Diseño e Implementación de un Sistema de Encriptación de Voz para la Red Telefónica

Fabian Valero Duque fabian.valero@binaryti.com Hacking Research

***Resumen*—Se ha desarrollado un sistema de encripación de voz en tiempo real que trabaja sobre la telefonía fija; combinando dos tipos de crifrado. El primer tipo, un protocolo de clave pública llamado *RABIN* (Algoritmo de cifrado asimétrico basado en el problema del cálculo de raíces cuadradas módulo un número compuesto) para intercambiar las claves privadas, y el segundo se basa sobre un protocolo de llave privada llamado *TEA (Tiny encryption algorithm, peueño sistema de cifrado e.)* realizando además un procedimiento de enmascaramiento de las claves cifradas del algoritmo privado. XTEA_E (*TEAX_E)* es un aporte entregado en el proyecto de grado basado en el algoritmo XTEA(*TEAX)*. (Pequeño algoritmo de cifrado).**

El prototipo se desarrolló sobre tecnología de microprocesadores, compresores de voz, módems, conversores analógicos a digital y viceversa.

El sistema permite una conversación telefónica en donde la voz cifrada se transmite en forma digital por medio de módem entre los usuarios, sin comprometer la legibilidad del mensaje.

***Glosario*—Bitio, bit, cifrado, encriptación, enmascaramiento, esteganografía, micro, microcontrolador, conversor analógico digital,texto plano, texto cifrado, clave, claves conexas TEA, TEA_E, XTEA, XTEA_E (TEAX_E).**

I. Introducción

En la actualidad, el desarrollo de las comunicaciones y el uso creciente de los sistemas de información, le han dado la posibilidad al hombre de transmitir sus mensajes a cualquier lugar y en cualquier momento, superando las barreras materiales de su entorno.

La sociedad actual es demasiado compleja y multifacética, para poder interactuar exclusivamente por medio de una comunicación directa entre sus integrantes.

A día de hoy, se ofrecen servicios y aplicaciones en los cuales, el usuario final no necesita estar de forma presencial con otras personas, organizaciones, etc., para poder enviar o recibir sus mensajes. Esto se logra a través de diversos sistemas de conexión llamados *redes*[1], cuya función es posibilitar la transmisión de datos.

Uno de los aspectos fundamentales que aparecen como requisito en la mayoría de los procesos de transferencia de información tiene que ver con la seguridad y la privacidad de los datos y mensajes involucrados. La existencia de la red implica que la información que circula por ella pueda ser interceptada, alterada y/o borrada, dando lugar a la pérdida de prioridad y seguridad de la misma. Esto obliga a contar con mecanismos de protección suficientemente capaces de proveer transmisiones seguras. Mecanismos fundamentados en la ciencia *Criptográfica*[2].

Una de las redes más usadas en la actualidad es la telefónica. La información que transita por ésta, se convierte en un blanco fácil de cualquier forma de escucha[1]-[3][11].

Un sistema de cifrado como el propuesto en este trabajo resuelve los principales problemas de seguridad de la red telefónica como son: la privacidad, la integridad, la autenticación y la no negación del mensaje[4][3], convirtiéndose en un *Criptosistema*[3] [3].

II. DESARROLLO

A. Diseño

Las prioridadedes o los objetivos trazados para el diseño del dispositivo fueron dos: 1)Tener la capacidad de codificar y decodificar manteniendo la conversación sin tener algún tipo de retardo que afectara tal. 2)Cumplir los objetivos de seguridad propuestos en [4][6].

Teniendo en cuenta que los recursos técnicos se limitaban a la potencia de trabajo de un pequeño microprocesador y algunos periféricos, se decidió buscar un algoritmo lo suficientemente rápido y seguro que pudiera ser usado en un microprocesador, el resultado fue ***TEA***[9] *(Pequeño al*goritmo de cifrado).

***T.E.A** e*s un algoritmo de cifrado en bloque y simétrico[4].

Las dos partes que se comunican han de ponerse de acuerdo de antemano sobre la clave pública a usar. Una vez ambas tienen acceso a esta clave, el remitente cifra un mensaje usándola, lo envía al destinatario, y éste lo descifra con la misma.

T.E.A. posee una clave de 128 bitios de longitud, lo que dá una capacidad aproximada de 10^40 dígitos. Este algoritmo fué diseñado por *David Wheeler* y *Roger Needham* del *Computer Laboratory* de la universidad de *Cambridge* en Inglaterra hacia finales del año de 1.994 [5].

