PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

FACULTAD DE CIENCIAS E INGENIERÍA

DISEÑO E IMPLEMENTACIÓN DE UN CONTROL REMOTO SEGURO ANTE INTERCEPTACIÓN PARA PUERTA LEVADIZA DE GARAJE

Tesis para optar el Título de Ingeniero Electrónico, que presenta el bachiller:

Rubén Paul Alvarado Martínez

ASESOR: Javier Chang Fu

Lima, Febrero del 2011

RESUMEN

Vivimos en una sociedad en la cual la posibilidad de sufrir un robo se encuentra siempre presente en nuestras actividades diarias. Según el INEI, 8.3% de las viviendas en Lima fueron víctimas de asalto en el año 2006. Un método conocido para ingresar sin autorización a una residencia consiste en el sondeo y retransmisión de señales que accionan la apertura de una puerta de garaje a control remoto. El problema es grave debido a que muchos usuarios cuentan con sistemas de control remoto de puerta de garaje obsoletos que no proveen ninguna seguridad ante este tipo de ataque, esto último, debido al desconocimiento de las características de seguridad de sus sistemas o al elevado costo que implica la adquisición de equipos importados, ya que en el Perú no se fabrican estos dispositivos.

El presente tema de tesis tiene por objetivo diseñar e implementar un transmisor/receptor de control remoto cifrado para puerta de garaje en base al algoritmo de cifrado SNOW 2.0, el cual garantiza que únicamente la persona autorizada en posesión del control remoto puede accionar la apertura y cerrado de la puerta. Cualquier transmisión grabada por personas no autorizadas y que sea retransmitida será reconocida por el sistema e invalidada. Ello servirá para un posterior desarrollo de un sistema completo de puerta de garaje a control remoto con las características mencionadas anteriormente y con un costo similar al que se pagaría por un equipo adquirido en los Estados Unidos.

FACULTAD DE
CIENCIAS E
INGENIERÍA

PONTIFICIA
UNIVERSIDAD
CATÓLICA
DEL PERÚ

TEMA DE TESIS PARA OPTAR EL TÍTULO DE INGENIERO ELECTRÓNICO

Título	:	Diseño e implementación de un control remoto seguro ante interceptación para puerta levadiza de garaje
Área	:	Circuitos y Sistemas # 859
Asesor	:	Javier Chang Fu
Alumno	:	Rubén Alvarado Martínez
Código	:	20060202
Fecha	:	4 de octubre de 2010

PONTIFICIA UNIVERSIDAD CATOLICA DEL PERU
FACULTAD DE CIENCIAS E INGENIERÍA
DECANO
19-10-10

Descripción y Objetivos

Vivimos en una sociedad en la cual la posibilidad de sufrir un robo se encuentra siempre presente en nuestras actividades diarias. Según el INEI, 8.3% de las viviendas en Lima fueron víctimas de asalto en el año 2006. Un método conocido para ingresar sin autorización a una residencia consiste en la interceptación y retransmisión de señales que accionan la apertura de una puerta de garaje a control remoto. El problema se agrava debido a que muchos usuarios cuentan con sistemas de control remoto de puerta de garaje obsoletos que no proveen ninguna seguridad ante este tipo de ataque. Ello debido al desconocimiento de las características de seguridad de sus sistemas o al elevado costo que implica la adquisición de equipos importados, ya que en el Perú no se fabrican estos dispositivos.

El presente proyecto de tesis tiene por objetivo diseñar e implementar un sistema de control remoto seguro ante interceptación para puerta levadiza de garaje en base a algoritmo de encriptación, el cual garantice que únicamente la persona autorizada en posesión del control remoto pueda controlar la apertura y cerrado de la puerta. Cualquier transmisión grabada por personas no autorizadas y que sea retransmitida no generará acción alguna por parte del sistema. Se busca demostrar además que es posible fabricar un equipo con las características mencionadas anteriormente con un costo similar al que se pagaría por un equipo adquirido en los Estados Unidos.

Javier Chang Fu

PONTIFICIA UNIVERSIDAD CATOLICA DEL PERU
SECCION ELECTRICIDAD Y ELECTRONICA
Ing. ANDRES FLORES ESPINOZA
Coordinador de la Especialidad de Ingeniería Electrónica

MÁXIMO 50 PÁGINAS

FACULTAD DE
CIENCIAS E
INGENIERÍA

PONTIFICIA
UNIVERSIDAD
CATÓLICA
DEL PERÚ

TEMA DE TESIS PARA OPTAR EL TÍTULO DE INGENIERO ELECTRÓNICO

Título : Diseño e implementación de un control remoto seguro para puerta levadiza de garaje

Índice

Jower Chang Fu

PONTIFICIA UNIVERSIDAD CATOLICA DEL PERU
SECCION ELECTRICIDAD Y ELECTRONICA
Ing. ANDRES FLORES ESPINOZA
Coordinador de la Especialidad de Ingeniería Electrónica

MÁXIMO 50 PÁGINAS

ÍNDICE

INTRODUCCIÓN

El control remoto es hoy en día un dispositivo de uso altamente extendido debido a su pequeño tamaño y facilidad de uso. Encontramos controles remotos tanto en dispositivos que proveen seguridad como alarmas de autos y puertas de garaje así como en juguetes y equipos de uso doméstico.

La tendencia tecnológica actual es la reducción de costos y tamaño de equipos electrónicos. Ello ha permitido que sea cada vez más sencillo interceptar señales transmitidas utilizando computadoras portátiles, software libre y antenas fabricadas con materiales de fácil adquisición [1]. Esta falla de seguridad es especialmente importante en dispositivos de control de acceso debido a la posibilidad de ingreso por parte de personas no autorizadas [2].

El presente documento se divide en 4 capítulos. En el capítulo 1 se expone la problemática actual de los controles remotos de garaje y los productos ofrecidos por los fabricantes. A partir de ello se formulan las hipótesis de la tesis. En el capítulo 2 se detallan los conocimientos requeridos para la realización de un control remoto cifrado. El capítulo 3, enfocado a la solución planteada, muestra el diagrama de bloques de la solución y las consideraciones tomadas para ello. El capítulo 4 abarca la selección de componentes y pruebas realizadas. Todos los archivos utilizados para la realización de estas últimas se encuentran en el CD adjunto al presente documento.

CAPÍTULO 1 USO DE CONTROLES REMOTOS PARA PUERTA DE GARAJE

En el presente capítulo se presenta un estudio realizado sobre el estado del arte de equipos para apertura de puertas de garaje. Dicha investigación se enfocó en averiguar los principales productos que se encuentran en el mercado actual. A partir de ello se compararon precios entre el mercado nacional y el mercado estadounidense. Posteriormente se analizó el marco problemático que presentan los controles remotos utilizados hoy en día. A partir de estos factores se elaboraron las hipótesis que justifican la realización de la tesis.

1.1 Consideraciones iniciales en la investigación

Al utilizar la frase “control remoto seguro” se comete una ambigüedad en el sentido de que la palabra “seguro” tiene más de una acepción. Con ella podemos referirnos a que dicho control está exento de peligro o que el dispositivo posee una comunicación infalible. Es por ello que resulta necesario aclarar ante que factor es seguro un control remoto. En el primer caso se trata de un control seguro ante fallas, mientras que en el segundo nos referimos a un control seguro ante interferencia.

Autores como Wilkinson [3], Rentergent y Hachmeister [4] abordan el tema al mencionar dispositivos con comunicación bidireccional, que sirven para el mando a distancia de maquinaria, por ejemplo grúas. La característica de seguridad, en este caso radica en el hecho de que si se produce alguna falla en la comunicación, el dispositivo en la zona de trabajo desactivará automáticamente un relé que impedirá un mal funcionamiento de la maquinaria, evitando así posibles daños a los operarios.

En sistemas de control remoto para puerta de garaje este tipo de característica es añadida mediante el uso de sensores ópticos que detectan la presencia de algún objeto que interfiere en la trayectoria de apertura o cerrado de una puerta y detienen el movimiento del motor [5], sin embargo esta característica de seguridad no ha sido considerada fundamental para el desarrollo de la presente tesis. Es por esta razón que se insiste en emplear del término “control remoto seguro ante interceptación” o de manera más corta, “control remoto cifrado”.

Por convención se considera dicho concepto definido de la siguiente manera:

“Dispositivo que permite únicamente que las personas autorizadas activen o desactiven funciones del dispositivo en la zona de trabajo, en este caso específico se trata de un motor acoplado a una puerta de garaje”.

Finalmente es necesario poner en claro que una puerta de garaje a control remoto consta de brazos mecánicos, resortes, un motor, unidad transmisora y receptora. Es este sistema transmisor/receptor en el que se enfoca la presente tesis, por ser la parte más importante de una puerta de garaje a control remoto.

1.2 Estado del arte

1.2.1 Fabricantes y productos ofrecidos

Los fabricantes de controles remotos de garaje conocen las fallas de los sistemas tradicionales. Se han desarrollado soluciones de validación de mensajes transmitidos que incluyen métodos criptográficos. Actualmente en el mercado peruano se comercializan sistemas de las marcas LiftMaster, Craftsman, Sears, entre otras.

Durante la etapa de investigación se averiguaron los precios de diversos equipos de control remoto de garaje seguros ante interceptación. Se pudo notar que todos los

modelos presentados cuentan con un sistema denominado comercialmente Security+® que ofrece la transmisión de un código diferente cada vez que el control remoto es accionado, con lo cual pueden resistir un ataque por repetición de códigos. La Tabla 1-1 muestra algunos de estos dispositivos.

	Modelo	Fabricante	Características	Precio
	1345	LiftMaster	Control remoto con tecnología Security+® Sistema de motor con cadena.	$215.00*
	3585	LiftMaster	Control remoto con tecnología Security+® Sistema de motor con faja.	$260.00*
	53920	Craftsman	Control remoto con tecnología Security+® Sistema de motor con cadena.	$139.99**
	53915	Craftsman	Incluye 2 controles remotos con tecnología Security+® Sistema de motor con faja	$229.99**
*Precios ofrecidos en www.ebay.com **Precios ofrecidos por fabricante.				

Tabla 1-1 Sistemas de Puerta de Garaje a Control Remoto

Se consultó en el sitio web del fabricante Craftsman [6], donde se averiguó que el costo por compra más instalación del modelo 53915 en Estados Unidos es de $390.00, se obtuvo con la empresa Perú Door S.A.C. [7] una cotización en la que el

precio por compra e instalación de un sistema de puerta de garaje a control remoto es de $500. De esto último se obtiene que el precio a pagar en el mercado local es mayor en un 28.21%. Esta diferencia es un importante indicador para hacer notar la necesidad de un producto de origen nacional con un costo cercano al de los Estados Unidos que ofrezca un nivel de confiabilidad similar. Es este el motivo por el cual se consideró adecuado desarrollar un control remoto cifrado que pueda ser parte de un sistema completo de puerta de garaje a control remoto.

1.2.2 Sistema de control remoto con código variable

El siguiente paso en la investigación fue encontrar información acerca del sistema Security+®. No se encontró en la web referencias a este nombre comercial, sin embargo al visitar la página web de la Oficina de Patentes y Marcas Registradas de los Estados Unidos (USPTO) se obtuvo acceso a la patente de código US 7,623,663 B2, publicada en el año 2005, asignada a The Chamberlain Group, Inc. [8]**.** A continuación se describen los datos más resaltantes del sistema especificado en el documento.

Se trata de un transmisor de código variable diseñado para control de vehículos o permitir acceso mediante la apertura de una puerta u otra barrera. El dispositivo es útil para proveer una transmisión segura por RF mediante el uso de cifrado de datos. En la transmisión se emplea una cadena compuesta por una serie de bits ternarios de secuencia fija y bits ternarios de secuencia variable entrelazados. El receptor del sistema demodula la señal y separa la secuencia fija y la secuencia variable. Por comparación del código fijo y variable con una serie de códigos almacenados, el dispositivo es capaz de reconocer si la señal proviene de un transmisor autorizado o si se trata de un código repetido.

Como se ha podido apreciar Chamberlain Group, propietario de la marca LiftMaster, ya ha desarrollado un sistema seguro ante interceptación para la apertura de puertas de garaje, debido a ello se asume que los controles LiftMaster, fabricados a partir del 2005, ya cuentan con el sistema descrito en la patente especificada.

1.3 Planteamiento del marco problemático

1.3.1 Variables Internas

La adquisición de un equipo de control remoto de garaje ocurre tradicionalmente en la forma mostrada en la Figura 1-1.

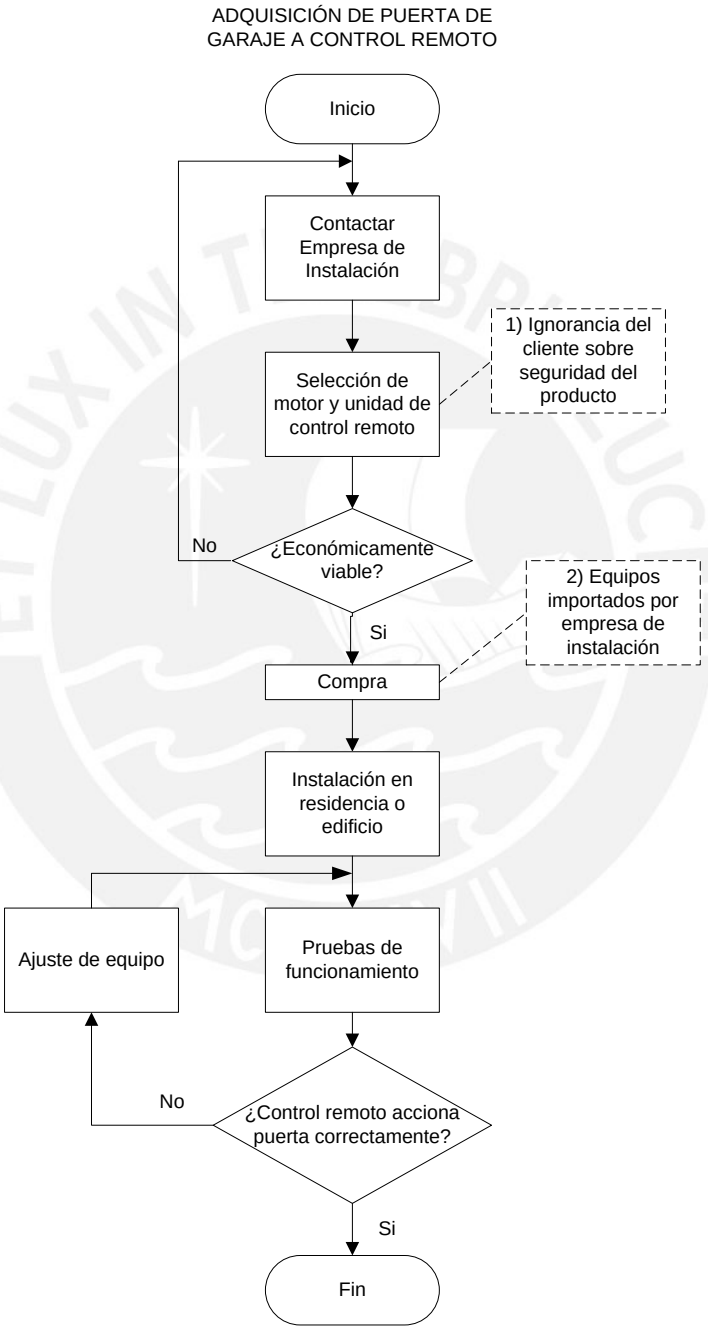


Figura 1-1 Adquisición de Puerta de Garaje a Control Remoto

Debe notarse que la problemática al adquirir sistemas de puerta de garaje a control remoto reside principalmente en 2 factores siendo el primero los costos por importación, que elevan el precio a pagar por un equipo de este tipo. En segundo lugar, se observa que hay usuarios que no están al tanto de las falencias en seguridad que tiene un control remoto tradicional, por lo cual los usuarios de equipos obsoletos han decidido no cambiarlos.

