UNIVERSIDAD AUTÓNOMA DE BAJA CALIFORNIA

Facultad de Ingeniería, Arquitectura y Diseño

Programa de Maestría y Doctorado en Ciencias e Ingeniería

ENCRIPTADO CAÓTICO BASADO EN MICROPROCESADOR CON COMUNICACIÓN Wi-Fi

TESIS

que para cubrir parcialmente los requisitos necesarios para obtener el grado de

MAESTRO EN INGENIERÍA

presenta:

ABRAHAM FLORES VERGARA

Director de tesis

Dr. Enrique Efren García Guerrero

Ensenada, Baja California, México. Octubre de 2013.

UNIVERSIDAD AUTÓNOMA DE BAJA CALIFORNIA

Facultad de Ingeniería, Arquitectura y Diseño

ENCRIPTADO CAÓTICO BASADO EN MICROPROCESADOR CON COMUNICACIÓN Wi-Fi

TESIS

que para obtener el grado de MAESTRO en INGENIERÍA presenta:

ABRAHAM FLORES VERGARA

Y aprobada por el siguiente comité:

Dr. Enrique Efren García Guerrero
Codirector del Comité

Dr. Everardo Inzunza González
Codirector del Comité

Dr. Oscar Roberto López Bonillar
Miembro del Comité

Dr. Juan Iván Nieto Hipólito
Miembro de Comité

MC. Sergio Omar Infante Prieto
Miembro del Comité

RESUMEN de la tesis de **Abraham Flores Vergara**, presentada como requisito parcial para obtener el grado de MAESTRO EN INGENIERÍA, del programa de Maestría y Doctorado en Ciencias e Ingeniería de la UABC. Ensenada, B. C. México, Octubre de 2013.

ENCRIPTADO CAÓTICO BASADO EN MICROPROCESADOR CON COMUNICACIÓN Wi-Fi

Resumen aprobado por:

Dr. Enrique Efren García Guerrero
Codirector de Tesis

Dr. Everardo Inzunza González
Codirector de Tesis

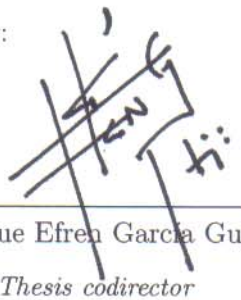
El presente trabajo de tesis propone un método para generar series caóticas e implementarlas en sistemas de comunicación con criptografía caótica, aplicando las técnicas de diseño con electrónica digital basadas en sistemas embebidos con microcontrolador. Se propone, una metodología de encriptado y desencriptado de señales analógicas y la aplicación del generador propuesto en un sistema de comunicación con canal público en RF; Se propone otra metodología para el encriptamiento y desencriptamiento de imágenes a color y en escala de grises con la aplicación del generador propuesto basado en un microcontrolador Rabbit RCM5600W en un sistema de comunicación con canal público en Wi-Fi. Para verificar la viabilidad de los métodos y prototipos propuestos, se realiza el correspondiente análisis con base en los conceptos de: espacio de claves, entropía de información e histograma.

Palabras clave: Generador digital de caos, encriptado caótico, comunicaciones inalámbricas seguras, microprocesador.

ABSTRACT of the thesis of **ABRAHAM FLORES VERGARA**, presented as a partial requirement to obtain the degree of MASTER in ENGENIEERING, of the program of MSc and PhD in Sciences and Engineering of UABC. Ensenada, B. C., Mexico, October 2013 2013.

CHAOTIC ENCRYPTION BASED ON MICROPROCESSOR WITH Wi-Fi COMMUNICATION

Abstract approved by:



Dr. Enrique Efren García Guerrero
Thesis codirector

Dr. Everardo Inzunza González
Thesis codirector

This thesis work presents a method to generate chaotic series in order to be implemented in a secure communication system by using chaotic cryptography. The above, by using design techniques with embedded systems microcontroller-based. Specifically this work presents a methodology to encrypt-decrypt analogical signals with the chaos generator application proposed in a communication system with RF public channel. This work too, proposes a methodology to encrypt-decrypt color images and gray scale images with the chaos generator application in a communication system with Wi-Fi public channel by using the microcontroller Rabbit-5600W. To verify the viability of the methods and prototypes presented an analysis based on the concepts of entropy, key space and histogram is performed.

Keywords: Digital generator of chaos,chaotic encryption, secure wireless communications, microprocessor.

A mis hijos: José Eduardo, Abraham e Isaac

Agradecimientos

*A **DIOS**, por tenerme siempre bajo su protección y por todas las bendiciones que me ha dado todos los dias de mi vida.*

*Al **Dr. Enrique Efrén García Guerrero**, por haberme dirigido en la realización del presente trabajo de tesis de maestría, por su amistad, la atención y el apoyo incondicional que me ha brindado.*

*Al **Dr. Everardo Inzunza González**, por su amistad, atención y por sus enseñanzas que me permitieron desarrollar con éxito el presente trabajo de tesis de maestría.*

*Al **Dr. Juan Iván Nieto, Dr. Oscar Roberto López Bonilla, MC Sergio Omar Infante Prieto**, un especial agradecimiento por sus comentarios muy acertados en las presentaciones y revisiones del presente trabajo de tesis de maestría.*

*A mi madre **Margarita Vergara Ávila**, sin tu apoyo no hubiese hecho realidad este sueño. Â¡Gracias por todo mamá!.*

*A mis **hermanos(a), Ma del Rosario, Cecilia, Vicente, Juan, Humberto, Juan Ramon, Lidia** , por ser ejemplos de vida, por su apoyo y sus consejos.*

*A mi amigo **Victor Manuel Maldonado Lopez.** un especial agradecimiento por su valiosa amistad y apoyo incondicional. Â¡Gracias amigo!.*

*A mis amigos **José Juan Villegas Leon y familia.**, Â¡Gracias por su amistad y su apoyo amigos!.*

*Al **CONACyT**, que con su programa de becas me proporcionaron los recursos necesarios durante esta etapa importante en mi vida profesional.*

*A nuestra alma mater: **Universidad Autónoma de Baja California**, que es como mi segundo hogar y donde se me ha permitido desarrollarme profesionalmente.*

*Al **coordinador de posgrado**, Dr. Juan de Dios Sánchez, por sus asesorías administrativas.*

Ensenada, B. C. México. ABRAHAM FLORES VERGARA
de Octubre de 2013.

Tabla de Contenido

Página

Tabla de Contenido (Continuación)

Tabla de Contenido (Continuación)

Página

Lista de figuras

Lista de figuras (Continuación)

Lista de figuras (Continuación)

Lista de tablas

Capítulo I

Introducción

El hombre, desde sus orígenes, además de la necesidad de comunicarse a corta y a larga distancia ha tenido la premura de que en muchos casos sea de manera secreta y segura. En la actualidad, existe una grán variedad de servicios y aplicaciones electrónicas modernas que realizan intercambio de información confidencial, que entre otras podemos mencionar: transacciones bancarias por Internet, sistemas de acceso a zonas restringidas, sistemas de TV satelital o por cable, etc. Si bien es cierto que existen en la actualidad métodos que garantizan la confiable transmisión de información privada, el avance y evolución en el desarrollo de tecnología computacional con el tiempo les adiciona cierto grado de vulnerabilidad; tal es el caso del método utilizado por los Estados Unidos como un estandar federal de procesamiento de información (FIPS, de sus siglas en inglés) llamado DES (Data Encryption Standard) que, en 1998 fue comprometida su seguridad y se logró romper una clave en 56 horas y, un año después, se logró romper una clave en 22 horas 15 min (EFF, 1998).

El presente trabajo de tesis trata sobre la aplicación de la criptografía caótica digital como método con aproximación a incondicionalmente seguro, en sistemas de comunicación a través de un canal público. Se propone una metodología de protección de información confidencial en sistemas de comunicación inalámbrica, desde la perspectiva de las técnicas de diseño con electrónica digital en sistemas embebidos. Los sistemas embebidos, a diferencia de los sistemas computacionales de oficina o Laptop, solucionan problemas específicos y están dispersos en muchos de los ambientes posibles de

la vida cotidiana, como por ejemplo: equipos celulares, agendas de bolsillo, cajeros automáticos, cámaras fotográficas, equipo médico, electrodomésticos, juguetes, entre muchos otros (Galeano, 2009).

En este trabajo de tesis, abordamos el problema del encriptado digital de información confidencial en sistemas embebidos de comunicación inalámbricos, de forma progresiva y por etapas:

- En la primera etapa, se desarrolla e implementa un método para generar señales caóticas mediante el uso de un microcontrolador (μC) PIC16F877A.

- En la segunda etapa, se implementa una metodología para el envío de señales analógicas de manera segura (encriptadas) en un sistema de comunicación inalámbrico en RF (Radio Frecuencia, 3KHz a 300GHz), utilizando el generador caótico basado en el μC PIC16F877A.

- Por último, se implementa un sistema de comunicación inalámbrico vía WiFi (Wireless Ethernet Compatibility), aplicado a imagenes digitales a color y en escala de grises encriptadas caóticamente, empleando como generador de señales caóticas a un microprocesador Rabbit RCM5600W.

I.1 Motivación

Derivada del crecimiento y evolución de los sistemas de comunicación actual y la acelerada proliferación y uso en todo el mundo de diversos sistemas de telecomunicación, surge la necesidad de servicios y aplicaciones que garanticen seguridad en el almacenamiento y en la transmisión de la información confidencial. Como por ejemplo, con el

crecimiento de las transferencias electrónicas de información, surge la necesidad de proteger dichos datos y asegurar su integridad. Dos técnicas para llevar a cabo de manera secreta y segura una comunicación y que han venido posicionandose en años recientes son: la esteganografía y la criptografía.

La esteganografía es una disciplina que estudia las comunicaciones seguras y secretas, de tal forma que, un probable intruso ni siquiera sabe que se está transmitiendo información; como ejemplo de ello se puede citar: las tintas invisibles, las marcas de agua en las imágenes y los hologramas, entre otros mas. La criptografía se utiliza para modificar el mensaje de manera que sea ininteligible para un probable intruso, auque éste, tenga el conocimiento de su existencia.

El uso de la criptografía se ha extendido en aplicaciones dentro de la comunicación digital. En tiempos recientes, dos aplicaciones donde se utilizan ampliamente las técnicas y los métodos estudiados por la criptología son: la protección de información digital almacenada o más conocidas como bases de datos y la comunicación segura por canales públicos (comunicaciones digitales seguras). Dentro de las técnicas modernas criptográficas se encuentran los estandares DES (FIPS, 1977), LUCIFER (Sorking, 1984), FEAL (Fast Data Encipherment Algorithm) (Shimizu y Mitaguchi, 1988) y el actual AES (Advanced Encryption Standard).

En la actualidad, los métodos estandarizados para realizar comunicaciones seguras han caido en cierto grado de vulnerabilidad debido al crecimiento en el desarrollo de poder computacional y se han logrado romper claves para descifrar información confidencial. Por lo anterior, es necesario desarrollar nuevos métodos y técnicas de protección de información confidencial que garanticen la máxima seguridad. El avance tecnológico en el desarrollo de dispositivos electrónicos para el procesamiento de datos

e información, como lo son los microcontroladores, microprocesadores avanzados en sistemas embebidos y más recientemente los FPGA's (Field Programmable Gate Array), nos brindan la posibilidad de desarrollar nuevos métodos y técnicas para resolver los problemas derivados de las necesidades de la comunicación segura.

Por otra parte, en las últimas decadas, comunidades de investigadores han centrado sus atención en el estudio y aplicación de la teoría del caos. Después de muchos estudios teóricos e investigación experimental se reconoce que el caos es útil en muchas aplicaciones y se ha incrementado el interés por utilizarlo en diversas disciplinas. La razón principal por el interés en el caos, se debe a su complejidad y a su comportamiento dinámico muy parecido al ruido, comportamiento adecuado para incorporarse a los diseños electrónicos digitales de sistemas de protección de información confidencial, objetivo central de este trabajo de tesis.

I.2 Planteamiento del problema

I.2.1 Descripción del problema

La transmisión de información privada de manera segura por canales de comunicación públicos, o bien, el almacenamiento de la información confidencial son problemas abiertos y a los que se enfrenta la humanidad hoy en día. Una forma de proteger o resguardar dicha información es mediante el uso de criptografía. El presente trabajo de tesis propone diseñar, implementar y validar un sistema de comunicación basado en electrónica digital conjuntamente con criptografía caótica para transmitir, de forma segura, información confidencial por un canal inalámbrico. Más específicamente se propone la puesta en operación de un transmisor y un receptor basados en microprocesadores en sistemas embebidos, que utilicen criptografía caótica para enviar de manera secreta

y segura información visual plasmada en imágenes digitales a través de un canal de comunicación inalámbrica en RF, o vía WiFi. En la figura 1 se representa el sistema de comunicación segura por un canal público, en donde el transmisor envia un mensaje M encriptado utilizando un canal de comunicación inalámbrico; el mensaje lo recibe un receptor que aplica un método inverso al del transmisor para su recuperación. Se observa también un intruso, el cual, si no aplica el mismo método que el receptor, no logra recuperar el mensaje.

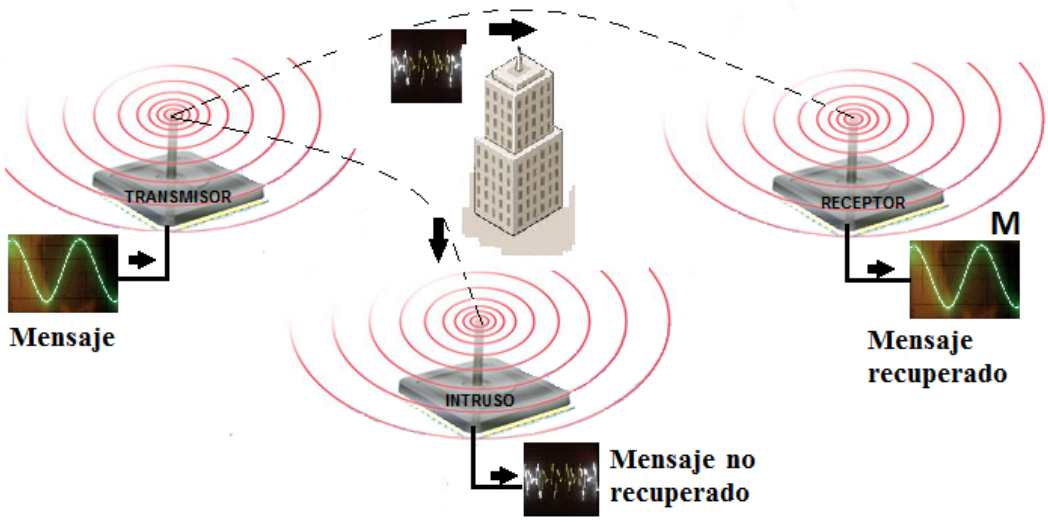


Figura 1: Sistema de comunicación segura por canal inalámbrico.

I.2.2 Preguntas de investigación

- ¿Cómo generar caos mediante la implementación de mapeos caóticos, ampliamente documentados en la literatura, desde la perspectiva de la electrónica digital y el uso del μC PIC16F877A en un sistema embebido, para su aplicación en las comunicaciones seguras?

- ¿Cómo encriptar y desencriptar una señal analógica mediante criptografía caótica

con un generador digital de caos a base del μC PIC16F877A en un sistema embebido, utilizando el canal inalámbrico de comunicación en RF?

- ¿Cómo encriptar y desencriptar una imagen a color o en escala de grises, mediante criptografía caótica con un generador digital en base al microprocesador Rabbit RCM5600W en un sistema embebido, utilizando el canal inalámbrico de comunicación WiFi?

I.2.3 Delimitación del problema

Delimitación geográfica

En los sistemas de comunicacón a distancia se estudian redes de comunicación inalámbrica clasificadas segun su alcance dentro de las cuales se encuentran: las redes de área personal, de área local y de área amplia; el proyecto tiene delimitación a nivel mundial con la aplicación del envío del criptograma (información encriptada) a través de Internet.

Delimitación de tecnología

- Utilización de sistemas empotrados basados en microcontrolador PIC 16F877A de Microchip Inc. y microprocesador RCM5600W de Rabbit semiconductor Inc. y sus complementos para realizar el desencriptado de un mensaje digital previamente encriptado mediante critografía caótica.

- Utilización del canal inalámbrico de comunicación en RF mediante módulos de comunicación con tecnología ZigBee para ser utilizados con el μC 16F877A y módulos de comunicacion inalámbrica Wi-Fi incluido en microprocesador RCM5600W.

- La información en forma digital son: imágenes a color en composición RGB (Red Green Blue) e imágenes en escala de grises, procesadas mediante una computadora

personal PC (de sus siglas en inglés) y señales analógicas proporcionadas por un generador de funciones analógicas de laboratorio.

- Bloques de conversión Analógica-Digital (ADC) y Digital-Analógico (DAC). ADC incluido en microcontrolador PIC16F877A, DAC MCP4921 de Microchip Inc. o DAC0800 de National Semiconductor.

Delimitación de usuarios

En este proyecto se propone la implementación de un sistema embebido que transmita un criptograma, otro que lo reciba para desencriptar y obtener el mensaje original y un tercer usuario que realice criptoanálisis utilizando el mismo canal de comunicación inalámbrico en RF o WiFi.

I.3 Metodología

La figura 2 muestra el esquema a bloques de la propuesta de solución y se describe cada bloque a continuación:

- **Información digital (M):** representa una imagen a color en composición RGB o una imagen en escala de grises, para ambos casos en formato PNG (Portable Network Graphics), a ser enviada caóticamente encriptada a través de un canal inalámbrico y público de comunicación.

- **Información analógica (M):** representa una señal, como por ejemplo, senoidal, cuadrada, triangular y diente de sierra, a ser enviada caóticamente encriptada a través de un canal inalámbrico y público de comunicación.

- **ADC:** Cuando el mensaje a encriptar es una señal analógica, se añade un bloque de conversión Analógico-Digital en el transmisor a fin de que el mensaje llegue al bloque de encriptamiento caótico en formato digital.

- **Generación de señales caóticas:** En esta etapa se implementa el sistema caótico para la generación del caos. Los sistemas caóticos a considerar son mapeos ampliamente estudiados y documentados en la literatura de los cuales podemos citar: el de Tinkerbell (Shaoliang y Jiang, 2011), Logistic 2D (Verhulst, 1845), de Chen (Chen, 2001), de Ikeda (Ikeda y Daido, 1980), entre otros.

- **Encriptamiento caótico:** En esta etapa se implementa el método para el encriptado de la información con la señal caótica generada.

- **RF/WiFi:** Para el envío del criptograma se considera el canal de comunicación inalámbrica en RF o vía WiFi. Dos formas de realizar la comunicación son: en su modalidad de comunicacón punto a punto o mediante la infraestructura de la red de Internet.

- **Desencriptado caótico:** En esta etapa se implementa el algoritmo inverso de encriptamiento para la recuperación del mensaje digital.

- **DAC:** Bloque de conversión Digital-Analógico para el caso en el que el mensaje a recuperar sea una señal analógica.

- **Información recuperada ($\hat{M}$):** representa la recuperación de la información una vez desencriptada, es decir, la correspondiente a la información digital de entrada o a la información analógica.

I.4 Objetivos del proyecto

I.4.1 Objetivo general

Implementar un dispositivo electrónico como generador de señales caóticas, desde la perspectiva del diseño electrónico digital y sistemas embebidos, para el encriptado caótico

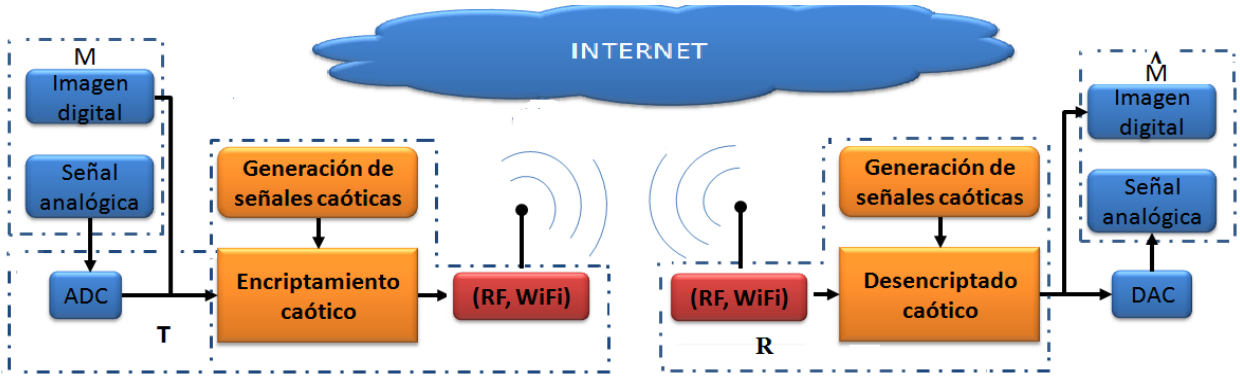


Figura 2: Esquema a bloques del proyecto propuesto.

de información aplicado a sistemas de comunicación inalámbrica.

I.4.2 Objetivos específicos

- Implementar un generador digital de señales caóticas basado en un μC PIC16F877A.
- Implementar un dispositivo electrónico digital de encriptado caótico basado en un μC PIC16F877A.
- Implementar un dispositivo electrónico digital de desencriptado caótico basado en un μC PIC16F877A.
- Implementar un dispositivo electrónico digital basado en un μC PIC16F877A en un sistema embebido, con módulos de comunicación inalámbrica de tecnología ZigBee, para la transmisión de información encriptada caóticamente.
- Implementar un dispositivo electrónico digital basado en el microprocesador RCM5600W, con comunicación vía WiFi, para la transmisión de información encriptada caóticamente.

I.5 Organización de la tesis

El presente trabajo de tesis se organiza de la siguiente manera. En el **capítulo II** se presenta un marco teórico relacionado con los conceptos generales de criptografía y la teoría del caos. En el **capítulo III** se presenta la implementación de la metodología propuesta para la generación de caos desde la perspectiva de la electrónica digital y el uso de microcontroladores PIC tipo RISC. En el **capítulo IV** se presenta la implementación de una metodología de encriptado y desencriptado de señales analógicas mediante el uso de caos generado por microcontroladores, aplicado a un sistema de comunicación inalámbrica en RF. En el **capítulo V**, se presenta la implementación de una metodología de encriptamiento de imágenes a color y en escala de grises mediante el uso de caos generado por el microprocesador Rabbit RCM5600W y su aplicación en un sistema de comunicación inalámbrica vía WiFi. En el **capítulo VI** se presentan los resultados experimentales de las tres metodologías propuestas e implementadas para la generación y aplicación de las señales caóticas generadas en base al diseño electrónico digital. Finalmente, en el **capítulo VII** se dan las conclusiones generales de nuestro trabajo de tesis y planteamos posibles líneas de investigación para trabajos a futuro.

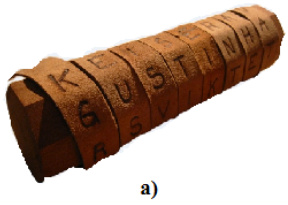
En el **apéndice A** se incluye información sobre la configuración de los módulos de comunicación RF utilizada en este trabajo. En el **apéndice B** se incluye información del ensamble y la configuración del sistema Rabbit RCM5600W. En el **apéndice C** se incluyen las publicaciones derivadas del presente trabajo de tesis y las publicaciones en colaboración.

