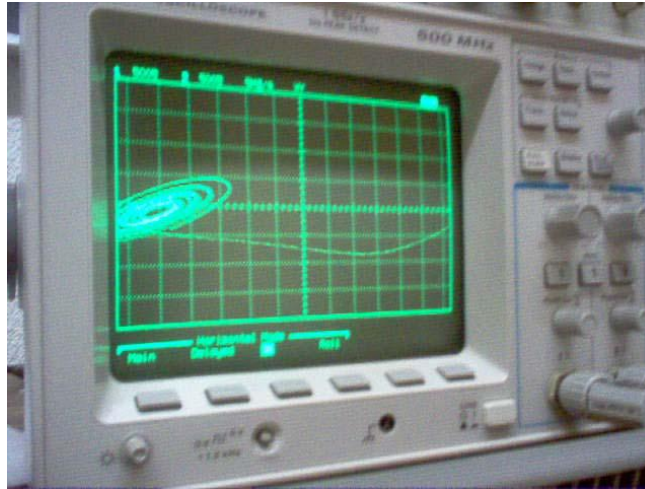


Fig. 4.4.10. Gráfica de espiral caótico $x_1(t)$ vs $x_2(t)$

4. En la figura 4.4.11 se muestran las señales de x_1 y x_2 las cuales graficadas en el plano XY muestran un atractor donde todos los puntos fijos son hiperbólicos como se ve en la figura 4.4.12, para los valores de parámetros en los que se tiene $\alpha=9$, $\beta=14.87$, $a=-8/7$, y $b=-5/7$.



Fig. 4.4.11. Gráficas de $x_1(t)$ vs $x_2(t)$

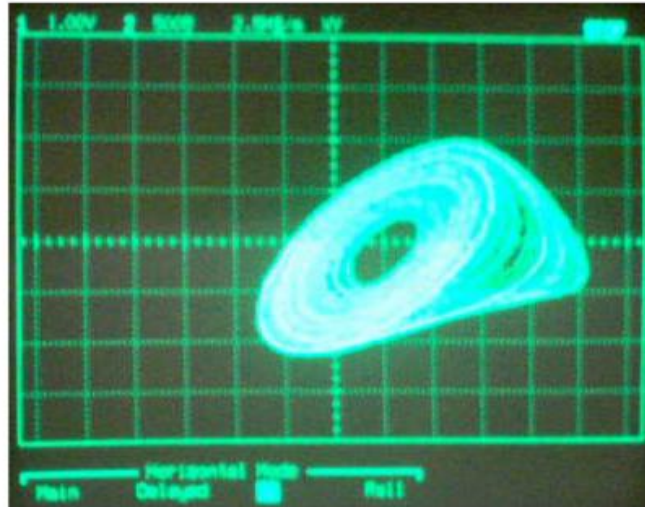


Fig. 4.4.12. Atractor con puntos fijos hiperbólicos

5. En la figura 4.4.13 se muestra la intermitencia presentada en el Circuito Chua para los valores de $\alpha = 4.295$ y $\beta = 5$ que se muestra en la simulación.

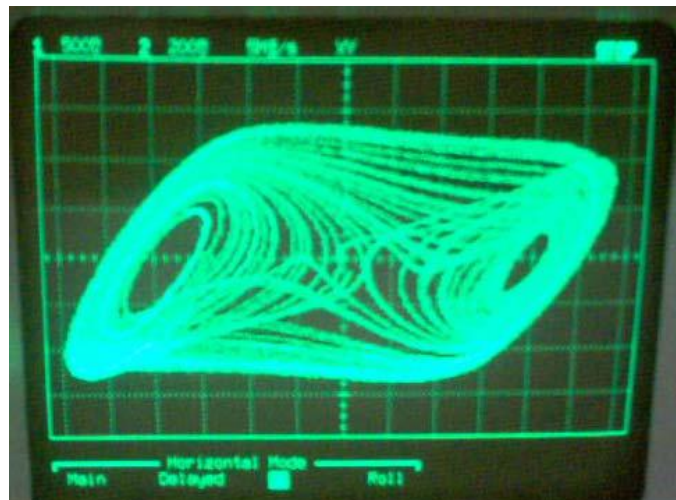


Fig. 4.4.13. Gráfica de intermitencia $x_1(t)$ vs $x_2(t)$

6. Finalmente en la figura 4.4.14 se muestra el Circuito de Chua operando como un doble atractor (scroll) caótico para los valores de $\alpha = 10$ y $\beta = 14.87$. En las figuras 4.4.15 y 4.4.16 se muestran las señales de x_1 y x_2 .

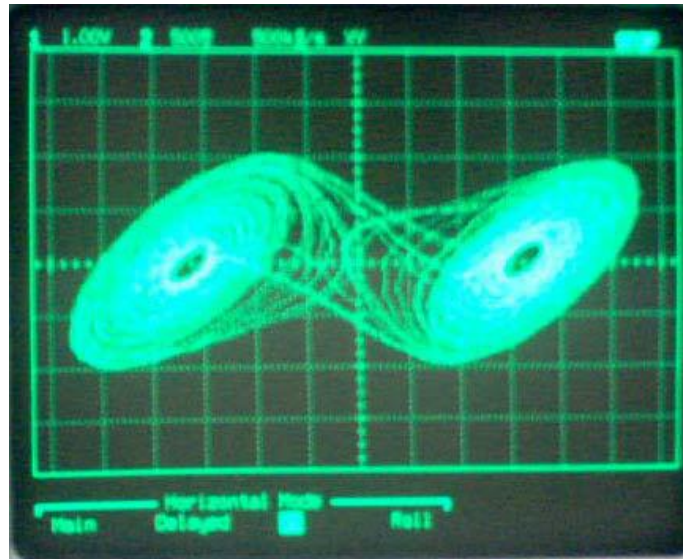


Fig. 4.4.14. Gráfica del doble scroll



Fig. 4.4.15. Gráfica de $x_1(t)$

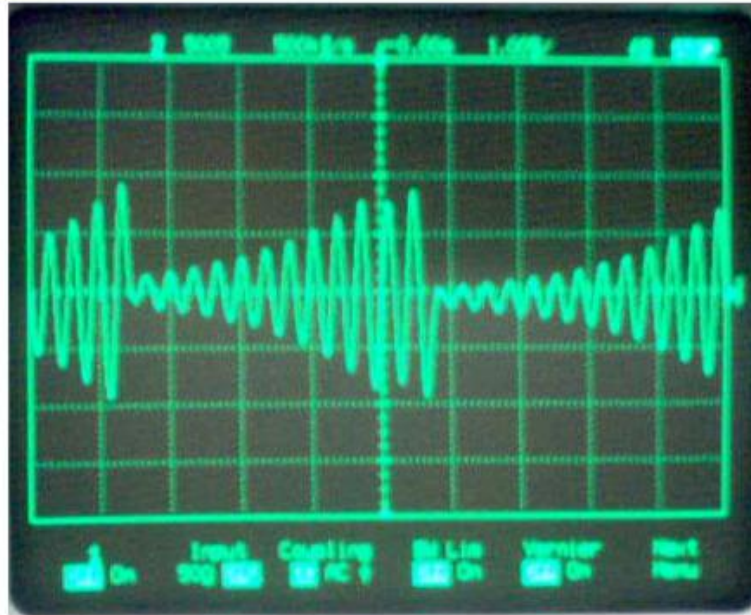


Fig. 4.4.16. Gráfica $x_2(t)$

4.5 SIMULACIÓN DE LA SINCRONIZACIÓN DE DOS CIRCUITOS DE CHUA MEDIANTE EL PROGRAMA SIMNON VER. 1.0.

El programa elaborado en el programa Simnon para realizar la simulación de la sincronización de dos circuitos de Chua se muestra a continuación. El método para realizar dicha sincronización fue el conocido como retroalimentación de error.

CONTINUOUS SYSTEM CHUADUO

" Version: 1.0

" Abstract:

" Description: Synchronization of two Chua's Circuits

" Revision: 1.0

" Author: DelFin

" Created: 07/08/2006

" States, derivates and time:

STATE x1 x2 x3 xr1 xr2 xr3

DER dx1 dx2 dx3 dxr1 dxr2 dxr3

" Initializations:

x1:0.1

x2:0.02

x3:0

xr1:0

xr2:0

xr3:0

" Equations for SYSTEM 1:

$f1 = b \cdot x1 + (1/2) \cdot (a - b) \cdot (\text{ABS}(x1 + 1) - \text{ABS}(x1 - 1))$

$dx1 = \text{alfa} \cdot (x2 - x1 -$

$f1)$ $dx2 = x1 - x2 + x3$

$dx3 = -\text{beta} \cdot x2$

" Coupling signal

$$u=c*(x1-xr1)$$

" Equations for SYSTEM 2:

$$f2=b*xr1+(1/2)*(a-b)*(ABS(xr1+1)-ABS(xr1-1))$$

$$dxr1=alfa*(xr2-xr1-f2)+u$$

$$dxr2=xr1-xr2+xr3$$

$$dxr3=-beta*xr2$$

" Equations for SYNCHRONIZATION

$$\text{ERRORS: } e1=x1-xr1$$

$$e2=x2-xr2$$

$$e3=x3-xr3$$

" Parameter values:

$$a=-8/7 \quad b=-$$

$$5/7 \quad alfa=10$$

$$beta=14.87$$

$$c=7.7$$

END

La grafica 4.5.1 muestra la calidad de sincronía que se presenta en nuestro sistema.

Sincronía [ashow x1(xr1)]



Fig. 4.5.1 Señal de sincronización entre los dos circuitos de Chua $x_1(t)$ vs $x_{r1}(t)$

La grafica 4.5.2 muestra la señal de error e1 al sincronizar los dos circuitos de Chua. Error e1

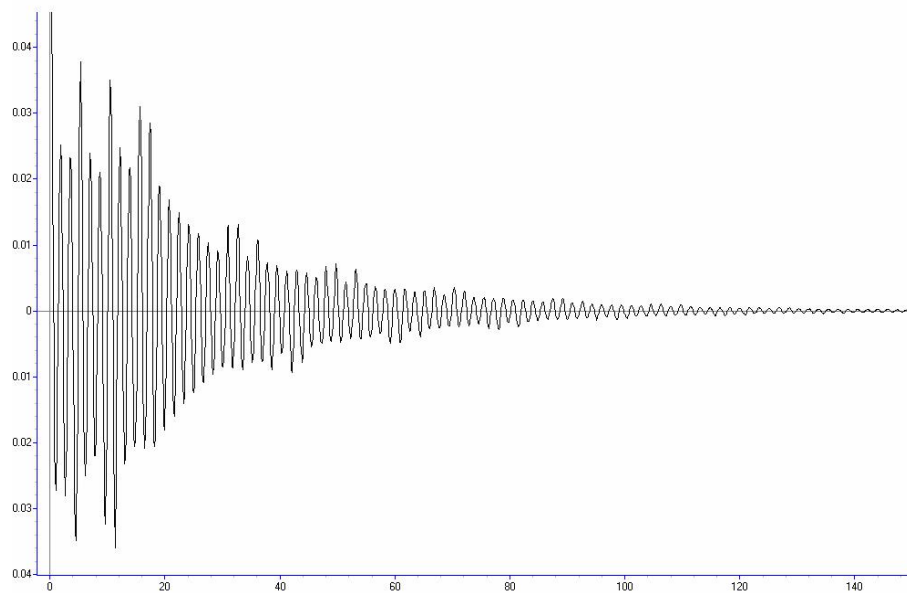


Fig. 4.5.1 Señal de error $e_1 = x_1(t) - x_{r1}(t)$

4.6 IMPLEMENTACIÓN FÍSICA Y RESULTADOS EXPERIMENTALES DE LA SINCRONIZACIÓN DE DOS CIRCUITOS DE CHUA.

La implementación electrónica para realizar la sincronización de dos circuitos de Chua se muestra en la figura 4.6.1. El método para realizar dicha sincronización es el conocido como retroalimentación de error.