1.4 Hipótesis de la Investigación

1.4.1 Hipótesis principal

Dado que un control remoto tradicional es proclive a un ataque por repetición o captura de códigos por parte de personas no autorizadas, entonces el diseño e implementación de un control remoto cifrado permitirá obtener una alternativa confiable para un sistema de control de acceso como es el caso de una puerta de garaje a control remoto.

1.4.2 Hipótesis secundarias

- Es posible evitar un ataque por repetición o captura de código utilizando una transmisión de datos cifrada.

- Debido a los elevados costos por adquirir un nuevo equipo y al desconocimiento de las características de seguridad que debería tener un control remoto de garaje; muchos usuarios han permanecido utilizando sistemas obsoletos.

- La presente tesis será de utilidad para el desarrollo de un equipo de puerta de garaje a control remoto de origen peruano que provea un nivel de confiabilidad similar a los productos extranjeros.

CAPÍTULO 2 CONTROL REMOTO CON TRANSMISIÓN ENCRIPTADA

En este capítulo se abordan los conocimientos requeridos para elaborar un diseño de control remoto cifrado para una aplicación de control de acceso. Se explican fundamentos de criptografía, códigos de corrección de errores, transmisores y receptores de radiofrecuencia.

2.1 Criptografía

La criptografía es el proceso por el cual se convierten datos a una forma de difícil lectura por parte de personas no autorizadas. El propósito de esta operación es proveer seguridad a un canal carente de la misma, de modo tal que la información solo puede ser interpretada por aquellos que conocen un procedimiento o llave para descifrar. Los datos originales son llamados texto plano y los datos modificados son llamados texto cifrado. Los algoritmos de encriptación van desde simples sustituciones y rotaciones hasta algoritmos complejos aplicados a letras, palabras o frases [9].

En sistemas de control de acceso como puertas de auto o de garaje o bien la llave secreta es programada tanto en transmisor y receptor al ser fabricados o el receptor cuenta con un modo de aprendizaje mediante el cual incorpora nuevos transmisores válidos a una lista [10]. En la presente tesis se optó por considerar que tanto transmisor y receptor son previamente programados con las llaves secretas correspondientes, por lo que se empleó de un algoritmo de criptografía simétrica.

2.1.1 Criptografía simétrica

Como se describió en la sección anterior, los esquemas de criptografía simétrica requieren el uso de una llave secreta conocida o transmitida por un canal seguro a las

partes en comunicación. La Figura 2-1 muestra un sistema de comunicación que utiliza esta técnica.

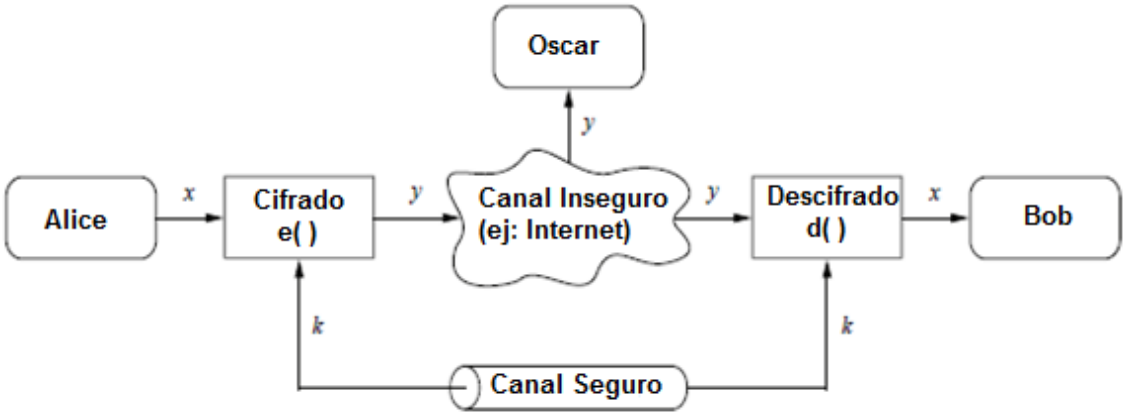


Figura 2-1 Esquema de criptografía simétrica [11]

Donde:

- Alice: es el remitente del mensaje.
- Bob: es el receptor de este mensaje y se encuentra autorizado a leerlo.
- Oscar: es un intruso del canal, puede recibir el mensaje, sin embargo no puede interpretarlo.
- E: Algoritmo de cifrado, hace que los datos que viajan por el canal aparezcan como caracteres aleatorios sin relación aparente entre ellos.
- D: Algoritmo de descifrado, ejecuta las operaciones inversas al algoritmo de cifrado para recuperar un mensaje que será leído únicamente por personas autorizadas.
- X: Texto plano, mensaje o información escrita bajo algún alfabeto o conjunto de símbolos.
- Y: Texto cifrado, información modificada para ser enviada por un canal inseguro. En la mayoría de casos la longitud y alfabeto del texto plano y cifrado son los mismos.

- K: llave secreta, conocida por las partes en comunicación o intercambiada por un canal seguro antes de llevar a cabo la transmisión de un mensaje. El conjunto de todas las llaves posibles a utilizar se conoce como espacio de llaves.

Se enuncian 2 propiedades fundamentales que debe cumplir un cifrador para ser empleado en la práctica:

Propiedad 1: Principio de Kerchoffs

"Un sistema de comunicación secreta puede ser seguro inclusive si el atacante conoce los detalles del sistema con excepción de la llave secreta. En particular el sistema puede ser seguro si el atacante conoce el algoritmo de cifrado y descifrado." [12]

Un sistema puede parecer más seguro si se ocultan los detalles de funcionamiento del cifrador, lo cual es denominado seguridad por oscuridad. Sin embargo, este tipo de sistemas no han sido sometidos a pruebas de criptoanálisis para demostrar la resistencia ante ataques. Un ejemplo es el CSS (Content Scrambling System) para protección de contenido en DVD, el cual una vez sometido a ingeniería inversa fue fácilmente roto. Por ello se recomienda el empleo de algoritmos de conocimiento público certificados por estándares de seguridad.

Propiedad 2: Confusión y Difusión

Shannon identificó 2 características con las que todo cifrador seguro debe contar. El término confusión se refiere a la capacidad del algoritmo para ocultar la relación entre el texto plano de entrada y el texto cifrado. En la práctica esto se obtiene mediante el uso de operaciones no lineales en el cifrador, por ejemplo la caja de sustitución (S-box) del cifrador AES [12]. Por otro lado el término difusión se refiere a la capacidad

del algoritmo para ocultar la relación entre 2 textos cifrados cuyas entradas difieren en un único bit. Un ejemplo de este tipo de operación es la transformación de columnas (MixColumn) del cifrador AES [11].

2.1.2 Fundamentos de cifradores de flujo

Los cifradores simétricos se clasifican en 2 tipos: de flujo (Stream Ciphers) y de bloques (Block Ciphers). Los cifradores de flujo cuentan con un estado o memoria interna y realizan cifrado de los símbolos recibidos uno a uno, mientras que los cifradores de bloques son algoritmos sin memoria interna que utilizan un tamaño de bloque de datos fijos para el cifrado [12].

La ventaja de los cifradores de flujo se debe a que son algoritmos sencillos cuyas funciones de cifrado y descifrado son las mismas, además ejecutan menos operaciones por dato cifrado que un cifrador de bloques, por lo cual pueden ser más rápidos, consumir menos potencia y utilizar menor área en un chip [13]. Es por ello que son recomendables para sistemas con hardware reducido [14].

Un cifrador de flujo perfecto, conocido como OTP (One Time Pad), consiste en utilizar una cadena infinita de bits aleatorios, llamados flujo de llave o “keystream”, con los que se puede cifrar un mensaje realizando la operación XOR bit a bit entre el mensaje y la cadena bits. Si en el lado del receptor se cuenta con esta misma cadena aleatoria, la función de descifrado consistirá en realizar un XOR del mensaje cifrado con la cadena de bits aleatorios [11] , [12].

En términos matemáticos se tiene lo siguiente:

Función de cifrado:

$$e(x) = x \oplus s = y \tag{2.1}$$

Función de descifrado:

$$d(y) = y \oplus s \tag{2.2}$$

Reemplazando (2.1) en (2.2) se obtiene:

$$d(y) = x \oplus s \oplus s = x \tag{2.3}$$

La seguridad incondicional del algoritmo está garantizada si se cumplen las siguientes condiciones:

- El flujo de llave utilizado es escogido al azar.
- Cada bit del flujo de llave es utilizado solamente una vez.

Se ha demostrado lo simple que resulta realizar una operación de cifrado o descifrado para un cifrador de flujo, sin embargo es importante observar las restricciones prácticas que dificultan cumplir los requerimientos de un OTP. La primera restricción en un sistema real consiste en la capacidad de memoria limitada con la que cuenta un computador para guardar una gran cadena de bits aleatorios, la segunda restricción importante es la necesidad de generar números que no presenten una relación conocida entre ellos.

Se hace notar que para sistemas de comunicación secreta es un requerimiento fundamental generar números aleatorios con algoritmos que impidan que un atacante prediga el resultado siguiente. Es esta una razón por la cual generadores de números

pseudoaleatorios como los utilizados en lenguaje C no proveen seguridad al sistema, ya que es posible deducir una ley de formación conforme se tengan más muestras de números generados [12] [15]. Otra alternativa para generar números aleatorios es el ruido térmico de semiconductores, sin embargo este método se descarta debido a que es complicado que ambas partes en comunicación generen los mismos números aleatorios para cifrar y descifrar [11].

2.1.3 Cifrador de flujo SNOW 2.0

Cifrador de flujo propuesto por Patrick Ekdhal y Thomas Johansson en el 2002 [16]. Estandarizado bajo la norma ISO/IEC 18033-4:2005 [17], diseñado para una rápida implementación en software El algoritmo consta de una llave secreta de 128 o 256 bits y una variable de inicialización (IV0, IV1,…, IV3) de 128 bits de conocimiento público. La operación del mismo está basada en una maquina de estados finitos (FSM) con 2 registros de 32 bits y un registro de desplazamiento con realimentación lineal (LFSR) con un tamaño de palabra de 32 bits. El cifrador utiliza las operaciones de caja de sustitución (S-BOX) como elemento no lineal que permite obtener la propiedad de confusión y la transformación MixColumns del cifrador AES como elemento que permite obtener difusión.

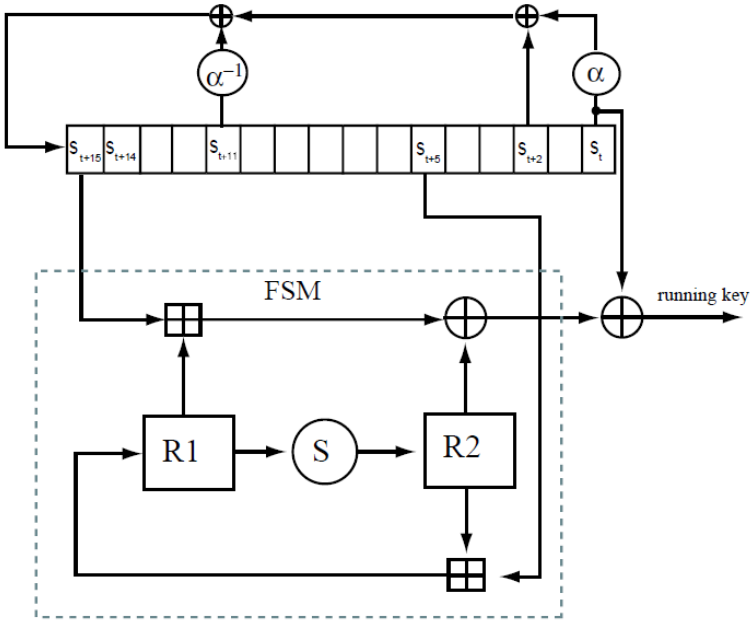


Figura 2-2 Cifrador SNOW 2.0 [18]

Para inicializar el cifrador es necesario introducir estados internos en cada una de las palabras del LFSR (St0, St1,…, St15), para ello se siguen las siguientes fórmulas en el caso de una llave (K0, K1,…, K7) de 256 bits:

$St15 = K7 \oplus IV0$	$St14 = K6$	$St13 = K5$	$St12 = K4 \oplus IV1$
$St11 = K3$	$St10 = K2 \oplus IV2$	$St9 = K1 \oplus IV3$	$St8 = K0$
$St7 = NOT(K7)$	$St6 = NOT(K6)$	...	$St0 = NOT(K0)$

Además de ello es necesario guardar un valor cero en cada uno de los registros de la FSM:

$$R1 = R2 = 0 \qquad (2.4)$$

Luego de esto se procede a actualizar 32 veces la salida del LFSR utilizando el esquema de realimentación mostrado en la Figura 2-3

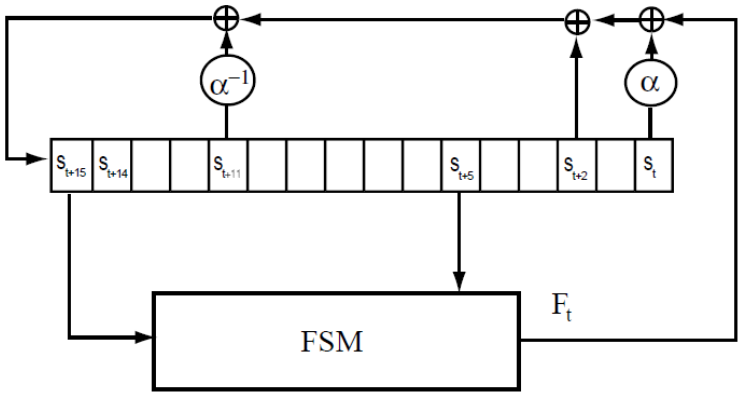


Figura 2-3 Realimentación al inicializar cifrador SNOW 2.0 [18]

Finalmente se actualiza una vez más la salida del LFSR mediante el esquema de la Figura 2-2

Realizadas estas operaciones, el cifrador se encuentra listo para generar un flujo de llave (running key en la Figura 2-2) que será añadido al texto plano mediante la operación XOR. Para descifrar deberá inicializarse el algoritmo con la misma llave secreta e IV, con ello se generara el mismo flujo de llave, luego de ello se realizará la operación XOR con el texto cifrado con lo cual se recuperará el mensaje original.

