Mensajería Cifrada en Radios VHF Comerciales

Ramirez Javier Eduardo
Ingjavierramirez@gmail.com
Universidad Piloto de Colombia

Abstract-This paper presents a radio link on inexpensive commercial radios highlighting the encrypted data sent. Data transmission is done by FSK (frequency shift keying) and for this a microchip from freescale empela family. Developed interfaces allow communication between computers and mobile phones that have bluetooth.

Resumen— El presente trabajo presenta un radio enlace sobre radios comerciales de bajo costo resaltando él envió de datos cifrados. El envío de datos se hace mediante FSK (Modulación por desplazamiento de frecuencia) y para ello se empela un microship de la familia freescale. Las interfaces desarrolladas permiten la comunicación entre computadoras y teléfonos móviles que cuenten con bluetooth.

Índice de Términos— Modulación FSK, Criptografía, Rs232, Seguridad en radios comerciales, Mensajería, Cifrada.

I. INTRODUCCIÓN

En el mercado es fácil encontrar soluciones de radio comunicación en la gama VHF. Algunas más costosas que otras, todo depende de lo que ofrezca el radio. En este sentido es más barato un radio que no tiene manos libre que otro que si lo tiene.

Lo anterior, también se refleja en la parte de seguridad, pues sí un radio tiene algún sistema que asegura la transmisión de voz es más caro. Y será mucho costoso si el sistema con el que asegura la comunicación es difícil de violar o si el sistema aplica a la voz y a datos.

Los sistemas empleados por instituciones del estado entre ellas el Ejército Nacional son de alta seguridad y por ende costosos. Y la pérdida de uno de ellos ocasiona una investigación de tipo administrativa, la cual genera alguna anotación en la hoja de vida del militar.

Los soldados ante la necesidad de mantener comunicación y con la finalidad de evitar investigaciones que dañen sus hojas de vida han optado en algunos casos por adquirir radios comerciales que no cuentan con ningún tipo de seguridad.

Este problema de la inseguridad en los radios comerciales de bajo costo también lo enfrentan empresas de seguridad privada y otras empresas que requieren seguridad tal como el sector minero entre otros.

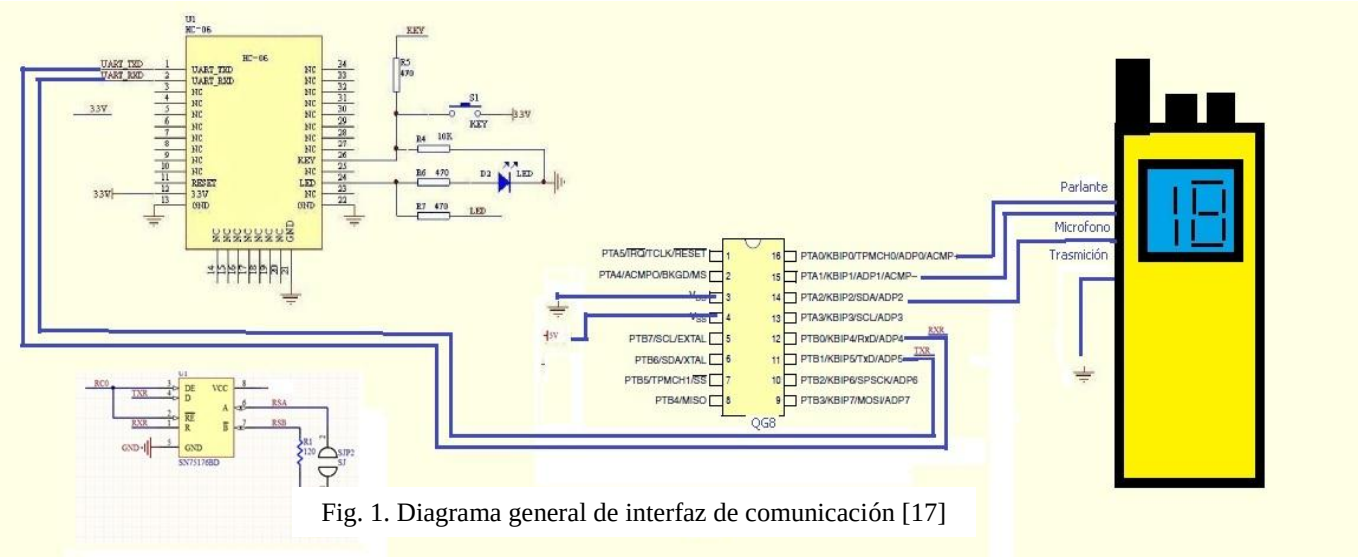

Fig. 1. Diagrama general de interfaz de comunicación [17]

En el presente ensayo se busca aplicar conceptos de criptografía en él envió de datos empleando radios comerciales de bajo costo que permitan asegurar este tipo de comunicaciones.