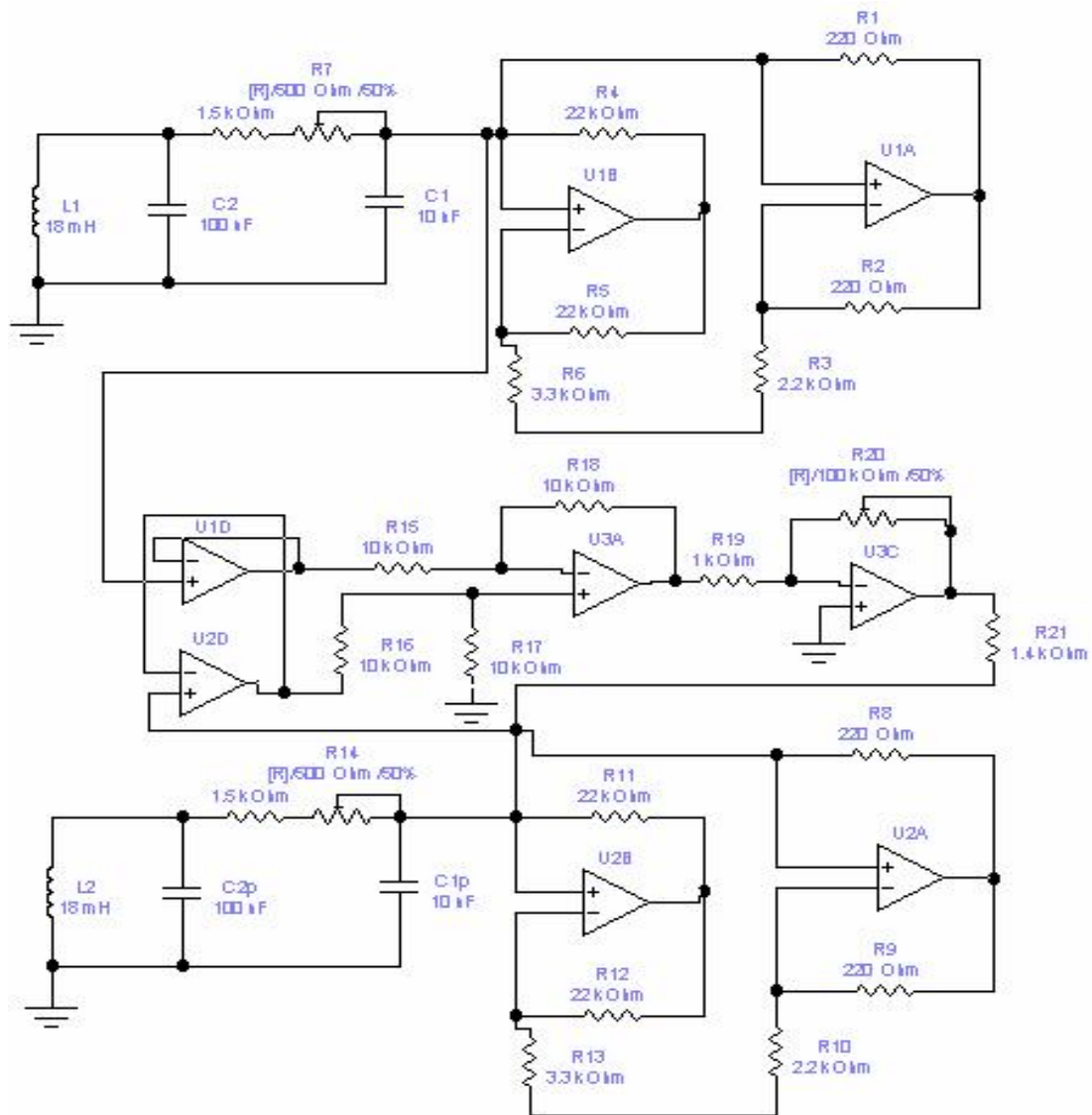


Fig. 4.6.1 Implementación electrónica de la Sincronización de dos circuitos Chua

La grafica 4.6.2 muestra la calidad de sincronía que se presenta en la implementación física para lograr la sincronía entre dos circuitos de Chua.

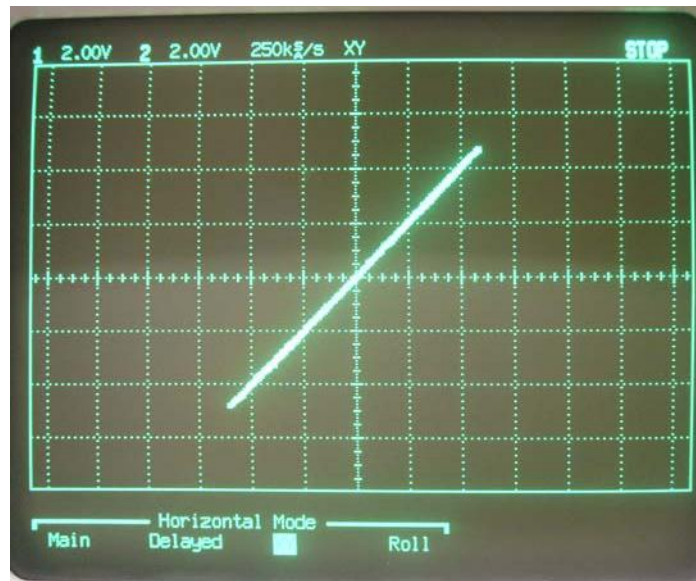


Fig. 4.6.2 Señal de sincronización entre los dos circuitos de Chua $x_1(t)$ vs $x_{r1}(t)$

La grafica 4.6.3 muestra la señales en el tiempo de $x_1(t)$ y $x_{r1}(t)$.

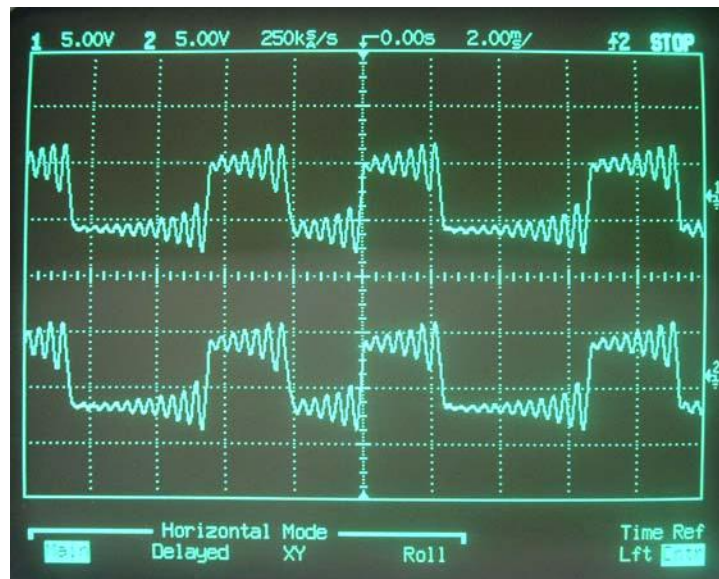


Fig. 4.6.3 Gráficas de $x_1(t)$ y $x_{r1}(t)$

4.7 SIMULACIÓN DEL ENCRİPTADO DE UNA ONDA SENOIDAL A DIFERENTES AMPLITUDES Y FRECUENCIAS POR EL MÉTODO DE ENMASCARAMIENTO CAÓTICO ADITIVO.

El siguiente programa muestra la simulación del encriptado de una señal senoidal por el método de enmascaramiento caótico aditivo.

CONTINUOUS SYSTEM CHUADUO

" Version: 1.0

" Abstract:

" Description: Sent and Received Messages

" Revision: 1.0

" Author: DelFin

" Created: 07/08/2006

" States, derivates and time:

STATE x1 x2 x3 xr1 xr2 xr3

DER dx1 dx2 dx3 dxr1 dxr2 dxr3

TIME t

" Initializations:

x1:0.1

x2:0.02

x3:0

xr1:0

xr2:0

xr3:0

" Equations for SYSTEM 1:

$f1 = b \cdot x1 + (1/2) \cdot (a - b) \cdot (ABS(x1 + 1) - ABS(x1 - 1))$

$dx1 = \alpha \cdot ((x2 + m) - x1 - f1)$ $dx2 = x1 - (x2 + m) + x3$

$$dx3 = -\beta(x2 + m)$$

" Coupling signal

$$u = c(x1 - xr1)$$

" Equations for SYSTEM 2:

$$f2 = b \cdot xr1 + (1/2) \cdot (a - b) \cdot (ABS(xr1 + 1) - ABS(xr1 - 1))$$

$$dxr1 = \alpha \cdot ((xr2 + m) - xr1 - f2) + u \quad dxr2 = xr1 - (xr2 + m) + xr3$$

$$dxr3 = -\beta(xr2 + m)$$

" Equations for SYNCHRONIZATION

$$ERRORS: e1 = x1 - xr1$$

$$e2 = x2 - xr2$$

$$e3 = x3 - xr3$$

" Equation for MESSAGE:

$$m = Amp \cdot \sin(w \cdot t)$$

" Equation for ENCRYPTED

$$MESSAGE \quad em = x2 + m$$

" Equation for the difference between MESSAGE and RECEIVED

$$MESSAGE \quad q = m - rm$$

" Equation for RECEIVED MESSAGE:

$$rm = x2 + m - xr2$$

" Parameter

$$values: a = -8/7$$

$$b = -5/7$$

$$\alpha = 10$$

$$\beta = 14.87$$

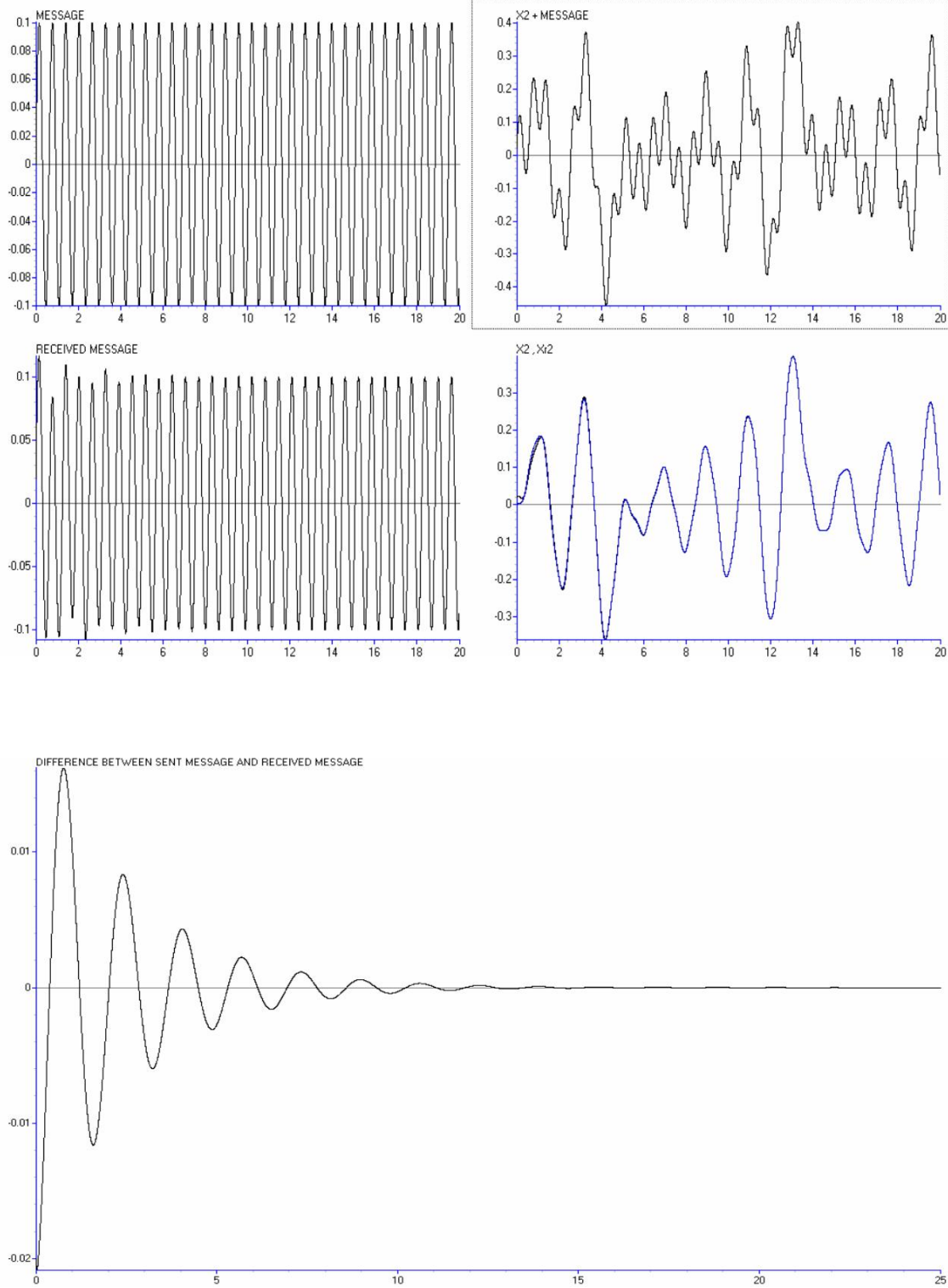
$$c = 10$$

$$Amp = 0.1$$

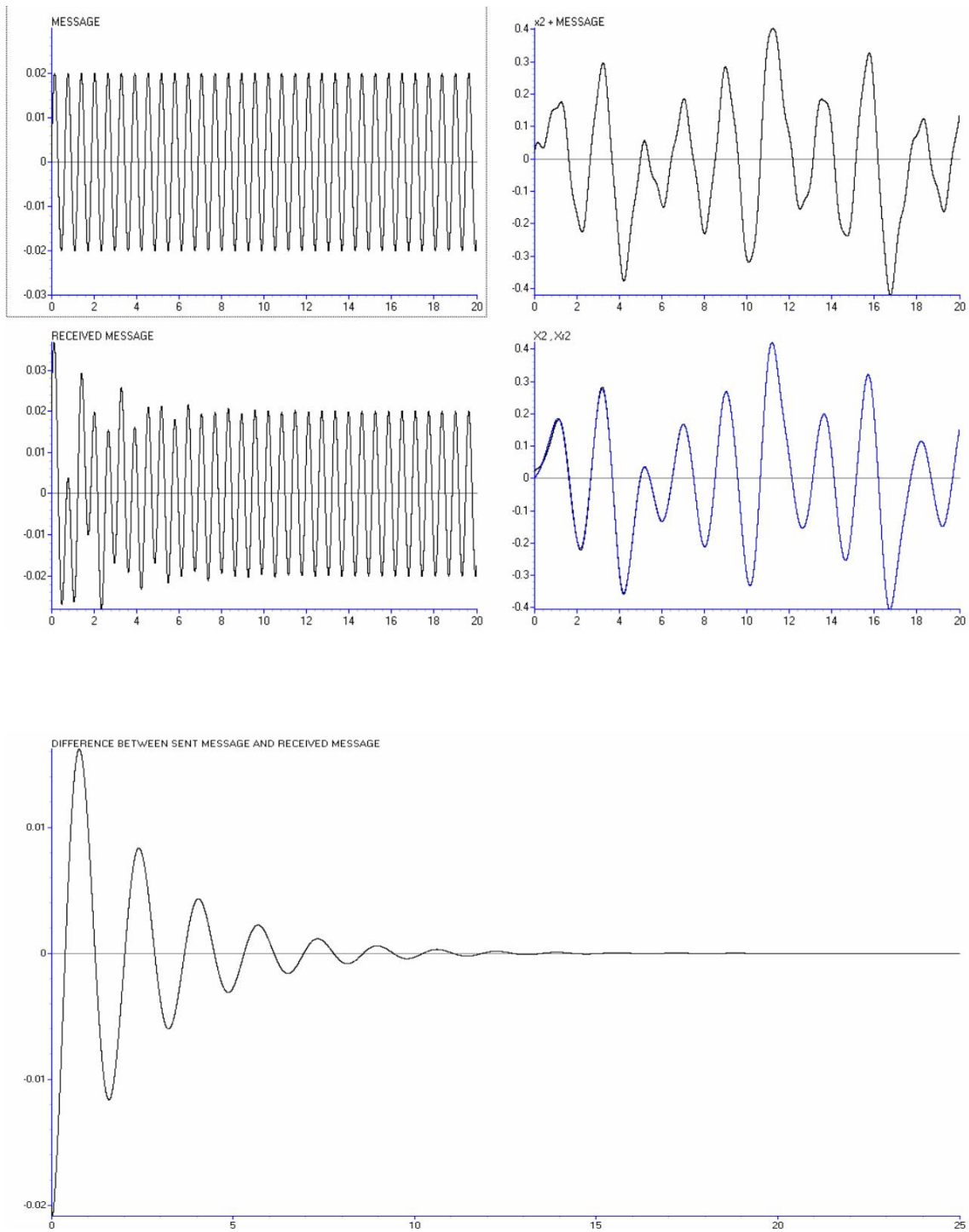
$$w = 10$$

END

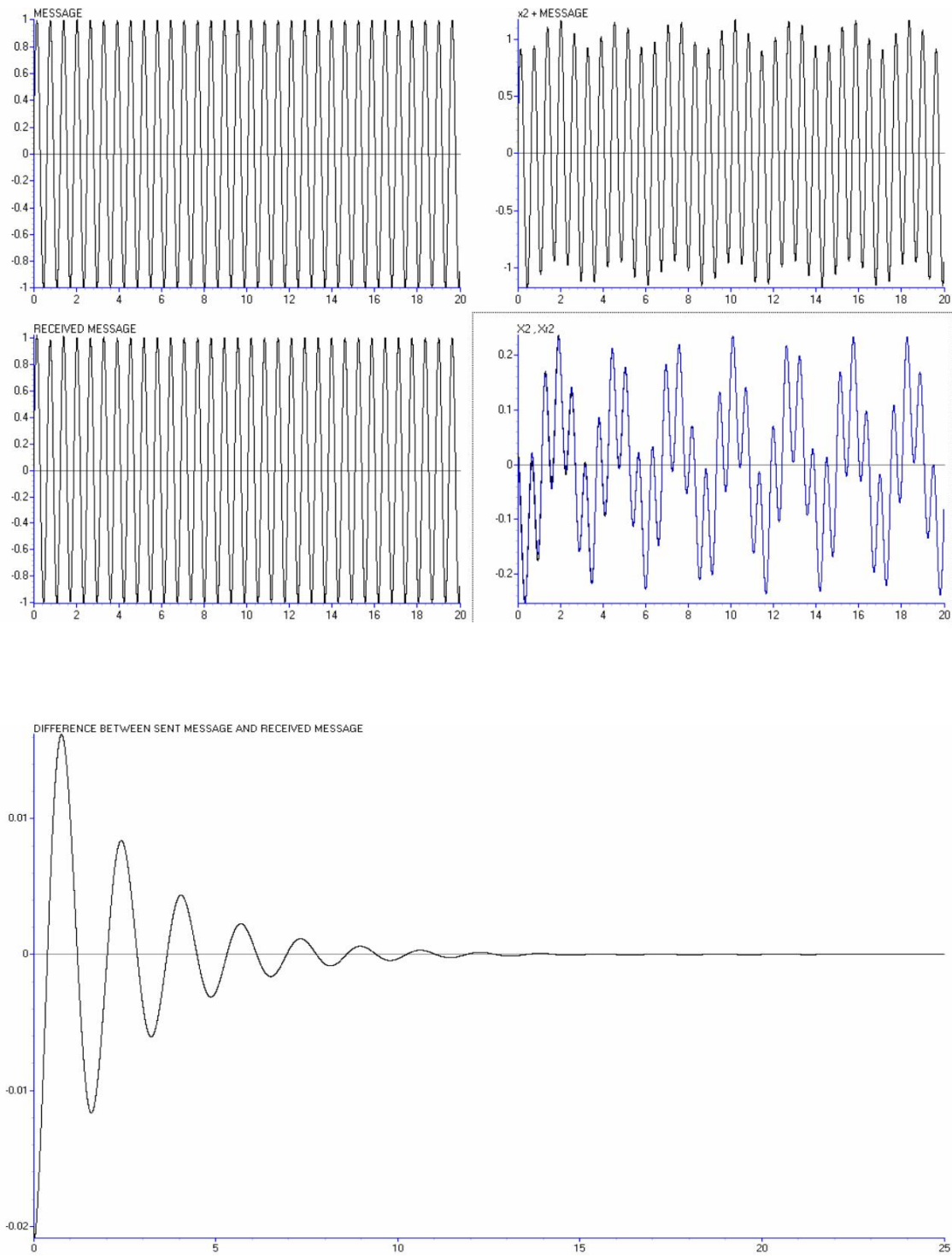
1. Mensaje: Amp= 0.1 $w=10$



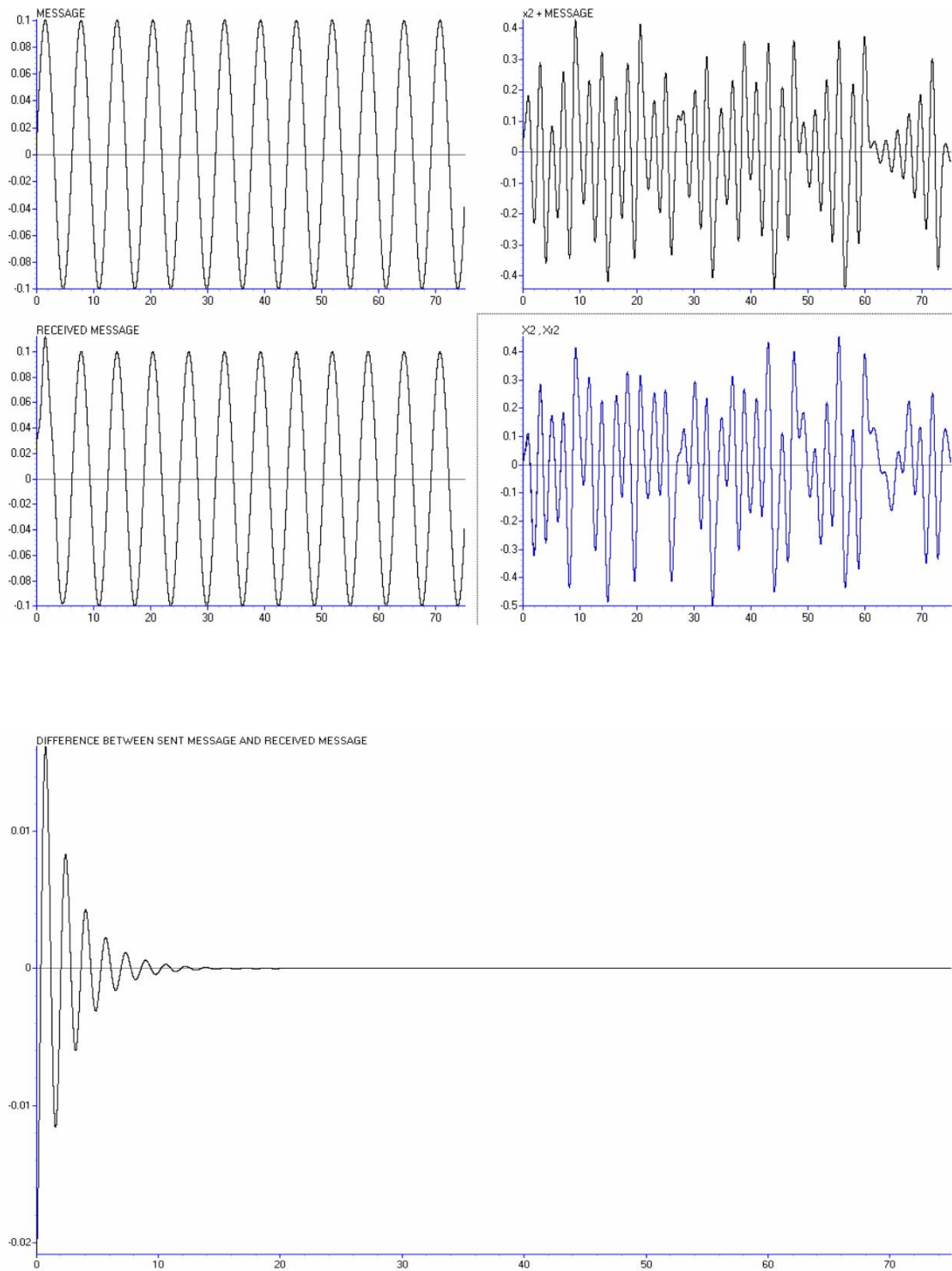
2. Mensaje: Amp= 0.02 $w=10$



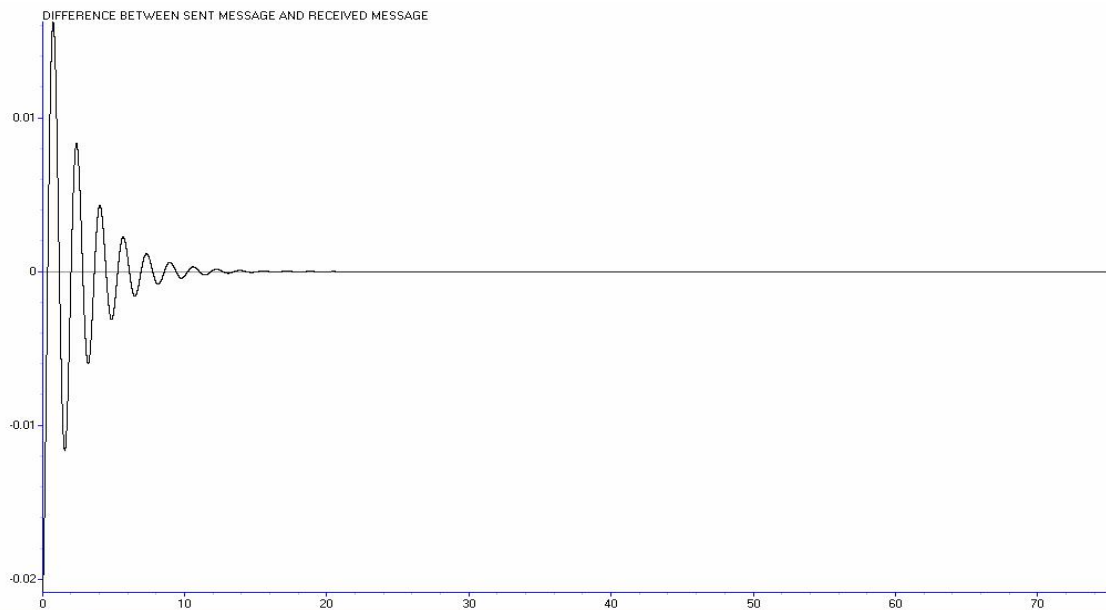
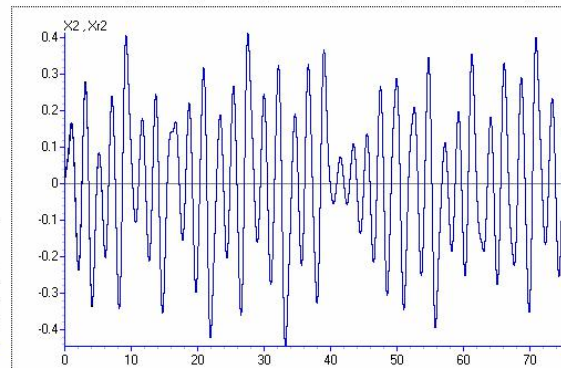
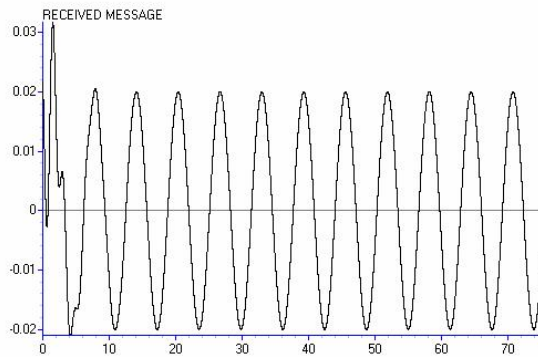
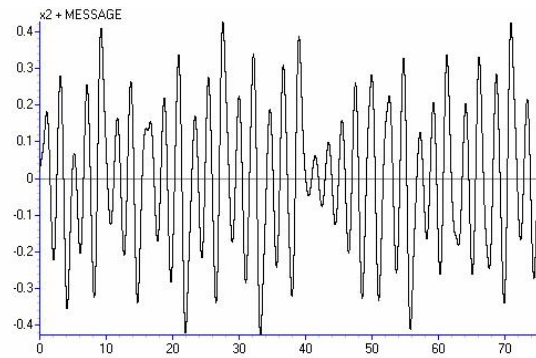
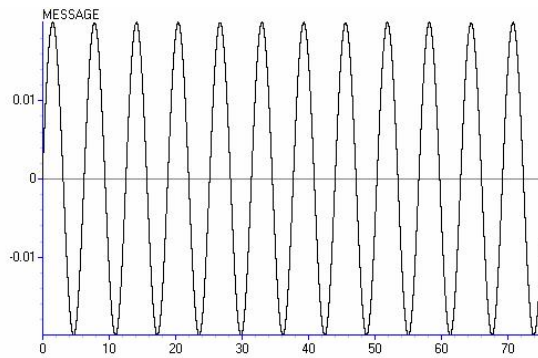
3. Mensaje: Amp= 1 w=10