2.2 Códigos de corrección de errores

Son modos de comunicación que utilizan redundancia en la transmisión para proveer robustez al sistema, es decir que la información pueda interpretarse aunque algunos bits transmitidos cambien su valor al viajar por un canal ruidoso [19]. Para ello se define la relación entre bits de mensaje y bits enviados también llamada eficiencia de código [20].

$$\eta = \frac{k}{n} \qquad (2.5)$$

Donde:

- K: número de bits de datos.
- N: número de bits de datos más redundancia.

Para disminuir la cantidad de errores de bits en la comunicación existen 2 alternativas. La primera es aumentar la potencia de transmisión, lo cual generalmente eleva los costos del sistema. Por esta razón se prefiere disminuir la eficiencia de código agregando bits de redundancia que permitan detectar o corregir bits que han sido alterados por el canal ruidoso [21]. Los principales tipos de códigos son FEC y BEC, los cuales se definen a continuación.

Definición: FEC (Forward error correction)

"Técnicas de detección y corrección de errores en comunicaciones digitales. Para ello se agregan bits de redundancia, con los cuales es posible corregir algunos errores en la recepción del mensaje" [22].

Definición: BEC (Backward error correction)

"Técnicas de detección de errores utilizadas en canales dúplex o half dúplex en las que ante errores en la recepción se envía una solicitud de reenvio, para este caso es necesario enviar siempre un bloque de datos y un checksum" [23].

Debido a que un código FEC es capaz de detectar y corregir errores y utiliza la energía más eficientemente que un código BEC, se consideró adecuado el empleo del primero. Códigos FEC notables son los códigos hamming y el código Reed Solomon utilizado para el almacenamiento de información en CD's.

2.2.1 Códigos Hamming (n,k)

Códigos con capacidad de corrección de 1 error por bloque de datos definidos por:

$$(n,k) = (2^m - 1, 2^m - 1 - m) \quad (2.6)$$

$$m = n - k \quad (2.7)$$

Donde:

- K: número de bits de datos.
- N: número de bits de datos más redundancia.

De esta manera, algunos posibles códigos son: (7,4); (15,11); (31,26); etc.

En códigos Hamming se cumple que d_{min}=3, lo cual es el mínimo número de cambios de bits entre uno y otro código sin errores [20]. Un código en el cual los primeros k-bits son datos y los siguientes son de redundancia es denominado sistemático. En el caso de códigos de bloques la redundancia es agregada mediante la siguiente multiplicación de matrices:

$$C = d.G \quad (2.8)$$

$$[c_1 c_2 ... c_n] = [d_1 d_2 ... d_n].[I, P]$$

$$[c_1 c_2 ... c_n] = [d_1 d_2 ... d_n].\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

Donde:

- C: vector de código.
- d: vector de datos.
- G: matriz generadora.
- I: matriz identidad.
- P: matriz paridad, hay diferentes ordenes posibles para los coeficientes.

Los errores en el código se representan mediante la adición del vector error 'e', de modo que el código recibido es:

$$R = C \oplus e \tag{2.9}$$
$$[r_1, r_2, ..., r_n] = [c_1 \oplus e_2, c_1 \oplus e_2, ..., c_n \oplus e_n]$$

Para corregir errores se utiliza una matriz de chequeo de paridad H^T (de n x m), definida por:

$$H^T = \begin{bmatrix} P \\ I \end{bmatrix} \tag{2.10}$$

En la que se cumple que:

$$C.H^T = 0 \tag{2.11}$$

Con la matriz H^T se obtiene el vector síndrome 'S' dado por:

$$S = R.H^T = C.H^T \oplus e.H^T$$
$$S = e.H^T \tag{2.12}$$

Por ejemplo si:

$$S = e.H^T = [011]$$

$$e \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = [011]$$

Posibles soluciones para esta última ecuación son e=1000000; e=0001100; etc. Dado que este código considera que la probabilidad de un error en un bit es menor a 0.5, se

elige la primera solución por ser esta la más probable. De esta forma se ha detectado el bit que debe ser corregido en el código recibido [20].

2.2.2 Códigos entrelazados

Los códigos de Hamming son adecuados para corrección de errores aleatorios que se presentan en bits alejados unos de otros, sin embargo en un canal de comunicación inalámbrico práctico ocurren errores tanto aleatorios como en ráfaga [24]. Se puede mejorar el desempeño del código de corrección, al dispersar los errores en ráfaga, ello se consigue utilizando una matriz de entrelazamiento. Dicha técnica consiste en la escritura de los datos por columnas en una matriz para su posterior transmisión por filas. El receptor también utiliza una matriz del mismo modo para así recuperar la palabra en código Hamming [20]. De esta manera se logra un código de corrección más robusto tal como se muestra en la Figura 2-4.

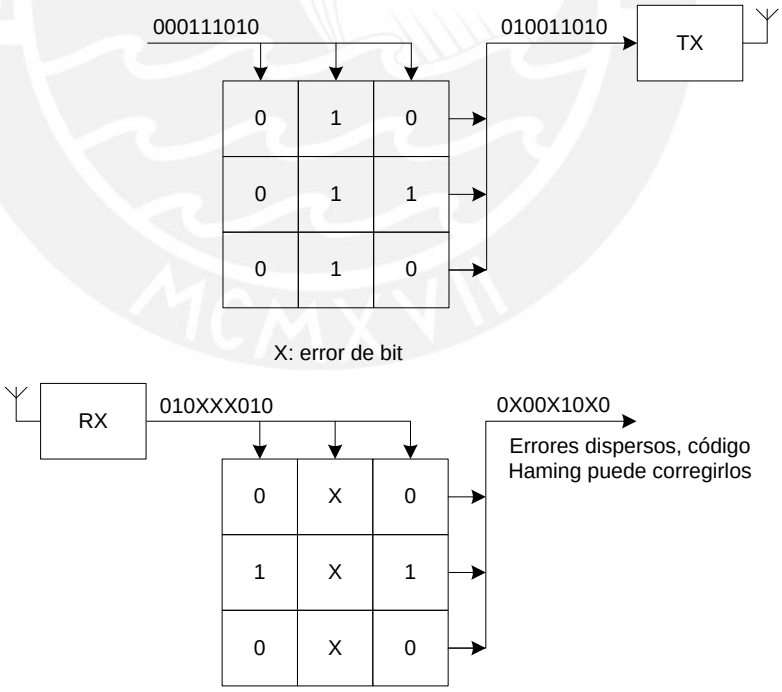


Figura 2-4 Esquema de Código Entrelazado

2.3 Transmisores y receptores digitales RF

El espectro radioeléctrico está conformado convencionalmente por ondas con frecuencias debajo de los 300 GHz [25]. De manera general se clasifica en las siguientes bandas [26]:

- ULF: 300-3 000 Hz, ondas hectokilométricas
- VLF: 3-30 kHz, ondas miriamétricas
- LF: 30-300 kHz, ondas kilométricas
- MF: 300-3 000 kHz, ondas hectométricas
- HF: 3-30 MHz, ondas decamétricas
- VHF: 30-300 MHz, ondas métricas
- UHF: 300-3 000 MHz, ondas decimétricas
- SHF: 3-30 GHz, ondas centimétricas
- EHF: 30-300 GHz, ondas milimétricas

Los criterios principales que se toman en cuenta para un formato de comunicación son la potencia de transmisión y el ancho de banda disponible. En nuestro medio, el Ministerio de Transportes y Comunicaciones (MTC) dispone que los equipos con una potencia efectiva irradiada en antena menor a 10 mW (10dBm) estén exentos del proceso de homologación. Para el radiocontrol se ha establecido que es posible utilizar frecuencias superiores a los 70MHz como frecuencia central [27]. Frecuencias centrales típicamente utilizadas son 315MHz, 433MHz, 868MHz, etc. las cuales son válidas nacional e internacionalmente [25], [28].

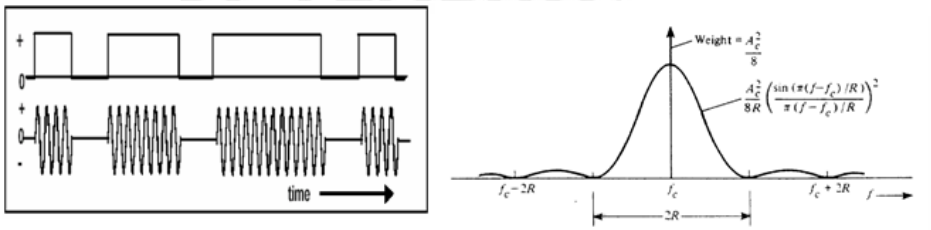
Algunos formatos de modulación utilizados en transmisores digitales son los siguientes:

- ASK/OOK: modulación digital en amplitud.
- FSK: modulación digital en frecuencia

- GFSK: modulación FSK con filtro gausiano
- MSK, QAM, PSK, etc.

2.3.1 Modulación ASK/OOK

Modulación en la cual para un bit con '1' lógico se obtiene un nivel de señal portadora y para un '0' se obtiene otra amplitud. OOK es un caso especial de esta modulación en la que no se obtiene nivel de portadora al transmitir un '0' lógico [29] tal como se muestra en la Figura 2-5.



a) b)

Figura 2-5

a) Señal OOK (abajo) y señal mensaje (arriba) [30]

b) Espectro de señal modulada en ASK/OOK [31]

El modulador consiste en un multiplicador y un filtro que reduce los cambios abruptos en la señal con lo cual se evita un ancho de banda excesivo. En la Figura 2-5 se aprecia que el ancho de banda es el doble que el de la señal en banda base. Para recuperar la señal se utiliza detección síncrona o de envolvente, en ambos casos la demodulación consiste en recuperar la señal en banda limitada y regenerar la cadena de bits original [30] tal como se muestra en la Figura 2-6.

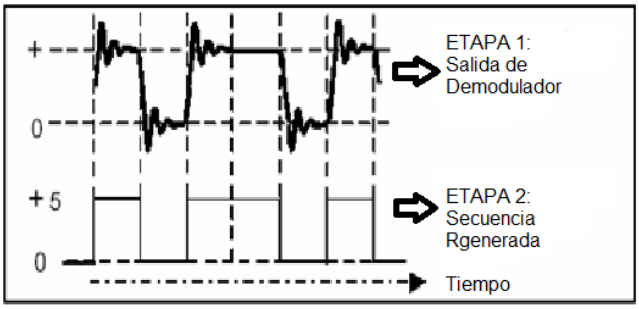


Figura 2-6 Etapas de demodulación ASK/OOK [30]

CAPÍTULO 3 CONSIDERACIONES PARA EL DISEÑO E IMPLEMENTACIÓN

En el presente capítulo se expone la solución planteada, explicando el funcionamiento de los componentes del sistema. Para ello se plantean los objetivos trazados, para luego exponer el diagrama de bloques general y el diagrama de flujo, que muestra la secuencia lógica que siguen las unidades de mando y trabajo del control remoto.

3.1 Objetivos de la investigación

3.1.1 Objetivo general

Diseñar e implementar un control remoto con transmisión cifrada, el cual garantice que únicamente la persona autorizada en posesión del mismo pueda accionar un indicador luminoso en la unidad de trabajo. Cualquier transmisión grabada por personas no autorizadas y que sea retransmitida será reconocida por el sistema e invalidada.

3.1.2 Objetivos específicos

- Diseñar e implementar un sistema de transmisión/recepción en RF con un protocolo que genere mensajes difíciles de predecir y que reconozca sólo a usuarios válidos con alcance de 20m.

- Accionar un indicador luminoso en la unidad de trabajo cuando se cumpla la condición de recepción de un código válido.

- Realizar pruebas que demuestren la inmunidad del sistema ante un ataque por repetición y captura de códigos para asegurar la confiabilidad del sistema.

- Diseñar un protocolo de comunicación cifrada que pueda formar parte de un sistema completo de puerta de garaje a control remoto.

- Realizar un diseño eficiente y de bajo consumo de energía que garantice la durabilidad del sistema al ser operado con baterías.

3.2 Solución propuesta

La solución al problema de control de acceso en su forma más básica, sin considerar cifrado y redundancia, se realiza enviando códigos que cuentan con una parte fija, que identifica al usuario, y otra variable, que evita que un código repetido sea validado [8]. En el caso de emplear comunicación simplex, la unidad transmisora incrementa la parte variable cada vez que se acciona. Por su parte la unidad receptora cuenta con un rango de códigos siguientes válidos [10], dicho rango es generalmente un número grande, con lo cual se procura evitar desincronizar las unidades al accionar fuera de rango la unidad transmisora [32]. Bajo este esquema, teóricamente siempre es posible desincronizar las unidades tal como se muestra en la Figura 3-1.

