21
2ej.

UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES

CAMPUS ARAGON

"BASES PARA EL DISEÑO DE ENCRIPTADORES DE VOZ"

T E S I S

QUE PARA OBTENER EL TITULO DE:

INGENIERO MECANICO ELECTRICO

(AREA ELECTRONICA Y COMUNICACIONES)

P R E S E N T A N :

ULISES OCTAVIO DIAZ NIETO

JOSE ADRIAN MENDEZ TAPIA

ASESOR: ING. DAVID BERNARDO ESTOPIER BERMUDEZ

MEXICO 1998

A LA MEMORIA DE MI MADRE
CON TODO EL AMOR QUE
PODRE SENTIR A LO LARGO
DE MI VIDA
Por que su legado e increible
cariño me enseñaron a seguir mi
propio camino.

A MI TIA
Por el amor. cariño y la ayuda
siempre incondicionales que me
ha dado. Sin ella no hubiera
podido hacer esto.

A GABRIELA
Agradezco a Dios por permitirnos
compartir nuestra vida y sueños, y
darme una razón más para nunca
darme por vencido.

A MIS PRIMOS
Por darme su apoyo y ser parte de mis
logros

ADRIÁN...

A MIS DOS GRANDES
AMORES
MINERVA Y JENNIFER
Por ser mi fuerza y alegría para
salir adelante.
LAS AMO

A MI MADRE RITA
Por quererme tanto y darme la
oportunidad de superarme

A MIS PADRES
Por darme el mejor regalo del
mundo, la vida

A MIS HERMANOS
ANA, RITA, LAURA, CECI,
AMADO, Y EDUARDO
Por ser mi ejemplo y siempre estar
para ayudarme en todo momento

Y MUY EN ESPECIAL A LA
MEMORIA DE MI HERMANA
ELSA
Sé que está orgullosa de mí...

ULISES...

A NUESTRO ASESOR EL INGENIERO DAVID BERNARDO ESTOPIER BERMUDEZ

Por sus valiosos consejos, amistad y apoyo incondicional para la elaboración de este trabajo de tesis

A NUESTROS AMIGOS

EDGAR, JESUS, JORGE E., CARLOS, ISRAEL, PAUL Y JORGE V.

El orden no altera los sentimientos.

Por su sincera amistad.

"Siempre hemos sido un gran equipo"

A LA UNIVERSIDAD NACIONAL AUTONOMA DE MÉXICO

Con gratitud imperecedera

ADRIÁN Y ULISES

CONTENIDO

CAPÍTULO 3.
CRIPTOGRAFÍA

PRONTUARIO.

DEL

CAPITULO 3.

CAPÍTULO 4

ANÁLISIS DE IMPLEMENTACIÓN DE UN SISTEMA DE ENCRIPTAMIENTO.

PRÓLOGO

Lo que compete a este trabajo es presentar al lector una visión introductoria y general de lo que es el encriptamiento, y presentar lo más sobresaliente que cualquier persona debe tomar en cuenta para poder adentrarse aún más en este tema, en cualquiera de sus áreas, ya sea desde los principales protocolos, procesamiento digital de señales, importancia de la seguridad, evaluación de necesidades, etc.

Consideramos en nuestra investigación, debía tener fines de divulgación, ya que aunque es una ciencia muy usada y constantemente renovada, existe gran ignorancia respecto a ella, aún con personas que tienen un respaldo académico notable, por lo menos en el sentido que se debe explotar, protección de información en múltiples áreas y medios de comunicación; aun que casi todos recordaron el clásico cuaderno con símbolos asociados utilizado en la Escuela Secundaria para pasarse mensajes durante las clases, consideramos esto por ser un ejemplo bastante primitivo de lo que es en sí la criptografía.

Al hacer popular a una ciencia o tema se ganan adeptos, lo que contribuye a hacerla mejor, puesto que más cerebros aportan algo que podríamos llamar como lluvia de ideas, de toda esa información y propuestas podría revolucionarse para hacerla más evolucionada, difundida y alcanzable a un mercado más extendido de los que es el actual, siempre se ha dicho que la competencia mejora el producto y esto no es la excepción.

Si usted no tiene nada que proteger, si toda la información que procesa puede ser publicada, si algún desarrollo de proyecto no es innovador, si la distorsión de información no es una amenaza para usted o para quien trabaja, si no usted no tiene competencia y si usted no usa computadoras o teléfonos, le agradecemos por aceptar esta tesis, pero no se moleste en leerla, porque usted no necesita criptografía.

Si en cambio, usted procesa información importante y si la distorsión o el acoso de la misma por agentes ajenos a sus intereses es una amenaza para usted o su empresa, usted debe utilizar criptografía.

Las técnicas de criptografía han sido usadas para propósitos militares por décadas, pero en el ambiente comercial no ha sido tan común como se hubiera esperado. La razón para eso es que las técnicas han sido muy caras comparadas a la necesidad de utilizarla. Sin embargo, la situación está cambiando rápidamente. Hoy en día el hardware y el software criptográfico se han vuelto más barato, y las necesidades se han vueltas más obvias. De hecho la criptografía se ha vuelto una herramienta de todos los días en los sistemas comerciales.

La información es un recurso muy importante de una compañía. Usted puede invertir dinero y esperar muy buenas ganancias de dicha inversión. Usted debe ser capaz de confiar en la calidad de la información y estar convencido de que información confidencial no caiga en manos de alguien no deseable.

Existen riesgos en el proceso, almacenamiento y el transporte de información. Esta puede ser distorsionada o falsificada durante el procesamiento. La información almacenada puede ser copiada o cambiada sin autorización. Al transmitirla vía disquetes, cintas o teléfono pueden ser dirigidas a las manos equivocadas o inclusive substituida.

¿Qué clase de problemas puede usted resolver con métodos criptográficos?. Criptografía es un medio práctico para proteger la transferencia de información y en muchos casos es la mejor forma de protegerla en su forma almacenada. La criptografía es el

proceso de transformar en una forma ininteligible para que pueda ser enviada a través de canales inseguros o que pueda ser almacenada en archivos inseguros, Hoy en día, en la era de redes abiertas, hackers y crackers, no podemos considerar cualquier canal de comunicación como seguro.

Con el encriptamiento usted puede traducir datos a una forma que el intruso no pueda interpretar como usted lo haría, a menos que él o ella conozca el método y la clave utilizada en el proceso.

El proceso inverso consiste en traducir los datos encriptados a información clara. Al encriptar los datos antes de transferirlos o almacenarlos y desencriptarlos antes de su proceso uno puede asegurarse de su confidencialidad.

Los datos falsificados parecen tan genuinos como los originales. Por lo que la autenticación de información debe ser evidente, puesto que se maneja para hacer decisiones vitales. Con las técnicas criptográficas usted puede descubrir la distorsión o falsificación de datos. Pero uno debe darse cuenta de que la criptografía no previene de que un intruso obtenga sus datos ni de que los substituya, pero si de que utilice lo que obtuvo en su beneficio. Los procedimientos criptográficos pueden ser usados para identificación personal, firmas digitales, control de acceso, etc. El criptosistema tiene usualmente un algoritmo criptográfico, que puede ser público o secreto, y un grupo de caracteres que es conocido como la llave. En la mayoría de los casos la llave es la fuerza básica para mantener el secreto de todo el sistema. Las medidas por las cuales las llaves son generadas, almacenadas, transferidas y cambiadas. Se les llama administración de llaves. Por lo general, se refiere a un sistema jerárquico muy complejo, y es aquí precisamente donde se encuentra el punto más débil de casi todos los sistemas.

Cuando usted decida usar criptografía, debe recordar dos cosas: la decisión no es suficiente y la criptografía no es suficiente. Esta no es el camino más fácil para protección. Hay muchos obstáculos en el camino: la velocidad de un algoritmo puede ser una restricción, la complejidad de una red puede hacer una solución muy cara, la creación junto con el almacenamiento y la distribución de llaves puede ser la tarea más difícil. Si usted decide usar criptografía, debe planearlo muy cuidadosamente. Un criptosistema mal planeado da un falso sentido de seguridad. Bien es cierto que la criptografía es una herramienta muy poderosa, pero no puede hacer por sí sola su ambiente de transmisión completamente seguro, además, usted debe usar precauciones de seguridad apropiadas.

Al aplicar técnicas criptográficas, uno debe tener en mente que las medidas adoptadas deben ser administrables por todos los elementos involucrados, especialmente por el usuario, quién, como regla, sabe muy poco o nada de criptografía. El riesgo de fallar en la administración puede venir de varios puntos, el primero es el hecho de que las llaves de encriptamiento deben ser distribuidas a todos los lugares donde la transformación criptográfica se va a llevar a cabo, otro es la incompatibilidad de los productos hechos por diferentes fabricantes, algo común es que ciertos sistemas requieren seguridades con adaptaciones muy específicas, lo cual causan dificultades al intentar estandarizar equipos.

Afortunadamente en los últimos años esto ha estado cambiando con el advenimiento de los criptosistemas de llave pública y la finalidad de lograr una estandarización se ha vuelto un esfuerzo en el ámbito mundial, apoyado por ISO y CCITT, para llevarla adelante del diseño de productos comerciales. Estos puntos proporcionan nuevas áreas de aplicación o bien facilitan soluciones rápidas a viejos problemas. Algunos proyectos en otras áreas ayudan de gran forma a la criptografía como es el desarrollo de tarjetas con chips. Todo esto puede resolver algunos problemas en técnicas empleadas.

No es para sorprendernos que la representación binaria de caracteres en computadoras, estimularon el desarrollo de nuevos algoritmos criptográficos. Las técnicas criptográficas basadas en estos algoritmos son mucho más poderosas que las tradicionales. Pero las técnicas de criptoanálisis también han sido desarrolladas al mismo tiempo. Las preguntas a contestar más frecuentemente son: ¿dónde colocar encriptamiento en un sistema sin disminuirlo o alterarlo?, ¿Que información vale la pena cifrar?, ¿Es administrable el problema de la distribución y control de llaves?, En computadoras o sistemas que las utiliza más de una persona y que no tienen los mismos accesos ¿es confiable aplicar encriptamiento en una forma de selección individual?, etc.

Usualmente los productos para encriptar son hardware, por tres razones principalmente: velocidad, seguridad y facilidad de instalación. El hardware es deseable debido a que la mayoría de algoritmos de encriptamiento no están adaptados al conjunto de instrucciones de una computadora de propósito general. Un ejemplo de esto es el DES, el cual contiene permutaciones entre 64 bits. Generalmente no hay computadoras que operen en bits por separado, así que ésta parte debe ser implementada con simulación de un tratamiento de bit por bit, lo cual es lento, o también con la ayuda de tablas gigantescas, las cuales no pueden ser colocadas en un espacio razonable. De esta forma el software del DES utiliza mil veces el tiempo necesitado para una implementación de hardware en un circuito dedicado.

Actualmente el DES es estandarizado como hardware por el NBS. Otro de los algoritmos más conocidos, RSA, sufre los mismos problemas con la velocidad en implementaciones de software. La encripción de un solo bloque de 512 bits puede tomar hasta varios segundos, lo cual no puede ser aceptable y por esto las implementaciones del RSA utilizan chips VLSI de diseño especial. En general, los algoritmos de encripción son diseñados de acuerdo a su propio criterio y no a las instrucciones de computadoras. Es por

eso que la mayoría de los algoritmos son más rápidos en hardware dedicado que en rutinas de software.

Otro aspecto del problema con la velocidad es que la encripción mantiene al procesador ocupado por una extensión de tiempo bastante grande. Vale la pena usar encripción con un dispositivo específico aún si se usa un procesador estándar, mucho tiempo es ganado gracias al paralelismo que es introducido.

Respecto a la seguridad, el problema es que una computadora común no tiene protección física para su contenido, casi siempre su gabinete puede ser abierto y ser intervenido para exponer su contenido tanto en software como en hardware. Un chip dedicado a encriptamiento puede ser encapsulado seguramente, la lógica interna puede ser diseñada para que llaves sin encriptar permanezcan dentro del dispositivo y no hay instrucciones que puedan leerse desde afuera.

Un problema más es que la radiación electromagnética puede revelar que sucede en el interior de cualquier equipo electrónico, un hábil oponente puede aprovechar esto, el hardware dedicado también resuelve esto.

Finalmente la facilidad de instalación depende de donde pueda encontrar interfaces lógicas estándar para su encriptamiento; hoy se utiliza para comunicaciones, en un nivel del standard OSI donde la protección no debe enmarañar su trabajo; por esto si usted decide utilizar software debe ser depositado muy adentro del sistema. No existen estándares y aún la misma versión del mismo equipo puede diferir en aspectos cruciales debido a la configuración de los sistemas donde trabajarán. Las interfaces físicas de este nivel son estandarizadas y son convenientemente disponibles, casi cualquier persona puede desenchufar su terminal y conectarla su "caja negra" en el mismo lugar y finalmente conectar la línea del módem a la "caja negra".

Existen dos tipos de software que dominan el mercado: cajas que son destinadas a conectarse en una línea de comunicaciones y tarjetas para PC´s. Las criptocajas han estado en el mercado por mucho tiempo, originalmente las únicas disponibles eran para uso militar, lo cual se reflejaba tanto en el precio como en su protección.

Hoy en día la seguridad y el precio dependen del uso; el mercado cambia rápidamente y aunque algunos proveedores se han mantenido activos por años, algunos pueden desaparecer en los próximos meses. Los objetivos del momento es alcanzar tazas de bits mayores y mayor flexibilidad en el uso.

La administración interna de llaves es de tal cualidad que es raro que el usuario deba intervenir. Hay otros productos menos sofisticados con solo una llave disponible, es adecuado para algunas situaciones, pero el comprador debe asegurarse siempre de que su administración sea confiable.

El equipo de encriptamiento puede ser diseñado tanto para encriptar todo lo que sale de un sistema y desencriptar todo lo que entra, o para encriptar y desencriptar el actual mensaje debido al estándar del protocolo de comunicaciones. Este tipo de equipo puede ser instalado sin adiciones o cambios en el software en algunas ocasiones, en otros será necesario crear rutinas que puedan seleccionar que información será encriptada.

Con algunas desventajas cualquier algoritmo de encriptamiento puede ser implementada como rutina de software, pero sus ventajas son la portabilidad y la flexibilidad. Un programa escrito en un lenguaje estándar de alto nivel puede ser instalado en cualquier máquina que soporte ese lenguaje, lo cual ofrece cada vez más cualquier máquina. Un programador puede hacer conversiones entre lenguajes y puede usar el

programa si desea protección extra para alguna comunicación o ser incluido como parte de un sistema más grande.

El software es muy popular entre los usuarios de PC´s. Tal encriptamiento es propuesto cuando se comunique con otra PC o deje desprotegida la suya. Es importante que el usuario desarrolle una administración de llave de acuerdo a sus necesidades específicas, que él programa borre llaves y archivos después de encriptarlos, datos importantes nunca deben dejarse desprotegidos, etc., de no tomar estas y otra medidas, un oponente diestro podría destruir su perímetro de seguridad.

CAPÍTULO 1

LA VOZ Y LAS COMUNICACIONES

1.1 CARACTERISTICAS DE LA VOZ

La voz humana en esta y todas las épocas, ha sido la más importante forma de comunicación, de ahí que se han buscado diferentes maneras de transmitirla, pero a su vez protegerla para que esta solo sea entendible para una de las partes destino.

El encriptamiento es una de las formas más comunes de proteger las señales de voz, ya que gracias a él es difícil que una persona ajena logre entender el mensaje que se esta transmitiendo. Sin embargo, para poder procesar las señales de voz y contar con los grandes beneficios que se tienen al encriptarla, se deben tener en cuenta sus características eléctricas.

En principio sabemos que las señales de la voz humana son señales acústicas y por tanto señales analógicas, al observar el espectro en frecuencia de una señal de voz (fig.1) nos damos cuenta que estas se encuentran en el intervalo de 300 a 3300 Hz.

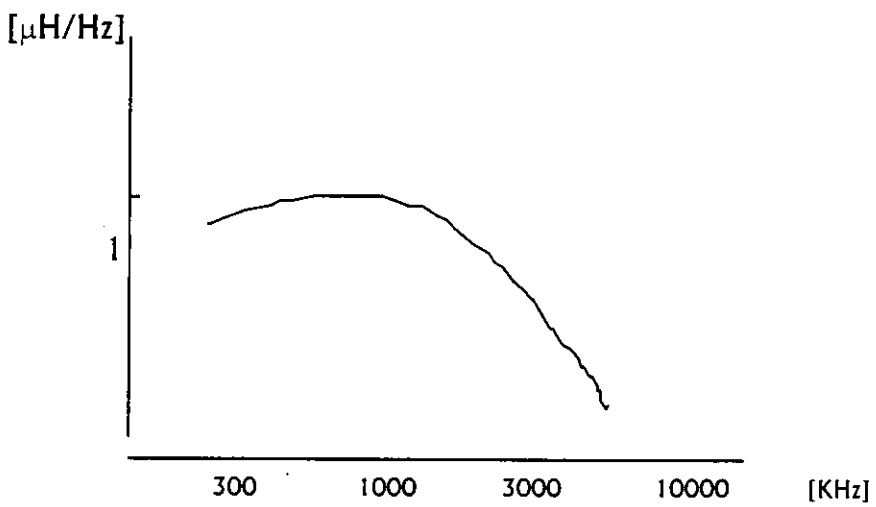


Figura 1

Esta observación es muy importante puesto que para poder diseñar un convertidor analógico digital estas frecuencias serían las que nos interesan.

La potencia de las señales de voz es otra de las características importantes, su nivel efectivo de tiempo largo depende de cada individuo y esta variación depende también del modo de pronunciación de cada persona, en promedio el nivel efectivo de tiempo largo de la voz de distintas personas se sitúa aproximadamente en los 59 dB. La desviación estándar de la voz de un hombre y una mujer es aproximada a 3.75 dB.

La producción de la voz en el humano se realiza con un conjunto de músculos, los cuales tienen un objetivo en especial, por ejemplo: el tracto vocal entre los labios y el glotis puede ser comparado electrónicamente con la respuesta que tiene un filtro (lineal) en función del tiempo, en otras palabras si unimos una fuente de ruido con una fuente de impulsos eléctricos que trabaje periódicamente y esta señal la hacemos pasar por un filtro lineal lograremos producir un sonido muy parecido a la voz humana (figura 2)

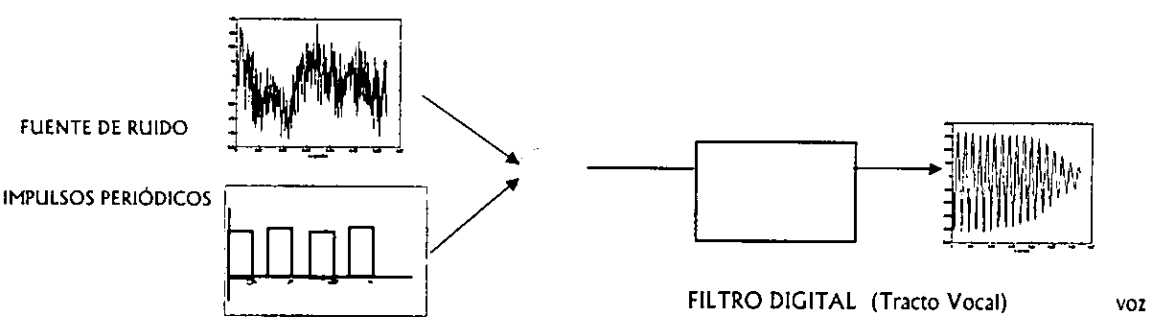


Figura 2. - Producción de voz Electrónica.

La fuente de ruido es la que asemeja las vibraciones que producen las cuerdas vocales, ya que éstas solo producen sonidos que serán manipulados en el tracto vocal, que en este

caso será simulado por el filtro lineal quien hace la transformación a parámetros espectrales.

Como se había dicho anteriormente, la pronunciación y los mecanismos físicos del tracto vocal provocan redundancias en las señales de voz, la envolvente de su espectro se encuentra determinada por la frecuencia del filtro (tracto vocal), esta resonancia se observa como picos en la envolvente espectral.

1.2. FONEMAS DE LA VOZ

El estudio de espectros de los fonemas es muy importante, ya que dependiendo de la forma de emitir los sonidos los espectros presentarán características destacables.

La voz es una onda acústica. Para procesarla es necesario transformarla en una magnitud eléctrica. En la figura 3 se puede observar la señal eléctrica medida con un micrófono y que corresponde a un segmento de voz de un cuarto de segundo de duración, correspondiente a la palabra ``sent''.

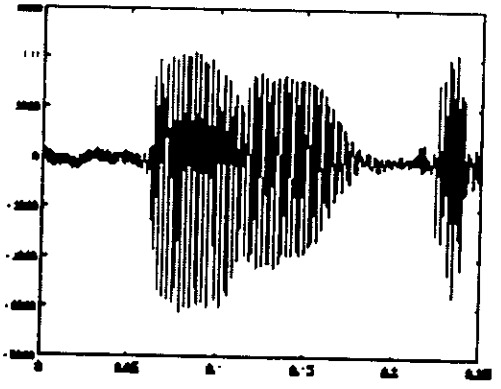


Figura 3: Segmento de voz. Se corresponde con la palabra ``sent''

En la figura anterior pueden encontrarse cuatro características destacables

• Fonema /s/: Se caracteriza por tener poca energía y una tasa de cruces por cero muy alta (la tasa de cruces por cero tiene una estrecha relación con la frecuencia). Estas propiedades las tienen todos los fonemas fricativos (letras cuya articulación hace salir el aire con cierto roce o golpeteo de la boca /z/, /f/, /x/, /p/..). En la figura 4 se puede apreciar con mayor detalle la forma de onda correspondiente a este fonema.

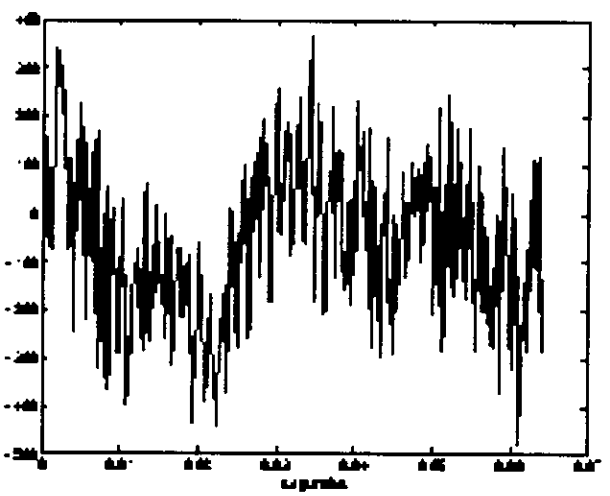


Figura 4: Segmento de voz. Correspondiente al fonema /s/

Puede apreciarse la naturaleza ruidosa de los fonemas fricativos. El espectro asociado al fonema /s/ se representa en la figura 5.

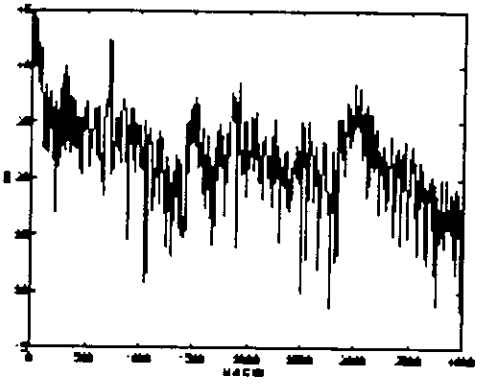


Figura 5: Espectro del fonema /s/

A partir de esta figura puede concluirse que los sonidos fricativos están asociados a componentes de frecuencia elevadas.

• Fonema /e/: Se caracteriza por tener una alta energía (amplitudes elevadas). En las figuras 6 y 7 se representan su forma de onda asociada y el espectro, respectivamente.

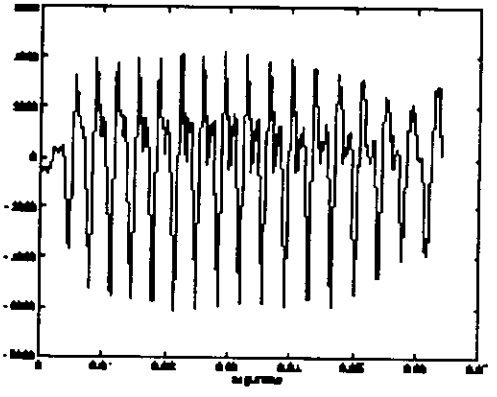


Figura 6: Segmento de voz. Correspondiente con el fonema /e/

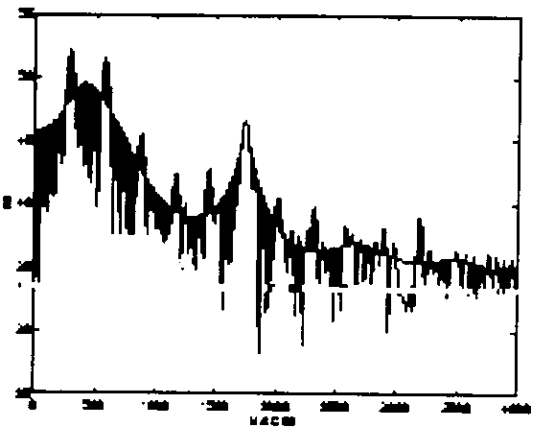


Figura 7: Espectro del fonema /e/. Aparece superpuesta la envolvente del espectro

A partir de la representación de la forma de onda, puede concluirse que el fonema /e/ tiene una estructura casi periódica. Esta periodicidad se debe a la vibración de las cuerdas vocales que se produce en todo fonema sonoro (fonemas vocálicos,...). Esta propiedad se refleja también en el espectro. Así, en la figura 7 puede apreciarse que en el espectro pueden distinguirse dos estructuras.

• Envolvente del espectro. Es la estructura que aparece superpuesta al espectro original. Su forma viene determinada por las modificaciones que impone el tracto vocal (laringe, faringe, lengua, cavidades palatal y nasal) al chorro de aire expulsado desde los pulmones. Se pueden apreciar unos máximos relativos en la envolvente. La frecuencia de esos máximos relativos depende del fonema que se esté pronunciando. A las frecuencias en las que se producen esos máximos se denominan ``formantes''. Para modelar la respuesta del tracto vocal se suele emplear un filtro como

$$H(z) = \frac{G}{A(z)} = G\frac{1}{1 - \sum_{k=1}^{p} a_k z^{-k}}$$

• Componente periódica. Se puede apreciar una componente periódica en el espectro, mucho más clara en frecuencias inferiores a 2 kHz. La diferencia entre las frecuencias de dos picos consecutivos es lo que se denomina ``pitch'' o frecuencia fundamental. Los valores típicos del pitch oscilan entre 60 y 400 Hz. (en las mujeres el valor es mas alto que en los hombres)

• Fonema /n/ Es un fonema nasal que tiene una estructura muy parecida a los vocálicos. La forma de onda y su espectro se representan en las figuras 8 y 9 respectivamente.

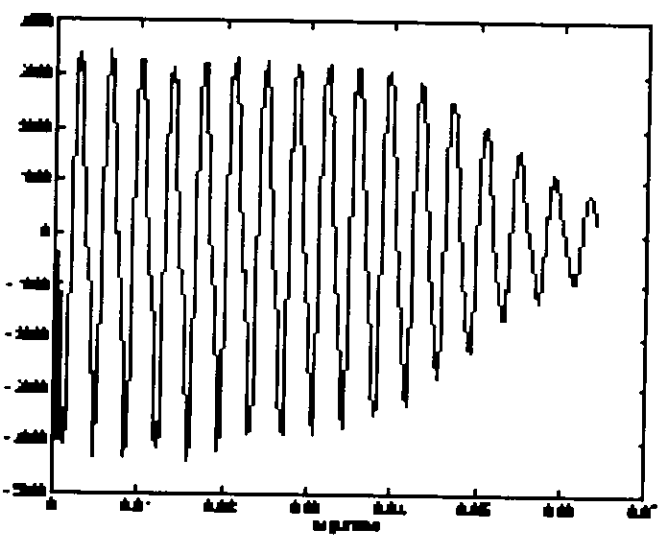


Figure 8: Segmento de voz. Correspondiente con el fonema /n/

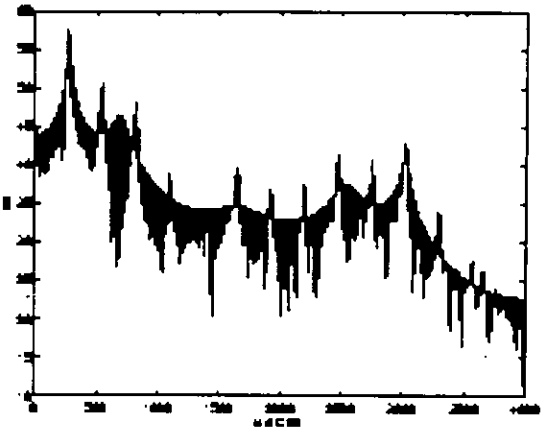


Figura 9: Espectro del fonema /n/. Aparece superpuesta la envolvente del espectro

• Fonema /t/. Este fonema oclusivo se caracteriza por un intervalo de silencio seguido de un rápido incremento en los niveles de la señal. Esta ``explosión'' de señal está directamente relacionada con el violento movimiento de apertura y cierre del aparato fonador. En la figura 10 puede apreciarse la forma de onda asociada.

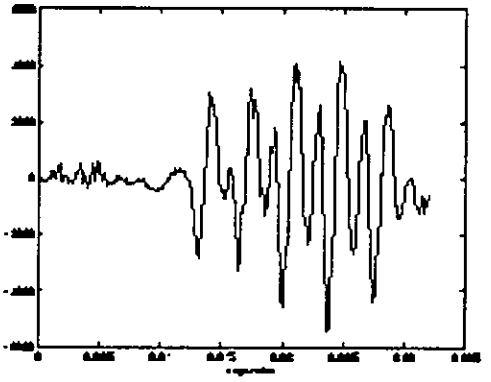


Figura 10: Segmento de voz. Se corresponde con el fonema /t/

1.3. MUESTREO Y LAS SEÑALES DE VOZ

El muestreo es un método para procesar las señales analógicas digitalmente, este método consiste en representar la señal analógica como una sucesión de números, estos números son las muestras que se toman periódicamente de la señal analógica, esto se representa como $x(n)=x_{\infty}(nT)$ en donde $-\infty < n < \infty$ y n tiene valores enteros.

Para realizar el muestreo de las señales digitales de voz se deben considerar también las propiedades espectrales de estas. Como ya se vio, los espectros de los fonemas fricativos, las señales de voz no son exclusivas de banda limitada, aunque su espectro desciende a altas frecuencias. Cuando la voz es muy sonora tiene magnitudes mayores a 40 dB, mientras que cuando la voz es no sonora (X dB's), el espectro no se reduce para frecuencia mayores de a 8 Khz aproximadamente.

Con esto nos damos cuenta de que el promedio requerido de muestras para representar a la voz debe ser de aproximadamente 20 Khz. Algo importante en el muestreo es que aunque la forma de onda puede tener el aspecto de una onda de banda limitada, esta señal es degenerada casi generalmente por el ruido, para evitar esto la señal debe ser filtrada por un filtro paso banda que cortara la frecuencia en la frecuencia de Nyquist, así esta señal de ruido será descartada en la banda base. Esto es sumamente importante para la conversión de las señales analógicas a digitales.

1.4. SISTEMA DE COMUNICACIÓN

Por distintas razones, el hombre busca siempre la forma más fácil, económica y rápida para comunicarse, para esto se ha valido de lo que conocemos como sistemas de comunicación, cuyo concepto es universal y que aquí explicaremos parte por parte; esto es debido a que el tema principal de éste trabajo es un elemento de un sistema de comunicación, agregado a causa de la rápida evolución de los métodos para irrumpir de forma indeseable, por agentes externos a nuestros intereses y beneficios (criptoanalista), en dichos sistemas.

Un sistema de comunicación es en sí un conjunto de elementos y/o dispositivos cuya finalidad es transportar un mensaje (contenido, información, etc.) en espacio y tiempo a través de un medio, desde un punto que llamamos transmisor (Tx) hasta otro que llamaremos receptor (Rx) situados a los extremos del medio de transmisión. Fig. 1 1

Ahora bien, para fines prácticos se busca manejar el mensaje en forma de señales eléctricas para que se pueda desplazar por el medio (alambre de cobre, microondas, fibra óptica, etc.). En nuestro caso específico el mensaje se trata de la voz humana, y para transformarla en señales eléctricas necesitamos adicionar elementos a nuestro sistema de comunicación los cuales se conocen como transductores, uno colocado en el transmisor y otro en el receptor. A continuación ilustraremos dicho sistema:

Figura 1 1

La función del transductor en sí es adaptar la información para que el transmisor la pueda enviar por el medio, después de esto el transmisor la prepara para viajar, esto

comprende varias etapas, entre las cuales están la modulación que puede ser en varios parámetros de la señal y otra la de amplificación, esto es debido a que muchas veces nuestras señales recorren grandes distancias geográficas por el medio de transmisión, lo cual provoca que se vuelvan susceptibles a distorsiones, interferencias y/ o ruido, lo cual es indeseable y aleatorio, estos factores muchas veces provocan la pérdida parcial o total de nuestro mensaje, con la amplificación nuestra señal puede tener la potencia necesaria para llegar a su destino o bien si la distancia es mucho muy grande ser recibida en otra etapa que la regenera o amplifica para que pueda seguir viajando.

El medio de transmisión, como se dijo anteriormente es el camino que recorre nuestra señal para llegar a su destino, y pueden ser de varios tipos: par torcido, cable coaxial, aire, fibra óptica, etc. el escoger que medio utilizaremos dependerá de nuestras necesidades y recursos disponibles, ya que cada uno tiene distintas características que nos puedan beneficiar o perjudicar.

El receptor captura las señales del medio de transmisión y las obliga a pasar por las mismas etapas del transmisor pero de forma inversa para que recobre su forma original y pueda ser entendida como lo envió el transmisor, tiene su etapa de amplificación, demodulación y transducción, en ésta parte el transductor recibe las señales eléctricas y las convierte en voz.

1.5. SISTEMAS DE COMUNICACIÓN DIGITAL.

Los Sistemas de Comunicación Digitales (DSC) se basan en lo anteriormente descrito y a continuación se da una explicación de sus características. Consideramos importante mencionar que la descripción de las etapas que damos del Sistema de Comunicación Digital es en forma cronológica, es decir la señal o información recorre cada una de las etapas en el orden en que las estamos mencionando.

Lo primero es transformar el mensaje en símbolos digitales para hacerla fácil de procesar, a esto se le llama formateo. Después la codificación del transmisor hace la conversión analógica-digital, en caso de ser necesaria, y elimina la redundancia de información en el mensaje. Por seguridad se pasa por una etapa de encriptamiento o ciframiento para que únicamente ciertos usuarios comprendan el contenido del mensaje; esta etapa también evita adiciones falsas de mensajes.

La siguiente etapa se conoce como codificación del canal, el cual reduce el ancho de banda en la relación señal a ruido, esto dependerá de las características de nuestro sistema. Esta etapa la realiza un codificador para tener un seguimiento por medio de un mapeo de las señales que ingresan en nuestro sistema en la parte de recepción se realiza la operación inversa con un decodificador.

Inmediatamente está la multiplexación, cuyo fin es el lograr que todas las señales que entran salgan por un mismo medio compartido.

Después se encuentra la modulación que como ya dijimos es la alteración de alguno de los parámetros de la señal para una adecuación a las cualidades del medio de transmisión seleccionado.

Como una forma de protección a nuestra señal contra interferencias de cualquier tipo (naturales y/o artificiales), se comprime en frecuencia, y de esta forma aumentamos la privacidad de nuestro canal.

Cabe mencionar la etapa de acceso múltiple, la cual tiene como finalidad repartir un recurso único en varias partes iguales para distintas señales. Se vale de distintas técnicas, por mencionar algunas diremos: FDMA (Frecuency Division Multiple Access), TDMA(Time Division Multiple Access), etc. Sus diferencias se establecen en variaciones de potencia y frecuencia; se utilizan de acuerdo a los criterios de preasignación, asignación en tiempo y asignación por demanda.

En cuanto al receptor de un sistema de comunicación digital, nuestra señal pasa por cada una de las etapas que posee el transmisor, pero de forma inversa para devolver las características originales de la señal inyectada en el sistema, de forma que solo las mencionaremos, pues basta con decir que su función será la inversa de la etapa antes mencionada: Acceso Múltiple, Descompresión de Frecuencia, Demultiplexaje, Decodificación de canal, Demodulación, Desciframiento, Decodificación de Fuente, Formateo y Sincronización, éste permite que todos los elementos interactúen en armonía.

Ahora hablaremos del medio de comunicación el cual puede ser de distintas clases o tipos, ya los hemos mencionado, pero lo que nos importa momentáneamente son los fenómenos que producen daño a nuestra señal y estos son: atenuación, distorsión, interferencia y ruido.

El primero se refiere a una pérdida de potencia gradual que aumenta conforme nuestra señal recorre más distancia, de ahí la importancia de seleccionar medios de comunicación que eviten esto, o bien colocar amplificadores a lo largo del camino para que éstos le apliquen potencia a nuestra señal hasta su destino; de lo contrario se puede perder la señal o alterar de forma significativa.

La distorsión se define como la alteración de la señal debido a la respuesta imperfecta del sistema a ella misma. Para contrarrestar esto se debe aplicar compensación a nuestra señal, aunque en la práctica muchas veces es mejor permitir que nuestra señal posea cierta distorsión siempre y cuando no exceda límites de calidad.

La interferencia es la invasión de señales ajenas a la nuestra, es decir si detectamos dos o más señales en nuestro canal es que existe interferencia.

El ruido lo manejaremos como señales aleatorias e impredecibles de tipo eléctrico originadas de forma natural dentro o fuera del sistema. Digamos que el ruido de alguna manera oculta o "tapa" nuestras señales evitando su apreciación correcta.

1.6. IMPORTANCIA DE LA SEGURIDAD EN LAS COMUNICACIONES.

El riesgo siempre vive. Todos de alguno forma u otra dependemos de las comunicaciones en algún momento. Son usadas para enviar información que pueden ser desde archivos médicos, planes económicos hasta reportes criminales. Y aunque confiamos en ellas, éstas serán siempre vulnerables a diversos problemas como lo son, un diseño deficiente, control de calidad insuficiente, accidentes y posiblemente el más alarmante de

todos, el ataque deliberado. Los ladrones modernos pueden robar más con una computadora que usando armas, o bien los ataques terroristas pueden ser más efectivos al manejar un teclado que al hacer detonar una bomba en algún lugar estratégico.

Si hasta el momento no nos ha sucedido nada malo en nuestro campo de comunicaciones, podemos decir que hemos tenido suerte, pero nadie nos puede asegurar que continuaremos así, debemos reflexionar en el tema ya que en muchas ocasiones, dinero, bienes materiales y hasta vidas dependen de las comunicaciones.

Bien puede ser que hemos confiado nuestro sistema de seguridad a la ausencia de personas maliciosas; pero es un error mantener esa actitud, debemos intentar construir sistemas que sean seguros y confiables.

Ahora bien, debemos identificar las causas de las posibles violaciones a nuestro sistema, pues bien pueden ser debidas a un deficiente diseño del sistema, una implementación defectuosa, una mala administración de los procedimientos que lo rigen, accidentes, etc. pero cualquiera de estas situaciones favorecen a posibles ataques, y por supuesto que un sistema confiable es aquel que sobrevive ante cualquier incidencia que amenace su privacidad.

La seguridad es una preocupación de organizaciones cuyos bienes son controlados por las comunicaciones. Alterando o simplemente accesando a nuestra información, un atacante puede robar bienes tangibles o ayudar a que determinada organización emprenda acciones que de otra forma no pudiera realizarlas. Solo por examinar lo que estamos enviando, la competencia puede obtener ventaja sobre nosotros.

Las seguridad debe también concernir a individuales, ya que si se puede accesar sin nuestro consentimiento o nuestro sistema sea carente de seguros, el daño que se pueda ocasionar no solamente puede ser sobre el dueño del sistema sino también sobre aquellos individuos u objetos a quien nos referimos en los mensajes que estamos enviando.

Las razones para intentar violar nuestra seguridad son variadas y bien pueden ser de carácter político, competitivo, personal, militar, etc. La amenaza crece con la proliferación de redes de comunicación en el ámbito mundial. La concentración de información y actividades económicas, convierten a determinados lugares en blancos atractivos para entidades hostiles.

Mientras que la frágil seguridad que nos ofrece la mayoría de los servicios comunicadores disminuye, es necesario que se diseñen sistemas que nos den la privacidad requerida, los fabricantes y vendedores de equipos deben tomarlo más en consideración, ya que la falta de seguridad es más que suficiente para que comercialmente cualquier empresa note una baja alarmante en sus ventas. En Europa, actualmente, algunos gobiernos promueven la revisión de productos, diseños y estándares que integren confianza y seguridad.

Aunque algunas veces, organismos que evalúan, solo se basan en datos técnicos y comerciales, reconocen que hay un buen número de elementos legales asociados con la investigación y persecución de crímenes. Es importante hacer aproximaciones técnicas y no técnicas para saber como aumentar la confianza y seguridad de un sistema. Es conocido que el desarrollo de las legislaciones es rebasado por el crecimiento de la tecnología y los cambios sociales. Y aunque las leyes resultan efectivas para castigar la mayoría de los crímenes cometidos; en cuanto a lo que se pudiera llamar crímenes, sobre todo en el área de la computación o medios de comunicación, las sanciones o procedimientos para

aplicarlas no están bien estipuladas y en muchas ocasiones resultan ineficaces. Pero lo que si se considera como acto criminal es el atacar a los sistemas computacionales y de comunicaciones y se sanciona como cualquier otro delito. De cualquier forma no hay un consenso acerca de los usos que sean legítimos y socialmente aceptables. Muchísimas preguntas sobre este tema se han hecho en todas las áreas sociales y es causante de gran controversia, aún dentro de las comunidades de ingenieros.

La seguridad en sistemas de comunicación y su confiabilidad debe tener altas prioridades entre diseñadores, vendedores, administradores de sistemas, usuarios, educadores, gobiernos y público en general.

En tiempos de cambios lentos, la práctica prudente puede sugerir que es razonable esperar para evidencia explícita de amenaza antes de desarrollar una respuesta, pero en estos tiempos de cambios rápidos, daños significativos pueden ocurrir si uno espera a desarrollar una contramedida hasta después de que el ataque es manifestado.

Nuestro punto de vista es que por varias razones antes mencionadas, no podemos esperar que clase de ataques se puedan desarrollar en nuestra contra, o que accidente pueda suceder, debemos comenzar nuestra defensa y desarrollar un plan, basado en predicciones, para proporcionar una seguridad adecuada.