Una de la peculiaridades es la posibilidad que brinda para ser implementado en casi todas los tipos de procesadores de una manera rápida y segura.[5].La fortaleza que posee el algoritmo es comparable con otro tipo de cifrados en bloque aún más que el DES[5].[5]. Una de las ventajas es la de tener

[1] Una red es un conjunto de elementos que permite conectar dos a más usuarios o puntos previamente establecidos, para realizar una comunicación entre ellos, presentando diversos servicios.

[2] Conjunto de códigos y algoritmos con los cuales se cifra la información para enviarse por canales inseguros, dificultando la decodificación por terceros.

[3] Al proceso de cifrar, codificar, enviar, recibir y descifrar o decodificar el mensaje se le llama *Criptosistema.*

[4]Tipo de cifrado en el cual la clave que se usa para encriptar es la misma que se usa para desemcriptar.

[5] Data Encryption Estándar. Propuesto por los Bell Laboratories para la NSA.

iteraciones y operaciones no lineales, las cuales le dan gran seguridad.[6].
El tipo de algoritmo usado es de ***Feistel,*** el cual usa operaciones de suma, resta y operadores lógicos, que en el caso de TEAX son XOR(Función O Exclusiva); además de realizar las mismas operaciones una determinada cantidad de veces.
El método ***Feistel*** se describe a continuación: Se selecciona una cadena, N (información a cifrar o texto plano), normalmente de 64 o 128 bitios, y se divide en partes de 32 bitios c/u llamadas D e I al igual que la clave. R es la cadena resultante de las operaciones matemáticas (se convertirá en la infornación cifrada o texto cifrado).

1. Se selecciona una función, F, y una clave Ki.
2. Se realizan una serie de operaciones complejas con F y Ki, y con D e I, con sólo uno de ellos a la vez.
3. La cadena resultante se cambia por la cadena con la que no se han realizado operaciones, y se siguen haciendo las rondas.

El uso alternado de operaciones XOR y de suma en el momento del cifrado lo hacen tener un comportamiento no lineal. El corrimiento de la información hacia derecha e izquierda antes de las operaciones de suma hacen que la clave y el texto plano cifrar no se mezclen y cumpla con unas de las proposiciones de *Shannon* [6][8] para el cifrado(Difusión y Confusión).

El modelo de cifrado en **TEA**[9]se describe a continuación:

1. Se nombra una variable llamda DELTA y una variable llamada SUMA.
   DELTA=0x9e3779b9;
   SUMA=0;
2. Una vez escogida la clave K de 128 bitios, es dividida en cuatro cadenas de 32 bitios c/u.
   K dividida en :K[0], *K*[1], *K*[2], *K*[3] (k_1, k_2, k_3, k_4).
3. La información a cifrar o *texto plano* de longitud de 64 bitios también es divida en dos partes de 32 bitios c/u
   Texto_plano dividido rn: V[0],V[1],
4. Realizar las siguientes operaciones treinta y dos (32) veces.
   SUMA=SUMA+DELTA;
   `V[0]+=(V[1]1<<4)+K[0] XOR V[1]+SUMA`
   `XOR (V[1]>>5)+K[1];`
   `V[1]+=(V[0]<<4)+K[2]XOR V[1]+SUMA`
   `XOR (V[0]>>5)+ K[3];`
5. EL resultado del cifrado queda en V[0] y V[1] que formaría el texto cifrado.
   TEXTO_CIFRADO=V[0]V[1];.

Las operaciones de cifrado son complementarias o inversas a las descritas en el párrafo anterior y se pueden ver en [9].

El número mínimo de rondas que se necesita para cubrir la información es de diez y seis (16), pero los autores recomiendan que se haga un número de treinta y dos.
La longitud de clave del cifrado propuesta en ***TEA*** es de 128 bitios, pudiendo ser menor o mayor, pero en múltiplos de 8 bitios. Si se usa una clave menor de 128 bitios se está en riesgo mostar algún tipo de debilidad con respecto a algoritmos de búsqueda y ataques de fuerza bruta.

Habrá que tener en cuenta que la clave que se usa para cifrar es la misma para descifrar (algoritmo simétrico), y además si se usa el mismo número de rondas para cifrar, entonces también para descifrar.

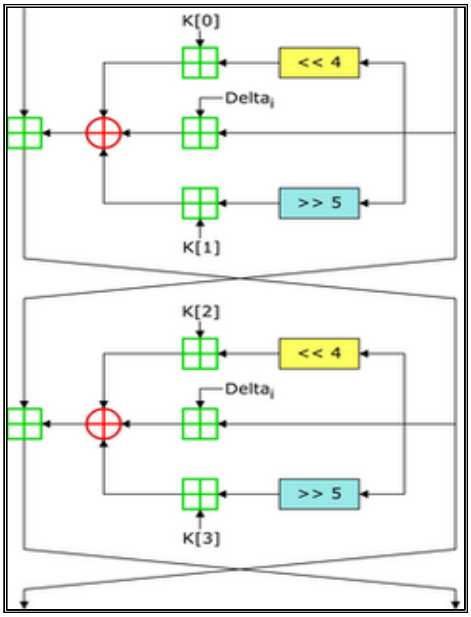

Fig. 1. Modelo de cifrado TEA.[6]
En un ciclo de cifrado se realiza doble bloque Feistel.