Capítulo II

Marco Teórico

II.1 Criptografía

La palabra criptografía segun la Real Academia Española (RAE) proviene de los vocablos griegos "kryptos"que significa oculto y "graphos"que significa escribir y se utiliza para nombrar una de las disciplinas de la ciencia de la criptología que se ocupa del diseño de procedimientos para cifrar o enmascarar una determinada información de caracter confidencial. En ocasiones se emplean los verbos encriptar y cifrar como sinónimos, así como sus respectivas contra partes desencriptar y descifrar; al mensaje cifrado se le conoce como criptograma. Cada civilización, a su manera, ha desarrollado y utilizado formas o métodos secretos para mantener incomprensibles textos que, de alguna manera, comprometían su permanencia. La criptografía, como medio para proteger la información confidencial, es entonces un arte tan antiguo como la propia escritura (Fuster *et al.*, 2001).



a)

Original	a	b	c	d	e	f	g	h	i	j	k	l	m
Cifrado	d	e	f	g	h	i	j	k	l	m	n	o	p

Original	n	o	p	q	r	s	t	u	v	w	x	y	z
Cifrado	q	r	s	t	u	v	w	x	y	z	a	b	c

b)

Figura 3: Criptografia clásica: a) escitala, b) cifrado Julio César

II.1.1 Orígenes de la criptografía

En el período 3500-4000 a.C. los sumerios desarrollaron la escritura cuneiforme y los egipcios la escritura jeroglífica. La escritura cuneiforme sumeria es la más vieja lengua escrita conocida de la historia humana y no fue descifrada hasta el siglo XIX. Se han encontrado jeroglíficos escritos con pluma y tinta sobre papiros pintados o grabados sobre piedra, consistiendo este lenguaje en más de 750 signos diferentes.

En el período 500-600 a.C los escribas hebreos, utilizaron el alfabeto inverso conocido como cifrado ATBASH, que consistía en sustituir la primera letra del alfabeto hebreo por la última y la segunda letra por la penúltima y así sucesivamente. Más tarde, en 486 a.C. los antiguos griegos inventaron la escitala, una especie de bastón envuelto con estrechas tiras de pergamino; el mensaje se escribía longitudinalmente en la tira envuelta en un baston, después, el baston se removía quedando una tira con un mensaje incomprensible y se entregaba al mensajero; solamente si el receptor tenía un bastón del mismo diámetro podía leer el mensaje. Entre los años 50-60 a.C. se inventó un encriptado conocido como cifrado Julio César, simple y extensamente aplicado por sus técnicas conocidas de encriptado; cada letra del texto era sustituida por una letra sobre un determinado desplazamiento numérico del alfabeto; por ejemplo, un desplazamiento de 4 movería la A a D, B a E, etc.; fue llamado así debido a que Julio César lo empleaba durante sus campañas militares, ver figura 3.

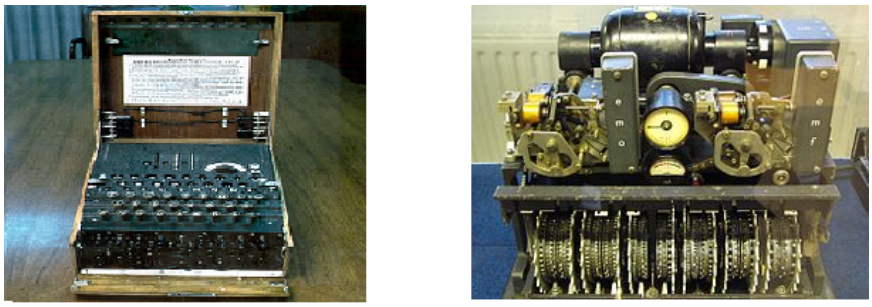
II.1.2 Criptografía clásica

Al cifrado Julio César le siguieron otros métodos, todos bajo los principios de la sustitución o la transposición y, en la actualidad a este proceso se le conoce como criptografía clásica, la cual se describe a continuación:

- **Métodos por sustitución:** consisten en establecer una correspondencia entre las letras del alfabeto del mensaje original y los elementos de otro conjunto, pudiendo ser los del mismo alfabeto, ejemplo de estos se puede citar: el cifrado Julio César, el cifrado Vigenere en 1586, el cifrado Beaufort en 1710, el cifrado Vernam en 1917, entre otros. Particularmente el cifrado Vernam, emplea un alfabeto binario haciendo uso del código Baudot, la operacion aritmética de cifrado es una suma módulo 2 y como clave, una secuencia binaria pseudoaleatoria de la misma longitud que el texto claro.

- **Métodos por transposición:** consisten en desordenar los símbolos del mensaje original colocándolos en un orden distinto, de esta forma, el criptograma contenía los mismos símbolos pero ordenados de tal forma que resultan incomprensibles, por ejemplo, la escitala, ver figura 3.

Hacia el año 1000 d.C. el análisis de frecuencia conduce a técnicas para el descifrado monoalfabético por sustitución, muy probablemente debido al análisis de textos del Corán; se basaba en el hecho de que cualquier lenguaje, letras y combinaciones de letras ocurren en diferentes variaciones de frecuencia. En una distribución frecuencial típica correspondiente a un texto de 10 000 letras en inglés y en castellano, en inglés la letra E es la más común y la Z es la más rara, mientras que en el castellano la más común es la letra E. El análisis de frecuencia fue el avance de criptoanálisis más importante hasta la segunda guerra mundial, casi todos los métodos por sustitución quedaron vulnerables. En 1918 Arthur Scherbius, ingeniero alemán, inventó la máquina Enigma que mediante un teclado de 26 letras, un tablero de 26 bombillas luminosas, una unidad de 26 discos o rotores, un clavijero y un reflector, cifraba mensajes con una técnica avanzada para ese tiempo hasta la llegada de la computadora. Las máquinas Lorenz sz40 y sz42, eran también máquinas de cifrado alemanas, ver figura 4.



a) b)

Figura 4: Máquinas de cifrado Alemanas: a) máquina enigma, b) máquina Lorenz sz40.

II.1.3 Métodos modernos de cifrado

Después de la segunda guerra mundial, en 1949, Claude E. Shannon proporciona fundamentos teóricos sobre las "condiciones de secreto perfecto"(Shannon, 1949). Con el avance de la tecnología computacional en combinación con métodos matemáticos, el desarrollo de la criptografía de clave secreta dió lugar a dos nuevas metodologías de cifrado: cifrado en flujo y cifrado en bloque. El cifrado en flujo utiliza generadores pseudoaleatorios de secuencia cifrante, de entre los cuales se encuentran: generador de Geffe, generador en cascada de Gollmann, generadores de caos, entre otros. Como ejemplo de cifrado en bloque podemos citar el cifrado DES (FIPS, 1977) y el FEAL (Shimizu y Mitaguchi, 1988).

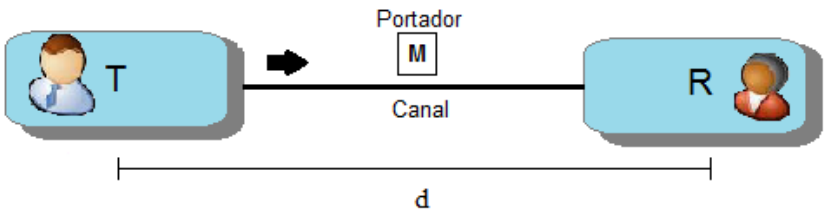


Figura 5: Sistema básico de comunicación remota.

II.2 La criptografía y los sistemas de comunicación segura

En el ámbito de las comunicaciones al elemento que transmite información se le conoce como **transmisor** (T), al elemento que recibe la información se le llama **receptor** (R), a la información que se transmite se le conoce como **mensaje** (M), al medio por el cual el mensaje viaja se le llama **canal** de comunicación (Canal) y, al elemento que lleva propiamente el mensaje a través del canal de comunicación hacia al receptor se le conoce como **portador** (P). Cuando se trata de comunicaciones distantes (d) nos referimos a comunicaciones remotas, en la figura 5, se presenta una representación gráfica de un sistema de comunicación remota.

En las comunicaciones remotas, uno de los objetivos es el lograr la transmisión de información segura. En el estudio de las comunicaciones seguras, se considera un elemento adicional que puede interceptar al portador de la información privada, a través del canal de comunicación y obtener el mensaje antes de que este llegue al receptor, comprometiendo así, la seguridad en la comunicación. Este elemento comúnmente se le denomina **intruso** (I). La criptografía surge entonces con la finalidad de enmascarar un mensaje confidencial a través de un proceso de encriptado, de modo que sea incomprensible a toda persona distinta al destinatario en caso de que sea interceptada del canal comunicación.

En la figura 6 se hace una representación gráfica del concepto de comunicación segura utilizando criptografía. El trasmisor (T) envía un mensaje (M) al receptor (R) remoto. Al mensaje (M) antes de ser enviado, se le aplica un proceso de cifrado o encriptado, lo cual en principio, lo hace incomprensible para cualquier intruso (I). Éste mensaje cifrado se le conoce como **criptograma** (C) y es el que viaja por el canal de

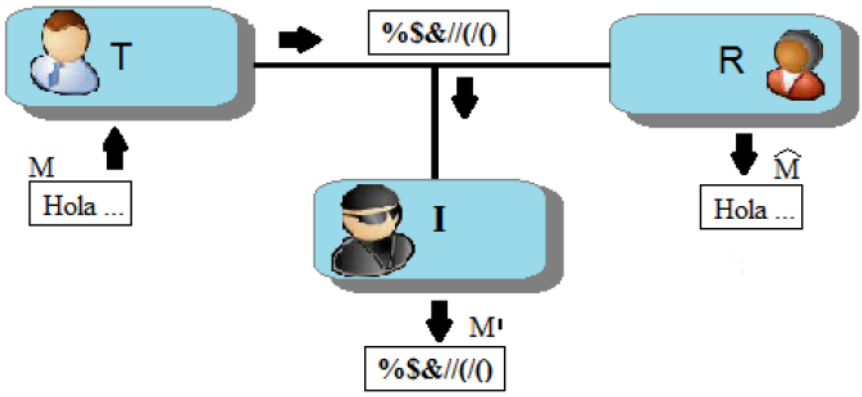


Figura 6: Sistema de comunicación segura

comunicación. En el receptor (R), el criptograma (C) pasa por un proceso de desencriptado (proceso inverso al de encriptado) del cual se obtiene o se recupera el mensaje original ($\hat{M}$), para que finalmente se interprete la información original por parte del receptor (R). En el diagrama, se muestra también al intruso (I) cuya función es la de obtener el mensaje (M') contenido en el criptograma (C). A la acción del intruso (I) de intentar obtener el mensaje se le conoce como Criptoanálisis. El objetivo de la comunicación segura es que $M = \hat{M}$ y que $M \neq M'$ durante todo el proceso propio de la comunicación. Es importante mencionar que en la criptografía, para la etapa de cifrado y la de descifrado, se lleva acabo a partir de un algoritmo y un elemento fundamental conocido como llave o clave de cifrado (k). De esta forma, podemos plantear la función $E = E(M, k)$ donde E es la función de cifrado del mensaje (M) a partir de la clave (k), y una función inversa de descifrado $D = D(C, k)$, donde D es la función de descifrado; inversa a $E = E(M, k)$, del criptograma (C) con la clave (k).

II.2.1 Seguridad criptográfica y el secreto perfecto de Shannon

Una primera clasificación de los métodos criptográficos con base en las claves utilizadas se puede describir como sigue:

- **Criptografía con clave simétrica:** es el método criptográfico que utiliza la misma clave (k) en el cifrado y en el descifrado. Luego entonces, la clave tiene que permanecer secreta, lo cual presupone que tanto el emisor como el receptor se han puesto de acuerdo previamente en la determinación de la misma. Este tipo de métodos son propios de la criptografía clásica (Diffie y Hellman, 1976).

- **Criptografía con clave asimetrica:** es el método criptográfico que utiliza claves (k) diferentes en el cifrado y en el descifrado. Generalmente, la clave para cifrar es conocida libremente, mientras que la clave para descifrar es conocida solamente por el receptor. Estos métodos son propios de la criptografía de clave pública (Diffie y Hellman, 1976).

La principal diferencia entre los métodos clasicos y los métodos que se utilizan en la actualidad radica en el concepto de seguridad. En la antigüedad, los métodos criptográficos contaban con una seguridad "probable", a diferencia de los métodos criptográficos modernos, que deben tener una seguridad matemáticamente demostrable; de lo anterior se establece una primera clasificación de seguridad criptográfica (Fuster *et al.*, 2001):

- **Seguridad incondicional (teórica):** el sistema es seguro frente a un atacante con tiempo y recursos computacionales ilimitados, ejemplo: cifrado Vernam (Fuster *et al.*, 2001).

- **Seguridad computacional (práctica):** el sistema es seguro frente a un atacante con tiempo y recursos computacionales limitados, ejemplo: sistemas de clave asimétrica basados en problemas de alta complejidad de cálculo (Fuster *et al.*, 2001).

- **Seguridad probable:** no se puede demostrar su integridad, pero el sistema no ha sido violado (Fuster *et al.*, 2001).

- **Seguridad condicional:** todos los demás sistemas, seguros en tanto que el enemigo carece de medios para atacarlos (Fuster *et al.*, 2001).

Los expertos en criptografía creyeron en la seguridad total del método de Vernam, pero el primero en proporcionar pruebas teóricas sobre la seguridad total fue Claude Shannon en 1994. Shannon definió sus condiciones de secreto perfecto partiendo de dos hipótesis básicas:

1. La clave secreta se utiliza solamente una vez.

2. El enemigo criptoanalista tiene acceso sólo al criptograma, después, se limita a atacar el texto cifrado únicamente.

A partir de la cuales, se enuncian sus condiciones que se describen a continuación.

Un sistema criptográfico verifica las condiciones de secreto perfecto si el texto claro X es estadísticamente independiente del criptograma Y, lo que en lenguaje de probabilidad puede expresarse como:

$$P(X = x|Y = y) = P(X = x), \tag{1}$$

para todos los posibles textos fuente $x = (x_1, x_2, ..., x_M)$ y todos los posibles criptogramas $y = (y_1, y_2, ..., y_N)$, es decir, la probabilidad de que la variable aleatoria X tome el valor de x es la misma, con o sin conocimiento del valor tomado por la variable aleatoria Y.

Asimismo, y basado en el concepto de entropía, determina la menor cantidad de clave necesaria para que pudieran verificarse las condiciones de secreto perfecto. La

longitud de la clave K debe ser igual o mayor a la longitud del texto claro.

$$K \geq M. \tag{2}$$

Esta desigualdad se convierte en igualdad para el caso del cifrado Vernam.

Se verifica entonces de lo anterior que, el cifrado Vernam cumple con las condiciones de secreto perfecto definidas por Shannon y se clasifica como el único procedimiento de cifrado incondicionalmente seguro. Sin embargo, presenta el inconveniente de que se requiere de un bit de enmascaramiento por cada bit de mensaje. Por lo que, teniendo en cuenta las exigencias actuales de información a cifrar, se tiene que el método no es viable; debido a que al hacer llegar tal cantidad de bits del emisor al receptor por un canal de comunicación se desbordaría la propia capacidad del canal. En la práctica se utiliza el método de cifrado en flujo el cual se describe a continuación (Fuster *et al.*, 2001).

II.2.2 Cifrado en flujo

El cifrado en flujo es una aproximación al cifrado Vernam. El método utiliza generadores pseudoaleatorios de secuencias cifrantes, es decir, mediante la implementación de algoritmos determinísticos que, a partir de una clave secreta conocida únicamente por el emisor y el receptor autorizado, generan simultáneamente en uno y otro, una determinada secuencia cifrante de una longitud deseada, haciendo las veces de la clave en el cifrado Vernam. Debido a que estas secuencias son generadas por una maquina de estados finitos, a partir de un algoritmo determinístico, núnca podrán ser autenticamente aleatorias (Fuster *et al.*, 2001). A estas secuencias que se intentan sean lo más posiblemente semejantes a secuencias aleatorias, se les denomina secuencias pseudoaleatorias o caóticas. En la figura 7, se muestra un diagrama a bloques del proceso de cifrado en flujo.

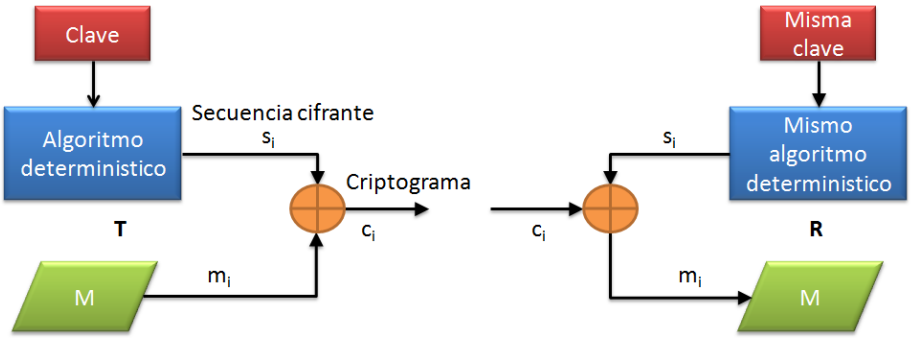


Figura 7: Método de cifrado en flujo.

II.3 Criptoanálisis

Mientras que la criptografía se encarga del estudio de los métodos para encriptar información confidencial, el criptoanálisis se encarga del estudio de cómo romper estos métodos de cifrado y descubrir la información original. El criptoanálisis esta ligado implicitamente al método de cifrado, ya que, al diseñarse un método de cifrado se tienen en cuenta los posibles ataques que este pueda sufrir, cada prodedimiento de encriptado que se implementa, en el diseño se está correspondiendo a un hipotético procedimiento de ataque o ruptura (Fuster *et al.*, 2001).

II.3.1 Espacio de claves y el ataque de fuerza bruta

Las posibilidad de que un criptoanálisis tenga éxito en el ataque o ruptura de un sistema de cifrado, tiene una fuerte dependencia de la información con la que dispone el criptoanálista y de las circunstancias que lo rodean. Luego entonces, el atacar un sistema de cifrado desconocido demanda un mayor esfuerzo que el ataque a un sistema conocido. Si el sistema es conocido, existe un primer ataque que se enfoca en probar el número total de claves posibles que admite el sistema de cifrado llamado **espacio de claves**, este ataque se le conoce como **de fuerza bruta** (Fuster *et al.*, 2001).

II.3.2 Entropía de la información

La información se mide en "unidades de información"(Abramson, 1981). Sea E un suceso que puede presentarse con la probabilidad $P(E)$, cuando E tiene lugar, se dice que se ha recibido.

$$I(E) = log\frac{1}{P(E)} \qquad \text{[unidades de información/símbolo].} \tag{3}$$

Si la base del algoritmo es la natural, la unidad de información tiene el nombre de *nat*, mientras que si la base es 10 se le conoce como *hartley*, y si la base es 2 se denimona *bit*.

La entropia $H(S)$ de una fuente de información se define como la cantidad media de información por símbolo emitido por ella. Matemáticamente se define como (Fuster *et al.*, 2001):

$$H(S) = \sum_{s} P(s_i) log_2 \frac{1}{P(s_i)} \qquad \text{[bits/símbolo],} \tag{4}$$

en donde $P(s_i)$ es la probabilidad de ocurrencie del símbolo s_i.

Para una fuente puramente aleatoria que esta emitiendo 2^N símbolos con la misma probabilidad de ocurrencia, despues de evaluar la ecuación 4, se tiene que:

$$H(S) = N \qquad \text{[bits/símbolo].} \tag{5}$$

II.4 Generadores de secuencia Caótica

En la actualidad, existen comunidades de investigadores que centran su atención en el uso de los sistemas caóticos como medio para la generación de secuencias pseudo-aleatorias. Los generadores caóticos en combinación con la criptografía se le conoce como criptografía caótica. La criptografia caótica utiliza como generador de secuencia

pseudoaleatoria un sistema caótico determinístico que, a pesar de no tener entradas aleatorias, presenta un comportameniento sumamente complejo aparentemente aleatorio, de los cuales a continuación se presenta una breve descripción.

II.4.1 Origen del caos

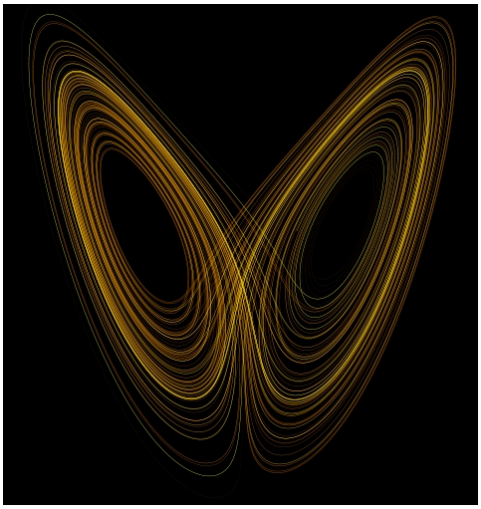


Figura 8: Atractor de Lorenz

En la antigüa cosmología griega la palabra caos se utilizaba para referirse a la sustancia primordial de la que nació el universo. En la actualidad, la palabra caos se utiliza para referirse a los sistemas dinámicos determinísticos no lineales que presentan un comportamiento aparentemente aleatorio y con una gran sensibilidad a condiciones iniciales (Moon, 1992).

El descubrimiento del caos como se conoce hoy en día se debe a Edward Lorenz y, en gran medida a la invención de las computadoras de alta velocidad que surgieron en la decada de los 60's y que han permitido a la fecha, analizar comportamientos de sistemas no lineales mediante métodos numéricos y visualizarlos gráficamente a partir

de representaciones visuales. Edward Lorenz trabajaba en sus mundialmente conocidas ecuaciones (Lorenz, 1963), mediante las cuales pretendía predecir el clima. Después de estudiar detenidamente su sistema y realizar pruebas con diferentes parámetros llegó a la conclusión de que las simulaciones eran muy diferentes para condiciones iniciales muy próximas. El comportamiento representativo de sus investigaciones se plasman en el atractor de Lorenz, mostrado en la figura 8.

II.4.2 Dinámica caótica

En el contexto de la dinámica, se observan diferentes comportamientos de movimientos dinámicos que pueden ser: estables, inestables y caóticos (Moon, 1992).

Un movimiento dinámico estable a lo largo del tiempo, tiende a un punto fijo u órbita según su dimensión conocido como **atractor**. Un sistema inestable se escapa de los atractores y un sistema caótico manifiesta una dualidad en su comportamiento. Es decir, por un lado, existe un dimensión finita (atractor) por el que el sistema es atraído, pero de la misma manera existen "fuerzas"que lo repelen, de tal forma que el sistema se mantiene oscilando en una zona especifica, pero sin converger a un punto fijo ni salirse de la dimensión del atractor. A la forma que presentan las oscilaciones de los sistemas caóticos se les conoce como atractores extraños (Moon, 1992).

II.4.3 Atractores extraños

Una manera de identificar un sistema a partir de su comportamiento dinámico es mediante su atractor, esto es, a partir de su diagrama de fase. En este diagrama de fase el tiempo está implícito y cada eje representa una dimensión de cada estado del

sistema y que se plasman en un sistema de ecuaciones. De acuerdo a la forma en que sus trayectorias evolucionan, los atractores pueden ser clasificados como atractor punto fijo (comportamiento estable), atractor período o ciclo límite (comportamiento período) y atractor cuasiperiódico. Los atractores son a menudo asociados con formas geométricas clásicas en el espacio de fase, como las que se muestran en la figura 9:

- **Atractor punto fijo:** es asociado con la convergencia a un punto, es decir, después de un parte transitoria el sistema converge a un punto en específico (Moon, 1992).
- **Atractor periódico o ciclo límite:** es asociado con una curva cerrada, esto es, que después de una etapa transitoria el sistema queda oscilando periódicamente en una curva cerrada específica (Moon, 1992).
- **Atractor cuasiperiódico:** es asociado a una figura tridimensional toroidal (Moon, 1992).

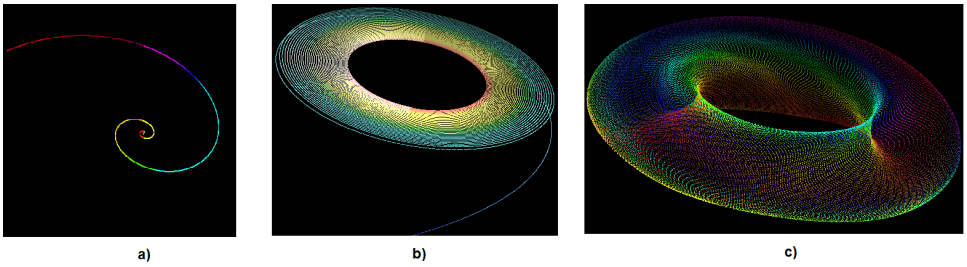


Figura 9: Tipos de movimiento dinámico: a) atractor punto fijo, b) atractor ciclo límite y c) atractor cuasiperiódico.