CAPÍTULO 2
CONVERSION DE SEÑALES

2.1. RESEÑA TÉCNICA DEL CONCEPTO DE RED DIGITAL.

La revolución de las Redes Públicas de Telecomunicaciones existentes, está basada en el desarrollo de la integración de las tecnologías digitales y analógicas. Esta integración que *en su primera etapa se* denomina RDI (RED DIGITAL INTEGRADA), lleva como base las siguientes premisas,

- INTEGRACIÓN DE EQUIPO DE TRANSMISIÓN ANALÓGICO Y DIGITAL
- INTEGRACIÓN DE COMUNICACIÓN DE VOZ Y DATOS.
- INTEGRACIÓN DE CONMUTACIÓN DE CIRCUITOS Y CONMUTACIÓN DE PAQUETES.

La filosofía digital de comunicaciones es la plataforma básica para cubrir las expectativas demandadas por el usuario, dado que las preguntas de éste se han transformado de un "¿se puede?" a un "¿cuanto? y ¿a que velocidad? Esta filosofía tiene su base en la conversión de señales continuas a discontinuas, es decir analógico/digital por lo que antes de entrar a cualquier tema de redes digitales y protocolos, sería necesario definir y comprender algunos conceptos. Así, a continuación se inicia un análisis de la digitalización de señales.

2.2. DISEÑO TÍPICO DE UN SISTEMA DIGITAL DE COMUNICACIONES

Primeramente definiremos a la señal binaria o mensaje binario como una secuencia de dos tipos de pulsos ó formas de onda conocidas que se presentan a intervalos regularmente espaciados en el tiempo:

Consideremos entonces como ejemplo un mensaje digital (o binario) aleatorio tal, que además sirva de referencia en varias partes de la presente sección.

Pese a que se conoce la forma de los pulsos, su ocurrencia, y la información transmitida, están dadas realmente por la secuencia particular de unos y ceros que llegan.

Podemos decir que la frecuencia de los pulsos es 1/R o sea a razón de R pulsos por segundo

R/S.

DONDE 1R=INTERVALO BINARIO

El transmisor es la fuente de señal que está generando R, dígitos binarios o bits por segundo la palabra bit proviene de binary digits, por ejemplo:

SI $1/R = 10^{-3}$seg. R ES ENTONCES 1000 bits seg.

SI 1/R= 1 MICROseg. ENTONCES $R = 10^{6}$ bits seg.

Si queremos transmitir la secuencia a un destino lejano tendremos que enfrentarnos con problemas del ruido y la interferencia, tal como se muestra en la figura 12 siguiente:

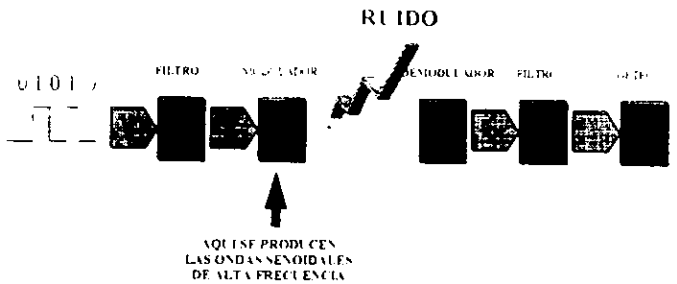


Fig. 12

Los filtros provocan que las señales transmitidas, en intervalos de tiempo, se traslapen en instantes de tiempo adyacentes. Esto se conoce como interferencia entre símbolos y causa errores.

Shannon descubrió (en el año 1948) que: *"La probabilidad de que ocurra un error puede idealmente reducirse tanto como se deseé por medio de una codificación adecuada de la señal de entrada"* siempre que la velocidad de señalización binaria R en bits por segundo sea menor que el número especificado, el cual se determina por medio de la potencia del transmisor. El ruido del canal y la respuesta de tiempo o ancho de banda del canal.

Si se intentan introducir demasiados bits por segundo en un mismo canal, la cantidad errores aumentará rápidamente. La máxima velocidad de transmisión de señales se conoce como capacidad de canal.

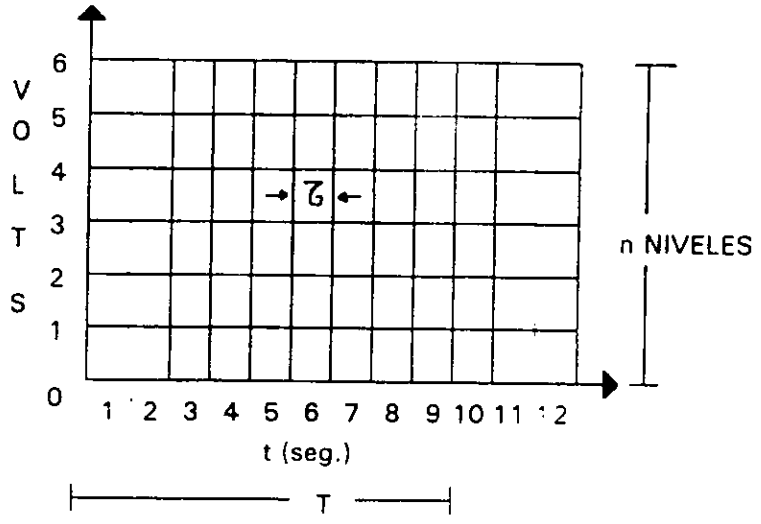
La capacidad de canal C estará en función de ancho de banda W y la cantidad de intervalos binarios T que intervienen en la transmisión, es decir:

$$C = W \log_2 T \ldots\ldots \quad (1)$$

donde W es el ancho de banda y T el número de intervalos,

Cuando la información es enviada deben tenerse señales que cambien con el tiempo, es decir, la transmisión de información está relacionada con las señales que se modifican con el tiempo y cuyo cambio es impredecible.

Supongamos un intervalo de T segundos en el cual se transmite información y una amplitud máxima de voltaje mismos que se muestran en la figura 13 siguiente.



T= 10 SEG

V= 3 VOLTS

DIAGRAMA DE VOLTAJE Y TIEMPO

Figura 13

Para que una señal cambie es necesario cambiar el nivel de la misma y esto tiene un límite de rapidez.

Por otra parte hay un nivel mínimo de umbral de voltaje que permite distinguir la señal del ruido.

Hay entonces un tiempo mínimo T que se requiere para que la energía cambie a una variación mínima detectable de amplitud.

Tomando en cuenta la figura anterior (figura 13), si T vale 1 segundo y si se considera que las variaciones son de */- 1 volt la mayor parte del tiempo (variación mínima detectable 1 volt), cuando la amplitud máxima de voltaje varía por ejemplo a 5 s. solo existen 6 niveles de voltaje detectables (contando el cero como valor).

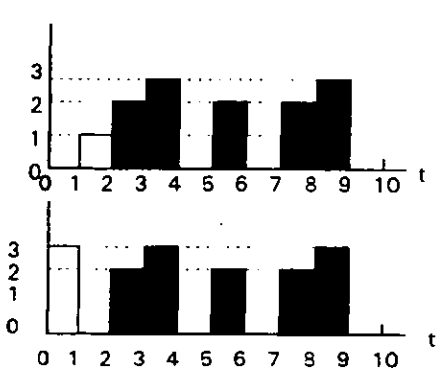
Así, por cantidad de información transmitida en T segundos, se entienden el número de combinaciones diferentes y distinguibles de amplitud de la señal, que pueden transmitirse al mismo tiempo.

Por tal motivo es evidente que la capacidad de información es limitada

Por lo tanto, la velocidad del sistema o capacidad máxima para transmitir información, está en términos de T y del número de niveles de amplitud distinguibles n.

De la figura 14, si se supone que la información transmitida en 10 segundos está relacionada con las diferentes combinaciones de amplitud y que se envían dos señales diferentes que son las mostradas en la figura 14:

Figura 14



Podremos observar en la figura 14, que estas señales son diferentes en los dos primeros intervalos de tiempo y coinciden en amplitud en los otros 8 (barras obscuras).

Existen 4 niveles de voltaje en cada uno de los dos intervalos diferentes, lo cual produce un total de 16 (dos intervalos de I segundo de 4 posibilidades c/u).

Así en 10 segundos hay 4^{10} combinaciones, es decir en forma general el número de combinaciones será:

$$\eta \quad \text{INTERVALOS (T) / DURACION DE CADA INTERVALO (T)} \ldots\ldots\ldots \quad (2)$$

para el caso anterior

n= 4 COMBINACIONES

T= 10 SEG

τ= I SEG

por lo tanto

$$\eta^{T/\tau} = 4^{10/1} = 1048576$$

Dado que la información debe ser proporcional al tiempo de transmisión, es decir, si ahora T=20, entonces se duplica el contenido de información del mensaje.

Para hacer esto proporcional se puede usar el logaritmo de n del modo siguiente:

Información transmitida en T segundos = (T/τ) (LOG n)

El factor de proporcionalidad dependerá de la base logarítmica empleada.

La base mas usada es 2, por lo que

$$INFO = T/\tau \ LOG_2 n \ldots\ldots (3)$$

La unidad definida con esta ecuación es el bit y se observa claramente su similitud con ecuación (1)

Así para el ejemplo anterior, el contenido de información de un intervalo de 10 segundos es:

$$10 \text{ SEG.}/1\text{SEG.} \ (LOG_2{}^4) = 20 \text{ BITS}$$

es decir, que la máxima cantidad de información enviable son 20 bits.

Si se hubieran tenido solo 2 niveles de voltaje posibles (0 y 1), la información contenida en 10 segundo, habría sido de 10 bits.

La capacidad del sistema puede definirse como la máxima velocidad de transmisión de información lo cual a partir de la ecuación anterior es:

$$C = \text{INFORMACION}/T = 1/\tau \ (LOG2n) \text{ en bits por segundo} \ldots\ldots\ldots (4)$$

Así, la capacidad de información es directamente proporcional al logaritmo de n e inversamente proporcional al mínimo intervalo de tiempo τ.

Estos dos parámetros de rendimiento del sistema. τ (ó su inverso, el ancho de banda) y n (o relación señal a ruido del sistema) son básicos en cualquier estudio de los sistemas de comunicación.

2.3. LAS SEÑALES ANALÓGICAS Y DIGITALES COMO MENSAJES

El mensaje es la forma mediante la cual podemos transmitir la información que se desee, los mensajes pueden ser digitales o iniciales, Los mensajes digitales se constituyen con un numero finito de símbolos. Por ejemplo, el lenguaje impreso consta de 28 letras , 10 números , un espacio y varios signos de puntuación . De esta manera , un texto es un mensaje digital de 50 símbolos. La voz humana es también un mensaje digital , ya que se construye con un vocabulario finito de un lenguaje esto sin tomar en cuenta los detalles, como son la pronunciación de las palabras, el énfasis, etc. si estos detalles fueran tomados en cuenta como cuando la señal que se produce en un micrófono esta señal seria analógica. De igual manera un mensaje telegráfico en código morse es un lenguaje digital construido con un conjunto de dos símbolos: raya y punto; es, por lo tanto un mensaje binario. Cuando un mensaje digital es constituido por M símbolos es llamado mensaje M-ario.

Los mensajes analógicos se caracteriza por tener datos cuyos valores varían en un rango continuo. Por ejemplo , la temperatura o la presión atmosférica de cierta localidad puede variar dentro de un rango continuo y puede tomar un número infinito de valores posibles. En forma similar , la forma de onda de un discurso contiene amplitudes que varían dentro de un rango continuo. En un intervalo de tiempo dado existe un número infinito de

las formas de onda de la voz en contraste con solo un numero finito de mensajes digitales posibles.

Los mensajes digitales se transmiten utilizando un conjunto finito de formas de onda eléctricas; por ejemplo, en el código morse, una raya puede transmitirse mediante un pulso eléctrico de amplitud A/2 , y un espacio puede transmitirse mediante un pulso de amplitud -A/2. En un caso M-ario, se utiliza M pulsos (o formas de ondas) eléctricos distintos; cada uno de los M pulsos representa a uno de los M símbolos posibles. La tarea del receptor consiste en obtener un mensaje de la señal distorsionada y afectada por el ruido a la salida del canal. La extracción del mensaje es por lo regular mas fácil en las señales digitales que en las señales analógicas , para entender esto supongamos que se codifican dos señales rectangulares de amplitudes A/2 y -A/2. La decisión en el receptor será la selección entre dos pulsos posibles a recibir, sin importar los detalles de la forma del pulso. Siendo así mas fácil la decisión , aun si los pulsos se distorsionan y se afectan por el ruido.

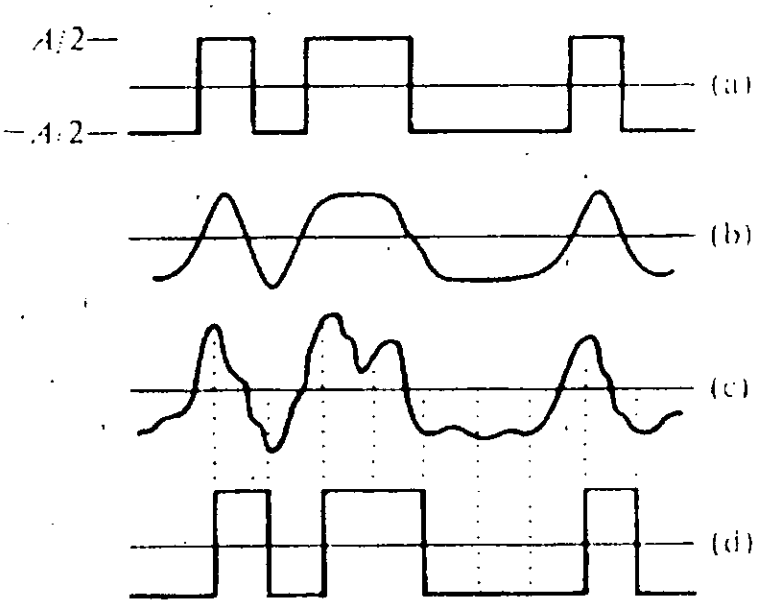


Figura 15

La posibilidad de utilizar repetidores regenerativos es una ventaja adicional para la comunicación digital. Una estación repetidora detecta los pulsos y transmite nuevos pulsos limpios, combatiendo de esta forma la acumulación de distorsiones y de ruido, permitiendo con esto la transmisión a mayor distancia y con más exactitud.

En contraste con los mensajes digitales, la forma de onda de los mensajes analógicos es importante y la mas leve distorsión en la forma de onda coaccionará un error en la señal recibida. Existe una dificultad adicional: un repetidor regenerativo no es visible para las señales analógicas, ya que las distorsiones y el ruido , por pequeños que sean no podrán ser eliminadas de una señal.

Como resultado, la distorsión y la interferencia son acumulativas através toda la trayectoria de transmisión. Para superar esta dificultad, la señal se atenúa constantemente a lo largo del trayecto de transmisión; entonces, con el aumento de la distancia la señal se hace más débil mientras que la distorsión y el ruido se hacen cada vez más fuertes. Finalmente, la señal, denominada por la distorsión y el ruido, queda mutilada.

La amplificación es de escasa ayuda, ya que acentúa la señal y el ruido en la misma proporción. En consecuencia , la distancia através de la cual se puede transmitir un mensaje analógico es limitada por la potencia del transmisor. No obstante la comunicación analógica está ampliamente utilizada a pesar de estos problemas. Cabe señalar que existe una tendencia a reemplazar a los sistemas analógicos por sistemas digitales ya que estos han venido a ser mas económicos debido a una dramática reducción de costos lograda en la fabricación de los circuitos digitales.

2.4. LA DIGITALIZACIÓN

La primera pregunta que surge es, ¿Por que digitalizar una señal si las señales analógicas en algunos servicios también analógicos (como la voz) operaban correctamente y con mucho menor ancho de banda?

Las ventajas básicas de la digitalización son:

I.- Las señales pueden regenerarse ó rearreglarse periódicamente durante la transmisión, puesto que la información ya no se encuentra contenida en la amplitud continuamente variable de pulsos, si no que consiste en símbolos discretos

Si bien la señal analógica logra transmitir la información, a mayor cantidad de repetidores mayor cantidad de ruido se adhiere a la misma. Además el concepto de repetidor se viene a sustituir con el advenimiento de las tecnologías digitales, por el de regenerador, permitiéndose con este último la reconstrucción fiel en cada punto, de la señal originalmente transmitida y manteniendo un control del ruido. Esto se debe a lo siguiente:

a) El proceso de digitalización de señales se conoce como cuantificación, la cual consiste en la subdivisión de amplitudes en un número discreto de niveles de amplitud.

b) Las señales resultantes se denominan cuantizadas.

c) Al contrario del proceso de muestreo (previo a la cuantización), este resultado produce una pérdida irregular de la información, debido a que es imposible reconstruir la señal analógica original a partir de su versión cuantizada. Esto puede resultar ventajoso, ya que si se conoce la pérdida originada en el transmisor, también es posible conocer la cantidad de ruido que se deberá compensar en la sección receptora.

2.- Toda clase de circuitos digitales pueden emplearse a lo largo del proceso disminuyendo entre otras cosas, el consumo de potencia.

3.- El ruido y la interferencia se minimizan mediante códigos.

2.5. CONVERSIÓN ANALÓGICA-DIGITAL DE SEÑALES (A/D)

Es posible que las señales analógicas y digitales se encuentren en un punto, este punto sería su conversión de señales analógicas a señales digitales. Esto es sumamente importante para el encriptamiento de la voz, puesto que es mucho mas fácil la manipulación de la señal digital que la manipulación de la señal analógica. El espectro de frecuencia de una señal indica las magnitudes relativas de las diferentes componentes de la frecuencia. El teorema de muestreo establece que si la magnitud más alta del espectro de la señal es B (en Hz.), la señal se puede reconstruir apartir de sus muestras, tomadas a una razón no menor que $2B$ muestras/segundo. Esto significa que para transmitir la información dentro de una señal continua, se necesita solamente transmitir sus muestras (fig 16).

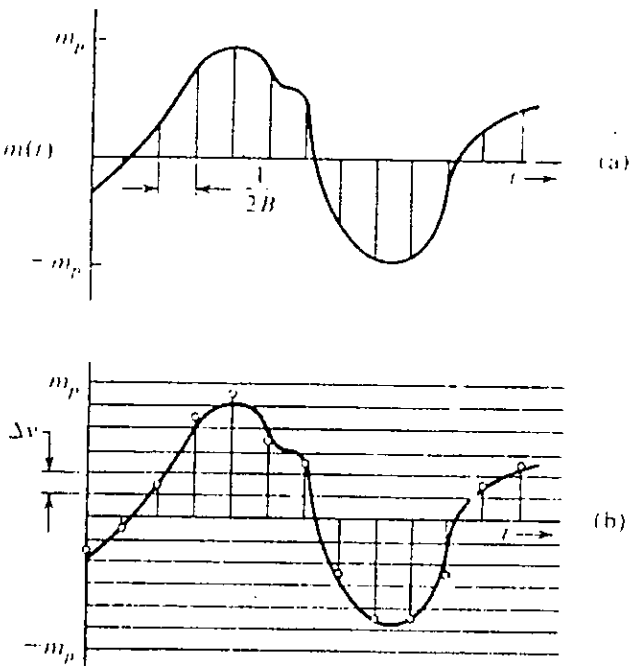


Figura 16

Desafortunadamente, los valores de las muestras no son todavía digitales ya que se encuentran dentro de un rango continuo y pueden tomar uno cualquiera del numero infinito de valores del rango. Esta dificultad se puede resolver mediante lo que es llamado como cuantificación, esto es , cada muestra se aproxima o redondea, al nivel cuantificado más próximo (fig 16). Las amplitudes de la señal m(t) están dentro del rango (-mp, mp), que se subdivide en L intervalos, cada uno de magnitud $\Delta v = 2mp/L$. La magnitud de cada muestra se aproxima al punto medio del intervalo en el cual cae el valor de la muestra. Cada muestra se aproxima ahora a uno de los L números, quedando así la información digitalizada.

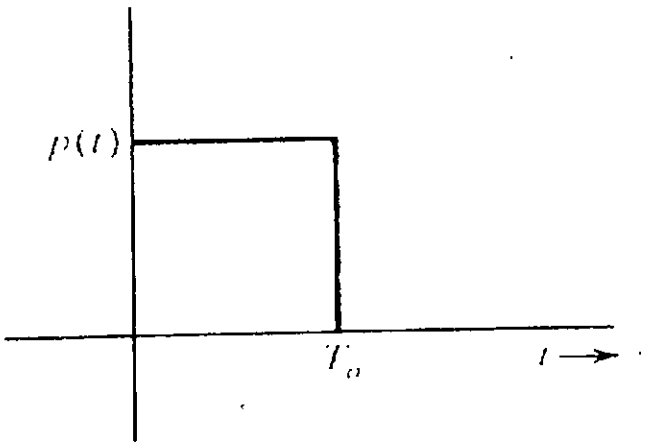
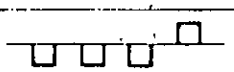
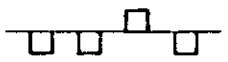
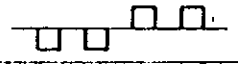
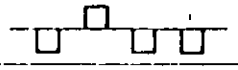
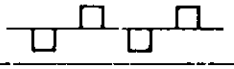
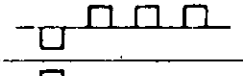
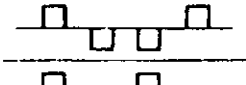
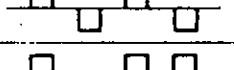
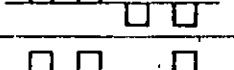


Figura 17

La señal cuantificada es una aproximación de la señal original. Se puede mejorar la exactitud de la señal cuantificada a cualquier grado que se desee aumentando el número de niveles L . Para la inteligibilidad de las señales de voz, por ejemplo, L=8 ó L=16 será suficiente. Para uso comercial, L=32 es un mínimo, y para comunicación telefónica se usa comúnmente L=128 o L=256.

Durante cada intervalo de muestreo To, se transmite una muestra cuantificada, la cual toma uno de los L valores. Esto requiere L distintas formas de onda, cada una de duración To . Se pueden construir éstas, por ejemplo, utilizando un pulso básico rectangular de amplitud A/2 (fig. 17) y sus múltiplos para formar L distintas formas de onda que se asignarán a los L valores que se van a transmitir. Las amplitudes de dos cualesquiera de estas formas de onda son separadas cuando menos en A para protección contra interferencia debida al ruido y la distorsión del canal. Otra posibilidad es utilizar menos de L formas de onda y formar sus combinaciones (códigos) para producir L patrones distintos. Para poner un ejemplo , en el caso de L=16 se pueden utilizar 16 pulsos, ±(A/2), ±(3A/2)... ±(15A/2), cada uno de duración To . La segunda alternativa es utilizar

solamente dos pulsos básicos A/2 y -A/2. Cada uno de To/4. Una de cuatro de estos pulsos da 2x2x2x2 = 16 patrones distintos (fig.16). Se puede asignar un patrón a cada uno de los 16 valores cuantidicados que se transmitirán. Cada muestra cuantificada se codifica ahora en una sucesión de cuatro pulsos binarios. Este caso es una codificación binaria, en el cual la señalización se lleva a cabo por medio de sólo dos pulsos (o símbolos) básicos.

Dígito	Equivalente binario	Forma de onda del código de pulso
0	0000	
1	0001	
2	0010	
3	0011	
4	0100	
5	0101	
6	0110	
7	0111	
8	1000	
9	1001	
10	1010	
11	1011	
12	1100	
13	1101	
14	1110	
15	1111	

Este tipo de codificación es de suma importancia para nuestro trabajo , ya que su detección es fácil y simple por constar solo de dos estados (1 y 0), además de que hoy en día toda la comunicación digital es binaria.

Físicamente existen muchos métodos de producir un convertidor Analógico Digital. Una forma de producir dicho convertidor es incrementar un contador, que alimenta a un convertidor Digital Analógico, (el cual se verá más adelante) y parar el contador cuando la salida del convertidor digital analógico exceda la tensión analógica en cuestión (fig.18). La salida del convertidor digital analógico es una función escalera. Que se puede pensar como una serie de funciones rampa discretas. El número de pasos antes de que la rampa cruce el valor analógico es proporcional a ese valor. La palabra de salida digital es la salida del contador. Un contador de 8 bits comienza desde cero para cada medida.

Otro método de generar una palabra digital a partir de una tensión analógica es utilizar aproximaciones sucesivas. Si se asignan números binarios a diferentes niveles de tensión iniciando con el más bajo (todos ceros), y contando hacia el mayor (todos unos), se pueden utilizar las propiedades básicas de las secuencias binarias para simplificar la conversión. El bit más significativo en el numero binario indica si la tensión se encuentra en la mitad inferior o superior del intervalo. El siguiente bit subdivide este intervalo a la mitad, y así sucesivamente. Esto equivale a la observación de que en un contador binario, cada bit oscila a la mitad de la frecuencia del bit anterior. La conversión se lleva acabo mediante una serie de comparaciones con los puntos de división regional.

Un ejemplo específico de este tipo de convertidor analógico-digital es el circuito integrado ADC0801, que contiene un comparador de alta impedancia de entrada, 256 resistores en serie y conmutadores analógicos, lógica de control y memorias de paso en la salida. La conversión se realiza utilizando la técnica de aproximación sucesiva, donde la

tensión analógica desconocida se compara con la tensión en los puntos de unión de los resistores utilizando conmutadores analógicos. Cuando la tensión apropiada en el punto de unión coincide con la tensión desconocida, la conversión está completa. Las salidas digitales contienen una palabra binaria complementaria de 8 bits que corresponde a la tensión de salida.

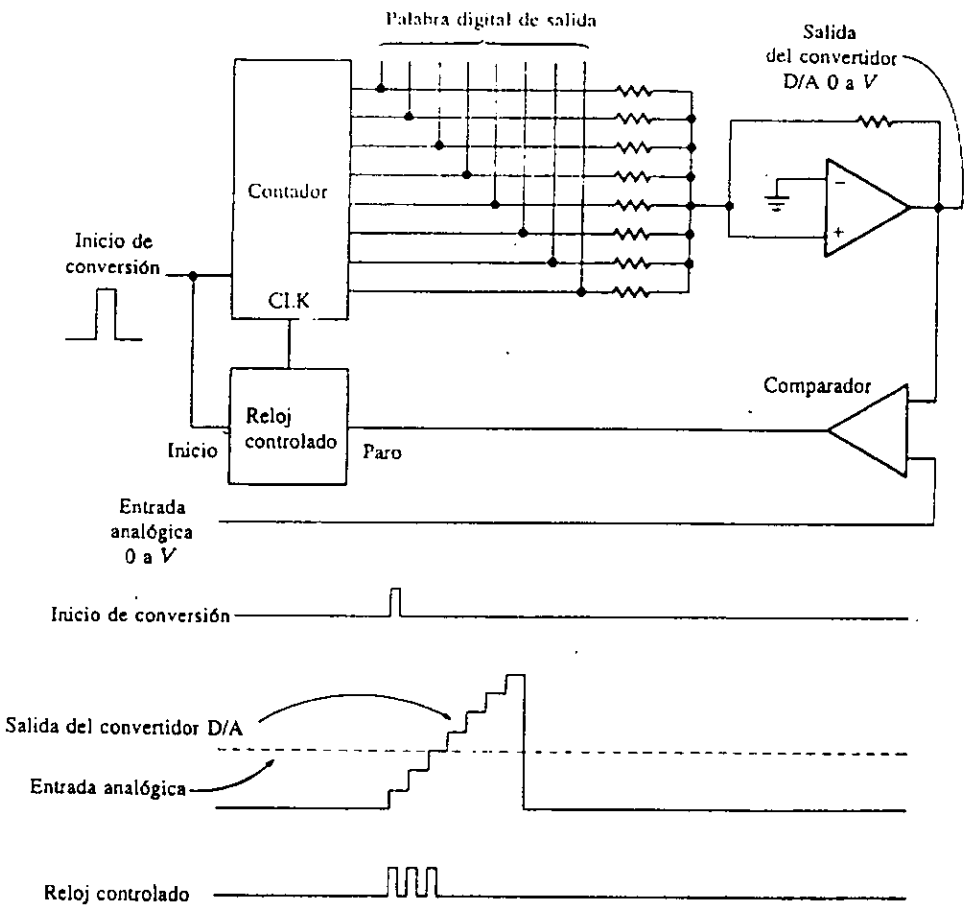


figura 18

2.6. CONVERSIÓN ANALÓGICA A DIGITAL: APLICACIÓN A LA MODULACIÓN POR CODIFICACIÓN DE PULSOS.

Como se mencionó con anterioridad, el proceso de digitalización de las señales originalmente analógicas se conoce como digitalización y las señales que resultan se llaman cuantizadas.

En un sistema específico, los pulsos muestreados deben cuantizarse. El proceso de muestreo implica definir los niveles de voltaje en niveles predeterminados y medibles.
Para ejemplificar esto, en primera instancia utilizaremos la figura siguiente,

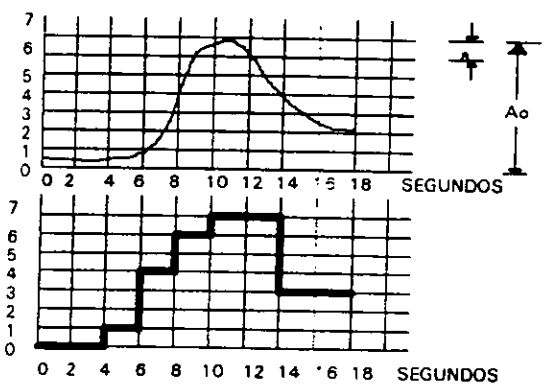


figura 19

La variación total de amplitud $A_o = 7$, se divide en los niveles de amplitud igualmente espaciados $a = 1$, existen así $M = Ao\ a + 1$ posibles niveles de amplitud incluyendo el nivel cero.

Aunque la separación entre niveles de amplitud en la figura 19 es uniforme, normalmente dicha separación es no uniforme con objeto de mejorar el comportamiento del sistema al ruido.

En general el espaciamento entre niveles se hace disminuir con los niveles bajos de amplitud esto se realiza por medio de una técnica conocida como compresión.

El ruido de cuantización se disminuye obviamente disminuyendo los niveles en separación ó aumentando M.

De acuerdo a los experimentos, con 8 y 16 niveles la voz es totalmente inteligible.

2.7. COMPRESIÓN

Una vez que la señal muestreada ha sido cuantificada en un número de intervalos, éste debe ser traducido ó trasladado a un set de bits.

El circuito que convierte ó traduce la señal cuantificada se llama codificador. el circuito que realiza la operación inversa es llamado decodificador.

La combinación de ambos es llamada codec.

La forma mas sencilla de codificar es producir una salida que sea lineal con respecto a la entrada, es decir si se recibe un I decimal, se produce una salida de 001.

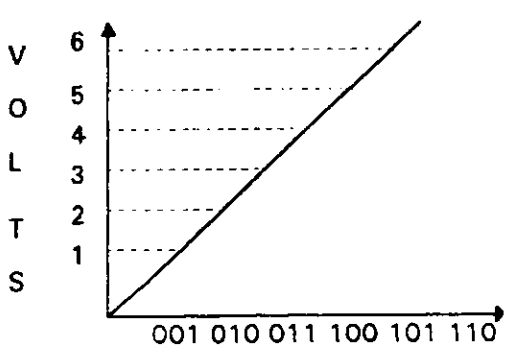


Figura 20

Las salidas de un codificador dependen del número de intervalos de cuantificación. El número de intervalos avanza por potencias de dos al ser añadidos bits en el código como se muestra en la tabla siguiente

NUMERO DE BITS EN EL CODIGO	NUMERO DE INTERVALOS
1	2
2	4
3	8
4	16
5	32
6	64
7	128
8	256

Es necesario cuantificar ambas polaridades, positiva y negativa de la señal, por lo que uno de los bits del código debe ser utilizado para identificar la polaridad.

Por lo anterior el número de bits es reducido por potencias de 2, es decir, un número de 8 bits proveerá 128 intervalos, más un bit de signo.

En general el número de bits en el código para un número de intervalos requeridos es

$n = LOG_2 (2 \times N)$..... (8)

donde n es el número de bits y N el número de intervalos.

N es multiplicado por 2 para ganar el bit extra de señalización, por ejemplo si tenemos 64 intervalos:

$$n = LOG_2(2X64) = 7 \text{ BITS}$$

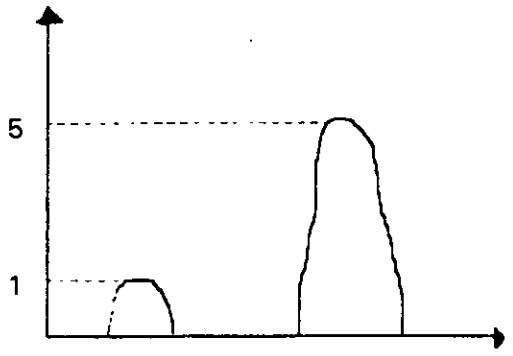
Es decir, se requieren 7 bits para representar 64 intervalos de muestreo.

Adicionalmente, uno de los parámetros fundamentales de la cuantificación es la razón señal a ruido.

Para un sistema lineal, la relación señal a ruido es la amplitud de la señal de entrada a 0.25 de la amplitud del intervalo de cuantificación.

Este valor es determinado estadísticamente, asumiendo que en un período largo de tiempo la entrada de la muestra cuantificada tienen niveles de distribución uniforme dentro de un período particular, esto significa que la relación señal a ruido aumenta con el incremento en la amplitud de la señal, por lo que las señales de mayor amplitud tendrán una mejor s/n.

La siguiente figura muestra como una señal de pequeña amplitud (1) tiene una razón de 4, mientras que una de amplitud 5 tiene una razón de 20.



$$S/N = \frac{\text{NIVEL DE SEÑAL CUANTIFICADA}}{0.25}$$

$S/N = 1/0.25 = 4$ Y $S/N = 5/0.25 = 2$

figura 21

Se ve obvio que esta condición no es adecuada, puesto que las señales pequeñas ocurren con mayor frecuencia que las grandes en una comunicación telefónica La manera de solucionar lo anterior es ajustar el tamaño de los intervalos de cuantificación, de tal forma que cuando ocurran señales de gran amplitud existan intervalos grandes y en las de pequeña amplitud intervalos pequeños.

Esto nos da una relación entrada salida no-lineal como resultado de la compresión de salida con respecto a la entrada.

Idealmente, la curva característica de un cuantificador no lineal, debe ser 1 /X.

SALIDA/ENTRADA= dY/dX= 1 /kX siendo K una constante.

INTEGRA-N-DO

$$Y = 1/K \int 1/X \, dX = 1/K \, Ln\,(X \text{ -.....(9)}$$

Su gráfica aparece en la siguiente figura, en la cual por cierto se puede apreciar que la curva no pasa por el origen dando así la simetría positiva.

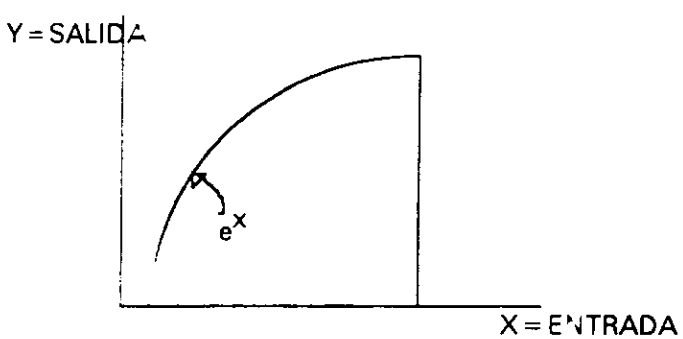


figura 22

2.8. LEYES DE COMPRESIÓN

Para los requerimientos de conversión analógica a digital y compresión, dos leyes matemáticas han sido aceptadas, la ley μ y la ley A.

2.8.1. Ley μ

La ley μ utilizada en E.U.A. y JAPÓN entre otros Logra simetría cambiando el origen hacia la curva característica.

Los circuitos de ley μ operan a 255 de compresión-expansión usando la siguiente relación

$$F\mu(X)=SGN(X)\ Ln\ (1+\mu/X)/(Ln\ (1-\mu)) \quad (10)$$

Donde X= a la señal de entrada normalizada (entre +1 y +1)

SGN= al signo que tome X

μ=255 para EUA y JAPON

$F\mu$ (X) es el valor de compresión de la señal de salida.

El codificador produce una salida de 8 bits. De las señales, 7 son para la magnitud más uno para el signo (1 = + y 0= -).

Así mismo la velocidad de transmisión de datos para un canal es de 64 kbps.

Utilizando la técnica PCM se muestrean y cuantizan las señales para dar a los 256 posibles valores obtenidos de los citados procesos y referidos en la tabla I la forma apropiada para transmitirlos, lo cual se logra mediante los pulsos binarios.

Ocho de tales pulsos son suficientes para formar un código único para cada valor de los intervalos ($2^8 = 256$).

Estos intervalos son la representación del proceso de modulación por codificación de pulsos (PCM) lo cual da como resultado un código binario de 8 bits, conocido como una palabra PCM.

Una palabra PCM corresponde a una muestra y como la velocidad de muestreo es de 8000 htz (teorema de Nyquist), entonces se obtienen 8000 palabras PCM por segundo, por lo que para cada conversación la velocidad de transferencia de bits en un enlace digital, es de 8x8000=64000 bits/seg. (este valor se conoce como canal B).

A continuación se muestra la gráfica de compresión de la Ley μ. Es conveniente hacer énfasis en la cantidad de segmentos y niveles que pueden manejarse para ubicar de manera rápida la diferencia entre esta Ley μ y la Ley A que se explica más adelante.

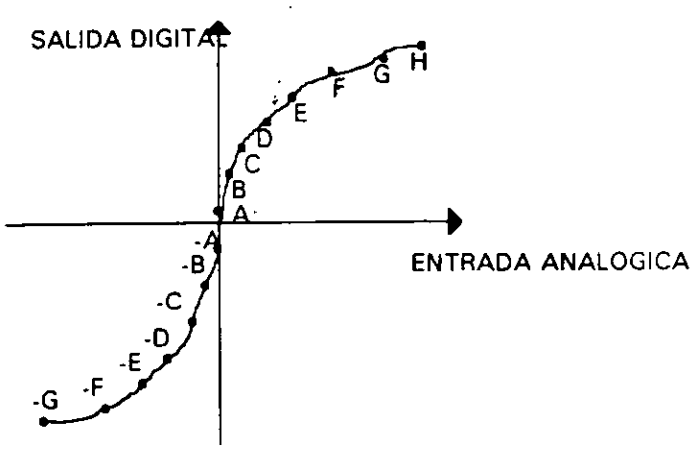


Figura 23: Curva de compresión con Ley μ

Tabla 2

VALORES DE DECISION	SEGMENTO	CODIGO DE 8 DIGITOS							
		1	2	3	4	5	6	7	8
		POLARIDAD	DESCRIPCION DE AMPLITUD						
		1=+ 0=-	SEGMENTO			16 POSIBLES VALORES DE AMPLITUD			
112-127	G-H	1	1	1	1	W	X	Y	Z
96-111	F-G	1	1	1	0	W	X	Y	Z
80-95	E-F	1	1	0	1	W	X	Y	Z
64-79	D-E	1	1	0	0	W	X	Y	Z
48-63	C-D	1	0	1	1	W	X	Y	Z
32-47	B-C	1	0	1	0	W	X	Y	Z
16-31	A-B	1	0	0	1	W	X	Y	Z
0-15	0-A	1	0	0	0	W	X	Y	Z

NOTA: Para la sección de polaridad negativa está excluido el valor 00000000.

2.8.2. LA LEY A.

La ley A. utiliza una pendiente lineal para interpolar el origen y la ley logarítmica. Su ecuación característica es:

$$Fx = SGNx\ A/x/(1+LnA) \quad \ldots\ldots (11)$$

Cuando x tiene un rango entre 0 y 1/A

para valores de 1/A hasta 1

$$Fx = SGNx\ (1+LnA/x)/(1+LnA) \quad \ldots\ldots (12)$$

Donde A=87.6 de compresión para las redes europeas,

La velocidad de transmisión por canal sigue siendo 64Kbps.

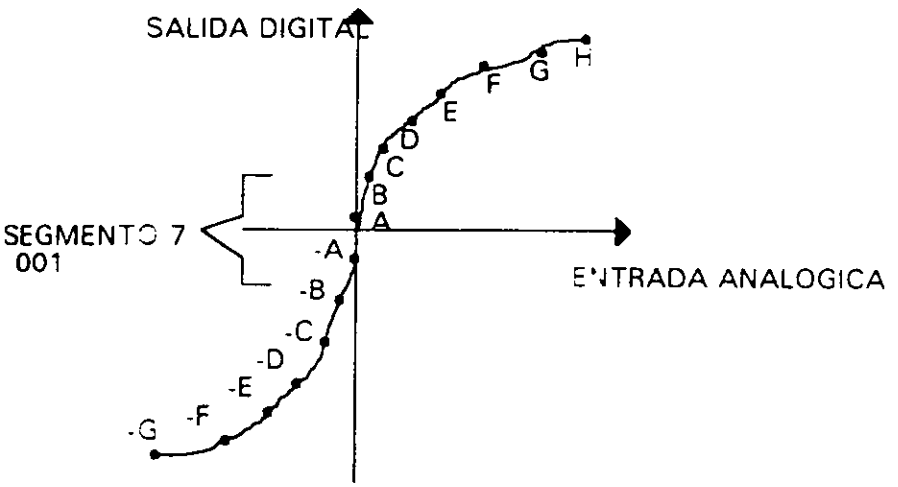


Figura 24: Curva de compresión con Ley μ

Tabla 3.

VALORES DE DECISION	SEGMENTO	CODIGO DE 8 DIGITOS							
		1	2	3	4	5	6	7	8
		POLARIDAD	DESCRIPCION DE AMPLITUD						
		1=+ 0=-	SEGMENTO			16 POSIBLES VALORES DE AMPLITUD			
112-127	G-H	1	1	1	1	W	X	Y	Z
96-111	F-G	1	1	1	0	W	X	Y	Z
80-95	E-F	1	1	0	1	W	X	Y	Z
64-79	D-E	1	1	0	0	W	X	Y	Z
48-63	C-D	1	0	1	1	W	X	Y	Z
32-47	B-C	1	0	1	0	W	X	Y	Z
16-31	SEGMENTO 7	1	0	0	1	W	X	Y	Z
0-15		1	0	0	0	W	X	Y	Z

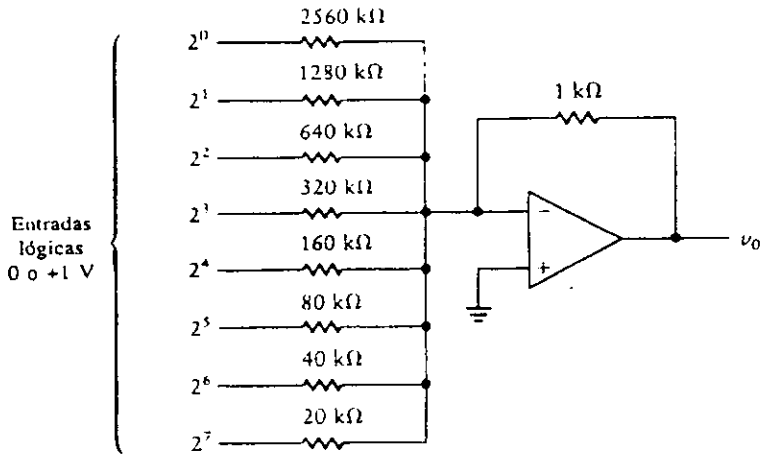
2.9. CONVERSIÓN DIGITAL ANALÓGICA DE SEÑALES (D/A)

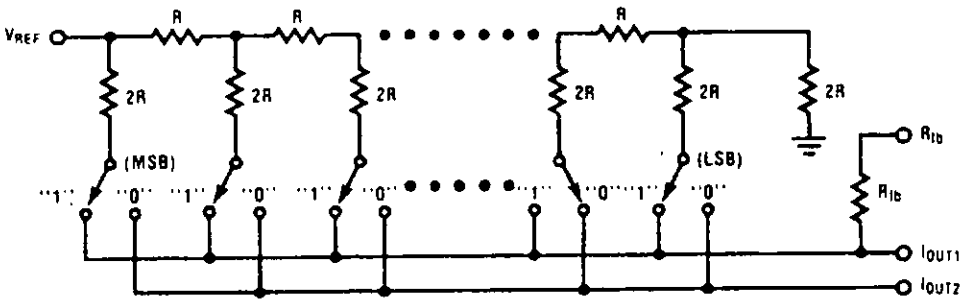
Los convertidores de señales digitales a señales analógicas transforman una palabra digital en una tensión o corriente analógica. Se utilizan varias técnicas para conseguir esto. En este apartado se mostraran solo dos de estos métodos.