La capacidad de cifrado por ronda de ***TEA*** es de 64 bitios u ocho (8) octetos de ocho bitios, de los cuales los más débiles y propensos para ser atacados son los primeros cinco (5) bitios y los últimos cinco (5) bitios. Para evitar tal inconveniente el texto plano a cifrar se divide en dos cantidades iguales de treinta y dos (32) bitios llamados *Y*[0] e *Y*[1] ó Z[0] (y_0 y z_0), trabajándolos como unidades independientes pero referenciadas entre sí, aumentando la difusión del texto plano y disminuyendo la cantidad y redundancia del mismo.

Otra parte activa del algoritmo es ***DELTA***, que actúa como constante de enmascaramiento y cuyo valor típico es 2.654'435.769 (1,618033989...), en decimal ó 9E3779B9[7] en hexadecimal. Este número puede ser cambiado por π o por alguna otra constante matemática que represente una relación.

En [5] y [9] muestran lo rápido que es el algoritmo y que posee un mejor comportamiento que el ***DES*** *(Data encryption standar)* y hasta el triple ***DES***.

Hacia el año de 1.999 el señor *David Wagner*[9] encontró dos debilidades menores en ***TEA***, las cuales se nombran a continuación:

[6] Imagen obtenida de www.wikipedia.org
[7] También denominado *sección áurea*, *razón áurea o dorada*, *media áurea*, *divina proporción* o *número de oro*, representado por la etra griega Φ (fi), es un número irracional .

La primera está su parte entrelazada, ***TEA*** podrá parecer irrompible, pero ataques o criptoanálisis de claves conexas[8] de partes de texto divididos en una longitud de treinta dos bitios podría resultar exitoso. Aunque éste ataque al parecer puede resultar impráctico.

Parte entrelazada de tea (4):

5. V[0]+=(V[1]1<<4)+K[0] ***XOR*** V[1]+SUMA
   XOR (V[1]>>5)+K[1];
   V[1]+=(V[0]<<4)+K[2]***XOR*** V[1]+SUMA
   XOR (V[0]>>5)+ K[3];

La segunda debilidad mostrada de ***TEA,*** tiene que ver con la verdadera longitud de la clave usada, que es de 126 bitios y no de 128. Esto se dá desde el momento de la división de la clave en cuatro partes iguales, unido al momento en el cual se hacen los corrimientos de los bitios del texto claro a cifrar.

Para corregir esas debilidades en 1.997 *Roger M. Needham y David J. Wheeler*[10] propusieron una mejora al algoritmo ***TEA***, tratando de mantener los objetivos que son, ser fuerte criptográficamente hablando en poco tiempo de cifrado.

La primera mejora consistió volver dinámico el uso del segmento de la clave asignado cada espacio de cifrado.
En ***TEA,*** cada cadena de 32 bitios correspondiente a la clave *K*[0], *K*[1], *K*[2], *K*[3] (k_1, k_2, k_3, k_4) trabaja de forma estática en el algoritmo (4). En ***TEAX*** la fracción de la clave a usar depende del valor que posea ***SUMA*** en un momento dado, quitando la *linealidad* en intervención de cada componente de la clave en el cifrado.

6. Operaciones de entrelazado un determinado número de veces.
   V[0]+=((V[1]<< 4 XOR V[1] >> 5)+V[1]) ***XOR***
   (SUMA + K[SUMA Y 3]);
7. La variable SUMA es actualizada después de la primera transformación.
   SUMA+=DELTA;
8. La segunda operación de entrelazado
   V[1]+=((V[0]<<4 ***XOR*** V[0]>>5)+ V[0])
   XOR (SUMA+K[SUMA>>11 & 3]);

La segunda mejora consistió en involucrar un valor diferente de la variable ***SUMA*** para cada segmento de la rutina de cifrado. Para el segundo segmento de cifrado (7), la variable ***SUMA*** ya ha cambiado ***DELTA*** veces con respecto al primer segmento de cifrado (6). El resto del algoritmo sigue permaneciendo igual.
El algoritmo de cifrado y descifrado se convierte en una adaptación propia del original propuesto por *Roger M. Needham y David J. Wheeler*[9].
De nuevo habrá que tener en cuenta que la clave que se usa para cifrar es la misma para descifrar, y que si se usa el mismo número de rondas para cifrar, entonces también para descifrar.
Las mejoras propuestas presentan los siguientes efectos:
Un cambio de un bitio en el texto claro o en la clave de cifrado hace que el bloque encriptado resultante cambie. Y sólo la repetición del texto claro entrega el mismo texto cifrado sin involucrar las fortalezas del mismo.