En sistemas de oscilaciones no lineales se estudia un tipo de atractores que no es ninguno de los tres mensionados anteriormente, esta clase de movimiento o comportamiento se denomina caótico y es en el sentido de que no puede ser predecible dicho comportamiento cuando hay una diferencia en la condicion inicial, este atractor es asociado con una figura muy particular y se le denomina **atractor extraño** (Moon, 1992).

Ejemplo de estos es el atractor de Lorenz de la figura 8.

II.4.4 Sistema caótico en tiempo contínuo y en tiempo discreto

En el estudio de los sistémas caóticos, los modelos matemáticos generalmente se describen mediante sistemas de ecuaciones diferenciales para el análisis en tiempo contínuo; a este tipo de representación se le conoce como **flujos**, o mediante sistemas de ecuaciones en diferencias, para el caso en donde la variable tiempo es discreta; comúnmente conocidos como **mapeos**. El término flujo se refiere a un conjunto de trayectorias en el espacio de fase procedentes de muchas condiciones iniciales contiguas; en el estudio de oscilaciones en ingeniería, la contínua evolución en el tiempo de una partícula es el ejemplo más común del concepto de flujo. Sin embargo, información cualitativa y cierta información cuantitativa puede obtenerse de un sistema mediante el estudio de evolución de las variables de estado en tiempo discreto (Moon, 1992).

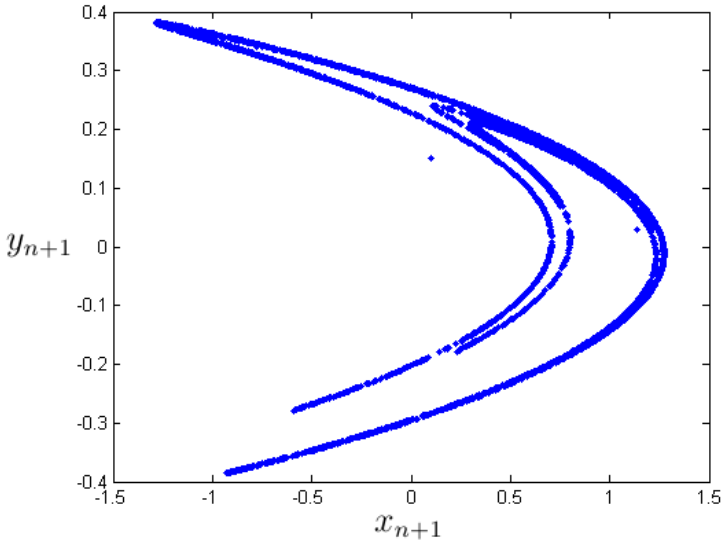


Figura 10: Atractor de Hénon.

Un método para obtener el mapa de un sistema contínuo es mediante la aplicación del modelo de sección o Mapeo de Poincaré. La principal ventaja de utilizar un mapeo de un sistema contínuo es, que las propiedades del sistema original (sistema contínuo) se conservan en el sistema discreto y el resultado de este proceso es un sistema de ecuaciones en diferencias con igual o generalmente menos ecuaciones que el sistema original. A este proceso se le conoce como **discretización** de sistemas continuos.

$$\begin{aligned} x_{n+1} &= y_n + 1 - ax_n^2 \\ y_{n+1} &= bx_n. \end{aligned} \tag{6}$$

La ecuación (6) representa un sistema caótico en tiempo discreto conocido como Mapa de Hénon (Hénon, 1976) y que se muestra en la figura 10. Este mapeo surge de aplicar el método de sección de Poincaré al sistema de Lorenz, cuyo atractor se muestra en la figura 8. El sistema depende de dos parámetros a y b, que para el modelo canónico genera un comportamiento caótico con $a = 1.4$ y $b = 0.3$. Para otros valores de a y b el mapeo de Hénon puede continuar en régimen caótico o converger en una órbita periódica.

En general, para que un mapeo pueda clasificarse como caótico debe tener las siguientes propiedades (Inzunza, 2012):

- Ser sensible a condiciones iniciales.
- Su serie de tiempo debe estar acotada en amplitud.
- Las iteraciones de la serie son infinitas.
- La serie es oscilatoria aperiódicamente
- La serie no converge.

- El sistema es no lineal.
- Proviene de un modelo determinístico.
- Debe ser transitivo.
- Sus atractores deben formar un conjunto denso en una región compacta del espacio de fases (atractor extraño).
- Su atractor extraño presenta dimensión fractal.
- Tener al menos un exponente de Lyapunov positivo.

En el contexto de la criptografía caótica, los mapeos hipercaóticos resultan ser más atractivos a implementarse en un algoritmo de encriptamiento, esto se debe a que presentan mayor complejidad y pseudoaleatoriedad en su comportamiento dinámico. Por citar un ejemplo, el mapeo hipercaótico de Rössler (Itoh *et al.*, 2001; Aguilar-Bustos *et al.*, 2008), está compuesto por el sistema de ecuaciones en diferencias (7) que depende de los parámetros α, β, γ, δ, ζ, η y θ.

$$\begin{aligned} x_1(k+1) &= \alpha x_1(k)(1-x_1(k)) - \beta(x_3(k)+\gamma)(1-2x_2(k)), \\ x_2(k+1) &= \delta x_2(k)(1-x_2(k)) + \zeta x_3(k), \\ x_3(k+1) &= \eta((x_3(k)+\gamma)(1-2x_2(k))-1)(1-\theta x_1(k)). \end{aligned} \tag{7}$$

Para cuando $\alpha = 3.8,\ \beta = 0.05,\ \gamma = 0.35,\ \delta = 3.78,\ \zeta = 0.2,\ \eta = 0.1$ y $\theta = 1.9$, el sistema exhibe una dinámica hipercaótica que se muestra en la figura 11.

En la literatura se encuentran ampliamente documentados una gran variedad de mapeos caóticos. En el presente trabajo de tesis implementamos experimentalmente, solo algunos, entre los que se encuentran: el mapeo de Tinkerbel, Logistic 2D, Ikeda y Chen. A continuación se presentan sus sistemas de ecuaciones en diferencias y sus respectivos diagramas de fase.

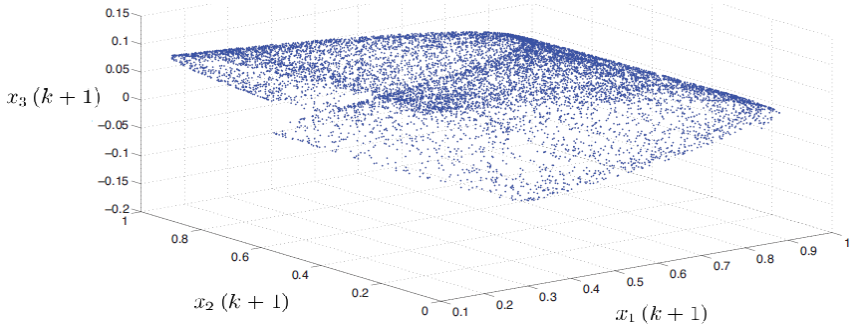


Figura 11: Atractor hipercaótico de Rössler.

II.4.5 Mapeo de Tinkerbell

Recientemente se ha reportado en la literatura el mapeo Tinkerbell (Shaoliang y Jiang, 2011; Goldszztejn *et al.*, 2011). El mapeo exhibe un nuevo e interesante comportamiendo dinámico representado por las ecuaciones (8). El atractor se puede observar en la figura 12.

$$\begin{aligned} x_{n+1} &= x_n^2 - y_n^2 + ax_n + by_n \\ y_{n+1} &= 2x_n y_n + cx_n + dy_n, \end{aligned} \tag{8}$$

donde: $a = 0.9, b = -0.6013, c = 2$ y $d = 0.5$.

II.4.6 Mapeo Logístico 2D

El mapeo Logístico 2D, es un modelo aplicado al análisis del crecimiento poblacional y fue publicado por Pierre Verhulst (Verhulst, 1845). Es considerado como mapeo polinomial y a menudo es citado como un ejemplo arquetípico de lo complejo. Su comportamiento en régimen caótico surge de ecuaciones de la dinámica no-lineal. El mapeo logístico fue popularizado en 1976 por el biólogo Robert May (May, 1976). Se le ha utilizado en aplicaciones tan diversas como en el encriptado de imágenes en adición con codificación DNA (Zhang *et al.*, 2010). El mapeo Logístico 2D se describe

matemáticamente por el sistema de ecuaciones en diferencias dadas en (9). Su atractor se muestra en la figura 12.

$$\begin{aligned} x_{n+1} &= \mu_1 x_n(1-x_n) + \gamma_1 y_n^2 \\ y_{n+1} &= \mu_2 y_n(1-y_n) + \gamma_2(x_n^2 + x_n y_n), \end{aligned} \tag{9}$$

donde: $2.75 < \mu_1 \leq 3.4$, $2.75 < \mu_2 \leq 3.45$, $0.15 < \gamma_1 \leq 0.21$ y $0.13 < \gamma_1 \leq 0.15$

II.4.7 Mapeo de Ikeda

El mapeo de Ikeda (Ikeda y Daido, 1980) está descrito por el sistema de ecuaciones en diferencias dadas en (10). El atractor generado se muestra en la figura 12. El mapeo originalmente fué propuesto como un modelo de luz que pasa a través de un resonador óptico no-lineal.

$$\begin{aligned} x_{n+1} &= 1 + u(x_n cos(t_n) - y_n(sin(t_n)), \\ y_{n+1} &= u(x_n sin(t_n) + y_n cos(t_n)), \end{aligned} \tag{10}$$

donde: $t_n = 0.4 - (\frac{6}{1+x_n^2+y_n^2}), u = 0.9.$

II.4.8 Mapeo de Chen

El mapeo de Chen (Chen, 2001) se describe por el sistema de ecuaciones en diferencias (11) y el atractor generado se muestra en la figura 12.

$$\begin{aligned} x_{n+1} &= 1 - a(x_n^2 + y_n^2, \\ y_{n+1} &= 2 - abx_n y_n, \end{aligned} \tag{11}$$

con $a = 1,95$ y $b = 1$, el mapeo exhibe una dinámica hipercaotica.

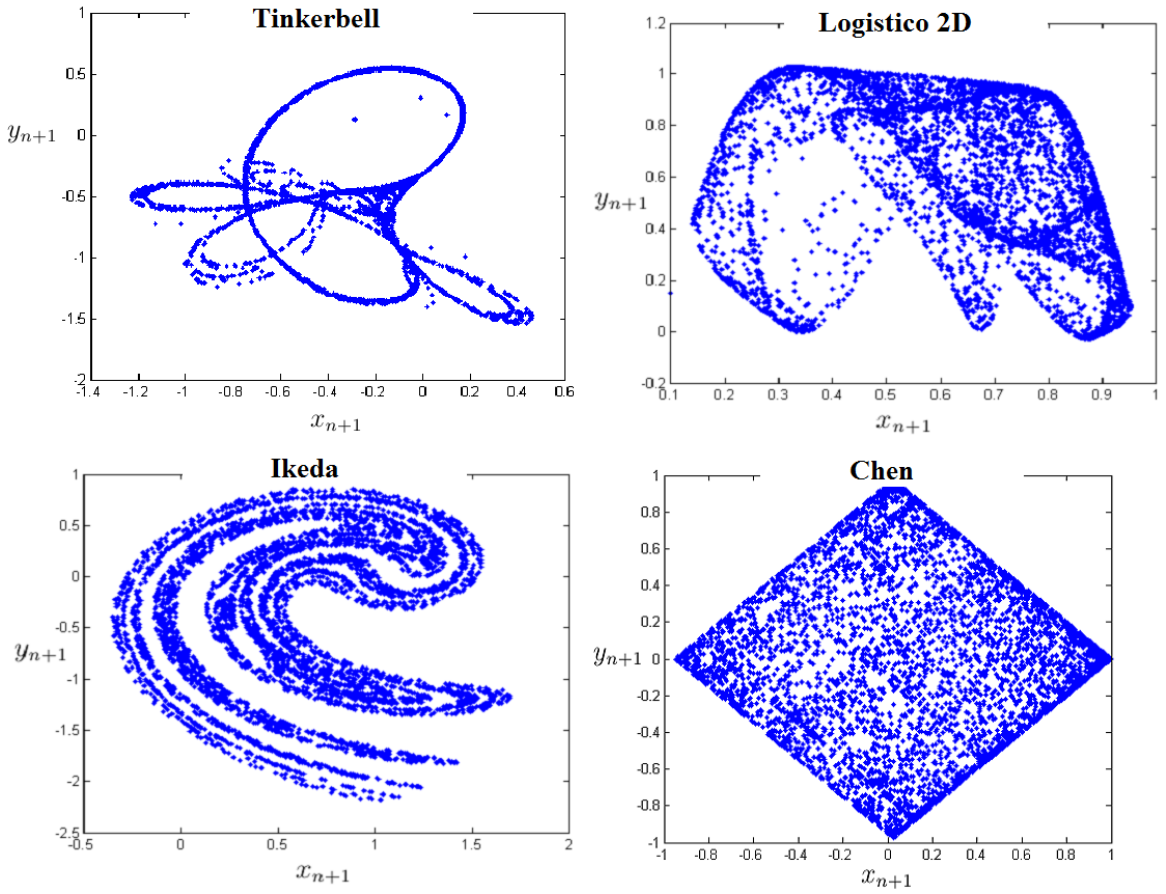


Figura 12: Atractores caóticos.

Siguiendo las ideas planteadas en la sección **II.2** referente a la criptografía y a los sistemas de comunicación segura, el paso natural es implementar en el sistema esquematizado en la figura 6, el concepto de criptografía caótica. Es decir, mediante la implementación de un mapeo caótico; como alguno de los mostrados en la figura 12, se generara la señal portadora con las que la información privada se encripta.

En la actualidad, la criptografía empleando medios caóticos, se ha establecido como nueva línea de investigación (Kocarev y Shiguo, 2011) y es de gran interés para los investigadores incrementar la seguridad de los sistemas criptográficos y desarrollar métodos criptográficos lo más incondicionalmente seguros.

II.5 Conclusiones

El método Vernam ofrece sin duda alguna las máximas garantias de seguridad, sin embargo, presenta un inconveniente muy evidente. Se requiere de una clave tan larga como el texto claro, es decir, un dígito de clave secreta por cada dígito de texto claro, lo cual resulta inviable para las aplicaciones habituales criptográficas, considerando las actuales exigencias de información a cifrar. El cifrado Vernam queda reservado para aquellas circunstancias en que se necesite el máximo grado de seguridad con un mínimo de información a proteger. En la práctica, es viable utilizar el cifrado en flujo; el presente trabajo de tesis, está basado en métodos de cifrado en flujo con generadores caóticos, es decir, se desarrollan algoritmos a partir de los modelos determínisticos caóticos. De una clave conocida únicamente por el transmisor y el receptor, se generan simultáneamente las secuencias caóticas que nos permitirán según sea el caso, el encriptado o desencriptado de la información privada. El cifrado en flujo es una aproximación al cifrado Vernam y alcanza su máximo grado de seguridad dependiendo de dos aspectos: la aproximación de la secuencia generada para encriptar, a una auténtica secuencia aleatoria y el tamaño del espacio de claves.

Capítulo III

Generación de caos con microcontroladores PIC

III.1 Introducción

En la literatura actual, se puede encontrar una amplia gama de trabajos que describen diferentes metodologías para implementar generadores de caos. Dentro de esta gran variedad de trabajos, se encuentran aquellos que utilizan técnicas de diseño basados en circuitos analógicos (Lindsay, 1981), (Newcomb y Sathyan, 1983), (Saito, 1985), (Chua *et al.*, 1986), (Wu y Chua, 1993), (Kennedy, 1993), (Chen y Chandran, 2007), (Sunnel, 2006), (Campos-Cantón *et al.*, 2007), (Campos-Cantón *et al.*, 2008), (Lu *et al.*, 2004). Algunos otros han diseñado e implementado circuitos para generar atractores caóticos de multiples enrollamientos (Simin *et al.*, 2005), (Han *et al.*, 2007; Gamez-Guzmán *et al.*, 2009), también bajo los conceptos de la electrónica analógica. En el diseño de circuitos analógicos y particularmente para la generación de caos, es necesario emplear una gran variedad de componentes electrónicos tales como: bobinas, amplificadores operacionales, diodos, resistores, capacitores, multiplicadores, entre muchos otros. En la mayoría de los casos, se requiere llevar acabo ajustes muy precisos y se hace en general complicada la implementación experimental. Adicionalmente, algunos de los componentes electrónicos no son muy comerciales por lo que no son de fácil adquisición. El punto más vulnerable de los circuitos analógicos es su gran sensibilidad al ruido del entorno, manifiestándose sobre los circuitos a partir de interferencias electromagnéticas.

Desde la perspectiva de la electrónica digital, al utilizar componentes electrónicos digitales y en específico los microcontroladores (μC's), se reduce entre otras cosas, la cantidad de componentes en la construcción de los circuitos generadores de caos, debido a que la implementación propia de los sistemas caóticos se lleva acabo mediante programación en el μC y no por componentes electrónicos analógicos. Esto ayuda en la reducción de la complejidad en la circuiteria y tiempo de implementación, no son necesarios ajustes precisos sobre algunos componentes y se aminora considerablemente la sensibilidad al ruido.

En cuanto a diseños de generadores de caos empleando electrónica digital podemos citar a (Sinha y Ditto, 1998, 1999; Ditto *et al.*, 2006), los cuales llevan acabo una emulación de las compuertas lógicas AND, OR, NOT y XOR. En el trabajo reportado por (Ameer, 2010) se implementa el uso de Flip-Flops para le generación del caos, mientras que en (Amini, 2009) se reporta una implementación digital en una computadora personal. Las técnicas de diseño de hardware digital se pueden utilizar para implementar generadores caóticos eficientes utilizando dispositivos digitales en sistemas embebidos, tales como FPGA's (Field-Programmable Gate Array), ver por ejemplo (Tanougast, 2011; Kocarev y Shiguo, 2011).

En el trabajo reportado por (Yu-Ming *et al.*, 2010), se presenta la generación de atractores caóticos de tipo rejilla de 9x7 y atractores hipercaóticos con enrrollamientos tipo rejilla en sistema cuadrimencional, para lo cual utilizan: un μC tipo ATmega 128L de ATMEL con arquitectura RISC, un aislador digital ADUM1410 y un DAC AD420 de 16 bits-serial, ambos de Analog Devices. En el trabajo de (Acho-Zuppa, 2010), se presenta la implementación del mapeo Logistic 1D en un μC PIC12F629 fabricado por Microchip Inc., programando en lenguaje ensamblador. En (Aboul-Seoud *et al.*, 2011)

se presenta la implementación del mapeo Logistic 1D pero en un μC Atmega 16. En (Tang *et al.*, 2008) se presenta un generador de números aleatorios utilizando el microcontrolador 8051 en conjunción con una versión modificada del circuito de Chua; el circuito impreso mostrado, nos permite ver que el sistema depende del circuito analógico de Chua modificado y de una etapa de conversión analógica-digital para un procesamiento digital con el microcontrolador.

Como primera etapa del presente trabajo de tesis, proponemos una metodología para el diseño e implementación de un generador de caos empleando electrónica digital, basado en un μC. Particularmente, en esta etapa se utiliza el PIC16F877A de Microchip Inc. Su programación es con lenguaje C del compilador CCS y empleamos un DAC MCP4921 de 12 bits con comunicación serie tipo SPI. Para la validación de los resultados, se realiza la implementación de algunos mapeos caóticos ampliamente documentados y estudiados en a literatura.

III.2 Metodología

La figura 13 muestra el esquema a bloques del circuito basado en μC propuesto para generar caos. El PIC16F877A es programado utilizando la implementación de un mapeo caótico para la generación de las series pseudoaleatorias. Con el propósito de observar y verificar el comportameinto caótico de las series generadas, dichas series pasan por un proceso de conversión digital-analógico mediante la implementación de DAC's MCP4921. Una particularidad de los sistemas caóticos es que generan tantas series pseudoaleatorias como ecuaciones contenga su sistema de ecuaciones. Cada una de las series generadas se envía a su correspondiente DAC por comunicación SPI con la finalidad de observar el comportamiento de las trayectorias mediante un osciloscopio

y realizar la comparación con los atractores documentados en la literatura. Con lo anterior validar que, en efecto, el comportameinto es caótico de acuerdo a la forma de su atractor. Si se observa que el atractor generado corresponde a la forma del atractor extraño del mapeo implementado, entonces las series generadas son caóticas.

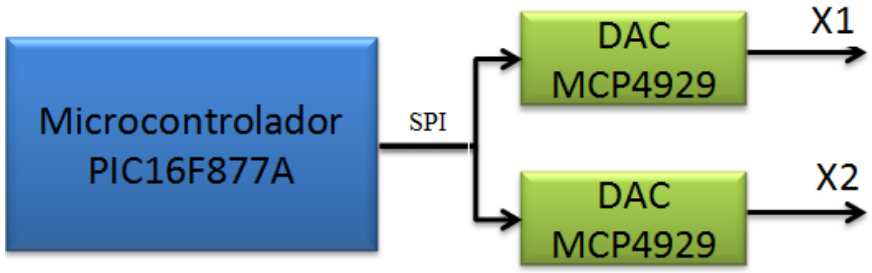


Figura 13: Esquema a bloques del generador de caos.

III.2.1 Programación del PIC16F877A

El lenguaje de programación que se utiliza es el lenguaje C para microcontroladores y el software de programación es el compilador PCWH de CCS. El programa del generador de caos se describe a continuación:

- Primeramente se escriben las directivas de configuración en donde se define principalmente el procesador a utilizar, el tipo de señal de reloj y la velocidad de reloj. Lo anterior se realiza con el siguiente bloque de codigo:

  #include $< 16F877A.h >$

  #fuses XT,NOWDT

  #use delay(clock = 4000000) // Reloj de 4 MHz

- En la función principal, se declaran las variables auxiliares a utilizar asi como las correspondientes a los parámetros del mapeo caótico a utilizar, en seguida se realiza el ciclo de iteraciones del mapeo caótico por i número de elementos de la serie a generar, el ejemplo a continuación es con base en el mapéo de Hénon:

```
//sistema de ecuaciones de Hénon
x1b=c-a*x1a*x1a+x2a;     //X1
x2b=b*x1a;               //X2
x1a=x1b;
x2a=x2b;
```

III.2.2 Circuito eléctrico

En la figura 14 se observa el circuito eléctrico utilizado para la implementación física del generador de caos. Se utiliza un circuito generador de reloj en las terminales $OSC1/CLKIN$ y $OSC2/CLKOUT$, en este caso, un cristal de 4MHz y el circuito de reset en la terminal $\overline{MCLR}/Vpp/TVH$ del μC, ver figura 15. Para observar los resultados se utiliza un osciloscopio digital con la función de mostrar en pantalla $X1 contra X2$. Los resultados se muestran en el capítulo VI.