La magnitud de la salida del convertidor digital-analógico es en general proporcional o inversamente proporcional a la corriente que fluye através de resistores ponderados. En la figura 25(a) se muestra un convertidor digital-analógico de 8 bits con un amplificador operacional como convertidor de corriente a tensión. Cada una de las entradas están ponderadas de acuerdo con los resistores de suma de la entrada de tal forma que se obtenga la potencia de 2 apropiada. Una señal analógica de 8 bits en la entrada proporciona una salida analógica.

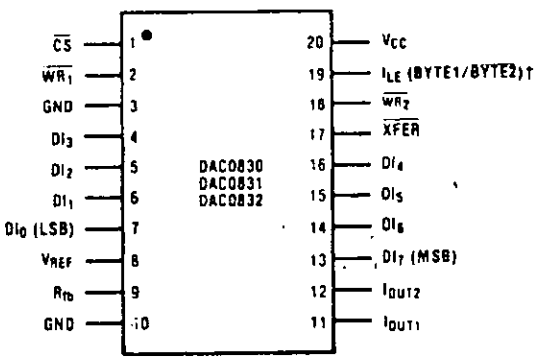
Otro método se basa en la utilización de un conmutador CMOS para cambiar los resistores en una red escalera de resistencias, como se muestra en la figura 25(b). Este método se denomina escalera de conmutación de corriente R-2R y utiliza una serie de resistores de silicato de cromo depositado. Estos resistores , de valor R o 2R, están acomodados en forma de escalera como en la figura . El código de entrada digital aplicado en la entrada del convertidor D/A controla la posición de los conmutadores de corriente. De esta forma, la corriente disponible en la escalera se dirige a I_{SAL1} o I_{SAL2}, de acuerdo con lo determinado por el nivel lógico (0 ó 1 respectivamente). Los conmutadores CMOS son bilaterales, de modo que se pueden conmutar corrientes de cualquier polaridad con sólo una pequeña caída de tensión.

El diagrama de terminales para el convertidor digital analógico de 8 bits, el DAC0830, se muestra en la figura 25. Utilizando la red escalera R-2R, este convertidor D/A produce un 0.05% de error máximo lineal a escala completa. El tiempo típico del convertidor es de 1 μs , y con una entrada de 8 bits este circuito es capaz de generar 256 distintos niveles de corriente de salida. La resolución es de 8 bits.


2560 kΩ
1280 kΩ
640 kΩ
320 kΩ
160 kΩ
80 kΩ
40 kΩ
20 kΩ
1 kΩ
Entradas lógicas 0 o +1 V
v_o


V_{REF}
R
2R
(MSB)
(LSB)
R_{fb}
I_{OUT1}
I_{OUT2}

(a)


$\overline{CS}$
$\overline{WR_1}$
GND
DI_3
DI_2
DI_1
DI_0 (LSB)
V_{REF}
R_{fb}
GND
DAC0830
DAC0831
DAC0832
V_{CC}
I_{LE} (BYTE1/BYTE2)†
$\overline{WR_2}$
$\overline{XFER}$
DI_4
DI_5
DI_6
DI_7 (MSB)
I_{OUT2}
I_{OUT1}

(b)

figura 25

CAPÍTULO 3.

CRIPTOGRAFÍA.

3.1 HISTORIA

Etimológicamente la palabra criptografía es: Kriptos (oculto) y Graphos (escribir).

De los significados más comúnmente aceptados para la palabra "criptografía" en los diccionarios enciclopédicos consultados, se han escogido los de "arte de enviar mensajes en clave secreta " y "escritura secreta realizada mediante clave, de manera que sea imprescindible conocer ésta para descifrarla". Otro término relacionado con el anterior es "criptograma", que el diccionario de la Real Academia de la Lengua define como "documento cifrado". Continuando con el análisis de los términos empleados en las definiciones expuestas, la palabra "cifrar" significa "escribir en cifra", atribuyendo a "cifra" el significado de "escritura secreta". En algunos textos consultados la palabra "criptología" es sinónimo de "criptografía".

La criptografía o ciencia criptográfica estudia los procesos de cifrado y descifrado de los mensajes, así como el análisis de los criptogramas para descubrir la clave y texto original. Este último aspecto de la ciencia criptográfica recibe el nombre de criptoanálisis.

La información es algo consustancial en el hombre, incluso puede afirmarse que lo es respecto a la vida misma en todas sus manifestaciones. La comunicación de información es absolutamente necesaria para el desarrollo de la actividad humana.

En los entornos de la actividad humana, la comunicación de información a veces se realiza de forma selectiva, es decir, se efectúa una transmisión de información que

únicamente debe ser recibida por determinados elementos receptores. Esto ocurre cuando la información tiene un carácter privado, restringido o secreto. Esta selectividad en la comunicación de la información debe tener sus orígenes comunes con las formas más elementales de la sociedad, al aparecer intereses que defender o proteger.

Cuando las situaciones en que la información debe ser recibida por elementos seleccionados son numerosas, o bien cuando la información a transmitir respalda intereses de gran valor, se hace necesario disponer de algún procedimiento que asegure el carácter privado y secreto de lo que se comunica.

Los sistemas más elementales e inicialmente utilizados en éstas ocasiones fueron , con toda probabilidad, algo parecido a lo que hoy llamamos valija diplomática, es decir, un recipiente enviado por algún mensajero hacia el elemento receptor. La posibilidad de vulnerar éste método de comunicación de información es alta. Sólo se necesita capturar al mensajero y obtener fácilmente la información que se transporta. La evolución de éste rudimentario y elemental procedimiento de comunicación secreta fue la de ocultar información, cambiando los símbolos del mensaje, para que en caso de ser capturado el mensajero, no fuera posible develar su secreto. Este simple pero ingenioso paso hacia adelante requirió una cierta organización, ya que el elemento receptor debía conocer previamente el significado atribuido a los símbolos que componían el mensaje.

3.2 NECESIDAD DE ENCRIPTAR

El usuario o responsable de un sistema informático, está sujeto a una serie de aspectos críticos que pueden afectar gravemente a la seguridad de la información que es procesada automáticamente en su ordenador . Como puntos principales aparecen los relativos a los dispositivos de almacenamiento y a los medios de transmisión de información a través de líneas telefónicas de cualquier naturaleza. Respecto a los primeros, el robo del dispositivo, sea disco, cinta, disquete o cualquier otro soporte, no es solamente el principal peligro que afecta la seguridad, sino el acceso indebido por parte de personas no autorizadas, que en un centro de informática pueden tener al alcance de la mano el soporte en cuestión. Respecto a los segundos, los enlaces telefónicos pueden ser intervenidos, o ser accidentalmente "escuchados", introduciendo así otro factor de inseguridad, ya que además, no están bajo el control del utilizador.

Por otro lado , el impulso que los avances tecnológicos han prestado a la informática durante los últimos años con la consiguiente disminución de los precios de los componentes, han conducido a una situación caracterizada por un continuado incremento de la utilización del ordenador en nuevos campos y aplicaciones.

La extensión de la informática no ha incrementado únicamente los usos, sino también los usuarios, siendo muy frecuente el acceso a un mismo ordenador de usuarios diferentes que son potenciales vulneradores y/o víctimas de vulneración, de información confidencial o secreta.

Las claves que se han venido dando son de fácil violación, como lo son: claves de acceso a ficheros, ficheros sólo escritura, lista de usuarios permitidos, etc.

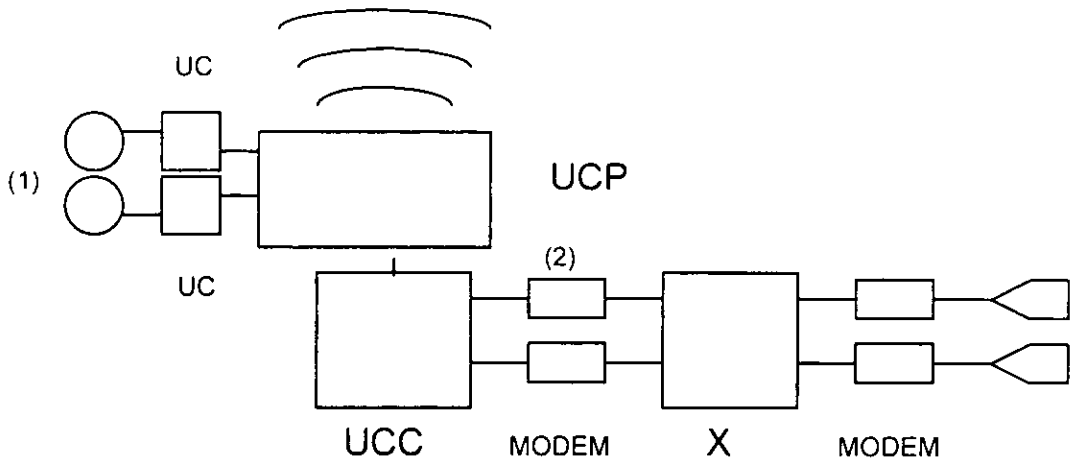


figura 26

UC = Unidad de Control
UCC = Unidad de Control de Comunicaciones
X = Central de Teléfonos, Caja de distribución (sin control de usuario)

Puntos Vulnerables: (1) = Robo, acceso no permitido
(2) = Intervención de líneas
- Robo de información
- Corrupción de información
- Destrucción de información
- Obtención de palabras clave
- Obtención de comandos de uso del sistema

La aplicación de técnicas criptográficas es la solución universalmente aceptada para evitar los actos que pueden vulnerar la información.

3.3 ESTRUCTURA DE UN SISTEMA SECRETO.

La protección de la información en un sistema automático de tratamiento de la información se aplica mediante técnicas criptográficas, tanto a los datos almacenados en soporte, discos, etc., como a la información transmitida a través de algún canal de comunicación. De esta forma, un acceso indebido a los soportes, o una escucha realizada interceptando un canal de comunicación presentará información en forma de criptogramas, resultando incomprensibles al que no posea al resto de la información necesaria para su descifrado.

El esquema de funcionamiento de un sistema secreto es idéntico, tanto si se trata de un sistema de comunicación , como si es un sistema de almacenamiento. En un sistema secreto hay dos funciones elementales que intervienen, que se denominan función o proceso de cifrado, y función o proceso de descifrado. Las funciones de cifrado o descifrado se suponen conocidas por el oponente (hipotético escucha o ladrón de información). Si el sistema fuera dependiente únicamente de las funciones de cifrado y descifrado (E y D, de aquí en adelante), el oponente tendría suficiente información para vulnerar el sistema, por tanto es preciso la existencia de algo que siendo desconocido impida al oponente obtener la información. Ese algo es la clave, necesaria para descifrar el mensaje.

La función de cifrado E, es tal que combina de alguna manera el mensaje original, o mensaje en claro, con la clave K, para obtener el mensaje cifrado o criptograma . Consecuentemente, la función de descifrado D, combina el mensaje cifrado o criptograma, con la clave K para obtener el mensaje original o mensaje en claro.

De este funcionamiento se deducen dos cosas al menos: la primera, es que las funciones E y D provocan unas transformaciones en los mensajes, que son inversas una de

otra. La segunda, que la clave empleada en la función de descifrado, debe ser la misma que fue empleada en la función de cifrado, por tanto, pensando en un sistema secreto donde hay un emisor y un receptor, éste debe poseerla, habiéndola recibido mediante algún sistema no interceptable.

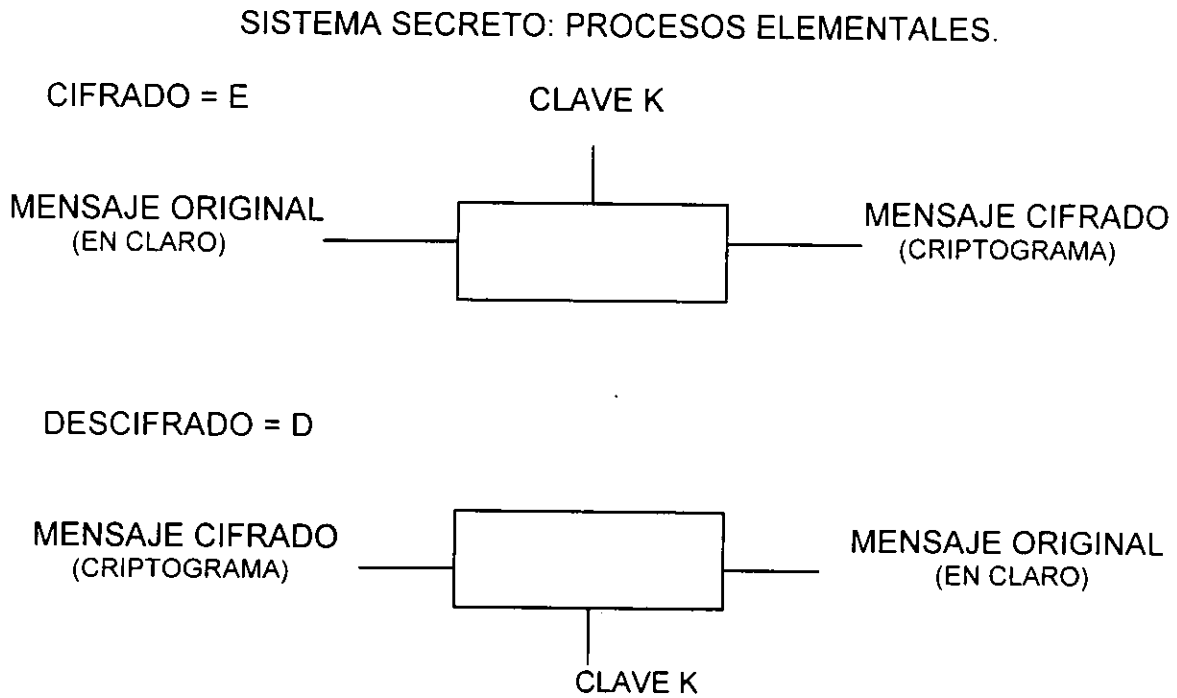


figura 27

Por lo tanto, siendo M el mensaje original y K la clave, el mensaje cifrado C, será:

$$C = (M,K)$$

que expresado en forma de aplicación es:

$$(M \times K) - C$$

donde se ha designado a M como el espacio de mensajes originales, a K como el espacio de claves, y a M X K el espacio de todas las inyecciones M X K.

Análogamente, designando a D como función de descifrado:

$$M = D\,(C,K) = D\,(E(M,K),K)$$

que expresado en forma de aplicación es:

$$((M \times K) \times K) - M$$

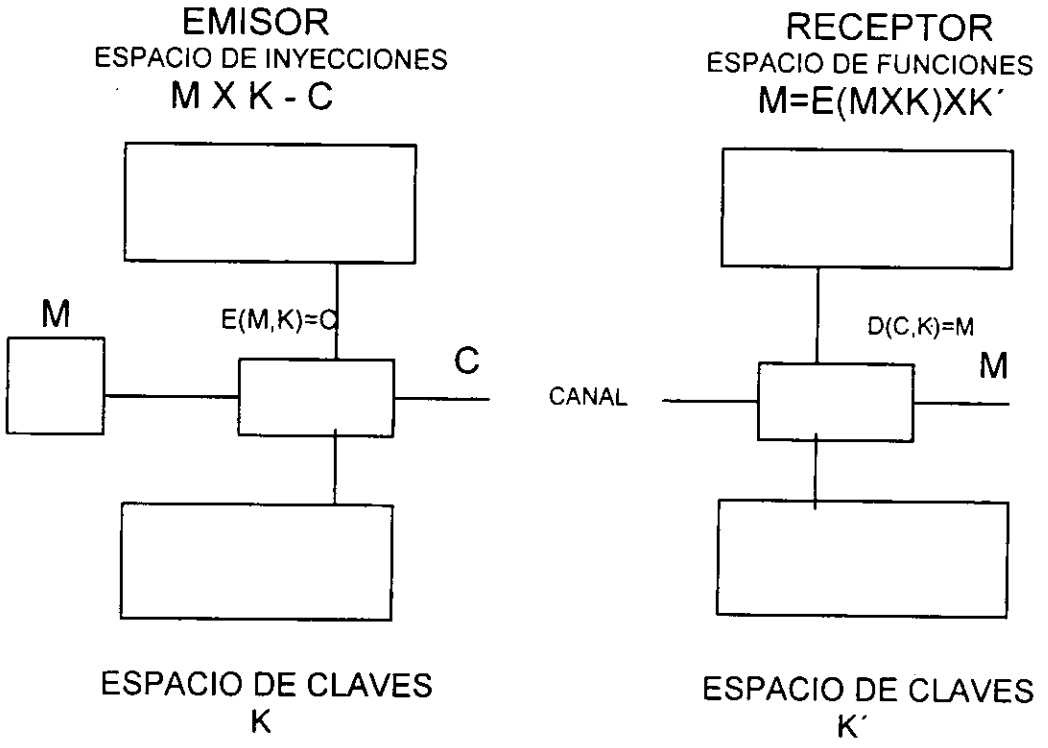


Figura 28

El parámetro que selecciona una transformación concreta se llama clave, siendo el sistema criptográfico un conjunto de instrucciones, un dispositivo electrónico, o un

programa de ordenador que es capaz de cifrar o descifrar en un amplia gama de modos, uno de los cuales es la clave escogida.

Por convenio se considera al sistema criptográfico, es decir, a la familia de transformaciones, como información pública, permaneciendo su seguridad en el hecho de mantener secreta la clave. Este hecho, aunque criticado, se basa en una regla importante de los estudios de seguridad: la seguridad de un sistema no debería depender del nivel de secreto de algo que no puede ser cambiado fácilmente si está comprometido.

El sistema criptográfico es generalmente, o una pieza del equipo, o un programa, que solamente pueden ser reemplazados con un fuerte gasto y empleando mucho tiempo, mientras que la clave puede ser cambiada muy fácilmente.

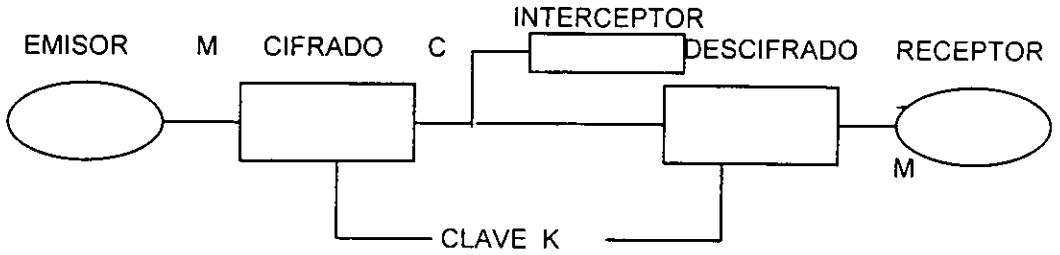
Como que toda la seguridad reside en mantener el secreto de la clave, el elemento que efectúa el cifrado y el descifrado debe poseer un método seguro de distribución de claves. Debe adelantarse aquí, que la mayoría de los protocolos empleados en sistemas criptográficos, envían las claves a su vez cifradas con otra clave denominada clave maestra, como precaución necesaria en la distribución de claves.

En la figura anterior se puede observar el funcionamiento de un sistema secreto. En él pueden apreciarse claramente las partes que intervienen: un emisor a la izquierda y un receptor a la derecha, conectados a través de un canal de comunicaciones.

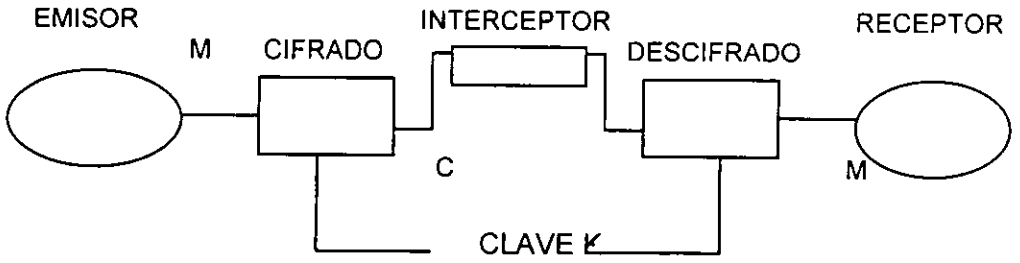
En la siguiente figura puede apreciarse el esquema de los flujos de información en un sistema secreto. En ambos (a) y (b), la clave es comunicada al emisor/receptor mediante un medio seguro. En el esquema (a) la posición del espía de información es pasiva respecto de inyectar información al sistema, solamente escucha y analiza la información.

En el esquema (b), el escucha además inyecta información, que una vez recibida en el receptor éste depurará, aceptando únicamente mensajes cifrados con la clave correcta, a ésta última modalidad se le llama certificación.

(A)



(B)



3.4 CRIPTOLOGÍA CLÁSICA.

Como arte, la criptología data de los primeros tiempos de la historia registrada. Como ciencia se encuentra en una etapa preliminar de búsqueda de los criterios más adecuados de seguridad y medidas de complejidad de los métodos empleados.

Diferentes aportaciones realizadas durante los siglos XV y XVI por Alberti y Trithemius, respectivamente, fueron ayudando a conocer métodos más seguros, como fue el sistema de substitución polialfabética de Alberti, o los cuadros para sistemas de cifrado de substitución polialfabética del monje Trithemius. Paralelamente Vignere introdujo perfeccionamientos al método de autoclave. No obstante, el mayor desarrollo de la criptología se ha realizado durante el siglo XX con la utilización comercial del telégrafo y los impulsos proporcionados en las dos grandes guerras para buscar métodos de comunicación secretos, siendo de interés el desarrollo de sofisticadas máquinas de cifrado durante la Segunda Guerra Mundial.

Desde un punto de vista taxonómico, las dos principales herramientas de la criptología clásica son los códigos y los sistemas de cifrado. Ambos son diseñados para transformar mensajes claros en criptogramas. El código es un diccionario fijo, predeterminado que asigna palabras código a los mensajes; su naturaleza fija, impacta en la seguridad que suministra, y por eso se usa el conjunto con sistemas de cifrado. Por otra parte, las palabras código son típicamente más cortas que las expresiones que representan, ofreciendo por tanto la ventaja de la comprensión de información, además de la seguridad. Si los códigos se usan adecuadamente, son más difíciles de vulnerar que algunos sistemas de cifrado clásicos, siendo la razón de su éxito, fundamentalmente, la gran longitud de la clave. Sin embargo, la dificultad de automatizarlo en un sistema de transmisión o en uno de almacenamiento y la vulnerabilidad estadística, ofrecen peligros que desaconsejan su uso.

3.5 MÉTODO CÉSAR.

Es un método utilizado por los romanos y atribuido a Julio Cesar. Originalmente el cifrado por el método Cesar consistía en una clave simple con la siguiente transformación única:

$$C : M - M + 3 \qquad (\text{mod. } 27)$$

Posteriormente fue generalizado a un sistema de cifrado con 26 claves, $0 < K < 26$, correspondientes a los 27 desplazamiento cíclicos del alfabeto :

$$C_K : M + K \qquad (\text{mod. } 27)$$

El número de claves al ser tan pequeño, facilita la labor del criptoanalista, haciendo vulnerable el sistema. La generalización del sistema de cifrado por el método Cesar da lugar al cifrado por simple substitución o substitución monoalfabeto.

El método Cesar substituye cada letra del mensaje original o mensaje en claro, por otra letra que formará parte del criptograma, de acuerdo al siguiente procedimiento:

1.- A cada letra del alfabeto correspondiente al lenguaje natural se le asigna un número secuencialmente.

2.- La correspondiente letra del mensaje cifrado, se obtiene desplazándose tres posiciones con respecto al número que tiene la letra del mensaje en claro.

A continuación ilustraremos el Método Cesar con un ejemplo:

Utilizaremos como mensaje en claro el siguiente: PROYECTO ZX EN LINEA, el cual tiene un criptograma asociado.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19

T	U	V	W	X	Y	Z
20	21	22	23	24	25	26

CORRESPONDENCIA PARA EL MÉTODO CÉSAR.

MENSAJE EN CLARO		MENSAJE CIFRADO
A	=	D
B	=	E
C	=	F
.		.
.		.
.		.
X	=	A
Y	=	B
Z	=	C

CIFRADO POR EL MÉTODO CÉSAR.

Mensaje en claro: PROYECTO ZX EN LINEA.

Mensaje cifrado: SURBHFWR CA HP ÑLPHD.

Para este ejemplo se recorrió 3 lugares el desplazamiento para encontrar la letra correspondiente, puesto que era la cantidad que originalmente se instauró con dicho método, pero éste número de desplazamientos puede ser variable y puede ser de 0 a 26, en el caso de una generalización del Método Cesar, es decir que si el desplazamiento (K) fuera cero el mensaje en claro y el mensaje cifrado serían iguales.

3.6 SUBSTITUCIÓN SIMPLE.

Es un método de cifrado que permite que cualquier permutación del alfabeto sea utilizada como clave de substitución en base a un sistema letra por letra, y que, como ya se ha adelantado antes, incluye como caso particular al método Cesar, tanto a la versión simple como a la generalizada. El sistema de substitución simple, también conocido como substitución monoalfabeto, aplica una transformación que es una congruencia lineal, cuya representación general es del tipo:

$$C : M - YM + K \qquad (\text{mod. } 27)$$

Donde M, igual que en el sistema anterior, es el valor numérico asignado a cada letra del alfabeto correspondiente al mensaje en claro. Y es una constante para determinar una correspondencia concreto entre todas las posibles para el conjunto de letras del alfabeto del criptograma y el alfabeto del mensaje en claro. K es una constante para fijar un

desplazamiento entre letras de uno y otro alfabeto dentro de la correspondencia determinada. Así, para el caso concreto de la correspondencia:

$$C: M - 7M + 3 \qquad (\text{mod. } 27)$$

3.7 CIFRADOS HOMOFÓNICOS.

Son cifrados por substitución de tal modo que cada símbolo en el alfabeto del mensaje en claro, es correspondido por uno de un conjunto de símbolos denominados homofónicos. A cada símbolo del alfabeto español, por ejemplo, se le asigna al azar un cierto número de enteros entre 0 y 99, de tal modo que el número de enteros asignados es proporcional a la frecuencia relativa de cada letra, y ningún entero es asignado a más de una letra.

3.8 CIFRADO DE BEALE.

Es otro tipo de cifrado substitución propuesto por Jefferson Beale en el cual a cada símbolo del alfabeto del mensaje en claro, le es asignado un entero que corresponde a ese símbolo en un texto tomado como referencia, que constituyen la clave. En el texto clave, los símbolos que lo componen reciben un número secuencial a partir de 0, de tal modo que para cifrar un determinado mensaje en claro se procede a buscar cada símbolo del mensaje entre los de la clave, y una vez encontrado se le substituye por su entero equivalente, sin que sea obligado que esto ocurra en la primera correspondencia encontrada. Si el texto del mensaje en claro es muy largo habrá que usar una clave que contenga por lo menos uno de cada uno de los símbolos del mensaje en claro, para que pueda realizarse la correspondencia.

3.9 CIFRADO POR EL MÉTODO DE TRANSPOSICIÓN.

El cifrado por transposición se efectúa operando en bloques de longitud n , empleando como claves las n! permutaciones posibles transponiendo los símbolos del mensaje. Para cifrar, se siguen los dos pasos siguientes:

1.- Se divide el mensaje en claro en bloques de longitud n, resultando por tanto, un cierto número de grupos de n símbolos de longitud.

2.- Se aplica a cada grupo de longitud n, la transposición determinada por la clave particularmente seleccionada.

3.10 MÁQUINAS DE CIFRAR HAGELIN C-48

Durante la Segunda Guerra Mundial se desarrollaron y utilizaron intensamente dispositivos electromecánicos que servían, y aún hoy se usan para cifrar información. La descripción de algunas de éstas máquinas es pública y su solución criptoanalítica es alcanzable fácilmente. La máquina Hagelin C-48 combina el texto original, símbolo a símbolo con la fuente de la clave, que es una larga secuencia pseudoaleatoria derivada de la clave. Tanto el texto en claro. Como la clave, como el criptograma que se produce, se componen de letras de un alfabeto con 26 símbolos, siendo el texto en claro restado , en vez de sumado a la fuente de la clave, módulo 26,
haciendo al cifrado como "autoinverso".

$$C = FC - M \qquad \text{(mod. 26) cifrado}$$

$$M = FC - C \qquad \text{(mod. 26) descifrado}$$

3.11 MÁQUINAS DE ROTOR.

Fueron usadas por los aliados en la Segunda Guerra Mundial, permaneciendo intensamente utilizadas hasta los años cincuenta, aunque incluso hoy permanecen algunas activas. Consta de una serie de discos conectados uno a otro sobre el mismo eje, de tal modo que una señal que entra por la cara del disco es permutada en él antes de salir, para entrar en otro donde se realiza una nueva permutación. El contacto entre ambos discos se realiza mediante un cableado. Además, cada disco puede ser movido, con lo que la permutación producida cambiará de una señal a otra.

Una máquina de rotor consiste en un banco de rotores con un mecanismo que cambia posición de los rotores cada vez que se cifra un carácter. El movimiento de los rotores es predeterminado, pudiendo producir un período antes de volver a repetir la clave de 266 símbolos, compuesto por un alfabeto de 26 caracteres y un banco con 6 rotores.

Tanto este procedimiento de cifrado como el anterior, ambos sobre máquinas, han sufrido estudios serios para averiguar su resistencia a ataques de los criptoanalistas, resultando que, en general, el criptoanálisis puede basarse en una serie de suposiciones.

Por citar algún punto débil de la máquina de rotor, está el hecho de que el cifrado de un simple carácter depende únicamente de los cableados o conexiones escogidas para que la señal circule a través de los discos. Si se intercambian los cableados que no intervengan

en el camino de ésta señal, el símbolo del criptograma no varía, lo que permite comprobar las hipótesis más fácilmente. El texto cifrado debería depender de toda la clave, no sólo de una porción.

3.12 CIFRADO POR SUBSTITUCIÓN POLIGRÁFICA.

El cifrado por substitución poligráfica más simple, es aquél que permite que una pareja de símbolos sea substituida por otra pareja equivalente, de acuerdo con una matriz de substitución que constituye la clave. Esto se designa como substitución digráfica, el sistema puede expandirse a substituciones de trigramas, o de bloques superiores en longitud.

3.13 EL CIFRADO ACTUAL.

La orientación inicial de la criptografía, la transmisión de mensajes cifrados , se ve complementada con el proceso de información en los ordenadores, y su consiguiente almacenamiento. La velocidad de cálculo proporciona ahora una solución más rápida y flexible para efectuar el cifrado y descifrado, y por tanto, para la puesta a punto de un criptosistema, pero al mismo tiempo, también dota de una herramienta más poderosa al criptoanalista, aumentando sus posibilidades de vulnerar la información. Con los ordenadores empleados para cifrar o descifrar información se añade, apoyándose en las teorías de la computabilidad y complejidad, un nuevo elemento: la complejidad de las funciones de cifrado y descifrado. Si al oponente se le presenta la información de tal modo, que para vulnerarla necesite una cantidad de cálculo, que bien es imposible o tome unidades tan elevadas que lo hagan infructuoso, el sistema habrá ganado en seguridad.

De otra parte, el criptoanalista tiene una nueva herramienta que le permita explorar sus hipótesis con mayor rapidez; los análisis de tipo estadístico son totalmente posibles con una

cantidad de criptograma suficiente, el análisis exhaustivo de todas las claves, pasa a ser una posibilidad que antes no era considerada y ahora sí.

3.14 COMPLEJIDAD DE LOS ALGORITMOS: CLASIFICACIÓN DE PROBLEMAS.

La Teoría de la Complejidad da una base que permite el análisis de los recursos de cálculo, necesarios en las técnicas criptográficas, así como una medida de la dificultad para resolver un criptograma por un criptoanalista. Como una primera aproximación, puede indicarse que un sistema criptográfico será tanto más seguro, cuanto más complejos sean los algoritmos necesarios para que el criptoanalista vulnere el sistema.

Existen dos medidas básicas en la complejidad computacional de un algoritmo: complejidad tiempo y complejidad espacio, o lo que es equivalente, el tiempo necesario para que a partir de unos datos (entrada), el algoritmo produzca los resultados deseados (salida), apoyándose en algún soporte de transición para que la información intermedia que necesite pueda ser utilizada. Las medidas T y E, tiempo y espacio respectivamente, son expresadas en función de I, siendo I la longitud de los datos de entrada al algoritmo. Así, una función f(I) para expresar complejidad, se suele representar en los términos de la teoría de la complejidad como O (g(I)) con una "O grande " para significar "del orden de".

La medida con una magnitud de las necesidades de tiempo y espacio de un algoritmo por el orden de su complejidad, tiene la gran ventaja de ser independiente del sistema ordenador en que se implante, ofreciendo la visión del crecimiento de esos requerimientos según sea I, la longitud de la entrada.

Un algoritmo es de complejidad polinomial si el tiempo de funcionamiento, o sea el número de operaciones que necesita efectuar es del tipo:

$$T = O(l^t)$$

siendo t una constante, que según tome los valores 0, 1, 2, 3, etc., dará el nombre de constante, lineal, cuadrático, cúbico, etc. Si el algoritmo es exponencial, entonces:

$$T = O(t^{h(l)})$$

siendo t una constante, y h (l) una función polinómica de l.

De acuerdo con la taxonomía de la complejidad de los algoritmos, los problemas que pueden resolverse en un tiempo polinomial, son denominados tratables, porque pueden ser utilizados con longitudes de entrada relativamente razonables. Los que no pueden resolverse en un tiempo polinomial son llamados intratables, ya que según aumenta la longitud de su entrada, la solución es imposible ni siquiera en los ordenadores más rápidos. Puede suponerse que los problemas se estructuran de acuerdo con sus diferentes complejidades, de tal modo que idealmente pueden ser agrupados en esferas concéntricas cada una conteniendo problemas de un determinado tipo, siendo los menos complejos los del interior, y los más complejos los del exterior. En la siguiente figura se representa esquemáticamente esta estructura, siendo los distintos tipos o clases los siguientes:

Los problemas de clase P son aquellos que se resuelven en un tiempo polinomial. Los problemas NP son aquellos que pueden ser resueltos o no por una máquina no determinista. En cualquier caso, si la máquina obtiene la solución puede comprobar si es correcta en un tiempo polinomial, pero no hay garantía de que la encuentre. Dentro de éstos, existe un grupo más complejo, los NP-completos. Los problemas de complejidad P-espacio, son los que pueden resolverse con un recurso de espacio polinomial, pero no

necesariamente en un tiempo polinomial. Por último, los exponenciales son aquellos que necesitan un tiempo exponencial para ser resueltos.

Estructura de las complejidades de los algoritmos.

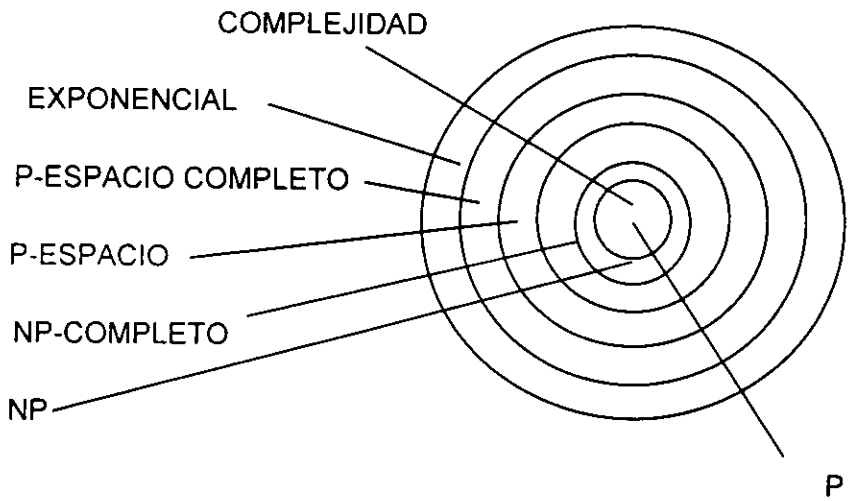


Figura 30

La situación de la teoría de la complejidad computacional, indujo a su aplicación al diseño de los sistemas criptográficos, ya que algunos de los problemas podrían ser ideales como funciones de cifrado, puesto que no es posible resolverlos en un tiempo polinomial: se trata de los problemas NP. Sin embargo, ya se ha indicado que un problema del tipo NP, permite comprobar si una solución es correcta, en un tiempo polinomial, lo cual puede facilitar la labor de intercepción de un criptoanalista. Para evitar ésta debilidad se ha sugerido construir algoritmos de cifrado que involucren una función de las denominadas "sentido único", cuya principal característica es su facilidad de cómputo en un sentido y la imposibilidad de hacerlo en el otro.

En 1976, Diffie y Hellman propusieron la aplicación de la complejidad computacional al diseño de algoritmos de cifrado. Observaron que los problemas NP-completos pueden ser candidatos excelentes para cifrados, ya que no pueden ser resueltos en un tiempo polinomial por ninguna de las técnicas conocidas.

Se deben citar tres razones que denotan las características que desde el punto de vista de la complejidad computacional, debe poseer un sistema criptográfico, algo diferentes de un problema general:

Mientras la teoría de la complejidad estudia problemas aislados, el criptoanalista posee para solucionarlos una colección de criptogramas, algunos generados incluso con la misma clave.

La teoría de la complejidad mide los problemas dando una dimensión en el peor de los casos, un sistema criptográfico debe ser "difícil" en todos los casos posibles.

La teoría de la complejidad califica como difíciles a determinados tipos de problemas, esto no significa que todos ellos puedan ser transformados en sistemas criptográficos. Debe ser posible, además, que tengan una fácil solución si se aporta una determinada información; y sólo con esa información. A esto se le denomina "puerta de escape".

3.15 TRANSFORMACIONES POR MÉTODOS COMPUTACIONALES ARITMÉTICOS: SUMA Y RESTA.

Debido a que las operaciones de suma y resta tienen operaciones inversas perfectamente definidas en los sistemas de numeración convencionales, estos métodos estrictamente numéricos, pueden usarse como apoyo a la técnica de diseño de los sistemas criptográficos, que van a ser usados en un ordenador.

Con este sistema el mensaje en claro es considerado como una serie de bloques de números en base n , mediante la asignación de una correspondencia entre los símbolos del alfabeto a que pertenecen los del mensaje en claro, y un dígito del sistema de numeración en base n. El cifrado puede realizarse mediante una substitución numérica, a la que se le suma o resta una determinada cantidad denominada clave. Este tipo de transformación es fácilmente implantable en un ordenador, y responde al siguiente esquema:

$$M + K = C$$

siendo M el mensaje en claro, K la clave, y C el criptograma.

La función de descifrado será consecuentemente.

$$M = C + K$$

3.16 MULTIPLICACIÓN Y DIVISIÓN.

Es un sistema parecido al anterior, aunque el cifrado se efectúe haciendo una multiplicación o una división del mensaje en claro utilizando una clave escogida. Igual que con el caso de la suma y resta se trata de representar tanto el mensaje en claro como la clave mediante un número en base n, procediendo a multiplicarlos o dividirlos. Con la multiplicación el criptograma obtenido será más largo, ya que se expande el número de dígitos base n obtenidos en la multiplicación. Con la división se reduce la longitud del mensaje, ya que el criptograma obtenido será el cociente de la división. Por cierto, que será conveniente escoger una clave tal que la división sea de resto 0, para que no exista ambigüedad en el descifrado. Además, si la clave es larga la reducción en la longitud del mensaje, al emplear la división, puede proporcionar notables ahorros.

3.17 OTRAS TRANSFORMACIONES.

Aquí mencionaremos que existen métodos o transformaciones empleados para obtener criptogramas, que están basados en la aplicación de simples reglas aritméticas. Podemos citar como muy efectivo el de cambios de base, según el cual, dada una asignación de cada símbolo del alfabeto a un número decimal entero a la manera usual, es decir, espacio = 0, A = 1, B = 2, etc., puede considerarse al criptograma como una representación en base K de un grupo de longitud l de símbolos del mensaje en claro representados por sus dígitos decimales.

Estos sistemas destruyen la posibilidad de estudio estadístico de los símbolos del criptograma, aumentando en consecuencia la dificultad de vulneración. Además, dado que

están fundamentados en operaciones aritméticas, son fácilmente implantables en un ordenador, ya que no requieren un gran número de operaciones para cumplir su función.

3.18 TRANSFORMACIONES CRIPTOGRÁFICAS MEDIANTE OPERACIONES LÓGICAS.

El empleo de operaciones binarias elementales en el funcionamiento del ordenador hace de éstas una herramientas idóneas, en cuanto a su facilidad de ejecución y manejo, para el diseño y la implantación de sistemas criptográficos en sistemas de tratamiento automático de información con ordenador. Las operaciones son muy simples y generalmente son empleadas varias, de tal modo que el cifrado resultante es un cifrado de los que han sido denominados productos, para dotar de cierta consistencia a la característica de seguridad que debe aportar el cifrado.

De las operaciones lógicas booleanas existentes sólo pueden usarse aquellas que tengan inversa, pues de otro modo no puede realizarse la operación de obtención del mensaje en claro. Estas operaciones lógicas con inversa son la operación or-exclusiva, la negación y la equivalencia, y son las únicas que permiten su aplicación en sistemas criptográficos. La aplicación se efectúa teniendo en cuenta que la representación de cualquier información en la memoria de un ordenador es en binario, y por lo tanto es apropiada para la realización de las operaciones lógicas mencionadas, ya que en los lenguajes de programación suelen existir instrucciones binarias de muy rápida ejecución para resolver las funciones mencionadas.

La aplicación criptográfica de estas funciones se hace aplicando la operación escogida directamente a la secuencia de dígitos binarios que representan el mensaje en claro y a la clave, o a la clave y al criptograma. La operación da como resultado otra secuencia de dígitos binarios que es fácilmente vulnerable, ya que por sí sola no destruye los parámetros del lenguaje, por lo que se encadena con otras operaciones formando cifrados producto.