[8] Es sacar parte del texto cifrado y a partir de ahí construir la clave de acuerdo a un algoritmo dado.

La seguridad de este algoritmo fué comprobada por *Dukjae Moon*[11]. Cuando le realizaron un criptoanálisis diferencial a TEAX, encontraron imposible de llevar a término positivo el criptoanálisis y demostrando la seguridad que posee éste.

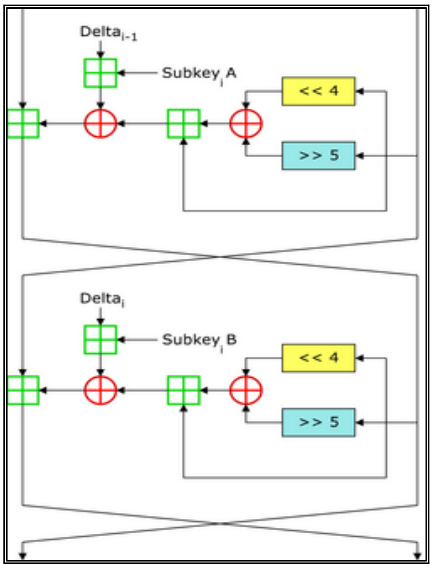

Fig. 2. Modelo de cifrado XTEA o TEAX.[9]
Segmento de clave dinámico al rotar y mezclar cada parte de la clave entre sí, En un ciclo de cifrado se realiza doble bloque Feistel.

Aunque hasta el momento no hay publicado en forma oficial un criptoanálisis efectivo se puede encontrar de forma conceptual [6].
La debilidad planteada consiste.dada una sóla clave de cifrado para un determinado texto claro (*texto plano o información sin cifrar)* mucho mayor a 64 bitios;la variación del texto claro puede ser mostrada por el mismo texto cifrado. Más aún teniendo un valor público en el algoritmo que es la variable ***DELTA***, entonces cabe la posibilidad de entregar información a medida que se transmite el texto codificado [4][6][9][10], y extraerla del texto cifrado utilizando ***DELTA.***

La debilidad posible no comprobada de TEA y TEAX radica en el uso del mismo DELTA o el mismo uso de la clave para varios bloques de la información sin cifrar, y más aún cuando las conversaciones telefónicas presentan flujos de varios megas, generando lo que se denomina «marcas de agua»
Para cada momento o ronda de cifrado del mensaje con TEA o con TEAX tendrá en toda su extensión dos mismos valores, la clave y ***DELTA***.[10]

[9] www.wikipedia.org
[10] Impossible Differential Cryptanalysis of Reduced Round XTEA and TEA, Centro para las tecnologías de la información y seguridad (CIST siglas en inglés) Universidad de Korea, Seúl, Korea del Sur.

III MEJORAS PROPUESTAS AL AGORITMO TEA Y XTEA.

TEA_E y XTEA_E (TEAX_E). Es el aporte del proyecto al algoritmo TEA y TEAX cuya descripción se presenta a continuación. 1.

En TEA y TEAX la función de la variable ***DELTA*** es de suma importancia para el algoritmo, pues se involucra de manera directa en el cifrado.Siempre para cada nuevo texto que se va a cifrar, la variable ***DELTA*** participa activamente y de forma directa en el algoritmo siendo partícipe en el resultado, dando la posibilidad de entregar información valiosa. [6].

La duda de seguridad queda planteada y es aquí donde se presenta las siguientes propuestas.

- Primera propuesta: Tener un valor de ***DELTA*** dinámico en el tiempo de cifrado sin involucrar de los objetivos del TEA que es la de mínimo tiempo de cifrado y ser seguro.A su vez, variando sutilmente en 1 la cantidad de rondas usadas por el algoritmo, quedando en 33 rondas para textos impares.

- Segunda propuesta: hacer un cambio dinámico de la clave de cifrado en el cual participe el texto claro o la información sin cifrar [3][4][6][12].

Para el proyecto se estudiaron los dos tipos de soluciones, involucranado ambas. Sin embargo se prefirió usar la segunda propuesta, pues valor de «enmascaramiento» ***DELTA*** ha de mantener condiciones de seguridad.[5] y cumple un *servicio místico*. En este documento se presentan una solución para cada debilidad.