III.3 Conclusiones

El principal inconveniente en el uso de generadores con técnicas de diseño analógicas es que, debido a que la generación del caos depende directamente del diseño del circuito eléctrico, si una persona requiere experimentar con varios sistemas caóticos tiene que considerar adquirir una gran cantidad de componentes para su construcción. La complejidad en la implementación de los sistemas de ecuaciones en circuito eléctrico,

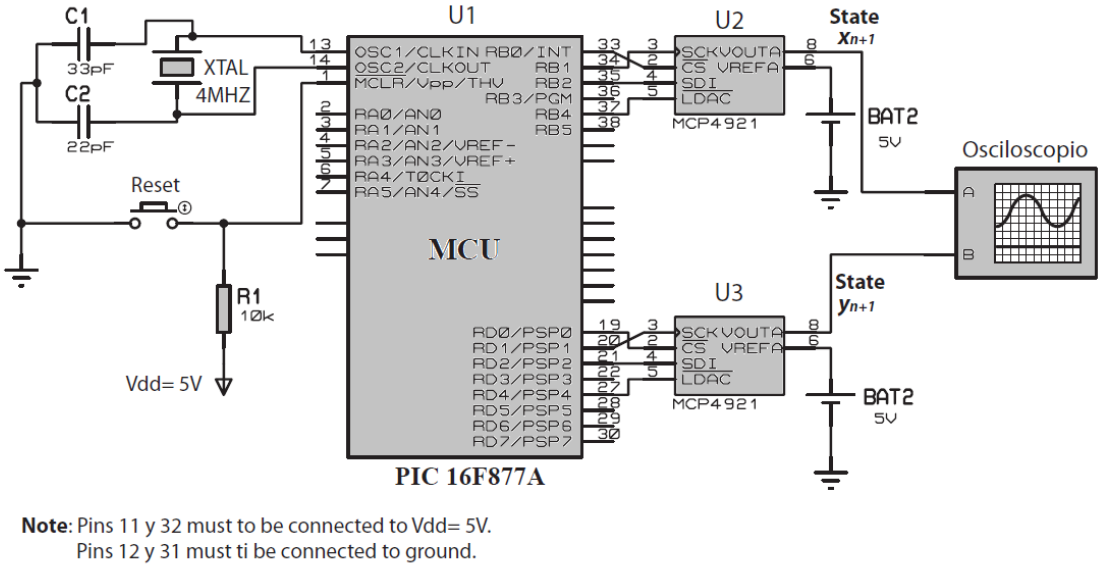


Figura 14: Diagrama eléctrico del generador de caos.

el tiempo de implementación, asi como los complicados ajustes muy precisos o finos que requieren ciertos componentes; se multiplica por tantas veces el número de sistemas caóticos con los que se requiera experimentar. En la metodología propuesta, sencillamente basta con cambiar el modelo caótico a implementar en el programa del μC sin modificar el circuito general, es decir, se puede implementar diferentes sistemas caóticos en un mismo generador. Debido a lo anterior, también se reduce la sensibilidad al ruido. Adicionalmente, si se desea transferir las series pseudoaleatorias digitales se tiene la variante mostrada en la figura 15, en donde se eliminan los DAC's y se incluye un convertidor MAX232 para comunicación serie con conector DB9. Una variante más se describe en el capítulo IV, donde se elimina el circuito convertidor MAX232 y se implementa un módulo de comunicación inalámbrica.

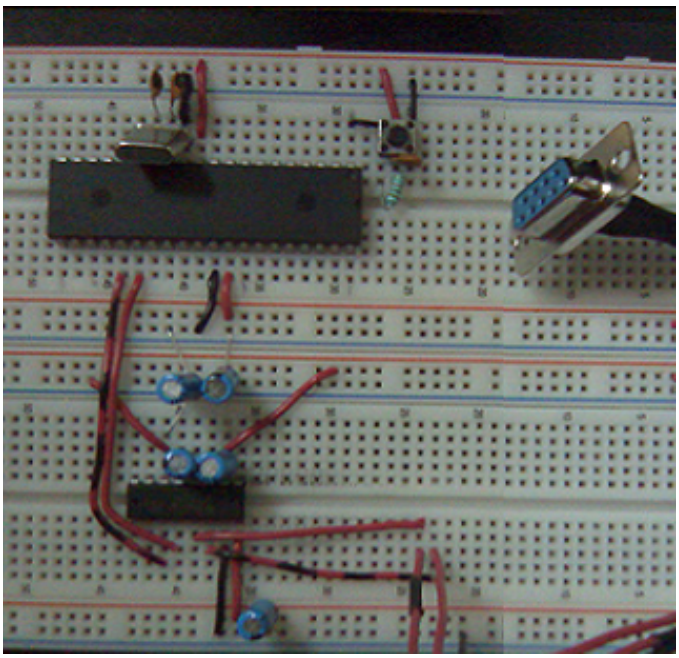


Figura 15: Circuito del generador de caos con interfaz DB9.

Capítulo IV

Sistema de comunicación en RF con encriptamiento caótico basado en generador de caos digital

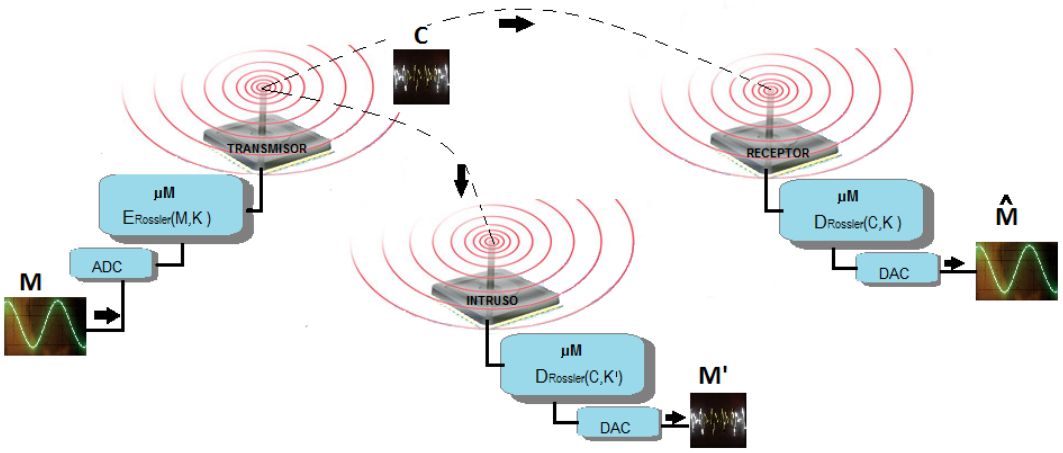


Figura 16: Sistema de Comunicación en RF con encriptamiento caótico basado en μC .

IV.1 Introducción

Las propiedades del caos han demostrado ser adecuadas para el diseño de sistemas de protección de información confidencial; actualmente en la literatura se encuentran documentadas una gran cantidad de investigaciones que demuestran la efectividad de la utilización del caos como medio para encriptar información confidencial. Desde los primeros trabajos de Pecora y Carrol Pecora y Carrol (1991), quienes lograron mostrar que dos circuitos caóticos (replica uno del otro) pueden sincronizar sus trayectorias y encriptar un mensaje en una de sus señales; hasta los estudios más recientes de Inzunza

(2012), en donde realiza el encriptado caótico en sistemas biométricos y su analisis de seguridad; podemos referirnos de entre muchos a estudios donde se han implementado diversos métodos de encriptamiento basados en criptografía caótica: algunos basados en sincronización de subsistemas transmisor y receptor mediante técnicas de diseño con electrónica analógica, otros mediante el diseño de metodologías implementadas en software, ver por ejemplo Baptista (1998); Dac (2001); Aguilar-Bustos *et al.* (2008); Aguilar-Bustos y Cruz-Hernández (2009); Behnia *et al.* (2007); Fateri y Enayatifar (2011); Jakimoski y Kocarev (2001); Liu *et al.* (2009); Abundiz (2010); Cruz-Hernández *et al.* (2010).

En cuanto a cifrado caótico de información confidencial utilizando sistemas basados en microcontrolador en comunicación inalámbrica en RF, pocos estudios se encuentran documentados. Recientemente se publicó un estudio donde utilizan un entorno de desarrollo con módulo de comunicación inalámbrica incluido, a base del microcontrolador 8051 Abid *et al.* (2010) y lenguaje de programación en C; en este estudio encriptan y desencriptan audio utilizando el canal inalámbrico en RF; el método de cifrado utilizado está basado en el cifrado en bloques con clave asimétrica y para encriptar y desencriptar el mensaje se recurre a la sincronización de los sistemas transmisor y receptor.

El presente capítulo presenta una metodología para el encriptamiento de información utilizando criptografía caótica, el método de cifrado en flujo con clave simétrica y su implementación en un sistema de comunicación inalámbrica en RF con al menos tres usuarios (transmisor, receptor e intruso), ver figura 16.

IV.1.1 Comunicación inalámbrica

Las comunicaciones inalámbricas se realizan mediante redes inalámbricas de comunicación. Según la distancia las redes inalámbricas se clasifican como, redes de distancia corta y redes de distancia larga. Las redes de distancia corta son utilizadas en un mismo edificio o varios edificios cercanos y las redes de distancia larga son utilizadas para distancias grandes como puede ser otra ciudad u otro país. Según su cobertura, las redes inalámbricas se clasifican como:

- **Wireless Personal Area Network (WPAN):** Este tipo de red es de cobertura personal y contempla las siguientes tecnologías:
  - HomeRF: el cual es un estándar para conectar todos los teléfonos móviles de la casa y las computadoras personales mediante un aparato central.
  - Bluetooth: protocolo que sigue la especificación IEEE 802.15.1 el cual permite que dispositivos como PC, PDA's, teléfonos, sensores y actuadores utilizados en domótica, entre otros, puedan comunicarse e interoperar.
  - ZigBee: basado en la especificación IEEE 802.15.4 y utilizado en aplicaciones como la domótica, que requieren comunicaciones seguras con tasas bajas de transmisión de datos y maximización de la vida útil de sus baterías, bajo consumo.
  - RFID: sistema remoto de almacenamiento y recuperación de datos con el propósito de transmitir la identidad de un objeto (similar a un número de serie único) mediante ondas de radio.
- **Wireless Local Area Network (WLAN):** En las redes de área local podemos encontrar las siguientes tecnologías:

  - Basadas en HIPERLAN (del inglés, High Performance Radio LAN), un estándar del grupo ETSI.
  - Basadas en Wi-Fi, que siguen el estándar IEEE 802.11 con diferentes variantes.

- **Wireless Metropolitan Area Network (Red de area Metropolitana):** Aplicado en redes de área metropolitana y contempla las siguientes tecnologías:
  - Basadas en WiMAX (Worldwide Interoperability for Microwave Access) que es un estándar de comunicación inalámbrica basado en la norma IEEE 802.16. WiMAX es un protocolo parecido a Wi-Fi, pero con más cobertura y ancho de banda.
  - También podemos encontrar otros sistemas de comunicación como LMDS (Local Multipoint Distribution Service).

- **Wireless Wide Area Network (WAN):** Una WWAN difiere de una WLAN (wireless local area network) en que usa tecnologías de red celular de comunicaciones móviles como son:
  - Basadas en WiMAX (aunque se aplica mejor a Redes WMAN).
  - UMTS (Universal Mobile Telecommunications System).
  - GPRS.
  - EDGE.
  - CDMA2000.
  - GSM.

- CDPD.
- Mobitex.
- HSPA.
- 3G.
- También incluye LMDS y Wi-Fi autónoma para conectar a internet.

Siguiendo las técnicas de diseño basadas en electrónica digital, se propone un método para encriptar un mensaje utilizando el método de cifrado en flujo y el generador caótico propuesto en el capítulo III para generar la secuencia pseudoaleatoria cifrante. El emisor, el receptor y el intruso se conectan a una red de tipo WPAN utilizando la tecnología Zigbee.

IV.2 Metodología

La figura 17 muestra el cifrado en flujo con clave simétrica a utilizar de acuerdo a lo estudiado en la sección II.2.2 en conjunto con el generador de caos propuesto en el capítulo III. Un emisor T, con una clave secreta y un algoritmo determinístico que puede ser público (mapeo caótico), genera una secuencia cifrante $\{x_i\}$ cuyos elementos se suman con los correspondientes elementos de la serie m_i, dando lugar a los elementos de C. Esta serie $\{c_i\}$ es la que se envía por el canal público en donde un receptor R mediante el mismo mapeo caótico, genera la misma serie $\{x_i\}$ cuyos elementos se restan con los correspondientes elementos de C para obtener los correspondientes elemementos de M.

Tomando en cuenta el diagrama de bloques de la figura 2 se construye el sistema de comunicación segura con criptografía caótica utilizando μC's PIC16F877A y el mapeo

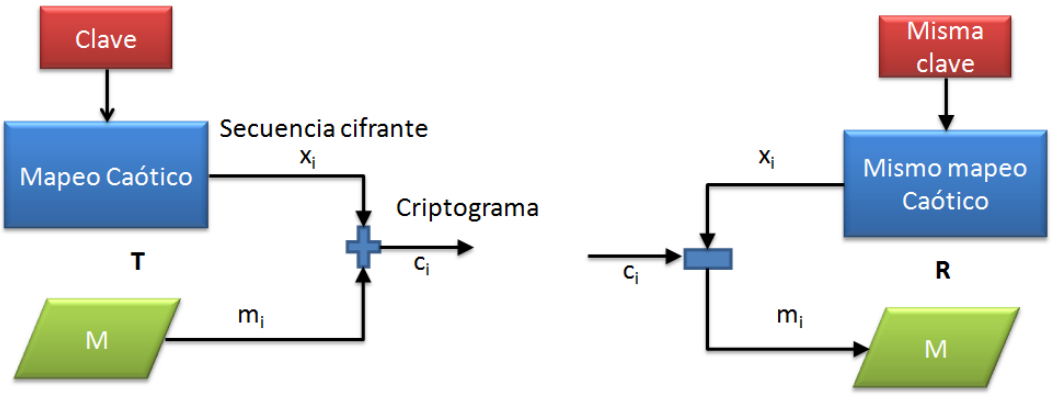


Figura 17: Procedimiento de cifrado en flujo con generador caótico en operación adición

hipercaotico caótico de Rössler como algoritmo generador mostrado en la figura 16. Las señales utilizadas como mensaje, son en este caso, señales analógicas de baja frecuencia obtenidas de un generador de funciones analógicas. El proceso general se describe a continuación:

- Un primer μC **T**, es programado para leer un mensaje **M**, encriptarlo y enviarlo por el canal público de comunicación en RF. En específico, primeramente el **ADC**, incluido en el μC, lee el mensaje y entrega cada elemento de M en su forma digital; en seguida, cada elemento de la serie m_i se encripta utilizando la técnica aditiva con su correspondiente de la serie x_i generada por el mapeo caótico usando una clave secreta (en específico, con los generados por X_1), para obtener los correspondientes elementos de C. Finalmente, cada elemento de la serie c_i, es enviado por el canal público mediante un módulo de comunicación con tecnología ZigBee.

- Un segundo μC **R** es programado para leer el criptograma proveniente del canal público, luego desencriptar el criptograma aplicando el método inverso usado en

T y entregar el mensaje recuperado a un usuario autorizado. Específicamente, primero R lee C proveniente del canal público y, aplicando el método inverso utilizado en T, desencripta los elementos de la serie c_i con los correspondientes x_i generados utilizando el mismo mapeo caótico. Debido a que ambos sistemas (T y R) cuentan con la misma clave secreta, generan la misma secuencia x_i, por lo que, al desenccriptar cada elemento de la serie x_i con su correspondiente de la serie c_i y la operación inversa (resta), se obtiene el correspondiente de la serie m_i; cada elemento recuperado de M pasa por un proceso de conversión digital a analógico para ser entregado en su forma original al usuario receptor.

- Un tercer μC **I**, realiza un criptoanalisis y es programado y configurado de la misma forma que R, la diferencia es que no cuenta con la misma clave secreta usada en T y en R.

El criptoanalisis que se realiza es el más elemental y se utiliza cuando se conoce el algoritmo de cifrado y descifrado. Consiste en realizar una prueba exhaustiva con todas las claves posibles para descifrar el criptograma. No se necesita el conocimiento o fundamentos de criptoanalisis específicos, basta con tener tiempo y paciencia. Si la cantidad de claves posibles es pequeña el trabajo será corto, si esta cantidad de claves es grande, el trabajo será largo. Al número total de claves posibles que admite un sistema criptográfico se le denomina **espacio de claves**; a la prueba exhaustiva con todas las claves posibles para el desencriptamiento del criptograma se le conoce como **ataque de furza bruta**.

IV.2.1 Diagrama de flujo

La figura 18 muestra el diagramas de flujo de los programas utilizados en los μC que a continuación se describen. Para la implementación, se utilizan μC con ADC integrado, comunicación serie tipo RS232 y DAC0800 para la recuperación analógica del mensaje.

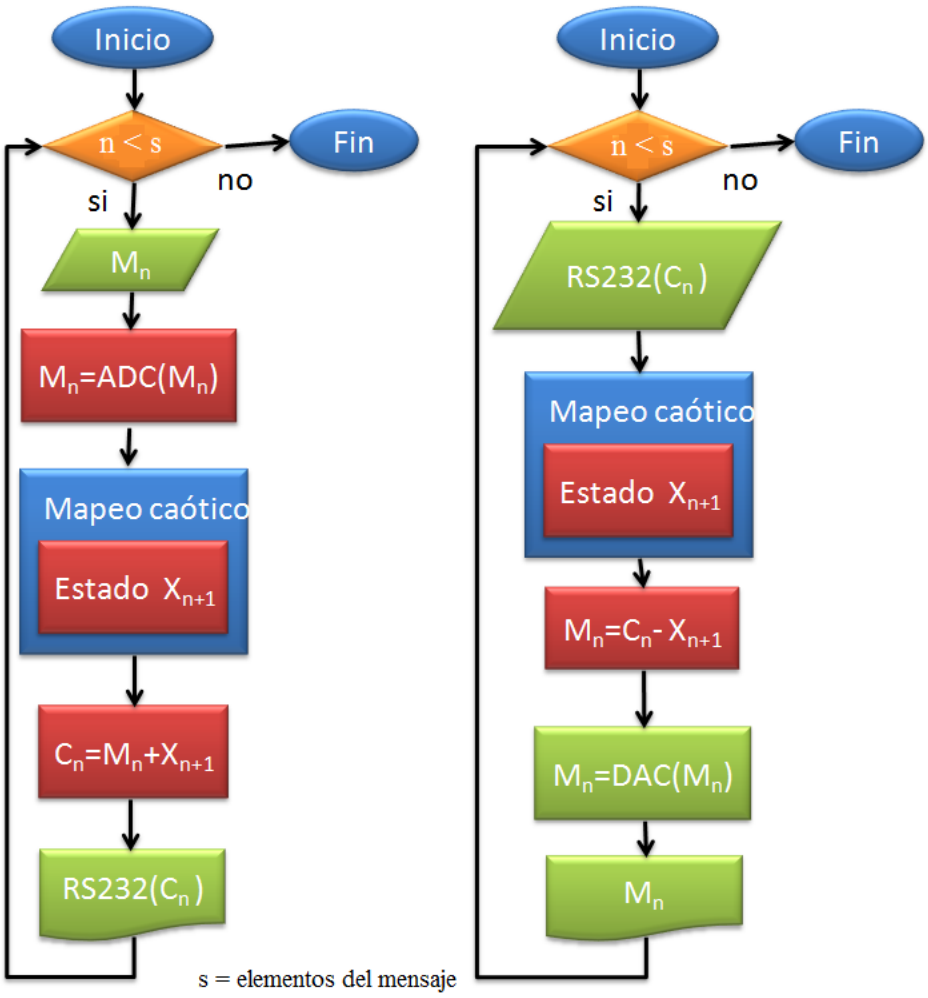


Figura 18: Diagramas de flujo, Transmisor y Receptor.

IV.2.2 Programa transmisor

Se considera un μC PIC16F877A de 8 bits, por lo que su ADC interno, realiza una conversión Analógica-Digital de 8 bits. Se establece que el μC funciona con una señal de reloj dada por un cristal externo de 4MHz y se desabilita el Wath Dog Timer. La comunicación RS232 se realiza mediante las terminales $RC6/TX/TX$, $RC7/RX/DT$ del μC. Se configura la velocidad de comunicación a 9600 $Baudios$, la asignación de terminales Tx y Rx del puerto C, la comunicación es de 8 bits y no hay bit de paridad. Las directivas para configurar lo anterior son las siguientes:

```
#include $<16F877A.h>$

#device adc=8

#fuses XT, NOWDT

#use delay(clock = 4000000)

#use rs232(baud= 9600,xmit=PIN_C6, rcv=PIN_C7,bits=8, parity=N)
```

La funcion *main* del programa del transmisor se diseña para que reciba una señal analógica de baja frecuencia por un canal del ADC interno del μC, posteriormente se implementa el sistema caótico para genera caos (en este caso el mapeo de Rössler), en seguida, se encripta dicha señal mediante la operacion de adición y se envía el criptograma por comunicación serie al módulo de transmisión inalámbrica. Las siguientes líneas de código muestran la operación de encriptado y el envío del criptograma:

$crip = adc_val + x$; //encripta el mensaje en X
$printf("\%f", crip)$;

IV.2.3 Programa receptor

El programa del receptor, recibe el criptograma por comunicación serie a la misma velocidad (también genera caos mediante el mapeo de Rössler) para desencriptar y recuperar la señal original, una vez recuperada, se envía por el puerto de I/O PORT B (previamente configurado para salida de datos) del μC y es recibida por el dispositivo de conversión Digital-Analógica para su observación mediante un osciloscopio. Las directivas de configuración son las siguientes:

#use fast_io(b)
#BYTE TRISB = $0x86$
#BYTE PORTB = $0x06$
#BYTE OPTION_REG = $0x81$
#use rs232(baud=9600, xmit=pin_c6, rcv=pin_c7, bits=8)

y las sentencias de recuperación y envio del mensaje recuperado son:

$adc\_val = cript - x$; //recupera el mensaje
$adc\_rd = adc\_val * 256$; //convierte el valor a escala 0-255
$output_b(adc\_rd)$; //envia por el PORT B el mensaje hacia

IV.2.4 Programa intruso

El programa del intruso, realiza la misma operación que el programa del receptor. Se hace suponer que cuenta con el mismo circuito e incluso utiliza la misma función de desencriptado con la diferencia de que no conoce los parámetros y claves secretas utilizadas, es decir, realiza un ataque de fuerza bruta. Para demostrar la sensibilidad a condiciones iiniciales del proceso de encriptamiento, en el programa intruso se realiza

un pequeño cambio en la condición inicial en el estado x_1.

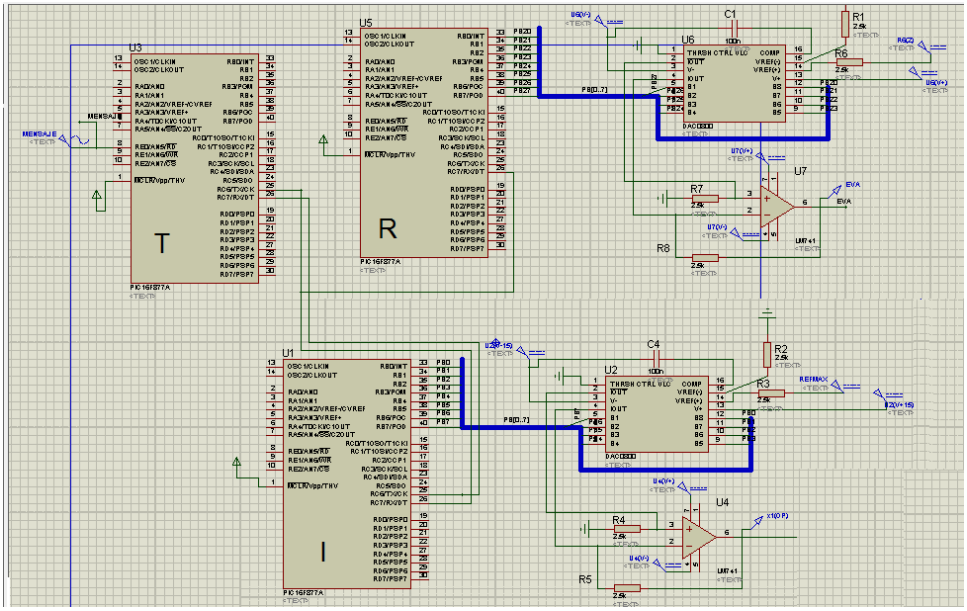


Figura 19: Simulación en PROTEUS.

IV.3 Simulación

Antes de realizar la implementación física de los prototipos, se realiza la simulación del sistema de comunicación en el software PROTEUS y el compilador PCWHD. La figura 19 muestra una pantalla del sistema con los tres elementos interconectados encriptando y desencriptando una señal.