Se busca integra la plataforma Android y Sistemas Operativos con un una interfaz que envié al radio los datos ya cifrados y de esta forma garantizar la seguridad en caso de interceptación de la comunicación. Valga la pena decir que se quiere mantener el bajo costo y que será aplicable en cualquier ámbito fuera del militar o civil que busque seguridad en las comunicaciones.

II. DISEÑO DE LA INTERFAZ DE TRANSMISIÓN POR RADIO FRECUENCIA

Se buscó implementar el sistema de la figura 1, y para ello se necesitó del siguiente material:

- ✓ Radio Motorola Mh230r.
- ✓ Micro controlador Freescale QG8
- ✓ Conversor de rs232 a USB FT231X
- ✓ Conversos rs232 a Bluetooth HC06
- ✓ Diferenciador de señal SN75176A.

A. Fase de Transmisión

Al radio fueron conectados tres cables los cuales cumplen la labor de transmisión de datos, recepción de datos, y obturador. El cable de transmisión se conectó al micrófono, el de recepción al parlante y el de obturador al botón que permite transmitir.

De igual forma, en el radio fueron desconectados el parlante y el micrófono para lograr una transmisión sin interferencia del medio ambiente.

Si se va a transmitir desde un computador se conecta la interfaz USB y se debe tener el driver para el conversor FT231X. Si se va a emplear conexión por bluetooth solo es emparejar los dispositivos.

Ya sea por el terminal del computador o por el bluetooth el microcontrolado recibe una señal digital y este a su vez la convierte en análoga y la modula en FSK y la envía al radio para ser transmitida.

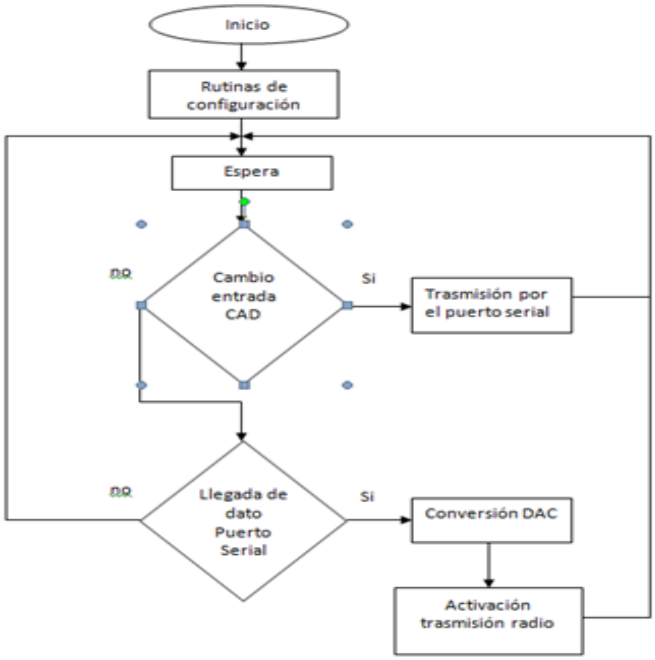

Fig. 2. Flujograma de comunicación [17]

En la Figura 2. Se ve un flujograma de los pasos a seguir para enviar y recibir datos. En primer lugar hay un inicio del programa que configura el circuito y que posteriormente queda a la espera para detectar cambios en el envío de datos o recepción de los mismos.

En el flujo grama se ve como al recibir datos digitales se hace la conversión a analógico y se activa la transmisión en el radio.

B. Fase de Recepción

El circuito maneja los cambios de estado por tiempo, es decir, cuando uno de los radios detecta un cambio en la entrada de datos para enviar este efectúa la rutina y envía. A su vez el radio receptor detecta la recepción de datos y lee datos durante un determinado tiempo y luego se coloca a la espera para enviar o recibir más datos.

La rutina de recepción de datos es la inversa de la rutina de transmisión. En ésta rutina el radio está leyendo constantemente el canal y cuando detecta una transmisión lee los datos análogos,

posteriormente los pasa al convertidor análogo / digital del microship freescale. Finalmente los datos se colocan en forma serial para que sean manejados ya sea por el convertidor USB o por el convertidor bluetooth.

En éste punto se analiza que el canal es transparente e inseguro, pues el canal transporta los datos pero no los cifra. De otro lado las emisiones radiales son omnidireccionales y cualquier receptor las puede escuchar.