IV VARIACIÓN DEL VALOR DE ENMASCARAMIENTO COMO PRIMERA MEJORA TEA Y XTEA (TEAX).

Tener un valor de ***DELTA*** dinámico en el tiempo de cifrado sin involucrar de los objetivos de mínimo tiempo de cifrado y ser seguro en TEAX.

1. Se usa el ***DELTA*** de ***TEAX*** como base del nuevo ***DELTA*** de la próxima ronda de iteración.
   DELTA_S; Es el delta siguiente, que empieza con el valor: *DELTA_S=0x9e3779b9;*
   DELTA=DELTA_S;
2. Se extraen 32 bitios del texto plano. Estos han de ser los menos significativos porqué poseen gran variación.
   U_TEXTO=*32 primeros bits ó los 32 menos significativos.*
3. Se efectúa una operación de XOR con el valor del ***DELTA*** actual y con el segmento de texto plano extraído, además de actuará como semilla a un generador pseudoaleatorio de tipo *gaussiano.*
   *VAR= (DELTA **XOR** U_TEXTO).*
   Establecer el nuevo ***DELTA*** y dejarlo para la siguiente ronda de cifrado, siguiendo las consideraciones presentadas en [6][7].

La condición para hacer el cambio del delta se describe a continuación:

4. EL número equivalente en decimal del *texto plano* deberá ser impar, si es impar entonces se cambia el DELTA para la próxima iteración del cifrado del texto, si es par entonces el valor del DELTA no cambia, evitando así el determinismo en el cambio del DELTA, aumentando la aleatoriedad de la variación.
   SI(*U_TEXTO es IMPAR*)
   DELTA_S=VAR;
   SI(U_TEXTO es PAR)
   DELTA_S =DELTA_S;

Son cambios dinámicos que aumentan la seguridad del algoritmo cuando se usa para cifrar textos muy superiores a una longitud de 64 bits, elevando un máximo del cuatro por ciento el tiempo de cifrado o descifrado.

El algoritmo transformado XTEA (TEAX) se llamará XTEA_E (TEAX_E) y TEA_E quedando:

Guía: ⊕ Equivale a la función *XOR*
N_S=32;
{
DELTA = **DELTA_S**
N = N_S;
U_TEXTO=32 primeros bits ó los 32 menos significativos.
mientras que N sea mayor de cero haga:
{
Y_0 += (Z_0<<4)+ ($K_1 \oplus Z_0$)+ (SUMA⊕(Z_0>>5))+ K_2 ;
SUMA = SUMA + DELTA;
Z_0 += (Y_0<<4)+ ($K_3 \oplus Y_0$) + (SUMA⊕(Y_0>>5))+ K_4 ;
N = N-1;
} --- fin del ciclo hasta que n se haga cero
Si (TEXTO es impar)
{
DELTA_S=DELTA⊕(U_*TEXTO*).
}
Si (TEXTO es par)
{
DELTA_S=DELTA;
}
}---Hasta que termine de cifrar todo el texto plano.

Fig. 3. Modelo de cifrado XTEA_E (TEAX_E)
Nótese la variación dinámica de **DELTA** al mezclar cada parte ésta con el texto en claro, eliminando la «marca de agua» en textos supetiores aumentando la entropía del textocifrado.

5. Texto claro de 64 bitios =TEXTO.(Cualquier dato que se desee cifrar, de 64 bitios d elongitud, igual que el original).
6. Clave de cifrado de 128 bitios = CLAVE.

7. ***DELTA*** = ***DELTA_S*** (9E3779B9 en hexadecimal). Sería el ***DELTA*** semilla, y su valor cambiaría de acuerdo a la paridad o imparidad del texto claro a cifrar.
8. Se nombra una variable llamada N que es la encargada de contar la cantidad de rondas. N = 32 que son las rondas que se quieren para el caso, y es el valor de inicio. N cambiará según la siguiente fórmula: si el texto claro es impar N=32 si es par N=33, que será N_S.
9. Se mantiene la variable llamada ***SUMA***.
   SUMA =0;
10. Se divide la clave en cadenas de 32 bitios cada una: K_1 , K_2, K_3,K_4, como en el algoritmo original .
11. Se divide la información a cifrar de 64 bitios en dos de treinta y dos así:
    $Y_{0\_}$= primeros 32 bits menos significativos del TEXTO PLANO.
    $Z_{0\_}$= últimos 32 bitios más significativos TEXTO PLANO.