Si a los criptogramas obtenidos se les aplica otra vez una nueva función lógica con diferente clave, se habrá obtenido un criptograma en el que los parámetros del lenguaje han sido desfigurados.

3.19 REGISTROS DE DESPLAZAMIENTO. (SHIFT REGISTERS)

En la técnica de implantación actual de los sistemas criptográficos, imperan varios procedimientos que son constantemente reseñados en la descripción teórica y diseño de los cifrados. Los métodos actualmente empleados, sea su versión hardware mediante componentes electrónicos dedicados, sea su versión software mediante rutinas o módulos de programas para cifrar o descifrar, están basados generalmente en alguno de los siguientes procedimientos simples:

- Operaciones lógicas.
- Registros desplazamiento.
- Manipulación de bits.

- Permutaciones
- Substituciones

La razón fundamental de esta utilización de operaciones simples está en la facilidad de manejo de ristras o secuencias de bits en un ordenador, y en la facilidad de concatenación de operaciones simples o compuestas que dan lugar a cifrados producto muy seguros.

Los diseñadores de sistemas criptográficos han realizado esfuerzos, encaminados a encontrar métodos de generación de bits que sean de naturaleza pseudoaleatoria, para producir secuencias binarias largas no repetidas y aleatorias partiendo de una clave dada.

3.20 TRANSFORMACIONES MEDIANTE MANIPULACIÓN DE BITS.

La existencia de instrucciones de manejo de bits de una forma no predeterminada, por ejemplo de cualquier longitud, o de secuencias no limitadas por la unidad de direccionamiento, byte o palabra. Este hecho condicionará el que algunos de los métodos que se presentan a continuación no sean fácilmente implantables en ordenador mediante el uso de instrucciones, y requieren la construcción de un dispositivo electrónico que realice las operaciones necesarias.

Entre las operaciones realizadas con bits, como componentes simples de las operaciones de cifrado y descifrado, están las siguientes:

Permutaciones de bits, o cajas P.
Substituciones no lineales, o cajas S.

3.20.1 PERMUTACIÓN DE BITS.

En algunas referencias se denominan cajas P, debido a que pueden ser presentadas y construidas como una caja cableada en la que entran n señales 0 ó 1, y salen n señales 0 ó 1, pero habiendo sufrido una permutación en su interior. También recibe el nombre de transposición aplicado a un alfabeto de dos símbolos. Las cajas P suelen ser generalmente fijas, y su única función es la de crear difusión. El número de permutaciones posibles dependerá de n, siendo n!.

3.20.2 SUBSTITUCIÓN DE BITS.

Suelen denominarse cajas S, y su estructura interna está dividida en tres etapas. La primera etapa es un decodificador en el que n bits son codificados, generalmente de binario a decimal, aunque podría usarse otro código, produciéndose 2n bits sufren una permutación antes de entrar en la tercera etapa en la que un codificador convierte los 2n bits resultantes de la permutación en otros n bits, haciendo la codificación inversa de la inicial. Estas transformaciones pueden ser singulares o no singulares, siendo reversibles en principio únicamente las no singulares, ya que las transformaciones singulares son irreversibles. El número total de transformaciones diferentes posibles son (2n)2n mientras que el de transformaciones no singulares diferentes es 2n!. Este tipo de transformaciones es difícilmente realizables para valores grandes de n con la tecnología actual, por la cantidad de manipulaciones que encierran y las diferentes opciones que permiten, por lo que normalmente se realiza en paralelo utilizando cajas S que trabajan con pequeños bloques de bits, generalmente 4 ó 6.

3.21 TAXONOMÍA DE LOS CIFRADOS.

Los sistemas de cifrado utilizados en la actualidad se encuadran en uno de los dos grupos siguientes, si se tiene en cuenta el modo según el cual el algoritmo de cifrado va alimentándose para producir el criptograma.

El primer grupo es el de los cifrados en bloque, en el que el sistema de cifrado va operando con bloques de bits con una longitud predeterminada. El segundo gran grupo es el de los cifrados denominados en flujo, en los que el sistema de cifrado va operando sobre una base no de bloques, como en el anterior sino de uno o más bits, desplazando previamente el conjunto de bits existente del estado anterior, en un número suficiente para albergar a los nuevos.

3.21.1 CIFRADOS EN BLOQUE.

La estructura básica de un cifrado en bloque actual es la de un cifrado producto. El cifrado en bloque trabaja con grupos de bits de una determinada longitud fija denominados bloques.

Las versiones comerciales trabajan en longitudes generalmente de múltiplos de ocho. Cada bloque es tratado por separado, de la misma manera que el anterior, con lo que cada bloque del mensaje es cifrado únicamente en base a él mismo y a la clave de cifrado, apareciendo dos bloques idénticos de mensaje en claro, cifrados también con el mismo criptograma como resultado. El cifrado en bloque puede ser utilizado de varias maneras distintas: como cifrado en bloque propiamente dicho, que responde al esquema de bloques separados y como cifrado en bloques encadenados, en el que se sigue cifrando la información en base a grupos o bloques de bits, pero cada bloque se forma con dos

porciones de texto, una con mensaje en claro , y la otra con una parte del criptograma correspondiente al bloque anteriormente cifrado, o del mensaje en claro del bloque anterior, dando lugar a dos tipos de cifrado en bloque encadenado: el cifrado encadenado modalidad criptograma, y cifrado encadenado modalidad mensaje en claro. Existe también un tercero que es una mezcla de ambos, en el que cada bloque de entrada al proceso de cifrado se compone de una parte de mensaje en claro correspondiente al bloque en curso, otra parte correspondiente al último criptograma obtenido, generalmente relacionados con alguna función de tipo lógico y reversible, como la suma módulo dos, o simplemente concatenados.

El cifrado en bloque encadenado modalidad criptograma alimenta sus bloques al cifrado, formando cada uno de ellos con una parte del mensaje en claro y otra parte del criptograma resultante anterior. El primero de los bloques, al no existir criptograma anterior, se nutre con una palabra clave (no la clave del cifrado).

La versión de cifrado en bloque encadenado modalidad mensaje en claro, nutre al cifrado bloques de información formados por trozos de mensaje en claro del bloque a cifrar, y del bloque ya cifrado con anterioridad. Igualmente, el primer bloque es alimentado parcialmente con alguna palabra clave inicial.

La tercera versión puede ser denominada cifrado en bloque encadenado modalidad mixta (criptograma-mensaje en claro). En ella cada bloque que entra al proceso de cifrado se compone de tres partes, la que corresponde al mensaje en claro que va a ser cifrado, otra que pertenece al mensaje en claro cifrado con anterioridad, y una tercera que pertenece al último criptograma obtenido, usando una palabra clave para el caso del primer bloque.

El uso de la función concatenación para formar los bloques está limitado por la naturaleza propia del cifrado en bloque. La longitud fija de los bloques a cifrar. Para salvar o mitigar ésta limitación se recurre al uso de funciones lógicas reversibles, como la suma módulo dos, para combinar los distintos componentes de cada bloque a cifrar, permitiendo en este caso utilizar cantidades de bits de igual longitud al bloque a cifrar.

Una importante propiedad de los cifrados en bloque encadenados es su fuerte dependencia intersímbolos de naturaleza no lineal, en la que cualquier tipo de corrupción manifestada en un bloque afectará a uno o más bloques de criptogramas, según el tipo de cifrado encadenado utilizado. Esta propiedad presentada tiene sin embargo algún aspecto positivo, que es la "Comprobación de Autenticidad", donde se comprueba que la propagación del error de un bloque al siguiente es útil, y evita que un oponente o un escucha en un sistema secreto pueda efectuar modificaciones no detectables en la información, a no ser que conozca la clave.

En el cifrado en bloque encadenado resulta que dos bloques de idéntica configuración de bits no producirán exactamente el mismo criptograma, dada la dependencia de cada criptograma con el criptograma anterior, o con ambos.

3.21.2 CIFRADOS DE FLUJO.

En lugar de usar una clave relativamente corta, incluso fácil de recordar, sería preferible utilizar una clave con las características de las secuencias de bits producidas por los registros de desplazamiento. Las características reseñables a recordar son, para los registros de desplazamiento: naturaleza pseudoaleatoria, y sucesión de dígitos binarios determinada a partir de un estado inicial, de donde puede reproducirse toda la secuencia, aunque ésta última tiene de por sí el grave inconveniente de que, pese a la facilidad de generación de secuencias pseudoaleatorias con dispositivos de bajo costo, son fáciles de

reproducir, a no ser que se manipulen con alguna función compleja que añada confusión y difusión.

Un cifrado en flujo no trata los caracteres o símbolos del lenguaje en claro independientemente, sino en función del estado de algoritmo de cifrado, que a su vez depende de los símbolos que hayan llegado al cifrado y de la clave utilizada. Después de cifrar cada carácter, el cifrado considerado como un algoritmo o un dispositivo, cambia de estado de acuerdo a una regla determinada. Esto impide que dos símbolos idénticos sean cifrados produciendo idéntico símbolo e el texto cifrado. Generalizando, dos secuencias de dígitos binarios que sean idénticos producen distinta secuencia de dígitos binarios en el criptograma. Su comportamiento es tal que la longitud de la salida es igual a la longitud de entrada, por lo que si ésta es pequeña habrá que hacer un número de operaciones de cifrado mucho mayor.

Siendo L la longitud total de un mensaje en claro a cifrar, y l la longitud característica del cifrado a flujo, es decir, los bits que se cifran cada vez que se hace una operación, el número total de operaciones de cifrado a realizar para obtener el criptograma total será:

$$L / l = N$$

Este hecho debe tenerse en cuenta cuando se diseña o escoge un sistema de cifrado, ya que si l es 8 en lugar de 1 bit, por ejemplo, el número de operaciones de cifrado necesarias para efectuar el proceso total será ocho veces menor, es decir, es inversamente proporcional a l, lo que afectará en términos de tiempo al sistema criptográfico, ya que tardará más tiempo en cifrar/descifrar.

Se considera que existe una distinción entre aquellos sistemas con un solo estado, el inicial, que por tanto siempre transitan a él mismo, y aquellos otros con más de un estado,

que transitan a distintos estados del inicial. A los primeros les denominan cifrados en bloque, ya que cada bloque cifrado finaliza y comienza en el mismo estado, produciendo para dos entradas idénticas la misma salida. Los cifrados en bloque encadenados se comportan del mismo modo, aunque la entrada del mensaje en claro es modificada con otra secuencia de bits para evitar estas posibles repeticiones.

A los segundos, es decir, a aquellos con más de un estado, los denominan cifrados en flujo, siendo por tanto el caso general, mientras que los cifrados en bloque son el caso particular de los cifrados en flujo cuando el cardinal del conjunto de estados es 1, o siendo mayor, el sistema solo transita por un estado, permaneciendo el resto de los estados sin ser transitados.

Los cifrados en flujo tal como se han descrito, no son aplicables en términos generales a cualquier necesidad de cifrado dada su naturaleza y comportamiento, según los cuales el bloque de bits que se cifren un momento dado, dará un criptograma que depende además de los bits de la clave, de los mensajes en claro anteriores. Esta característica impide que en un sistema secreto pueda realizarse un descifrado selectivo, o cifrado seleccionando determinados bloques de un fichero, o páginas de una base de datos, ya que la utilización del cifrado en flujo considera toda la información, y la utilización selectiva rompería la natural secuencia del algoritmo. Esta restricción hace menos aceptables a los cifrados en flujo para su utilización en un ordenador, aunque es más fuerte un cifrado en flujo, en términos generales, que un cifrado en bloque.

Los cifrados en flujo será preferible usarlos en aquellos casos en que la información sea altamente estructurada o redundante, para disminuir las posibilidades de vulneración por análisis estadístico. También son útiles aquí los cifrados en bloque encadenados. Sin embargo, en aquellos casos en que se deseen simples transformaciones y la información no

sea muy estructurada, pueden usarse los cifrados en bloque. Ejemplos del primer caso: ficheros secuenciales. Ejemplos del segundo caso: Mensajes transmitidos por un teletipo.

Desde el punto de vista informático, la utilización más adecuada para cifrados fuertes, choca contra el inconveniente mencionado anteriormente respecto a la necesidad de cifrar o descifrar todos los bloques antes y después, si se usa un cifrado en flujo. Mientras la conveniencia de un cifrado en flujo para un fichero secuencial es manifiesta, porque aquellas partes redundantes van a ser cifradas con distinto criptograma, la posibilidad de seleccionar un registro, o reescribir o intercalar, se ve condicionada por toda la operativa necesaria para utilizar el cifrado. Sería necesario cifrar lo subsiguiente y lo anterior. Este tipo de cuestiones es necesario sean consideradas concienzudamente antes de escoger un sistema de cifrado concreto para alguna aplicación, por sus incidencias en el tratamiento postcifrado.

3.22 REGLAS DE ENCRIPTAMIENTO DE DATOS. (DES)

El 15 de enero de 1977, la National Bureau of Standards (NBS) del Departamento de Comercio de USA, publicó su Federal Information Processing Standards Publication (FIPS PUB no. 46) con el título de Data Encryption Standard. Este procedimiento es la conclusión de los estudios y desarrollo de un método criptográfico realizado durante los años 1968 a 1975 por una importante constructora de computadoras, y básicamente consiste en 16 pasos o ciclos de substitución o permutación de bits, controlados por una clave, y fue basado en un trabajo realizado por Horst Feistel. Finalmente en la fecha mencionada fue aceptada como estándar, y todas las máquinas vendidas al gobierno de los Estados Unidos están obligados a incluir la capacidad de utilizar este estándar.

Un algoritmo como el DES puede ser considerado como un número grande de procedimientos matemáticos llamados transformaciones, que definen como secuencias de datos inteligibles que representan un mensaje, son cambiadas en secuencias de bits que aparentemente son ruido, no inteligibles a hombres o máquinas. La clave criptográfica es mantenida en secreto y está formada por una secuencia de caracteres, generalmente corta, que identifica las transformaciones a realizar.

Para que sea útil, el algoritmo tiene para cada una de sus transformaciones, una única operación inversa que cambia el "ruido no inteligible" por los datos originales; esta operación es el descifrado, y solo puede hacerse si se tiene conocimiento de la clave de cifrado.

El algoritmo criptográfico suministra seguridad entre dos nodos de un sistema de proceso de datos si los dos nodos tienen instalado el algoritmo, sea con tecnología hardware, como obliga la norma de utilización estándar en USA, o con tecnología

software. Es preciso además que ambos nodos tengan exacto conocimiento de la clave utilizada.

A continuación se cita parte del documento conocido como FIPS PUB 46:

"La aplicación selectiva de seguridades tecnológicas y procedimientos afines es una importante responsabilidad de cada organización Federal, suministrando la seguridad adecuada a sus sistemas de procesos de datos.

Esta publicación suministra un estándar a ser usado por las organizaciones Federales cuando estas organizaciones precisen la protección criptográfica para datos valiosos o sensibles en informática.

La protección de los datos de un ordenador durante la transmisión entre componentes electrónicos o de almacenamiento puede ser necesaria para mantener la confidencialidad e integridad de la información representada por esos datos. El estándar especifica un algoritmo de cifrado que tiene que ser implantado en un dispositivo electrónico para ser usado en los sistemas y redes Federales de proceso de datos. El algoritmo define únicamente los pasos matemáticos requeridos transformar datos de ordenador en datos cifrados criptográficamente. También especifica los pasos requeridos para transformar estos datos cifrados a su forma original. Un dispositivo ejecutando este algoritmo puede ser utilizado en muchas áreas de aplicaciones donde la protección criptográfica es necesaria. Dentro del contexto de un programa de seguridad total comprendiendo procedimientos de seguridad física, manejo de información correcta y controles sobre el acceso a sistemas o redes de ordenadores, el Data Encryption Standard se hace disponible para ser usado por las agencias Federales.

3.22.1 DESCRIPCIÓN DEL ALGORITMO.

El DES cifra un bloque de texto original de 64 bits en un bloque de texto cifrado de 64 bits bajo el control de una clave criptográfica de 64 bits, de los cuales 56 son usados directamente por el algoritmo y 8 son utilizados para detección de errores. El descifrado convierte los datos a su forma original si se usa la misma clave.

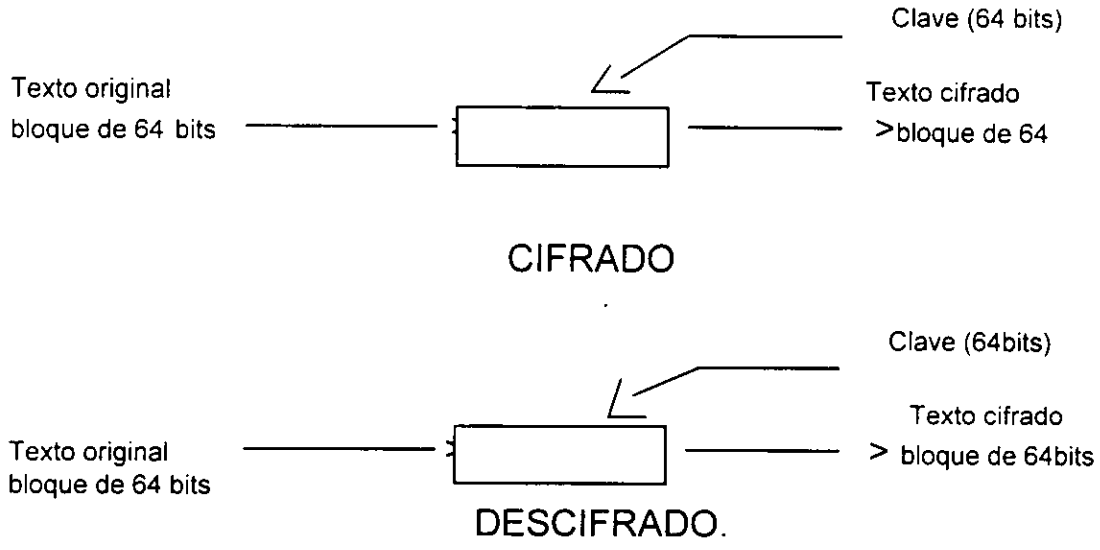


Figura 31

La clave es generada de tal modo que 56 bits de los 64 son usados por el algoritmo y 8 no los utiliza directamente el algoritmo sino que son usados para detección de errores, como bits de paridad impar de cada byte de 8 bits de la llave, es decir existe un número impar de bits "1" en cada byte.

Todos los usuarios conocedores de la clave, pueden cifrar o descifrar datos intercambiables con el resto de los miembros del grupo que posean la clave y el algoritmo.

La seguridad del dato depende solamente de la seguridad con que se mantenga el secreto de la clave usada. Si no se posee la clave o se desconoce, no se puede obtener el dato original. Como puede fácilmente deducirse por los tamaños de la clave y del bloque de datos usado, éste algoritmo está diseñado para ser utilizado en máquinas cuya longitud de palabra sea de 32 bits o de 64, lo cual no es óbice para que se haya podido desarrollar un algoritmo software para ser usado en máquinas con diferente longitud de palabra, aunque en esta caso ha sido preciso añadir una serie de instrucciones adicionales para emular el comportamiento marcado por el estándar.

El bloque a cifrar se somete a una permutación inicial de sus bits denominada IP, y a continuación se inicia un cálculo complejo cuyo resultado depende no sólo de la entrada, sino de la clave. De tal modo que existe una interacción entre clave y datos. Después de éste cálculo, que en realidad son 16 cálculos distintos, se efectúa una nueva permutación que es la inversa de la inicial, denominada IP-1. La función compleja puede definirse simplemente en términos de una función f denominada función de cifrado y una función KS denominada planificación de clave.

El cálculo que utiliza el bloque inicial permutado como su entrada, para producir el bloque de presalida, consiste, excepto en un intercambio final de bloques, en 16 iteraciones de un cálculo lo que se explica en términos de la función de cifrado f, la cual opera en dos bloques, uno de 32 bits y uno de 48 bits, produciendo un bloque de 32 bits.

De acuerdo con la notación introducida, sean 64 bits de un bloque de entrada, que consta de un bloque de 32 bits, L, seguido de otro bloque de 32 bits, R, por tanto el bloque de entrada es LR. Sea K un bloque de 48 bits elegido de la clave de 64 bits. La salida L´R´ de una iteración, cuya entrada es LR, está definida por:

$$L' = R \qquad (1)$$

$$R' = L * \mathbf{f}(R, K) \qquad (2)$$

donde * denota la operación binaria suma módulo dos.

En cada iteración se escoge un bloque diferente K, de bits de la clave elegida, de tal modo que, denominando Kn a un bloque de 48 bits proporcionado por la función KS en el ciclo n (1 a 16) siendo KEY la clave elegida, Kn se obtiene:

$$K_n = KS(n, KEY) \qquad (3)$$

Expresando ahora las ecuaciones (1) y (2) teniendo en cuenta la (3) y las iteraciones efectuadas, resulta para valores de n desde 1 a 16.

$$L_n = R_{n-1} \qquad (4)$$

$$R_n = L_{n-1} * \mathbf{f}(R_{n-1}, K_n) \qquad (5)$$

El bloque de presalida es entonces $R_{16} L_{16}$

El descifrado se efectúa aplicando el mismo algoritmo usado para cifrar el bloque de entrada, pero en cada iteración hay que tener cuidado en utilizar el mismo bloque de bits de la clave KEY, que fue utilizado durante el proceso de cifrado. Utilizando la misma notación que anteriormente se ha usado, resultará:

$$R_{n-1} = L_n \qquad (6)$$

$$L_{n-1} = R_n * \mathbf{f}(L_n, K_n) \qquad (7)$$

Ahora el bloque R16 L16 es el bloque de entrada permutado, con el que se inicia el proceso de las 16 iteraciones, y LO RO es el bloque de presalida. Consecuentemente K16 se utiliza en la primera iteración, en la segunda K15 ya así sucesivamente hasta la iteración número 16.

3.22.2 UTILIZACIÓN DEL DES.

Se describen en la publicación del FIPS, dos modos diferentes de utilizar el algoritmo estándar. El primero de ellos se denomina "libro de códigos electrónico", y supone que bloques de 64 bits de datos son introducidos directamente en el dispositivo en el que se generan 64 bits de texto cifrado bajo el control de la clave. Con éste método, cada bloque cifrado es independiente de todos los demás. El segundo método es usado como generador binario de ristras de bits estadísticamente aleatorios, que son combinados con los datos originales mediante una operación Or-exclusivo. Para asegurar el sincronismo del cifrado y del descifrado, sus correspondientes entradas se ponen siempre iniciadas con los 64 últimos bits cifrados que llegaron al proceso de descifrado, u obtenidos en el proceso de cifrado. Este método se llama modo CFB o retro alimentado.

Este algoritmo queda encuadrado por la técnica usada dentro de los que se denominan cifrado producto, perteneciendo su utilización a diversos tipos simultáneamente. El algoritmo puede utilizarse como cifrado en bloque puro, trabajando con bloques de 64 bits, haciendo que bloques idénticos se cifren del mismo modo. Pero también puede ser utilizado como cifrado en bloque encadenado en dos de las tres modalidades, así como cifrado en flujo.

Originalmente el DES fue creado para el encriptamiento y el desencriptamiento de datos. Pero, su aplicación se puede extender también a la autenticación de datos. En sistemas de procesamiento de datos de carácter autómata, es frecuente que sea imposible para los humanos el rastrear datos a tal exactitud para determinar si han sufrido alguna modificación. La examinación puede consumir gran cantidad de tiempo debido a las vastas cantidades de datos involucrados en los sistemas modernos de procesamiento de datos, o bien los datos pueden tener demasiada redundancia para la detección de errores. Aún si la capacidad humana de rastreo fuera suficiente para revisar todos los datos utilizados, los datos pudieran haber sido cambiados de tal forma que sería muy difícil para un humano notar dicho cambio. Por ejemplo, casa pudiera cambiar a caza o $ 1 900 puede ser cambiado a $ 9 100. Sin información adicional el rastreador humano puede aceptar los datos modificados como auténticos. Estas amenazas existen aún utilizando encriptamiento de datos. Por lo que es deseable tener medios autómatas para detectar modificaciones en nuestros datos ya sean intencionadas o accidentales. Los códigos de detección de errores ordinarios no son adecuados, ya que si nuestros adversarios llegan a conocer el algoritmo que genera el código es conocido, éste podría generar el código correcto después de modificar los datos. La modificación intencional es indetectable con tales códigos. El DES puede ser usado para producir una suma de revisión que puede protegernos contra modificaciones de datos no autorizadas ya sean accidentales o intencionadas.

Algunas formas de utilizar este método de detección de errores es enviar y recibir de forma aleatoria y/o constante bloques encriptados de un valor constante (ya sea ceros o unos) a lo largo del enlace y revisarlos, sin concuerdan dichas constantes no han existido errores. Con éste método el rango de posibilidad de error varía entre 216 a 224.

3.23 CIFRADOS SIMÉTRICOS Y CIFRADOS ASIMÉTRICOS.

Los sistemas en los que se han encuadrado las explicaciones para los cifrados estudiados son claramente simétricos, si se tiene en cuenta que los dos puntos o elementos que intervienen en el sistema secreto tienen que utilizar y guardar en secreto la misma secuencia

de dígitos binarios, que se han etiquetado con el nombre de clave. En un entorno de comunicaciones esto significa que, si en el transcurso del envío de la clave entre los puntos emisor y receptor, ésta se ve comprometida, la comunicación no puede asegurarse. Los nuevos sistemas secretos son asimétricos en el sentido de que el transmisor y receptor manejan claves diferentes, siendo alguna de ellas imposible de calcular por derivación de las otras. La cuestión que se analiza es la seguridad del criptosistema, medida en términos de complejidad computacional, pues el entorno en que se mueve el análisis es el de su aplicación a sistemas informáticos. Por otro lado, se relaciona la seguridad con las claves de cifrado, la longitud más adecuada al tratamiento criptográfico en la computadora, y la arquitectura simétrica o asimétrica de los sistemas de cifrado.

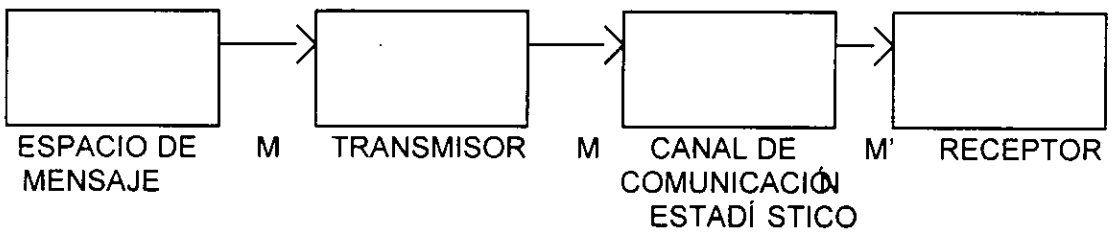
3.24 CANAL DE CIFRADO-DESCIFRADO.

El clásico canal de Shannon es tal que los códigos C se han diseñado para que la posibilidad de un mensaje alterado recibido en el receptor sea interpretado erróneamente con probabilidad mínima. Si el código es corrector de errores, se ha diseñado para maximizar la posibilidad de que el receptor pueda recuperar el mensaje original a partir del recibido.

El canal general de cifrado-descifrado se compone de un emisor que quiere enviar un mensaje M a un receptor, aunque ahora el canal puede estar bajo la acción de un oponente con uno de los siguientes propósitos:

- Obtener y determinar el mensaje M.
- Alterar M y hacer que el mensaje M' (M alterado), sea aceptado en el receptor, engañándole.
- Suplantar al emisor.

CANAL DE COMUNICACIONES CLÁSICO.



ESQUEMA FUNCIONAL DEL CANAL CODIFICADOR/DECODIFICADOR SEGÚN SHANNON

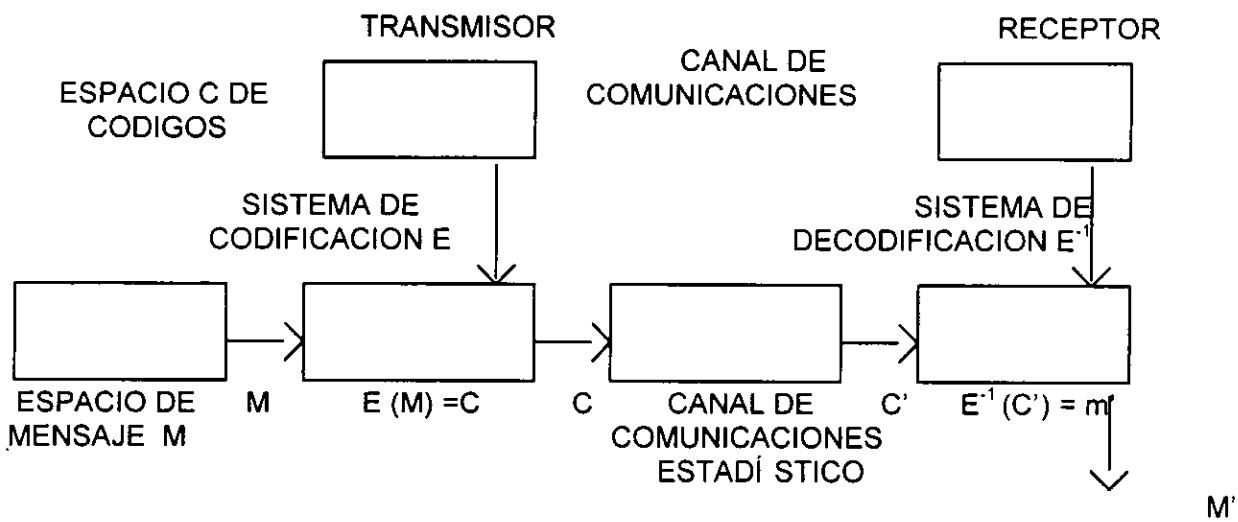


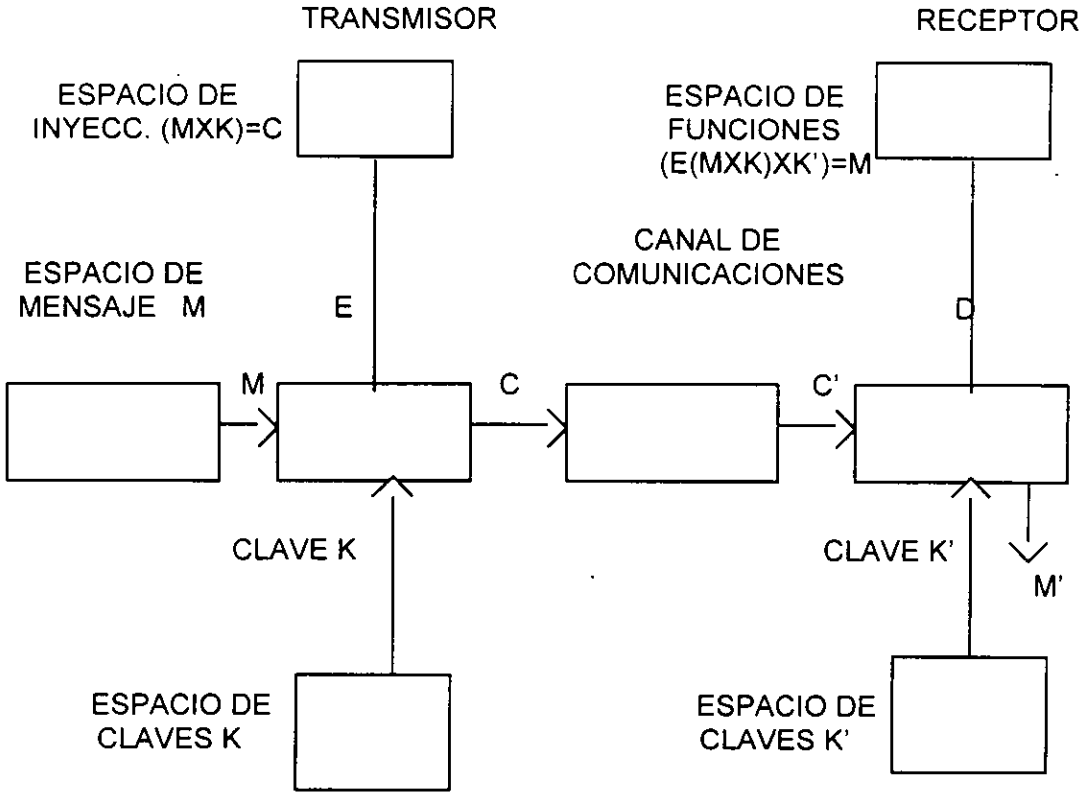
Figura 32

Con este planteamiento, el clásico canal probabilístico de comunicaciones según el modelo codificación-decodificación, se convierte en aras de la criptografía, en un canal con un comportamiento típicamente estudiado en teoría de juegos, en el que la naturaleza y el azar se han substituido por un oponente con inteligencia, y para el que la teoría de la criptografía, diseña y estudia formas de producir código que no pueden ser distinguidos sistemáticamente de secuencias aleatorias de ruido, invalidando la acción del oponente.

En muchos casos el objetivo de comunicación secreta y privada como tal, es secundario. Es relativamente fácil la tarea de un oponente inyectando mensajes que originen interpretaciones incorrectas en el receptor, o incluso, romper el código utilizado.

Un código perfectamente seguro es tal que a cada símbolo del mensaje en claro le puede corresponder cualquier símbolo del cifrado con igual probabilidad, independientemente de la clave utilizada. Un sistema perfectamente seguro debería distribuir el espacio de mensajes en claro sobre sí mismo, de modo aleatorio, de tal manera que un oponente interceptador de un mensaje cifrado tuviera que considerar todos los puntos de M, como candidatos igualmente probables al mensaje en claro original. Un generador de números aleatorios considerado como bueno, no es necesariamente un buen sistema de cifrado, pero sí es cierto lo contrario: un buen sistema de cifrado es necesariamente un buen generador de números aleatorios.

ESQUEMA FUNCIONAL PARA EL CANAL GENERAL DE CIFRADO/DESCIFRADO.



E = Sistema de cifrado
D = Sistema de descifrado

figura 33

Un esquema del cifrado perfecto es equivalente a una matriz donde las filas corresponden a los mensajes en claro, las columnas a los criptogramas, y las entradas a las claves, tal como lo sugirió Shannon. Sin embargo, un criptosistema perfecto es incapaz de verificar la autenticidad de mensajes, ya que no habría redundancia en ellos y por tanto no

hay una base sobre la que se puede deducir la autenticidad. Para que un sistema efectúe autenticidad con perfección debe introducir redundancia, de tal modo que el espacio de cifrados sea dividido en dos partes o clases. Las imágenes cifradas de los mensajes en claro, y los cifrados que se llamarán inaceptables. La perfección se logrará si dada cualquier pareja mensaje en claro-mensaje cifrado, el oponente, que no conoce la clave es incapaz de seleccionar un mensaje del espacio de criptogramas con otro criterio que el de elección al azar, supuesto que ha intervenido el mensaje en claro. El sistema perfecto difundirá y extenderá los cifrados no aceptables a través de todo el espacio de mensajes cifrados.

3.25 CIFRADOS "MOCHILA".

Con este nombre genérico se conocen varias proposiciones de cifrado que toman en la literatura especializada el nombre ingles "knapsack", destacando como más importantes los pertenecientes a Merkle, Hellman, Shamir y Lempel. Algunos son útiles especialmente en el campo de verificación de autenticidad, mientras que otros son sistemas asimétricos que pueden usarse en cualquier sistema secreto en el que se pretenda mantener el secreto de la información.

La proposición de Merkle y Hellman sobre el problema de la mochila, está basada en un esquema en un esquema cuya seguridad depende de la dificultad de resolver el siguiente problema: dado un entero positivo C y un vector V = (v 1, v 2, ..., v n), de enteros positivos, encontrar un subconjunto de elementos de V que sumen C.

Es importante recordar que la complejidad computacional de los problemas NP se mide por la dificultad de resolver el peor de los casos, por lo que algunas situaciones particulares dadas por condiciones concretas de los vectores, que hacen al problema de la mochila, muy fácil de resolver, no se consideran aplicables a sistemas criptográficos.

Merkle y Hellman han demostrado cómo convertir un problema de la "mochila" en lo que en términos de criptografía se llama "trampa de la mochila", o "puerta de escape de la mochila", y permitir su solución fácil conociendo cierta información, o siendo muy difícil sin conocerla.

3.26 MÉTODO DE FACTORIZACIÓN.

Otro sistema de cifrado asimétrico con aplicación bidireccional se basa en el procedimiento propuesto por Rivest, Shamir y Adleman, que esquemáticamente se basa en la complejidad computacional necesaria para encontrar números primos grandes. Los mejores algoritmos conocidos hoy pueden encontrar un número primo de d dígitos en un tiempo O (d3), mientras que obtener sus factores lleva una complejidad, O (n (ln (ln n) ln n) ½), cálculo debido a Shroeppel. Este esquema, recibe el nombre de esquema RSA, dado por las iniciales de sus autores, propone la elección de un número n que es producto de dos grandes números primos p y q:

$$n = p * q$$

La factorización de n está fuera de todas las posibilidades actuales de cómputo, si p y q son suficientemente largos.

La conversión en número de un mensaje con texto en idioma natural puede hacerse asignando un valor numérico a cada símbolo, o bien usando como número su propia codificación en el código que se represente en memoria. Puede ser interesante subdividirlo en bloques de determinada longitud para no exceder las características de diseño del ordenador en cuanto a operaciones con coma fija, ya que la representación de los valores debe hacerse sin pérdida de precisión. La elección de valores debe hacerse en consonancia

con este condicionamiento, ya que de otro modo será preciso utilizar rutinas especiales que permitan trabajar con magnitudes especialmente altas.

Los esquemas de cifrado asimétrico basan su seguridad en la dificultad de factorizar n en p y q, así como de la selección cuidadosa de los primos p y q.

3.27 VERIFICACIÓN DE AUTENTICIDAD.

La verificación de autenticidad previene la posibilidad de que un oponente inyecte datos falsos en el canal de comunicaciones, o altere los mensajes cambiando su significado. En comunicación a través de línea telefónica el problema de verificación de autenticidad es relevante, ya que la parte receptora de la información no puede determinar quién la envía. Sin embargo, la escucha e interceptación es técnicamente más difícil y legalmente más peligrosa que la inyección de información, o que el hecho de hacerse pasar por alguien. En comunicación por radio la situación es justo al revés, ya que la escucha es una actividad pasiva, mientras que la inyección de información supone un actitud ilegal en el transmisor, así como su persecución. Algunas veces será suficiente con la comprobación de que un mensaje no ha sido modificado por un tercero, mientras que en otros se necesitará probar la identidad del emisor.

En un entorno de tiempo compartido con muchos usuarios, hay dos aspectos diferentes de la verificación de autenticidad. Uno de ellos es la determinación por parte del operador del terminal y por parte del ordenador, que "el otro" es legítimo, mientras que el otro aspecto es la verificación de la integridad del mensaje, es decir, que todos los mensajes cifrados intercambiados entre el terminal y el ordenador se han recibido correctamente, y que están en el contexto correcto.

Los usuarios que tratan con información secreta necesitan terminales equipados con la posibilidad de cifrar-descifrar, y cada utilizador deberá tener un sistema de almacenamiento donde guardar la clave de cifrado, como una tarjeta con banda magnética. Dicha clave nunca deberá ser transmitida por el canal normal de comunicaciones, sino por un medio más seguro, como correo privado o certificado.

La pregunta básica para medir el grado de legitimidad de un usuario es : ¿conoce el usuario la palabra clave de acceso al sistema, y posee la clave de cifrado correspondiente a esa pretendida identidad?. A continuación se da un esquema de un sistema criptográfico con verificación de autenticidad en el que puede observarse la aplicación de un cifrado en bloque encadenado para tal fin.

1. El usuario teclea y envía su identidad.
2. El ordenador responde con una información que forma parte de un protocolo general de identificación y acuse de recibo. Suele constar esta información de una o más palabras D con la fecha y hora de conexión, siendo distinto en cualquier momento. Esta información se completa con algunos símbolos de relleno.
3. El terminal recibe este bloque, lo descifra con su clave y lo muestra en pantalla, permitiendo al operador analizar si la información D es normal o no, en caso positivo reconocerá que su comunicación con el ordenador está abierta. A continuación el usuario del terminal teclea su palabra clave de acceso al sistema y el mensaje a enviar al ordenador. Se forma un bloque claro constituido por D y la palabra clave de acceso, éste bloque se cifra con la clave correspondiente al usuario, en su terminal con dispositivo de cifrado y se envía al ordenador.
4. Cuando éste bloque se recibe en el ordenador, se descifra con la clave correspondiente, y comprueba que hay correspondencia entre la palabra D, guardada antes, y la recibida del terminal. Igualmente procede con la palabra de

acceso recibida, comprobando que se encuentra en el fichero de usuarios permitidos. Si es positivo, se permite continuar al usuario, y en caso contrario su acceso se le prohibe, pues supone que ha habido una vulneración.

Nadie que no tenga la clave de cifrado puede producir el bloque cifrado, para cuando se descifre en un bloque en claro, contenga D y la palabra de acceso, y por tanto, no puede incidir positivamente en el sistema suplantando la persona de un usuario autorizado. Hay un proceso de encadenamiento que asegura desde el principio la certificación de autenticidad, al efectuarse un cifrado en el que cada bloque depende del anterior, y una parte está cifrada varias veces con un procedimiento de supercifrado con la misma clave.

Este proceso se repite hasta que todo el mensaje ha sido enviado a la computadora, que va descifrando los bloques recibidos en el orden que han llegado. La llegada del primer bloque cifrado a la computadora es seguida de su descifrado, usando la clave correspondiente al usuario. Una vez obtenido el bloque en claro, se procede a efectuar dos correspondencias de control. La primera es verificar que D es exactamente el texto que se guarda la computadora. La segunda es verificar la palabra clave de acceso al sistema, de acuerdo con la lista que la computadora posea. La llegada del segundo bloque es seguida de su descifrado y posterior control de la información, que debe ser precisamente una parte del bloque cifrado recibido anteriormente, también se habrá obtenido el mensaje M1. Para el tercer bloque se comprobará, después de descifrarle, que parte del bloque en claro obtenido corresponde con la parte correspondiente del bloque cifrado anterior, además se habrá recibido el mensaje M2. Por supuesto, la negación en cualquiera de estos controles de correspondencia, da como resultado la imposibilidad de que el usuario pueda usar el sistema.

Si durante la transmisión de cualquiera de los bloques cifrados hay una corrupción de información, el bloque en claro resultante del descifrado no será válido, resultando cada bit con una probabilidad de error de 0.5. No obstante, la inclusión en el sistema de cifrado de dispositivos codificadores-correctores antes de descifrar, puede dejar esta posibilidad muy reducida.

Si la información etiquetada como D es única, también será único el primer bloque enviado al ordenador.

La probabilidad de que un mensaje sea único, incluso aunque la parte no tomada del bloque anterior sea igual a la misma parte del bloque precedente, es del orden de 1 - 2-m, asegurando que cada vez se recibirá un bloque diferente, dada la naturaleza del cifrado de encadenamiento.