III. CRIPTOGRAFÍA

La comunicación ha sido una de las principales herramientas de la evolución del hombre, desde el lenguaje de señas, el habla, la escritura y ahora las nuevas formas de interacción que ofrece la tecnología.

La humanidad ha atravesado muchas guerras por diferentes motivos tales como intereses religiosos, sociales, económicos, geopolíticos, entre otros esto ha hecho que el hombre evoluciones en diferentes aspectos uno de ellos las tecnologías de las comunicaciones.

En tiempos antiguos para enviar un mensaje al frente de guerra se empleaba estafetas o mensajeros para comunicar una instrucción o una orden y de esta forma orientar el accionar de las tropas.

Con el avance de los años nace la escritura y ahora se emplean los mensajes escritos, que de igual forma son transportados por un mensajero que goza de excelente confianza y que es leal a su comandante. Se anota que en las comunicaciones se emplearon señas con banderas, el agua para señales sonoras, humo para señales de alerta y auxilio, pero el cambio radical llega en la revolución francesa en 1789 cuando Claude Chape desarrolla el telégrafo óptico, el cual era una red de torres que enviaban mensajes mediante el uso de señales con luz solar, para la época mencionada existían 22 torres que unían la población Lille con Paris que se encontraban separadas a 240 kms, se podían enviar 196 caracteres y trasmitir un mensaje podía durar de 2 a 6 minutos. Es decir era un sistema de comunicación más eficiente que el mensajero a caballo.

El telégrafo electro químico en sus inicios no era muy eficiente y se vio complementado cuando se descubre que el fenómeno del magnetismo no es aislado de la circulación de electricidad y es por ello que para el año de 1819, Hans Crinstian Oersted encontró que un hilo con electricidad era capaz de mover una aguja y en 1820 se crea la bobina y se publica la ley de Ohm.

El telégrafo se fue perfeccionando en los años venideros y fue así como entre 1833 y 1837 los científicos Carl Friedrich Gauss y Wilhelm Weber inventan una serie de telégrafos electromagnéticos y efectúan diferentes conexiones empleando solo dos hilos.

En 1840 nace la primera patente Morse, y en 1844 Joseph Henry logro comunicaciones a 12 km empleando un circuito de carga eléctrica. La perfección de este tipo de comunicación se vio en 1844, cuando Samuel Findley Breese Morse presenta su versión final del código morse y se logran establecer comunicaciones entre Washintong y Baltimore.

Posteriormente, ya los países desarrollados emplean éste invento en mayor escala y así como en 1849 se instala un cableado entre Berlín y Frankfurt y 1850 otro cableado que une Inglaterra y Francia.

Las comunicaciones siguen su avance y para el año de 1861 Philip Reis demostró a varios profesores alemanes el primer teléfono que tenía la capacidad de reproducir sonido a una distancia de 90 metros.

Para el año de 1876 Edison patenta su teléfono que ya contaba con parlante y micrófono, a la par que Elisa Gray patenta el micrófono de esta forma se hace el salto a la comunicación oral.

En 1878, en New Haven Estados Unidos se instala la primera central telefónica que constaba de

un cuadro controlador manual y 21 abonados.

La comunicación mediante hilos creció constantemente pero en poco tiempo las comunicaciones inalámbricas nacieron y dieron sus primeros pasos así como en 1894, el científico italiano Marconi efectúa transmisiones a 2 millas de distancia y más adelante logró transmitir voz sobre el canal de la mancha entre Inglaterra y Francia.

La transmisión vía radio creció y dio lugar a centrales y organizaciones alrededor del tema, incluso Marconi en 1920 transmite a través de su emisora un concierto de música clásica es decir nace otro tipo de comunicación que es la radio.

Los años siguientes se crearon mejores antenas y nuevas centrales de radio y solo hasta 1925 se da un nuevo salto con los primeros experimento de la televisión. Que por supuesto vuelve y cambia la forma de interactuar y comunicar.

Posteriormente nacen las comunicaciones satelitales y Arpanet que fue el origen del Internet que se tiene hoy en día y que se emplea en la mayoría de los campos por no decir que en todos.

Desde tiempos prehistóricos se habla de la criptografía que no es otro que escribir un mensaje que solo sea entendido por el destinatario. Uno de los ejemplos clásicos y que mezcla la seguridad del estado en lo militar y las comunicaciones es el "cifrado Cesar" que consiste en desplazar cierto número de posiciones cada letra en el alfabeto distorsionando de esta forma el mensaje.