IV.3.1 Implementación física

La figura 20 muestra el esquema del Transmisor; recibe una señal, la encripta y envía el criptograma por comunicación serie. La figura 22 muestra la construcción del Receptor que recibe el criptograma por comunicación serie a la misma velocidad. Para la presentación del mensaje recuperado por el receptor se implementa un DAC de 8

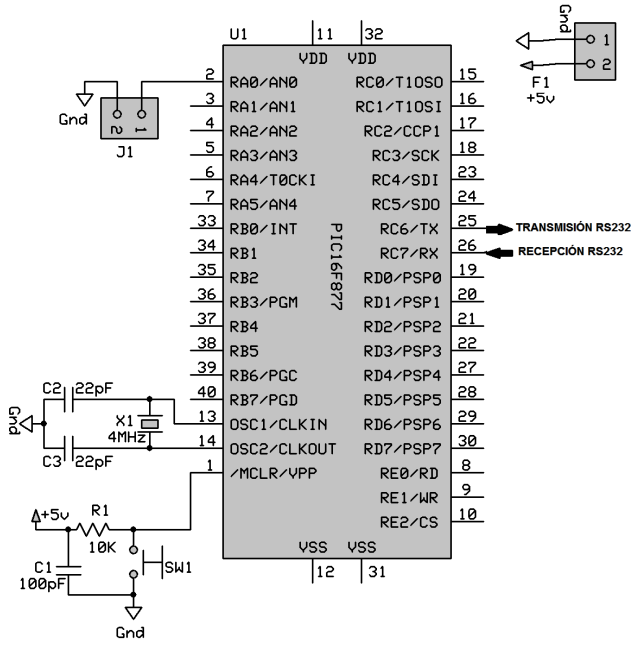


Figura 20: Esquema eléctrico del Transmisor.

bits en comunicación con el PORT B. La señal analógica a encriptar proviene de un generador de señales y se considera un offset de $2v$ para garantizar lecturas positivas. Se convierte el dato digital que resulta del ADC interno del Transmisor a escala de (0-1) para asegurar que la amplitud del mensaje sea similar a la amplitud de la señal x_1 y con esto lograr esconder el mensaje en la señal caótica; el voltaje de referencia que se aplica al DAC es de $2v$ para garantizar una salida de voltajes en el rango de $(-2v,2v)$ y recuperar la señal con la misma amplitud que la original.

Nota: El intruso se construye de igual forma que el Receptor.

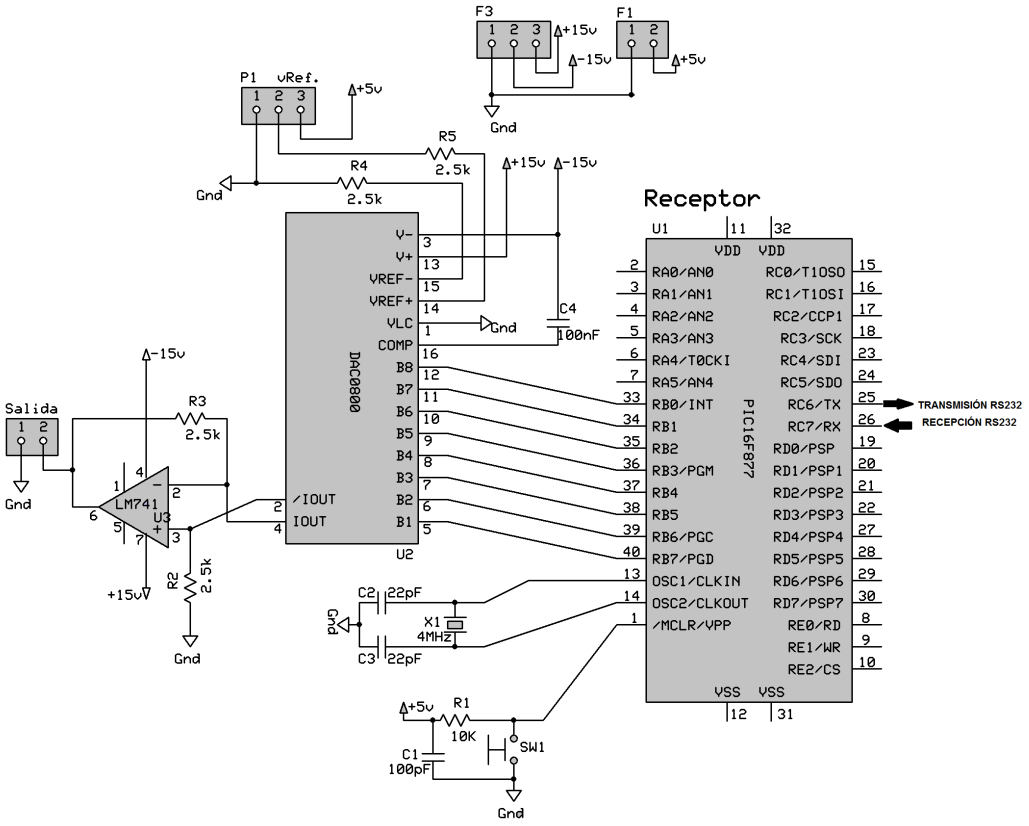


Figura 21: Esquema eléctrico del Receptor.

IV.3.2 Implementación de módulos XBee

Los módulos de comunicación inalámbrica que se utilizan para el presente trabajo pertenecen a la familia XBee. En específico el modelo XBee PRO s1 que proporciona tecnología ZigBee, basado en la especificación IEEE 802.15.4 con topología de red multipunto. Para la implementación de los módulos XBee en el sistema de comunicación encriptada se realiza lo siguiente:

- Se conecta la terminal de transmisión serie Tx del μC que corresponde al bloque de transmisión a la terminal de entrada de datos $pin\,3$ del modulo $Xbee$ que utilizaremos como transmisor y se configura el ID de módulo de comunicación.

- Se conecta la terminal de recepción serie Rx del μC que corresponde al bloque de recepción a la terminal de salida de datos $pin\,2$ del modulo $Xbee$ que utilizaremos como receptor y se configura el ID de módulo de comunicación.

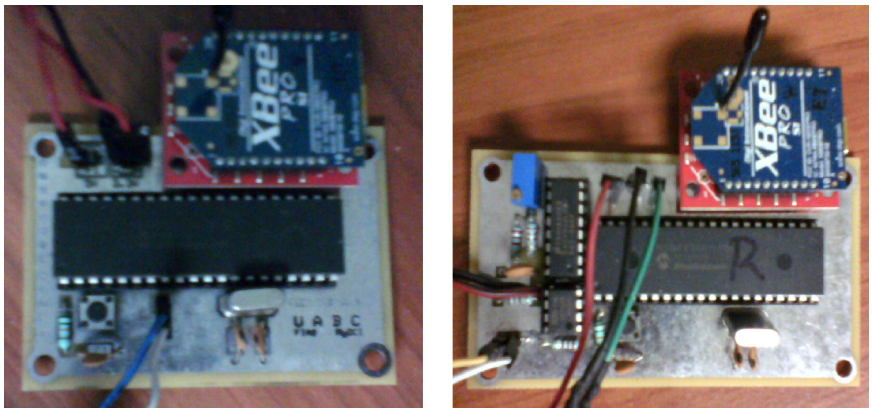


Figura 22: Transmisor y receptor con módulos de comunicación inalámbrica.

IV.4 Conclusiones

En este trabajo se realizó la implementación de un sistema de encriptamiento caótico con microcontroladores utilizando el canal público de comunicación inalámbrica mediante

el uso de modulos de comunicación XBEE. Se comprueba que tiene aproximación a ser incondicionalmente seguro ante el ataque de fuerza bruta de un intruso, aun cuando este implementa el mismo método de desencriptamiento, mientras desconosca la clave secreta de la comunicación. La experimentación se realizó aplicando como mensaje señales muy conocidas de baja frecuencia y se concluye en primera instancia, que para la comunicación a frecuencias mas altas, los factores a considerar son: la velocidad del protocolo de comunicación y la velocidad de procesamiento del microcontrolador, así como de la precisión en la etapa de la conversión digital analógica de recuperación.

Capítulo V

Encriptamiento caótico de imágenes en sistema de comunicación sobre Wi-Fi

V.1 Introducción

El método propuesto, en general, es muy semejante al método del capítulo IV, ambos emplean el tipo de cifrado en flujo con clave simétrica y utilizan generadores de secuencia cifrante basados en sistemas caóticos. La diferencia principal radica en el tipo de canal de comunicación que utilizan. En este caso, el canal público es inalámbrico y el sistema embebido en el que se implementa realiza la comunicación con tecnología IEEE 802.11b/g conocida como WiFi.

Debido a que la criptografía basada en caos es de reciente investigación, se encuentran en la literatura diversos estudios donde implementan métodos para su experimentación en software de computadora y su futura implementación en los diversos sistemas y tecnologías de comunicación, ver por ejemplo Geng y Ding (2012); Feng-ying *et al.* (2012); Wei *et al.* (2006); Behnia *et al.* (2007). A nuestro conocimiento, no existe documentado algún trabajo que realice el cifrado de imágenes con criptografía caótica implementado un dispositivo embebido a base de microprocesador y utilizando el canal inalámbrico sobre tecnología Wi-Fi.

En cuanto a cifrado de imágenes con criptografia caótica en sistemas a base de

microcontrolador, recientemente se publicó un estudio donde, utilizando el mapeo de Hénon y microcontroladores Atmel AVR proponen un método para el encriptamiento de imágenes en formato JPEG, la comunicación la realiza mediante comunicación serie utilizando el estandar RS-485, ver Stanciu y Datcu (2012).

Cuando decimos que el sistema propuesto tiene delimitación geográfica mundial, debida a su implementación en la red de internet, no quiere decir que el dispositivo transmisor mediante la tecnología WiFi, alcance por si sólo, una cobertura de tipo WAN con otro dispositivo receptor. Esta delimitación está basada en que los dispositivos con tecnología WiFi, junto con una gran cantidad de medios y sistemas de comunicación como son: enrutadores, satélites, líneas de comunicación de fibra óptica, entre muchos otros; son parte de una compleja infraestructura de redes descentralizada de comunicación a la que se le conoce como **red de internet**. Debido a la gran variedad de tipos de redes y tecnologías de sistemas de comunicación, surge la necesidad de utilizar protocolos de comunicación que garantizan que las redes físicas heterogéneas que componen dicha red, funcionen como una red lógica única. A la familia de protocolos que enlazan las redes heterogéneas que componen la red de internet se le conoce como: **protocolos TCPIP**.

V.1.1 Protocolos de comunicación TCP/IP

El nombre de TCPIP, es en referencia a los dos protocolos mas importantes que componen la familia de protocolos de internet, y estos son: **TCP** e **IP**. La familia esta compuesta por más de 100 protocolos de entre los cuales podemos mencionar:

- **HTTP:** Por sus siglas en inglés de Hyper Text Transfer Protocol, utilizado para acceder a las paginas de web.

- **ARP:** Por sus siglas en inglés de Address Resolution Protocol, utilizado para la resolución de direcciones.
- **FTP:** Por sus siglas en inglés de File Tranfer Protocol, utilizado para la transferencia de archivos.
- **SMTP:** Por sus siglas en inglés de Simple Mail Transfer Protocol, utilizado para el intercambio de mensajes de correo electrónico.
- **POP:** por sus siglas en inglés de Post Office Protocol, utilizado para recibir correo electronico.
- **Telnet:** protocolo para conexiones a equipos remotos.

El protocolo **TCP**, por sus siglas en inglés de **Transmission Control Protocol** se utiliza para crear conexiones entre dispositivos de una red a través de las cuales puede enviarse un flujo de datos. Una de las principales características es que este protocolo garantiza que el flujo de datos llega de transmisor a receptor sin errores y en el mismo orden en el que se transfirierón. De lo anterior se clasifica como un protocolo de comunicación orientado a conexión fiable del nivel de transporte.

El protocolo **IP** a diferencia del TCP, no garantiza la correcta transmisión entre emisor y receptor, incluso, no se necesita de ninguna configuración de conexión antes de que un equipo intente enviar paquetes a otro con el que no se había comunicado antes. La transmisión de los datos es mediante bloques conocidos como paquetes o datagramas. De lo anterior se clasifica como un protocolo de comunicación no orientado a la conexión.

Debido a que el correcto funcionamiento, así como, la correcta recuperación del mensaje original, en el método de cifrado propuesto en los capítulos anteriores, es

completamente dependiente de la total correspondencia entre las series x_i, m_i y c_i; es inviable utilizar canales de comunicación donde no se garantice la correcta y completa transmisión de los datos entre emisor y receptor; tal es el caso de transmisión utilizando paquetes o datagramas. Si existe la necesidad de utilizar el cifrado de información confidencial sobre canales que utilizan este tipo de protocolos, es necesario implementar algun otro método; un ejemplo de estos métodos son los que involucran el concepto de sincronización, ver por ejemplo Abid *et al.* (2010).

El presente trabajo de investigación realiza el cifrado caótico de imágenes en composición RGB y en escala de grises; envía el criptograma por el canal público a un dispositivo receptor ubicado remotamente. Debido a que el mensaje viaja a través de la red de internet y que el método de cifrado realiza la tranferencia de la serie c_i en forma de flujo de datos; es impresindible utilizar un protocolo de comunicación que garantice la correcta y ordenada transmisión de flujo de datos. Dicho de otra manera, se necesita de un protocolo oriantado a conexión.

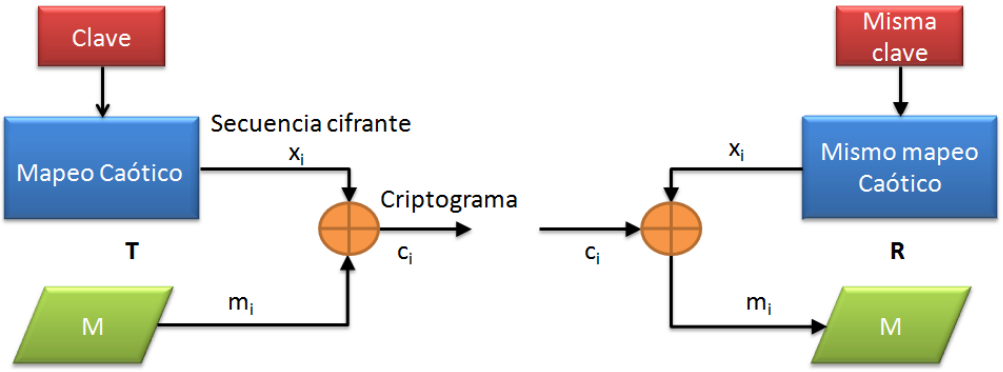


Figura 23: Procedimiento de cifrado en flujo con generador caótico y en operación XOR

V.2 Metodología

V.2.1 Diagrama de flujo

El diagrama de flujo de la figura 23 muestra el método criptográfico utilizado, se puede observar que corresponde al tipo de cifrado en flujo con clave simétrica. El envío del criptograma se realiza mediante un e-mail por la red de internet.

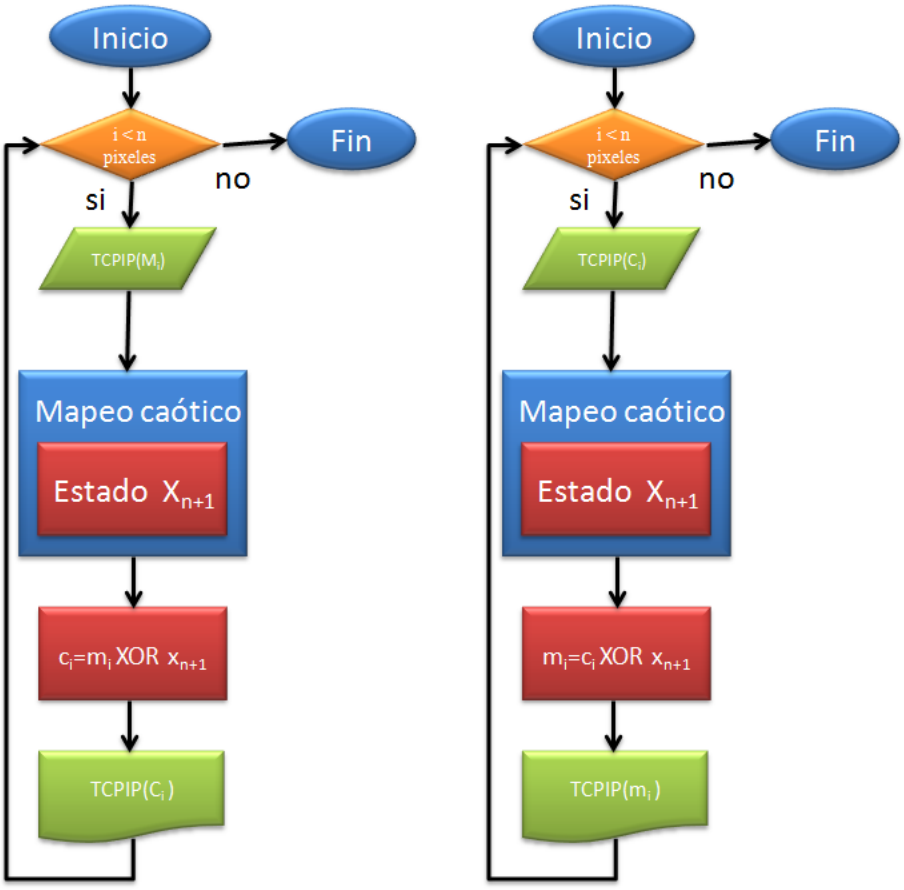


Figura 24: Diagramas de flujo, Transmisor y Receptor.

V.3 Implementación física

El procesador RCM5600W es un sistema embebido, para su uso en las diversas aplicaciones, con una gran variedad de complementos incluidos, como ejemplo el módulo de comunicación WiFi; en este caso en específico, no se necesita de la implementación de circuiteria auxiliar para la experimentación del sistema de comunicación cifrada que se propone; basta con diseñar el programa que corresponde a cada etapa del sistema de cifrado y cargarlo en el dispositivo embebido mediante su plataforma de programación. En el apendice A se mencionan aspectos importantes de puesta en operación y de configuración del RCM5600W.

El complemento sobre el cual esta basado el método de experimentación es el módulo de comunicación TCP/IP que incluye el sistema RCM5600W y las interfaces que soporta son:

- Ethernet.
- PPP (Point-to-Point Protocol) sobre comunicación serie.
- PPP sobre Ethernet
- Wi-Fi (802.11b)

Cada interface es asignada a una única dirección IP, conocida como "home IP address".

V.3.1 Programa del Transmisor

De acuerdo al diagrama de flujo de la figura 24 se diseña un programa para el proceso de encriptamiento de la imagen y en general realiza lo siguiente:

- Defnición de la directiva **define TCPCONFIG 1**: La directiva de configuración define la identificación del dispositivo mediante una dirección IP, así como el tipo de conexión (entre otros):

  #define TCPCONFIG 1

  #define _PRIMARY_STATIC_IP "10.10.6.91"

  #define _PRIMARY_NETMASK "255.255.255.0"

  #define MY_GATEWAY "10.10.6.1"

  #define MY_NAMESERVER "10.10.6.1"

  #define IFC_WIFI_SSID "RabbitTest"

  #define IFC_WIFI_ROAM_ENABLE 1

  #define IFC_WIFI_ROAM_BEACON_MISS 20

  #define IFC_WIFI_CHANNEL 1

  #define IFC_WIFI_MODE IFPARAM_WIFI_ADHOC

  #define IFC_WIFI_REGION IFPARAM_WIFI_REGION_AMERICAS

  #define IFC_WIFI_ENCRYPTION IFPARAM_WIFI_ENCR_NONE

- Definición del puerto de comunicación mediante la directiva **define PORT**:

  #define PORT 23 //DEFINE PUERTO DE COMUNICACION

- Se establece la comunicación, es decir, se inicia el dispositivo para que espere conexiones entrantes:

  $tcp_Socketsocket$;

  $sock\_init\_or\_exit(1)$;

$tcp\_listen(\&socket, PORT, 0, 0, NULL, 0);$

$printf("Waitingforconnection...");$

$while(!sock\_established(\&socket)\&\&sock_bytesready(\&socket) == -1)$

$tcp\_tick(NULL);$

$printf("Connectionreceived...");$

- Una vez que se realiza la conexión, mediante un ciclo definido por el número de elementos de la serie m_i se realiza la lectura de cada elemento de M:

  $bytes\_read = sock\_read(\&socket, buffer, 1); //LEEBYTEODATO(PIXEL)$

  $if(bytes_read > 0)$

- Se encripta con su correspondiente elemento de la serie x_i (ajustado a 8 bits) para obtener los correspondientes elementos de C mediante la operación XOR; en seguida, se envía cada elemento de C por el canal público:
  buffer[0]≙x1_mej; //METODO DE ENCRIPTAMIENTO POR XOR
  $sock_write(\&socket, buffer, 1);$ //ENVIA DATO ENCRIPTADO POR TCP/IP

Lo anterior se realiza dentro de un ciclo que itera i número de pixeles .

V.3.2 Programa del Receptor

De acuerdo al diagrama de flujo de la figura 24 se diseña un programa para el proceso de desencriptamiento de la imagen criptograma y en general realiza lo siguiente:

- Defnición de la configuración de la directiva **define TCPCONFIG 1**, para el caso del receptor solo se modifica la línea de dirección IP con el objetivo de que

emisor y receptor tengan diferente identificador:

#define _PRIMARY_STATIC_IP "10.10.6.90"

- Definición del puerto de comunicación mediante la directiva **define PORT**.
- Se establece la comunicación, es decir, se inicia el dispositivo para que realice la conexión al dispositivo transmisor:
- Una vez que se realiza la conexión, mediante un ciclo definido por el número de elementos de la serie c_i se realiza la lectura de cada elemento de C y se desencripta con su correspondiente elemento de la serie x_i (ajustado a 8 bits) para recuperar los correspondientes elementos de M.

V.4 Conclusiones

El uso del RCM5600W nos permite espacios de clave en relación a la longitud de los tipos de dato que procesa, en este caso, para el tipo de dato flotante, la longitud máxima l, para este caso es de tipo flotante de 32 bits, se ve en desventaja sobre los dispositivos que proporcionan una longitud de tipo flotante de 64 bit. En la actualidad, una gran variedad de generadores caóticos implementados en sistemas basados en el RCM5600W alcanzan la clasificación de viables en términos de su espacio de claves.
Adicionalmente podemos mencionar:

- Con la verificación de los resultados se propone el metódo con aproximación a incondicionalmente seguro con clasificación, en términos de la velocidad de computo actual, viable.
- Soporta imágenes de cualquier tamaño en composición RGB y en escala de grises.

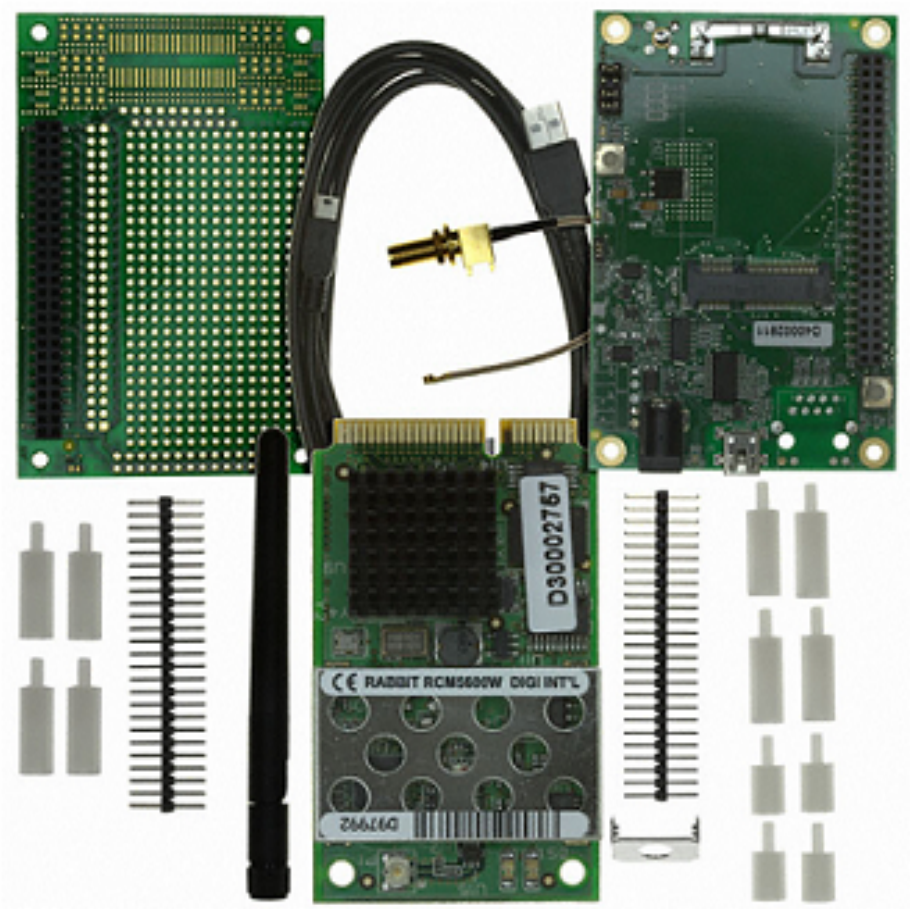


Figura 25: Microprocesador Rabbit RCM5600W

- Con minimos ajustes en el diseño de programación puede soportar cualquier composición de imagen o tipo de imagen.
- Con el uso del módulo de comunicación Wi-Fi incluido en el RCM5600W se puede implementar el sistema propuesto en una red a nivel internacional.
- Se verifica la sensibilidad a condiciones iniciales.
- Se puede implementar una gran variedad de mapeos caóticos para su experimentación.