3.28 SISTEMAS DE CLAVE PÚBLICA.

El concepto de criptosistema de clave pública empezó a manejarse a partir de 1976 según una publicación (Diffie y Hellman), que proponía un sistema de comunicación privada que emplea un directorio de claves públicas, de tal modo que cada utilizador fija un procedimiento E para que sea usado por otros usuarios cuando cifren mensajes que vayan dirigidos a él, mientras guarda en secreto su propio procedimiento D de descifrado. Para que éste sistema sea viable, debe existir un sistema simple, mediante el cuál cada usuario pueda producir su propio E y D.

Un criptosistema de clave pública puede ser definido como un par de familias de algoritmos que representan transformaciones invertibles. Con un espacio finito de mensajes M. Tanto E como D deben ser rápidos de obtener y fáciles de aplicar. El conocimiento

público de E no implica el conocimiento ni pérdida de seguridad de D, lo que significa, la obtención de D a partir de E es un problema intratable desde el punto de vista de teoría de la calcubilidad.

La principal diferencia de los sistemas de clave pública respecto de otros sistemas que pudieran denominarse de clave secreta, es precisamente la característica de asimetría. Podría afirmarse que los cifrados asimétricos pueden ser sistemas de cifrado de clave pública, en los que la clave para cifrar y para descifrar son distintas y prácticamente imposibles de obtener ésta a partir de aquella. En este sistema son necesarias las funciones de "un solo sentido" como herramientas fundamentales a utilizar en los cifrados de este tipo, de relativa facilidad para cifrar pero de gran dificultad para descifrar si no se conoce la segunda clave.

La razón por la que las claves deben estar cuidadosamente protegidas en los sistemas de clave secreta, es que las funciones de cifrado o descifrado son inseparables, estándole permitido a cualquiera que tenga acceso a la clave de cifrado, el correspondiente cifrado. Si las capacidades de cifrar y descifrar se separan, se puede proteger la información sin guardar en secreto la clave de cifrado, ya que no será necesaria para descifrar.

La utilización práctica de estos sistemas de clave pública, envuelve, no obstante, algunas cuestiones adicionales relacionadas con el suministro de las claves allí donde son necesarias, para que cada usuario pueda hacer la elección apropiada. Este suministro da nombre a una serie de procedimientos que suelen recibir el nombre de protocolos de distribución de claves en los sistemas de clave pública.

3.29 MANEJO DE CLAVES EN UN SISTEMA CRIPTOGRÁFICO.

El problema del manejo de claves en un sistema criptográfico abarca la generación, distribución y protección de las clave, necesaria para que en un sistema secreto de comunicaciones, tanto el emisor como el receptor tengan garantizada la seguridad. En un sistema multiusuario hay un número de pares de conexiones que crece con el cuadrado de n y es $(n2^{\cdot n}) / 2$, siendo n el número de usuarios.

En una estructura jerarquizada arborescente, el problema de la distribución puede resolverse a través de la cadena de mando, pero aún en este punto hay serios impedimentos en el uso de la criptografía. En términos generales, la utilización de alguno de los esquemas asimétricos facilita el problema de la distribución de claves.

3.29.1 SOLUCIÓN MEDIANTE JERARQUÍA DE CLAVES.

Propuesto por Everton, el manejo de claves está basado por principio simple según el cuál, cuando una clave no puede ser físicamente protegida, se debe cifrar bajo otra clave de orden superior. La ejecución de esto se basa en el establecimiento de una jerarquía de claves en cuya cúspide se encuentran las claves maestras, que son almacenadas en los dispositivos de cifrado y utilizadas para proteger el nivel siguiente inferior de claves , o claves submaestras. Estas a su vez son almacenadas en los nodos, si se trata de una red y son utilizadas para proteger el nivel inmediatamente inferior de claves, que en un entorno transaccional suelen denominarse claves de sesión.

Las claves de sesión son las de más bajo nivel siendo utilizadas únicamente para proteger datos, permaneciendo activas mientras que los datos que han cifrado están en

forma de criptograma, esto significa, que las claves de sesión estarán activas solamente mientras dura la sesión de comunicaciones. Las claves maestra y submaestra son generadas por un responsable de seguridad. Las primeras permanecerán en claro ya que no hay claves de nivel superior a éstas, sirven para cifrar a las claves submaestras. Según Everton, cada dispositivo de la red del sistema criptográfico debe tener su propia clave maestra, y cada nodo, en ésta visión estructurada, debe tener las claves submaestras cifradas, tanto la suma como la de los nodos con los que se comunica.

Everton sugiere que las claves maestras y las claves submaestras cifradas se transporten a los nodos por un medio seguro, probablemente no por la red, entregando el fichero de claves al representante responsable de seguridad en cada uno de los puntos. Permaneciendo ocultos en un sitio seguro, como una caja fuerte.

Este procedimiento es transparente al usuario final y exceptuando al responsable de seguridad en cada nodo, no hay nadie que tenga que manipular las claves.

3.29.2 SOLUCIÓN MEDIANTE CLAVES CENTRALIZADAS.

Ha sido propuesta por IBM y tiene algunas similitudes con la propuesta de Everton. Se basa en la existencia de una clave maestra en el ordenador central (Host Master Key, HMK). Hay un criterio de centralización de tal modo que las restantes claves es generan en ese ordenador, por razones de economía, siendo transferidas a los demás sitios donde se necesitan. La HMK se almacena en claro en el dispositivo que efectúa el cifrado del ordenador central, impidiendo su acceso por no autorizados. Cada terminal atendida por éste ordenador necesita su propia clave maestra de terminal (TMK), almacenada en claro en su dispositivo de cifrado . El ordenador también guarda una copia cifrada de cada TMK.

El protocolo seguido por un terminal que solicita una sesión de comunicaciones cifradas con el ordenador central, comenzará con la respuesta a ésta petición de una clave compuesta por una secuencia de dígitos binarios de naturaleza pseudoaleatoria. A partir de éste estado inicial se hace evolucionar un registro desplazamiento, produciendo la secuencia deseada.

Esta secuencia puede considerarse como clave de sesión cifrada, por haber sido generada fuera del dispositivo de cifrado. Al introducirla al dispositivo, éste la descifra usando la HMK, la almacena para uso posterior , y finalmente la vuelve a cifrar usando la TMK para transmitirla al terminal. A la recepción por parte del terminal, su dispositivo de cifrado la pone en claro utilizando la TMK, existiendo ya la misma clave en el dispositivo de cifrado en la computadora. La computadora posee a su vez las TMK cifradas con otra clave especial denominada "variante".

Respecto a la distribución de claves, la regla general es que las claves que están fuera de un dispositivo de cifrado deben estar siempre en forma de criptograma, siendo la única excepción las HMK y TMK que deben ser transportadas y creadas en claro, ya que no hay claves de orden superior que puedan cifrarlas y descifrarlas. Esto implica un manejo totalmente secreto.

El sistema es transparente al usuario final, relevándole de la responsabilidad del manejo de claves, ya que las claves de sesión pueden ser transportadas por la red, cifradas por la TMK. La distribución de claves a más alto nivel deben ser por medios extraordinariamente seguros.

3.30 FIRMA DIGITAL: ESQUEMA PSO.

Reciba el nombre de firma digital aquel procedimiento de seguridad que permite al autor de un mensaje representando en forma digital binaria, firmarlo con las mismas propiedades que tiene la firma de un documento escrito sobre papel, a la manera convencional. Sin éste método no sería posible el desarrollo y crecimiento que se ha experimentado en los sistemas de proceso distribuidos o redes de terminales interactivas. Las propiedades que se exigen a la aplicación de firma digital efectuada con métodos de cifrado son las siguientes:

a) Imposibilidad de falsificación. Solamente el autor de la firma será capaz de crearla.
b) Autenticidad. El proceso deberá incluir un fuerte método de verificación de autenticidad que demuestre de una manera concluyente que la firma es válida.
c) No rechazo. El autor del mensaje firmado no debe recusar su autoría.
d) Bajo costo y alta conveniencia que hagan atractivo su uso cuando se necesite.

Desde el punto de vista del receptor, la firma digital proporciona la prueba legal de que el mensaje ha sido emitido por el emisor cuya identidad es la supuestamente conocida.

Los sistemas convencionales de certificación de autenticidad son capaces de evitar falsificaciones de terceras partes, ajenas al sistema o a la comunicación establecida, pero no son capaces de promover una discusión entre el emisor y el receptor acerca de la legitimidad del mensaje.

La idea principal de la firma digital es que solamente una persona pueda producirla y cualquiera pueda reconocerla, del mismo modo que ocurre en la práctica comercial

corriente. La inclusión de nuevas aplicaciones, como el correo electrónico, obligan a buscar métodos de firma de mensajes electrónicos.

El receptor del mensaje exige la prueba de que la información ha sido enviada realmente por el emisor que dice enviarla. Como se ve, la firma digital requiere un control estrictamente más fuerte y seguro que la certificación de autenticidad, donde el receptor puede verificar que el mensaje proviene del punto asignado al emisor, pero no está seguro de que sea él quien la envía. Con la firma digital, el receptor se convence de que el emisor realmente envío y firmó el mensaje.

La firma digital exige una dependencia del mensaje y del firmante, para evitar la posibilidad de que el receptor pueda modificar el contenido e incluso la firma. Se trata también de evitar la manipulación asignando firmas a mensajes que no la llevan, o que llevan otra firma.

Los sistemas de cifrado que utilizan clave pública pueden suministrar una solución directa al problema de la firma digital, siempre que sean puestos en funcionamiento con un sistema de cifrado asimétrico mediante una función de un solo sentido.

El procedimiento de firmado digital puede también ser utilizado cada vez que un usuario hace una búsqueda en el directorio de claves pública, haciendo que el fichero público firme digitalmente sus mensajes a los usuarios garantizando aún más la seguridad del sistema secreto.

3.31 CRITERIOS DE SHANNON.

Shannon considera los criterios que deben cumplir así como las propiedades deseables que deben poseer los sistemas de comunicación secreta.

Shannon especificó cinco criterios para un sistema secreto en un entorno de comunicación mediante el uso de criptografía.

El primero es relativo a la relación entre el grado de protección que se desea y la complejidad del cifrado y descifrado: la cantidad o grado de protección necesario, decidirá la cantidad de trabajo del sistema de cifrado y descifrado.

De aquí se puede inducir que a mayor grado de protección, más fuerte debe ser el cifrado y por tanto más difícil de vulnerar. Este principio está claramente orientado a dificultar la labor del criptoanalista.

El segundo trata de la elección de la clave de cifrado. El conjunto de reglas o clave que se usen para cifrar o descifrar debe ser de tamaño pequeño.

El tercer criterio añade la conveniencia de que los sistemas secretos sean lo más simple posibles en las operaciones de cifrado y descifrado, disminuyendo así las posibilidades de error.

El cuarto criterio está relacionado con la propagación de errores, sugiriendo que un error de transmisión que ocurra durante la comunicación de un criptograma no debe alterar necesariamente a todos los caracteres del mensaje, es decir, no deben propagarse los errores ocasionales de transmisión.

El quinto criterio de Shannon establece que la longitud del criptograma no debe ser mayor que la longitud del mensaje en claro al que pertenece.

Dada la fecha en que fueron enunciados estos criterios, no se contempló la posibilidad de que una computadora pudiera realizar los procesos de cifrado y descifrado, así como la existencia de sistemas secretos de almacenamiento. La disponibilidad de una gran potencia de cálculo, de almacenamiento, y de diferentes modos de representación codificada de la información, obliga a efectuar una revisión de los criterios de Shannon, para actualizarlos se transforman en las siguientes reglas.

a) La cantidad de seguridad deseada, determina la cantidad de trabajo y tiempo de cálculo necesario para vulnerar el mensaje cifrado.
b) Las claves utilizadas deben ser de fácil construcción, lo más cortas posibles, fáciles de alimentar, modificar y consecuentemente que ocupen poca memoria.
c) Las operaciones de cifrado y descifrado, conocida la clave deben implicar la menor cantidad de cálculo posible.
d) Las claves y el sistema de cifrado deben ser tales que destruyan los parámetros estadísticos del lenguaje, o bien su estructura natural.
e) Los errores de transmisión en los criptogramas, no deben originar ambigüedades o pérdida del sentido en la información original, haciéndola inútil.
f) La necesidad de almacenamiento para los criptogramas no debe ser mayor que la necesaria para los mensajes en claro equivalentes.
g) El análisis de un criptograma tratando de vulnerarlo debe necesitar una cantidad de cálculo tal, que sea considerado como un problema intratable incluso con una computadora como apoyo.

3.32 CRIPTOÁNALISIS.

El criptoanálisis es aquella actividad que realiza el supuesto oponente, encaminada a obtener el mensaje en claro, y contempla el conjunto de técnicas que usualmente se utilizan para este fin, desde los análisis estadísticos hasta las técnicas computacionales y examen exhaustivo del espacio de claves y de mensajes. Las técnicas criptoanalíticas forman parte de una disciplina llamada criptología.

En una primera aproximación se establece inmediatamente que el trabajo de criptoanálisis requiere una vulneración del método de comunicación o de almacenamiento, obteniendo información. Si no se posee información cifrada el criptoanalista no puede trabajar. Todas las técnicas que el criptoanalista tiene a su alcance se basan en su aplicación a los criptogramas que son interceptados de algún modo en el sistema secreto de almacenamiento o de comunicación.

Cuando se diseña un sistema criptográfico hay que pensar en los diferentes tipos de ataque que pueden ser inferidos por el oponente, por eso, el primer y más importante punto es conocer que tipo de información podría disponer el criptoanalista en caso de una vulneración al sistema de comunicación o de almacenamiento. El peor de los casos para el criptoanálisis es el de que solo se dispone del material de información interceptado, un ligero conocimiento general del sistema y alguna orientación acerca de la naturaleza de los mensajes. En esta situación, las posibilidades de ataque se limitan al conocimiento de las propiedades estadísticas del lenguaje y al determinadas palabras probables. Esta limitación es la amenaza más débil a que está sujeto un sistema secreto, y cualquier sistema que sucumba a ella deberá ser considerado como totalmente inseguro. Esta situación es denominada como ataque en base a criptograma. Es evidente que la utilización de cualquier de los métodos criptográficos que elimina la naturaleza estadística del lenguaje, es apropiada para ésta situación, y en general, para cualquiera, ya que la técnica

criptoanalítica de análisis estadístico será una de las primeras pruebas del criptoanálisis en su intento de vulneración.

En ocasiones, cuando la naturaleza del lenguaje es tal que se dan muy frecuentes repeticiones de palabras o frases, como en un sistema criptográfico usado para proteger programas, el criptoanalista concede cantidades considerables de texto en claro y de criptogramas a que da lugar, posibilitándose la situación denominada ataque por mensaje en claro conocido, el cual es una natural consecuencia de los lenguajes con estructura muy rígida, como los de programación. En éste tipo de lenguaje o en los altamente estructurados, como los normalmente usados en informática de gestión para representar la información en ficheros, está garantizado un conocimiento a priori de alguna fracción de los mensajes en claro. Un ataque de este tipo no es siempre posible, pero su aparición es lo frecuentemente suficiente como para que un sistema que sucumbe a él, sea considerado como inseguro.

Una posición aún más fuerte del criptoanalista le permite disponer de criptogramas correspondientes a mensajes en claro escogidos por él. Su problema ahora es determinar la clave para usarla en posteriores cifrados o descifrados. Esta posición se denomina ataque en base a texto en claro escogido. Otra posición, la mejor de todas para el criptoanalista es la de seleccionar a voluntad el texto en claro o el criptograma que intercepta, denominándose a esta situación ataque en base a texto escogido.

Existen dos modos diferentes bajo los que un sistema secreto puede estar seguro. Un sistema incondicionalmente seguro y un sistema computacionalmente seguro, son dos modos diferentes bajo los que un sistema está protegido de las técnicas del criptoanálisis.

Si la cantidad de información que el criptoanalista tiene a su alcance es insuficiente para averiguar la clave, y consiguientemente insuficiente para averiguar las transformaciones a realizar durante el cifrado o descifrado, el criptoanalista no podrá llegar a ningún resultado útil aunque dispusiera de una potencia de cálculo ilimitada.

En otra situación, aunque el criptoanalista dispusiera de información suficiente para encontrar una solución única al problema criptográfico, no se garantiza que pueda encontrarla con unos recurso de cálculo limitados a los que actualmente proporcionan las computadoras existentes. Los diseñadores de sistemas criptográficos establecen un compromiso entre los costos de operaciones de cifrado y descifrado que deben ser sencillos de realizar conociendo la información necesaria, y las operaciones de criptoanálisis que deben ser muy caras y muy complejas de realizar.

Al criptoanalista solo le queda la posibilidad del método de prueba y error mediante análisis exhaustivo y utilización de los recursos de cálculo a su alcance. En este estado de cosas se deben considerar las necesidades de tiempo de cálculo y de memoria que son precisas para una búsqueda o análisis de un criptosistema mediante la técnica de análisis exhaustivo. A estas consideraciones se les suele contemplar con el nombre de compromisos entre tiempo y memoria, ya que se supone que van a ser tratados en una computadora.

Muchas tareas de este tipo, de búsqueda total, como en los problemas "mochila", permiten un compromiso entre memoria y tiempo, es decir, si existiesen N soluciones sobre las que buscar, sería posible que la solución se encuentre en T operaciones (tiempo) con M palabras de memoria, consumiendo el producto T x M. El criptoanalista deberá considerar la posibilidad de la búsqueda exhaustiva usando más o menos memoria mediante la búsqueda en tablas previamente almacenadas, o bien sin ningún tipo de búsqueda, lo que resultará en mayor tiempo de cálculo.

El criptoanálisis permite cualquier punto intermedio entre el compromiso tiempo-memoria, y será importante estudiar qué posibilidades existen en el citado compromiso. Hay estudios realizados para algunos sistemas de cifrado, como el efectuado para el DES, en el que se plantea un estudio exhaustivo del cifrado mediante el uso de una máquina que podría realizar el trabajo en minutos. Se han realizado algunos estudios también de compromiso tiempo-memoria en el caso de los cifrados que usan el problema de la "mochila".

3.33 APLICACIONES DE LA CRIPTOGRAFÍA.

Es más importante la criptografía como herramienta de protección en las redes de teleproceso que en los sistemas de tiempo compartido. La razón es que en un sistema de tiempo compartido, los datos más importantes están centralizados y pueden ser protegidos físicamente. Sin embargo, en una red, distribuida geográficamente, los nodos juegan un papel fundamental, ya que la información debe ser transmitida a través de los enlaces de comunicación, y en este caso la protección física no es posible, porque en cada nodo habría que proceder a la misma, resultando seguramente antieconómica.

Existen dos maneras según las cuales la criptografía puede aplicarse a las redes, dependiendo si la protección de la información es responsabilidad del usuario o de la red. En el cifrado a nivel de enlace de comunicaciones, un mensaje que viaja a través de la red, se cifra y se descifra mientras éste decide el camino a tomar.

El segundo método es el cifrado a niveles finales, en el cual cada mensaje es cifrado en la fuente y descifrado en el destino, con la ventaja de que los datos son protegidos a través de todos su viaje por la red. Por supuesto, las direcciones de destino no pueden ir cifradas.

El cifrado a niveles finales tiene la desventaja de que se necesitará un sistema de intercambio seguro de claves entre cada par de usuarios, a no ser que se utilice un esquema de clave pública. En el cifrado a nivel de enlace cada usuario necesita una clave para comunicarse con su nodo local.

Respecto a los sistemas secretos de almacenamiento, el procedimiento inmediato para la aplicación de la criptografía es el de cifrar el fichero objeto de protección con alguna clave que generalmente se presenta de forma cifrada con una clave maestra.

Si se guarda durante mucho tiempo dentro del sistema, se debe pensar algún sistema de protección, pues el uso de ese valor por parte de personas no autorizadas, puede violar la información almacenada. Este problema puede evitarse sin más que utilizar una clave personal que no permanezca almacenada en el sistema, aunque éste método no proporciona transparencia al sistema criptográfico, ya que obliga al usuario a la responsabilidad de manejo de claves. Si se trata de información almacenada que es compartida entre varios usuarios, la única solución práctica puede ser la del manejo automático de las claves por el sistema.

En conclusión la idea básica es la de usar los sistemas de cifrado con claves cifradas, de tal modo que permanecen en la cabecera del fichero y en el ordenador, necesitándose de ambos para poder recuperar la información. Además se trata de evitar las claves maestras usadas en comunicación, para evitar posibles vulneraciones en caso de transporte de datos de un lugar a otro.

El cifrado a niveles finales suministra un nivel mayor de seguridad, ya que los datos no se descifran hasta que alcanzan su destino final, siendo por tanto preferible este tipo de utilización de la criptografía para aplicaciones tales como correo electrónico, o transferencia electrónica de fondos en un sistema bancario. Sin embargo, en esta modalidad, como las

direcciones de destino van en claro, es más fácil someter a la comunicación a un ataque inyectando información.

Con el cifrado a nivel de enlace de datos están más expuestos a la vulneración, ya que en los nodos intermedios permanecen en claro, aunque la dirección de los destinos finales puede ir cifrada a través de la red.

Cada trama que es enviada a través de un enlace, posee un campo de cabecera y otro de datos. La cabecera contiene el destino final del mensaje, cifrado con la clave del enlace, además de la información de control usada por el sistema de comunicaciones. Si el canal se utiliza para más de una conexión, la cabecera deberá contener en claro la fuente y el destino del mensaje.

Un paquete que llega a un punto, contiene información en claro e información cifrada, con lo que el dispositivo receptor debe ser capaz de operar en ambos modos, en claro y cifrado , ya que los símbolos a que dé lugar el texto cifrado deben ser transparentes al dispositivo.

Aún así, un oponente puede verificar actividad en el canal y en el punto receptor y deducir que recibe información. Para evitar esta deducción se puede inyectar en el canal tráfico falso, aunque esto puede suponer un costo adicional.

PRONTUARIO.
CAPÍTULO 3.

La necesidad de utilizar el encriptamiento se deriva de la importancia de cierta información que manejan algunos usuarios de redes computacionales, y de la necesidad de transportarla de un lugar a otro usando las mismas redes sin que algún oponente o agente ajeno a nuestros intereses pueda modificarla, substituirla, captarla o evitar que llegue a su destino. Todo esto se complica por dos razones principalmente: el usar algunos medios públicos para transportar la información y la creciente facilidad de adquirir equipo computacional en forma masiva para distintos usos, debido al abaratamiento de los precios por la producción en serie.

Para proteger la información se utilizan distintas técnicas criptográficas, pero básicamente su funcionamiento es el siguiente: todo sistema posee dos funciones que son las de cifrado y descifrado, las cuales actúan sobre nuestra información y las transforman, no importa que se conozcan las funciones por cualquier persona, pero lo que se debe guardar celosamente es la clave con la cual se puede descifrar la información.

Ahora bien, la criptología no es obra de la ciencia moderna, ya desde épocas antiguas se manejaba la protección de la información, un método que vale la pena mencionar es el Método Cesar, utilizado por los romanos.

Algo que impulsa a la fuerza a la ciencia es la guerra y en éste caso no fue la excepción, durante la Segunda Guerra Mundial se le dio gran importancia al encriptamiento de información, el resultado fueron: en primer lugar la máquina de cifrar Hagelin C-48 y las máquinas de rotor.

Como siempre estamos en busca de lo más eficiente, en este caso estamos en busca de lo más seguro e indescifrable, para lo cual fue necesario hacer estudios sobre análisis de recursos de cálculo y la dificultad de resolución de un criptograma en base al tiempo y al espacio. Fue necesario clasificar los problemas que se pudieran enfrentar y algunos son: Problemas P, Problemas NP, Problemas NP-completos, etc.

Algunas herramientas que son valiosas para las transformaciones son las operaciones aritméticas como la suma, resta , división, multiplicación, etc. debido a que son operaciones inversas perfectamente definidas.

De igual forma podemos mencionar las facilidades que nos presentan las operaciones lógicas para el funcionamiento de nuestro sistema criptográfico, ya que son operaciones simples y el resultado es un producto que aporta parte de la seguridad requerida.

La ciencia criptográfica actual utiliza algunos procedimientos, los cuales deben ser de tratamiento simple, y generalmente están basados en los procedimientos como lo son: operaciones lógicas, registros de desplazamiento, manipulación de bits, permutaciones y substituciones.

Los sistemas de cifrado apartan en dos grupos a los algoritmos que se utilizan y son los cifrados en bloque, el cuál trabaja con bloques de bits con longitud predeterminada, y el segundo grupo es el de cifrados en flujo, que como su nombre lo indica trabaja con uno o más bits y continuamente se van desplazando dando lugar a nuevos bits.

Un algoritmo que merece mención aparte es el conocido como DES (Data Encryption Standard), el cual tuvo una aceptación a nivel mundial gracias al apoyo que

recibió del NBS (National Bureau of Standards) del Departamento de Comercio de Estados Unidos. Fue creado en 1977 y el cuál consiste en 16 pasos o ciclos de substitución o permutación de bits, controlados por una clave, fue basado en un trabajo realizado por Horst Feistel.

Los cifrados se clasifican como simétricos y asimétricos, los "antiguos" son simétricos y se les conoce así debido a que ambos lados del sistema de comunicación guardan y utilizan la misma clave, lo que podría perjudicar nuestra seguridad. Los más "modernos" son los asimétricos y éstos se conocen así debido a que el emisor y el receptor usan claves distintas.

Existen varias proposiciones de cifrado conocidas como cifrados "mochila", de las más importantes son las propuestas por Merkle, Hellman, Shamir y Lempel. Algunos son especialistas en la verificación de autenticidad, mientras que otros pueden ser utilizados en cualquier sistema cuyo fin sea proteger su información.

A mediados de la década de los 70 surgió un concepto dentro del área, los sistemas de clave pública, cuyo funcionamiento se basa en el esquema de un sistema de comunicación privada que emplean un directorio de claves públicas, de tal modo que cada usuario fija un procedimiento de encriptamiento para que sea usado por otros usuarios cuando cifren mensajes que vayan dirigidos a él, mientras guarda en secreto su propio procedimiento de descifrado.

La firma digital es un procedimiento de seguridad que permite al usuario representar su autenticidad mediante una cantidad en forma binaria, la cuál tiene las mismas propiedades que una firma convencional sobre papel.

Shannon trata de generalizar las características que deben cubrir todos los sistemas de seguridad para que sean considerados perfectos en cuanto a la transmisión de datos encriptados. El expone cinco criterios.

El criptoanálisis es aquella actividad que realiza nuestro oponente, cuya finalidad es obtener el mensaje en claro, y contempla el conjunto de técnicas usadas para este fin. Está claro que el éxito del criptoanálisis es la vulneración del método de comunicación.

CAPÍTULO 4

ANÁLISIS DE IMPLEMENTACIÓN DE UN SISTEMA DE ENCRIPTAMIENTO.

4.1 LOS PRIMEROS SISTEMAS DE ENCRIPTAMIENTO MÁS UTILIZADOS.

El teléfono es un medio de excesiva conveniencia para comunicarse. Que placentero y simple es levantar un auricular, hablar con otra persona y arreglar todo en una sola conversación; mucho más fácil que enviar mensajes escritos. Pero el teléfono es notoriamente susceptible a intervenciones, y su descendencia, el radioteléfono lo es aún más. El solamente intervenir una línea puede permitir el acceso a una conversación telefónica, y solo un radio es necesario para escuchar plática radiotelefónica, hechos que espías siempre han aprovechado para sus fines.

La medida de protección más obvia es hacer códigos para las conversaciones, y esto ha sido hecho por casi todos aquellos que hemos usado el teléfono. El rango de códigos puede ir desde hacer referencias a sucesos a modificar lo que hablamos por medio de un caló o jerga común entre ambas partes de la conversación. Menos común, pero más útil es el cifrar un mensaje en un sistema arreglado previamente y descifrarlo después letra por letra. Otro método que estuvo muy de moda es el hablar en un lenguaje extranjero.

Los Estados Unidos utilizaron el último método a toda escala en ambas Guerras Mundiales, haciendo uso de un recurso que virtualmente ningún otro oponente tenía: lenguas tan recónditas que nadie más en el mundo los entendería. Los dialectos de Indios Americanos, los cuales estaban aislados geográfica y lingüísticamente. En 1918, el Capitán E. W. Horner ideó este sistema. Se probaron varios dialectos y el más útil fue el Navajo

por varias razones: su tribu consistía de más de 50,000 personas, lo cual aportaba un buen número de encriptadores; además de ellos únicamente 28 personas que no eran Navajos

podían hablar el dialecto, y nadie de ellos era Alemán o Japonés y la tercera razón era que la dificultad de la lengua es tal que es imposible falsearla.

El antropólogo Clyde Kluckhohn dice que el hablar en Navajo es hablar con una nitidez casi pedante, y aquellos que lo aprenden de adultos pueden ser descubiertos por los oídos de los Indios, quienes dicen que existe una mínima vacilación al pronunciar las raíces de las palabras. Un rasgo de su complejidad se basa en la insistencia de sus formas verbales. Dichas raíces se refieren a los objetos sobre los que se hablan. Una forma verbal totalmente diferente se refiere a la manera de conocer los eventos.

Un criptosistema como ese era bastante seguro para su época; no era sorprendente ver a los indígenas en los puestos de comando y en los centros de transmisión. El uso de éstos codificadores floreció de tal forma que aumentó su uso de 30 a 420 al final de la Guerra.

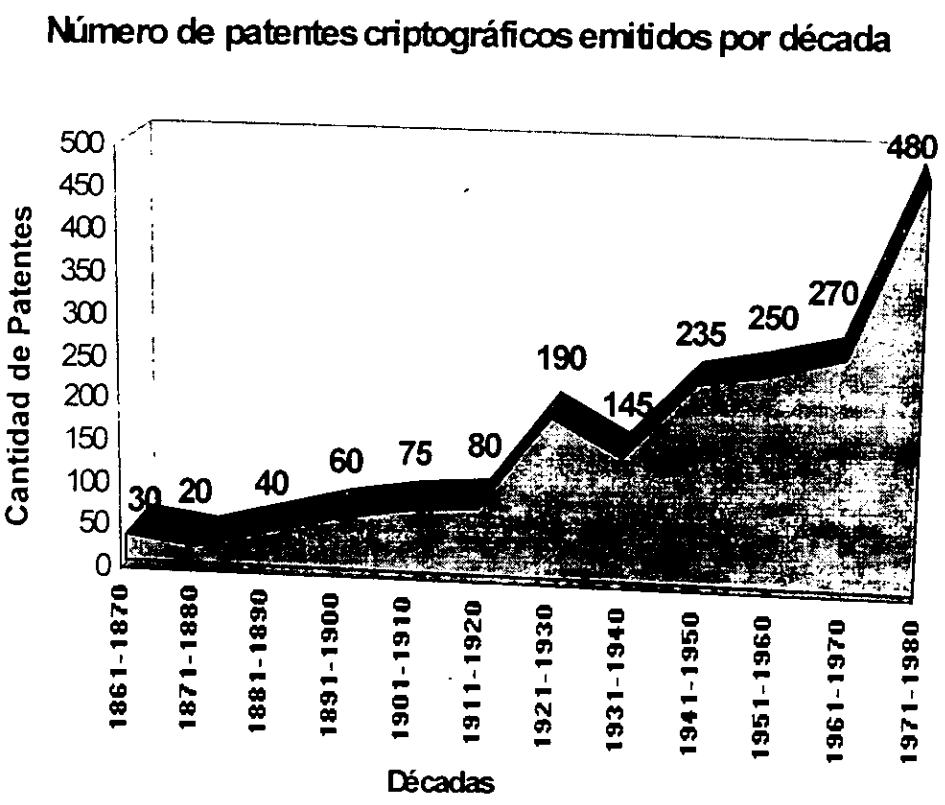
Codificación lingüística, códigos de jergas o doble sentido era usado por el hombre como máquina codificadora, pero fue relegado por una verdadera máquina: el ordenador. Estas dos formas de clandestinidad oral, la humana y la mecánica, corresponden a las dos formas básicas de criptosistemas. La codificación humana transmuta los elementos de la Lingüística en formas secretas. Los ordenadores trabajan sobre partículas de texto cortado sin importar las funciones lingüísticas. De ésta analogía los métodos de modificar el lenguaje por medio de ordenadores se llama cifonía compuesto de cifrado y telefonía. El campo de las comunicaciones secretas de voz puede ser llamado como criptofonía.

A pesar de esto, a partir de la Segunda Guerra Mundial, los ordenadores empezaron a tener un uso masivo, dispositivos que aseguraban rudimentariamente la comunicación telefónica existen casi desde que se inventó el teléfono. El primero de estos aparatos fue patentado el 20 de diciembre de 1881, por James Harris Rogers.

NÚMERO DE PATENTES CRIPTOGRÁFICOS EMITIDOS POR DÉCADA

1861-1980

1861-1870	30
1871-1880	20
1881-1890	40
1891-1900	60
1901-1910	75
1911-1920	80
1921-1930	190
1931-1940	145
1941-1950	235
1951-1960	250
1961-1970	270
1971-1980	480



Otros métodos posteriores operan directamente sobre la voz, utilizando transposición, substitución y otro tipo de cifrados. En la mayoría de los sistemas de substitución, se selecciona uno de tantos componentes que constituyen el habla y lo alteran. Generalmente se escoge la frecuencia y el volumen. Aquí la frecuencia se refiere al número de veces que las cuerdas vocales vibran, se declaran en ciclos por segundo o c.p.s.. A causa de los órganos vocales, el habla combina varias frecuencias y cada sonido tiene su propia combinación distintiva de frecuencias.

La cifonía busca arreglar esto combinando las frecuencias de los sonidos. Lo puede hacer porque el teléfono primero convierte estos sonidos en corriente eléctrica fluctuante,

la cual, los tubos, los switches, los filtros y los circuitos que componen un ordenador lo modifican de acuerdo a los principios de electricidad. Debido a que la corriente puede ser transformada en un gran número de formas, muchas de estas pueden dañar significativamente la voz.

La modificación más simple es la inversión. Prácticamente voltea la voz. A pesar de que los rangos de la voz van desde los 70 c.p.s. a 7,000 c.p.s., el teléfono por razones de ingeniería puede transportar sonidos en un rango de 300 c.p.s. a 3,300 c.p.s. El ancho de banda que es invertido es de 0 a 4,000 c.p.s.. Un tono de voz de 300 c.p.s. emergerá desde el inversor de 3,300 c.p.s. y viceversa. Utilizando este método se altera bastante la voz y no tiene fidelidad, debido a que la inversión se pivotea en el centro del ancho de banda, lo que significa que los tonos en ésta área saltan y rebotan en un rango bastante pequeño.

Otra técnica simple es el cambio de banda. Este es una especie de substitución Cesar telefónica, en la que todas las frecuencias son "empujadas" ascendente y descendentemente en cierta distancia, con ciertas porciones de la señal reentrando en el fondo o en la cima.

La división de banda la parte en bandas más pequeñas y las intercambia, identificándolas por rangos de subbandas asignándoles variables, las cuales organiza el ordenador. Entre más veces y más rápido cambie la reorganización el sistema será más seguro.

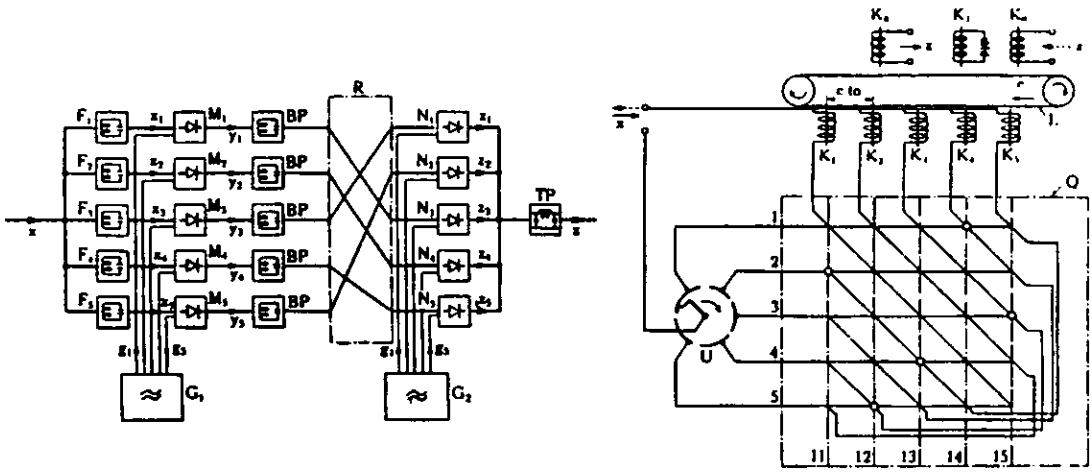


Figura 35

Ordenadores de voz. En el diagrama de la izquierda vemos un divisor de banda. La señal x de voz entra y es dividida en 5 bandas de frecuencia por los filtros F, modulada por los moduladores M con una frecuencia auxiliar proveniente del generador G, atraviesa los filtros paso banda BP hacia el dispositivo codificador R, donde las bandas son intercambiadas, pasadas por los moduladores M y combinadas en el filtro TP, obteniendo una señal reordenada Z. A la derecha tenemos un reordenador por división de tiempo. La señal X de voz entra al conmutador U, el cual la divide en cinco porciones y las envía a través de las conexiones codificadas Q en un orden hacia las cinco cabezas grabadoras K. Por ejemplo, el segmento uno se va a la cabeza K4. Este procedimiento se graba en una cinta sin fin L. La cabeza elegida K6 envía la señal modificada Z al magneto K el cual la borra. Para decodificar, la cabeza k8 coloca la señal reordenada entrante Z en la cinta y el proceso es revertido.

El sistema de enmascaramiento prácticamente entierra la voz. Música de algún reproductor puede ser eléctricamente sobrepuesta para ahogarla. El ordenador del decodificador debe tener una grabación de la misma música y reproducirlo sincronizado con el del transmisor y substrae la señal de música, dejando únicamente la voz. Estos sistemas utilizan lo que se conoce como cifrados nulos, los cuales insertan el mensaje verdadero dentro de un movimiento de símbolos adulterados. Otro sistema es la modificación de forma de onda: una corriente eléctrica opera sobre la corriente eléctrica de la voz para producir variaciones rápidas y extremas en la amplitud de la señal

transmitida. Para ilustrar esto consideremos que se utiliza el control de volumen de un reproductor y que en un instante se encuentra en el mínimo volumen y en el siguiente instante cambia hasta el máximo. En el decoficador, una corriente sincronizada idénticamente revierte los efectos.

Todos los cifrados transforman el habla en el dominio de la frecuencia, a lo largo del eje vertical. Ninguno se extiende en el eje horizontal o dominio del tiempo. Los sistemas que cifran cambiando las relaciones temporales del flujo de la voz deben preservarla momentáneamente para permitir la transposición.

El ordenamiento por división de tiempo, corta el flujo de la voz en milisegundos y las mezcla. Se logra grabando la voz y después eligiendo fragmentos en un orden confuso. El resultado es una revoltura de sonidos. El decodificador debe tener el mismo número de grabadoras que utilizó el codificador para acomodar después la señal en el orden correcto. Otro método es el reproducir la conversación más rápido y más lento de lo normal a lo largo de toda la conversación haciendo combinaciones que el codificador haya seleccionado.

La mayoría de los ordenadores fueron inventados en los años veinte y treinta por ingenieros de compañías de radio y teléfono en expansión. Se convirtió en una necesidad ya que algunas personas, por accidente y otras a propósito comenzaron a escuchar conversaciones; para prevenir esto la American Telephone & Telegraph Company colocó un inversor , y aunque sirvió al principio, algunos amateurs consiguieron nulificar esta acción para continuar con sus intervenciones.

Sabiendo esto, A. T. & T., para mejorar su seguridad instaló divisores de frecuencia, dándole preferencia a sus canales de radioteléfonos transatlánticos. Este dispositivo fue bautizado con el nombre de A-3, y fue tal su desempeño que el Presidente Roosevelt lo

utilizaba para sus conversaciones poco antes de la Segunda Guerra Mundial y aseguró que era muy de su agrado. Quienes inmediatamente intentaron conocer como trabajaba el sistema y descifrar las conversaciones entre Estados Unidos e Inglaterra fueron los alemanes, quienes en Septiembre de 1941 lograron hacerlo y para Marzo de 1942 también tenían sus teléfonos codificados. Como se dieron cuenta fue gracias a sus oficinas de correo.

Poco antes de que los alemanes se plantearan el objetivo de la decodificación telefónica, El Comité de Investigación de la Defensa Nacional (N.D.R.C.), dedicó un grupo a la investigación de esta área, parte para romper con cifrados ya establecidos y otra parte para evaluar nuevas propuestas. El N.D.R.C. contrató a A.T.T. para que realizará la mayor parte del trabajo y así lo hizo. A cargo estaba el Ingeniero Walter Koening Jr., quien decía que el mejor y más común aparato para resolver cifonía era el oído humano, ya que era sorprendente como puede tolerar o aún ignorar sorprendentes cantidades de ruido no lineal, con distorsión de frecuencias, componentes mal puestos, sobreimposiciones y otras formas de interferencia. De esta forma se puede obtener la información parcial o casi totalmente y reducir el retraso de decodificación notoriamente, de hecho ellos probaron el teléfono A-3 y al escuchar algunas veces la misma conversación se pudo descifrar el 47% de la conversación, debido a que el habla contiene más elementos de los que necesita para ser entendido.

Koening dijo que existían muy pocos sistemas seguros para transmitir voz; tal vez se podría hacer alguno muy complejo pero el problema se haría presente cuando se tratara de convertir la voz a su forma original. Claro que el oído no puede diferenciar con exactitud todas las frecuencias, pero con la invención del espectrógrafo de sonidos el criptoanálisis se facilitó bastante. Este aparato grababa los sonidos de la voz en papel como una serie de líneas horizontales representando las frecuencias principales. En el habla normal las líneas

aparecen y desaparecen, ascienden y descienden en patrones que fluyen como las frecuencias lo hacen. En el habla codificada los patrones normales son distorsionados.

La examinación del espectrograma ilustra el tipo de codificación que se realizó, la solución se convierte en un juego de rompecabezas donde se divide gráfica a lo largo de todo el tiempo de ordenamiento y reagruparlos para recrear el patrón de flujo del habla normal. Todo esto fue de gran ayuda en la guerra contra los japoneses.

Koening y su equipo analizó un sistema que combinaba ordenación por división de tiempo y división de banda, el cual era de manufactura inglesa y se llamaba 2-D, operaba en los ejes de frecuencia y tiempo, con ayuda del espectrógrafo se derrotó a este dispositivo. La reconstitución de los patrones del habla con pequeños rectángulos que mostraba el espectrógrafo era una tarea aburrida pero rápida, a un equipo de seis hombres le tomaría dos o tres horas el descifrarlo. La experiencia mostró que al hablar con voz baja y monótona se complicaba un poco la labor, ya que se alteraban los patrones de la voz, además un poco de ruido era agregado artificialmente, variar elementos para eliminar periodicidad, etc., el ruido no molestaba al oído pero si confundía al espectrógrafo.