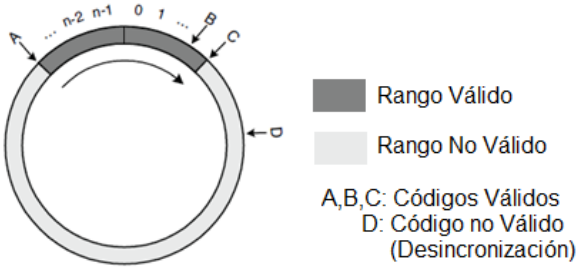


Figura 3-1 Desincronización en comunicación simplex

Otro inconveniente respecto a esta solución es la vulnerabilidad del sistema ante una captura de código, la cual consiste en la grabación de un código que no llega al receptor, por ejemplo al accionar el mando fuera de rango o con el receptor apagado. En este último caso es posible obtener acceso no autorizado al reproducir el código [10].

Se propone como alternativa emplear comunicación half-duplex, ya que, con este esquema es posible solucionar los inconvenientes de desincronización y captura de códigos anteriormente descritos con lo cual se obtiene un sistema más confiable. Para este caso se denominó unidad de mando al circuito que inicia la comunicación y unidad de trabajo al circuito que proporciona o niega el acceso.

3.2.1 Fases de comunicación Half-duplex

Todos los códigos transmitidos por este sistema son cifrados y codificados para la corrección de errores en la recepción. Los códigos constan de 48 bytes. El sistema realiza comunicación half-duplex, la cual se lleva a cabo en 3 fases. Al completarse una fase de comunicación se procede con la siguiente o en caso contrario se reiniciará la primera fase al accionar un pulsador.

Fase de Identificación

Esta primera etapa se lleva a cabo cuando el usuario presiona un pulsador en la unidad de mando. Dicha unidad envía como mensaje su identificación de usuario. Si la unidad de trabajo recibe este mensaje y reconoce que se trata de un usuario registrado se conmuta el LED respectivo en la unidad de trabajo y se prosigue con la fase de interrogación. En caso se reciba un código repetido o capturado, se logra completar esta fase, mas no las siguientes.

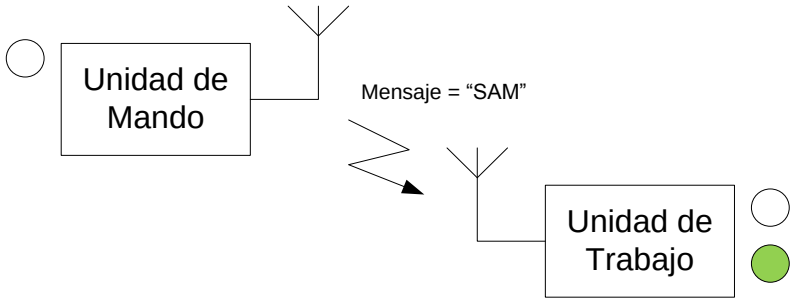


Figura 3-2 Fase de Identificación completada

Fase de interrogación

La unidad de trabajo genera un número aleatorio llamado secuencia, el cual es enviado a la unidad de mando. Si esta última reconoce un mensaje válido dirigido hacia ella, se conmuta un LED en la unidad de mando y se prosigue con la fase de validación.

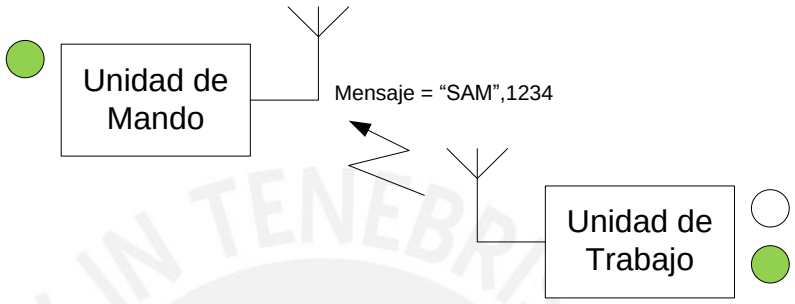


Figura 3-3 Fase de Interrogación completada

Fase de validación

La unidad de mando incrementa el valor de la secuencia recibida, agregando el comando correspondiente al pulsador accionado y envía estos datos a la unidad de trabajo. Si dicha unidad reconoce un mensaje válido en el que la secuencia generada ha sido incrementada, permite el acceso y conmuta el LED respectivo en la unidad de trabajo.

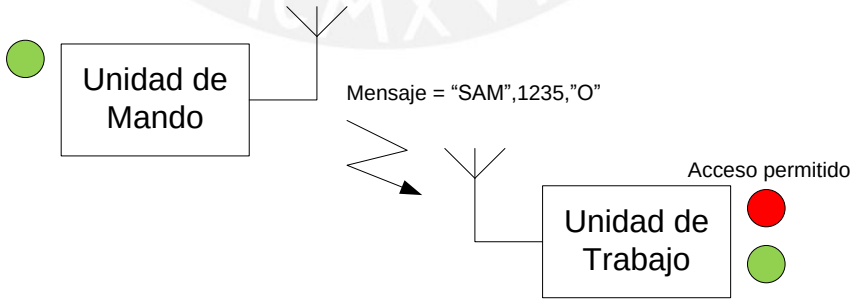


Figura 3-4 Fase de validación completada

Nótese que en este caso, la unidad de mando conoce el código que debe recibir la unidad de trabajo, de este modo se evita una posible desincronización de las

unidades. Adicionalmente se logra seguridad ante captura de códigos, ya que un intruso no puede descifrar el valor de la secuencia que envía la unidad de trabajo para incrementarla. Dicha secuencia es generada aleatoriamente cada vez que se completa la fase de identificación, por lo cual los ataques por repetición y por captura no son aplicables.

3.3 Diagrama de bloques

La transmisión y recepción de los códigos se realiza bajo el diagrama de bloques de la Figura 3-5.

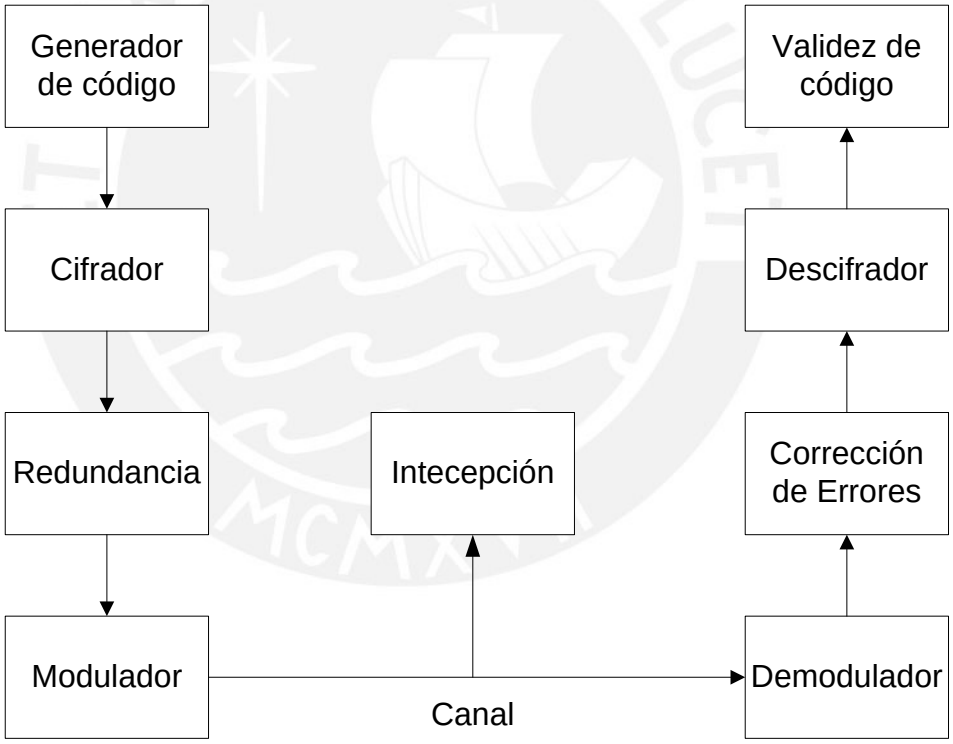


Figura 3-5 Diagrama de bloques de Transmisión y Recepción de códigos

3.3.1 Generador de código

Según la fase de comunicación en la que se encuentre el sistema, genera el mensaje respectivo. La salida de esta etapa es un bloque de 8 bytes. Si el mensaje es de una menor longitud, se completa con ceros los demás bytes.

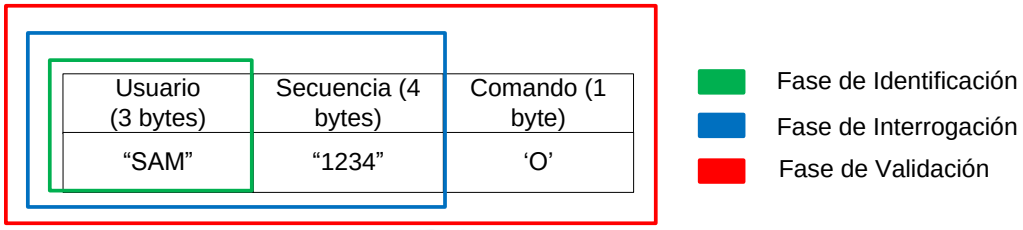


Figura 3-6 Mensajes según fases de comunicación

3.3.2 Cifrador

Se utiliza el cifrador de flujo SNOW 2.0, el cual es de conocimiento público y con características de seguridad comprobadas mediante criptoanálisis [14]. En esta aplicación, las unidades de mando y trabajo son programadas previamente con las mismas llaves secretas, por lo cual no es necesario transmitir estas por un canal seguro. Luego de ejecutar el algoritmo se agrega una variable de inicialización (IV) de 16 bytes que es utilizada en el descifrado como estado inicial. La salida de esta etapa es un bloque de 24 bytes.

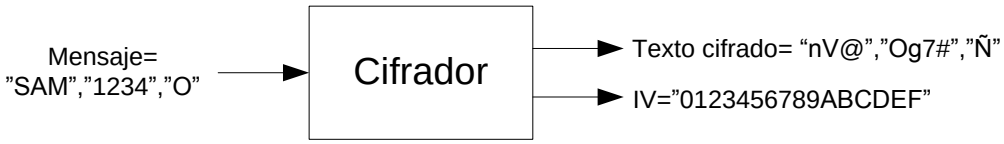


Figura 3-7 Entrada y salidas del bloque Cifrador

3.3.3 Redundancia en Transmisión

Esta etapa consta de codificación Haming (7,4) y entrelazado, los cuales proporcionan robustez al código ante errores de bits en el canal de radio. Esta es la etapa previa a la modulación. La salida de esta etapa es un bloque de 48 bytes.

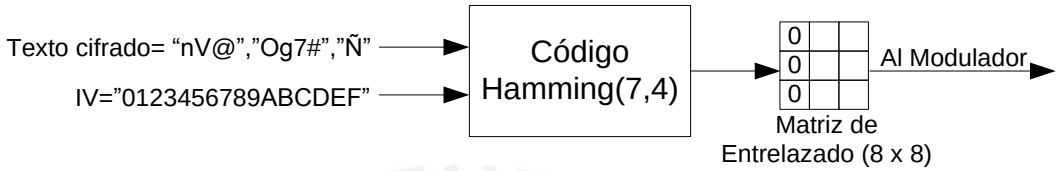


Figura 3-8 Entradas y salida del bloque de Redundancia en Transmisión

3.3.4 Modulador

Consta del módulo transceptor de radiofrecuencia TRM-315 en modo transmisor y la antena en chip ANT-315-SP. El bloque de entrada es modulado en OOK con una portadora de 315 MHz.

3.3.5 Demodulador

Consiste en el módulo TRM-315 en modo receptor y la antena ANT-315-SP. Limita en banda y regenera el bloque de 48 bytes. Es necesario que la salida de esta etapa pase a través del algoritmo de corrección de errores.

3.3.6 Corrección de Errores

Algoritmo que invierte el entrelazado, calcula el vector síndrome e invierte los bits errados en el código recibido. Posteriormente a este proceso es necesario descifrar el código. La salida de esta etapa es un bloque de 24 bytes.

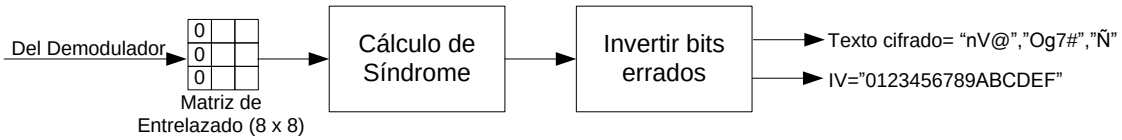


Figura 3-9 Entrada y salidas de bloque de Corrección de Errores

3.3.7 Descifrador

Convierte el mensaje cifrado en texto plano utilizando el mismo algoritmo que en el cifrado. Para realizar esta operación utiliza la llave secreta (compartida por ambas partes en comunicación) e IV recibida como estado inicial.

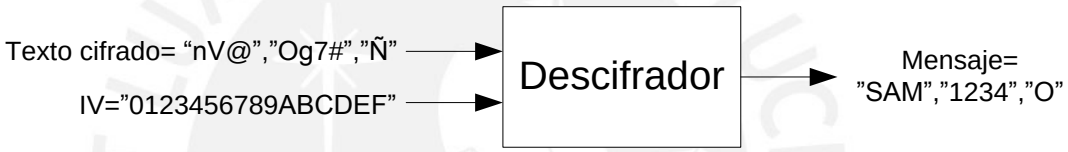


Figura 3-10 Entradas y salida del bloque Descifrador

3.3.8 Validez de código

Esta etapa comprueba que el código recibido corresponde con el código esperado en la fase de comunicación que se ha llevado a cabo. En caso de validez ejecuta la siguiente etapa de comunicación o permite el acceso en caso de la etapa de validación. En caso de código inválido se reinicia el esquema de comunicación.

3.4 Diagrama de flujo

En la solución propuesta se utilizan microcontroladores ATMEGA88PA, los cuales ejecutan los programas **"umando.hex"** y **"utrabajo.hex"** (Figura 3-11 y Figura 3-12). Ambas unidades requieren la grabación previa de las llaves de cifrado y usuario en EEPROM, para ello se emplea el archivo **"eeprom.hex"**. Para la presente tesis, se grabó en la unidad de trabajo los datos de un único usuario válido por simplicidad. En un caso general se pueden almacenar múltiples usuarios válidos y sus llaves.