En lo referente a las comunicaciones militares se destaca los medios criptográficos empleados en la segunda guerra mundial; por ejemplo los alemanes hicieron gran uso de la máquina de rotores que se conoció posteriormente como Enigma, a esta máquina se le reconoce como el avance más grande en las comunicaciones cifradas por más de varias décadas.

De igual forma los japoneses en 1940 emplearon la máquina "Purpura" que en el fondo era similar a Enigma. Estados Unidos empleo la "máquina M" que finalmente recibió el nombre de "Red", los británicos emplearon las maquinas Tipex y Sigaba. Los polacos usaron la maquina Lacida y ya las tropas en el campo de batalla emplearon las máquinas M-209 y M-94.

En la actualidad la tecnología para cifrar mensaje ya no emplea nada mecánico sino complejos algoritmos informáticos que requieren para su descifre o ruptura un poder de cómputo aun no existente o muy costoso.

Sin embargo, el punto débil de las comunicaciones desde hace mucho tiempo y que afecta a todos los niveles es la cultura de seguridad, y es que no todos los militares están entrenados o son conscientes de cuando violan el secreto y afectan las operaciones militares y la integridad del personal que las desarrolla.

Colombia enfrenta una guerra de guerrillas y ésta emplea como una de sus fortalezas la inteligencia en todo espectro. Se conoce de casos de penetración electrónica que efectúan sobre las tropas para conocer las comunicaciones. Con los recursos que cuenta la subversión y con un mercado tan amplio que existe en Colombia y el exterior no le es difícil al bandolero conseguir radio escáneres para interceptar las comunicaciones.

Otra forma de violentar las comunicaciones es el robo de material, ejemplo de un radio que cuente con las tarjetas de cifrado y la configuración apropiada y así poder escuchar las comunicaciones. Aunque este aspecto ya es ampliamente superado pues ya no solo basta con robar el radio para poder escuchar las comunicaciones.

De todo lo anterior se puede decir que por el lado técnico en lo referente a radio de VHF Y HF la interceptación es un poco complicada y obliga al terrorismo a recurrir a la infiltración y penetración para obtener información sobre las operaciones militares.

Entonces una de las técnicas empleadas por la

inteligencia de la subversión es usar gente que tenga acceso y ubicación. Ejemplo que la persona que atiende la tienda del soldado sea reclutada y se dedique a escuchar las conversaciones de los militares.

Otra técnica es incorporar a un soldado para que éste luego se destaque y sea asignado a oficinas sensibles como la de operaciones o comunicaciones, donde puede escuchar todo lo relacionado al accionar de las tropas.

Sin embargo, las fallas de seguridad son más comunes de lo que se piensa, pues ahora todos los soldados cuentan con un celular convirtiéndose en uno de los principales focos de fuga de información. Lo anterior queda evidenciado cuando se va a iniciar una operación que cuenta con excelente inteligencia y los soldados llaman a las familias para informarles que van a realizar una operación, cuando se llega al objetivo ya no se encuentra nada.

La contra inteligencia ha adoptado muchas medidas para limitar el uso de celulares y por ende la fuga de información y es por esto que algunas tropas al momento de iniciar un planeamiento y alistamiento lo primero que se les prohíbe es el porte y uso de celulares.

Pensar que las infiltraciones solo es en los mandos bajos o en la parte militar es erróneo o iluso, y es por esto que todos los días se deben adoptar medidas más eficientes en la parte del secreto y la seguridad operacional.

En operaciones militares de infiltración al área es muy complicado evitar la detección, pues cualquier rastro delata la posición de la tropa. Ejemplo, el trillo que deja la tropa al andar o la basura que arrojan los soldados, para nuestro caso destacamos el uso del susurro que no es lo suficiente seguro a la hora de usar el radio para comunicarse con el puesto de mando pues lo puede escuchar un animal como un perro o la misma persona y con eso se perdió el esfuerzo para sorprender al enemigo.

Otro factor que afecta la cultura del secreto es el empleo de teléfonos celulares inteligentes, pues los comandantes suelen emplearlos debido a que lo portan a toda hora, puede hablar o chatear con la tropa sin problemas y a la hora que quieran, pueden hasta recibir y enviar archivos o fotos cosas que no son fáciles de realizar en un radio que carga la tropa.

Los celulares como el BlackBerry tienen gran acogida dentro de la tropa y es por ello que lo que hay que hacer es minimizar la falla de seguridad al emplear estos medios. Una de las soluciones es la de emplear software para evitar la interceptación sin embargo es costoso y de paso sigue siendo vulnerable al emplear otros software espías que son de bajo costo.