Capítulo VI

Resultados

VI.1 Resultados de generación de caos con μC

Tomando en cuenta los tipos de comportamiento dinámicos estudiados en la sección II.4.3, se realizó la validación de las señales caóticas generadas mediante la forma de su atractor, esto es, se compararon los atractores de mapeos caóticos ampliamante documentados y citados en la literatura con los obtenidos experimentalmente y se verifica que, en efecto, el comportameinto de las series generadas por el generador propuesto son caóticas.

VI.1.1 Tamaño de serie caótica y longitud de x_i

El modelo matemático, se puede programar para un específico número de iteraciones o en un ciclo infinito, lo cual genera series caóticas de longitud específica o infinitas respectivamente. La longitud de cada elemento de x_i corresponde a la longitud máxima que pueda procesarse en el μC con el tipo de dato $float$, en este caso es de 32-bit (IEEE valor punto flotante) para el PIC16F877A y su rango es:

$$1.8x10^{-38} < x_i < 3.40x10^{38} \tag{12}$$

VI.1.2 Espacio de claves

Debido a que el comportamiento pseudoaleatorio de los generadores de caos está dado por un rango de valores en específico en los parámetros que intervienen en su sistema de ecuaciones, así como de los valores de las condiciones iniciales elegidas; el espacio

de claves que un generador de cáos puede proporcionar, es una composición de estos. El tamaño del espacio de claves depende del número de parámetros más el número de estados del mapeo caótico utilizado. La tabla I muestra los espacios de clave que pueden proporcionar los mapeos caóticos implementados en sistemas basados con PIC16F877A y su clasificación de viabilidad. En (Patidar *et al.*, 2011) se documenta que un generador de secuencias caóticas cifrantes que proporcione un espacio de claves mayor a 128 bits, se clasifica como viable para la mayoría de las aplicaciones criptográficas en términos de la velocidad de las computadoras actuales.

En las figuras 26 a la 30 se observan los resultados comparativos de la implementación física del generador de atractores caóticos propuesto; a la izquierda se observa el atractor obtenido mediante simulación numérica con el software MATLAB y a la derecha se observa el atractor obtenido con el generador propuesto y mostrado mendiante un osciloscopio, en efecto, los comportamientos de las trayectorias observadas sin duda alguna son caóticas debido a que corresponden a sus respectivos atractores extraños.

VI.1.3 Comparación con otro circuito impreso

En la figura 31 se compara el circuito impreso de el generador propuesto por [a k w tank] y el propuesto en este trabajo de investigación. Se observa en la imagen del inciso a) que el sistema depende físicamente de un circuito generador de Chua analógico, lo cual limita a la experimentación con otro sistema caótico. También, necesita de los ajustes precisos de los componentes de dicho circuito y de un módulo de memoria para almacenar los datos generados para su posterior procesamiento con el microcontrolador.

Viabilidad de mapeo caótico		
Mapeo caótico	Espacio de claves (bits)	Viable
Hénon	128	no
Tinkerbell	192	si
Logístico 2D	192	si
Ikeda	128	no
Chen	128	no
Rössler	320	si
Logístico 1D	64	no

Tabla I: Tabla comparativa de viabilidad de espacios de clave con base en sistemas de cifrado basados en PIC16F877A en términos de la velocidad de cómputo actual.

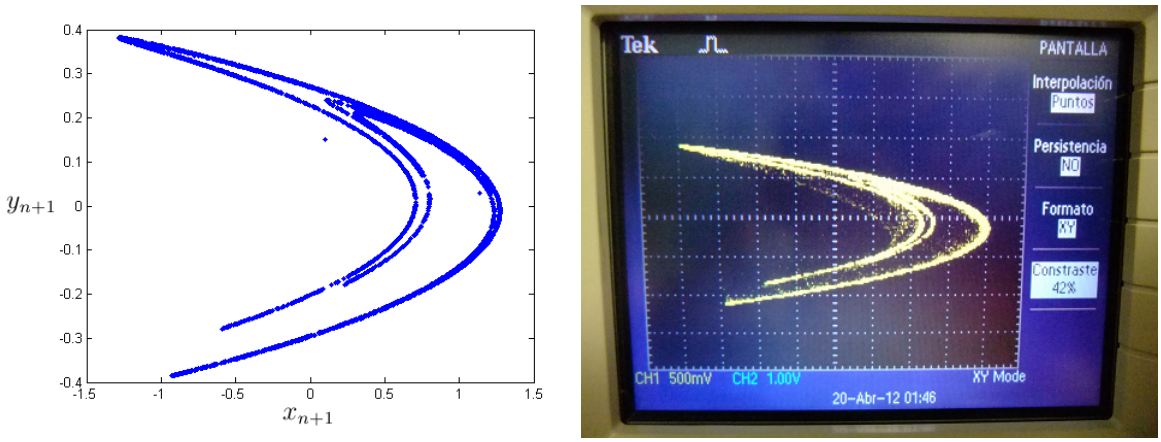


Figura 26: Atractor del mapeo de Hénon.

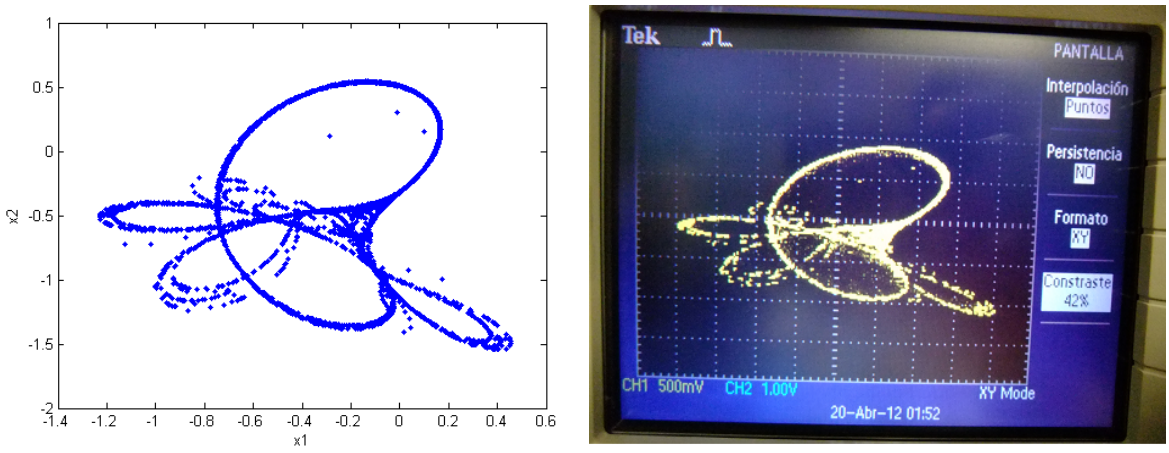
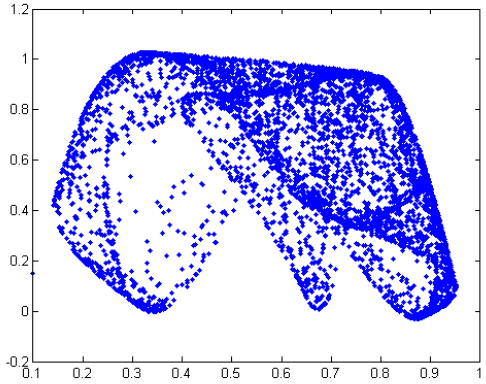


Figura 27: Atractor del mapeo de Tinkerbell.



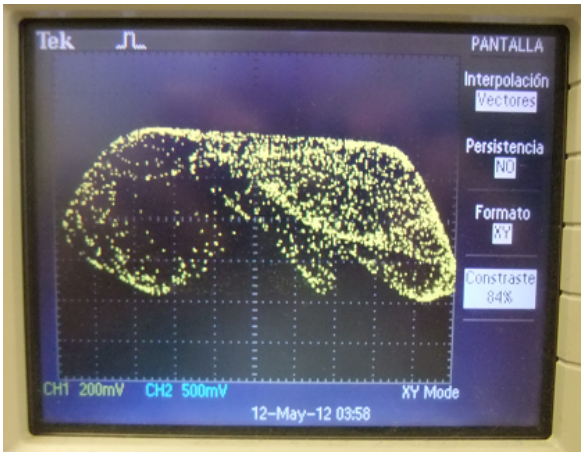
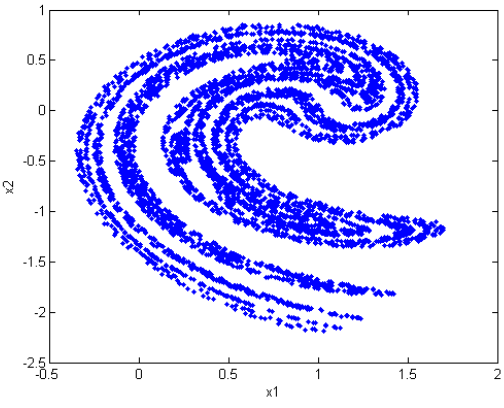


Figura 28: Atractor del mapeo Logístico 2D.



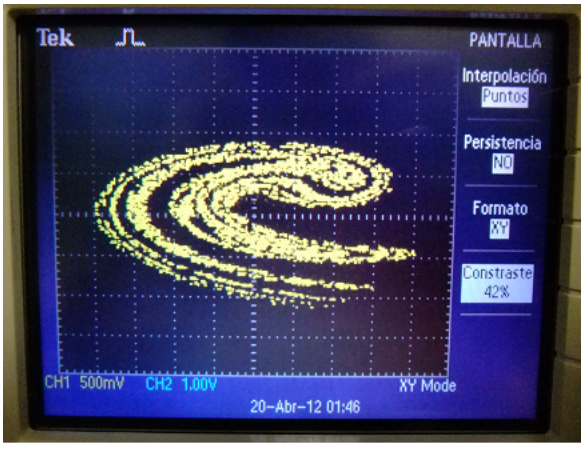


Figura 29: Atractor del mapeo de Ikeda.

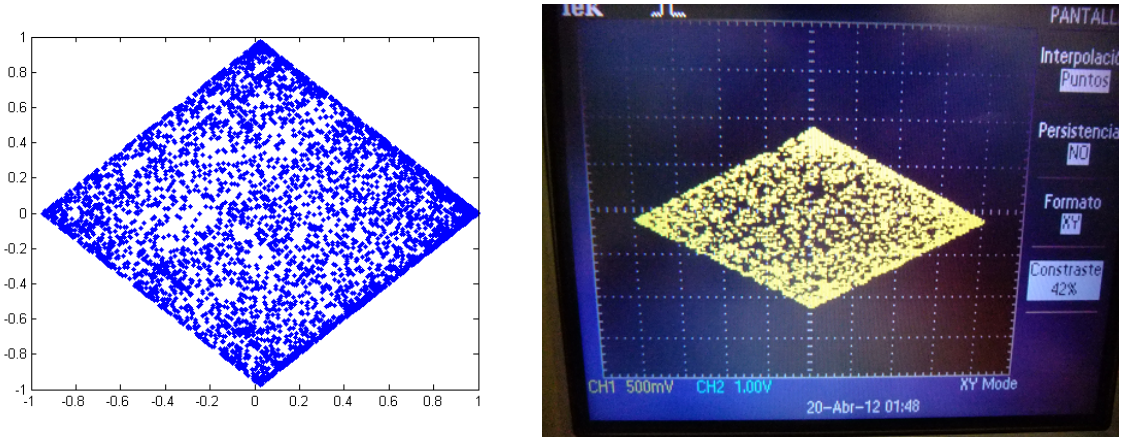


Figura 30: Atractor del mapeo de Chen.

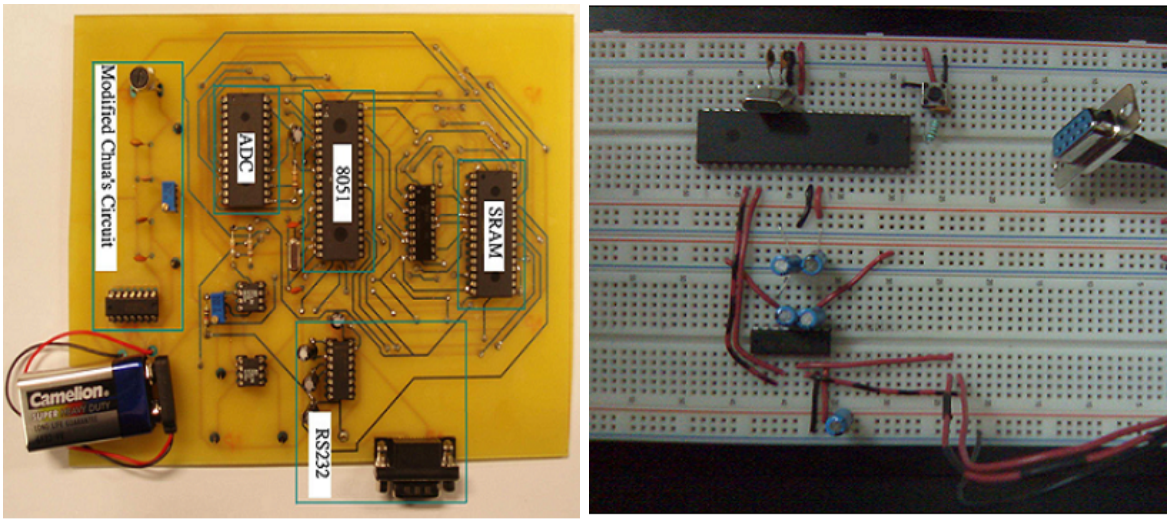


Figura 31: Generadores de caos: a) circuito basado en μC 8051, b) generador propuesto.

VI.2 Resultados de comunicación cifrada en RF

En la figura 32 a) se muestra el resultado de la simulación; la señal superior corresponde a la señal original que entra al ADC del transmisor, la señal al centro corresponde a la recuperación después del proceso de desencriptado del receptor, la señal inferior corresponde a la recuperación del intruso, verificando asi, la sensibilidad a cambios en condiciones iniciales. Se observa que la resolución de la señal de recuperación por el proceso de desencriptado se ve afectada por la limitante de la conversión digital-analógica a 8 bits, por la frecuencia de procesamiento del μC y principalmente por la velocidad de comunicación serie RS232. En la figura 32 b) se observa el resultado simulando el mismo proceso, pero, considerando una velocidad de reloj de 20MHz en el μC, 8 bits en la conversión digital-analógica y una velocidad de comunicación serie de 19200 Baudios.

En la figura 33 se observa el resultado de la implementación física del prototipo de comunicación. La señal superior corresponde a la señal que entra al ADC del transmisor, la señal al centro corresponde a la recuperación despues del proceso de desencriptado en el receptor y la señal inferior corresponde a la recuperación del intruso, verificando la sensibilidad a cambios en condidiones iniciales. En la figura 34 se observa el resultado considerando como mensaje una señal de tipo cuadrada con la misma amplitud y frecuencia que la señal senoidal. En la figura 35 se observa el resultado con una señal triangular.

Durante la experimentación, al utilizar un generador de funciones analógico y al realizar un cambio abrupto de tipo de señal con el sistema completo funcionando se observa que se produce un problema en el proceso de desencriptado; por lo que, al ocurrir este cambio se pierde la sincronía y, por lo tanto, la señal original ya no se recupera.

El problema anterior se debe a las vibraciones que se generan al girar la perilla selectora en el generador de funciones analógico. En la figura 36 se observa el resultado de aplicar las señales a encriptar mediante un generador de funciones arbitrarias digital. La señal recuperada no se ve afectada aun cuando en pleno funcionamiento se cambie abruptamente el tipo de señal.

VI.2.1 Tamaño de serie caótica y espacio de claves

El mapeo utilizado en esta experimentación es el sistema hipercaotico de Rössler; el método se hace iterar una cantidad de veces al infinito con el objetivo de encriptar una señal analógica en tiempo real sin conocer el número de sus elementos m_i, por lo que el tamaño de la serie cifrante es infinita.

Considerando la tabla I debido a que el sistema de encriptamiento esta basado en μC PIC16F877A, la clave secreta puede ser una de las 2^{320} posibles de su espacio de clave. Finalmente se concluye que el sistema criptográfico propuesto es viable con aproximación a incondicionalmente seguro.

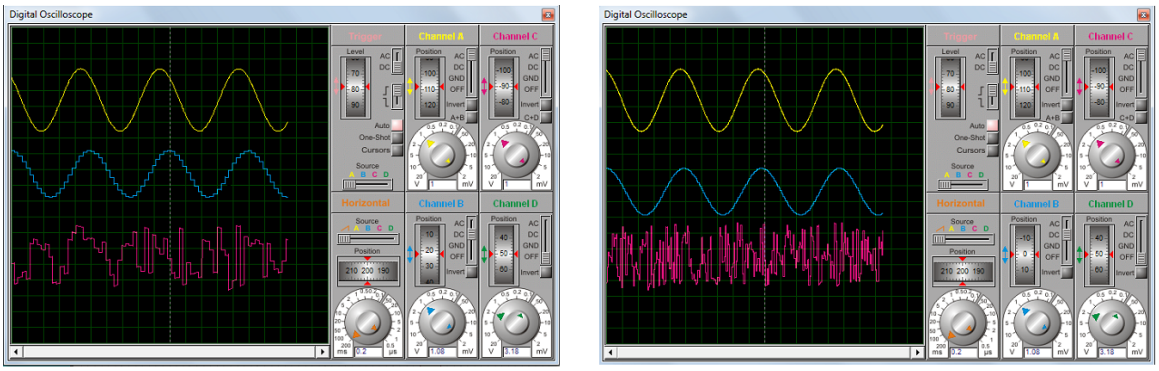


Figura 32: Resultado de simulación: a) considerando una señal de reloj de 4MHz, b) considerando una señal de reloj de 20MHz

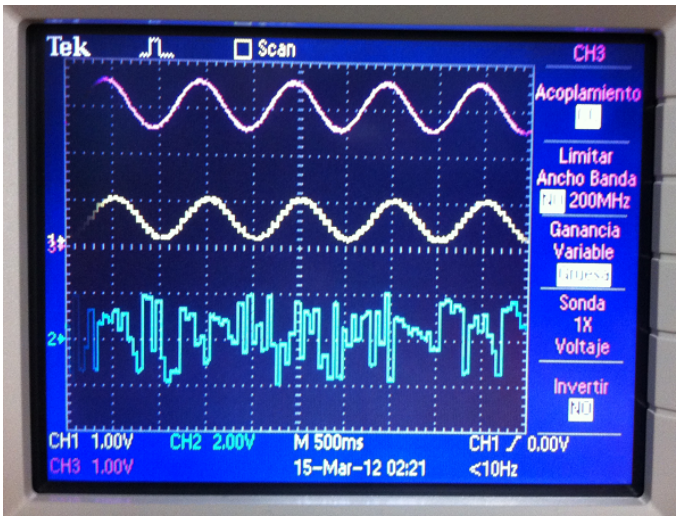


Figura 33: Comunicación cifrada con señal senoidal.

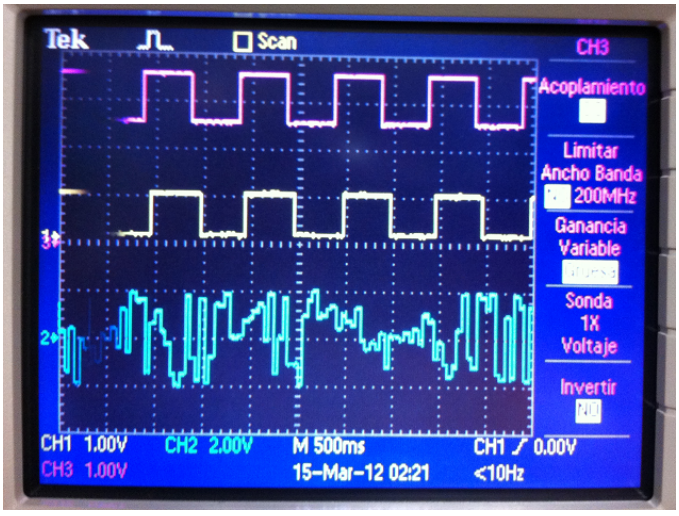


Figura 34: Comunicación cifrada con señal cuadrada.

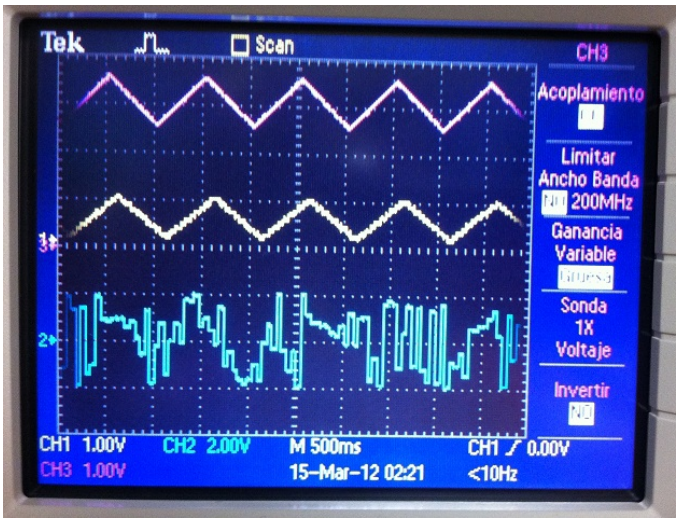


Figura 35: Comunicación cifrada con señal triangular.

Figura 36: Cambio abrupto de tipo de señal.

VI.3 Resultados de comunicación cifrada en WiFi

Con el objetivo de verificar la sensibilidad a cambios en las condiciones iniciales, las figuras 41 - 44 muestran los resultados de la comunicación segura inalámbrica WiFi utilizando imágenes a color como mensajes a encriptar. Las figuras 45 - 48 muestran los resultados de la misma implementación pero con imágenes en escala de grises como mensaje a encriptar.

VI.3.1 Tamaño de serie caótica y longitud de x_i

El tamaño de la serie cifrante, en el caso del cifrado de imágenes, si tiene un valor finito, este valor depende de el tamaño de la imagen a encriptar por lo que el sistema caótico en el programa del μC se hace iterar una cantidad específica de veces; las imágenes implementadas en los experimentos tienen una resolución de 200 x 200 pixeles, lo cual quiere decir, que la serie m_i tiene un total de $40,000$ elementos, luego entonces, se necesita una serie cifrante x_i proporcinada por el generador conteniendo $40,000$ elementos. La longitud de cada elemento de la serie x_i corresponde a la longitud máxima que pueda procesarse en el μC con el tipo de dato $float$, en este caso es de 32-bits (IEEE valor punto flotante) para el RCM5600W y su rango es el mismo que en (12).

VI.3.2 Espacio de claves considerando el uso de RCM5600W

La tabla I muestra los espacios de clave que pueden proporcionar los mapeos caóticos implementados en sistemas basados con microprocesadores RCM5600W y su clasificación de viabilidad. En (Patidar *et al.*, 2011) se documenta que un generador de secuencias caóticas cifrantes que proporcione un espacio de claves mayor a 128 bits, se clasifica como viable para la mayoría de las aplicaciones criptográficas en términos de la velocidad de las computadoras actuales.