El resultado cifrado estará en ***Y_0 e Z_0*** que se convertirán en ***Y_C e Z_C.***

El descifrado tendrá las operaciones inversas a la del cifrado., cuyo algoritmo es el siguiente:

Guía: ⊕ Equivale a la función *XOR*
N_S=32;
{
DELTA = **DELTA_S**
N = N_S;
SUMA=DELTA*N;
mientras que N sea mayor de cero haga:
{
Z_0-=((Y_0<<4)⊕(Y_0>>5)+ Y_0)⊕(SUMA+K[SUMA>>11 & 3])
;
SUMA = SUMA - DELTA;
Y_0= ((Z_0<<4)⊕(Z_0>>5)+ Z_0)⊕(SUMA+K[SUMA& 3]);
N = N-1;
}--- fin del ciclo hasta que n se haga cero
U_TEXTO= Y_0Z_0;
Si (U_TEXTO es impar)
{
DELTA_S=DELTA⊕(U_TEXTO).
}**Si (U_TEXTO es par)**
{
DELTA_S=DELTA;
}
}---Hasta que termine de descifrar toda información.

Fig. 4. Modelo de descifrado XTEA_E (TEAX_E) con el primer aporte.La variable DELTA cambia su valor dinámicamente.

12. Se obtiene el *texto cifrado* o la información cifrada que posee una longitud de 64 bitios.
    TEXTO_C_E
    $Y_{0\_}$= primeros 32 bits menos significativos del TEXTO CIFRADO.
    $Z_{0\_}$= últimos 32 bitios más significativos TEXTO CIFRADO.
13. Se usa el valor del ***DELTA*** de la primera ronda de cifrado, El nuevo ***DELTA*** de la siguiente ronda de iteración dependerá de la información descifrada.
    DELTA_S; Es el delta siguiente, que empieza con el valor: *DELTA_S=0x9e3779b9;*
    DELTA=DELTA_S;
14. Se nombra una variable llamada N que es la encargada de contar la cantidad de rondas. N = 32 que son las rondas que se quieren para el caso, y es el valor de inicio. N cambiará según la siguiente fórmula: si el texto claro es impar N=32 si es par N=33, que será N_S.
15. Se mantiene la variable llamada ***SUMA*** e inicia con un valor igual a cero.
    SUMA =0;
16. Se obtiene la clave de descifrado (la misma que se usó para el cifrado) y se divide en cuatro partes cada una K_1 , K_2, K_3,K_4.
    Clave de cifrado de 128 bitios = CLAVE. (La misma que se usó para el cifrado).
    $Y_{c\_}$= (primeros menos significativos 32 bitios) TEXTO_C_E.
    $Z_{c\_}$= (últimos más significativos 32 bitios)

VI VARIACIÓN DINÁMICA DE LA CLAVE COMO POSIBLE MEJORA TEA Y TEAX.

En este caso la clave de cifrado varía de acuerdo al tipo de *texto plano* que se desea cifrar y se presenta de la siguiente manera:

1. La primera ronda de cifrado se realiza bajo los lineamientos que entregan los algoritmos XTEA o TEA.
2. Al terminar de cifrar la primera ronda se escogen los cuatro octetos menos significativos del texto plano, se pasan por un generador pseudoaleatorio Gaussiano[13] y el resultado es mezclado con la clave de cifrado por medio de operaciones XOR. La razón de esto es por que son los bits que más tasa de variación poseen.

Algoritmo:
{
mientras que N sea mayor a Cero haga:
{---Primer bloque.
Y = Y + (Z << 4 XOR Z>>5) + Z XOR SUMA + K [SUMA **&** 3].
SUMA = SUMA + DELTA,
Z = Z + (Y<<4 XOR Y>>5)+Y XOR SUMA + K[SUMA>>11 **&** 3] ;
N = N-1-SE LE RESTA UNO A N
}
Si (TEXTO es impar)
{
entonces
K clave =⊕K Clave actual
}
} **Hasta que termine de cifrar todo el texto plano.**

Fig 5. Representación de la segunda propuesta de cambio para TEAX. Cifrado

3. Se procede a seguir el algoritmo como es planteado por TEA ó TEAX.

El descifrado se hace de manera análoga a lo que es el cifrado.Se recoge el texto cifrado y se empieza a des-codificar.

1. Obtenido el texto plano se prueba si el texto es impar, si es así se obtienen los cuatro octetos menos significativos del texto plano, se pasan por un generador pseudoaleatorio Gaussiano[13] y el resultado es mezclado con la clave de cifrado por medio de operaciones XOR, y así sale la clave de descifrado del siguiente bloque de texto.