El programa en la unidad de mando inicializa puertos y al cifrador e ingresa a modo ahorro de energía, tanto el microcontrolador como el módulo transceptor consumen 1000 veces menos corriente que en estado activo aproximadamente [33], [34]. El sistema sale de este modo al presionar un pulsador, luego de lo cual se habilita la comunicación UART, se forma el primer mensaje, se cifra, agrega redundancia y se transmite el código. Luego de esto el procesador cambia el módulo RF a modo receptor en espera del código de la fase de interrogación. Al recibir un mensaje con su mismo nombre de usuario, incrementa la secuencia recibida, conmuta a modo transmisor, codifica el mensaje y lo envía nuevamente, si se recibe este satisfactoriamente en la unidad de trabajo, se completa la fase de validación.

Por su parte el programa en la unidad de trabajo se inicia de manera similar al programa anterior. Coloca el módulo RF en modo receptor y espera a recibir un código válido para completar la fase de identificación. Una vez hecho esto, utiliza el cifrador para generar una secuencia aleatoria de 4 bytes. Se forma un mensaje que contiene el nombre de usuario y secuencia, se codifica con el cifrador y código de corrección de errores para transmitirse, si este código se recibe satisfactoriamente en la unidad de mando, se completa la fase de interrogación. Luego de esto la unidad de trabajo

cambia a modo receptor en espera del código de la fase de validación. Si el código requerido es recibido, se conmuta el LED de acceso en la unidad de trabajo.

Para asegurar la correcta operación de estos programas se utilizo el perro guardián (Watchdog Timer) del procesador, este módulo es utilizado para reiniciar los programas de las unidades en modo receptor en caso no lleguen a recibir un código, se temporizan 0.5 s antes de reiniciar la unidad respectiva.

Se muestran a continuación los diagramas de flujo de los programas mencionados y las subrutinas utilizadas en ambos.

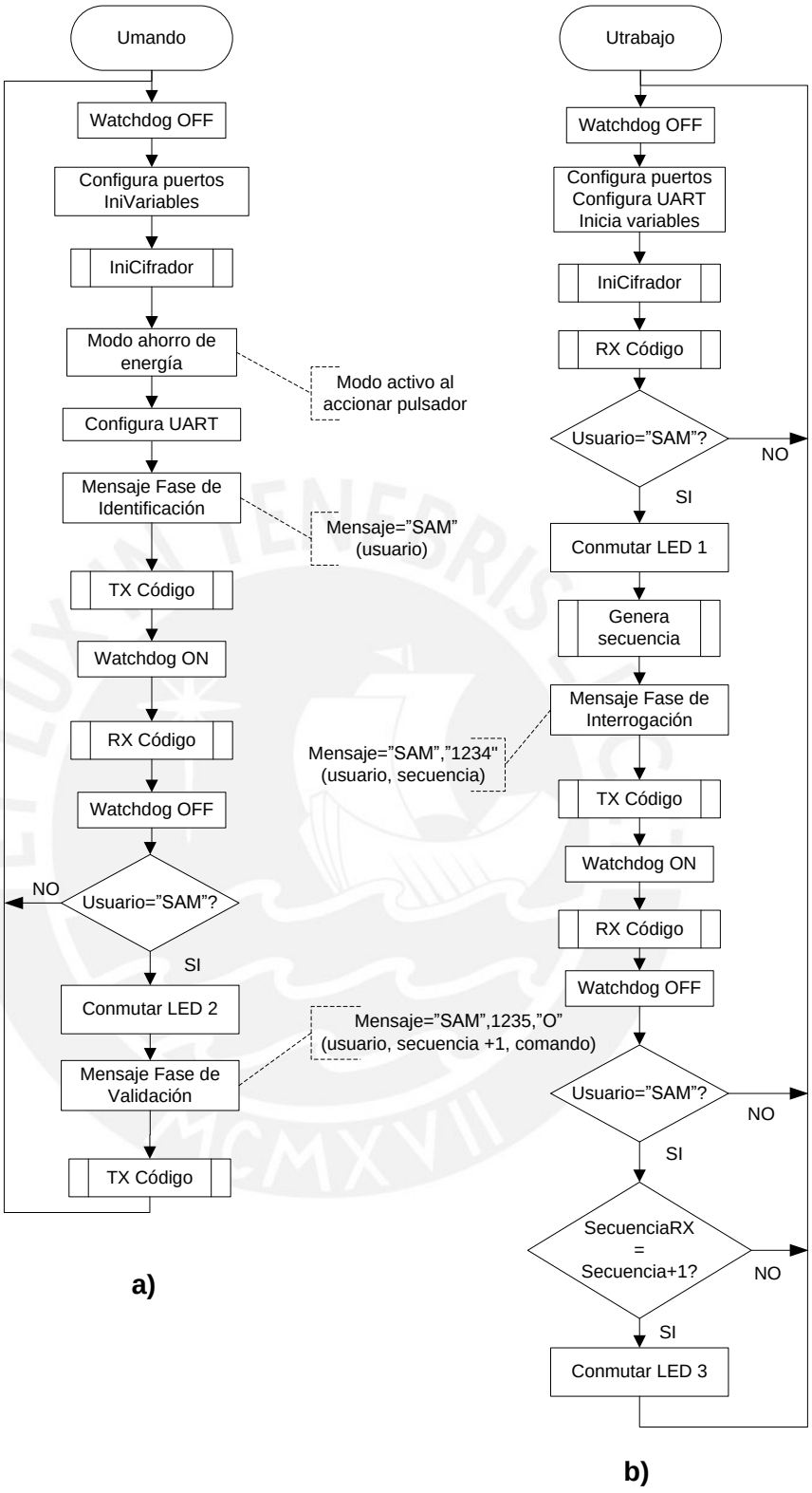


Figura 3-11

a) Diagrama de flujo de la unidad de mando

b) Diagrama de flujo de la unidad de trabajo

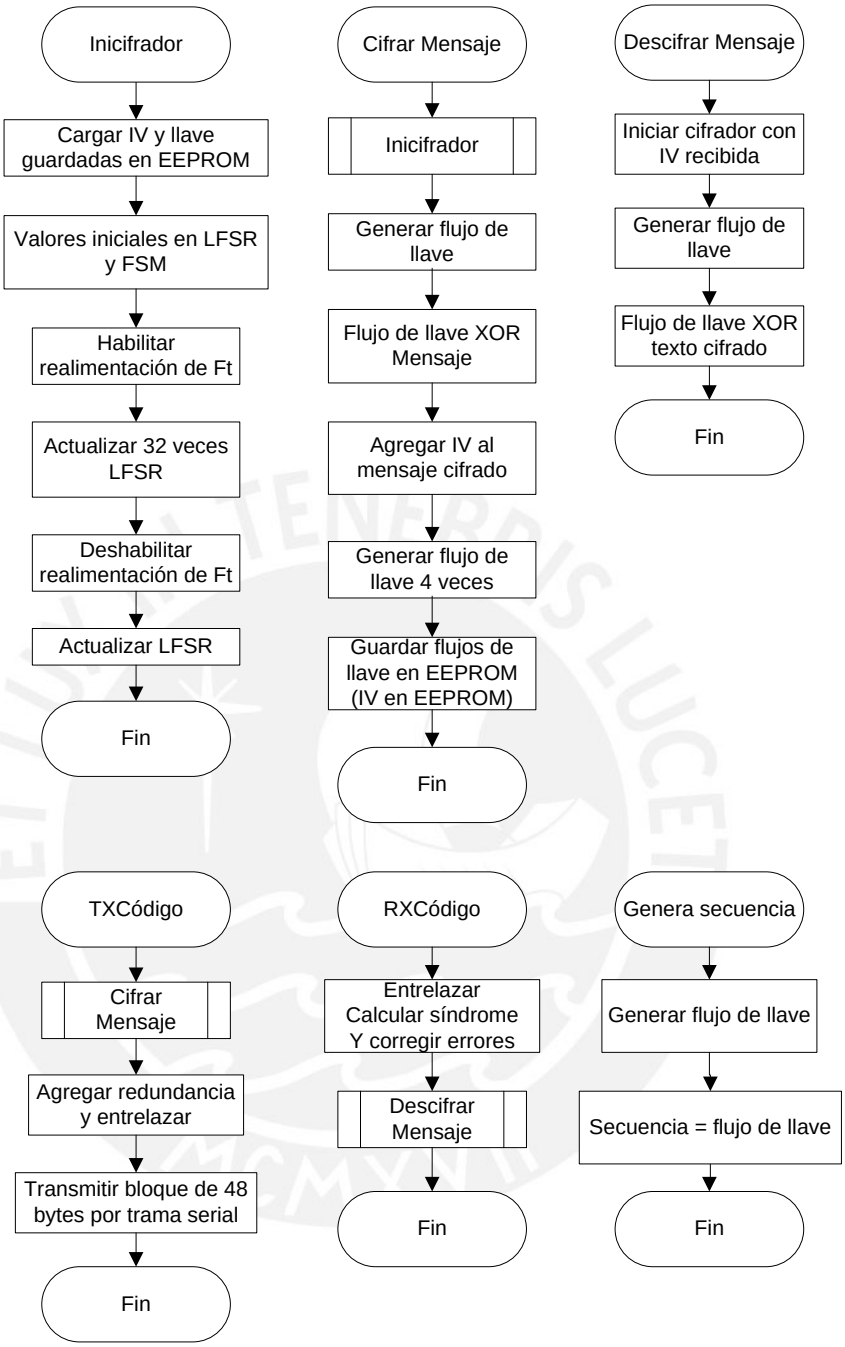


Figura 3-12 Subrutinas utilizadas en ambos programas

3.5 Diagrama esquemático

Para implementar la presente tesis se utilizaron 2 tarjetas idénticas que constan de un microcontrolador ATMEGA88PA, que realiza las 3 fases de comunicación descritas, el módulo transceptor TRM-315, la antena en chip ANT-315-SP, pulsadores y LEDS. Se utilizó una tarjeta adicional con este mismo diseño para realizar pruebas de repetición y captura de códigos.

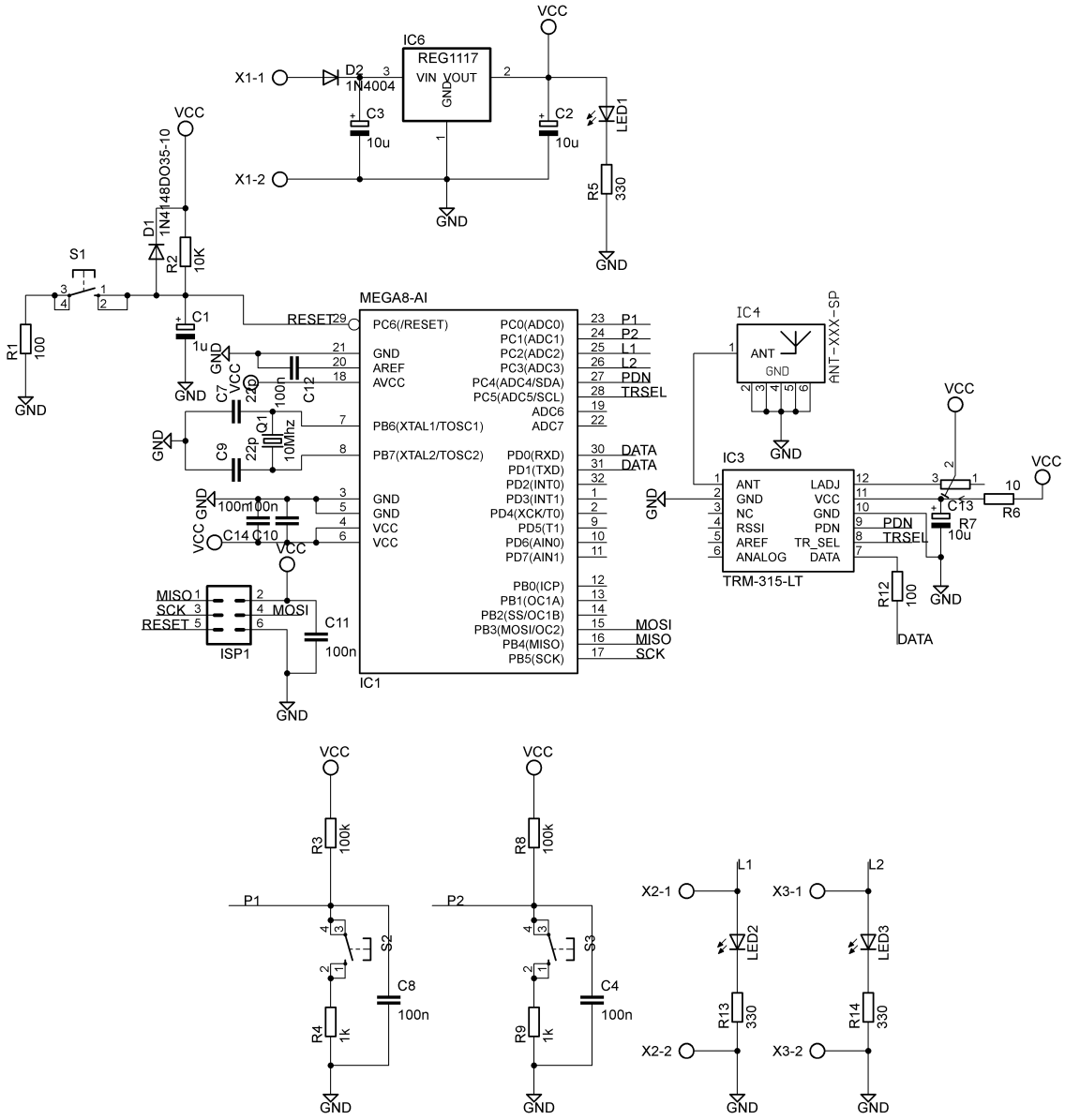


Figura 3-13 Diagrama esquemático de la Unidad de Mando y Trabajo

CAPÍTULO 4 CRITERIOS DE SELECCIÓN, IMPLEMENTACIÓN Y PRUEBAS

En el presente capítulo se define el proceso de selección de cada componente del sistema de control remoto cifrado enfocándose en las ventajas y desventajas de las alternativas encontradas y se describen las pruebas realizadas. Adicionalmente se muestra el presupuesto utilizado en la realización del proyecto.