Y como ya se había mencionado anteriormente la tropa es dada a usar radios comerciales VHF con la finalidad de evitar las investigaciones administrativas en caso de pérdida. Los radios comerciales son fácilmente interceptados por los equipos que usa la subversión en Colombia.

A. Historia de la Criptografía

Las raíces etimológicas de la palabra Criptografía son criptos (oculto) y graphos (escritura). Una definición clásica de Criptografía es la siguiente: Arte de escribir mensajes en clave secreta o enigmáticamente.

Anteriormente la Criptografía era considerada como un arte pero en la actualidad se considera una ciencia gracias a su relación con la estadística, la teoría de la información, la teoría de los números y la teoría de la complejidad computacional.

La Criptografía es la ciencia que se encarga del estudio de técnicas para transformar la información a una forma que no pueda entenderse a simple vista; sin embargo, el objetivo de la Criptografía no es sólo mantener los datos secretos, sino también protegerlos contra modificación y comprobar la fuente de los mismos.

A continuación se muestran algunos sistemas de

Criptografía históricos:

1. ***La escitala:*** Siglo V A.C. El sistema consistía en una cinta que se enrollaba en un bastón y sobre el cual se escribía el mensaje en forma longitudinal como se muestra en la Figura 3.

Fig.3 La escitala, tomado de [16]

La clave de éste método es el diámetro del bastón. El mensaje viaja siempre en texto claro. Se lograba el objetivo de confidencialidad, la integridad dependía de la fidelidad del mensajero.

De estos tiempos tan remotos se debe la famosa frase de ostentar el BASTON DE MANDO, dado que en él estaba la seguridad del sistema de información.

2. ***El Cifrador de Polybios***: Siglo II A.C. cifrador por sustitución de caracteres más antiguo que se conoce, atribuido al historiador griego Polybios, basado en la siguiente matriz:

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

Fig. 4. Cifrado de Polybios, tomado de [16]

Acorde con este método la letra M se cifraba como CB, la letra U como DE, etc.

3. ***El Cifrador del César:*** Siglo I A.C. En honor al emperador Julio César. En este método ya se incluye una transformación del texto en claro de tipo monoalfabética.

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

Fig. 5. Cifrado del Cesar, tomado de [16]

Aplica un desplazamiento constante de tres caracteres al texto en claro, veamos un ejemplo:
M = AL CÉSAR LO QUE ES DEL CÉSAR.
C = DÑ FHVDU ÑR TXH HV GHÑ FHVDU.

4. ***El Cifrador de Kamasutra***: Cifrador por sustitución de caracteres que usa una matriz como la que se muestra en la figura 6.

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

Fig. 6. Cifrado de Kamasutra, tomado de [16]

5. ***El cifrador de Masón***: En la figura se muestra el cifrador por sustitución de caracteres:

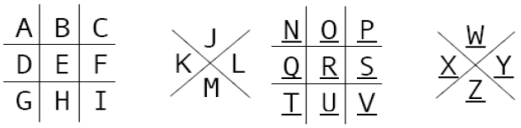

Fig. 7. Cifrado de Masón, tomado de [16]

6. ***Cifrador transposición Multicolumnar***

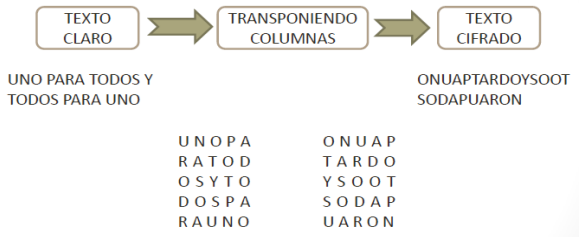

Fig. 8. Cifrado transposición Multicolumnar, tomado de [16]

7. ***Cifrador Playfair***: El científico Charles Wheatstone fue quien concibió este método de crifrado.

Playfair es un método de cifrado de bloque primitivo, usando algunos principios comunes a las cifras de bloque actuales. El mejor medio de aproximarse a la criptología moderna, sin tener que enfrentar la teoría de los números y la matemática, es entendiendo la Playfair.

El cifrado de Playfair es un ejemplo de sustitución digrámica, donde un par de letras de un texto en claro (mensaje sin codificar) se convierten en otro par distinto.

Reglas a tener en cuenta:

- ✓ Si m1 y m2 de la misma fila, coger c1 y c2 de su derecha (circularmente).
- ✓ Si m1 y m2 de la misma columna, coger c1 y c2 de abajo (circularmente).
- ✓ Si m1 y m2 de distintas filas y columnas, coger c1 y c2 de diagonal opuesta.
- ✓ Si m1 = m2, insertar carácter sin significado entre m1 y m2 para evitar su repetición, después aplicar reglas 1-3.