VII. FUNCIONAMIENTO

Los usuarios A y B desean comunicarse entre ellos y cada uno tiene el sistema conectado a la red telefónica de forma tradicional. Al prender el dispositivo ó al iniciar una nueva comunicación el sistema empieza a generar 512 octetos de forma aleatoria con un circuito generador de secuencias pseudo-aleatorias, el cual está conectado al micro procesador por medio de un terminal de entrada, éste a su vez tiene activa la función de conversión analógico a digital cuyo uno de sus puertos está libre y actuando como una antena receptora. En el momento que se termina la conversión, el sistema empieza a leer el puerto conectado al generador de secuencias aleatorias hasta completar ocho octetos. Teniendo los valores aleatorios, se hace la función ***xor*** entre lo recogido por el conversor A/D y lo entregado por el generador de secuencias aleatorias y el resultado se guarda en memoria. Esto se realiza hasta completar 512 octetos u obtener 4.096 bitios para ser usado enmascaramiento.

Por otra parte el micro escoge dos números primos previamente guardados en un banco de claves, de una longitud de 64 bitios c/u, llamados *p* y *q* para usarlos en el algoritmo de cifrado *Rabin[5]*. Los números *p* y *q* hacen parte de la clave privada, estos se multiplican generando la clave pública denominada *n.*

$$\mathbf{n} = p \times q \qquad (1).$$

En el momento que alguno de los dos desea comunicarse con el otro, empieza a formalizar el protocolo de intercambio de claves y el traspaso de la información cifrada, lo que se describe a continuación:
El usuario *A llama al usuario B* y deciden realizar una comunicación segura, en ese momento los *módem* de cada usuario comienzan a negociar el protocolo de comunicación, la velocidad de transmisión y recepción de los datos, mientras tanto el micro empieza a generar las claves para el sistema de cifrado TEAX_E. En el momento que el vínculo se ha estabilizado el usuario *A* transmite su clave pública llamada *nA(2)* al usuario *B*, a su vez éste retorna al usuario *A* su valor de clave pública *rabín nB(3)*. Una vez *A* recibe *nB* entonces cifra su clave privada del sistema TEAX_E.

Luego que *A* recibe la *nB*, escoge los 16 últimos bitios de *nB* y los hace pasar por un generador de secuencias pseudo-aleatorias del tipo gaussiano [13], al realizar esto el sistema sabe en que posición del bloque de 4kb se encuentra la clave cifrada del protocolo de llave privada TEAX_E, al tiempo *A* pasa los últimos 16 bitios de *nA* por un generador de secuencias pseudo aleatorias para encontrar la posición en la cual pondrá la clave privada de cifrado TEAX_E propia *con el bloque los bits de* enmascaramiento.
Acto seguido *A* enmascara su clave cifrada TEAX_E de 128 bits y la transmite a *B* dentro del bloque de 4.096 bitios ó 512 octetos. A su vez *B* transmite a *A* su clave enmascarada de 4.096 bitios. Una vez *A* recibe el valor enmascarado de *B* lo des enmascara de acuerdo con el lugar acordado por las claves públicas.
Después de obtener la clave cifrada de TEAX_E, se procede a descifrarla con el protocolo *RABIN*. Este proceso igualmente hecho por *B*. Teniendo cada uno las claves privadas del otro para el descifrado de la voz, el sistema informa que se puede empezar la comunicación segura.
Se asume que *A* empieza a hablarle a *B*, entonces el sistema de *A* la muestrea la voz a una tasa de 4.800 HZ (para un ancho de banda de 2.400 HZ) entregando una cantidad de 38.400 bps, luego pasa por un compresor de voz de tipo ADPCM[11] el cual entrega la información una tasa de 18.000 bps. El resultado de la compresión es recibido por microcontrolador y este implementa el algoritmo de cifrado TEAX_E de con la clave de cifrado de *A* de 128 bitios a una tasa de cifrado de 20 kilobitios por segundo, pudiendo llegar a cifrar a una tasa de 76 kilobiotos/s. Una vez terminado el protocolo de cifrado el resultado es transmitido a *B* para que sea descifrado. Es ese momento *A* recibe de *B* la información cifrada por éste, el proceso de descifrado empieza por *A*, haciendo la operación inversa al cifrado pero con la clave de cifrado de *B*. Una vez la información está en texto plano, se pasa al descompresor ADPCM y este la entrega al conversor digital analógico y a su vez al teléfono de *A*.

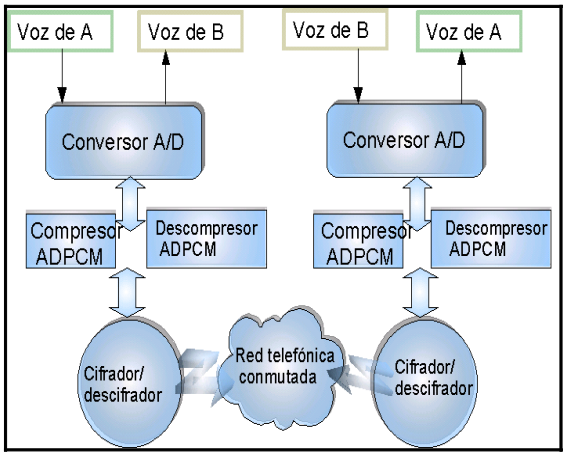

Fig. 7. Esquema del sistema.