4.1 Selección de Microcontrolador

El requisito principal para el microcontrolador a utilizar en el desarrollo de la presente tesis fue contar con un módulo de comunicación serial asíncrono UART para facilitar el envío de la trama de datos, memoria SRAM y EEPROM para almacenar la llave secreta y nombre de usuario. Fue también relevante el consumo de energía del procesador.

Ante los requisitos mencionados se encontraron 2 alternativas disponibles en el mercado local. En el primer caso se trata del microcontrolador ATMEGA88PA o un procesador superior de la misa serie. Se encontró además que otra posibilidad importante fue el microcontrolador PIC18F2550.

El primer criterio para la selección del procesador fue el número de instrucciones que este puede ejecutar por ciclo de reloj. En el caso del microcontrolador PIC, cada instrucción demora como mínimo 4 ciclos de reloj, mientras que en el ATMEGA88PA cada instrucción demora como mínimo 1 ciclo. La Tabla 4-1 presenta una comparación entre instrucciones básicas de ambos microcontroladores.

Instrucción ATMEGA88PA	Ciclos de reloj	Instrucción PIC18F2550	Ciclos de reloj
LDI	1	MOVLW	4
CLR	1	CLRF	4
ADD	1	ADDWF	4
DEC	1	DECF	4
BRNE	1 ó 2	BNZ	4 u 8
PUSH	2	PUSH	4
POP	2	POP	4
LPM	3	TBLRD	8
RCALL	3	RCALL	8
RET	4	RETURN	8
Fuentes: [33], [35]			

Tabla 4-1 Comparación de Instrucciones Básicas de ATMEGA y PIC

A partir de esta tabla se infiere que para que un PIC18F2550 pueda ejecutar un programa a una velocidad aproximadamente igual que un ATMEGA88PA, es necesario que funcione a una frecuencia 4 veces mayor.

El siguiente criterio de selección fue la potencia consumida por cada microcontrolador. Para ello se evaluó el consumo de corriente en ambos procesadores en estado activo (Tabla 4-2). Los parámetros de mayor influencia en el consumo de corriente son la frecuencia de operación y el voltaje de alimentación [33]. Se realizó la evaluación con alimentación de 5 voltios, ya que a este nivel es posible utilizar el microcontrolador PIC a su máxima frecuencia (48MHz).

ATMEGA88PA		PIC18F2550	
Vcc = 5V		Vcc = 5V	
Frecuencia (MHz)	Corriente (mA)	Frecuencia (MHz)	Corriente (mA)
0.25	0.2	1	1.1
1	0.8	4	2.5
10	5	40	21
12	5.8	48	25
Fuente: [33], [35]			

Tabla 4-2 Consumo de Corriente de ATMEGA88PA y PIC18F2550

Debido a la mayor velocidad de ejecución y eficiencia energética se seleccionó el microcontrolador ATMEGA88PA. Se utilizó un voltaje de alimentación de 3.3V y frecuencia de trabajo de 10MHz, lo cual genera un consumo de 3mA en estado activo [33]. Adicionalmente, se empleó el modo de ahorro de energía con el cual es consumo es de 0.1uA, este es el consumo del microcontrolador durante la mayoría del tiempo de operación del circuito de la unidad de mando.

4.2 Selección de Cifrador

El empleo de un cifrador en una aplicación de control de acceso es fundamental para garantizar que los códigos enviados sean impredecibles. La principal característica con la que debe contar el cifrador a ser utilizado es el bajo consumo de energía, por tratarse de una aplicación alimentada con baterías. Por otro lado, cualquier aplicación que requiera un cifrador necesita utilizar un algoritmo lo suficientemente maduro y con buenos resultados ante pruebas de criptoanálisis.

Se evaluaron como alternativas para la presente tesis los algoritmos SNOW 2.0, TRIVIUM y AES. Se muestran las características principales de estos cifradores en la Tabla 4-3:

Cifrador	Llave (bits)	Velocidad (Gb/s)*	Ataque conocido	complejidad
SNOW 2.0	128, 256	3	Distinguishing Attack	2^{174}
AES	128, 192, 256	3.82	Related-key boomerang	2^{119}
TRIVIUM	80	1.2	Brute-force	2^{90}
* Tasa de bits en procesador Pentium 4 de 1.8 Ghz ** Fuentes: [12], [36], [14]				

Tabla 4-3 Comparación de Cifradores

El indicador más importante en esta tabla fue la complejidad de ataque para cada algoritmo. Como se puede apreciar el cifrador de flujo TRIVIUM al utilizar una llave de pequeña longitud, logra brindar un menor nivel de seguridad ante un ataque de fuerza bruta, según estudios realizados por Maximov y Biryukov [37]. Por esta razón el cifrador de flujo TRIVIUM fue descartado.

El segundo lugar en complejidad de ataque fue para el estándar AES. Según investigaciones de la universidad de Luxemburgo [36] es posible realizar un ataque de recuperación de llave secreta al cifrador AES 256 con una complejidad de 2^{119}, la cual es bastante elevada. Debido a ello el cifrador continúa siendo confiable hoy en día. La National Institute of Standards & Technologies (NIST) señala que las versiones de 128, 192 y 256 bits del AES tendrán un tiempo de vida más allá del año 2030. Algunas

instituciones europeas menos optimistas estiman un tiempo de vida mínimo hasta el año 2020 [38].

Se analizó la complejidad de ataque sobre el cifrador de flujo SNOW 2.0. Según el reporte anual de ECRYPT (2009-2010) [14], es posible distinguir y predecir las salidas del cifrador al analizar 2^{174} bits de salida, lo cual es un número sumamente elevado por lo que este ataque es inaplicable en la práctica. Adicionalmente, los autores del algoritmo [18] recomiendan utilizar 2^{50} veces el algoritmo para luego cambiar la llave del mismo como una medida de seguridad.

Debido a la dificultad práctica para atacar el algoritmo SNOW 2.0, se seleccionó como el cifrador a utilizar en la presente tesis con una llave de 256 bits.

4.3 Selección de Código de Corrección de Errores

Debido a que se utilizó un protocolo de comunicación con mensajes de 8 bytes y 16 bytes de variable de inicialización (IV) del cifrador, se consideró pertinente agregar redundancia para asegurar la integridad y robustez de código. Para esta labor fueron criterios de selección la rapidez y eficiencia del código. Se consideró adecuado que esta última fuera mayor o igual al 50%.

Inicialmente se evaluó el empleo del código Reed-Solomon. Se trata de un código que trabaja con bloques de ‘m’ bits y cuya eficiencia y mejor desempeño se logra para grandes bloques de datos [39]. En este caso el bloque de datos es pequeño, lo cual resulta ineficiente para este código. Además, debido a razones de seguridad y óptimo desempeño es recomendable implementar este algoritmo en un dispositivo de mayor capacidad de cómputo como es un FPGA [40], por lo cual se descartó esta alternativa.

Posteriormente se evaluaron los códigos de Hamming y se consideró conveniente utilizar el código (7,4) debido a la eficiencia de 57.14%, que asegura integridad de la información frente a ruido, asumiendo que en el canal la probabilidad de error en un bit es menor a 0.5 [20]. Para mejorar el desempeño del código Hamming, se empleó una matriz de entrelazado de 8 x 8 bits, con lo cual se pueden corregir errores aleatorios y errores en ráfagas de hasta 8 bits. En este caso se utilizó la codificación Hamming para cada nibble de mensaje cifrado agregando un bit cero adicional para completar un byte. Con esta técnica se obtuvo código de un total de 48 bytes, los cuales incluyen mensaje cifrado y redundancia, la eficiencia en este caso es del 50%.

4.4 Selección de Módulo RF

Se evaluaron diversos módulos RF tomando como criterios la frecuencia central y máxima potencia en transmisión, además de la sensibilidad en la recepción de datos y facilidad de integración al proyecto. Estas características básicas son comparadas en la Tabla 4-4.

Fabricante	Modelo	Frecuencia central (MHz)	Potencia de transmisión máx. (dBm)	Sensibilidad en recepción (dBm)	Modulación
LYNX RF	TRM-315	315	10	-112	OOK
Texas Instruments	CC1100	300 – 928	10	-111	FSK, MSK, OOK
Hope RF	RFM12	315 – 915	8	-102	FSK

Tabla 4-4 Características básicas de Módulos RF

Estos módulos son capaces de enviar códigos hasta 1 Km de distancia en línea de vista, lo cual es más que suficiente para la presente aplicación, además de cumplir con los requerimientos legales de banda libre y potencia de transmisión [41], [28]. Se aprecia que todos estos módulos cuentan con indicadores de desempeño similares.

Por ello fue necesario analizar en detalle la sencillez de integración al presente proyecto.

Fabricante	Modelo	Requiere configuración	Componentes externos necesarios
LYNX RF	TRM-315	No	Sólo antena
Texas Instruments	CC1100	Sí (SPI)	Resistencias, bobinas, condensadores y antena
Hope RF	RFM12	Sí (SPI)	Sólo antena

Tabla 4-5 Facilidades de integración de Módulos RF al proyecto

De la Tabla 4-5 se concluye que el módulo más adecuado es el TRM-315 debido a que el único componente externo necesario es una antena y a que no es necesario configurar registros mediante un protocolo de comunicación para su funcionamiento.

Se seleccionó una antena en chip para la presente tesis debido a sus reducidas dimensiones, lo cual la hace ideal para equipos portátiles. Se seleccionó la antena ANT-315-SP debido a su adecuado desempeño y facilidad de integración en el proyecto. Otra opción similar fue el modelo KSCA-B0315AY de Systronic, sin embargo no fue posible encontrarlo en los sitios web de los distribuidores mundiales de componentes [42], [43].

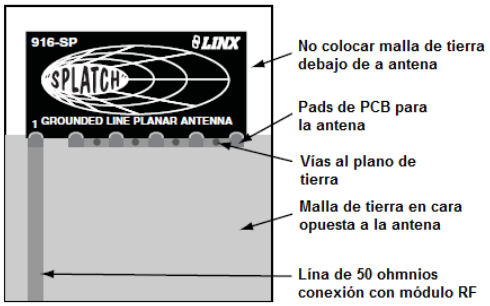
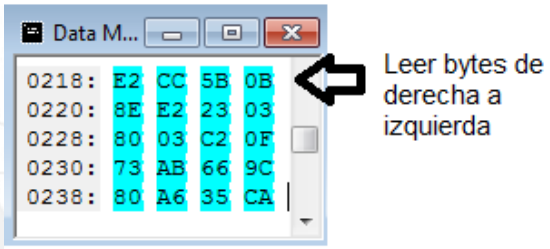
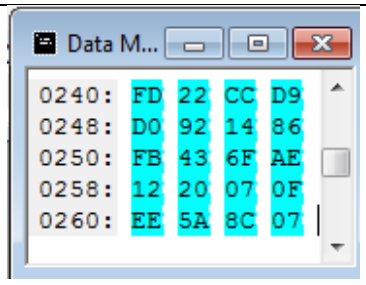


Figura 4-1 Recomendación de montaje de la antena en chip [44]

4.5 Pruebas realizadas

4.5.1 Vectores de prueba del cifrador SNOW 2.0

Una vez implementado el algoritmo para cifrado de datos se simuló el programa **"prueba1.hex"** en el entorno VMLAB. Se comprobó que para determinadas condiciones iniciales se obtienen resultados de flujo de llave especificados por los autores [18]. La Tabla 4-6 muestra los vectores de prueba (llave secreta e IV) y los flujos de llave obtenidos.

<table>
<tr><td colspan="2">Test vector 1:
LLAVE SECRETA = 0x80000000000000000000000000000000
(IV3,IV2,IV1,IV0)=(0,0,0,0)</td></tr>
<tr><td>Resultado Esperado</td><td>Resultado Obtenido</td></tr>
<tr><td>Keystream output 1...5:
keystream=0B5BCCE2
keystream=0323E28E
keystream=0FC20380
keystream=9C66AB73
keystream=CA35A680</td><td> 
</td></tr>
<tr><td colspan="2">Test vector 2:
LLAVE SECRETA = 0xAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
(IV3,IV2,IV1,IV0)=(0,0,0,0)</td></tr>
<tr><td>Resultado Esperado</td><td>Resultado Obtenido</td></tr>
<tr><td>Keystream output 1...5:
keystream=D9CC22FD
keystream=861492D0
keystream=AE6F43FB
keystream=0F072012
keystream=078C5AEE</td><td> 
</td></tr>
</table>

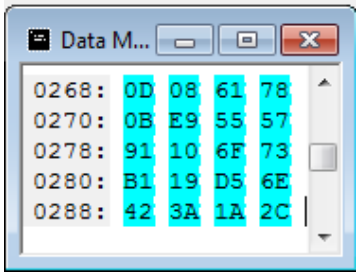
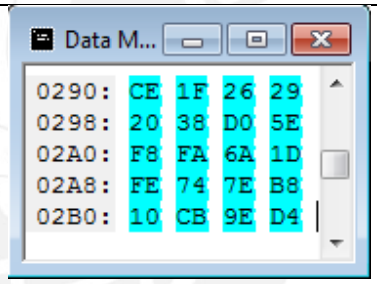
<table>
<tr><td colspan="2">Test vector 3:
LLAVE SECRETA = 0x80000000000000000000000000000000
(IV3,IV2,IV1,IV0)=(4,3,2,1)</td></tr>
<tr><td>Resultado Esperado</td><td>Resultado Obtenido</td></tr>
<tr><td>Keystream output 1...5:
keystream=7861080D
keystream=5755E90B
keystream=736F1091
keystream=6ED519B1
keystream=2C1A3A42</td><td> 
</td></tr>
<tr><td colspan="2">Test vector 4:
LLAVE SECRETA = 0x0xAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
(IV3,IV2,IV1,IV0)=(4,3,2,1)</td></tr>
<tr><td>Resultado Esperado</td><td>Resultado Obtenido</td></tr>
<tr><td>Keystream output 1...5:
keystream=29261FCE
keystream=5ED03820
keystream=1D6AFAF8
keystream=B87E74FE
keystream=D49ECB10</td><td> 
</td></tr>
</table>

Tabla 4-6 Vectores de prueba del cifrador de flujo SNOW 2.0 [18]

De este modo se comprueba que los flujos de llave obtenidos son correctos. Adicionalmente, se observó que la implementación del algoritmo tarda 1664 ciclos de reloj en cifrar 32 bits de datos, con lo cual se puede conseguir una tasa de 187.8 Kibps a 10MHz de frecuencia de reloj.