La cifonía nunca alcanzó el grado de seguridad de las comunicaciones escritas, casi al término de la guerra Roosevelt y Churchill cambiaron de conversaciones telefónicas a conversaciones por teletipo, utilizando el encriptamiento aportado por una pequeña caja llamada "Telekrypton".

Una oficina creada por Estados Unidos fue la COMSEC (Office of Communications Security), cuyas funciones abarcaron la cifonía, a través de los laboratorios Bell quienes hicieron grandes desarrollos de proyectos. Mejoraron notablemente los ordenadores que se usaron en la Segunda Guerra Mundial, se empezó a utilizar lo que conocemos como PCM

(Pulse Code Modulation). PCM convierte la señal a una secuencia pulsos, algo así como la señal del teletipo. El número de pulsos por segundo varía con la frecuencia de la voz. Esta forma digital permite entrelazar muchas señales de voz en un mismo circuito, de esta forma incrementando la capacidad de la red telefónica.

El solo usar PCM aporta seguridad, ya que el equipo PCM necesita recobrar la secuencia a la forma de voz, su principal ventaja criptográfica yace en la facilidad y seguridad del cifrado en el modo digital. El ordenador puede cifrar la secuencia de unos y ceros. Las llaves pueden ser almacenadas en cintas metalizadas, manchas de luz y sombra en transparencias, tarjetas perforadas o bien pueden ser generadas por una computadora a una velocidad de 8,000 pulsos por segundo durante 30 o 60 segundos. Existe un problema con el PCM y es la sincronización, pero es mínimo, su principal cualidad es que casi no existe la distorsión de voz, en los ordenadores sí y los vuelve muy vulnerables.

Por todo esto el Departamento de Estado y la Fuerza Aérea utilizó PCM para sus mensajes ultra secretos, principalmente el sistema conocido como KY-9, desarrollado por la Agencia de Seguridad Nacional (NSA), debido a su eficiencia se utilizan también en París, Génova, Londres, Bonn, Berlín, Roma y la delegación de Estados Unidos en las Naciones Unidas. Puestos Aéreos de Comando poseían estos sistemas y a pesar de que las instalaciones terrestres fueran devastadas por un ataque masivo se podría contraatacar gracias a los KY-9.

El trabajo del ordenador va de la mano con la compresión de voz, multiplexando, estrechando el ancho de banda necesitado para el radioteléfono y sistemas de comunicación forzada. Todo esto apunta principalmente a atestar más mensajes en el sobrepoblado espectro electromagnético y más aún a proporcionar seguridad ya que solamente equipos especiales pueden recibirlos. Un sistema militar que combinaba

seguridad y economía era aquel que enviaba señales de teletipo a baja frecuencia y señales de voz a alta frecuencia en la misma transmisión. Las armónicas de la señal del teletipo se derramaban sobre la frecuencia de la voz, enmascarándola. El resultado es el sonido de una sierra con murmullos debajo de ella. El sistema receptor utiliza un circuito de retroalimentación, el cual substrae el teletipo y eleva las armónicas de la voz.

Los sistemas de compresión no ofrecen el 100% de seguridad en contra de intervenciones no deseadas. Lo que se utiliza en batallas de tanques, en el mismo frente y con las guerrillas, es el ordenador integrado al teléfono o sistema de radio, el cuál es ligero; claro que entre más robusto sea un equipo, ofrece mayor seguridad. El ejército investiga activamente con división llamada Rama de Seguridad de Voz, ubicada en el Fuerte Monmouth.

Una de las líneas más seguras si no la más segura, es la famosa línea caliente o "hot line" que conecta a Moscú y a Washington. En Génova, el 20 de Junio de 1963, los Estados Unidos y la entonces Unión de Repúblicas Socialistas Soviéticas firmaron un acuerdo en el que aceptaban la instalación de una línea cuya ruta es Washington-Londres-Copenague-Estocolmo-Helsinki-Moscú para el canal principal y un canal de radio comunicación cuya ruta es Washington-Tánger-Moscú como apoyo.

Cuando se instaló, ésta línea empleaba en la terminal estadounidense, el ETCRRM II (Electronic Teleprinter Cryptographic Regenerative Repeater Mixer II), el cual fue fabricado por la Standard Telefon of Kabelfabrik of Oslo, la subsidiaria noruega de la International Telephone and Telegraph Corporation, y se instaló en el Centro Nacional de Comando Militar en el Pentágono, con cuatro traductores, dos en inglés y dos en ruso, además de cuatro equipos iguales adicionales.

La línea comenzó a funcionar el 30 de agosto de 1963 y desde entonces, cada hora se mandan mensajes de prueba para verificar su funcionalidad. Todo esto para reducir el riesgo de una guerra ocurrida por accidente o por malas interpretaciones, según los deseos del Presidente Kennedy. Otros sistemas de seguridad infalible se encuentran en el automóvil presidencial y en el Fuerza Aérea 1 (Avión Presidencial). Todos estos equipos cambian sus códigos diario.

4.2 SEGURIDAD BASADA EN ENCRIPTAMIENTO PARA COMUNICACIONES EN LA RED DIGITAL DE SERVICIOS INTEGRADOS (ISDN).

En años recientes, ha habido un tremendo incremento transferencia de datos e información en las redes telefónicas y de computadoras. Esta información abarca desde simple correo electrónico hasta datos militares de importancia altamente compleja. En cualquier transferencia de datos, la seguridad de los mismos es una preocupación constante. Hoy en día la solución a estos casos es el usar redes privadas caras e ineficientes o bien rentar canales.

La evolución que tiene hasta el momento la ISDN, con su conectividad digital punto a punto provee una excelente plataforma para trabajar en red y confiar en las comunicaciones de datos. A continuación veremos como desarrollar e implementar metodologías para que funcione correctamente el encriptamiento de datos a transmitirse en la ISDN además de que no requieran actualizaciones en el equipo de conmutación. Esto hará parecer a la ISDN, pública como una red privada para el usuario que es exigente en su seguridad. Aún más, la comunicación de datos será proporcionada por canales de voz y datos conmutados.

Mundialmente usados los proyectos de encriptamiento y administración de llaves basados en los algoritmos del DES, criptografía de llave secreta, y en la criptografía de llave pública RSA, estos todavía son investigados para sus aplicaciones en el ambiente ISDN. Investigaciones iniciales demostraron que un acercamiento criptográfico híbrido, RSA para autenticación y DES para el encriptamiento, puede ser el más apropiado. Dichas investigaciones están en camino de desarrollar una implementación en hardware y software para la aproximación llamada HYBRID.

Mencionaremos algunos posibles estándares para la seguridad en ISDN que permiten a voz y datos ser transmitidos por medio de la BRI (Basic Rate Interface) de la ISDN, por supuesto encriptados para que el receptor adecuado lo pueda entender. Las ideas aquí presentadas pueden ser transportadas fácilmente a canales de paquetes conmutados y a la ISDN de Banda Ancha (BISDN).

Con el advenimiento de la ISDN , la posibilidad de una red mundial es real. Muchas aplicaciones que actualmente usan líneas privadas alquiladas harán parecer a la ISDN como una alternativa muy atractiva. Mientras que el crecimiento potencial de la ISDN crece exponencialmente y sus tarifas bajan, la oportunidad de reemplazar líneas alquiladas a alto costo será difícil de ignorar. La ISDN puede atraer más clientes y atenderlos más rápidamente, excepto que la seguridad en su funcionamiento pareciera que ha sido olvidada. Evidentemente, los inversionistas dudarán el dejar sus líneas privadas "seguras" por la "insegura" ISDN pública aunque sus costo sea mayor. De aquí la importancia del desarrollo de una metodología que asegure la confidencialidad de las transmisiones en la ISDN.

Con la llegada de los sistemas distribuidos de computadoras, transferencia electrónica de fondos y las redes de computadoras, la necesidad para la seguridad ha hecho florecer un número considerable de técnicas de encriptamiento. Desafortunadamente muchas corporaciones se han aproximado por fragmentos al intento de controlar y administrar sus comunicaciones por redes. Evidentemente, un estándar de seguridad comprensible debe ser adoptado para corregir muchas de las debilidades que permanecen en las tecnologías emergentes.

El foro de Usuarios Norteamericanos de la ISDN (NIUF) ha identificado una serie de aplicaciones pertenecientes a la seguridad en la ISDN. Los estándares propuestos requieren conexión de un dispositivo seguro como el Secure Telephone Unit (STU) III a una terminal adaptadora de ISDN (TA).

Algunas de las investigaciones actuales proponen estándares que requieren actualizaciones en el software de conmutación. Lo idóneo sería usar el software actual y consecuentemente no requerir cargos extra por parte de la compañía de teléfonos a aquellos usuarios que lo necesiten.

Los servicios básicos de seguridad requeridos para proteger una red son definidos en la norma ISO 7498-2:

1.- Autenticación: Es la verificación de la identidad intercambiada entre las entidades involucradas en la comunicación. ISO define dos tipos de autenticación: origen de datos (proporcionado por la fuente de datos) y la pura entidad (proporcionado por la terminal receptora). En general, el propósito de la autenticación es la protección contra un atacante que pretenda falsificar la identidad de alguien mas que sea responsable por algunas acciones

y tenga acceso a fuentes de datos en el sistema. Los mecanismos típicos de autenticación son: contraseñas (palabras clave) y firmas digitales.

2.- Control de acceso.- Se ocupa de prevenir usos no autorizados de los recursos de la red. El control de acceso apoya una política de autorización, la cual es un conjunto de reglas que define las condiciones bajo las cuales un usuario pueda tener acceso a algún objeto en particular. Los típicos mecanismos son: listas de control de acceso y etiquetas de seguridad.

3.- Confidencialidad.- Asegura que solo los usuarios para quienes la información está destinada, puedan conocerla, y previene que la información sea disponible a usuarios no autorizados. La ISDN reconoce cuatro categorías de confidencialidad:

a) Orientada a conexión. Provee protección a toda la información intercambiada.
b) No orientada a conexión. Para este tipo de transmisión.
c) Campo selectivo. Solo porciones seleccionadas de información son protegidas.
d) Flujo de tráfico. Protege el conocimiento de que la transmisión está tomando lugar.

Su mecanismo típico es el encriptamiento de llaves públicas o privadas.

4.- Integridad. Asegura que la información no es destruida, alterada, duplicada o reordenada por un usuario no autorizado. Esto se logra con mensajes previamente seleccionados.

5.- No repudiación.- Proporciona una prueba de la integridad de una transmisión con una garantía de origen y entrega (es equivalente a la entrega certificada por correo con un recibo entregado a la oficina postal). Este servicio previene a un transmisor de negar falsamente que ha enviado determinada información, o a un receptor de negar falsamente de haber recibido alguna información. La no repudiación es proporcionado por firmas digitales y mecanismos de notificación. En el sistema de firmas, los mensajes enviados son firmados y el receptor verifica la validez y la autenticidad del mensaje. En la notificación, el transmisor envía información al receptor por medio de un intermediario que sirve como testigo.

Para describir parte de su implementación lo dividiremos en dos partes:

1. A nivel de OSI: Tal vez la pregunta más hecha por los administradores de una red sea ¿en qué parte de la Arquitectura de Seguridad OSI debe residir dicha seguridad?, la respuesta escuetamente es colocarla en el nivel de aplicación. El control de acceso y la autenticación será proporcionada en el nivel de aplicación, a través del uso de tarjetas (smart cards) equipadas con una llave pública o secreta. El sistema verificará que el usuario sea el auténtico preguntándole que conteste un mensaje encriptado con su llave pública, y de esta forma solo el usuario podrá descifrarlo. Se evitan algunos tipos de ataques ya que la llave está confinada en la tarjeta. La confidencialidad y la integridad será interpretada en el nivel de red ya que esta opción parece ser la más flexible, los dispositivos de seguridad pueden ser instalados en el punto de referencia T de la siguiente gráfica.
2. Donde colocar el criptosistema. Muchas de las soluciones actuales al problema de las comunicaciones seguras en ISND se basan en la conexión de un dispositivo como lo es el Secure Telephone Unit (STU) III. Este dispositivo de seguridad se conecta a través de una terminal adaptadora. Aún más, si desea comunicaciones de facsímile seguras se

puede conectar el grupo facsímile III al dispositivo. Esta alternativa no es barata ni práctica, pero se recomienda cuando ya se ha hecho la inversión en esos equipos.

Existen dos propuestas para comunicaciones seguras en ISDN. La primera es asegurar las terminales adaptadoras de ISDN conectadas al bus. La ventaja de esta aproximación es la facilidad para implementarla con el software del DES y RSA, el cual puede estar residente en una estación de trabajo segura conectada a una terminal adaptadora. Si la velocidad le preocupa, se puede instalar un chip de DES en la estación de trabajo para hacer la encripción y usar el software RSA para firmar digitalmente y hacer la distribución de llaves. La desventaja de ésta implementación es que cada estación de trabajo que pueda requerir seguridad tendría que estar equipada con el hardware y el software necesario para proporcionar este servicio.

La siguiente figura propone un estándar, muestra un SNTTC (Secure Network Terminator Terminal Controller), una desventaja más es que este equipo debe estar relativamente cerca del equipo del comprador ya que es difícil mantener una instalación grande asegurada. La ventaja del sistema ilustrado abajo es que es más barato ya que solo el debe estar equipado con el software y el hardware. También permite utilizar la inversión ya hecha en TA´s. Esta configuración permite crear conjuntos de equipo seguro. Los teléfonos análogos también pueden ser usados seguramente si son conectados por medio de un TA a un SNTTC.

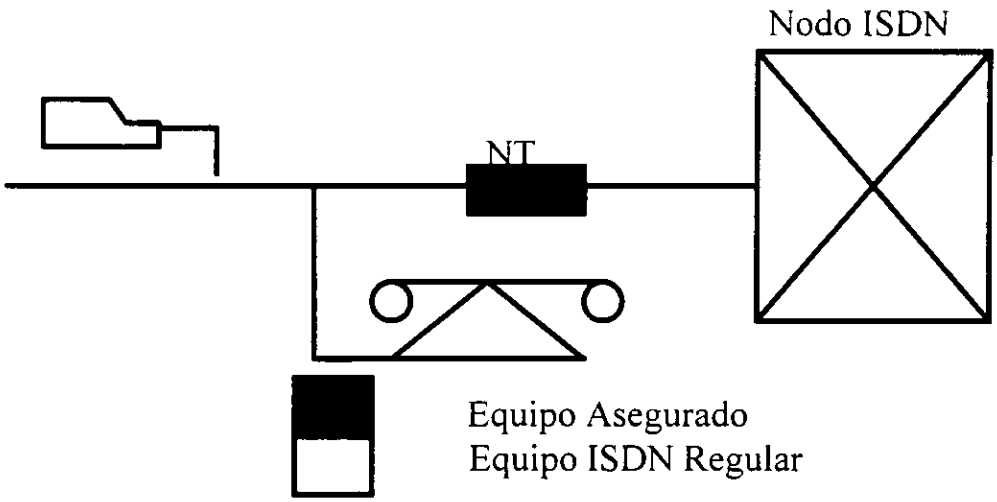


Figura 36

4.3 DESARROLLO DE UN DISEÑO CRIPTOGRÁFICO.

Es importante conocer como se concibe a nivel industrial el proyecto de un dispositivo criptográfico, es por eso que dimos seguimiento al método que realiza la Dutch Telecom Company (PTT Telecom BV), para la gestación de dicho dispositivo y conocer una visión general de dicho proceso..

Dicha empresa como su negocio principal la explotación de redes públicas de telecomunicaciones. Estos laboratorios dan apoyo para la resolución de muchos problemas involucrados con la administración de una red, como lo son consultas, estrategias y desarrollo de productos. En años recientes la centralización de la administración de redes se ha visto reflejado en la creación de centros de administración controlando distintos tipos de redes. La red telefónica es usada para dar servicio y administrar acceso de personal al centro de administración por medio de una terminal portable y un módem. Debido a las

partes vitales que existen en eso centros, un alto grado de seguridad debe ser mantenida en esas líneas telefónicas.

Desde hace años los laboratorios PTT estudiaron éste problema y la atacaron utilizando una variedad de productos entre los que destacan los módems criptográficos. Desde el punto de vista de la seguridad estas soluciones fueron suficientes. Combinando diferentes tipos de productos de seguridad, resultando en un número grande de distintos equipos, para un solo servicio de administración resultó ser un problema. El equipo resultó incompatible en su interfaz de usuario y tenía un uso limitado, además de grande y sobre todo caro en su uso y mantenimiento (diferentes proveedores, diferentes centros de mantenimiento, etc.).

Se hizo un estudio que consistía de un inventario de los sistemas y procedimientos usados en el campo, un estimado crecimiento para los próximos años y una definición de los requerimientos para un sistema futuro. Después el mercado fue investigado para encontrar equipos que satisfacieran esos requerimientos. La conclusión de este estudio fue que existen muchos sistemas de seguridad y muchos sistemas de administración de redes diferentes, pero no hay una industria que por sí sola pueda manejar los requerimientos de la red y su seguridad. El problema principal fue la falta de instalaciones de administración en el mismo sistema. Aún más, la mayoría de los sistemas disponibles fueron diseñados para un tipo de red en particular. Los que se necesitaba era un sistema uniforme, que fuera adaptable a diferentes tipos de redes.

El equipo que desarrolle el proyecto debe cubrir varios campos. Además de el encriptamiento, existen ingenieros de software y hardware involucrados. Durante la fase de especificación, se deben mantener contactos cercanos con los clientes potenciales. El

sistema se debe apoyar en un encriptamiento altamente seguro y un sistema central de administración de llaves.

Algo que recomienda el equipo de investigación es que se utilice un hardware dedicado, ya que cuando se hicieron las primeras propuestas para el algoritmo criptográfico se comprobó que una implementación de software no es factible.

El primer prototipo fue construido de dispositivos convencionales de Mediana Escala de Integración, el problema era que existía mucha circuitería de control implementada en lógica programable. Un procesado se contenía en una tarjeta aparte para la ejecución de la comunicación de datos y los protocolos criptográficos.

Después del desarrollo de un prototipo y la producción de una pequeña serie de sistemas, una prueba de campo los evaluó en la vida real. Aunque los usuarios se mostraron entusiastas con el desempeño de los sistemas, tenían un obstáculo muy grande que era el tamaño, resultó más grande que la terminal a proteger, y el costo de producción sería enorme.

Después de la evaluación solo quedaba una alternativa y esa era el rediseño del hardware de encriptamiento. Al hacerlo sería posible hacerlo más pequeño y abaratarlo.

Al diseñar e implementar un sistema se deben cumplir tres requisitos principales:

1) Especificar el sistema y definir todas las partes que los compondrán.
2) Diseñar e implementar todas las distintas partes.
3) Integrar todas las partes y probar el sistema completo.

Siendo un poco más específico en el desarrollo de un proyecto se pueden distinguir cinco partes:

1) La descripción del algoritmo.
2) La descripción del hardware.
3) El diseño de la lógica.
4) El diseño físico.
5) El diseño de silicón.

La compañía describe brevemente cada una uno de los pasos mencionados arriba:

1) La descripción del algoritmo. Junto con el departamento de encriptamiento una descripción matemática bastante formal del estándar de encriptamiento fue hecha. Esto es revisado por el departamento de hardware para armonizar el diseño criptográfico con la implementación del hardware. Utilizando simulación por computadora se revisaron tanto las especificaciones y medidas estadísticas del algoritmo como las condiciones del hardware.
2) La descripción del hardware. Utilizaron un diseño con direccionamiento y datos separados en un sistema enteramente síncrono. El camino de datos fue especificado de tal forma que permitía el alojamiento de una arquitectura jerárquica. La parte de control fue formada por varias máquinas de estado distribuido síncrono. Se utilizó simulación de software para la revisión de resultados y un lenguaje de alto nivel.
3) El diseño lógico. El diseño lógico fue hecho por otra empresa, utilizando un sistema de entrada esquemático. La conducta externa fue especificada utilizando simulaciones de algoritmo. Se utilizó una forma extendida de simulación. Nos

mostró todos los estados estables internos del sistema y fue usado para una prueba de generación de vectores.

4) El diseño físico. Al decidir que tecnología se debería utilizar para el diseño, se eligió utilizar tecnología cell/full de 1.5 micras, ya que un estudio de factibilidad demostró que el utilizar un arreglo de compuertas sería demasiado grande y muy complejo. Después de armado se realizan el (ERC) Electrical Rule Checking y el (DRC) Design Dule Checking.
5) El diseño de silicón. Éste fue realizado por una casa ajena a la empresa y el resultado final fue un chip de 50 mm^2, que opera a una frecuencia de 16 MHz y a una velocidad de encriptamiento de 2.048 Mbps, en una transmisión totalmente full-duplex.

Estas notas tratan de dar un punto de vista no sobre el proyecto en específico sino desde el punto de vista de un diseñador. Lo primero fue que partes del proyecto se realizarían en nuestra propia empresa y que partes se llevarían a otros lugares para su diseño. Se debe realizar una lista de revisión para los pasos técnicos y para los pasos de administración a ser tomados. Para la parte técnica la lista se dividió en dos partes, actividades para el laboratorio y actividades para la empresa contratada. Las siguientes actividades se realizaron en la propia empresa:

- Especificación de la arquitectura del hardware.
- Especificación de la conducta externa del chip.
- Especificación de las pruebas funcionales del sistema.
- Especificación de los parámetros mecánicos y eléctricos.
- Especificación del tipo y tamaño del proceso.
- Especificación del tipo de empaquetamiento.
- Pruebas de los dispositivos del prototipo.

- Discusión del tipo del lenguaje a utilizar, dispositivos de lectura, prueba de retroalimentación.

Las siguientes actividades fueron realizadas en la empresa contratada:

- Darle retraoalimentación al desarrollo del proyecto.
- Dar resultados en formatos entendibles, simplificados y prácticos.
- Dar asesoramiento sobre alternativas propuestas pro el equipo de diseño.
- Otorgar control de calidad al diseño.
- Dar información a la compañía que desarrolle el chip.

Las siguientes actividades serán en el laboratorio de casa con respecto a la administración:

- Realización de contratos legales con los participantes.
- Acuerdos con todos los participantes externos sin dar a conocer información confidencial extra.
- Realizar juntas con el equipo de laboratorio y el equipo del proyecto.
- Hacer revisiones financieras y contables.
- Arreglar juntas para revisiones periódicas con los participantes externos.
- Proponer mejoras y discutirlas con todos los participantes.
- Hacer un plan de emergencia en caso de: fallas con el prototipo, problemas con el equipo de diseño, etc..

Un consejo por parte de la empresa PTT, es hacer el diseño del hardware antes de entregarlo a la casa de diseño, de esta forma queda protegido en caso de que existan

problemas por parte de empresas externas, o bien si se deciden hacerle mejoras no interrumpe el proceso.

Según la empresa, gracias al avance diario de la tecnología, el ingeniero puede hacer el diseño casi en su totalidad sin ser un experto en silicones. El uso de técnicas de especificación formales (lenguajes de encriptamiento para hardware), simulaciones por computadora, poder observar los resultados de las elecciones de diseño en términos del área de silicón y límites de velocidades, la habilidad de generar patrones de prueba y la facilidad de obtener tecnología rápidamente. Todo esto ayudará para que la forma en que el hardware se diseña y se produce, resultará en sistemas más poderosos y confiables.

4.4 DISEÑO DE UN SISTEMA DE COMUNICACIONES DE VOZ PAQUETIZADA ASEGURADO POR ENCRIPTAMIENTO.

La naturaleza explosiva de las comunicaciones de voz deben ser explotadas para usar eficientemente la capacidad del canal de comunicaciones de una red utilizando técnicas de empaquetamiento conmutado. En tales sistemas, los usuarios pueden demandar un servicio para asegurar sus conversaciones. Para atender esta demanda, los paquetes de voz deben ser encriptados en la fuente transmisora del usuario y luego ser transmitida como paquetes de texto cifrado a la terminal receptora de usuario, donde se revertirá el proceso de encriptamiento en el orden idóneo para reconstruir las señales de la voz original. Ya que la comunicación hablada tiene que realizarse en un ambiente de tiempo real, varios problemas pueden surgir en el diseño de un sistema de comunicaciones de voz paquetizada asegurado por encriptamiento. Veremos algunos de esos problemas junto con la presentación de algunas posibles soluciones. Entre algunos de esos problemas están, por mencionar algunos: retraso en la paquetización de la voz, retraso en el cifrado y descifrado en los paquetes de voz debido a la simetría o asimetría de algunos algoritmos criptográficos, hacer la selección correcta del modo de operación del algoritmo criptográfico, control de errores, control de

flujo y generación y distribución de llaves para el encriptamiento y desencriptamiento de los paquetes de voz a través de una red WAN.

En general, el tráfico de comunicación de mensajes puede ser clasificado en dos clases principalmente:

1) Tráfico continuo (en flujo).
2) Tráfico no continuo (de carácter interrumpido).

Un ejemplo típico del tráfico continuo es la comunicación de voz telefónica, mientras que los datos son ejemplo de tráfico interrumpido. Aunque el tráfico de voz puede ser considerado típicamente como continuo, puede ser que a veces sea un poco interrumpido en su naturaleza. Se puede aprovechar esta característica para multiplexar varias transmisiones en un canal común.

En una conversación telefónica normal, cada bocina está activa menos de la mitad del tiempo que dura dicha conversación. El tiempo restante es ocupado para escuchar a la otra terminal y para que nosotros respiremos entre cada palabra. A esto se le llama el "período de silencio", de esta forma cada terminal alterna su tiempo entre silencio y plática. En la conversación, el tiempo que realmente habla una persona es del 35% o un máximo de 40%, lo que nos deja un tiempo libre para uso de canal de aproximadamente 60% ó 65%.

Aunque la técnica de conmutación de circuitos siempre se ha utilizado tradicionalmente para el tráfico de voz, parece ser que la conmutación de paquetes es mucho más barata y conveniente. Esto es debido a que el concepto de conmutación de paquetes permite al usuario explotar el manejo de voz casi en la misma forma en que lo hace para el manejo de datos, formando y transmitiendo paquetes solo durante los

períodos de actividad de la persona que este hablando en ese momento. Los períodos de silencio, bien pueden ser utilizados para transmitir datos u otras señales de voz, claro que todo depende de la prioridad del usuario y de la señal. En la fuente de generación, el habla es paquetizada y los paquetes resultantes son transmitidos a través de una red de conmutación de paquetes. En el destino, los paquetes recibidos son almacenados y reproducidos con retraso mínimo para la reconstitución de la voz.

Las redes WAN fueron diseñadas inicialmente para la transmisión y recepción de paquetes de datos entre dos usuarios del sistema. Ya que los paquetes de voz deben ser transmitidos en un ambiente de tiempo real, lo que puede provocar varios problemas distintos a los que se está acostumbrado cuando se trabaja en un ambiente de tiempo no real. Los paquetes de voz viajan a través de varios nodos y enlaces, la red de paquetes introduce en nuestra transmisión varios retrasos de acuerdo a la carga y a las características de la red. Los paquetes de voz llegan a su destino con un algún retraso, otros pueden llegar con errores y otros sencillamente se pierden en la red.

Debemos enfatizar que el límite máximo de retraso en los paquetes de voz debe ser del orden de los 250 a 300 milisegundos, no excediéndolo, la transmisión proporcionará un sonido de la conversación natural y tolerable. Otros tipos de retraso que debemos mencionar son los siguientes: paquetización de la voz, encriptamiento del paquete, retraso en varios nodos y enlaces de la red, reensamblaje de los paquetes y desencriptamiento del paquete en la terminal del receptor.

Para el encriptamiento y desencriptamiento de los paquetes de voz, pueden ser aplicados el Data Encryption Standard y algoritmos de llave pública. Hablaremos de como el DES introduce unos pocos microsegundos para el proceso de encriptamiento y desencriptamiento de la voz paquetizada, mientras que los algoritmos de llave pública

consumen hasta un tercio de segundo para el mismo proceso. De esta forma, para satisfacer las necesidades de reducir el retraso en el proceso, el Des es usado en esta propuesta. Aunque los algoritmos de llave pública no son adecuados para operaciones de encriptamiento y desencriptamiento de paquetes de voz, pueden ser aplicados para la generación de llaves de sesión y distribución durante la fase de llamada de establecimiento. También un Centro de Llaves de distribución (KDC), es usado para transferir llaves entre los sistemas fuente y destino.

Otro factor a considerar es la correcta selección del modo de operación del DES a usar. Entre los distintos chips de DES implementados pro fabricantes diferentes, se seleccionó el Advance Micro Device´s (AMD) AM 9568 Data Ciphering Processor (DCP) DES chip. El DCP puede ser operado en cualquiera de los modos siguientes: Electronic Codebook (ECB), Chainblock Cipher (CBC), Cipher Feedback (CFB) y Output Feedback (OFB). Necesitamos seleccionar el modo de operación del DCP adecuado con mucho cuidado. Ya que como mencionábamos, algunos paquetes se pueden perder en la red y otros más pueden ser recibidos con errores, la selección no adecuada puede provocar situaciones criticas en donde los paquetes no puedan ser desencriptados adecuadamente.

4.4.1 EL SISTEMA DE VOZ PAQUETIZADA.

El diagrama a bloques de nuestro sistema es presentado a continuación en la figura 37. Las señales de voz son paquetizadas en el abonado de transmisión y los paquetes resultantes son transmitidos a través de la red de conmutación de paquetes a su destino. Los períodos de silencio pueden ser utilizados para otro tráfico de los que sea (voz, datos, etc.).

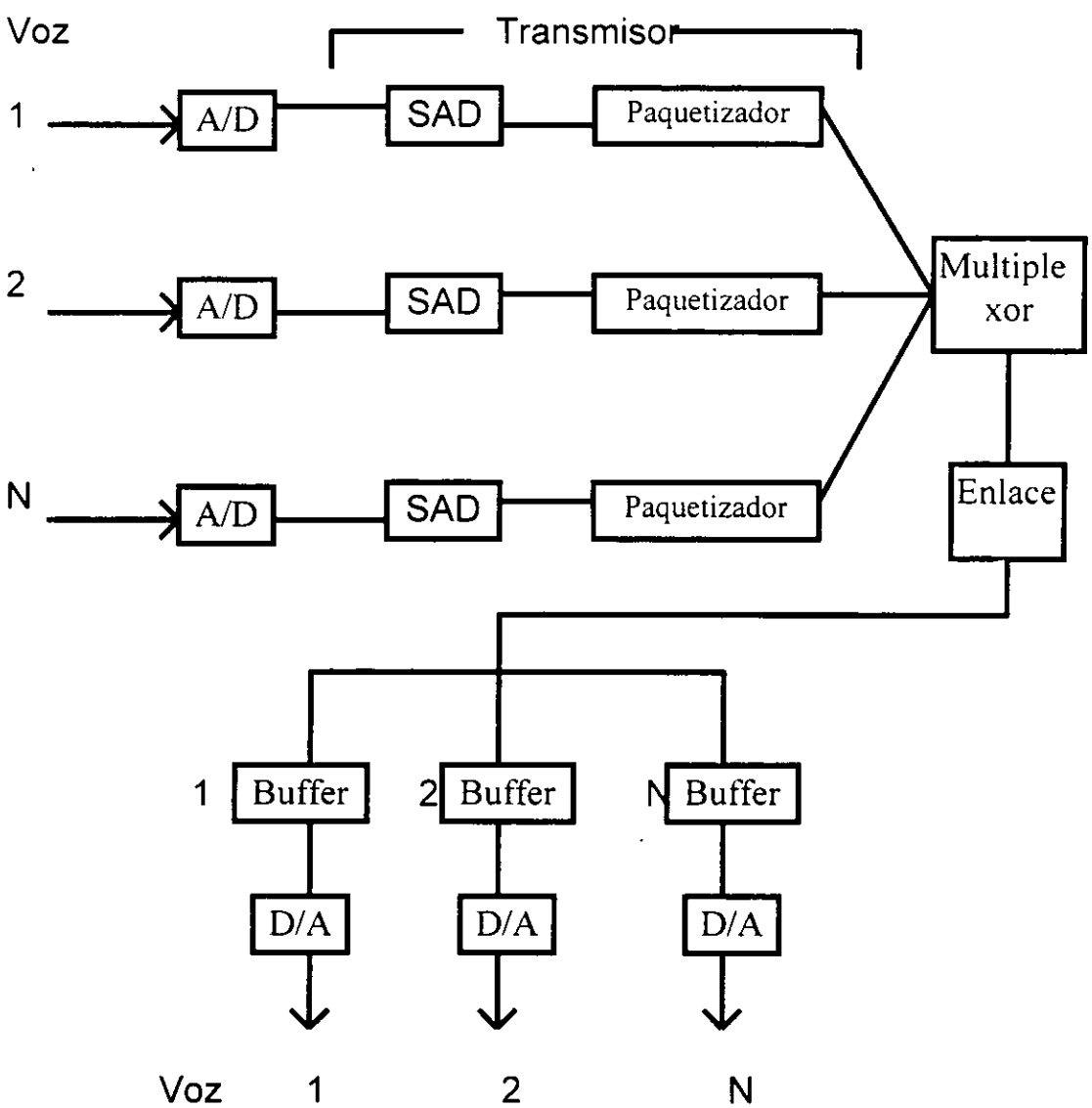


Figura 37

En la siguiente figura se muestran las formas de onda de una señal, que consisten de períodos de sonido y silencio. Los sonido son convertidos en paquetes de voz y el silencio

en paquetes de silencio. Números secuenciales son asignados a todos estos paquetes. Del abonado transmisor son enviados los paquetes de voz.

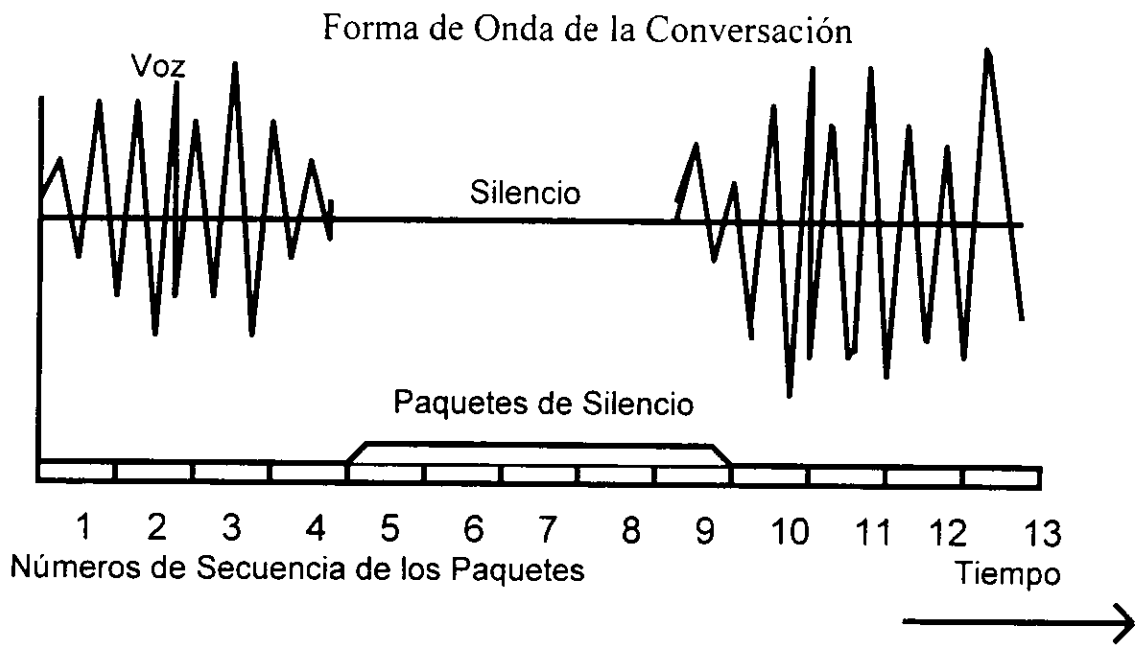


Figura 38

Como se ve en nuestra figura , en el sistema destino, los paquetes de voz recibidos son almacenados en un buffer y luego son desplegados con algún retraso para reconstituir la conversación original.

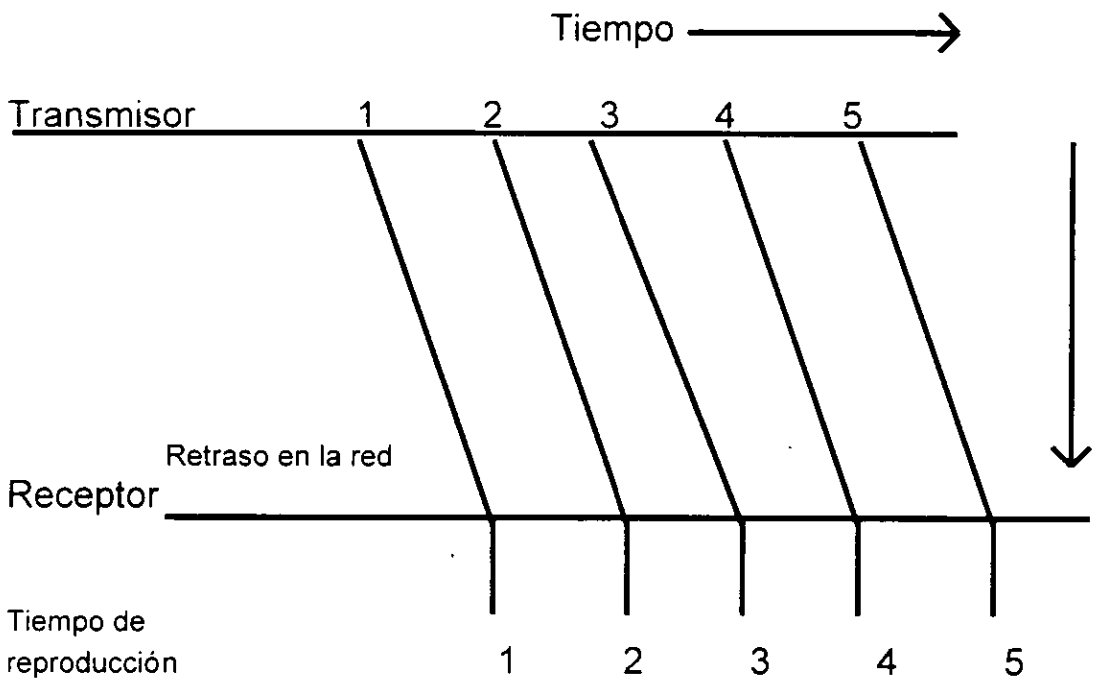


Figura 39

Para enrutar a nuestros paquetes, necesitamos usar ya sea el servicio de datagramas o el servicio de circuitos virtuales. Para nuestras necesidades de tiempo real, la técnica de circuito virtual conmutado es la más apropiada. Las ventajas resultan que en el servicio de datagramas provee una recepción de paquetes secuencial en el destino y existen reducidas pero considerables variaciones en la entrega promedio de paquetes.

4.4.2 PAQUETIZACIÓN Y RECONSTITUCIÓN DE LA VOZ.

El propósito de los algoritmos de paquetización y reconstitución es el proporcionar la conversación con el menor retraso en la transmisión de punto a punto y que cualquier anomalía causada por la pérdida o retraso de paquetes sea imperceptible para el usuario. Idealmente, la red debe otorgarnos un gran ancho de banda para el enlace y un poder de procesamiento nodal suficiente para mantener el retraso y la dispersión controlados para que no rebasen los límites controlados de tolerancia. De cualquier forma, en algunas situaciones donde se utilice paquetización, no nos es posible controlar el diseño de la red. Particularmente, cuando exista necesidad de transmitir voz cuando exista gran tráfico ajeno al nuestro, para estos casos será necesario utilizar algoritmos más elaborados.

Para minimizar tanto el retraso de la paquetización como el efecto de mala recepción por anomalías de pérdida de paquetes en la recepción, los paquetes deben ser lo más pequeño posible. Por otro lado, para mantener una alta utilización del canal, es preferible mantener el número de bits de voz por paquete tan alto como sea posible en relación a los demás bits de la trama. La elección del tamaño de la trama está influenciada por la capacidad de procesamiento de paquetes en la red, todo esto se mide por segundo.

Para ayudar a la reconstitución de voz, se debe incluir una marca de tiempo y un número que marque la secuencia de paquetes dentro de la transmisión. La marca de tiempo permite al receptor reconstituir la voz con momentos precisos de silencio (respiraciones, pausas, etc.), a pesar de retrasos variables entre sonidos. El número de secuencia permite al receptor detectar paquetes perdidos y complementa a la marca de tiempo, ya que esta no puede reconocer entre momentos de silencio y paquetes perdidos.

Los algoritmos de reconstitución tienen dos tareas principales:

1) Debe almacenar en su buffer todos los paquetes que reciba y organizarlos, para reproducirlos o mostrarlos en el orden correcto.
2) Debe decidir que mostrar cuando ha terminado de exhibir sus paquetes almacenados y el siguiente paquete no esté disponible.

4.4.3 CONTROL DE ERRORES Y CONTROL DE FLUJO.

En cuanto a paquetes de datos se refiere, para proveernos de un mensaje íntegro, un protocolo debe ser capaz de detectar Protocol Data Units (PDUs) ya sea borradas, duplicadas o fuera de orden, así como PDUs adulteradas de otras asociaciones y PDUs cuyos contenidos hayan sido modificados. Para recuperarse de ataques de modificación del mensaje en flujo, el protocolo debe poder retransmitir PDUs perdidas o modificadas, deshaciéndose de las adulteradas o duplicadas, y darles de nuevo secuencia a PDUs fuera de orden. Todos estos servicios son requeridos para las transferencias de datos. De cualquier forma, cuando se trata de voz paquetizada, las necesidades son de mucha mayor importancia. Para este caso, el protocolo a usar debe suministrar la habilidad de reproducir a tiempo para el receptor. Para lograr esto, un protocolo para paquetes de voz, puede sacrificar un mínimo de confiabilidad por el bien de la puntualidad de la transmisión. De hecho, la mayoría de estos sistemas de voz simplemente eliminan procedimiento de recuperación de aquellos paquetes perdidos o recibidos incorrectamente. Esto es de pequeñas consecuencias para la calidad de la voz recibida gracias a la naturaleza robusta de la misma.

Un análisis hecho a los principales aspectos de la transmisión de voz en redes de conmutación de paquetes muestra que los procedimientos para el control de errores y de flujo que se utilizan más actualmente no son los adecuados para este tipo de comunicación. Lo que parece más apropiado para este caso es el utilizar un protocolo dedicado rápido y simple, capaz de minimizar el retraso entre los puntos de transmisión y recepción, y preservar la información contenida en la redundancia de la voz, esto parece ser lo más apropiado, en lugar de mecanismos de control de errores. De esta forma, el control de errores se puede concentrar a revisar las cabeceras de las tramas recibidas y descartar las que no le corresponden, y los procedimientos relacionados a la recuperación de condiciones, consideradas como "fuera de secuencia", pueden ser omitidos en las capas de red y enlace. La revisión de errores, será hecho en la porción del encabezado de los paquetes de voz.