VI.3.3 Análisis estadístico con base en entropía de la información

La tabla II muestra los resultados del análisis estadístico de seguridad de los criptogramas con base en el concepto de entropía de la información. La escala de colores de las imágenes analizadas es de 8 bits, esto quiere decir, que cada pixel de la imagen toma uno de los 256 valores posibles. Evaluando la ecuación 4, se tiene que para fuentes generadoras que emiten 2^N simbolos equiprobables con $N = 8$: La entropía $H(s) = 8$ bits/símbolo . En las figuras 37 y 38, se observa que los métodos con un valor en entropía mas alejado al valor de la total aleatoriedad, dejan ver siluetas.

Entropía			
Mapeo caótico	Espacio de claves	COLOR	Escala de grises
Tinkerbell	192	7.9933	7.9939
Logistic 1D	192	7.9743	7.9858
Chen	128	7.9874	7.9907
Arnold's cat	64	7.9774	7.9862

Tabla II: Análisis estadístico con base en entropía

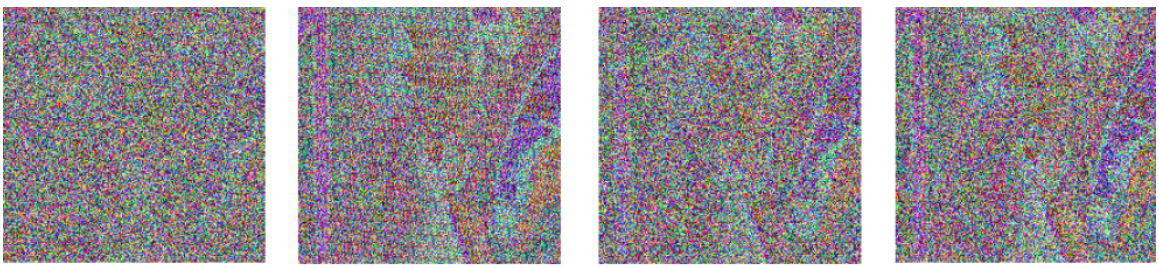


Figura 37: Efecto visual de entropía en los criptogramas con composición RGB utilizando los mapeos (de izquierda a derecha): Tinkerbell, Logistic 1D, Chen y Arnold's cat.

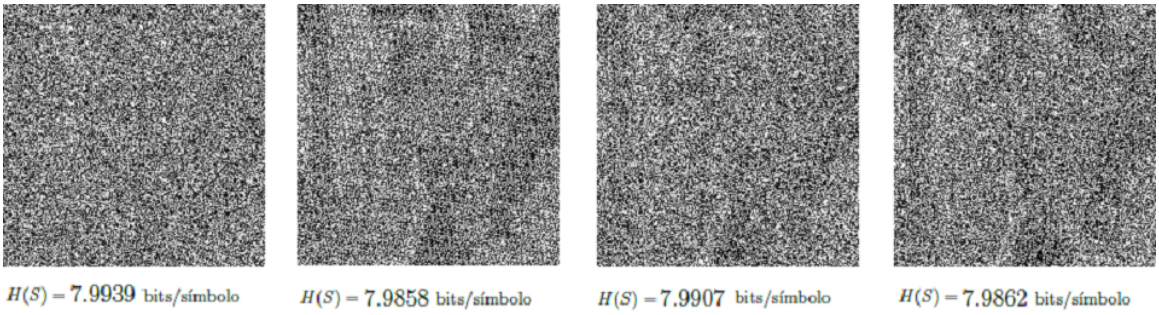


Figura 38: Efecto visual de entropía en los criptogramas en escala de grises utilizando los mapeos (de izquierda a derecha): Tinkerbell, Logistic 1D, Chen y Arnold's cat.

VI.3.4 Análisis estadístico con base en histogramas

En la figura 39 se observa la distribución de frecuencias de los colores de la imagen original y en la figura 40 se observa la distribuciń de frecuencias de los colores del criptograma aplicando el encriptado con distintos mapeos. Se puede observar que despues del encriptado, la distribución de las frecuencias tiende a ser más uniforme. Mientras más uniforme sea la distribución de las frecuencias en el histograma del criptograma significa que el algoritmo de encriptamiento utilizado ofrece mayor seguridad ante criptoanálisis estadístico.

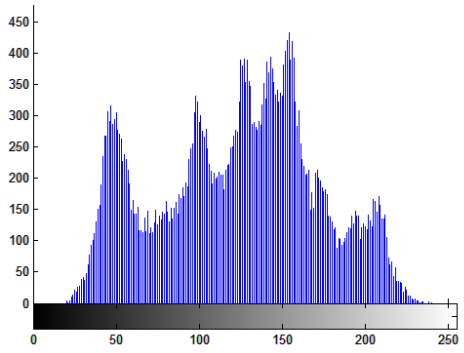


Figura 39: Histograma de la imagen original

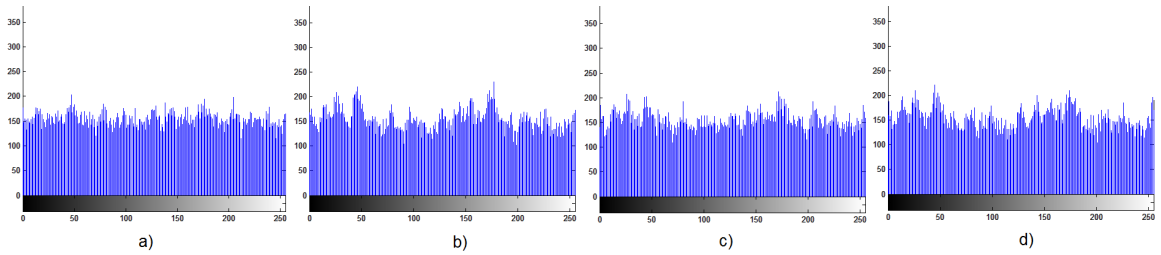


Figura 40: Histogramas del criptograma utilizando el mapeo de: a) Tinkerbell, b) Logístico 1D, c) Chen y d) Arnold's cat

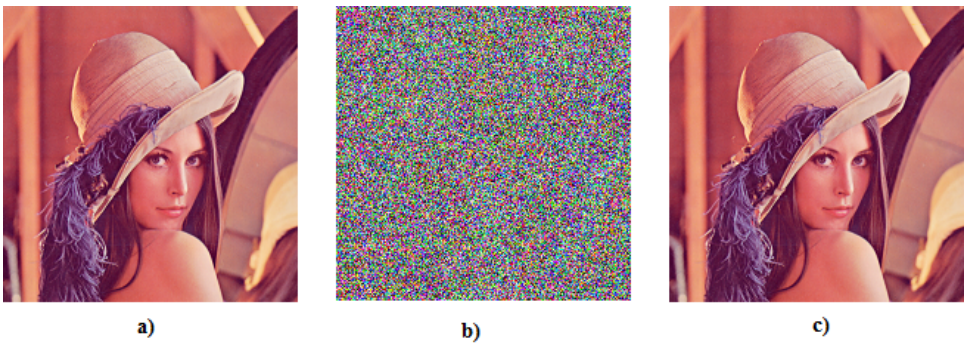


Figura 41: Cifrado con mapeo de Tinkerbell de imagen a color: a) original, b) criptograma c) recuperada.

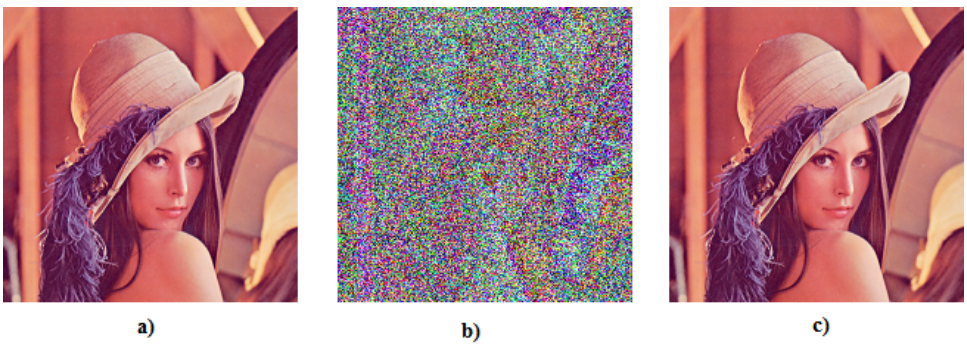


Figura 42: Cifrado con mapeo de Arnold's cat de imagen a color: a) original, b) criptograma c) recuperada.

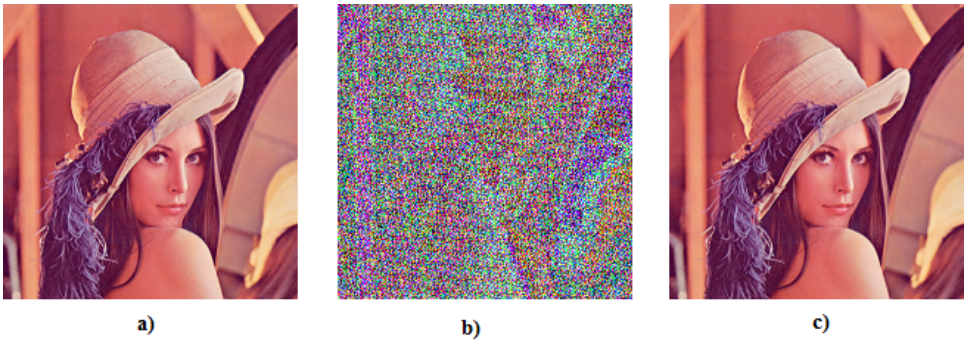


Figura 43: Cifrado con mapeo Logistic 1D de imagen a color: a) original, b) criptograma c) recuperada.

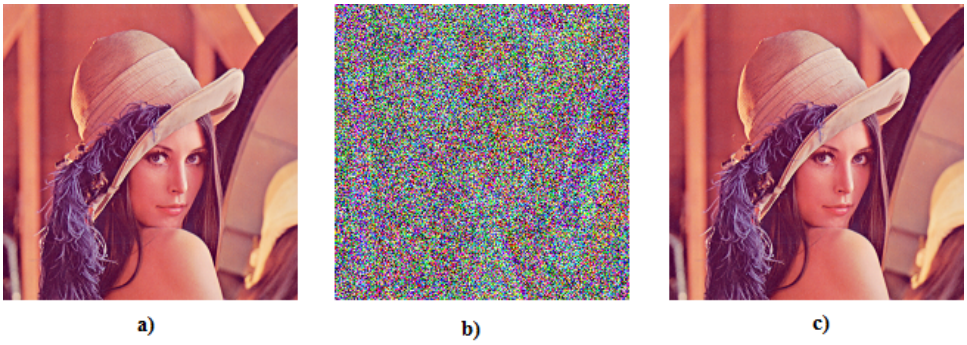


Figura 44: Cifrado con mapeo de Chen de imagen a color: a) original, b) criptograma c) recuperada.

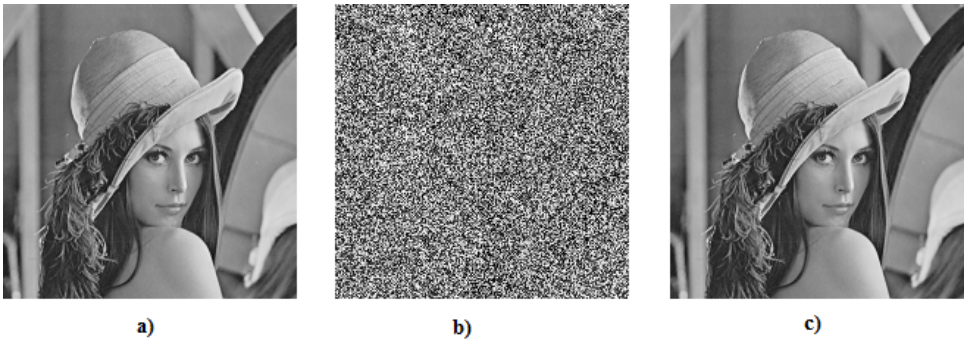


Figura 45: Cifrado con mapeo de Tinkerbell de imagen en escala de grises: a) original, b) criptograma c) recuperada.

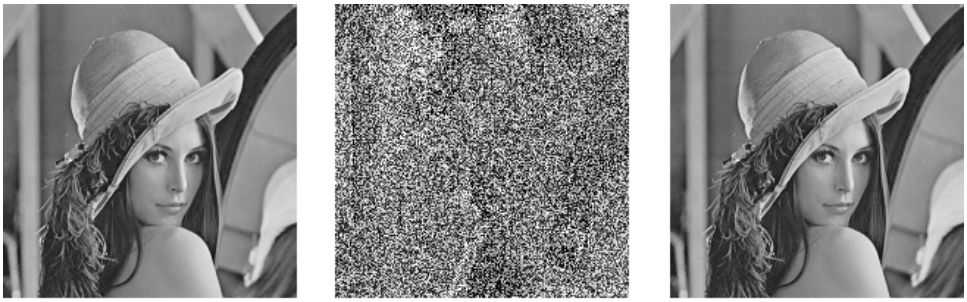


Figura 46: Cifrado con mapeo de Arnold's cat de imagen en escala de grises: a) original, b) criptograma c) recuperada.

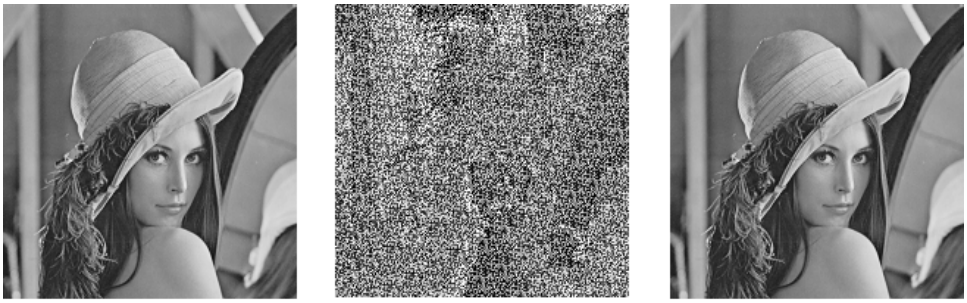


Figura 47: Cifrado con mapeo Logistic 1D de imagen en escala de grises: a) original, b) criptograma c) recuperada.

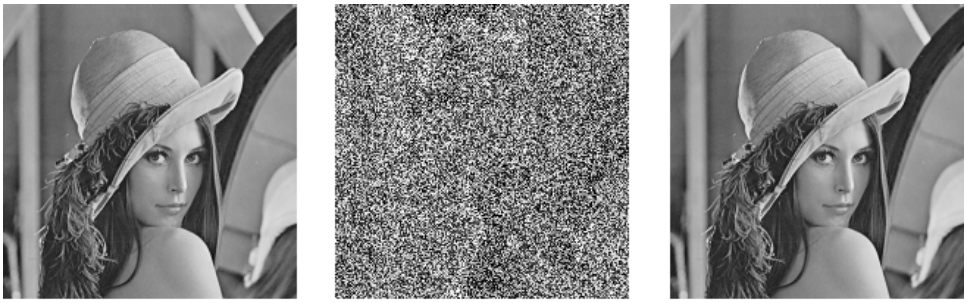


Figura 48: Cifrado con mapeo de Chen de imagen en escala de grises: a) original, b) criptograma c) recuperada.

Capítulo VII

Conclusiones generales y trabajo futuro

VII.1 Conclusiones

En el presente trabajo de tesis se presentó un método para la generación de atractores caóticos, desde la perspectiva de las técnicas de diseño de la electrónica digital y el uso de microcontroladores en sistemas embebidos, en específico con el uso del microcontrolador PIC16F877A. Se demostró, que mediante un mismo prototipo, se generaron una gran cantidad de atractores sin la necesidad de construir un circuito eléctrico para cada uno de ellos, como lo es en el caso del diseño con técnicas basadas en electrónica analógica; lo anterior, permite al experimentador utilizar diversos mapeos caóticos sin invertir tiempo, complejidad y adquisición de componentes en la construcción por cada uno de ellos, además de que los componentes utilizados son de fácil adquisición y económicos.

Se presentó también, una primer aplicación del generador propuesto en sistemas criptográficos; se propuso un método de cifrado en flujo con clave simétrica en un sistema de comunicación con canal público en RF en conexión Punto a Punto con protocolo ZigBee; se realizó su análisis en relación con el espacio de claves que proporcionan el método utilizando dicho microprocesador y se comprobó que son competentemente viables; se comprobó también la sesibilidad a condiciones iniciales, para el caso de un ataque de fuerza bruta.

Se propuso adicionalmente, un método para encriptado de imágenes a color en composición RGB y en escala de grises utilizando para ello el cifrado en flujo con clave símetrica y un canal público distinto, en este caso el canal inalámbrico en Wi-Fi. Se comprobó, que el método propuesto para la generación de caos se aplica en distintos sistemas de hardware con la finalidad de poder experimentar con distintos canales públicos. Se realizo el analisis de los resultados con base en los conceptos de entropía e histograma y se comprueba que, mediante la utilización del sistema RCM5600W se proporcionan espacios de clave competentemente viables.

VII.2 Trabajo futuro

Debido a que el avance en la velocidad de cómputo esta en constante crecimiento, es necesario el incremento en la seguridad de los sistemas criptográficos basados en sistemas embebidos y utilizando canales públicos inalámbricos modernos; lo anterior con relación al espacio de claves y al método criptográfico, por lo que a continuación se enlistan trabajos a futuro:

- Implementación de microprocesadores con mayor longitud en los tipos de datos que procese con la finalidad de que, en conjunto con el método criptográfico, proporcione un espacio de claves mayor.

- Diseño de métodos de cifrado en flujo para la implementación de los generadores propuestos en sistemas de comunicación segura con criptografía caótica en los cuales el canal depende de la transmisión de la información por bloques o datagramas.

- Implementación de los sistemas propuestos en el encriptado y desencriptado de otro tipo de mensaje como lo es, audio y video.

- Aplicar los métodos y prototipos propuestos en sistemas de control de acceso.

- Aplicar los métodos y prototipos propuestos integrando el sistema embebido a la red heterogénea de internet en un sistema de comunicación en tiempo real encriptando y desencriptando video conferencias.

- Implementar los mapeos caóticos y algoritmos de encriptado en otro tipo de dispositivos embebidos, tales como DSP y FPGA.

Bibliografía

(2001). *Chaos and Cryptography*, Vol. 48.

Abid, A. M., Nasir, Q., y Elwakil, A. S. (2010). Implementation of an encrypted wireless communication system using nested chaotic maps. *International Journal of Bifurcation and Chaos*, **12**: 4087–4096.

Aboul-Seoud, A. K., El-Badawy, E. S. A., Mokhtar, A., El-Masry, W., El-Barbry, M., y a. E. D. S. Hafez (2011). A simple 8 bit digital microcontroller implementation for chaotic sequence generation. *28th National Radio Science Conference*, **NRSC Egypt**: 5959–5965.

Abramson, N. (1981). *Teoría de la información*. Paraninfo, Madrid.

Abundiz, F. (2010). *Encriptado caótico de infirmación Biométrica para el Control de Accesos*. Tesis de doctorado, Universidad Autónoma de Baja California, Ensenada, Baja California. México.

Acho-Zuppa, L. (2010). Chaotic logistic map implementation in the pic12f629 microcontroller unit. *10th IFAC Workshop on Programmable Devices and Embedded Systems*, **10**: –.

Aguilar-Bustos, A. Y. y Cruz-Hernández, C. (2009). Synchronization of discrete-time hyperchaotic systems: An application in communications. *Chaos, Solitons and Fractals*, **41**: 1301–1310.

Aguilar-Bustos, A. Y., Cruz-Hernández, C., López-Gutiérrez, R. M., y Posadas-Castillo, C. (2008). Synchronization of different hyperchaotic maps for encryption. *Nonlinear Dynamics and Systems Theory*, **8**(3): 221–236.

Ameer, L. F. (2010). Implementation of digital chaotic signal generator based on reconfigurable lfsrs for multiple access communications. *Australian Journal of Basic and Applied sciences*, **4(7)**: 1691–1698.

Amini, S. (2009). A digital chaos generator for use within chaos encrypted communication systems. *2nd International Workshop on Nonlinear Dynamics and syncronization,*, **INDS 09**: 54–59.

Baptista, M. S. (1998). Cryptography with chaos. *Physics Letters A*, **240**: 50–54.

Behnia, S., Akhshani, A., Ahadpour, S., Mahmodi, H., y Akhavand, A. (2007). A fast chaotic encryption scheme based on piecewise nonlinear chaotic maps. *Physics Letters A*, **366**: 391–396.

Campos-Cantón, E., Murguía, J. S., Campos-Cantón, I., y Chavira-Rodríguez, M. (2007). Nonlinear element of chaotic generator. *Revista Mexicana de Física*, **53 (3)**: 159–163.

Campos-Cantón, E., Campos, I., Salas, J. S. G., y Cruz-Ordaz, F. (2008). A parameterized family of single-double-triple-scroll chaotic oscillations. *Revista Mexicana de Física*, **54 (6)**: 411–415.

Chen, B. y Chandran, V. (2007). Biometric based cryptographic key generation from faces. En *9th Biennial Conference of the Australian Pattern Recognition Society on Digital Image Computing Techniques and Applications*, Glenelg, Australia.

Chen, L. (2001). An open-plus-closed-loop control for discrete chaos and hyperchaos. *Physics Letters A*, **281**(5): 327–333.

Chua, L. O., Komuro, M., y Matsumoto, T. (1986). The double scroll family. *IEEE Trans. Circuits Syst.*, **33**: 1072–1118.

Cruz-Hernández, C., Inzunza-González, E., López-Gutiérrez, R. M., Serrano-Guerrero, H., y García-Guerrero, E. E. (2010). Encrypted audio communication based on syncronized unified chaotic systems. *World Academy of Science, Engineering and Technology*, **66**: 869–874.

Diffie, W. y Hellman, M. E. (1976). New directions in cryptography. *IEEE Transactions of Information Theory*, **IT-22**: 644–654.

Ditto, W. L., Murali, K., y Sinha, S. (2006). Chaos computing: Ideas and implementation. En *The 9th Experimental Chaos Conference*, São Paulo, Brazil.

EFF, editor (1998). *Cracking DES: Secrets of Encryption Research, Wiretap Politics and Chip Design*. O'Realli and Associates.

Fateri, S. y Enayatifar, R. (2011). A new method for image encryption via standard rules of CA and logistic map function. *International Journal of Physical Sciences*, **6**(12): 2921–2926.

Feng-ying, W., Xiao-li, H., y Guo-wei, C. (2012). An improved image encryption algorithm based on chaotic logistic map. *Fifth International symposium on Computational Intelligence and Design*, **1**: –.

FIPS, editor (1977). *Data Encryption Standard*, número Publication 46, Washington, DC.

Flores-Vergara, A., Inzunza-Gonzalez, E., Garcá-Guerrero, E. E., y Zamora-Arellano, F. (2012). Diseño e implementación de un generador de caos basado en un microcontrolador de 8 bits. En *LV Congreso Nacional de Física.*, Morelia, Michoacan.

Fuster, A., Martinez, D., Hernández, L., Montoya, F., y Muñoz, J. (2001). *Técnicas Criptográficas de Protección de Datos*. Alfaomega Ra-Ma.

Galeano, G. (2009). *Programación de sistemas Embebidos en C.*. Alfaomega Grupo Editor.

Gamez-Guzmán, L., Cruz-Hernández, C., López-Gutierrez, R. M., y García-Guerrero, E. E. (2009). *Elsevier, Commun Nonlinear Sci Numer Simulat*, **14**: 2765–2775.

Geng, X. y Ding, Q. (2012). Similar-short periodicity analysis and application in image compression. *Fifth International Workshop on Chaos-Fractals Theories and Applications*, **1**: –.

Goldszztejn, A., Hayes, W., y Collins, P. (2011). Tinkerbell is chaotic. *Siam Journal on Applied Dynamical Systems*, **10 (4)**: 1480–1501.