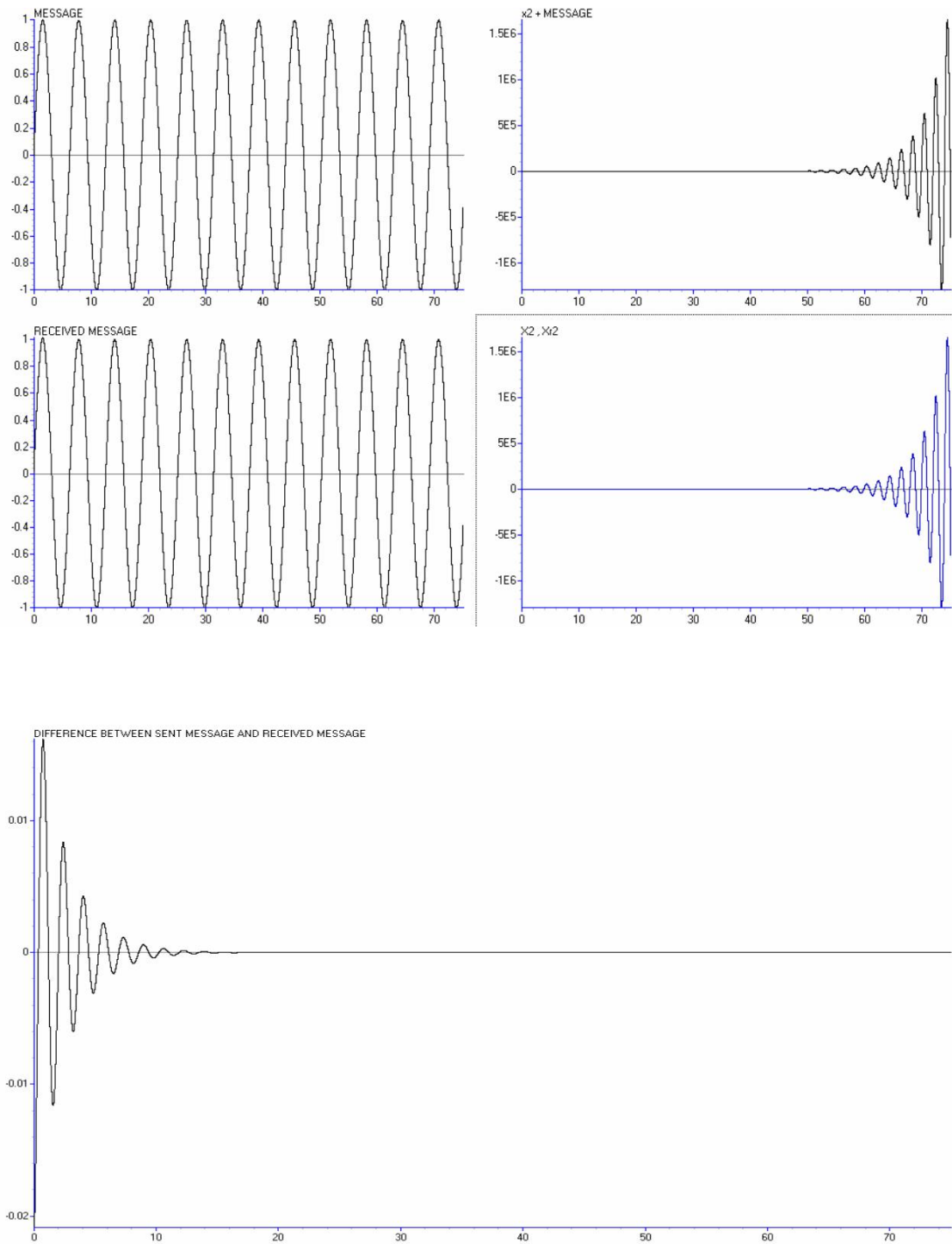
4. Mensaje: Amp= 0.1 $w = 1$



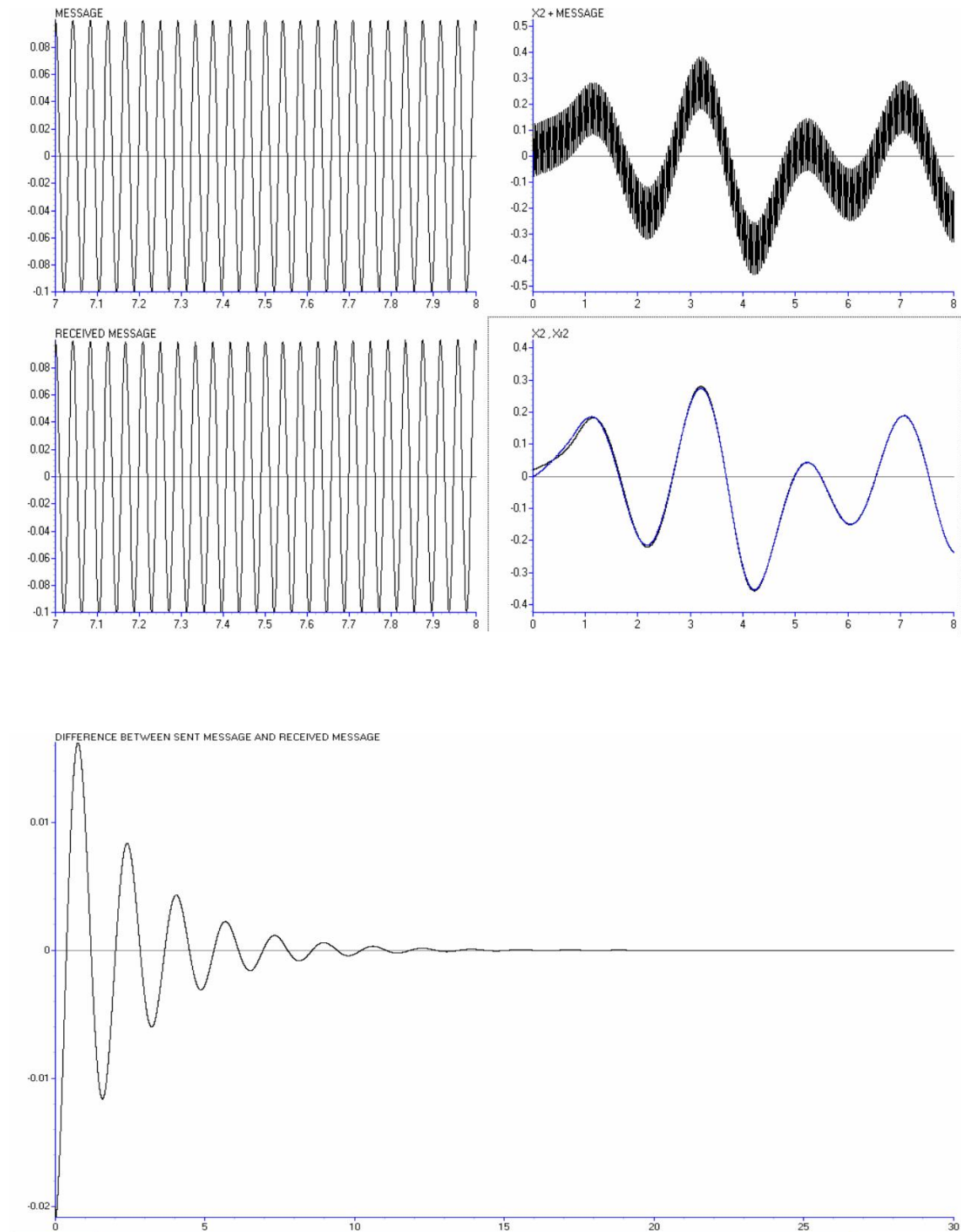
5. Mensaje: Amp= 0.02 $w= 1$



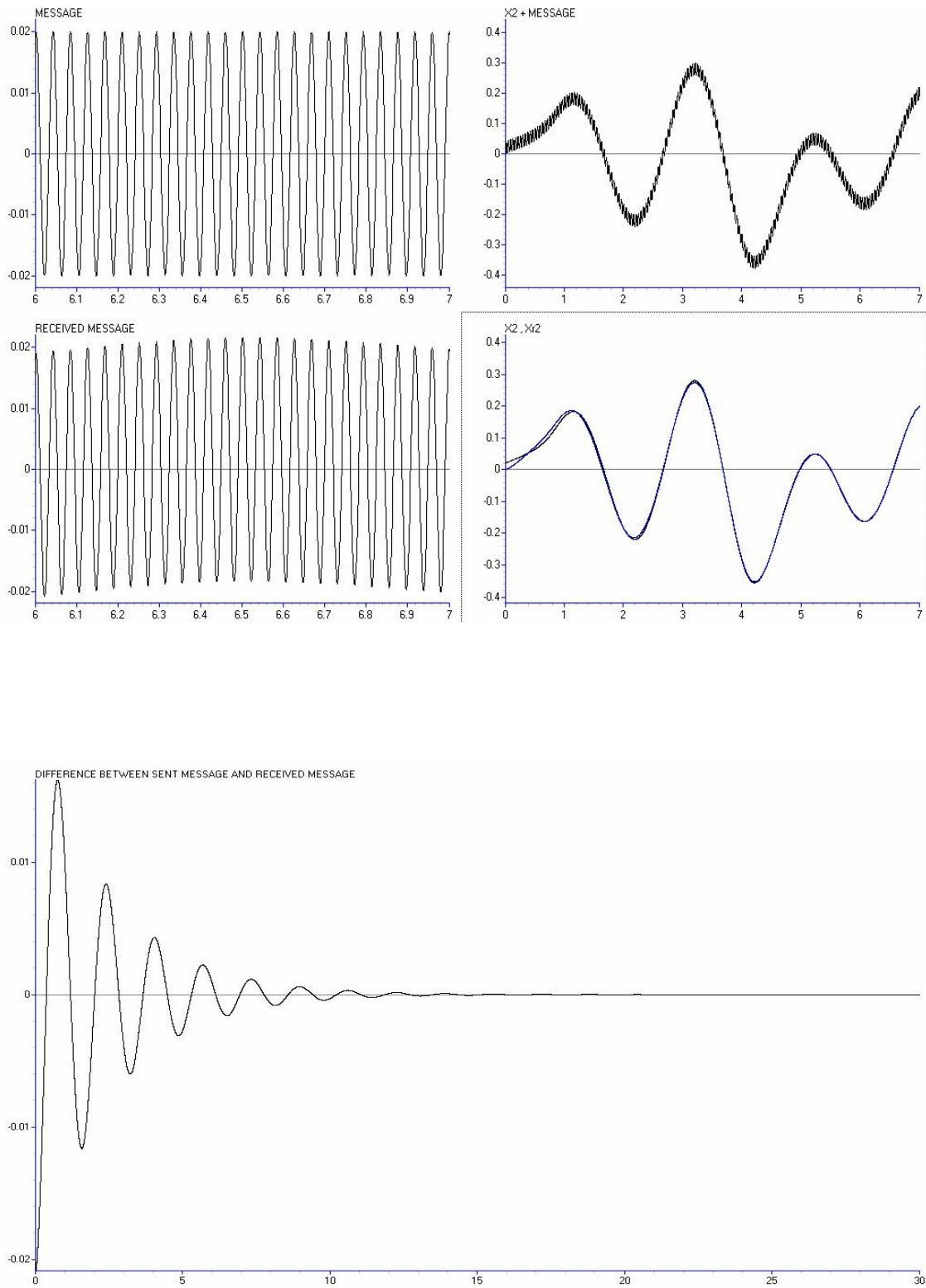
6. Mensaje: Amp= 1 $w= 1$



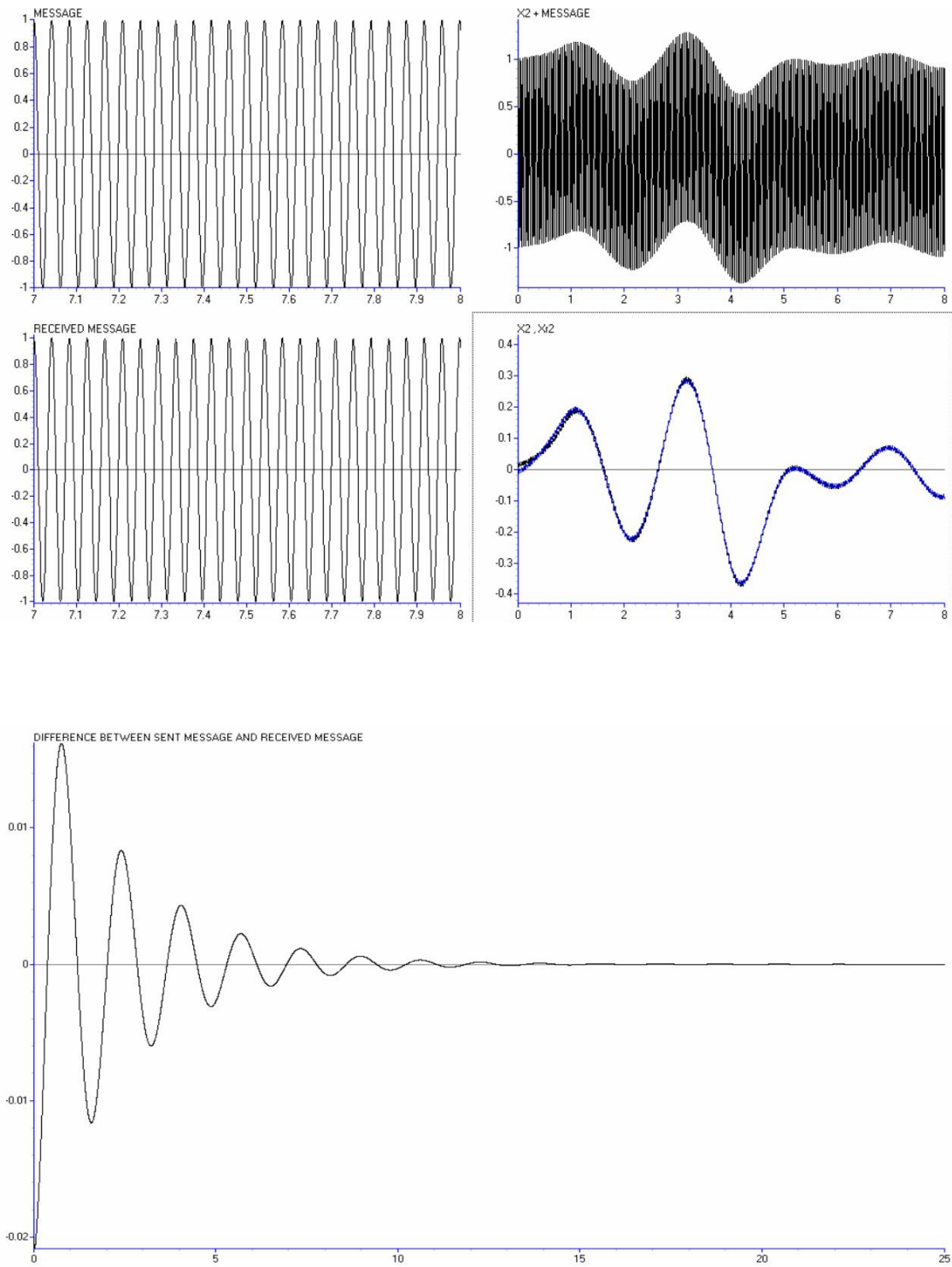
7. Mensaje: Amp= 0.1 $w = 151$



8. Mensaje: Amp= 0.02 $w= 151$



9. Mensaje: Amp= 1 w= 151



4.8 ENCRIPADO DE UN MENSAJE DE VOZ POR MEDIO DEL PROGRAMA MATLAB

Por medio del programa MatLab se realizó una simulación del encriptado de un mensaje de voz, en específico se empleo la herramienta de Simulink de este programa para poder construir el circuito de Chua como primer paso; la sincronización de dos circuitos de Chua como segundo paso y finalmente el envío del mensaje como un tercer paso. El método empleado para realizar la transmisión del mensaje es el llamado enmascaramiento aditivo caótico.

La figura 4.8.1 muestra la construcción en Simulink del circuito de Chua.

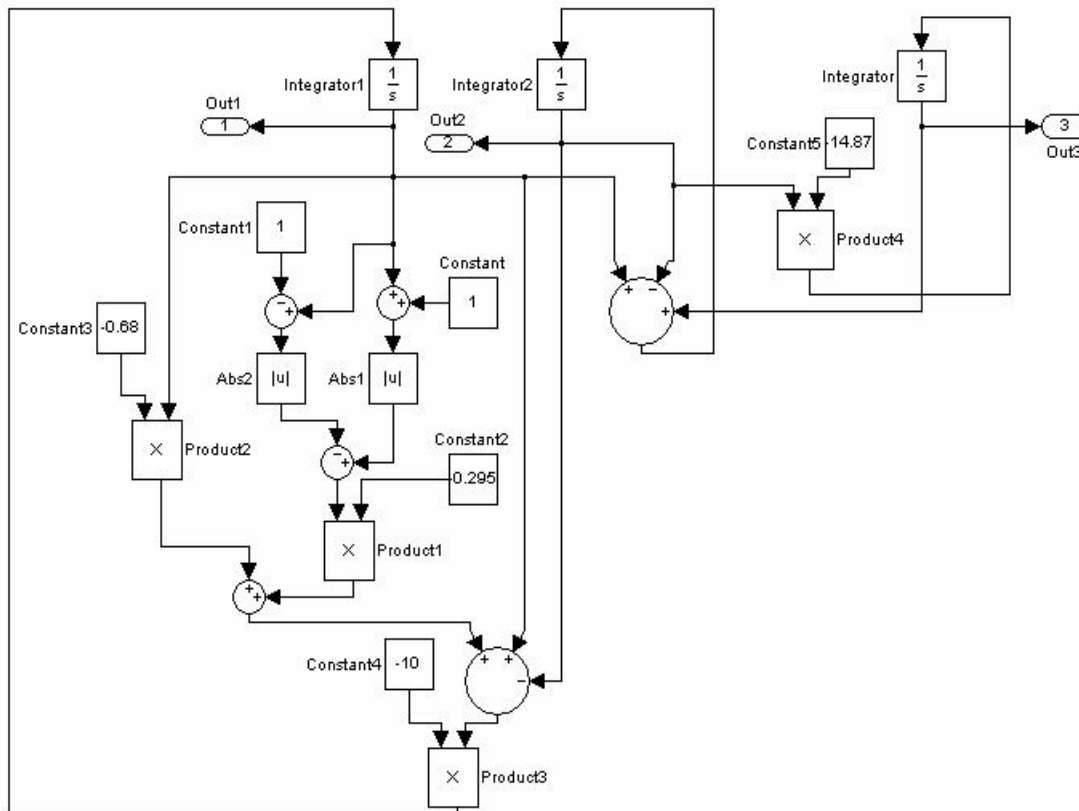


Fig. 4.8.1 Simulink (Chua's Circuit)

La figura 4.8.2 muestra la construcción en Simulink de la sincronización de dos circuitos de Chua.

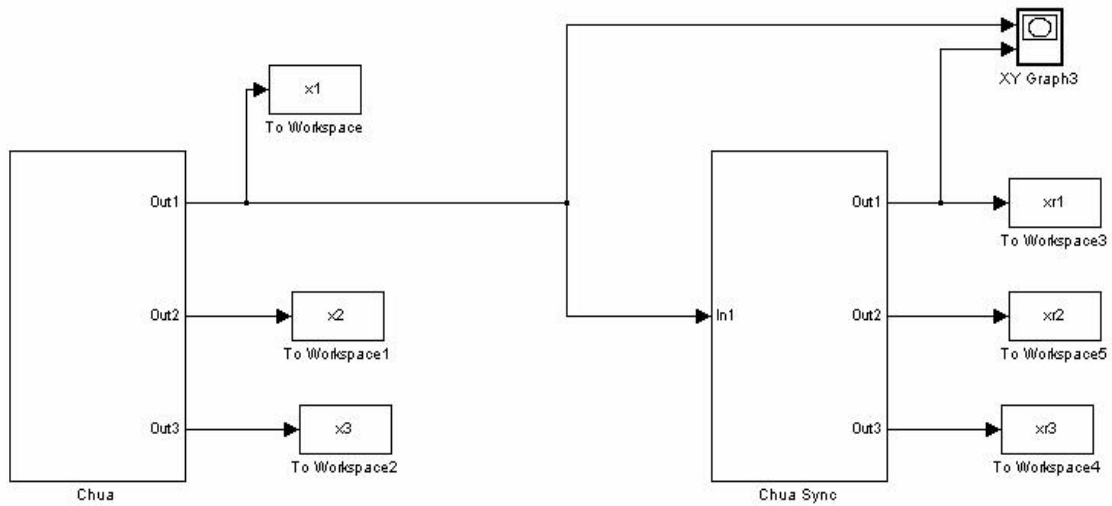


Fig. 4.8.2 Simulink Subsystem Synchronization Schematic Diagram