4.5.2 Prueba de autocorrelación del cifrador SNOW 2.0

La siguiente prueba se realizó con la finalidad de demostrar la impredicibilidad de las salidas del cifrador. Para ello se utilizarón los archivos "**prueba2.hex"** y **"graficos prueba2.m"** de MATLAB. se utilizo como entrada del cifrador 1 byte de datos, se obtuvieron las salidas para los 256 posibles valores decimales de este byte de entrada. Se empleó la llave secreta: 0x8000…00 y la variable de inicialización IV4..IV0=0. La Figura 4-2 muestra un fragmento de los datos de la gráfica.

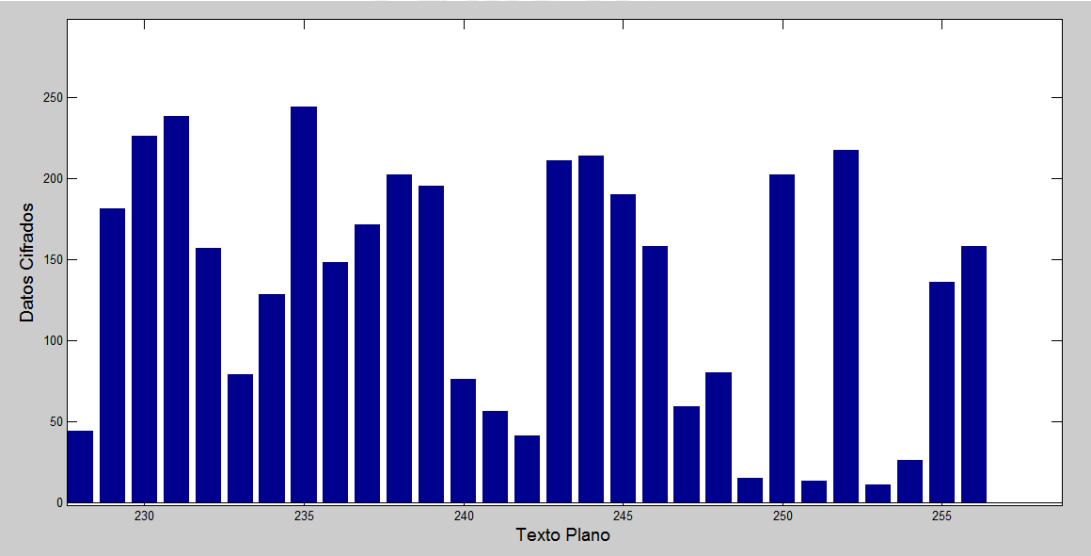


Figura 4-2 Salidas del cifrador VS entradas de texto plano

Con este resulado se demuestra que el algoritmo cumple con la propiedad de confusión pues se presenta una relacion no lineal entre texto plano y cifrado. Se observa además que el algoritmo cumple la propiedad de difusión, pues tampoco existe una relación aparente entre 2 textos cifrados que provienen de entradas que difieren en 1 solo bit [12].

Finalmente se obtuvó la autocorrelación del flujo de llave utilizado para conocer la periodicidad del mismo, el resultado obtenido se encuentra en el archivo **"graficos prueba2.m"** y se muestra a continuación.

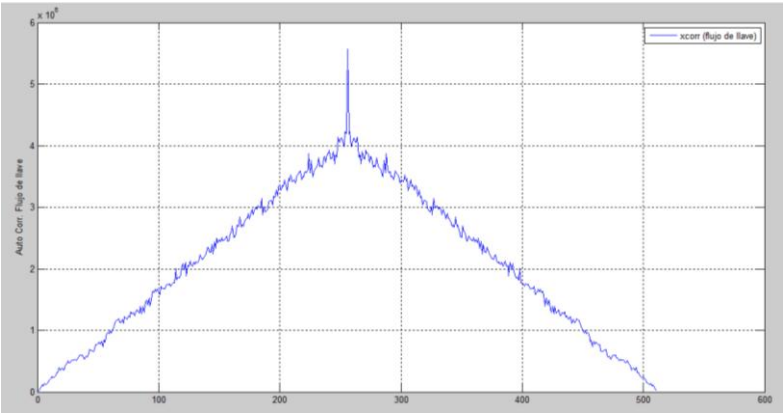
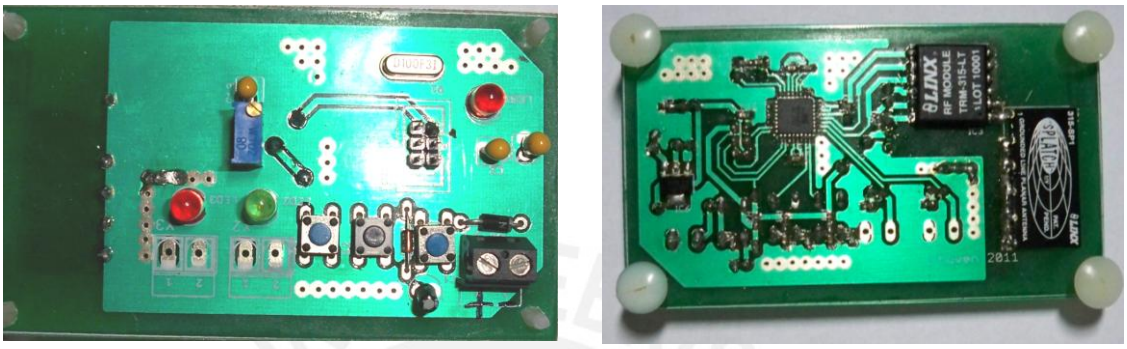


Figura 4-3 Autocorrelación de Flujo de Llave empleado

Observese que en la Figura 4-3 hay un único valor extremo, por lo cual se demuestra que el flujo de llave y las salidas del cifrador son aperiódicas para el tamaño de muestra utilizado. Esto último permite asegurar la correcta implementación del algoritmo SNOW 2.0, el cual brinda un fuerte nivel de seguridad frente a ataques por distinción como señalan sus autores [18].

4.5.3 Pruebas ante repetición y captura de códigos

Para estas pruebas se elaboraron 3 tarjetas con el diseño descrito en la sección 3.3. se observa en la Figura 4-4 una de las 3 tarjetas frabicadas.



a) **b)**

Figura 4-4

a) Circuito Implementado (capa superior)

b) Circuito Implementado (capa inferior)

Se utilizaron los programas **"umando.hex"** y **"utrabajo.hex"** en las unidades respectivas. Ambos programas utilizaron 6.6 KiB de memoria de programa en su implementación, esto se observó al simularlos en AVR Studio (Figura 4-5).

ATmega88 memory use summary [bytes]:

Segment	Begin	End	Code	Data	Used	Size
[.cseg]	0x000000	0x001a8e	3848	2944	6792	8192
[.dseg]	0x000100	0x000216	0	278	278	1024
[.eseg]	0x000000	0x000000	0	0	0	512

a) Unidad de Mando

ATmega88 memory use summary [bytes]:

Segment	Begin	End	Code	Data	Used
[.cseg]	0x000000	0x001a76	3798	2944	6742
[.dseg]	0x000100	0x000212	0	274	274
[.eseg]	0x000000	0x000000	0	0	0

b) Unidad de Trabajo

Figura 4-5 Reportes generados por entorno AVR Studio

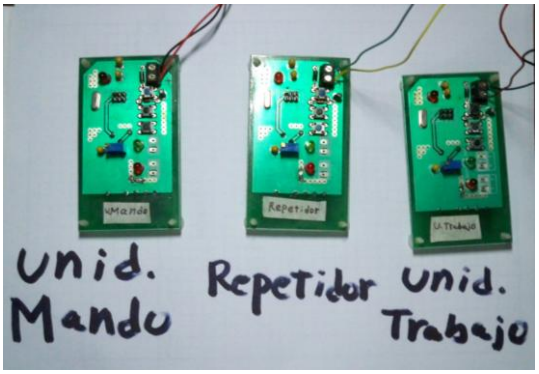
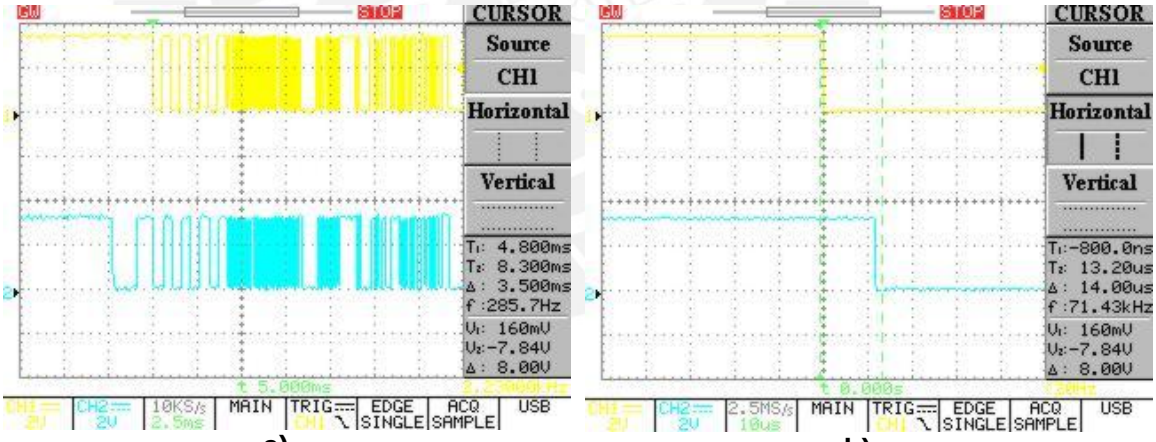


Figura 4-6 Circuitos utilizados en pruebas de repetición y captura de códigos

Para realizar un ataque por repetición se utilizó una tarjeta con el programa **"repite.hex"**, el cual graba las comunicaciones entre las unidades de mando y trabajo para repetirlas posteriormente, se emplearon los modos de grabación y transmisión del programa para copiar y reproducir los códigos de la unidad de mando, se demostró el funcionamiento del programa realizando mediciones con el osciloscopio GDS-820 (Figura 4-7).



a) b)

Figura 4-7

a) Trama enviada por unidad de mando (superior) y trama copiada (inferior)

b) Retardo entre trama original y trama copiada

Se colocó el repetidor en modo de grabación y se realizaron las 3 fases de comunicación entre las unidades, los LEDs en el la unidad de trabajo y mando, conmutan indicando las fases completadas.

Se utilizó el repetidor en modo de reproducción. Se comprobó que el código reproducido no logra ser validado por la unidad de trabajo, ello debido a que un atacante no puede incrementar el valor de la secuencia recibida en la fase de interrogación al no poseer la llave secreta. Por esta razón, envia una secuencia incorrecta, la cual impide su acceso. Se puede apreciar esta prueba en el archivo **“prueba repetición.mov”**

Adicionalmente se comprobó que el sistema es resistente a un ataque por captura de código utilizando estos mismos programas. Se colocó el repetidor en modo de grabación, se mantuvo apagada la unidad de trabajo y se inicio la comunicación en la unidad de mando. Al encender la unidad de trabajo y reproducir el código grabado por el repetidor, sólo se logra completar la fase de identificación al igual que el caso anterior, con ello se comprobó que un sistema con comunicación bidireccional es más seguro que un sistema unidireccional, ya que este último si es propenso a la captura de código. Se puede observar esta experiencia en el archivo **“prueba captura.mov”**

4.5.4 Prueba de Envió de Múltiples Códigos

Para esta prueba se utilizaron los programas **"prueba4m.hex"** y **"prueba4t.hex"** en las unidades de mando y trabajo respectivamente. Se utilizó el modo de envío de multiples códigos de la unidad de mando, con el cual se tratan de establecer las 3 fases de comunicación con la unidad de trabajo 250 veces. La unidad de trabajo llevó registro de la cantidad de los códigos que completaron la fase de validación, los cuales son guardados en EEPROM. Esta prueba fue realizada en un ambiente residencial, con las unidades colocadas en línea de vista. Se realizó la toma de datos para una distancia minima (un circuito al lado de otro) y para una distancia de 20m aproximadamente. Los resultados obtenidos se muestran en la Tabla 4-7:

Distancia	Códigos Enviados	Códigos Validados	Códigos no Validados
Mínima	500	493	7
20m	1000	974	26

Tabla 4-7 Resultados de Envío de Múltiples Códigos

De esta manera se observa que para la distancia máxima de 20m, el control remoto cuenta con una tasa de aciertos del 97.4%, con lo cual se asegura la robustez del ccódigo frente al ruido de canal que se encuentra en un ambiente real.

4.6 Cálculo de consumo de Energía

Se consideraron las corrientes consumidas por el microcontrolador, módulo transceptor y regulador empleado (AMS1117) en la unidad de mando. Se muestra el consumo de cada componente en modo de ahorro de energía (Tabla 4-8) y en modo activo (Tabla 4-9)

	Voltaje (V)	Corriente (mA)	Potencia (mW)
ATMEGA88PA	3.3	0.0001	0.00033
TRM-315	3.3	0.00015	0.000495
AMS1117	5	5	25
POTENCIA TOTAL			25
Fuentes: [33], [34], [45]			

Tabla 4-8 Potencia en Modo Ahorro de Energía

	Voltaje (V)	Modo Activo I(mA)	Potencia (mW)
ATMEGA88PA	3.3	0.5	1.65
TRM-315	3.3	12	39.6
AMS1117	5	5	25
POTENCIA TOTAL			66.25
Fuentes: [33], [34], [45]			

Tabla 4-9 Potencia en Modo Activo

Tomando en cuenta que la gran mayoría del tiempo el circuito de mando se encuentra en modo ahorro de energía se calculó el tiempo de duración de una batería de 9V Duracell MN1604 de 580mAh [43] es el siguiente.

$$t = \frac{9V}{25mW} * 580mAh = 208.8horas$$

4.7 Presupuesto

Los costos para la realización de la presente tesis son los siguientes:

Ítem	Cantidad	Costo (S/)
Microcontrolador ATMEGA88PA	3	40
Transceptor LINX TRM-315	3	170
Antena ANT-315-SP	3	20
Componentes diversos (resistencias, condensadores, reguladores, etc)	-	45
Fabricación de Circuitos Impresos	3	75
Computadora Personal	1	2600
Software VMLAB *	1	0
Software Eagle Light Edition *	1	0
MATLAB 2010 Student Version	1	270
Programador AVR ISP MKII	1	130
Multímetro CIE	1	30
Osciloscopio GWinstek GDS-820	1	4200
Costo de Ingeniería **	-	6200
	TOTAL	13780

Tabla 4-10 Presupesto del Proyecto

*Software sin costo.