Si el número de letras es impar, añadir una sin significado al final del texto.

Fig. 09. Cifrado Playfair, tomado de [16]

8. ***El cifrador de Alberti:*** Siglo XVI León Battista Alberti. Presenta en su círculo exterior los 20 caracteres del latín, esto es, los mismos del alfabeto castellano excepto las letras H, J, Ñ, K, U, W e Y, y se incluyen los números 1, 2, 3 y 4 para códigos especiales. Por su parte, en el disco interior aparecen todos los caracteres del latín además del signo & y las letras H, K e Y, para un total de 24 caracteres en cada disco.

Fig. 10. Disco de Alberti, tomado de [16]

La innovación que supone este sistema consiste en que el alfabeto de sustitución puede ser cambiado durante el proceso de cifrado, por ejemplo cada k caracteres, simplemente girando el disco interior y por tanto utilizando otro alfabeto de sustitución.

B. Modos de Cifrado

1) Cifrado por Bloques

En Criptografía, una unidad de cifrado por bloques (block cipher) es una unidad de cifrado de clave simétrica que opera en grupos de bits de longitud fija, llamados bloques.

Los algoritmos de cifrado por bloques toman bloques de tamaño fijo del texto en claro y producen un bloque de tamaño fijo de texto cifrado, generalmente del mismo tamaño que la entrada.

Funcionamiento. El texto a cifrar se divide en dos mitades, la función de rotación se aplica a una mitad usando una subclave y la salida de la función se emplea para hacer una OR-exclusiva con la otra mitad, entonces se intercambian las mitades y se repite la misma operación hasta la última rotación, en la que no hay intercambio.

Características: Una característica interesante de estos algoritmos es que el cifre y descifre son idénticas estructuralmente, aunque las subclaves empleadas en la encriptación se toman en orden inverso en el descifre. Se caracteriza por usar la misma clave para cifrar y descifrar.

El cifrado por bloques se apoyan en dos conceptos:

- ✓ Confusión: tratar de ocultar la relación que existe entre el texto normal, el texto cifrado y la clave, es decir, realizar sustituciones simples.

- ✓ Difusión: trata de repartir la influencia de cada bit del mensaje original lo más posible en el mensaje cifrado, es decir, realizar permutaciones.

Algunos métodos de cifrado por bloque son:

Electronic codebook (ECB). El método más simple de modo de cifrado es el llamado ECB (electronic codebook), en el cual el mensaje es

dividido en bloques, cada uno de los cuales es cifrado de manera separada. La desventaja de este método es que bloques idénticos de mensaje sin cifrar producirán idénticos textos cifrados. Por esto, no proporciona una auténtica confidencialidad y no es recomendado para protocolos criptográficos.

Cipher-block chaining (CBC). En el modo CBC (cipher-block chaining), antes de ser cifrado, a cada bloque de texto se le aplica una operación XOR con el bloque previo ya cifrado. De este modo, cada bloque es dependiente de todos los bloques de texto planos hasta ese punto. Además, para hacer cada mensaje único se puede usar un vector de inicialización.

Propagating cipher-block chaining (PCBC). El modo propagating cipher-block chaining fue diseñado para que pequeños cambios en el texto cifrado se propagaran más que en el modo CBC. PCBC es usado por Kerberos y Waste, aunque además de en éstos, su uso es bastante infrecuente.

Cipher feedback (CFB) y output feedback (OFB). Los modos cipher feedback (CFB) y output feedback (OFB) hacen que el cifrado en bloque opere como una unidad de flujo de cifrado: se generan bloques de flujo de claves, que son operados con XOR y el texto en claro para obtener el texto cifrado.

Counter (CTR). El modo contador convierte una unidad de cifrado por bloques en una unidad de flujo de cifrado. Genera el siguiente bloque en el flujo de claves cifrando valores sucesivos de un contador. El contador puede ser cualquier función sencilla que produzca una secuencia de números donde los resultados se repiten con muy baja frecuencia.

2) Algoritmos de Crifrado.

Algoritmo DES. El DES (Data Encription Standard o Estándar de Encriptación de Datos) fue un diseño de unidad de cifrado por bloques de gran influencia. Fue desarrollado y publicado por IBM y publicado como estándar en 1977.