La calidad de sincronización se muestra en la figura 4.8.3 y corresponde a la gráfica resultante de x_1 vs x_{r1} .

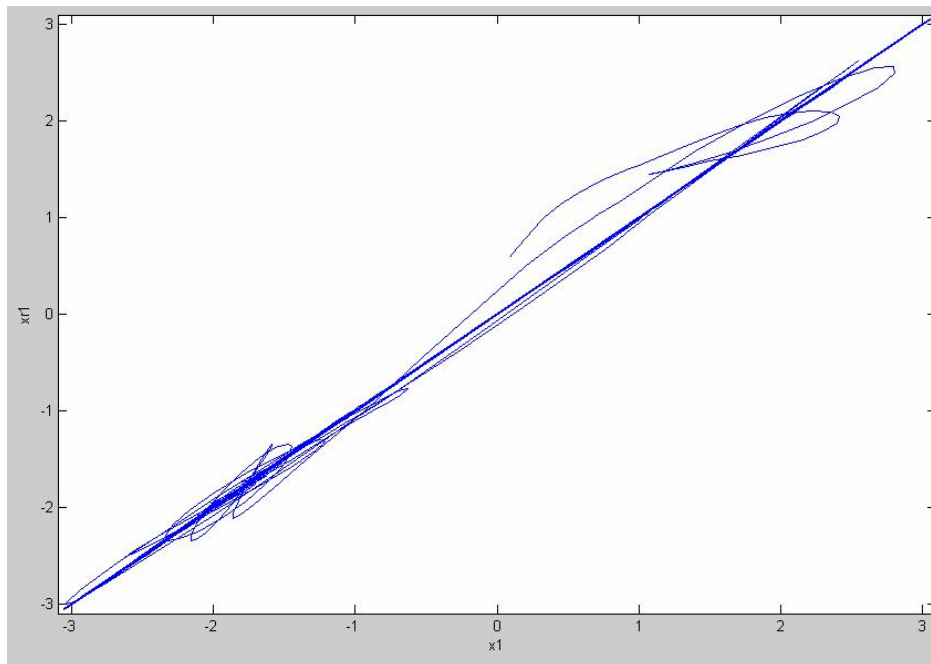


Fig. 4.8.3 Señal de Sincronización entre los dos circuitos de Chua x_1 vs x_{r1}

El siguiente programa muestra la forma en la que se realizó el encriptado del mensaje de voz: el archivo de voz es leído, convertido a un vector, se atenúa para luego por el método conocido como enmascaramiento aditivo caótico encriptar el mensaje. En el receptor el mensaje es recuperado y se amplifica.

```

1 - syms y y1 z t r ri;
2 - % y->original message ===== y1->message in one vector
3 - % z->decrease message ===== t->transmited encrypted message
4 - % r->received desencrypted message ===== ri->increase message
5 - y=wavread('alberto');
6 - y1=y(:,1);
7 - wavplay(y,44100); % 44100 Hz -> Frecuency Standard of Record
8 - z=0.1*y1;
9 - t=x2+z;
10 - wavplay(t,44100);
11 - r=t-xr2;
12 - wavplay(r,44100);
13 - ri=10*r;
14 - wavplay(ri,44100);
15 - % ===== graphics =====
16 - subplot(3,1,1);plot(y);
17 - subplot(3,1,2);plot(t);
18 - subplot(3,1,3);plot(ri);

```

Las figuras 4.8.3, 4.8.4 y 4.8.5 muestran el encriptado de los mensajes de voz de tres personas distintas, dichas figuras son el resultado del programa elaborado en MatLab.