Protocolos de redes de datos utilizan esquemas de control de tráfico para regular el flujo del mismo entre dos puntos y para controlar el nivel de congestión en la red. Para flujo de paquetes de datos, se utilizan esquemas como el de la ventana deslizante y evaluación de crédito del usuario. La entrega de dichos paquetes puede retrasarse, por razones de control de flujo y para no afectar dañinamente la información completa. Los paquetes de voz en tiempo real, son inútiles si se retrasan demasiado. Por esto, los esquemas de control de tráfico que impiden la entrega oportuna de paquetes deben ser eliminados de cualquier protocolo de voz. Aunque, alguno de estos esquemas puede ser utilizado para la protección de los recursos de la red para que su desempeño no se degrade a un nivel inaceptable. Esto puede lograrse disminuyendo el número de conversaciones atendidas en un determinado momento.

Una diferencia importante entre los protocolos de voz y otros tipos está en el procedimiento de conexión. Cuando una solicitud de conexión es hecha, un protocolo informa al usuario de la solicitud y espera una respuesta. Esta es generalmente para referirse a la aceptación o el rechazo de la solicitud. En la mayoría de los protocolos, el usuario es un proceso del servidor, tal como el sistema operativo. En un protocolo de voz paquetizada, el usuario del protocolo incluye a una persona en muchas ocasiones. La respuesta a la solicitud de conexión puede depender de la persona. Así que, el protocolo tiene que tomar en cuenta el factor humano en su procedimiento de establecimiento de la conexión.

Considerando todos estos hechos, mostramos a continuación un posible formato de trama para paquetizar voz. La porción de datos de voz puede ser variable en su tamaño. En estudios de simulación se han probado longitudes de 256 bits, 512 bits, 1024 bits y 2048 bits, bajo números diferentes estados de transiciones de voz-silencio por paquete. Por los estudios realizados fue demostrado que la elección óptima fue de una longitud de 512 bits por paquete de voz con un estado de transición voz-silencio, con esto se pueden obtener una mejor utilización del canal. Aunque longitudes más grandes de paquetes son posibles, tiene desventajas de un retraso de punto apunto debido a la paquetización que no sería aceptable para comunicaciones de voz en tiempo real.

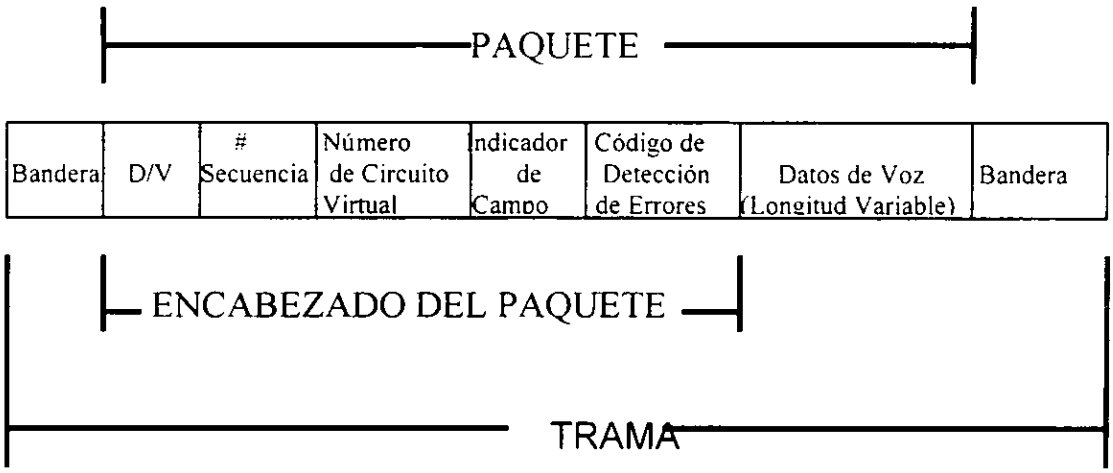


Figura 40

4.4.4 CONSIDERACIONES EN EL RETRASO EN VOZ PAQUETIZADA.

Para asegurar un tiempo de transmisión en la red compatible con los estrictos requerimientos (250 - 300 ms) para el retraso de los paquetes de voz entre abonados, debemos considerar siempre el tiempo utilizado en el encriptamiento y en el proceso inverso. No obstante, el retraso total comprende también la paquetización de la voz, el tiempo de reconstitución, el tiempo de espera, el número de saltos, etc.. Típicamente, los sistemas de este tipo, producen paquetes a intervalos de tiempos regulares. Mientras los paquetes pasan a través de la red, cada uno puede encontrar un monto distinto de espera en fila en los enlaces estadísticamente multiplexados. La variación del retraso depende de la naturaleza de la red (ya sea si son redes, LAN, MAN o WAN), del tráfico en la misma y de la velocidad en los dispositivos de la misma. Para una red LAN, el retraso variable es generalmente pequeño, menos de 10 ms. Para las redes MAN y WAN, el retraso variable depende del tiempo de espera en cada enlace. El retraso depende principalmente del

número de enlaces, su utilización, el tamaño de los paquetes y la velocidad del enlace, el retraso puede ser superior a los 100 ms.

En lo que concierne al modo de operación para el aseguramiento de la información, el Data Encryption Standard (DES) puede ser usado para soportar, un cierto grado de servicios de seguridad. Algunos chips comerciales de DES que pueden encriptar y desencriptar altas tasas de información son adecuados para el ambiente de voz paquetizada. Por ejemplo, el Western 2001 trabaja a 1.8 Mbps, Advanced Micro Devices 9568 a 12 Mbps, Dispositivo Z8068 a 13.6 Mbps, etc.. Ya que el tiempo de las operaciones de encriptamiento y desencriptamiento es de alrededor de 5 micro segundos o menos, el tiempo que ocupa el DES no es significante comparado con el de los otros retrasos. En la fase del establecimiento de la conexión de llamada, el esquema de llave pública en asociación con el centro de distribución de llaves (KDC) es considerado como el más apropiado para la administración de llaves.

De esta forma, los servicios de seguridad pueden ser usados para paquetes de voz bajo un protocolo que pueda proporcionar los servicios de transportación de paquetes entre sistemas de usuarios punto a punto. Debido a las necesidades de los paquetes de voz, el protocolo subyacente debe proveer el servicio de transporte punto a punto sin control de flujo o retransmisión de paquetes retrasados excesivamente o perdidos definitivamente. También ha sido estudiado que el retraso en el orden de los 300 milisegundos puede ser apropiado como límite superior en un paquete de voz de un sentido en una red. Si se respeta este límite la voz se escucha con resultados naturales en la terminal de recepción. También se descubierto que el procedimiento de encriptamiento y desencriptamiento punto a punto es el más adecuado para paquetes de voz. El procedimiento de encriptamiento y desencriptamiento orientado a enlace no es adecuado para paquetes de voz. En el procedimiento de punto a punto, los mensajes son encriptados y desencriptados

solamente en las dos terminales de usuario. En este caso, los mensajes están disponibles en forma de texto cifrado en los nodos intermedios. Los algoritmos de llave pública son mucho más adecuados para este tipo de ambiente. Ya que a los algoritmos de llave pública les toma aproximadamente un tercio de segundo para una operación de encriptamiento, se ha encontrado que el algoritmo de llave pública no puede ser usado para el encriptamiento de paquete de voz, pero puede ser usado para la distribución de las llaves de sesión.

4.5 SELECCIÓN DEL MODO OPERACIONAL DEL DES.

Como mencionamos antes, el algoritmo DES será usado para el encriptamiento y desencriptamiento de los paquetes de voz ya que requiere menos tiempo para dicha operación comparado con los algoritmos de llave pública. En esta sección hablaremos del Electronic Codebook Mode (ECM), Cipher Block Chaining Mode (CBC), Cipher Feedback Mode (CFM), y del Output Feedback Mode (OFM). Entre estos modos operacionales el ECB fue el seleccionado para nuestro sistema.

4.5.1 ELECTRONIC CODEBOOK MODE (ECB).

El ECB es ilustrado en la figura 41 y muestra que es una implementación directa del algoritmo DES. El bloque de texto sin cifrar (64 bits) entrante es procesado por el mismo. El proceso de descifrado es desarrollado en la misma forma, usando la misma llave con el bloque de entrada siendo este el texto cifrado y el texto descifrado se obtiene a la salida. Ya que los mensajes de entrada y salida están en un tamaño de 64 bits, y una llave similar es usada para cada bloque de mensaje a ser cifrado, el modo ECB es implementado como cifrado de bloques y cada bloque de mensaje cifrado independientemente. Puede notarse

que el mismo texto a cifrar siempre genera el mismo texto cifrado para una llave de encriptamiento dada.

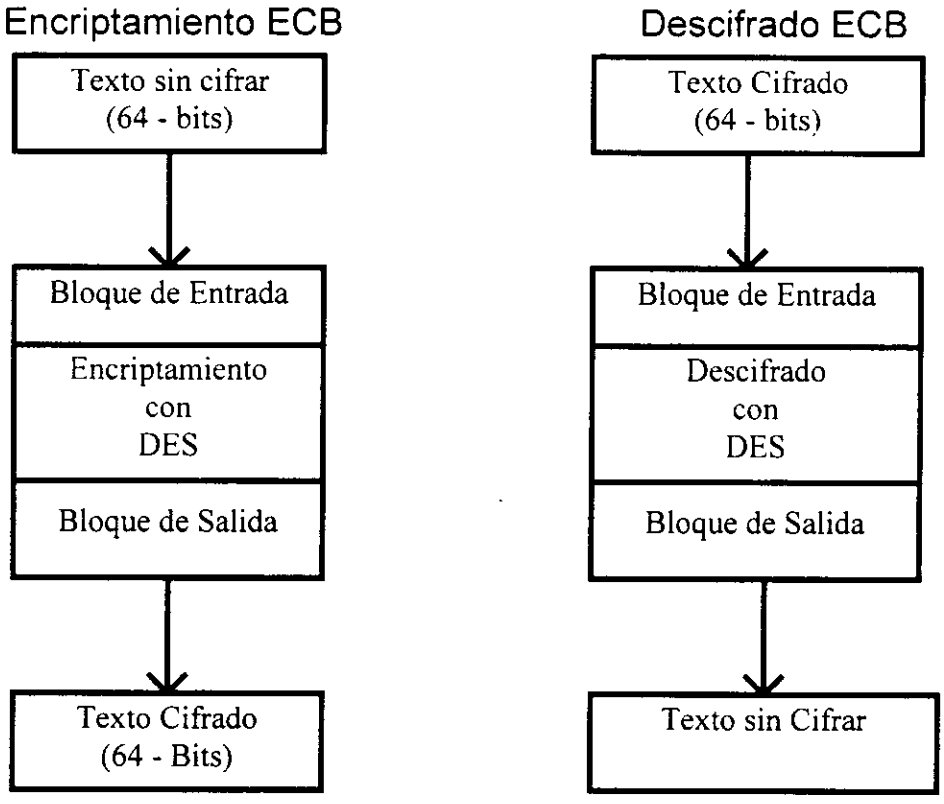
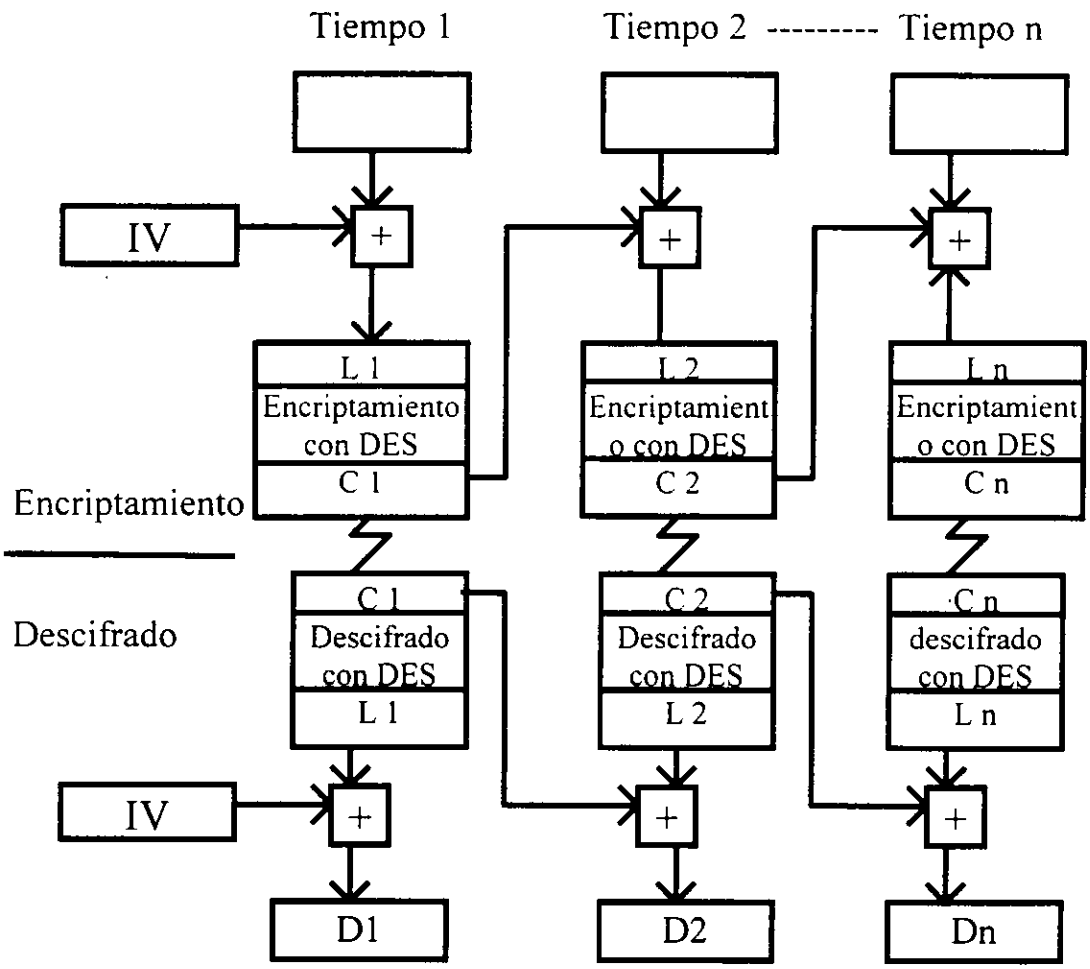


Figura 41

4.5.2 CIPHER BLOCK CHAINING MODE (CBC).

A continuación mostramos el CBC, el cual opera en bloques de mensajes de 64 bits. El bloque de mensaje entrante es procesado por una compuerta lógica XOR con un vector inicial de 64 bits (IV). La resultante es encriptada por el algoritmo DES. El mensaje encriptado es retroalimentado y cargado de nuevo en el cuarto registro, el cual es procesado por la compuerta XOR y el siguiente bloque de entrada, y de forma subsecuente con los siguientes bloques. Este encadenamiento de bloques asegura que los bloques de

mensaje entrantes idénticos no produzcan los mismos bloques de salida, incrementando así el nivel de seguridad. Como en el caso del ECB, el CBC es implementado como cifrado en bloque.



D j = Bloque de datos en tiempo j.
L j = Bloque de entrada para encriptamiento en el tiempo j.
C j = Bloque cifrado en el tiempo j.
I V = Vector de inicialización.
+ = Or - Exclusiva

Figura 42

4.5.3 CIPHER FEEDBACK MODE (CFB).

El CFB, mostrado en la figura 43, opera con bloques de mensajes de n cantidad de bits, donde n puede ser cualquier número del 1 al 64. La operación es desarrollada procesando los contenidos del registro IV por el algoritmo DES. Los bits más significativos son procesados por la compuerta XOR con el bloque de mensaje entrante de n bits. El resultado es un bloque de salida de n bits cifrado. Este bloque de salida es cambiado en el orden menos significativo del registro IV. En este modo el algoritmo DES es usado solamente en la generación de llaves en lugar de encriptar datos. El flujo de llaves es derivada de un número arreglado de un número n de caracteres precedentes de texto cifrado. En cada encriptamiento, un flujo de llaves diferente es derivado y usado para encriptar el flujo de mensaje. Ya que el flujo de llaves es dependiente del flujo de mensajes, el CFB es el típico ejemplo de una operación autosíncrona de cifrado en flujo. Como en el CBC, los bloques de datos entrantes idénticos no producen los mismos bloques de salida y cada bloque de texto cifrado es dependiente del bloque de texto cifrado anterior. Para $n < 64$, todo el proceso del CFB es considerablemente menor que los de los modos ECB o CBC, porque cada pase del algoritmo proporciona solamente los n bits comparados con los 64 bits en los modos ECB o CBC.

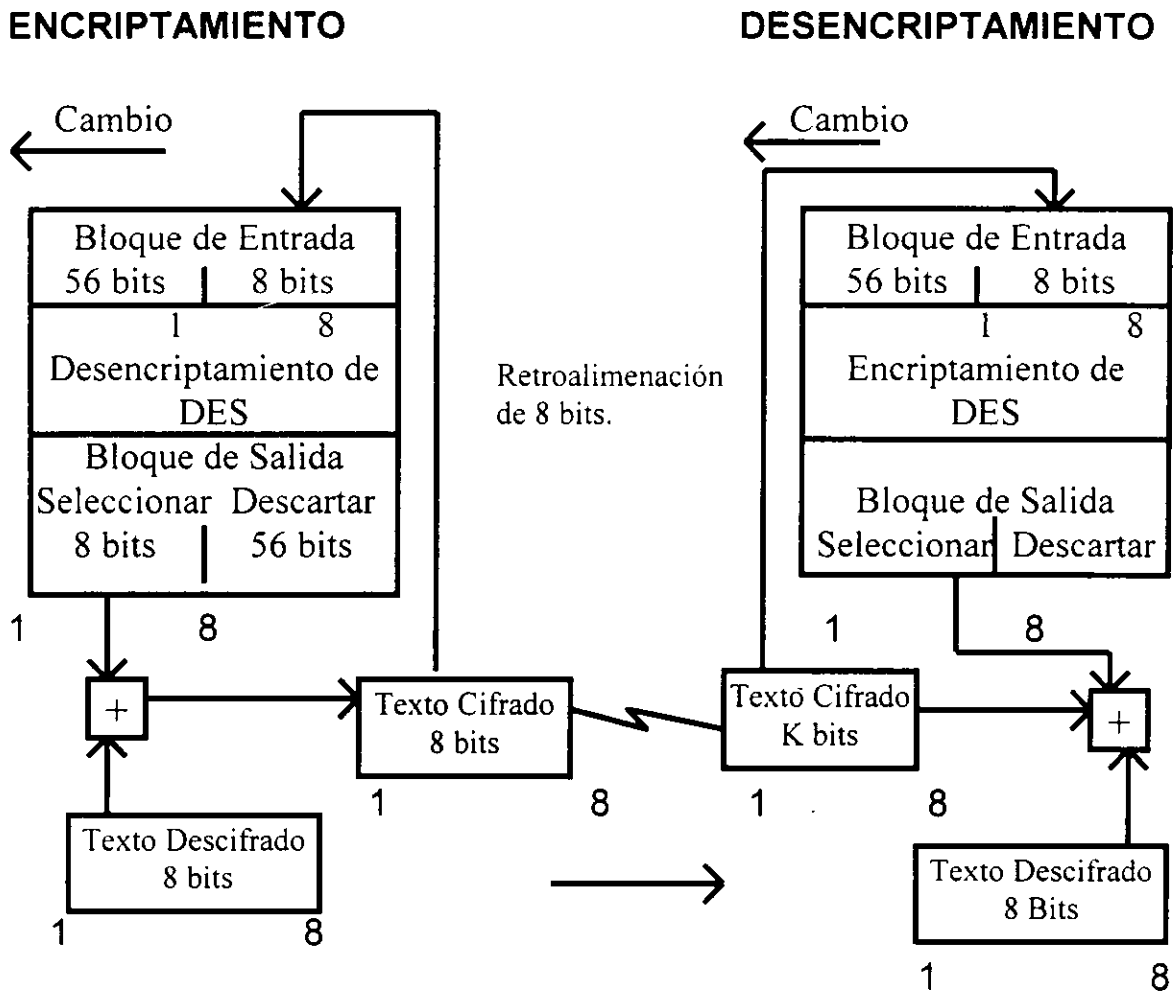


Figura 43

4.5.4 OUTPUT FEEDBACK MODE (OFB).

El OFB está ilustrado en la siguiente figura, este difiere levemente del CFB en la retroalimentación de los datos. Esta es independiente de los datos entrantes que son encriptados. También opera con bloques de mensajes de n bits, donde n es número que puede tomar valores desde 1 hasta 64. El vector inicial IV de 64 bits en el registro de entrada IV es primeramente procesado por el DES. Los n bits más significativos de la

resultante en el registro IV de salida son procesados por la compuerta XOR con los n bits del bloque de mensaje de entrada. También, los bits más significativos en el registro de salida IV son retroalimentados en el registro de entrada IV intercambiándose en la posición de los n bits menos significativos. Como en el CFB, el algoritmo DES en el modo OFB es usado para generar el flujo de llaves el cual es usado para encriptar el flujo de mensajes. De cualquier forma, como es distinto del CFB, el flujo de llaves generado es independiente de los bloques de texto cifrado, y así el modo OFB es un ejemplo de un flujo de cifrado síncrono.

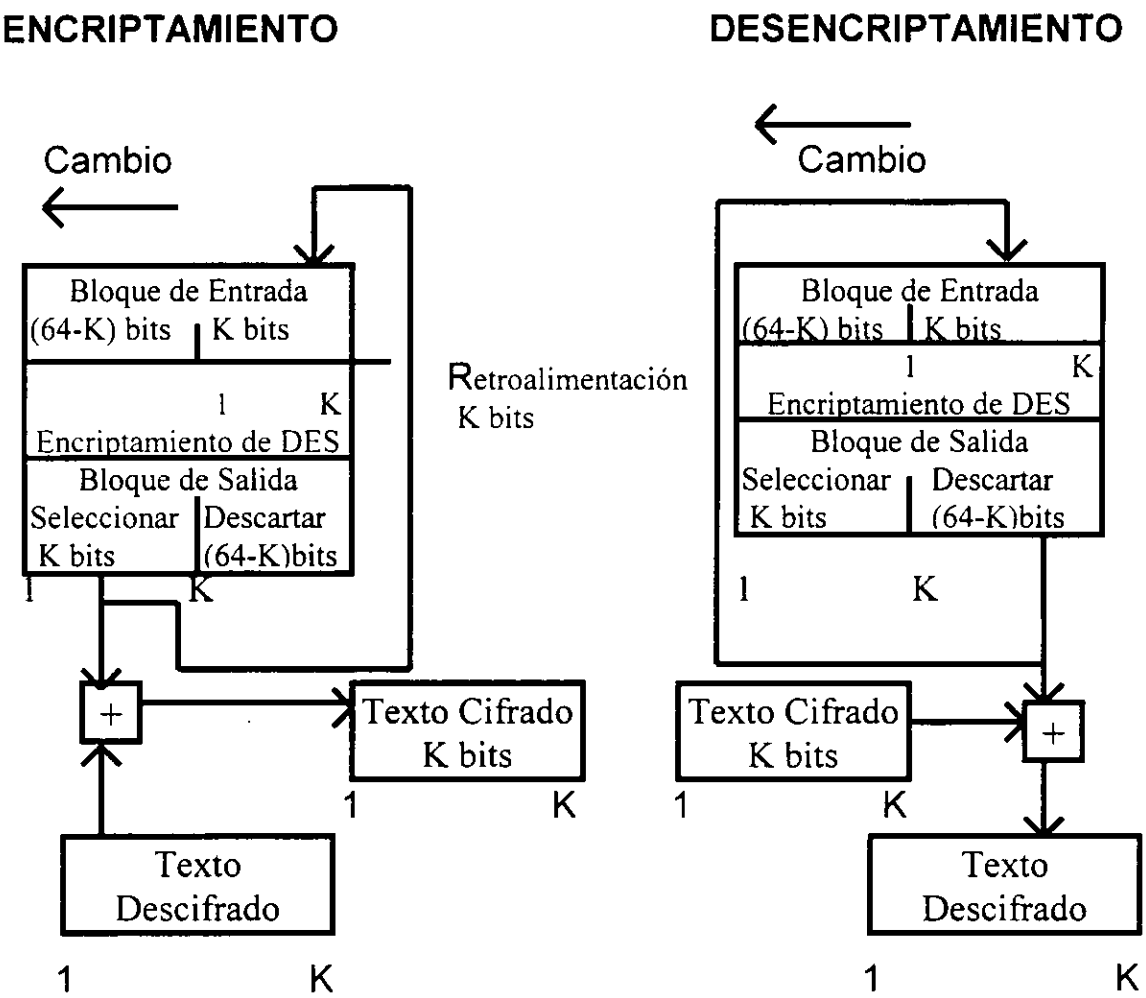


Figura 44

En los modos CBC, CFB y OFB algunos tipos de retroalimentación es involucrada. De esta forma, para usar estos modelos, los paquetes completos deben estar disponibles en el abonado destino del sistema en orden secuencial. Pero cuando se usa voz paquetizada, algunos paquetes pueden retrasarse en lo subnodos de comunicación debido al tiempo de espera en los nodos intermedios. También, paquetes erróneos deben ser descartados en la subred de comunicaciones, ya que algunos paquetes pueden perderse en la red. Adicionalmente, estos paquetes que arriban al destino, deben pasar por un tiempo de revisión en un umbral y no serán reproducidos por lo que estos paquetes no estarán disponibles en el destino para reconstituir el mensaje de voz original. Esto indica que si los modos CBC, CFB u OFB del algoritmo DES son usados para encriptar y desencriptar paquetes de voz, entonces, debido a las propiedades inherentes de la retroalimentación de esos modos de operación, estos paquetes de voz que se retrasaron más del tiempo de umbral y o que se hayan perdido en la red, tampoco estarán disponibles para el descifrado.

De esta forma, los paquetes de voz libres de errores que son recibidos en el abonado receptor del sistema, tal vez tampoco puedan ser descifrados debido a que los paquetes perdidos o retrasados poseen bits cifrados necesarios para el vector inicial. Esto significa que no podremos utilizar exitosamente los modos CBC, CFB y OFB para nuestro sistema. Esto nos deja solamente el modo ECB para trabajar; en este modo el mismo texto sin cifrar produce el mismo texto cifrado con una llave dada y viceversa. Así que, si algunos paquetes se retrasan o pierden, cada paquete es encriptado y descifrado independientemente. Esto significa que los paquetes libres de error que sean recibidos en el abonado receptor producirán la voz esperada cuando se descifren. Por estas razones, se recomienda el usar el modo de operación ECB para encriptar y desencriptar paquetes de voz para este sistema.

4.6 DISEÑO DEL SISTEMA DE COMUNICACIONES DE VOZ PAQUETIZADA.

El nivel de seguridad provisto por un esquema basado en encriptamiento para comunicaciones en una red de conmutación de paquetes es altamente dependiente de la seguridad de las llaves usadas para encriptar y descifrar. Para asegurar un más alto nivel de seguridad, estas llaves deben ser cambiadas frecuentemente, lo idóneo sería cambiarlas en para cada sesión, es decir una llave de sesión única es generada para cada nueva sesión y descartada al final de la misma. La facilidad de tal actualización, particularmente cuando se trata de encriptamiento de punto a punto, depende de la existencia de un mecanismo de administración de llaves que facilite la generación de la llave de sesión (en el inicio de la misma sesión) y la distribución a los dos abonados. Aún más, lo más deseable es que esta transferencia sea hecha en los canales de comunicación disponibles, los cuales demandarían el más alto nivel de seguridad durante esta transferencia. Consecuentemente, la administración de llaves es más importante para la seguridad de la red que la misma estructura matemática de los algoritmos, una transferencia ineficiente de la llave entre los abonados puede hacer que la seguridad sea inútil sin importar la complejidad de el encriptamiento.

En una red grande, la administración de tantos números puede ser engorrosa y costosa. Para simplificar este problema un Centro de Distribución de Llaves (KDC) es requerido para sistemas basados en DES y en algoritmos de llave pública. El KDC es un sistema anfitrión muy seguro, el cual está dedicado a la función de un intermediario confiable en le establecimiento de asociaciones que requieran seguridad. El KDC genera una llave de sesión y la distribuye a los usuarios transmisores. Estos usuarios transmitirán dichas llaves a los usuarios receptores. Entonces, los usuarios pueden comenzar a encriptar y desencriptar sus paquetes de voz para toda la sesión. Hay que decir que algunas variaciones en la generación

y distribución de las llaves de sesión son posibles, depende de las necesidades particulares de cada sistema.

El DES y los algoritmos de llave pública pueden ser usados para la generación y distribución de las llaves de sesión. El DES es mucho más rápido para encriptar y descifrar que los algoritmos de llave pública. Para voz el DES es más adecuado debido a su bajo índice de posible retraso, mientras que los algoritmos de llave pública poseen un índice más alto, y para transmisión de voz se necesita trabajar en un ambiente de tiempo real, por lo que el DES es más usado. Para encriptar y desencriptar , si es necesario usar DES.

4.7 ADMINISTRACIÓN DE LLAVES.

Existen dos hechos principales en este apartado: a) Generación de llaves y b) Distribución de llaves, y a continuación se detalla cada uno:

a) Generación de llaves.

Para este hecho, existen dos tipos de llaves a usar y las nombraremos:

1) Llave de sesión: Para mantener la seguridad de los mensajes

2) Llave pública. Para el intercambio de llaves e incluye dos llaves:
   - Llave pública: Esta llave es conocida por el público.
   - Llave privada: Esta llave es conocida por el usuario solamente. Aún el KDC no la conoce.

Cada usuario puede generar una llave de sesión por sí mismo, la cual es un número aleatorio de longitud variable. Y para mantener la seguridad de los mensajes, esta llave

puede ser actualizada frecuentemente por el mismo usuario. Todos los usuario tiene que registrar sus llaves en el KDC, siempre que requieran acceso a la

red. En general, esta llave no necesita ser cambiada antes de terminar la sesión, pero si para el inicio de la siguiente.

Ahora veremos un pequeño ejemplo:

1)La llave convencional (en un sistema de una llave) para la seguridad de los mensajes.

2) El sistema de llave pública (sistema de dos llaves) para el intercambio de la llave de sesión.

La idea básica es que cada usuario A tenga una llave pública EA, la cual es registrada en un directorio público en el KDC, y una llave privada DA, la cual es conocida solo por el usuario A. EA es la llave usada para el encriptamiento público de información y DA es la llave usada para el descifrado de la información. La segunda clave es relacionada con la primera, pero es imposible computacionalmente hablando determinar DA del conocimiento de EA.

Los siguientes pasos generales ilustran la generación y distribución de una llave de sesión entre dos usuarios A y B para una comunicación segura.

ALGORITMO:

PASO 1: Cuando el usuario A requiere acceso:

Genera EA y DA.

Después envía EA al KDC.

A – KDC : EA

(Ya que esta llave EA es conocida públicamente no necesita ser encriptada para ser transmitida).

KDC almacena EA en su directorio de llaves.

PASO 2: Cuando el usuario B requiere acceso:

Genera EB y DB.

Después envía EB al KDC.

B - KDC : EB

KDC almacena EB en su directorio de llaves.

PASO 3: Siempre que el usuario A quiera tener una comunicación segura con el usuario B, entonces el usuario A requerirá al KDC para obtener la llave pública de el usuario B y una llave de sesión SK.

A --- KDC. Requiere EB y SK

KDC generará una llave de sesión SK y la enviará EB y SK al usuario A, bajo el encriptamiento de la llave pública EA del usuario A.

KDC – A : EA (EB, SK)

El usuario descifrará este mensaje usando su llave privada DA y obtendrá EB y SK.

El usuario A enviará SK al usuario B bajo la protección del encriptamiento público EB del usuario B.

A – B : EB (SK)

Ya que solo el usuario B conoce DB, nadie más puede descifrar este mensaje para obtener SK. Ahora los usuarios A Y B tienen la llave de sesión SK para asegurar sus comunicaciones.

La generación y distribución de la llave de sesión mencionada anteriormente entre los usuarios A y B se desarrolla durante la fase de establecimiento de la conexión en la operación del circuito virtual en la WAN. Después en la fase de transferencia de datos los siguientes eventos tiene lugar:

PASO 4: Siempre que el usuario A quiera enviar un mensaje de voz paquetizada M al usuario M en modo secreto, ya que A tiene SK, puede enviar el texto cifrado como se muestra a continuación:

$$A - B : ESK (M) = C$$

donde C es el texto cifrado.

PASO 5: Cuando el usuario B recibe el texto cifrado C, lo puede descifrar usando su llave de sesión SK para obtener el mensaje M.

$$B : DSK (C) = M$$

Ya que solo el usuario B conoce la llave de sesión SK, nadie más puede obtener el mensaje de voz M. Al final de la transferencia de datos, la conexión se pierde y la llave de sesión es destruida. Algunas variaciones en el esquema anterior son posibles.

Como se mencionó en las secciones precedentes, las señales de voz pueden ser paquetizadas y encriptadas y después transmitidas al destino donde serán descifradas y reconstruidas a su forma original de señales de voz.

A continuación hablaremos en concreto de algunos sistemas telefónicos, que se usan actualmente y son considerados seguros para transmitir voz.

Existe una terminal, descrita por Diffie, para ISDN (Integrated Services Digital Network), que fue desarrollada en los laboratorios de investigación Bell-Northern. Puede enviar voz y datos a 64 Kbps. La criptografía pública es usada tanto para el intercambio de llaves como para la autenticación. Evidentemente es usado en conjunción con el DES.

Aunque no hay mucha información al respecto, la poca que existe indica que también utiliza firmas digitales, pero su implementación no está esclarecida.

En este sistema existe una llave para cada llamada. De esta forma, si llaves de larga duración están comprometidas, grabaciones de llamadas anteriores y posteriores serán decodificadas.

Las computaciones de llave pública de la terminal son implementadas vía un chip de procesamiento digital de señales (DSP), mientras que un circuito aparte implementa el DES, el cual es usado para el encriptamiento de datos. La administración de llaves involucra llaves instaladas en teléfonos, portadas por los usuarios e intercambiadas electrónicamente.

Cada terminal construida en Bell-Northern Research, Inc. (BNR) incorpora un teléfono de tacto M3000.

Un componente público-privado es instalado en el teléfono, éste es llamado llave intrínseca. El componente privado está contenido en un compartimiento sellado dentro del teléfono. El componente público sirve como el nombre del teléfono. Ambos no pueden ser alterados.

Una segunda llave pública almacenada en el teléfono es la llave del propietario. Esta es utilizada para autentificar las órdenes del propietario legítimo. Esta puede cambiarse mediante un comando firmado por el actual propietario para transferirlo a uno nuevo.

Una tercera llave pública en el teléfono es la llave de red. Esta identifica la red a la que el teléfono está asociado. Valida comandos firmados con el componente privado de la KDC. Puede autentificar llamadas de usuarios de la red y puede ser cambiada por medio de un comando firmado por el propietario.

Un componente de corta duración se encuentra almacenado en el teléfono y está firmado por el KDC. Durante el proceso de establecimiento de una llamada, los teléfonos intercambian certificados. La llave de red es usada para autentificar los certificados, y permite realizar las llamadas entre estaciones.

Más información es necesaria para autentificar llamadas de persona a persona. Esta información está contenida en un hardware llamado "llave de ignición", el cual debe ser insertado en el teléfono. Esta llave contiene el componente privado del usuario encriptado bajo una contraseña secreta conocida solo por el usuario. También contiene un certificado firmado por el KDC que contiene el componente público del usuario e información extra que sirve para su identificación. Esto último también está encriptado. El desencriptado de la información en la "llave de ignición" es efectuado gracias a la contraseña digitada en el teléfono de tacto.

Para agregar usuarios certificados y autorizados se utiliza el teléfono desde el KDC.

Una llamada persona a persona empieza como se describe a continuación: el usuario que llama inserta su llave de ignición y digita su número. El teléfono interroga a la llave de ignición para revisar la identidad del usuario. El teléfono revisa su memoria para encontrar un certificado de autorización para el usuario; si no lo encuentra lo adquiere del KDC. Después el teléfono marca el número del destino.

Los dos teléfonos establecen contacto. Esto empieza con un intercambio de llaves El teléfono que llamó transmite su certificado y autorización de uso. El teléfono receptor emplea pruebas, demanda respuestas en tiempo real y en tiempo dependiente, todas deben estar firmadas. Esto asegura que los certificados no son reproducidos de una conversación anterior. Una respuesta es formada por el teléfono transmisor y otra con la llave de ignición del usuario.

Ahora el teléfono llamado envía sus certificados y respuestas en tiempos distintos. La persona llamada inserta su llave de ignición. Si el teléfono llamado no tiene autorización debe obtener un certificado. Después se envían nuevas respuestas y pruebas, y finalmente la conversación puede empezar.

4.8 ALGUNAS ESPECIFICACIONES PARA TELEFONOS ISDN.

Para lograr la utilización en masa de la ISDN, fue necesario ofrecer dispositivos de comunicación de voz a precios equivalentes a los de los teléfonos análogos.

Se han desarrollado teléfonos basados en los siguientes objetivos:

a) Funciones Sofisticadas Internas.- Para lograr que los teléfonos ISDN llamen la atención de los usuarios, deben estar provistos de las capacidades de la ISDN. Algunas de estas funciones son: aceptación selectiva de llamadas, grabación de llamadas entrantes, etc. Funciones que habilitan el uso de servicios suplementarios también están previstos. Algunas funciones familiares a los usuarios de los teléfonos análogos también están instaladas, como: marcación abreviada, melodía de espera, etc..

b) Persecución de costos más bajos.- El reducir el precio de los teléfonos ISDN, requiere reducir el costo de los principales componentes. Para lograr esto, se deben

diseñar nuevos aditamentos que abaraten las funciones actuales o reduzcan las funciones superfluas para algunos usuarios.

c) Operación por alimentación de línea.- Los teléfonos convencionales operan por alimentación de línea y surten los medios para la comunicación los cuales deben estar siempre disponibles, especialmente en emergencias. La mayoría de los teléfonos multifunciones, como los que poseen contestadora automática, están diseñados también para que al menos las comunicaciones básicas funcionen con la alimentación de línea. Todos los nuevos teléfonos de ISDN están diseñados para que las funciones básicas puedan operar cuando al menos exista una alimentación por línea esté disponible. El teléfono de diseño básico está habilitado, para que casi todas las funciones, incluyendo una bocina altavoz, opere con alimentación de línea.

Estos teléfonos ISDN satisfacen algunas condiciones de consumo de poder definidas por la interface del usuario de la red en un modo restringido de abastecimiento de poder (un máximo de 380 mW en un estado activo y un máximo de 25 mW en un estado desactivado). Especialmente, en un estado desactivado, la operación de casi todos los circuitos cesan para satisfacer esta condición. En el estado desactivado, el poder para el circuito principal, el amplificador para la bocina principal, las señales de reloj para las funciones de los circuitos lógicos son cortadas. Los circuitos del teléfono son desactivados por el circuito de control cuando la llamada es completada, y están en este estado hasta la siguiente llamada o hasta que es detectado un cambio en la llave de operación.

Un diagrama a bloques del circuito que detecta llamadas y las operaciones del cambio de llaves es mostrado en la figura 45. Cuando una llamada entra la interfaz LSI detecta una cambio en las señales de salida del receptor. Cuando cualquier botón es oprimido, el circuito de control de teléfono detecta un cambio en el voltaje del switch del circuito. Cuando estos cambios son detectados, la generación de las señales de reloj de la interface

LSI y el circuito de control del teléfono comienzan. Todo esto requiere aproximadamente 20 msec.

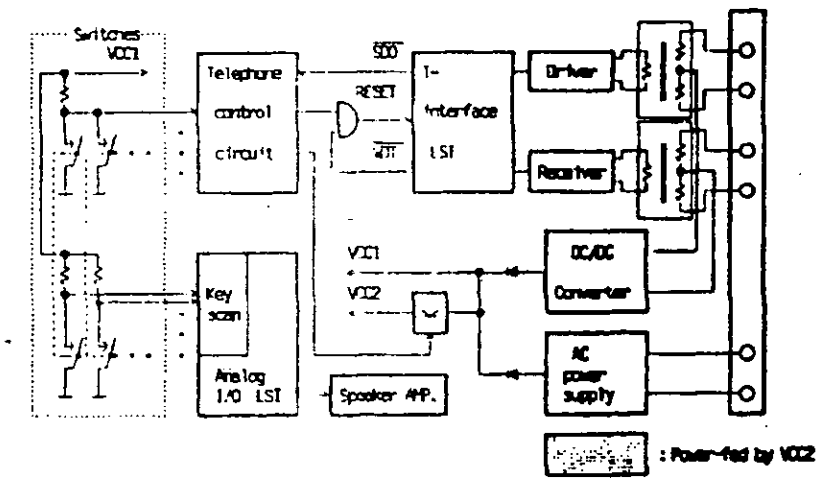


Figura 45

4.8.1 FUNCIONES INTERNAS PARA TELÉFONOS ISDN.

La siguiente tabla suma las funciones internas de los teléfonos ISDN de diseño básico.

Clase	Funciones
Funciones utilizando el diseño básico de ISDN.	Operaciones de llamada ■ Selección de modo de notificación o no notificación de señal ID. Aceptación de llamada. ■ Un tono especial que suena cuando la señal ID es reconocida. ■ Una aceptación selectiva de llamada sobre el reconocimiento de la señal ID. ■ Una aceptación selectiva de llamada sobre el reconocimiento de la dirección de la persona que llama. Display. ■ Muestra el número de la persona que llama. ■ Muestra el cargo de la llamada Almacenamiento y display. ■ Cargos de el total de llamadas. ■ Números incomunicados.
Funciones para el acceso a servicios de la red	■ Suspensiones o resúmenes. ■ Llamadas tripartitas, adición de llamadas, llamadas en espera, transferencia de llamadas, etc.
Funcionales familiares a usuarios de teléfonos convencionales.	Operaciones de llamada. ■ Marcación manual, marcación con el auricular colgado,, marcación abreviada, marcación con memorias. Aceptación de llamadas. ■ Tono con volumen ajustable y selección del mismo. Comunicación. ■ Hablar por el auricular. ■ Recepción en altavoz.. ■ Espera de llamadas con melodía. Display Muestre monitoreo del número marcado, fecha, tiempo, duración

Todas estas funciones con excepción de la corriente para el display de tiempo operan con alimentación de línea, haciendo este teléfono superior a los teléfonos análogos. Estas funciones se clasifican en las siguientes clasificaciones:

1) Funciones que utilizan las funciones básicas de ISDN.- Este teléfono habilita la recepción de la mayoría de los servicios proporcionados por ISDN. Estos servicios incluyen transmisión digital punto a punto, presentación de identificación de llamada en línea, reporte de carga, portabilidad terminal, dirección de la persona que habla, etc.. En la presentación de identificación de llamada en línea, la red envía una llamada ID (el número y dirección de la persona que habla) al receptor. Este teléfono tiene otras funciones útiles para este servicio: indicación de llamada ID, que es un tono especial que suena cuando recibe una señal ID; una aceptación selectiva de llamada después de reconocer la señal ID. Por ejemplo, la aceptación selectiva de llamadas recibe llamadas de transmisores específicos, el teléfono suena solamente si la señal ID de la llamada entrante está registrada en la memoria de nuestro teléfono, de lo contrario la llamada es rechazada y ni siquiera sonará el teléfono. Si el usuario no quiere conocer la señal ID de la llamada, el teléfono no la presentará para su conocimiento. Este teléfono también puede grabar llamadas y señales ID de las tres últimas llamadas con una marca de tiempo e información que indica cuando fue completada la llamada. Estos registros se pueden leer posteriormente y el usuario puede hacer llamadas utilizando estos archivos. Aún más, éste teléfono puede presentar los cargos por llamada cuando el usuario lo requiera.
2) Funciones para servicios de acceso a la red.- para que un teléfono ISDN provea servicios de acceso a la red, debe seguir procedimientos específicos. Tales servicios incluyen redireccionamiento de llamadas, transferencia de llamadas, llamadas tripartitas, espera de llamadas, etc.. El teléfono debe habilitar acceso a todas estos servicios por medio de una simple operación. Por ejemplo, existen teléfonos que

tienen un switch de redireccionamiento de llamadas junto con un área de memoria donde almacenan números y/o direcciones a donde redireccionarlos. Si el switch de redirección esta encendido, el procedimiento automática de redirección desvía cualquier llamada entrante. Al mismo tiempo, este teléfono proporciona acceso a nuevos servicios de la red a través de un identificador (un elemento de información que se distribuya a través de la red). Para éste propósito, debe tener switches de llaves y un software de control para recibir cualquier indicador. Para simplificar esta operación, el teléfono debe tener llaves de funciones programables para enviar un identificador registrado por algún usuario de la red.