[11] Siglas en inglés que significa: Modulación diferencial adaptativo por pulso codificado.

VIII CONCLUSIONES Y APORTES

Este trabajo ha explorado las posibilidades de aplicar los métodos modernos de cifrado en las comunicaciones en especial en la telefonía fija, haciéndose uso de las propiedades de la criptografía para mantener la información confidencial. Se hizo énfasis en la búsqueda de la información y el entendimiento de la misma para entregar un muy buen resultado en lo que se refiere a la parte algorítmica, buscando un sistema seguro y fuerte en contra de criptoanálisis genérico, no por fuerza bruta.
Se entrega en este proyecto tres tipos de aportes dos técnicos y uno académico. El primer aporte técnico es el diseño y la implementación de un sistema de cifrado de voz para la telefonía pública fija en Colombia, con posibilidades comerciales; el segundo aporte técnico es el uso de la esteganografía de acuerdo a un protocolo específico de involucrado dentro del sistema de cifrado y no como un enmascaramiento simple. El tercer aporte, es el académico al presentar de forma oficial el algoritmo de cifrado TEAX_E para textos mayores a 64 bitios, que se basa en el algoritmo TEAX, que es el cambio dinámico del valor de ***DELTA*** respecto a la entrada del texto claro, ó el cambio dinámico de la clave de cifrado enriqueciendo el algoritmo.

Esta mejora también es aplicable al TEA, quedando TEA_E. El algoritmo demuestra su funcionamiento en este proyecto.

Queda una consideración abierta, la de realizar un criptoanálisis al sistema TEAE y XTEA_E (TEAXE) que comprueba de forma contundente la mejora del algoritmo con respecto a su seguridad. Ëste estudio queda por fuera de los límites del proyecto y puede ser usado para una posible especialización en criptografía.

Referencias

[1] **CONSEJO DE LA UNIÓN EUROPEA.** Acto del consejo del 29 del mayo del 2.000 por el cual se reglamenta la asistencia judicial de los estados de la Unión. Diario oficial de las Comunidades Europeas. 12 de julio del 2.000.

[2] **ROTENBERG** Mark. CiberAttack: The National Protecction Plans And Its Privacy Implications. Electronic Privacy Information Center. Washington D.C. www.epic.org. 1 de febrero del 2.000.

[3] **LUCENA** López, Manuel J. Criptografía y Seguridad en Computadores. Tercera Edición. Departamento de Informática. Escuela Politécnica Superior Universidad de Jaén. Junio del 2.001.

[4] **MULLINS** Justin. Making unbreakable code. IEEE SPECTRUM mayo 2.002, páginas 40-45.

[5] **WHEELER** D. y R. Needham, TEA, a Tiny Encryption Algorithm, Fast Software Encryption, Second International Workshop Proceedings, Springer-Verlag. 1.995 Pág. 97-110.

[6] **SHANNON**, Claude E. Communication Theory of Secrecy Systems. Bell Syst. Tech. J. Vol 28, 1949.

[7] **ÁLVAREZ MARAÑÓN.** Contribución al estudio de la estructura interna Mandelbrot y aplicaciones en Criptografía. Universidad Politécnica de Madrid. Facultad de Informática. 2.000.

[8] Private Comunication, Eurocrypt 1.997.

[9] **ROGER M. NEEDHAM Y DAVID J. WHEELER.** http://www.cl.cam.ac.uk/ftp/users/djw3/xTEA.ps. 1.997. David A. G. Gillies: http://vader.brad.ac.uk/TEA/TEA.shtml.

[10] **MOON** Dukjae, Hwang Kyungdeok, Lee Wonil, Lee Sangjin y Lim Jongin. Impossible Differential Cryptanalysis of Reduced Round XTEA and TEA. Centro para las tecnologías de la información y seguridad (CIST siglas en inglés). Universidad de Korea, Seúl, Korea del Sur.

[11] http://www.xs4all.nl/~bslash/muren/contenido.htm. Buscadores español.yahoo.com & www.alavista.com..

[12] **MENEZES A.**, Van Oorschot P., Vanstone S. Handbook of applied cryptography. CRC Press, 1.996. www.math.uaterloo.ca/hac**.**

[13] **Amar Palarcherla**, DS00544D. Microchip Technology Inc. 1997.