** El costo de ingeniería asciende a S/6200 tomando en cuenta 10 meses dedicados al proyecto y un total de 620 horas dedicadas aproximadamente.

*** Todos los objetos listados fueron comprados.

CONCLUSIONES

- En la presente tesis se ha diseñado e implementado un sistema de comunicación bidireccional por RF capaz de reconocer usuarios autorizados y códigos anteriomente utilizados a 20m de distancia. Los códigos generados son difícilmente predecibles dado el uso del cifrador.
- Se ha probado la confiabilidad del sistema al realizar pruebas de repetición y captura de códigos notando que el sistema es capaz de reconocer estos ataques e invalidar el acceso, ello debido al protocolo de comunicación bidireccional empleado.
- Los resultados de las pruebas realizadas permiten asegurar que el presente control remoto puede ser de utilidad para el desarrollo de un sistema de puerta de garaje a control remoto de origen peruano.
- Se ha implementado el algoritmo de cifrado SNOW 2.0 en el microcontrolador ATMEGA88PA, alcanzando una velocidad de cifrado de 187.8 Kibps a 10MHz de frecuencia de reloj.

RECOMENDACIONES

- Una caraccterística adicional de especial utilidad que requiere el presente sistema, es un comando de aprendizaje por parte del receptor para de esta manera incorporar nuevos usuarios del garaje.
- La programación del algoritmo SNOW 2.0 fue realizada siguiendo una implementación referencial. Es deseable mejorar la velocidad de cifrado de datos por lo que se sugiere realizar una optimización de este programa para consumir menos tiempo y energía en generar un código a enviar.
- Se puede conseguir una implementación más eficiente del cifrador y un código FEC con mayor capacidad de corrección al emplear un dispositivio con mayor capacidad de cómputo como es un FPGA.
- Una posterior implementación de un sistema de puerta de garaje a control requerirá, además de la parte mecánica, de sensores de presencia que detenga la apertura o cerrado de la puerta al encontrarse un objeto en su trayectoria, con lo cual se obtendrá un producto más confiable.
- La implementación de un equipo comercial requerirá de un regulador con un menor consumo de corriente, con o cual se podrá extender el tiempo de operación de la unidad de mando alimentada por baterias.

BIBLIOGRAFÍA

[1]. *Scada Vs The Hackers.* **Brown, Alan S.** 12, New York : Research Library Core, 2002, Mechanical Engineering, Vol. 124, págs. 37-40.

[2]. *Control Remoto Basado En El Transceptor De Radiofrecuencia Con Microcontrolador NRF9NE5 De Nordic.* **A. Cebrián, J. Rey y J.Millet.** 2005, Revista Española de Electrónica, págs. 58-63.

[3]. *Fail Safe Radio Remote Control.* **Wilkinson, I.** 2, s.l. : Bradford, 1994, Sensor Review, Vol. 14, págs. 25-26.

[4]. **Peter Rentergent, Frank Hachmeister.** *RF Communnication In Municipal Infrastructure And Industrial Control Systems.* [Presentación] Frankfurt : s.n., 2001. Lonworld Expo.

[5]. **The Chamberlain Group, Inc.** LiftMaster Garage Door And gate Openers. *Matriz de Comparación De Modelos.* [En línea] [Citado el: 6 de Abril de 2010.] Http://Www.Liftmaster.Com/Consumerweb/Products/Gdomodelcomparisonmatrix.Htm.

[6]. **Corporation, Sears Holdings.** Craftsman Tools Homepage. [En línea] [Citado el: 20 de Abril de 2010.] Http://Www.Craftsman.Com/Shc/S/P_10155_12602_00953915000p?Vname=Storage+%26+Garage&Cname=Garage+%26+Work+Area&Sname=Garage+Door+Openers.

[7]. **Comtrol Remoto Peru Door S.A.C.** [En línea] [Citado el: 23 de Octubre de 2010.] Http://Www.Perudoor.Com/.

[8]. **Farris, Bradford L.** *Rolling Code Security System. US 7,623,663 B2* USA, 21 de Diciembre de 2005.

[9]. *Linux Security.* **Siddiqui, Shadab.** s.l. : Course Technology PTR, 2002. ISBN-10: 1931841993.

[10]. **Atmel Corporation.** *Avr411: Secure Rolling Code Algorithm For Wireless Link.* [En línea] [Citado el: 4 de Setiembre de 2010.] Http://Www.Atmel.Com/Dyn/Resources/Prod_Documents/Doc2600.Pdf.

[11]. **Paar, Christof Y Pelzl, Jan.** *Understanding Cryptography, A Textbook For Students And Practitioners.* s.l. : Springer-Verlag, 2010.

[12]. **Maximov, Alexander.** *Some Words On Cryptanalysis Of Stream Ciphers.* s.l. : Lund University, 2006. Ph.D Thesis.

[13]. **Preneel, Bart.** *Stream Ciphers: Past, Present And Future.* [Presentación] 15 de Diciembre de 2010. International ISC Conference On Information Security And Technology 2010 (ISCISC 2010).

[14]. **European Network of Excellence in Cryptology.** *Ecrypt II Yearly Report On Algorithms And Keysizes.* 2009-2010.

[15]. **Echaiz, Javier.** Universidad Nacional Del Sur. *Curso De Seguridad En Sistemas.* [En línea] [Citado el: 17 de Diciembre de 2010.] Http://Cs.Uns.Edu.Ar/~Jechaiz/Seguridad/Clases/.

[16]. *Resistance of Snow 2.0 Against Algebraic Attacks.* **Billet, Olivier And Gilbert, Henri.** s.l. : Springer, 2005. Lecture Notes in Computer Science.

[17]. **International Organization for Standarization.** Norma ISO/IEC 18033-4:2005. [En línea] 2005. [Citado el: 25 de Junio de 2010.] Http://Www.Iso.Org/Iso/Catalogue_Detail.Htm?Csnumber=39978.

[18]. *A New Version Of Stream Cipher Snow.* **Ekdahl, Patrick Y Johansson, Thomas.** s.l. : Springer-Verlag, 2002. SAC '02 Revised Papers from the 9th Annual International Workshop on Selected Areas in Cryptography.

[19]. **Linx Technologies, Inc.** Application Note AN-00160 Considerations For Sending Data Over A Wireless Link. [En línea] [Citado el: 3 de Enero de 2011.] http://www.linxtechnologies.com/Documents/TRM-xxx-LT_Data_Guide.pdf.

[20]. **Lathi, B. P.** *Modern Digital And Analog Communication Systems.* s.l. : The Oxford Series in Electrical and Computer Engineering, 1998.

[21]. **Wicker, Stephen B. Kim, Saejoon.** *Fundamentals Of Codes, Graphs, And Iterative Decoding.* s.l. : Springer, 2002. ISBN-10: 1402072643.

[22]. **Kramer, Glen.** *Ethernet Passive Optical Networks.* s.l. : The Mcgraw-Hill Companies, 2005.

[23]. **Heine, Gunnar.** *Gprs : Gateway To Third Generation Mobile Networks (Second Edition).* s.l. : Artech House, Incorporated, 2003.

[24]. **Hoel, Robin.** Texas Instruments. *FEC Implementation: Design Note Dn504.* [En línea] [Citado el: 16 de Noviembre de 2010.] Http://Focus.Ti.Com/Lit/An/Swra113a/Swra113a.Pdf.

[25]. **Ministerio De Transportes Y Comunicaciones (MTC).** Plan Nacional De Atribución De Frecuencias (PNAF). [En línea] [Citado el: 6 de Mayo de 2010.] Http://Www.Mtc.Gob.Pe/Indice/C.-%20sub-Sector%20comunicaciones/C.1.%20telecomunicaciones/C.1.4.%20bandas/C.1.4.1%20plan%20nacional%20de%20atribución%20de%20frecuencias/R.M%20187-2005mtc-03%20pnaf%20anexo.Pdf.

[26]. **International Telecommunication Union (ITU).** Nomenclature Of The Frequency And Wavelength Bands Used. [En línea] [Citado el: 20 de Diciembre de 2010.] Http://Www.Itu.Int/Dms_Pubrec/Itu-R/Rec/V/R-Rec-V.431-6-199304-S!!Pdf-E.Pdf.

[27]. **Federal Communications Commission (FCC).** Radio Frequency Devices. [En línea] [Citado el: 20 de Diciembre de 2010.] Http://Www.Gpo.Gov/Fdsys/Pkg/Cfr-2009-Title47-Vol1/Pdf/Cfr-2009-Title47-Vol1-Part15.Pdf.

[28]. —. Frequency Allocations And Radio Treaty Matters; General Rules And Regulations. [En línea] [Citado el: 20 de Diciembre de 2010.] Http://Www.Gpo.Gov/Fdsys/Pkg/Cfr-2009-Title47-Vol1/Pdf/Cfr-2009-Title47-Vol1-Part2.Pdf.

[29]. **Anthes, John.** RF Monolithics. *OOK, ASK And FSK Modulation In The Presence Of An Interfering Signal.* [En línea] [Citado el: 3 de Enero de 2011.] Http://Www.Rfm.Com/Corp/Appdata/Ook.Pdf.

[30]. **University Of Rhode Island, Department Of Electrical And Computer Engineering.** *Ele 436 Communication Systems Lab: Amplitude Shift Keying & Frequency Shift Keying.* [En línea] [Citado el: 3 de Enero de 2011.] Http://Www.Ele.Uri.Edu/Courses/Ele436/Labs/Asknfsk.Pdf.

[31]. **Couch, Leon E.** *Digital And Analog Communications Systems.* s.l. : Prentice Hall, 2001.

[32]. **Dawson, Steven.** Microchip Technology Inc. *Code Hopping Decoder Using Secure Learn.* [En línea] [Citado el: 28 de Diciembre de 2010.] Http://Www.Kitsrus.Com/Pdf/An662.Pdf.

[33]. **Atmel Corporation.** Atmega88pa Manual. [En línea] [Citado el: 29 de Diciembre de 2010.] Http://Www.Atmel.Com/Dyn/Resources/Prod_Documents/Doc8271.Pdf.

[34]. **Linx Technologies, Inc.** LT Series Transceiver Module Data Guide. [En línea] [Citado el: 5 de Enero de 2011.] Http://Www.Linxtechnologies.Com/Documents/Trm-Xxx-Lt_Data_Guide.Pdf.

[35]. **Microchip Technology, Inc.** Pic18f2550 Datasheet. [En línea] [Citado el: 30 de Diciembre de 2010.] Http://Ww1.Microchip.Com/Downloads/En/Devicedoc/39632e.Pdf.

[36]. *Related-Key Cryptanalysis Of The Full Aes-192 And Aes-256.* **Biryukov, Alex And Khovratovich, Dmitry.** s.l. : Springer, 2009. Lecture Notes in Computer Science.

[37]. *Two Trivial Attacks On Trivium.* **Maximov, Alexander And Biryukov, Alex.** 2007. The eSTREAM Project - eSTREAM Phase 3.

[38]. *On The Complexity Of Side-Channel Attacks On Aes-256 - Methodology And Quantitative Results On Cache Attacks -.* **Neve, Michael And Tiri, Kris.** 2007.

[39]. **Sklar, Bernard.** Reed-Solomon Codes. [En línea] [Citado el: 16 de Octubre de 2010.] Http://Ptgmedia.Pearsoncmg.Com/Images/Art_Sklar7_Reed-Solomon/Elementlinks/Art_Sklar7_Reed-Solomon.Pdf.

[40]. *Codificador Y Decodificador Digital Reed Solomon Programados Para Hardware Configurable.* **Sandoval, Cecilia E.** s.l. : Pontificia Universidad Javeriana, 2007. Ingeniería Y Universidad, Enero-Junio 2007.

[41]. **Ministerio De Transportes Y Comunicaciones (MTC).** Reglamento Específico De Homologación De Equipos Y Aparatos De Telecomunicaciones (D.S: 001-2006-MTC). [En línea] [Citado el: 17 de Mayo de 2010.] Http://Www.Mtc.Gob.Pe/Indice/C.-%20sub-Sector%20comunicaciones/C.1.%20telecomunicaciones/Ds-001-2006-Mtc.Pdf.

[42]. **Digi-Key Corporation.** Digi-Key Corporation Homepage. [En línea] [Citado el: 10 de Julio de 2010.] Http://Www.Digikey.Com/.

[43]. **Mouser Electronics, Inc.** Mouser Electronics, Inc. Homepage. [En línea] [Citado el: 10 de Julio de 2010.] Http://Www.Mouser.Com/.

[44]. **Antenna Factor.** Ant-315-Sp Data Sheet. [En línea] [Citado el: 6 de Enero de 2011.] Http://Www.Antennafactor.Com/Resources/Data-Guides/Ant-315-Sp.Pdf.

[45]. **Advanced Monolithic Systems.** Low Dropout Voltage Regulator Datasheet. [En línea] [Citado el: 28 de Diciembre de 2010.] Http://Www.Datasheetcatalog.Org/Datasheet/Advancedmonolithicsystems/Mxuxzrt.Pdf.

[46]. **Editec/Rede.** Apertura Auomática de Puertas. *Circuitos Prácticos De Control Remoto.* 1988.

[47]. **Texas Instruments, Inc.** CC1100 Low-Power Sub- 1 Ghz Rf Transceiver Datasheet. [En línea] [Citado el: 5 de Enero de 2011.] http://Focus.Ti.Com/Lit/Ds/Symlink/Cc1100.Pdf.

[48]. *Algebraic Cryptanalysis Of Simplified Aes.* **Simmons, Sean.** 2009, Cryptologia.

[49]. **Hope Microelectronics Co.** Universal ISM Band Fsk Transceiver Module Rfm12 Datasheet. [En línea] [Citado el: 6 de Enero de 2011.] Http://Svn.Clifford.At/Metaparts/Trunk/Datasheets/Ds_647a2fa8f4e97af8dc853299dc010412.Pdf.

[50]. **Insituo Nacional de Estadísica e Iinformática (INEI).** Nota De Prensa Inei N°130. [En línea] Mayo de 2006. [Citado el: 19 de Abril de 2010.] http://Www1.Inei.Gob.Pe/Web/Notaprensa/Attach/6350.Pdf.