Características:

- ✓ Longitud de bloque: 64 bits.
- ✓ Longitud de clave: 56 bits.
- ✓ Cifrado tipo Feistel.
- ✓ Usa sustituciones y permutaciones.
- ✓ Hay implementaciones hardware y software.
- ✓ Compresión y expansión para manipular los bloques de diferentes longitudes.

Ventajas del algoritmo: Es muy rápido y fácil de implementar.

Desventajas: Emplea una clave demasiado corta, lo cual hace que con el avance actual de los ordenadores, los ataques por la fuerza bruta se puedan llevar a cabo.

Algoritmo Rijndael (AES)

Advanced Encryption Standard (AES), también conocido como Rijndael (pronunciado "Rain Doll" en inglés), es un esquema de cifrado por bloques adoptado como un estándar de cifrado por el gobierno de los Estados Unidos. Estándar (AES) en EEUU desde 2000.

Este algoritmo se adoptó oficialmente en octubre del 2000 como nuevo Estándar Avanzado de Cifrado (AES) por el NIST (National Institute for Standards and Technology) para su empleo en aplicaciones criptográficas. Su nombre se debe a dos autores belgas Joan Daemen y Vincent Rijmen.

Características:

- ✓ Longitud variable de bloque y de clave: 128, 192, 256 bits.
- ✓ Número de iteraciones flexible: 10, 12, 14.
- ✓ No es de tipo Feistel.
- ✓ Implementación eficiente y con pocos requerimientos.
- ✓ Fácilmente paralelizable.
- ✓ Posible implementación en tarjeta inteligente.

IV. ASEGURAMIENTO DE DATOS

En este nivel del avance de la criptografía ya no se implementan, generalmente, sistemas como el crifrado Cesar sino que se aprovecha la tecnología de los computadores y se trabaja sobra los bytes que representa el mensaje o el archivo donde está contenido el mensaje a proteger.

Para el desarrollo de este documento se decidió implementa en código java dos algoritmos de los más conocidos hoy en el medio informático.

1) Algoritmo DES en java

Funcionamiento en Java – procedimiento:

- ✓ Generación de claves DES de forma aleatoria. (Usamos KeyGenerator).
- ✓ Cifrado del mensaje con DES, ingresado por la aplicación de usuario, se usará DES/ECB/PKCS5Padding.
- ✓ En una fase posterior se hace el Descifre con DES del mensaje, que se ingresó anteriormente.

Código Java:

```
cifrador.init(Cipher.ENCRYPT_MODE, clave);
byte[] buffer = new byte[1000];
byte[] bufferCifrado;
FileInputStream in = new FileInputStream(args[0]);
FileOutputStream out = new
FileOutputStream(args[0]+".cifrado");
int bytesLeidos = in.read(buffer, 0, 1000);
while (bytesLeidos != -1)
   {
bufferCifrado = cifrador.update(buffer, 0, bytesLeidos);
out.write(bufferCifrado);
bytesLeidos = in.read(buffer, 0, 1000);
   }
bufferCifrado = cifrador.doFinal();
out.write(bufferCifrado);
in.close();
out.close();
Y finalmente el código de la función inversa que descifra
nuestro mensaje:
cifrador.init(Cipher.DECRYPT_MODE, clave);
in = new FileInputStream(args[0]+".cifrado");
out = new FileOutputStream(args[0]+".descifrado");
2)  byte[] bufferPlano;
bytesLeidos = in.read(buffer, 0, 1000);
while (bytesLeidos != -1)
   {
bufferPlano = cifrador.update(buffer, 0, bytesLeidos);
out.write(bufferPlano);
bytesLeidos = in.read(buffer, 0, 1000);
   }
bufferPlano = cifrador.doFinal();
out.write(bufferPlano);
in.close();
out.close();
```

Lo primero que se analiza en el anterior código fuente en Java es que ya existen unas librerías que permiten trabajar de forma ágil con el cifrado DES.

El número de líneas de código es bastante reducido.

3) Algoritmo AES en java

```
import javax.crypto.Cipher;
import javax.crypto.spec.SecretKeySpec;
public class aes {
 public static void main(String[] args) {
  // llaveSimetrica es un String
  String llaveSimetrica = "univ_piloto_2014";
  SecretKeySpec key = new
SecretKeySpec(llaveSimetrica.getBytes(), "AES");
  Cipher cipher;
  try {
   cipher = Cipher.getInstance("AES");
   //Comienzo de cifrado
   cipher.init(Cipher.ENCRYPT_MODE, key);
   byte[] campoCifrado =
cipher.doFinal("mensaje_secreto".getBytes());
 System.out.println(new String(campoCifrado));

   //Comienzo de descifre
   cipher.init(Cipher.DECRYPT_MODE, key);
   byte[] datosDecifrados = cipher.doFinal(campoCifrado);
   String mensaje_original = new String(datosDecifrados);
   System.out.println(mensaje_original);
  } catch (Exception e) {
   e.printStackTrace();
  }
 }
}
```

Al igual que en el cifrado DES existen unas librería que facilitan el trabajo de cifrado y descifre. En esta ocasión se dio una clave simétrica arbitraria en lugar de aleatoria.