Han, F., Hu, J., Yu, X., y Wang, Y. (2007). Fingerprint images encryption via multi-scroll chaotic attractors. *Applied Mathematics and Computation*, **185**: 931–939.

Hénon, M. (1976). A two-dimensional mapping with a strange attractor. *Communications in Mathematical Physics*, **50**(1): 69–77.

Ikeda, K. y Daido, H. (1980). Optical turbulence: Chaotic behavior of transmitted light from a ring cavity. *Phys. Rev.*, **45 (9)**: 709–712.

Inzunza, E. (2012). *Encriptado Caótico en Sistemas Biométricos*. Tesis de doctorado, Universidad Autonoma de Baja California, Ensenada, Baja California México.

Itoh, M., Yang, T., y Chua (2001). L.o. conditions for impulsive synchronization of chaotic and hyperchaotic systems. *International Journal of Bifurcation and Chaos*, **11**(2): 551–560.

Jakimoski, G. y Kocarev, L. (2001). Chaos cryptography: Block encryption ciphers based on chaotic maps. *IEEE Trans. on Circuits and systems - I: Fundamental theory and applications*, **48**(2): 163–169.

Kennedy, M. P. (1993). Three steps to chaos, part ii: A chua's circuit primer. *IEEE Trans. Circuits Syst.*, **40**: 657–674.

Kocarev, L. y Shiguo, L. (2011). *Chaos - based cryptography, theory, algorithms and applications*, página 395. Springer-Verlag, first ed. edición.

Lindsay, P. S. (1981). Period doubling and chaotic behavior in driven anharmonic oscillator. *Phys. Rev.*, **47**: 1349–1352.

Liu, S., Sun, J., y Xu, Z. (2009). An improved image encryption algorithm based on chaotic system. *Journal of computers*, **4**(11): 1091–1100.

Lorenz, E. N. (1963). Deterministic nonperiodic flow. *J. Atmosph Sci*, **20**: 130–141.

Lu, J., Chen, G., Yu, X., y Leung, H. (2004). Desing and analysis of multiscroll chaotic attractors from saturated function series. *IEEE Trans. Circuits Syst. I Regular Papers*, **51(12)**: 2476–2490.

May, R. M. (1976). Simple mathematical models with very complicated dynamics. *Nature*, **261(5560)**: 459–467.

Moon, F. C. (1992). *Chaotic And Fractal Dynamics. An Introduction for applied Scientists and Engineers*. WILEY-VCH Verlag Gmbh & Co. KGaA, Cornell Univerity, Ithaca, New York.

Newcomb, R. y Sathyan, S. (1983). An rc op amp chaos generator. *IEEE Trans. Circuits Syst.*, **30**: 54–56.

Patidar, V., Pareek, N. K., Purohit, G., y Sud, K. K. (2011). A robust and secure chaotic standard map based pseudorandom permutation-substitution scheme for image encryption. *Optics Communications*, **284**(2011): 4331–4339.

Pecora, L. M. y Carrol, T. L. (1991). Driving systems with chaotic signals. *Phys. Rev*, **A44(4)**: 2374–2383.

Saito, T. (1985). A chaos generator based on a quasi-harmonic oscillator. *IEEE Trans. Circuits Syst.*, **32**: 320–331.

Shannon, C. E. (1949). Communication theory of secrecy systems. *Bell. Sys Tech. J.*, **28**: 656–715.

Shaoliang, Y. y Jiang, T. (2011). Bifurcation and chaos in the tinkerbell map. *International Journal of Bifurcation and Chaos*, **11**: 3137–3156.

Shimizu, A. y Mitaguchi, S. (1988). Fast data encipherment algorithm feal. *Eurocrypt '87*, **1**: 267–278.

Simin, Y., Jinhu, L., Leung, H., y Guanrong, C. (2005). Desing and implementation of n-scroll chaotic attractors from a general jerk circuit. *IEEE Trans. Circuits Syst. I Regular Papers*, **52(7)**: 1459–1476.

Sinha, S. y Ditto, W. L. (1998). Dynamics based computation. *Phys. Rev. Lett*, **81**: 2156–2159.

Sinha, S. y Ditto, W. L. (1999). Computing with distributed chaos. *Phys. Rev.*, **E(59)**: 363–377.

Sorking, A. (1984). A cryptographic algorithm. *Cryptologia*, **8**: 22–35.

Stanciu, M. y Datcu, O. (2012). *Atmel AVR Microcontroller Implementation of a New Enciphering Algorithm Based on Chaotic Generalized Hénon Map*. Tesis de doctorado, Politehnica University of Bucharest, Faculty of Electronics Telecommunications, and Information Technology., Bucharest, Romania.

Sunnel, M. (2006). Electronic circuit realization of the logistic map.

Tang, K. W., Kwok, H. S., y Man, K. F. (2008). A chaos-based random number generator for eight-bit micro-controller system. *International Journal of Bifurcation and Chaos*, **3**: 852–867.

Tanougast, C. (2011). Hardware implementation of chaos based cipher: Design of embedded system for security applications. *1st Edition, Springer-Verlag*, **Ch 9**: 297–330.

Verhulst, P. F. (1845). Recherches mathematiques sur la loi d' accroissement de la population. *Nouv. mém. de l' Academie Royale des Sci. et Belles-Lettres de Bruxelles*, **18**: 1–41.

Wei, J., Liao, X. F., Wong, K. W., y Xiang, T. (2006). A new chaotic crystosystem. *Chaos, Solutions & Fractals*, **30**: 1143–1152.

Wu, C. y Chua, L. O. (1993). A simple way to synchronize chaotic systems with applications to secure communication system. *Int. J. Bifurcacion and Chaos*, **3(6)**: 1619–1627.

Yu-Ming, X., Bo-Cheng, B., y Qiang, X. (2010). Grid-scroll hyperchaotic system based on microcontroller digital hardware implementation. *Acta Phys. Sin.*, **59(9)**: 5959–5965.

Zamora-Arellano, F., Inzunza, E., Garcá-Guerrero, E. E., y Flores-Vergara, A. (2013). Application of stenography and chaotic encryption to send a safety text message by e-mail. En *World Academy of Science, Enginnering and Technology.*, Paris, France.

Zhang, Q., Guo, L., y Wei, X. (2010). Image encryption using DNA addition combining with chaotic maps. *Mathematical and Computer Modelling*, **52**(2010): 2028–2035.

Apéndice A

Configuración de módulos XBee transmisión-recepción.

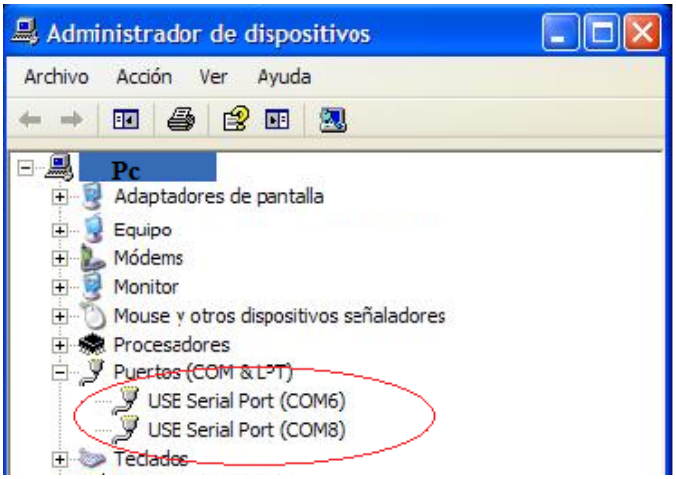


Figura 49: Asignación de puertos para módulos XBee.

Los módulos XBee utilizados en esta aplicación, son del tipo **Xbee PRO s1** y pueden ser configurados para trabajar en el modo bidireccional, es decir, un módulo puede transmitir y recibir información. Utilizan comunicación serie RS232. La forma de programar los módulos es conectándolos a una computadora con el software de control previamente instalado y grabar la configuración para comunicación según se necesite. Un método para realizar dicha operación puede ser el siguiente:

- Paso 1: Instalar en una computadora el software X-CTU y los drivers necesarios para el control de los módulos XBee.

- Paso 2: Montar el dispositivo en la placa base para comunicación con computadora, se conecta el cable en la computadora y se identifican los puertos asignados por el computador a cada dispositivo. En este caso se utiliza una PC con sistema

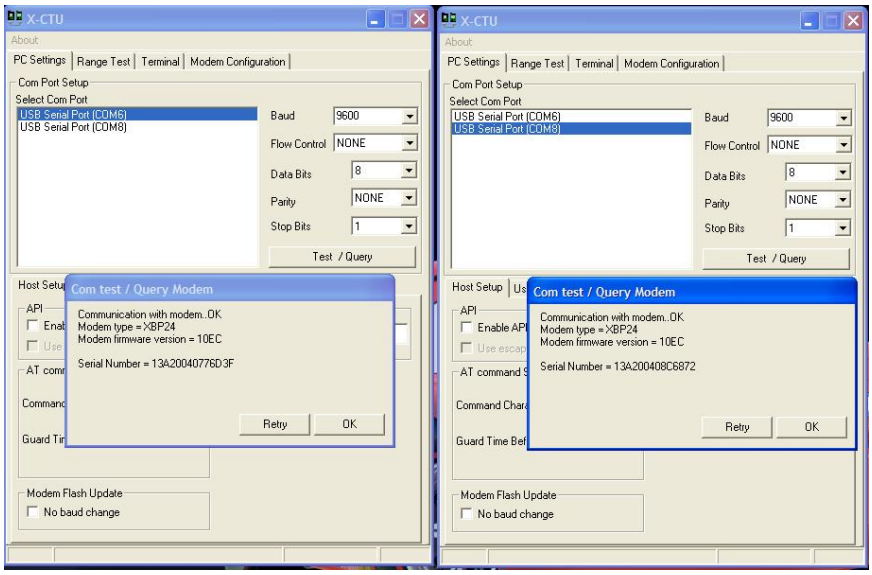


Figura 50: Prueba de detección e identificación.

operativo Windows y la figura 49 muestra la ventana de Administrador de dispositivos en la que se observa que a los módulos XBee se les asignan los puertos de comunicación serie **COM6** y **COM8** respectivamente.

- Paso 3: Una vez identificados los puertos asignados, ejecutar el software de control (X-CTU) para cada dispositivo, esto es, se ejecuta el programa dos veces al mismo tiempo. En la ventana que corresponde al primer XBee, en la sección de **Select Com Port** de la pestaña **PC Settings**, se selecciona uno de los puertos detectados y se realiza un **test-Query**, esto para garantizar la identificación y correcta comunicación del programa con el dispositivo. Si en la sección **select com port** no aparece ningún puerto **com** a seleccionar, estos se pueden agregar manualmente en la sección **User com ports** escribiendo el identificador del puerto y dando click en en botón **Add**. Este paso se realiza para los dos módulos, la figura 50 muestra las ventanas de confirmación del **test-query modem**, se observa en cada caso que se muestra el tipo de módem (en este caso dispositivos XBee), la versión del firmware del módem (en este caso **10EC**) y los números de serie respectivamente.

  Nota: si en este paso se presenta un mensaje de error en la identificación, debe

consultar el manual del dispositivo para identificar el error y realizar el proceso correspondiente para la solución del mismo. Puede que se estén aplicando parámetros distintos en la sección **PC Settings** que no corresponden o que el dispositivo tenga daño permanente. Los parámetros a utilizar son: **Baud=9600, Flow Control=NONE, Data Bits=8, Parity=NONE, Stop Bits=1**.

- Paso 4: Leer los parámetros y el firmware preinstalado en cada módulo y se modifican algunos parámetros para lograr la comunicación bidireccional en la pestaña **modem configuration**. Los parámetros a modificar son:

  1. **PAN ID**: Se asegura que ambos dispositivos tengan asignado el mismo número de ID.
  2. **Destination Address High**: Ambos dispositivos deben contener la misma dirección en este parámetro.
  3. **Destination Address Low**: Ambos dispositivos deben contener en éste parámetro,la dirección del parámetro **Serial Number Low** del módulo opuesto, esto es, el dispositivo 1 debe contener en este parámetro la dirección del **Serial Number Low** del dispositivo 2. Y el dispositivo 2 debe contener en este parámetro la dirección del **Serial Number Low** del dispositivo 1, ver figura 51. Todos los demás parámetros, deben contener los mismos valores, si alguno de ellos esta diferente, en este paso, se pueden igualar.

- Paso 5: Grabar la configuración anterior pulsando el botón **write** en la misma pestaña de **modem configuration**.

  Nota: Algunos dispositivos solicitarán el reinicio del mismo para completar dicho proceso de grabación, esto se realiza pulsando el botón de reset montado en la placa base. Si la placa base no cuenta con el botón de reset, es necesario realizar manualmente el reinicio, esto es, dando un pulso negativo en la terminal de reset en la placa base con un cable entre la terminal **Gnd** y la terminal **Reset**.

- Paso 6: Una vez grabados los dispositivos con los parámetros correspondientes,

realizar una prueba de comunicación (transmisión-recepción) entre los dispositivos, esto se realiza en la pestaña de *terminal* introduciendo datos en la sección donde se ubica el cursor, se observa como los datos que introducimos en la ventana de un dispositivo aparecen como recibidos en la ventana del segundo y viceversa, ver figura 52.

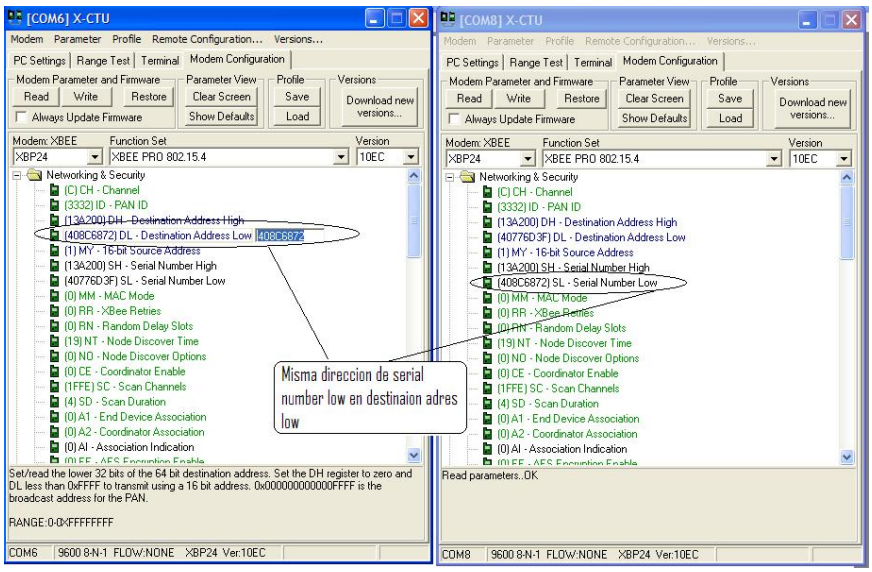


Figura 51: Configuración de direcciones destino de XBee

Figura 52: Prueba de transmisión-recepción en PC

Apéndice B

Instalación y configuración del entorno de programación Dynamic C.

B.1 Instalación de Dynamic C

Para la instalación del software realize lo siguiente:

Inserte el CD de instalación que viene junto con el hardware del sistema RCM5600W. La aplicación comienza automáticamente, siga las instrucciones a continuación. Si la aplicación no comienza automáticamente, realice la ejecución manualmente con el archivo setup.exe con la siguiente linea de comando:
¡CD¿: setup.exe

Otra forma de adquirir el software es mediante la página de soporte, donde se encuentra con la última versión del mismo.

http://www.rabbit.com/support/

B.2 Ensamble del sistema RCM5600W

El ensamble de la placa base para el desarrollo de proyectos consiste de 4 pasos básicos importantes que se describen a continuación, la figura 53 muestra los elementos que componen el equipo de desarrollo estandar:

- Primer paso: se prepara la placa base instalando los conectores standoff plásticos

en las esquinas de la misma, con el fin de protejer la placa base de superficies metálicas y para dar estabilidad. ver figura 54.

- Segundo paso:se instala el módulo del procesador en la placa base ajustandolo como se muestra en la figura 55 y asegurandolo con el clip de seguridad como muestra la figura 56; El clip de seguridad permite colocar y quitar el módulo procesador de la placa base con gran facilidad.

- Tercer paso: se instala la antena colocando la base de la misma en el soporte metálico que se incluye y colocándola en el extremo que corresponde y fijando dicho soporte con el conector stanoff; después enroscar la antena. ver figura 57.

- Cuarto paso: finalmente se conecta el cable USB, este cable tiene el propósito de funcionar como fuente de voltaje y de interface con el sofftware cuando se conecta con la PC. Para el caso en el que el dispositivo este en una aplicación real, el equipo cuenta con un adaptador AC.

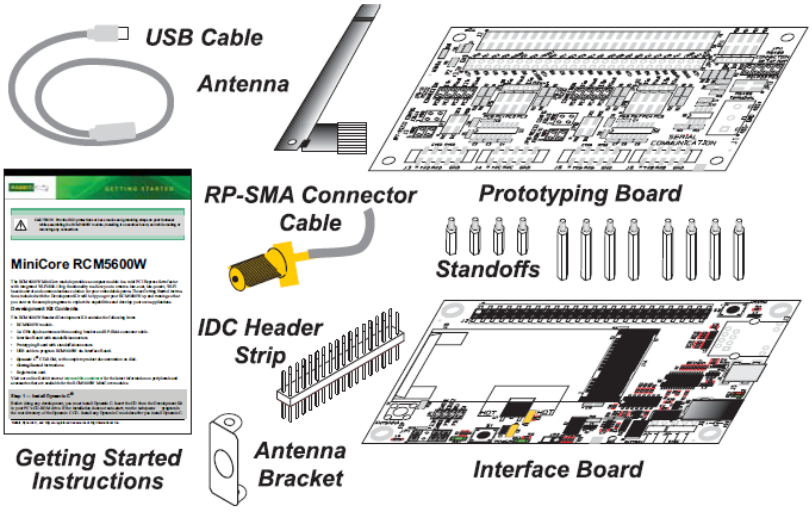


Figura 53: Equipo de desarrollo RCM5600W estandar.

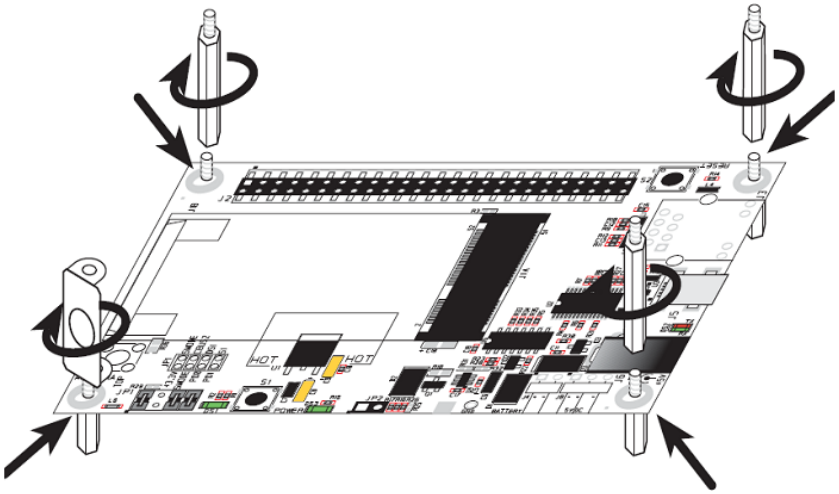


Figura 54: Instalación de conectores Standoffs en la placa base.

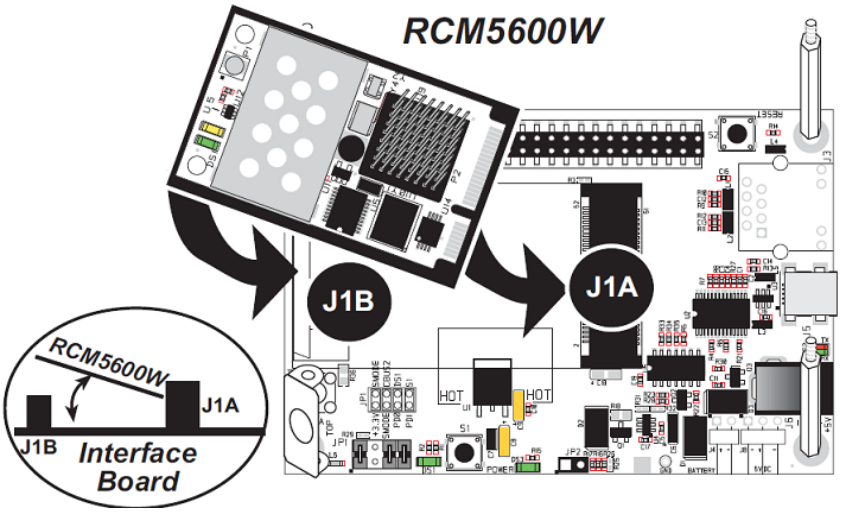


Figura 55: Instalación del procesador RCM5600W en la placa base.

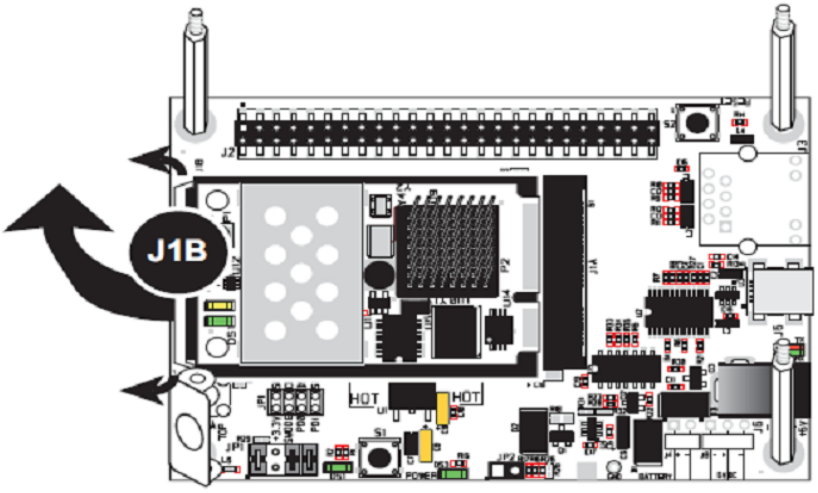


Figura 56: Clip de seguridad del procesador en la placa base.

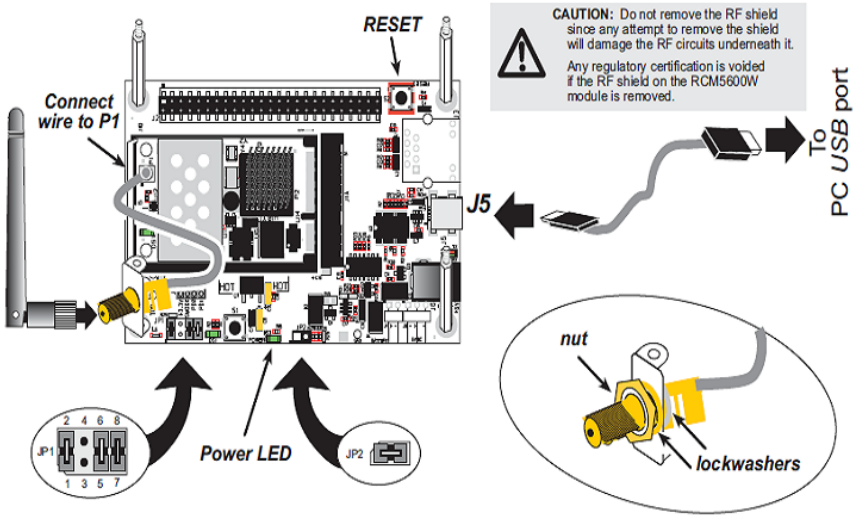


Figura 57: Conexión de antena y cable USB.

Apéndice C

Publicaciones derivadas del presente trabajo de tesis y publicaciones en colaboración.

C.1 Publicaciones

Flores-Vergara *et al.* (2012).

C.2 Publicaciones en colaboración

Zamora-Arellano *et al.* (2013).