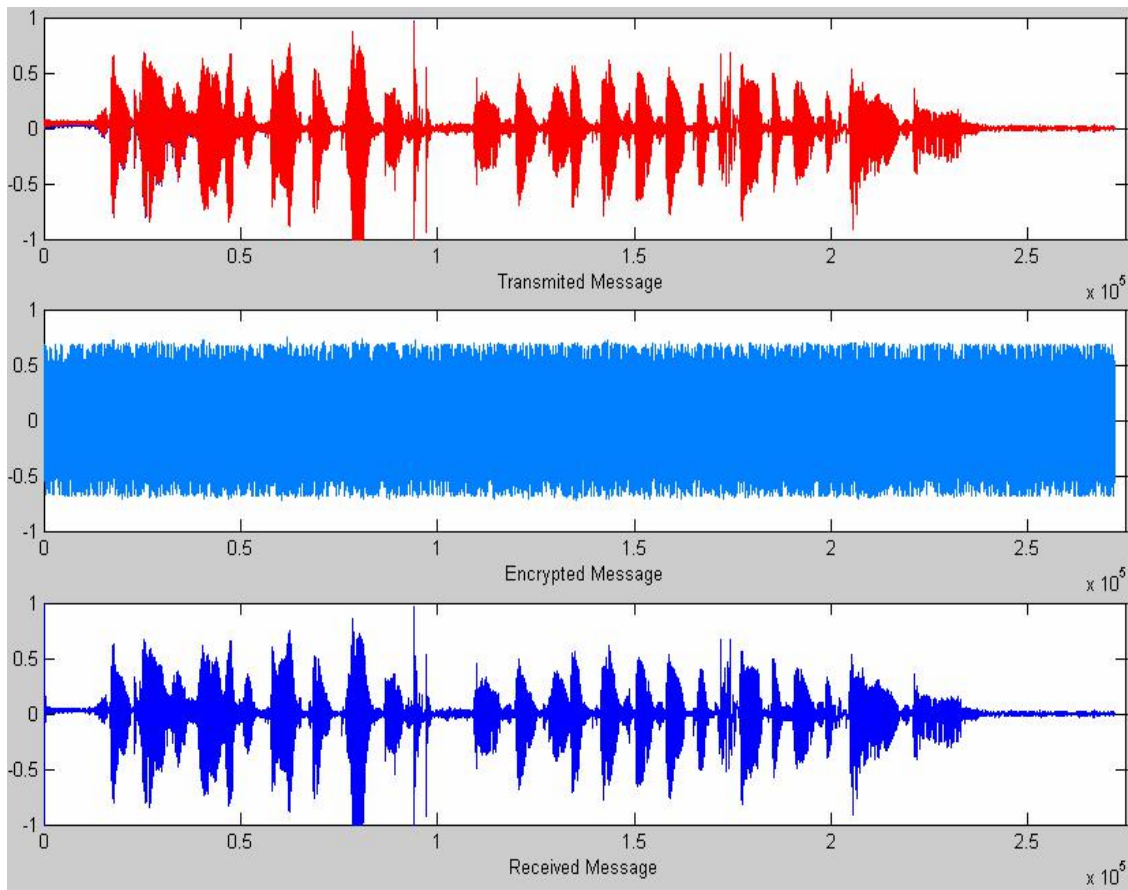


Fig. 4.8.4 MatLab Simulation
Alberto's message

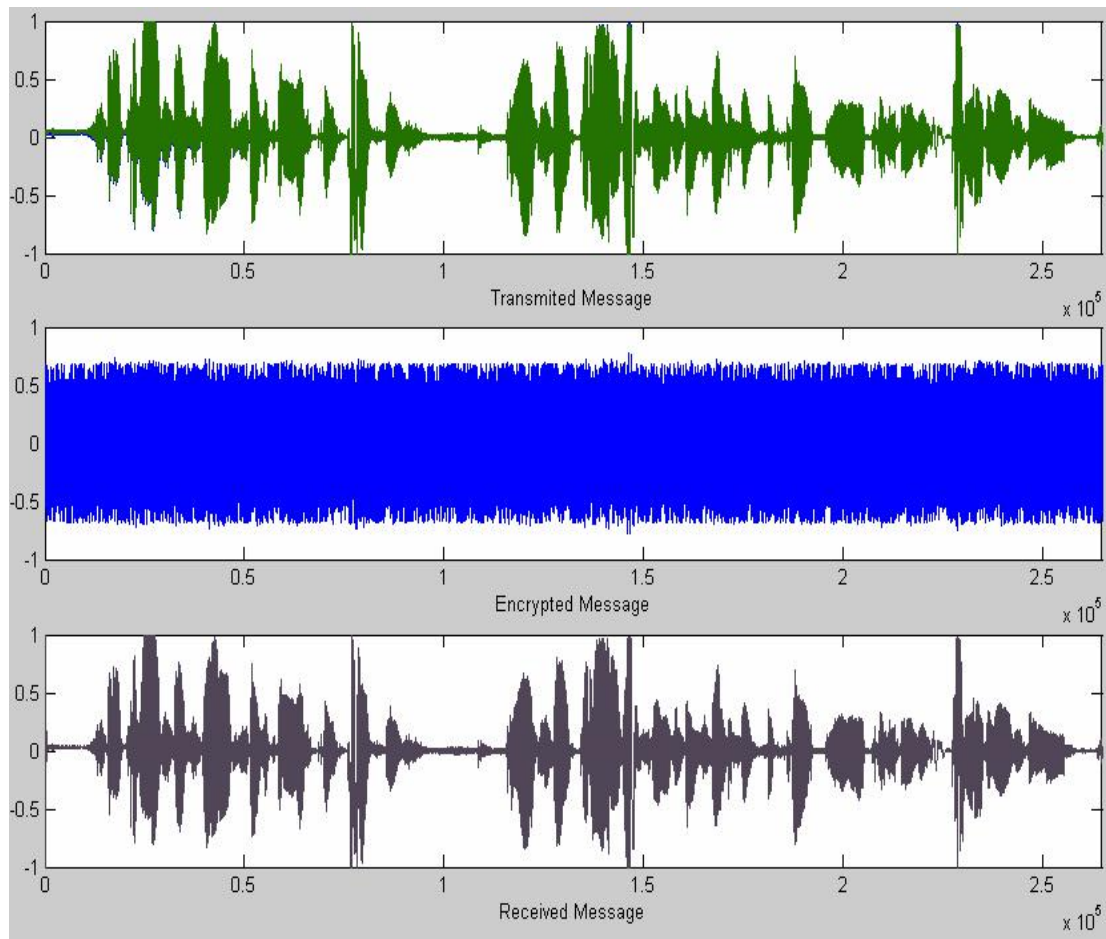


Fig. 4.8.5 MatLab Simulation
David's message

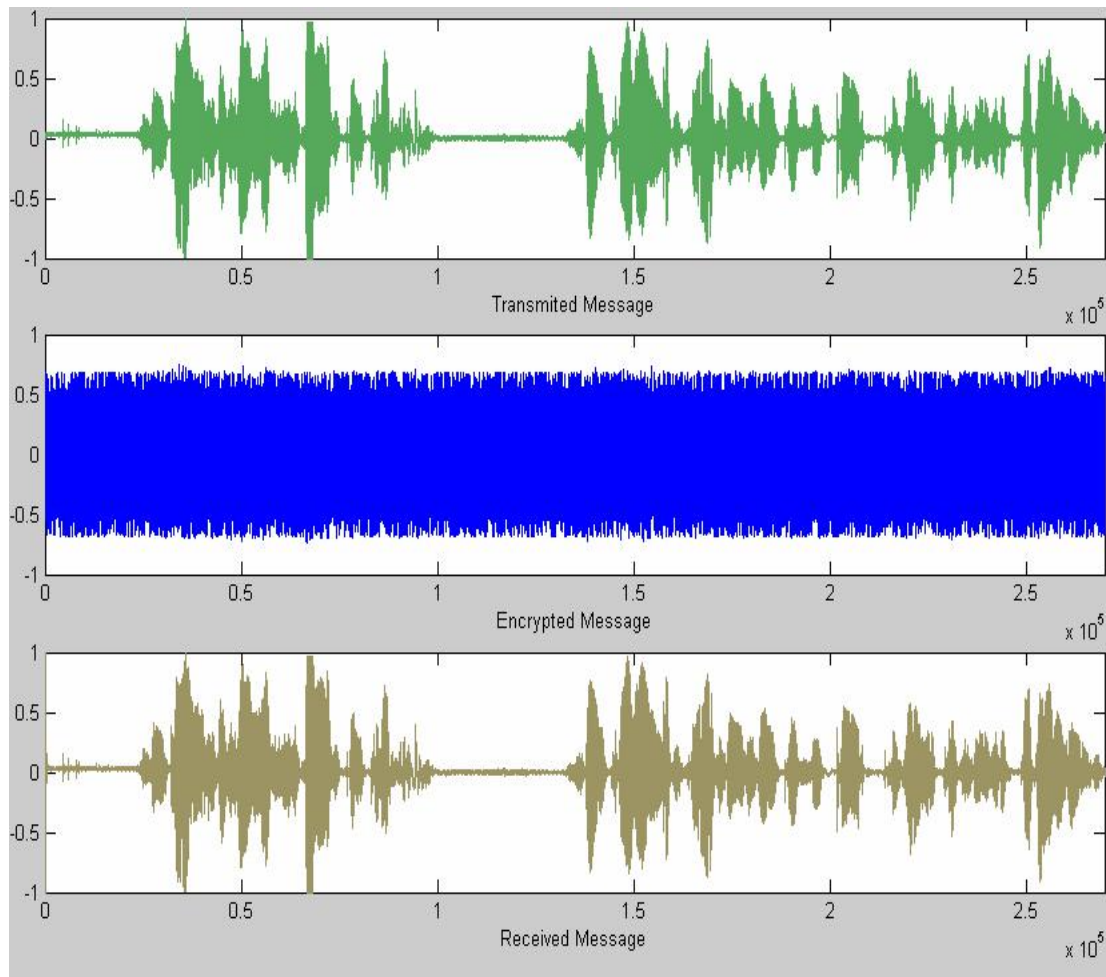


Fig. 4.8.3 MatLab Simulation Ruben's message

AMPLIFICADOR DE FIBRA ÓPTICA, EDFA (ERBIUM DOPED FIBER AMPLIFIER)

1. INTRODUCCIÓN

En fibra óptica, un amplificador óptico es un dispositivo que amplifica una señal óptica directamente, sin la necesidad de convertir la señal al dominio eléctrico, amplificar en eléctrico y volver a pasar a óptico.

Amplificadores en fibra son amplificadores ópticos que usan fibra dopada, normalmente con tierras raras. Estos amplificadores necesitan de un bombeo externo con un láser de onda continua a una frecuencia óptica ligeramente superior a la que amplifican. Típicamente, las longitudes de onda de bombeo son 980 nm o 1480 nm y para obtener los mejores resultados en cuanto a ruido se refiere, debe realizarse en la misma dirección que la señal.

Un amplificador óptico es capaz de amplificar un conjunto de longitudes de onda (WDM, wavelength division multiplexing).

2. ¿QUÉ ES EL CAOS?

2.1.- DEFINICIÓN:

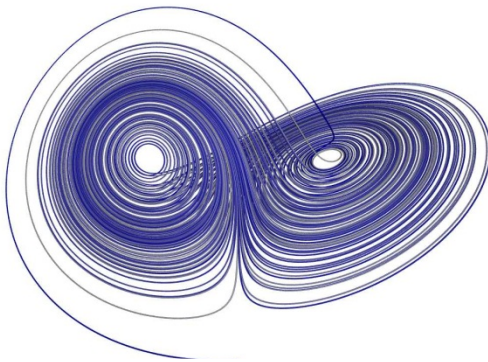


Figura 1: Atractor de Caos

El caos es un comportamiento impredecible que surge en un sistema determinista debido a la gran sensibilidad a las condiciones iniciales que presenta. El caos surge en un sistema dinámico si dos puntos arbitrarios iniciales y cercanos divergen exponencialmente tal que su comportamiento futuro es eventualmente impredecible.

El término caos se refiere a una interconexión subyacente que se manifiesta en acontecimientos aparentemente aleatorios.

El caos es impredecible, pero determinable. O dicho de otro modo, el caos no es aleatorio, tiene un orden subyacente.

La gran sensibilidad a las condiciones iniciales se observa en: “*El efecto mariposa*”.

A saber: “Si hoy agita una mariposa sus alas en Barcelona, con su aleteo puede producir un huracán en Tokio el mes que viene.”

Este concepto se conoce como “*Dependencia sensitiva de las condiciones iniciales*” que es determinante y básico para comprender este mundo tan maravilloso, tan caótico y regular a la vez.

Los **sistemas dinámicos**, son sistemas que varían con el paso del tiempo, tales como la teoría malthusiana de población y recursos, la meteorología, los seísmos, los movimientos que efectúa un chorro de café humeante al entrar en contacto con la leche de una taza (mecánica de fluidos), el giro impredecible de una noria de agua cuando su caudal es inusitadamente acelerado, la gran mancha de Júpiter, las fluctuaciones económicas de los precios, etc.

Es en los sistemas dinámicos donde podemos usar el término “caos” y donde una variación mínima de las condiciones iniciales supone un comportamiento totalmente distinto del esperado por parte del sistema, es decir que un sistema podrá ser caótico cuando su comportamiento sea impredecible.

El caos es determinista al estudiar uno de estos sistemas, si se trata en su globalidad. No podrá predecir el estado futuro del mismo pero sí moldear su comportamiento general. Estos sistemas pueden comportarse de diferentes formas, pero muchos de ellos tras suficientes iteraciones (repetición de un cálculo simple) de las funciones que los determinan, su función tiende a estabilizarse en uno o más valores. Este conjunto de valores para los cuales la función $f(x)$, se estabiliza cuando el número de iteraciones tiende a infinito, se denomina “*atractor*”.

Características de los sistemas caóticos:

- **Deterministas.-** Siguen unas reglas que pueden resumirse en una serie de funciones.
- **Sensibles.-** A las condiciones iniciales, ya que un cambio mínimo en sus datos iniciales puede provocar un resultado totalmente inesperado.
- **Simples.-** No en cuanto a su comportamiento sino en cuanto a las funciones que los determinan.

2.2.- ATRACTORES

Una manera de visualizar el movimiento caótico, o cualquier tipo de movimiento, es hacer un diagrama de fases del movimiento. En tal diagrama el tiempo es implícito y cada eje representa una dimensión del estado. Por ejemplo, un sistema en reposo será dibujado como un punto, y un sistema en movimiento periódico será dibujado como un círculo.