3) Funciones familiares a usuarios de teléfonos convencionales.- Algunas de estas funciones son: marcación abreviada, almacenamiento de números, etc.. En el área de aceptación de llamada, existe un control de volumen, selección de tonos, música de espera, etc..

4.8.2 CONFIGURACIÓN DEL CIRCUITO.

Un diagrama a bloques de este teléfono es mostrado en la siguiente figura.

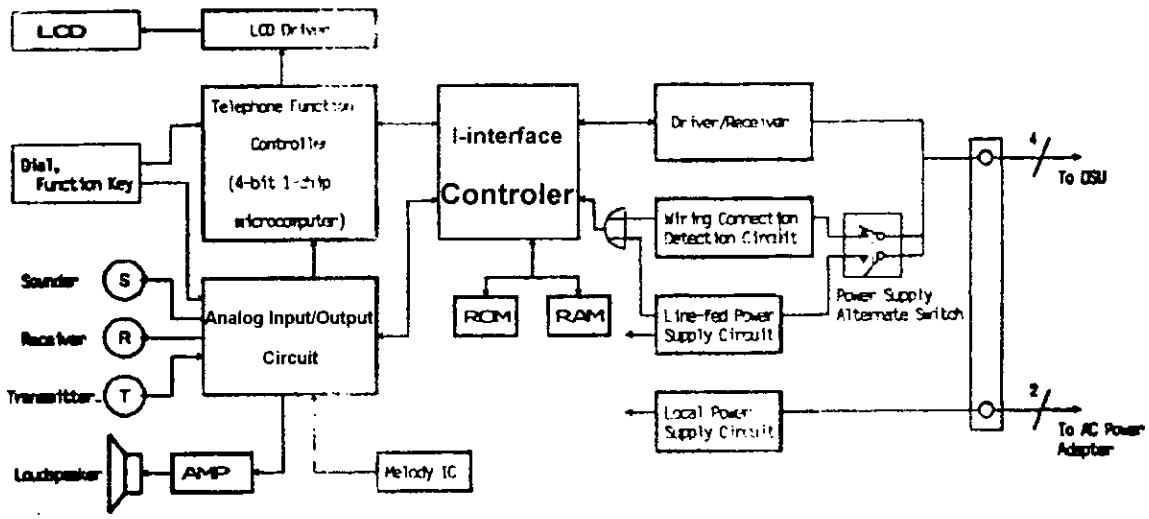


Figura 46

Dependiendo de que si es proporcionada la alimentación por línea, el circuito de detección de conexión declara si el teléfono tiene línea para que el usuario hable. El circuito de alimentación de poder por línea está estructurado con un convertidor DC/DC, el cuál cuando se enciende proporciona un voltaje de 5 V a todos los circuitos. Cuando existen más de dos teléfonos conectados al mismo bus, el circuito local de alimentación funciona para convertir el poder proporcionado por una fuente externa de AC, la cual es convertida posteriormente a DC. Cuando solamente se encuentra un teléfono en el bus la alimentación de AC es innecesaria.

Este teléfono utiliza un segmento tipo LCD (Liquid Crystal Display), ya que este dispositivo tiene las ventajas de un alto contraste, un bajo consumo de poder y un bajo costo. Los

segmentos tiene asignados 16 números (7 segmentos por número) y 16 símbolos, con los números usados para señales ID, marcación de números telefónicos, tiempo, indicador de funciones, etc. y los símbolos usados para indicar el estado tanto del teléfono como de la red.

La posición de las llaves indican el tipo de servicio que se está usando. Las llaves para las funciones de teléfono ordinario están localizadas en la parte frontal superior del teléfono y las llaves para las funciones para ISDN están localizadas junto al display, abajo de las primeras. Algunas llaves se consideran clasificadas y están especialmente marcadas para una operación fácil.

Las principales especificaciones de este teléfono están marcadas en la siguiente tabla. El volumen máximo del altavoz es de 70 dB. Con una alimentación por línea y de 76 dB con alimentación local. El máximo volumen de la campana es de 80 dB. Estos valores son equivalentes a los convencionales de teléfonos análogos. Este teléfono satisface las condiciones de consumo de poder con una alimentación restringida.

Característica	Especificación
Interfaz de la red	Interface de acceso básico para ISDN
Volumen máximo del altavoz y de la campana.	■ Poder de operación de una alimentación de línea: 70 dBsp ■ Poder de operación local: 76 dBsp
Máximo	80 dBsp
Disipación del poder de la alimentación de línea.	En estado de espera: 17 mW En estado de conversación: 165mW En estado de campana funcionando: 200 mW
Calidad de transmisión.	■ Tasa de volumen enviado: 8 dB ■ Tasa de volumen recibido: 2 dB ■ Tasa de tono de espera: 13 dB
Dimensiones	Aproximadamente 203 X 217 X 85 mm
Peso	Aproximadamente 1Kg. (excluyendo adaptador de AC)

4.8.3 TELÉFONO PARA ISDN CON VOZ CIFRADA.

Para las comunicaciones de voz, los esfuerzos fueron concentrados para evitar intervenciones no deseadas en las transmisiones. La comunicación de voz cifrada puede ser conducida con el mismo aparato telefónico. Un diagrama a bloques es mostrado en la figura 47. Casi todos los circuitos son los mismos que los de los teléfonos básicos para ISDN. La unidad de encriptamiento está insertada entre la terminal digital de entrada/salida del codificador de voz y la terminal de entrada/salida del canal de la interface LSI. Este debe desarrollar el encriptamiento y el desencriptamiento rápidamente sin obstruir la

comunicación. La llave necesaria para el encriptamiento y el desencriptamiento es guardada en el controlador de funciones del teléfono. El teléfono tiene un modo de seleccionamiento para escoger entre comunicación de voz encriptada y comunicación de voz normal.

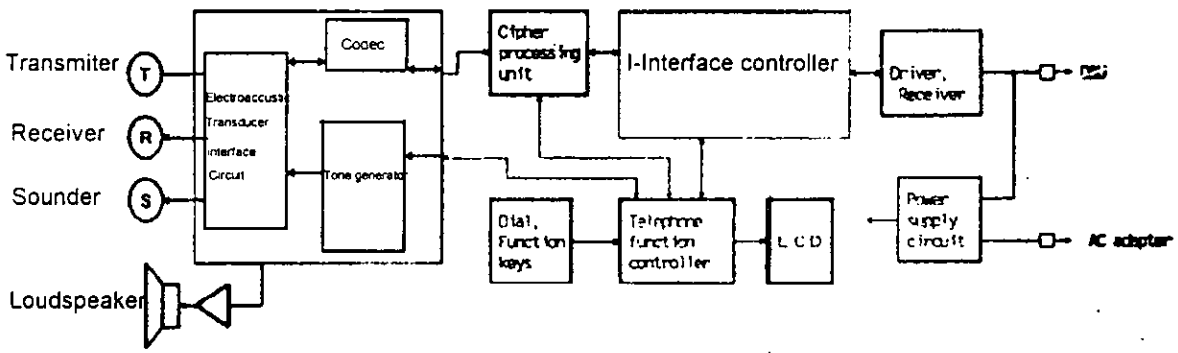


Figura 47

Este teléfono debe conducir transmisiones de voz cifrada sin deterioramiento de la misma debido al encriptamiento y desencriptamiento a utilizar. Otros objetivos son el bajo costo del aparato y la reducción del tamaño.

4.9 OTRO SISTEMA SEGURO DE TRANSMISIÓN DE VOZ.

Ahora hablaremos brevemente de otro sistema bastante utilizado en la actualidad para proteger llamadas telefónicas. A mediados de los años ochenta, la criptografía pública finalmente alcanzó su reconocimiento oficial. En 1983, la NSA empezó estudios de facilidad para un nuevo sistema seguro transmisor de voz. Existían menos de 10,000 de sus más modernos sistemas el Secure Telephone Unit o STU-II y el KDC de la red principal ya estaba saturado, y con muchos usuarios quejándose de la calidad de las transmisiones. A 12,000 dólares cada unidad, 10,000 unidades era lo más que podía pagar el gobierno, pero no cubrían las necesidades del mismo. En su deseo de proteger más que solamente conversaciones explícitas y clasificadas, la NSA soñaba con millones de teléfonos, capaces

de entablar comunicaciones con quien quisieran, lo cual no podía ser debido a la saturación del KDC.

El sistema a ser reemplazado empleaba distribución electrónica de llaves que permitía al STU-II, utilizar un encriptamiento de punto a punto con llaves distintas en cada llamada. Cuando un STU-II hacía una llamada a una terminal con la cual no compartía una llave, adquiría una llamando al KDC.

Aunque el STU-II parecía maravilloso cuando fue creado a finales de los años setenta, tenía algunas desventajas, como por ejemplo, no aceptaba todas las llaves existentes, y el adquirir una significaba costo extra. Peor aún, cada red debe tener un mismo nivel de disponibilidad, porque no había forma de que el STU-II pueda informar a su usuario, del nivel de disponibilidad que tiene el teléfono con el cual está entablando comunicación. Estos factores, junto con el precio y el gran tamaño, conspiraron contra la facilidad de seguir construyendo una red para los STU-II.

El STU-III, que se muestra en la figura 48, es del tamaño de un teléfono convencional y cuando salió al mercado costaba aproximadamente 3,000 dólares, más barato que su predecesor. Está equipado con un display de dos líneas, que provee información acerca de la localización, afiliación y posibilidades de la persona con la que se está hablando. Esto permite usar el teléfono para proteger la información en varios niveles de seguridad. Estos teléfonos son lo suficientemente resistentes a intervenciones físicas, a diferencia de el equipo fabricado anteriormente. Todos estos y otros elementos permitían al nuevo sistema estar mucho más disponibles, proyectando usarse para principios de los años noventa entre medio millón y tres millones de unidades.

Figura 48

Para hacer una llamada segura con un STU-III, la persona que llama primero se comunica de manera ordinaria con otro STU-III, después inserta un dispositivo en forma de llave que contiene una variable criptográfica y oprime el botón "go secure". Después de aproximadamente 15 segundos, en los que el encriptamiento se prepara e instala cada teléfono intercambia información acerca de la identidad y la autorización de los usuarios en sus displays, después la llamada puede proceder.

En una acción sin precedente, Walter Deeley, director general para la seguridad en la comunicaciones de la NSA, anuncio que el STU-III, en una entrevista exclusiva al New York Times. El objetivo del nuevo sistema era principalmente dar seguridad en transmisiones voz y datos a baja velocidad para el Departamento de Defensa de los Estados Unidos y sus contratistas. La entrevista no reveló mucho de como iba a trabajar, pero poco a poco después se supo que el nuevo sistema usaba llave pública.

Una nueva aproximación a la administración de llaves se reportó en un artículo que hablaba de teléfonos que podían ser "reprogramados una vez al año por medio de un enlace telefónico seguro", esto minimizaba las necesidades de los teléfonos de llamar constantemente al KDC. Reportes posteriores hablan de un sistema de administración de llaves llamado FIREFLY, el cual evolucionó de la tecnología de llave pública y es usado para establecer llaves de encriptamiento mediante una técnica que combinaba el intercambio de llaves y certificados similar al que se usa en ISDN y es posible que se base en la exponenciación, su descripción y detalles de funcionamiento están censurados por el Congreso de Los Estados Unidos.

Tres compañías manufacturaron los instrumentos, AT&T, Motorola y RCA, mientras que GTE construyó el sistema de administración de llaves. Inicialmente tuvieron pedidos de 75,000 unidades y su entrega comenzó en Noviembre de 1987.

4.10 LA BATALLA POR EL CONTROL DE LA TECNOLOGÍA DE ENCRIPTAMIENTO.

No hace mucho, mencionar encriptamiento evocaría visiones de James Bond o decodificadores en forma de anillo de cajas de cereal. Hoy en día, el encriptamiento es una parte real y muy común de los dispositivos de comunicación, como los teléfonos inalámbricos y celulares, redes de computadoras de cualquier tipo. Su propósito, a diferencia de la ilustrada en las historietas, es proteger la privacía y seguridad de los mensajes y otra información de carácter sensible, tal como transferencias electrónicas de dinero o contratos acordados electrónicamente. De cualquier forma, el mundo tiene necesidades conflictivas y se ha vuelto una necesidad utilizar esta técnica de protección a nivel masivo.

Hay básicamente dos tendencias en conflicto por el control de el encriptamiento. La primera la constituyen las agencias judiciales y de inteligencia, la National Security Agency, CIA, FBI, etc., quienes desean utilizar vigilancia como una herramienta para combatir crímenes, en especial el narcotráfico, pero también espionaje industrial, y cualquier cosa que, según ellos, amenace con la seguridad nacional. Las herramientas de regulación a su disposición incluyen:

- Acta de Exportación Administrativa.- Autoriza al presidente a prevenir la exportación de materiales y equipo que puedan ser considerados dañinos a la seguridad nacional si entidades enemigas los utilizan. Es necesario bloquear la exportación de armas y municiones. Como el encriptamiento es considerado como tecnología con fines civiles y militares, está sujeto a este acto.
- Acta de Seguridad Patente.- Permite al gobierno clasificar patentes pendientes y suprimir dispositivos de consumo, incluyendo encriptadores, para proteger la seguridad nacional.

La segunda tendencia la componen las compañías telefónicas y de computadoras, las cuales se quejan de cualquier requerimiento legal nuevo. También está el público en general o usuarios, quienes se arriesgan a perder su privacía. Los Profesionales en Computadoras para la Responsabilidad Social, una organización nacional compuesta por gente dedicada a la computación y otros intereses individuales que reside en Palo Alto, California, cree que debería existir un nuevo standard pública de encriptamiento para proteger las comunicaciones privadas y que las agencias de inteligencia no deben interferir con su creación.

También creen que existe un conflicto inherente de intereses cuando la agencia autorizada a intervenir comunicaciones es la misma que define el sistema que protege la

privacía individual. Ellos creen que el interés nacional está a favor de la promoción de tecnologías que aumenten la seguridad y del flujo libre de información científica.

Esta opinión se basa en que estas agencias se están involucrando demasiado en el desarrollo de encriptamiento. Se han obtenido memorándums internos de el Instituto Nacional de Tecnologías y Estándares (NIST), que indican que la NSA está usando asistencia técnica como una forma de asumir el control primario de los desarrollos criptográficos. Esta es una violación al Acto de Seguridad Computacional de 1987,la cual designa a la NIST como la principal agencia para el encriptamiento civil y limita la influencia de la NSA en seguridad no militar.

También algunas compañías ven a estas agencias involucradas hondamente, como una amenaza para su futuro:

- AT&T ha declarado repetidamente que la privacía es una parte esencial de sus negocios. Si la gente pierde esa confianza en esa privacía, tal vez ellos empiecen a evadir el uso de los teléfonos. También es muy caro rediseñar miles de equipos que satisfagan nuevos requerimientos.
- Otras compañías temen al espionaje industrial de compañías y gobiernos extranjeros, porque ellos dicen que el estándar de encriptamiento que ellos proponen es muy fácil de burlar.
- Los servicios que algunas empresas ofrecerán en el futuro, como el voto electoral electrónico, demandarán confidencialidad absoluta.
- Aquellos que deseen exportar dispositivos de encriptamiento deberán pasar a través de un largo proceso de revisiones para asegurarse de que la NSA pueda mantener su habilidad de vigilancia. En lugar de producir dos líneas de productos distintas, una para uso doméstico y otro para exportación, muchas empresas prefieren no ofrecer

el servicio de encriptamiento, en lugar de ofrecer una versión de seguridad débil aprobada por la NSA. Industriales de Estados Unidos han perdido parte del mercado frente a compañías extranjeras que pueden ofrecer un servicio mucho mejor. Y la opinión pública ha perdido su confianza en asegurar su privacía.

Existen dudas acerca de la efectividad de las intervenciones por parte de las agencias gubernamentales como una medida para la prevención del crimen. De acuerdo a datos del Departamento de Justicia de Estados Unidos, en 1992, existían 1,000 líneas intervenidas comparadas con más de 140 millones de líneas instaladas y medio trillón de llamadas realizadas en 1991. La cantidad y la duración de las llamadas se han multiplicado tres veces en los últimos 20 años, pero ahora menos del 20% de las llamadas intervenidas son de utilidad para la policía. De hecho , los arrestos debido a intervenciones telefónicas suman anualmente solamente 3,000 de los 14 millones arrestos que se hacen en total.

También existe la problemática de intervenciones ilícitas por parte de las agencias gubernamentales y empresas privadas. Muchos estados han reportado tales incidentes.

Desde los años setenta se han hecho esfuerzos obvios para detener el uso masivo de el encriptamiento, cuando el conocimiento de su utilización alcanzó niveles fuera de las agencias de inteligencia gubernamentales y judiciales y notaron que era necesario controlar la criptografía pública.

En 1972, el NBS se propuso crear un estándar de encriptamiento para información sin clasificar si era para uso gubernamental o público. El NBS hizo una convocatoria para desarrollar algoritmos y pidió a la NSA que proporcionara soporte tecnológico. IBM propuso su algoritmo llamada Lucifer, el cual tenía una llave de 128 bits. El NSA redujo la llave a solo 56 bits, cambió parte de la estructura interna y lo distribuyó como el algoritmo

modificado conocido como DES. Muchos criptógrafos prominentes creen que este corte en la llave del algoritmo, fue para facilitar la violación del código.

En 1975, los oficiales del NSA reclamaron control absoluto sobre los desarrollos criptográficos e intentaron prevenir de que la Fundación Nacional de Ciencias (NSF), proporcionara herramientas a los matemáticos que desearan estudiar encriptamiento. La NSF rechazó la propuesta de la NSA, pero permitió que revisara algunas propuestas estrictamente por su mérito técnico.

En 1975, la NSA intentó usar el Acta de Privacía de Patente para suprimir al Phasorphone, un aditamento de 100 dólares que conectado a cualquier teléfono invertía las frecuencias de la voz para evitar escuchas no deseadas. Cuando su inventor lo dio a conocer a los medios de comunicación, la NSA anuló su supresión calladamente.

A pesar de estas batallas la diseminación de la criptografía a través de todo el mundo continua, y no precisamente en pequeñas cantidades ya que el transferir datos cruzando fronteras es fácil. Cabe mencionar que algunos expertos en criptografía viven Europa y en Israel y numerosos paquetes están disponibles por todo el mundo.

Los cryptos son unas cajas que cuestan 50 dólares y se pueden encontrar en las calles de Moscú, las cuales ofrecen encriptamiento público utilizando DES y RSA (la caja explica estos términos en la parte inferior de la misma). Otro programa conocido como, Pretty Good Privacy, fue creado en los Estados Unidos, pero está disponible en todo el mundo por Internet y en muchas mesas de boletines. Las más recientes versiones del PGP fueron creadas en Europa e importadas a Estados Unidos para evadir las estrictas leyes de exportación de Estados Unidos, Europa no es tan estricta en sus leyes de exportación de software después de la guerra fría.

Mientras que el encriptamiento se vuelve algo común en muchos programas y productos de consumo general, el FBI y la NSA están renovando sus esfuerzos legislativos y administrativos para expandir sus límites de influencia.

En 1991, el Instituto Nacional de Estándares Americanos (ANSI), consideró un nuevo estándar de encriptamiento para teléfonos celulares. La NSA creyó que éste estándar sería muy difícil de romper y amenazaría el bloqueo de exportaciones por teléfono. Los fabricantes de teléfonos aceptaron consecuentemente un estándar que es vulnerable a ser violado por cualquier usuario bastante hábil en el manejo de una PC. En contraste cuando las agencias judiciales de Australia hicieron una propuesta similar en 1993. El gobierno australiano la rechazó, y propuso un estándar aún más seguro, el cual ni siquiera las agencias judiciales pueden violar.

También en 1991, el FBI pidió al entonces Senador Joseph Biden, que introdujera una resolución que recomendara, que con la autorización legal correspondiente, las compañías telefónicas intervinieran llamadas encriptadas para oficiales de instituciones judiciales. Surgió una oposición por parte de las industrias y grupos defensores de derechos civiles que hizo retroceder a tal resolución, los cuales decían que tal acción limitaría el desarrollo y la diseminación de la criptografía.

En marzo de 1992, el FBI acudió al Comité Judicial, con una propuesta que requeriría que todos los proveedores y fabricantes de servicios y equipo de telecomunicaciones, a rediseñarán sus equipos para satisfacer un estándar propuesto por el mismo. Para minimizar publicidad, el FBI intentó que la propuesta se le adjudicara a una institución ya existente (la cual se convertiría más tarde en el Acta de Reautorización de la FCC), y designar a la Comisión Federal de Comunicaciones, como la agencia que estaría a cargo de exponer los requerimientos técnicos para su cumplimiento. Los proveedores serían multados con

10,000 dólares diarios por no cumplir y aunque solamente tenían 180 días para rediseñar e instalar sus nuevos sistemas, ellos podrían recuperar el dinero gastado incrementando sus tarifas. No es necesario decir que toda esta propuesta causó controversia y nunca fue formalmente presentada.

En mayo de 1992, el FBI regresó con una nueva versión de la propuesta de marzo, la cual le daría poder a un monitor para que aprobara o rechazara todo el equipo de telecomunicaciones. La propuesta decía que todos los proveedores de equipo darían al gobierno y al monitor la facultad para interceptar cualquier transmisión, en un centro de monitoreo aislado dentro de 18 meses a partir de la fecha dada. Las multas seguían siendo de 10,000 dólares por día por no cumplir, no existía mención de como se podrían recuperar los gastos.

Para evaluar esto se utilizó el Acta de Libertad de Información, para requerir documentos de todas las agencias gubernamentales involucradas en la propuesta de mayo y para conocer sus efectos. Los documentos revelaron que había un debate bastante considerable dentro del mismo gobierno respecto a la utilidad de dicha propuesta. La Administración de Servicios Generales, el jefe de la agencia procuradora de equipo de comunicaciones del gobierno de los Estado Unidos, describió a la propuesta como una amenaza a la seguridad nacional textualmente dijo lo siguiente:

"La legislación propuesta podría hacer más fácil para criminales, terroristas, inteligencia extranjera (espías), y hackers, el penetrar electrónicamente en la red pública y espiar en áreas donde previamente era imposible."

La Oficina de Contabilidad General, también encontró problemas:

"Ni el FBI ni las industrias de telecomunicaciones han identificado sistemáticamente las alternativas, o evaluado los costos, beneficios o facilidades..."

A causa de la naturaleza de la controversia y la fuerte oposición, ningún senador o congresista desea patrocinarla, pero la expectación general es que el FBI tratará de proponerla nuevamente.

Desarrollos posteriores para limitar la diseminación de la tecnología de encriptamiento, la Casa Blanca el 16 de abril de 1993, anunció que la NSA creó un chip llamado Clipper, cuya forma de trabajo interna y sus algoritmos podrían convertirse en un estándar para todas las computadoras, máquinas de fax, teléfonos y para todos los contratistas gubernamentales que manejan información sensible. Aunque provee seguridad de algún tipo, el chip tiene una falla significativa. Se designaron a dos agentes confiables de plica, uno de los cuales es un miembro de una agencia gubernamental, que retiene la llave que descifra los mensajes del propietario. Los agentes cedieron la llave al gobierno cuando la requirió mediante una orden judicial. Consecuentemente el usuario debe depender de estos agentes para mantener las llaves seguras. Como criptógrafo Whitfield Diffie opina, que esto crea una puerta frontal y no una trasera al sistema.

La Casa Blanca está revisando la política de Estados Unidos referente a la criptografía, pero los documentos que la realizan no pueden ser revisados por el público en general. En Mayo de 1993, se pidió a la NSA, que hiciera público el funcionamiento del chip Clipper y el lenguaje de la directiva de la política.

Inteligencia y agencias judiciales seguirán tratando de detener el desarrollo de la criptografía, mientras la gente reconozca que esta tecnología es esencial para mantener sus comunicaciones privadas y seguras. Como usuarios hay cosas que todos podemos hacer :

- Incorporar privacía y seguridad, mejorando las tecnologías aplicadas en nuestros productos.
- Aconsejar que al comprar equipo para compañías, eviten dispositivos como el chip Clipper o algún otro sistema que facilite a alguien el romper nuestro algoritmo, ya que puede comprometer nuestra seguridad o la de nuestros clientes.

Involucrarse. Contactar a nuestros representantes gubernamentales y hacerles saber nuestras opiniones acerca de la limitación y control de la tecnología para el encriptamiento de información.

Conclusiones.

Uno de los puntos más importantes a discutir sobre utilizar criptografía es precisamente el saber si es necesario, o justificable su aplicación.

Desde el punto de vista del vendedor o proveedor claro que lo es, si existe y se mantiene en el mercado es porque hay demanda, para bien o para mal se ha llegado al extremo de encontrar gente casi mercenaria que vende software y hardware a quien tenga el dinero, no importando si el cliente es un alto funcionario gubernamental, el presidente de alguna megacorporación, o el dueño de la tienda de la esquina de su cuadra, y no está del todo mal puesto que cualquier ingreso monetario a alguna área provoca mejoras en la misma.

Ahora bien, nosotros como clientes debemos tomar en cuenta muchos factores a corto, mediano y largo plazo, como por ejemplo, nuestros alcances económicos, los beneficios que podemos obtener, en donde utilizarlo dentro de nuestra empresa, que protocolo usa, sus debilidades, actualizaciones próximas (mejoras), velocidad, facilidad de uso (complejidad), capacitación para su operación, etc..

No obstante a la fecha, la seguridad juega un papel preponderante en todo sistema, basta pensar en un banco o una casa de bolsa donde la transferencia es estratégica.

En sí uno de los "obstáculos" para usar criptografía es que sus resultados son abstractos, es decir, a muchas personas les parece mal que empleen dinero para obtener resultados que no se noten a simple vista. Por desgracia el trabajo del sistema de encriptamiento se nota a lo largo del tiempo; dicen que el desempeño de alguna función sale a la luz cuando se comete algún error en el desarrollo de la misma, y los encriptadores

no escapan a eso. Usted como dueño de una empresa muchas veces puede observar a su personal de seguridad como una parte ociosa del dinero que gasta. Muchas veces por la simple presencia se impiden infiltraciones y otras tantas por la acción directa de dicho personal, en el caso de los encriptadores es los mismo. Lo que es muy importante es el estar al tanto de los mejoras y/o nuevos protocolos de protección, porque así como usted tiene un excelente sistema de seguridad hoy en la mañana, en la tarde sus oponentes pueden tener uno mejor.

Con el paso del tiempo, si nadie ha logrado insertar un virus en sus sistemas, sus conversaciones con sus directores regionales, sus transferencias monetarias, conferencias a distancia con sus socios, etc. conservan su privacidad y logra introducir al mercado un producto nuevo antes de su competencia, o bien tomar nuevas direcciones en alguna campaña o fijar nuevas metas en inversiones próximas, etc., todo esto puede resultar en grandes ganancias, que comparado con el gasto que hizo en comprar el equipo de encriptamiento éste último será muy pequeño o hasta insignificante.

No podemos generalizar en las necesidades de todas las empresas, para saber si es necesario, cada entidad debe hacer un análisis de sus necesidades y su posición dentro de su área, para saber si es redituable para él, utilizar criptografía.

En algunas áreas es de carácter indispensable, para estas personas recomendamos el utilizar dispositivos con DES, por varias razones:

- Es el protocolo más usado en todo el mundo y aunque existen otros bastante utilizados en Asia, Oceanía y Europa como el MADRIGA, FEAL, NEWDES, LOKI, CRYPTO-MECCANO, Sesame, KRYPTOKNIGHT, etc., la mayoría de estos son derivados del DES o bien menos eficientes en cuanto a la seguridad que brindan.

- Gracias a la comercialización del DES, es el más fácil de comprar y de manejar por el personal o bien de obtener la capacitación para su uso.
- El Des cuenta con el apoyo de instituciones gubernamentales estadounidenses, lo que indica que debe cumplir con requerimientos bastante estrictos en cuanto su calidad en su funcionamiento.
- Bien puede ser, que sea más fácil cada día romper con la seguridad del DES, pero con la revisión en su algoritmo cada cinco años mejora sobre cualquier otro protocolo; precisamente en 1998 se realizará su próxima revisión.

Otra característica que creemos que debe poseer cualquier sistema de encriptamiento de voz, es la de la utilización de un KDC, debido a que existe un cambio constante en las claves usadas, lo cual mejora notablemente el nivel de seguridad en nuestros enlaces, se obtiene una seguridad mejor dedicando una parte del sistema a la administración de llaves, aumentará la rapidez puesto que nuestros aparatos no tendrán que realizar esa tarea.

Ahora bien, el involucrar una tercera entidad en una comunicación entre dos puntos puede tener algunas desventajas, con esto se incrementan las relaciones de confianza entre los puntos a comunicar y el KDC, que para el punto de vista de algunas personas bien puede ser una baja en el nivel de seguridad, ya que aparte de nuestros adversarios, agregamos a alguien que se encuentra dentro de nuestro sistema a quien no conocemos, y para algunos extremistas el no conocer a alguien implica una desconfianza, ahora bien, una compañía además de vender equipos, también vende confianza, por supuesto n la funcionalidad al 100% de sus equipos y de su desempeño dentro del sistema donde trabaja, y es la base para que cualquier producto logre éxito comercial. Obviamente si el producto y/o el ambiente no funcionan como sistemas seguros para la transmisión de voz, no hay forma de que cumplan con su objetivo principal. Proteger.

GLOSARIO

2-D. *Sistema que combinaba ordenación por división de tiempo y división de banda.*

A-3. *Divisores de frecuencia*

Aleatorio. *Dependiente de algún suceso fortuito*

Algoritmo. *Conjunto de reglas completamente definidas y procedimientos para resolver un determinado problema mediante un número finito de pasos.*

Amplificación. *Aumentar la amplitud o intensidad de un fenómeno físico mediante un dispositivo o aparato.*

Autenticación. *Acción de demostrar la autenticidad.*

Binario. *Sistema de numeración base 2, es decir, al operar sobre variables se pueden tomar dos valores, 0 y 1. El sistema binario se aplica en los ordenadores, en los circuitos lógicos y en la transmisión digital de información.*

Bit. *Abreviatura inglesa (binary digit). Unidad elemental binaria de información, o cantidad mínima de memoria necesaria para obtener el valor 0 ó 1 equivalente a la elección entre dos alternativas igualmente probables (par o impar, sí o no, etc.). La capacidad de un almacén o manejador de información se mide en bits.*
Por ejemplo en el código ASCII (ver ASCII) un conjunto de 7 bits

Buffer. *Área de la memoria ram en donde se almacena provisionalmente la información que transfiere un dispositivo periférico.*

Cardinal. *Se dice de los números que expresan cantidad y no orden.*

Certificación. *Instrumento acreditativo de la verdad de un hecho.*

Circuito virtual. *Circuito creado mediante software, el cual solo tiene un periodo de funcionamiento determinado, ya que no es un circuito físico.*

Clave. *Código de signos convenidos para la transmisión de mensajes secretos o privados.*

Codificador. *Instrumento que se utiliza para representar una información siguiendo una ley descrita en una tabla de correspondencia, denominada código.*

Código. *Sistema de signos destinados a la transmisión de un mensaje. El aspecto general de un código es su carácter arbitrario, que se basa en un consenso (comúnmente aprendido) entre los sujetos que lo utilizan; de esta manera, el mensaje emitido ha de tener cierta forma para que pueda ser trasmitido (codificarlo), debiendo el receptor identificar esta forma al (decodificarlo).*
como 1000111 representa la letra G.

Complejidad. *Calidad de complejo.*

Concatenación. *Enlazar causas, situaciones ideas o cosas, unas con otras como en cadena.*

Confidencialidad. *Hecho o dicho confiadamente.*

Crackers. *Persona dedicada a la intervención y desiframiento ilegal de mensajes cifrados.*

Criptoanálisis. *Arte de descifrar criptogramas.*

Criptografía. *Arte de escribir con clave secreta o de un modo enigmático.*

Criptograma. *Documento cifrado.*

Criptosistema. *Sistema encriptado.*

Chips. *Anglicismo por el cual se conoce los circuitos integrados desarrollados sobre obleas de silicio. Generalmente es una parte rectangular de una oblea de silicio o de otro material semiconductor como Arseniuro de Galio en el cual por sofisticadas técnicas microlitográficas se han implantado o desarrollado complejos circuitos electrónicos.*

El término 'chip' se ha popularizado a partir de la introducción de los microprocesadores en donde tanto éstos como las memorias y otros circuitos de control utilizan chips de silicio con unas dimensiones de entre 4 y hasta 4000 mm cuadrados de superficie.

Los primeros circuitos integrados usaban técnica SSI (Small Scale Integration) con menos de 20 transistores, seguidos por MSI (Medium Scale Integration) por encima de los 100 transistores y LSI (Large Scale Integration) por encima de 10.000 transistores. LSI hizo la construcción del microprocesador posible. La siguiente escala de integración fue VLSI(Very Large Scale Integration) por encima de 20.000 transistores.

En la actualidad se pueden encontrar circuitos integrados con varios millones de transistores.

Ejemplo son los microprocesadores que funcionan como unidades centrales de tratamiento de datos y se aplican en toda suerte de aparatos electrónicos: calculadoras, marcapasos, relojes, robots, videojuegos, etc.

Db. *Unidad práctica de potencia sonora, décima parte del bel.*

Decodificador. *Elemento que forma junto con el contador de programa, los registros auxiliares y el secuenciador, la Unidad Central de un ordenador. La salida del registro de instrucción está conectada al decodificador, el cual se encargará de averiguar de que instrucción se trata y de activar sus salidas para generar las microordenes al resto de los elementos de la CPU.*

Demodulación. *Proceso por el que se recupera la información transmitida por una onda modulada, a través de un circuito que detecta la señal. Es la operación inversa a la modulación.*

DES. *Digital Encrypted Standard.*

Emisor. *Cuerpo o Instrumento que actúa como una fuente de emisión de señales.*

Encriptamiento. *Acción de cifrar las señales para que estas sean solo entendibles para quien el emisor desee.*

FBI. *Agencia federal de inteligencia.*

Fonemas fricativos. *Fonemas que se producen mediante la fricción de algún músculo vocal.*

Glotis. *Orificio superior de la laringe.*

Hardware. *El hardware es, en el ámbito de los sistemas informáticos, los medios físicos que deben estar organizados hacia la realización de un objetivo. El hardware de un ordenador está formado por dos partes: un sistema de proceso o Unidad Central y un Sistema de Entradas y Salidas. A su vez la unidad central se compone de varios elementos: uno pasivo llamado Memoria Central y uno activo que recibe el nombre de Unidad Central de Proceso (CPU). La CPU está integrada por dos componentes principales: la Unidad Aritmética y Lógica (ALU) y la Unidad de Control (UC). Cada elemento efectúa una tarea específica en la ejecución de instrucciones.*

- La Unidad de Control: Es la parte de la CPU que se encarga de desencadenar, dirigir y coordinar el conjunto de tareas simples que es necesario realizar para procesar la información según las instrucciones del programa en ejecución.

- La Memoria Central: Es la unidad de almacenamiento del programa y los datos en curso de ejecución. La información relacionada en el proceso es trasladada de la unidad de almacenamiento masivo a la memoria central, ya que la CPU solo puede operar con la información contenida en la memoria central.

- La Unidad Aritmético y Lógica: Es la unidad que se encarga de operar los datos conforme a las indicaciones de la unidad de control. Las operaciones que puede realizar son: aritméticas, lógicas, desplazamientos y rotaciones.

- El Subsistema de Entradas y Salidas: Propicia el intercambio de información entre la unidad central y los periféricos. Sirve de adaptador entre las lógicas de trabajo de la CPU y los periféricos, ya que estas pueden no ser las mismas.

Hipótesis. *Suposición para sacar de ella una conclusión.*

Homofónico. *Conjunto de voces o sonidos simultáneos que cantan al unísono.*

Incompatibilidad. *Repugnancia que tiene una cosa para unirse con otra, o de dos o más personas entre sí.*

Intersimbolo. *Entre símbolos.*

ISDN. *Red dogital de servicios integrados.*

LAN. *Red de área local*

Muestreo. *Acción de escoger muestras representativas de la calidad o condiciones medias de un todo.*

Técnica empleada para esta selección.

Nodo. *Cada uno de los puntos que permanecen fijos En un cuerpo.*

Paralelismo. *Calidad de paralelo.*

Permutación. *Variar la disposición u orden en que estaban dos o más cosas.*

Poligráfica. *Gráfica compuesta de varias gráficas a su vez.*

Polinomio. *Expresión algebraica compuesta de varios términos.*

Protocolos. *Lenguaje informático de intercambio de información.*

Receptor. *Aparato destina a la recepción de señales eléctricas o radioeléctricas, y su conversión en señales directamente perceptibles, como las acústicas o visibles.*

Redundancias *Sobra o excesiva abundancia de una cosa.*

Rotor. *Parte giratoria de una máquina electromagnética.*

Sincronismo. *Correspondencia en el tiempo entre las diferentes partes de los procesos.*

Sincronización. *Hacer que coincidan en el tiempo dos o más movimientos o fenómenos.*

Software. *Conjunto de programas de un ordenador cualquiera. Se contrapone a hardware.*

Taxonomía. *Parte de la Historia Natural, que trata de la clasificación de los seres.*

Trama. *Tren de pulsos eléctricos, que forman información digital.*

Transductores. *Dispositivo que capta distintas señales (mecánica, eléctrica, magnética, etc.) que intervienen en los procesos industriales y las convierte en otra magnitud física proporcional a la medida y que no tiene porque ser del mismo tipo que la señal medida. Generalmente cualquier magnitud física es convertida por el transductor en una señal eléctrica equivalente, tensión o corriente.*

Un transductor viene caracterizado por:

- Magnitud a medir.

- Principio operativo.

- Elemento sensible a la magnitud a medir.

- Límites de medida, es decir, rango.

- Señal de salida.

Hay distintos tipos de transductores:

Transductores Capacitivos, Inductivos, Piezoeléctricos, Resistivos, Potenciométricos, Fotoconductores, Fotovoltaicos, Termoeléctricos, por Ionización.

Transposición. *Acción del encimamiento de objetos o señales.*

Virus Informático. *Programa oculto con características destructoras de los sistemas computacionales.*

XOR. *Compuerta lógica electrónica or exclusiva.*

BIBLIOGRAFIA.

CRYPTOGRAPHERS.
KAHN, DAVID.
THE CODEBREAKERS, THE STORY OF SECRET WRITING.
NEW YORK.
MCMILLAN.
1967.
1164 pp.

CRYPTOGRAPHY.
CHOR, BEN-ZION.
TWO ISSUES IN PUBLIC KEY CRYPTOGRAPHY. RSA BIT SECURITY AND A NEW KNAPSACK TYPE SYSTEM.
CAMBRIDGE MASSA.
MIT PRESS.
1986.
78 pp.

CRYPTOGRAPHY.
CONTEMPORARY CRYPTOLOGY THE SCIENCE OF INFORMATION INTEGRITY.
GUSTAVUS J. SIMMONS.
PISCATAWOR NJ.
IEEE PRESS.
1992.
640 pp.

CRYPTOGRAPHY.
CRYPTO USERS HANDBOOK: A GUIDE FOR IMPLEMENTORS OF CRYPTOGRAPHIC PROTECTION IN COMPUTER SYSTEMS.
CHRISTOFFERSON.
NEW YORK U.S.A.
EL SEVIER SCIENCE PUB. CO.
1988.
93 pp.

CRYPTOGRAPHY.
MACHINE CRYPTOGRAPY AND MODERN CRYPTOANALYSIS.
DEAVOURS, LOUIS .
DEDHAM MA.
ARTECH HOUSE.
1985.
258 pp.

CRYPTOGRAPHY.
KONHEIM ALAN.
NEW YORK.
WILEY INTERSCIENCE PUBLICATION.
1981.
432 pp.

CRYPTOGRAPHY. PRIMALITY AND CRYPTOGRAPHY.
KRANAKIS EVANGELOUS.
NEW YORK.
WILEY INTERSCIENCE PUBLICATION.
1986.
235 pp.

CRYPTOGRAPHY: A NEW DIMENSION IN COMPUTER DATA SECURITY.
MEYER, CARL H.
NEW YORK.
WILEY INTERSCIENCE PUBLICATION.
1982.
755 pp.

BASE DE DATOS DEL IEEE PROQUEST.
CINVESTAV DEL IPN.
PLANTEL ZACATENCO.
AV. MIGUEL BERNARD S/N. COL. SAN JOSÉ DE LA ESCALERA.

APUNTES DE EL CURSO: "REDES DIGITALES LAN Y WAN".
IMPARTIDO POR EL INGENIERO DAVID B. STOPIER BERMÚDEZ
UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO
CAMPUS ARAGÓN.

INTEGRATED ELECTRONICS.
MILLMAN-HALKIAS.
KOSAIDO PRINTING, JAPAN.
MCGRAW HILL INTERNATIONAL BOOK COMPANY
1986.
911 pp.

SISTEMAS DE COMUNICACIÓN.
B. P. LATHI.
MÉXICO D.F.
NUEVA EDITORIAL INTERAMERICANA S. A. DE C. V.
1986.
703 pp.

DISEÑO ELECTRÓNICO, CIRCUITOS Y SISTEMAS.
SAVANT, RODEN, CARPENTER.
WILMINGTON, DELAWARE. U.S.A.
ADDISON-WESLEY IBEROAMERICANA.
1992.
960 pp.

FUNDAMENTOS Y SISTEMAS ANALÓGICOS PARA SEÑALES ANALÓGICAS.
RAFAEL SANCHEZ LÓPEZ.
MEXICO D. F..
PUBLICACIONES MARCOMBO S. A.
1988.
252 pp.