4) Código Andriod Interfaz Bluetooth en Java

Teniendo ya cualquiera de las rutinas creadas anteriormente se generó un código que empela cualquiera de las clases (DES – AES) para descifrar y enviar los datos cifrados.

El código de la aplicación es más extenso debido a que tiene que presentar una interface al usuario para poder escribir y enviar el mensaje.

Método de envió de datos:

```
 private void sendMessage(String message) {
//se verifica si hay conexión
if (mChatService.getState() != BluetoothChatService.STATE_CONNECTED) {
Toast.makeText(this, R.string.not_connected, Toast.LENGTH_SHORT).show(); return; }
// se mira si hay mensaje a enviar
 if (message.length() > 0) {
//se cifra el mensaje
message=cifraaes(mensaje);
 byte[] send = message.getBytes();
mChatService.write(send);
 mOutStringBuffer.setLength(0);
mOutEditText.setText(mOutStringBuffer);
        }
    }
```

V. CONCLUSIONES

Implementar seguridad mediante cifrado en radios comerciales VHF es relativamente fácil debido a que lenguajes de programación como Java cuentan con librerías que agilizan el desarrollo y la implementación.

En el desarrollo del presente ensayo el principal problema fuè que el microchip freescale QG8 solo logró manejar tramas de 32 bytes y a una velocidad de 9600 baudios, lo cual es muy bajo para transmitir archivos o imágenes que se hayan cifrado.

La seguridad mediante cifrado de datos en el canal de radio comercial serial útil para chat o para enviar y recibir tramas de datos corta, ejemplo: coordenadas de un GPS, datos de telemetría, etc.

El bajo costo de la implantación del presente sistema contrasta con su deficiencia en el ancho de canal, que es muy bajo y de quererse un canal más amplio el costo sería mayor de forma drástica.

REFERENCIAS

[1] Miller, Nathan. Tecnología Bluetotoh. Madrid. Mc Graw Hill, 2002.
[2] Guía completa de protocolos de comunicaciones. Madrid. Mc Graw Hill, 2002.
[3] Ceballos, Fco. Javier. Java 2, curso de programación. Mc Graw Hill, 2011.
[4] Petersen, Richard. Fundamentos de programación en linux. Bogotá. Mc Graw Hill, 2001.
[5] Shah, Steve. Manual de administración Linux. Madrid. Mc Graw Hill, 2001.
[6] Davis, Hart. IPod, iPhone y iTunes. México. Mc Graw Hill, 2011.
[7] Rinehart, Martin. Desarrollo de bases de datos en java. Madrid. Mc Graw Hill 1998.
[8] Vesga Ferreira, Juan Carlos. Microcontroladores Motorola – freescale. Colombia. Alfa Omega, 2007.
[9] Sierra Perez, Manuel. Electrónica de comunicaciones. Madrid. Pearson Pritince Hall, 2003.
[10] Robbins, Allan. Análisis de circuitos teoría y práctica. México. Cengage, 2008.
[11] Walker, Melissa. Como escribir trabajos de investigación. Barcelona. Gedisa. 2000.
[12] Sabino, Carlos. El proceso de investigación. Bogotá. Panamericana, 2008.
[13] Gironés, Jesús Tomás. El gran libro de android. México. Alfaomega, 2012.
[14] Reglamento de operaciones y maniobras de combate irregular. Colombia. Publicaciones Ejército, 2010.
[15] ICONTEC, Norma Técnica Colombiana NTC 1486 (Sexta Actualización), Documentación. Presentación de Tesis, Trabajos de Grado y otros Trabajos de Investigación, 2008-07-23.
[16] Material de apoyo materia criptográfica. Cohorte 18 Especialización Seguridad de la información. Universidad Piloto de Colombia.
[17] Javier Eduardo Ramírez, Alumno Cohorte 18, Especialización Seguridad Informática, Universidad Piloto.
[18] ISO/IEC, "International Standard ISO/IEC 27005", 2008.

Javier Eduardo Ramírez, Ingeniero de Sistemas Fundación San Martin, estudiante de la "Especialización en Seguridad de la Información" Universidad Piloto de Colombia 2014.