Algunas veces el movimiento representado con estos diagramas de fases no muestra una trayectoria bien definida, sino que ésta se encuentra errada alrededor de algún movimiento bien definido. Cuando esto sucede se dice que el sistema es atraído hacia un tipo de movimiento, es decir, que hay un atractor. De acuerdo a la forma en que sus trayectorias evolucionen, los atractores pueden ser clasificados como periódicos, casi-periódicos y extraños. Estos nombres se relacionan exactamente con el tipo de movimiento que provocan en los sistemas. Un atractor periódico, por ejemplo, puede guiar el movimiento de

un péndulo en oscilaciones periódicas; sin embargo, el péndulo seguirá trayectorias erráticas alrededor de estas oscilaciones debidas a otros factores menores.

Atractores extraños

La mayoría de los tipos de movimientos mencionados en la teoría anterior sucede alrededor de atractores muy simples, tales como puntos y curvas circulares llamadas *ciclos límite*. En cambio, el movimiento caótico está ligado a

lo que se conoce como atractores extraños, atractores que pueden llegar a tener una enorme complejidad como, por ejemplo, el modelo tridimensional del sistema climático de Lorenz, que lleva al famoso atractor de Lorenz. El atractor de Lorenz es, quizá, uno de los diagramas de sistemas caóticos más conocidos, no sólo porque fue uno de los primeros, sino también porque es uno de los más complejos y peculiares, pues desenvuelve una forma muy peculiar más bien parecida a las alas de una mariposa.

- Atractor de Lorenz: es un sistema dinámico determinístico tridimensional no lineal derivado de las ecuaciones simplificadas de rolos de convección que se producen en las ecuaciones dinámicas de la atmósfera terrestre.

Para ciertos valores de los parámetros a , b , c el sistema exhibe un comportamiento caótico y muestra lo que actualmente se llama un atractor extraño; esto fue probado por W. Tucker en 2001. El atractor extraño en este caso es un fractal de dimensión de Hausdorff entre 2 y 3. Grassberger (1983) ha estimado la dimensión de Hausdorff en 2.06 ± 0.01 y la dimensión de correlación en 2.05 ± 0.01 .

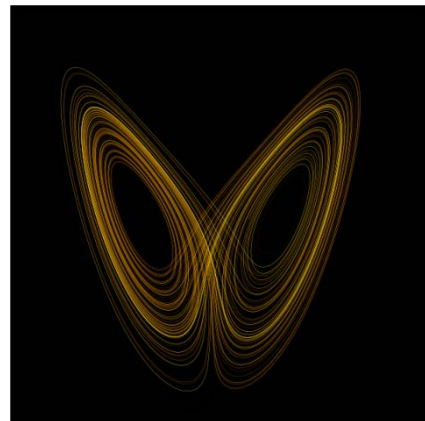


Figura 2: Atractor extraño de Lorenz

Los atractores extraños están presentes tanto en los sistemas continuos dinámicos (tales como el sistema de Lorenz) como en algunos sistemas discretos (por ejemplo el mapa Hènon). Otros sistemas dinámicos discretos tienen una estructura repelente de tipo Conjunto de Julia la cual se forma en el límite entre las cuencas de dos puntos de atracción fijos. Julia puede ser sin embargo un atractor extraño. Ambos, atractores extraños y atractores tipo Conjunto de Julia, tienen típicamente una estructura fractal.

El teorema de Poincaré-Bendixson muestra que un atractor extraño sólo puede presentarse como un sistema continuo dinámico si tiene tres o más dimensiones. Sin embargo, tal restricción no se aplica a los sistemas discretos,

los cuales pueden exhibir atractores extraños en sistemas de dos o incluso una dimensión.

- Mapa de Hénon: es un sistema dinámico en tiempo discreto. Es uno de los ejemplos más estudiados de los sistemas dinámicos que presentan un comportamiento caótico. El mapa Hénon toma un punto (x_n, y_n) en el plano y lo asigna a un nuevo punto.



Figura 3: Mapa de Hénon

$$x_{n+1} = y_n + 1 - ax_n^2,$$

$$y_{n+1} = bx_n.$$

El mapa depende de dos parámetros, a y b , que para el **mapa Hénon canónico** tienen valores de $1,4$ y $b = 0,3$. Para los valores canónicos el mapa Hénon es caótico. Para otros valores de a , b , y el mapa puede ser caótico, intermitente, o convergente en una órbita periódica. Una visión general del tipo de comportamiento del mapa a diferentes valores de parámetros, pueden ser obtenidos a partir de su diagrama de la órbita.

El mapa fue presentado por Michel Hénon como un modelo simplificado de la sección de Poincaré del modelo de Lorenz. Para el mapa canónico, un punto inicial del avión se acercará a un conjunto de puntos conocidos como el atractor Hénon extraño, o serán divergentes hasta el infinito. El atractor Hénon es un fractal suave en una dirección y un conjunto de Cantor (Cantor set) en otro. Estimaciones numéricas proporcionan una dimensión de correlación de $1,25 \pm 0,02$ y una dimensión de Hausdorff de 1.261 ± 0.003 para el atractor del mapa canónico.

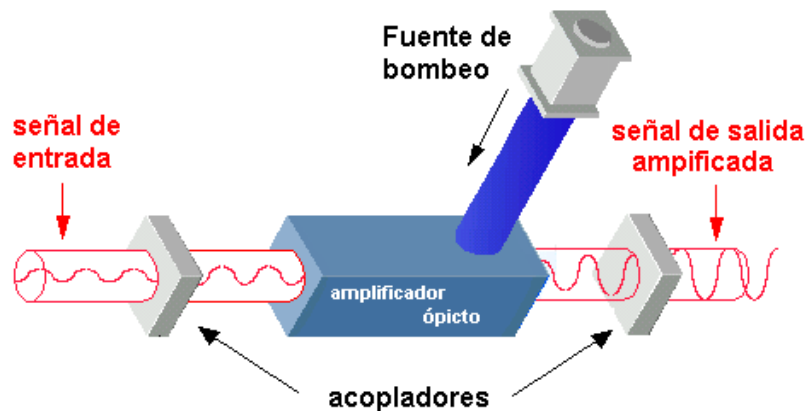
Como un sistema dinámico, el mapa Hénon canónico es interesante porque, a diferencia del mapa logístico, sus órbitas desafían una simple descripción.

6. PRINCIPIOS Y GENERALIDADES

2.1.- Amplificadores en fibra óptica

Los dos principales tipos de amplificadores ópticos son: los **SOA** (*Semiconductor Optical Amplifiers*) y los **DFA** (*Doped Fiber Amplifiers*).

El fundamento de un amplificador óptico es el proceso de emisión estimulada al



igual que en un láser. Su estructura es similar a la de un láser salvo que no posee una realimentación para evitar que el dispositivo oscile, de forma que puede elevar el nivel de potencia de la señal pero no generar una

señal óptica coherente. En la siguiente figura se muestra un esquema del funcionamiento de un amplificador básico.

Figura 4: Esquema de funcionamiento de un amplificador básico

La amplificación se produce dentro de un rango de frecuencias que dependen del material, así como su estructura.

7. EDFA (Erbium Doped Fiber Amplifier)

Los EDFA son los amplificadores de fibra más empleados en la actualidad no solo en el contexto de comunicaciones de largo alcance de fibra óptica, sino que de manera eficiente pueden amplificar la luz en la región de longitud de onda de 1550-nm, donde las fibras de telecomunicaciones tienen el mínimo de pérdidas. El motivo puede deducirse del diagrama de niveles del erbio.

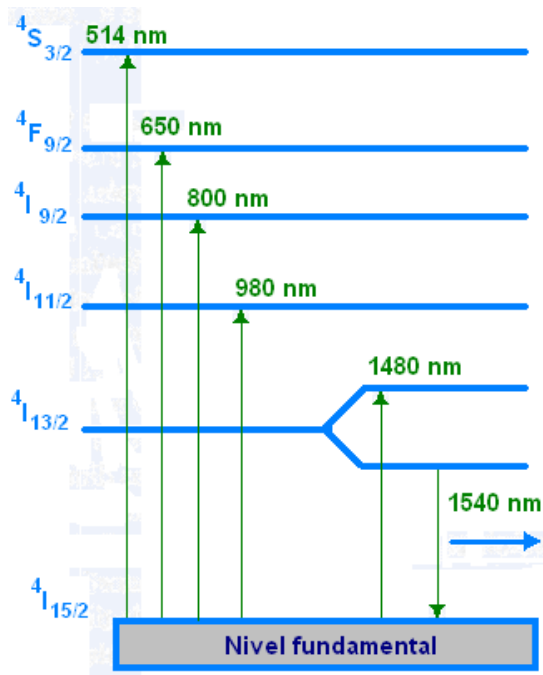


Figura 5: Diagrama de niveles energéticos del Erblio

Se puede ver en el diagrama de niveles de energía del erbio que la transición entre los niveles $4I_{13/2}$ y $4I_{15/2}$ corresponde a una longitud de onda comprendida entre 1530nm y 1560nm aprox. Luego al provocar una inversión de población entre dichos niveles se puede amplificar señales en la tercera ventana. El primer nivel excitado, $4I_{13/2}$, desde el que las frecuencias de transición se corresponden con la tercera ventana, tiene un tiempo de vida medio de unos 10ms, mientras que en los dos superiores es de 0.001ms, por lo que el nivel $4I_{13/2}$ es un estado meta estable. Por lo tanto todo ión que llegue a estos niveles por medio del bombeo acabara cayendo al nivel $4I_{13/2}$ por emisión espontánea, y a su vez cara al nivel fundamental por emisión estimulada, produciéndose así la amplificación.

Al dopar con iones de erbio el núcleo de una fibra óptica se provoca un ensanchamiento de las bandas de transición. Esto a su vez provoca un ensanchamiento considerable del rango de longitudes de onda que pueden ser amplificadas. Este efecto puede mejorarse añadiendo al núcleo, aluminio y óxido de germanio.

Las dos longitudes de onda de bombeo más adecuadas son 1480nm (mediante un diodo láser de InGaAsP) y 980nm (mediante un diodo láser de InGaAs). El empleo de una u otra longitud de onda depende de ciertas características del proceso de absorción en cada uno de estos niveles, derivadas de los diferentes tipos de ruido al que pueden originarse, de la disponibilidad de las fuentes de bombeo o de la saturación de ganancia. El bombeo a 1480nm supone un amplificador más ruidoso pero más inmune a la saturación de ganancia.

Mientras que el bombeo a 980nm proporciona un amplificador con prestaciones de ruido excelentes pero es más proclive a la saturación de ganancia. En ambos casos es posible obtener ganancias entre 30 y 50 dB.

3.1.- Configuraciones de bombeo

Los elementos básicos para implementar un EDFA son:

- El medio activo donde se produce la inversión de población. Formado por un tramo de fibra óptica de SiO₂ con el núcleo dopado con iones de erbio.
- La fuente de bombeo óptico a 1480 o 980nm, formada por un láser semiconductor.

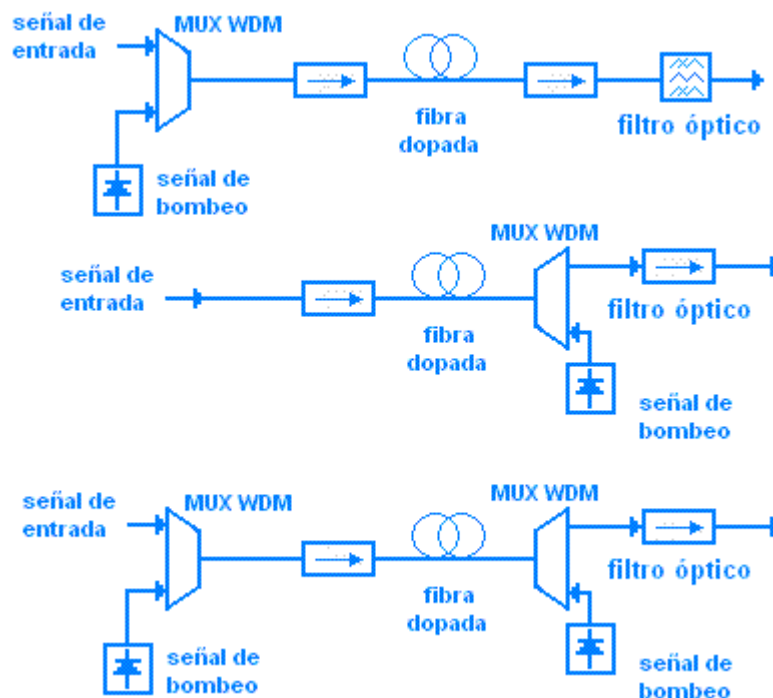


Figura 6: Configuraciones de un EDFA

En la figura anterior se muestran las configuraciones posibles del EDFA. La primera configuración es la más empleada hoy en día. La señal que hay que amplificar y la señal de bombeo se inyectan al EDFA combinadas por medio de un acoplador. El primer aislador se emplea para impedir la propagación hacia fuera del EDFA del emisión espontánea (ruido ASE) que se genera y se propaga en sentido contrario al de la transmisión. El bombeo y la amplificación se realizan en el mismo sentido que la propagación. A la salida se coloca otro aislador que evita la entrada al EDFA y por tanto su amplificación de cualquier señal reflejada. Finalmente se emplea un filtro óptico para filtrar el ruido ASE,

generado en el amplificador, que se encuentre fuera de la banda de la señal útil.

La siguiente configuración se diferencia de la anterior en que la señal de bombeo se inyecta al EDFA en sentido contrario a la propagación. El aislador de la entrada además de cumplir las funciones anteriores, tiene la misión de evitar la propagación de la señal de bombeo fuera del amplificador. La ventaja de esta configuración es permite ganancias más altas, pero sus características de ruido son peores.

La tercera configuración es una combinación de las dos anteriores. Consiste en un doble bombeo, por lo que se denomina *bombeo dual o bidireccional*. La ganancia por tanto puede llegar a duplicarse. Este esquema es muy empleado en la implementación de amplificadores repetidores.

3.2.- Ganancia de un EDFA

La siguiente figura presenta la ganancia de un EDFA en función de la longitud de onda para diferentes valores de potencia de entrada, con una señal de bombeo a 1480nm.

El EDFA no presenta una ganancia uniforme con la longitud de onda. Debido a la saturación según crece la potencia de entrada la ganancia disminuye hasta llegar a un punto en que se mantiene constante. El máximo de ganancia se alcanza alrededor de los 1530-1535nm. Como puede verse en la figura a potencias altas la respuesta de la ganancia en todo el rango la banda C (1530-1565nm) es bastante plano lo cual no sucede a potencia de entrada más bajas. Esto es un grave inconveniente en los sistemas WDM, ya que no todos los canales se amplifican por igual.

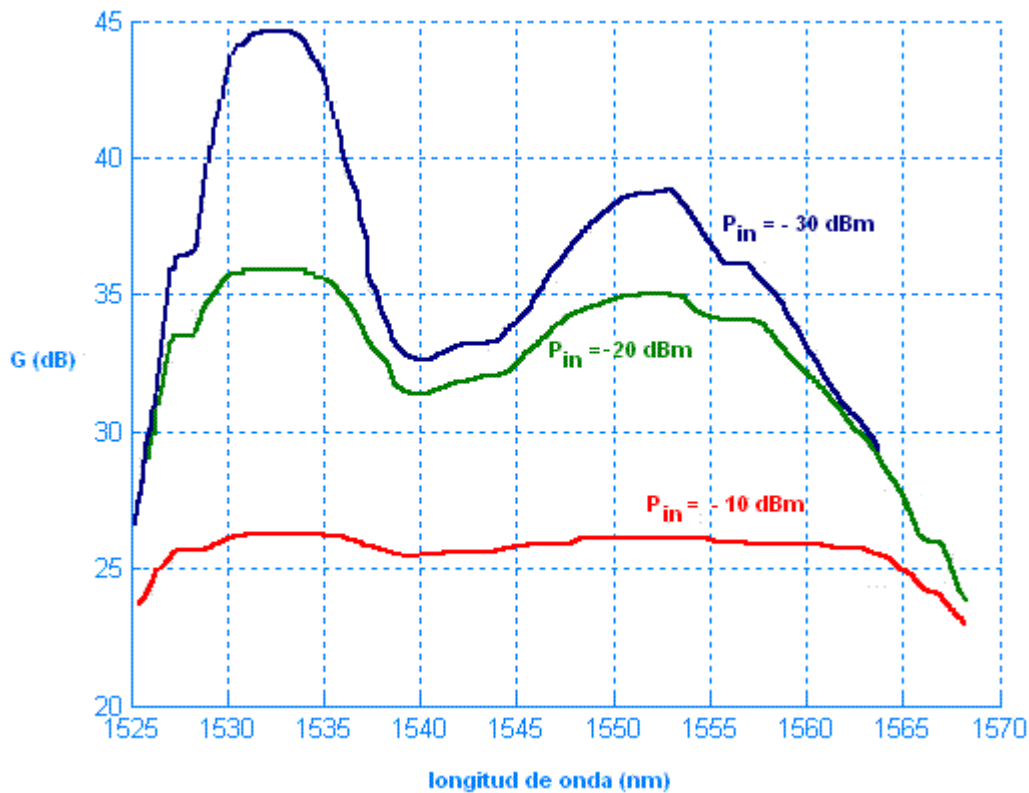


Figura 7: Representación de la ganancia de un EDFA respecto de la longitud de onda.

Las características técnicas que hacen del EDFA el amplificador más utilizado son:

- Como consecuencia de su geometría cilíndrica sus pérdidas de inserción en las uniones con la fibra óptica son muy reducidas.
- Debido también a su geometría su ganancia es poco sensible a la polarización de la señal.
- El ruido que genera es bajo.
- La saturación de la ganancia no ocasiona distorsión.

Su principal inconveniente es que sólo opera en la tercera ventana, aunque se existen dispositivos similares pero dopados con otros elementos que pueden operar en otra ventana. Otro problema es que su ganancia no es uniforme para todas las longitudes de onda, aunque esto se solventa trabajando cerca de su saturación, pues la curva de ganancia es más plana.

Longitud de onda de bombeo	1480 nm	980 nm
Eficiencia de bombeo (dB/mW)	5	10
Figura de ruido (dB)	5.5	3 – 4.5
Potencia de salida de saturación (dBm)	20	5
Ganancia (dB)	40	50
Potencia de bombeo (mW)	50 - 200	10 - 20

Tabla 1: Longitudes de onda de bombeo en un EDFA

3.3.- EDFA con caos

La demostración exitosa de la comunicación caótica en los circuitos electrónicos, allanó el camino para la exploración del caos óptico como candidato para las comunicaciones ópticas de seguridad. El caos óptico ha ganado mucha atención en la última década y varios esquemas prácticos basados en láseres de gas, así como los láseres semiconductores y los láseres de fibra dopada de erbio, han sido demostrados y comprobados con éxito en las comunicaciones seguras. También se ha logrado la recuperación de los mensajes que van desde pocos Kb/s hasta unos cuantos Gb/s con una señal aceptable a ruido en longitud de onda.

3.4.- Modelo matemático para la generación de caos usando un resonador de anillo de fibra óptica

En un resonador de fibra óptica, el cual es uno de los dispositivos ópticos principales, sus características fueron encontradas por primera vez por Ikeda, que Desde un punto de vista de interferencia óptica, un campo de entrada y los campos circulares con un cambio de fase no lineal, se superponen en el resonador, lo que da una dinámica complicada en una producción de interferencias. El modelo OFRR consiste en un anillo de fibra óptica y un acoplador de fibra.

Un campo de salida óptica en OFRR puede ser dado por la superposición entre la entrada de luz transmitida a través del acoplador y entre varios componentes circulares de la luz en el resonador.

Después, la salida del campo eléctrico de OFRR es escrita como:

$$E_{OUT} = i k (1 - \rho) E_{in}(t) + \sum_n (i^{n-1} (1 - \kappa) (1 - \rho)^{(n+1)/2} * E_{IN}(t - n\tau) * \exp(-n \alpha L/2) * \exp[-i(n\Phi + \sum_{l=1}^n \Delta \Phi(t - \tau))]) \quad (1)$$

Dónde j es el coeficiente de acoplamiento del acoplador de la fibra en el resonador, ρ es la pérdida del acoplador de fibra, α es la pérdida de la fibra en el anillo del resonador, L es la longitud del resonador de fibra de anillo, Φ es el cambio de fase lineal en el resonador, y $\Delta \Phi$ es el cambio no lineal de fase en el resonador, y está dado por:

$$\Delta \Phi = k L n_2 | E_t(t) | \quad (2)$$

k = número de onda de la entrada de luz en el vacío

$E_t(t)$ = luz que circula en el resonador

E_{in} = campo de entrada óptico, es dado por:

$$E_0 \exp \{ i \theta(t) \} \quad (3)$$

E_0 = amplitud del campo de entrada

$\theta(t)$ = representa la fluctuación de fase aleatoria que da lugar a la reducción de la coherencia de la luz que entra.

El poder de salida final del resonador de anillo puede expresarse como P_{OUT} , donde se representa el tiempo promedio del proceso. En la potencia de salida final, el factor de fase al azar, lleva a término la coherencia que está dada por:

$$\langle \exp \{ i[(\theta(t) - \theta(t - n\tau))] \} \rangle = \exp(-2p\nu n\tau) \quad (4)$$

Dónde:

$\theta(t)$ = es asumido como una variable obedeciendo el proceso aleatorio gaussiano.

El estado de coherencia de la luz de entrada es asumida para ser suficientemente alta, así que el poder de salida cambia en su estado estable a periódico; y finalmente a caótico, como el poder de entrada P_{IN} incrementa en el OFRR.

3.5.- Sincronización del caos en el transmisor y el receptor

Las comunicaciones ópticas con portadores caóticos requieren de una emisión de banda ancha caótica de dos láseres espacialmente separados, los cuales son sincronizados el uno del otro. La sincronización significa que la

evolución temporal irregular del láser emisor, por ejemplo, en la potencia óptica, puede ser perfectamente reproducido por el láser receptor. Una vez que los dos láseres han sido sincronizados, los mensajes pueden ser encriptados en el portador caótico.

El sistema receptor permite al mensaje encriptado ser extraído. La decodificación se basa en el fenómeno no lineal de la sincronización de caos entre el emisor y el receptor. Mediante la comparación de la entrada (portador + mensaje) y la salida (solo portador) del receptor, el mensaje se puede extraer. Debido a la alta sensibilidad del proceso de sincronización y la complejidad del portador, para lograr una eficaz decodificación se necesitan transmisores y receptores bien adaptados.

3.6.- Amplificación del caos en un EDFA

El caos generado por el resonador de anillo es amplificado por el EDFA en el final de transmisión. Existen diferentes parámetros tales como la longitud de la fibra, el poder de bombeo, la concentración de los iones de erbio, entre otros; los cuales afectan el rendimiento del EDFA. El objetivo es la optimización de estos parámetros de modo que podamos obtener un caos amplificado sin ningún cambio en su forma.

IMÁGENES DE UN EDFA REAL



Figura 8: EDFA, parte media frontal derecha



Figura 9: EDFA, parte media frontal izquierda

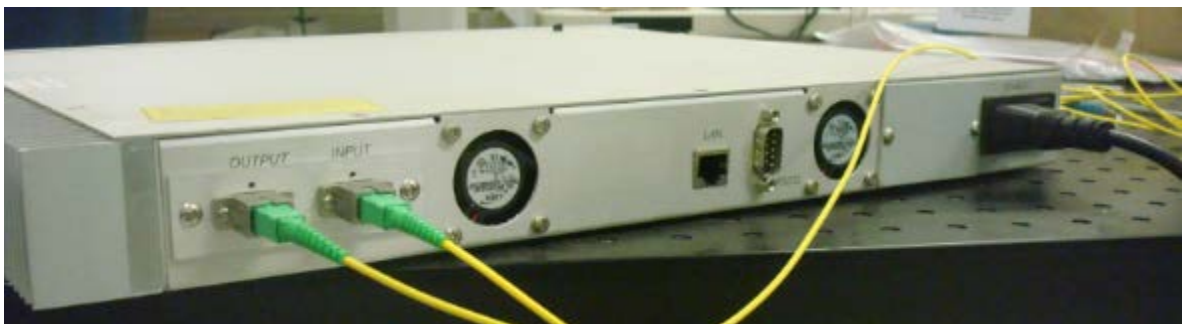


Figura 10: EDFA, parte trasera



Figura 11: EDFA, vista completa

REFERENCIAS

AMPLIFICADORES DE FIBRA ÓPTICA DOPADA CON ERBIO E ITERBIO (EDFAs y YEDFAs).

Autores: P. Martín-Ramos, J. Martín-Gil, P. Chamorro-Posada,.

Dpto. de Teoría de la Señal e Ingeniería Telemática, y Dpto. de Ingeniería Agrícola y Forestal, Universidad de Valladolid, Junio 2010.

<http://www.scribd.com/doc/33388581/Amplificadores-de-fibra-optica-dopada-con-Erbio-e-Iterbio-EDFAs-y-YEDFAs>

ERBIUM DOPED FIBER AMPLIFIERS

Autor: Dr. Rüdiger Paschotta, RP Photonics Consulting GmbH

Última edición: 2011-06-07

http://www.rp-photonics.com/erbium_doped_fiber_amplifiers.html

EDFA (ERBIUM DOPED FIBER AMPLIFIER) TUTORIAL

Autor: Exfiber Optical Technologies Co.,Ltd.

<http://www.exfiber.com/uploadfile/pdf/EDFA-Erbium-Doped-Fiber-Amplifier-Tutorial.pdf>

TUTORIAL DE COMUNICACIONES ÓPTICAS

Autor: Grupo de comunicaciones ópticas. 2006

http://nemesis.tel.uva.es/images/tCO/contenidos/tema2/tema2_8_2.htm

MODELING & SIMULATION OF ERBIUM DOPED FIBER AMPLIFIER (EDFA) FOR AMPLIFICATION OF OPTICAL CHAOS

Autor: EarnWrite. 2011

<http://www.earnwrite.com/articles/Science/Modeling+%26+Simulation+of+Erbium+Doped+Fiber+Amplifier+%28EDFA%29+for+Amplification+of+Optical+Chaos/239/>

SINCRONIZACIÓN DE REDES COMPLEJAS (Ref. THE ESSENCE OF CHAOS, Edward Lorenz). **Autores:** Belmonte Izquierdo Rubén, Noriega Urquidez David, Núñez Quintero Jesús Alberto. **Centro De investigación científica y de educación superior de Ensenada, B.C. (CICESE).** 18/Agosto/2006. Ensenada, B.C., México.



