PROLOGO

El desarrollo del campo de las telecomunicaciones ha tenido un rápido avance en años recientes y la red global de telecomunicaciones es el más grande y complejo sistema técnico que se ha creado, entendiéndose por telecomunicaciones, a todos los procesos que hacen posible transferir voz, datos y video con ayuda de alguna forma de sistema electromagnético, incluyendo métodos de transferencia óptica.

Estos rápidos cambios demandan un gran conocimiento de las personas que forman la parte activa de las modernas telecomunicaciones.

Desde la década de los cuarenta, la Teoría de las comunicaciones se han desarrollado a lo largo de dos líneas principales, estas líneas tienen sus orígenes en el trabajo de Wiener y Shannon, y son esencialmente de naturaleza estadística. La rama de las Comunicaciones que ha venido a ser asociada con el nombre de Shannon es la Teoría de la Información.

Wiener y Shannon trataron en particular el problema de codificar las señales seleccionadas de un conjunto dado, para hacer posible su apropiada reproducción después de su transmisión sobre sistemas de comunicación ruidosas.

La Teoría de la Información desarrollada por Shannon es una teoría de medida, en el sentido de que suministra al ingeniero de comunicaciones métodos para determinar los límites de ejecución, cuando se transmite información a través de un canal de comunicación con ruido. Shannon ha mostrado que es posible, aun con un canal de comunicación ruidoso, transmitir información a un cierto índice finito, determinado por la línea, con una probabilidad de error que puede ser tan pequeño como sea deseado, este es el mayor resultado de esta teoría.

La teoría de Shannon está relacionada con las propiedades estadísticas de los símbolos seleccionados a partir de adecuados alfabetos definidos (conjuntos), y no está relacionada con el significado asociado con la selección de símbolos. Como Shannon establece: "Estos aspectos semánticos de la comunicación son irrelevantes a los problemas de la ingeniería".

La Teoría de la Información clásica de Shannon proporciona al ingeniero métodos para determinar los límites del comportamiento para un sistema, trabajando sobre condiciones físicamente determinadas, esto se proporciona sólo con indicaciones vagas de cómo debe ser diseñado un sistema de transmisión de datos que ejecute una trans-

misión libre de errores en un tiempo de transmisión finito. Algunos de los principales desarrollos en la Teoría de la Información, durante los recientes años, tienen que ser concernientes con el refinamiento y extensión de la misma y con la vital importancia de problemas prácticos de codificación y decodificación de mensajes que son desarrollados en la transmisión libre de errores.

ÍNDICE

PRÓLOGO 2

UNIDAD I
EL LENGUAJE DE LOS DATOS
Valor de la información.....9
Entropía.....10
Transmisión de datos..... 11
El sistema numérico binario 11
Definición de bit 12
Medición de la información 12
Codificación dela información 17
Errores y paridad 17
Código ascii 18
El espectro de frecuencias 18
Frecuencia de una señal digital 20
Frecuencias de corte 20
Tipos de Ruido 21
Ruido parásito 21
Ruido blanco 21
Efecto del ruido sobre la capacidad del canal..... 22
Elementos de código con múltiples niveles 23
Redes Bluetooth 24
Formación de redes Bluetooth..... 25
Principios básicos de Bluetooth..... 26

UNIDAD II
MODELO DEL PROCESO DE COMUNICACIÓN
Fuente de información..... 33
Fuente codificadora de la señal 33
Codificador de transmisión al medio 34
Decodificador del medio al receptor 35

Canal 35
Fuentes de información discreta y codificación binaria de salidas 36
Una medida de información y función de entropía 36
Propiedades e interpretación de la función de entropía 39
Codificación binaria de una fuente de información 41
Entropía relativa y redundancia..... 43
Canal de comunicación..... 43
Representación de un canal 44
Una medida de la información transmitida sobre un canal 47
Propiedades de la información mutua y la entropía asociada 48
Capacidad del canal 49
Algunos canales simples 50
Teorema fundamental de la teoría de la información 54

UNIDAD III
SISTEMAS CONTINUOS DE INFORMACIÓN
Teorema del muestreo 57
Entropía de una función continua 58
Distribución máxima de entropía 59
Entropía de un conjunto de funciones 59
Potencia de entropía..... 60
Capacidad de un canal continuo 60
Capacidad de un canal por un tipo de ruido arbitrario 62
Códigos de corrección de error 63
Grupo de códigos, códigos de chequeo de paridad 64
Códigos sistemáticos 64
Códigos de detección de error 65
Elementos de codificación de comprobación de paridad 66
Código de corrección de error de Reed-Muller 72
Códigos de producto o iterados 77
Códigos Bose- Chaudhuri 77

UNIDAD IV
TRANSMISIÓN DE DATOS DIGITALES
Razón de error de bit (Ber) 89
Distorsión de cuantización 90
Ruido 91
Jitter 92
Scrambing 92
Transmisión digital de información 93
Combinaciones de modulación 96

Razón de modulación 96
Transmisión en banda base 97
adsl 97
Señales, espectros y filtros 98
Impulsos periódicos unitarios 99
Integral de Fourier 99
Pulso triangular 101
Pulso Gaussiano 101
Distribución Gaussiana o normal 102
Ruido en sistemas de comunicación 103
Niveles de decisión 112
Análisis de ruido 115
Autocorrelación 115
Potencia del ruido 116
Ruido blanco 118
Ruido a través de sistemas lineales 121
Filtros adaptivos 125
Ruido de banda angosta 130
Detección de señales binarias 133

UNIDAD V
ENCRIPTAMIENTO DE DATOS
Lucifer 139
Participación de nsa 140
El lucifer original 141
des 141
Extractos del des 141
Modos alternativos de usar el des 142
Métodos de encriptado de datos 143
Algoritmo encriptador de datos 143
Cifrado 144
Descifrado 146
Características del algoritmo des 149
Modo de libro de código electrónico 154
Modo de cifrado de bloque encadenado 154
Modo de cifrado retroalimentado 156
Relación de cbc y cfb de 64 bits 159
Condiciones de secreto perfecto 161
Seguridad informática 164
edi 167
Proyecto Bolero 168

Sistema swift..... 169
Conexión del sistema swift..... 170
Kerberos: arquitectura de seguridad 171
Firma digital 174
Tarjetas electrónicas 174
Bibliografía 177

UNIDAD I
EL LENGUAJE DE LOS DATOS

Una red de comunicaciones de datos puede ser tan sencilla como dos computadoras personales conectadas entre sí, o por medio de una red telefónica pública que abarque una red compleja de varias computadoras.

En principio, la palabra comunicación se puede emplear en varios sentidos, pero en todos ellos se hace referencia a un intercambio, al traslado de algo de un lugar a otro. En tanto el término telecomunicación, se refiere a un sistema y técnica que permite emisión y recepción de señales, sonidos, imágenes, video o información de cualquier naturaleza por procedimientos ópticos, electrónicos o electromagnéticos.

VALOR DE LA INFORMACION

La mayoría de las personas siempre han dado por sentado que la palabra información, no necesita definición alguna. Han proporcionado, obtenido y procesado información y sentido su necesidad. Sin embargo, cuando empezamos a considerar el tema, surge que la información tan apreciada por algunos significa poco o nada para otros.

La noticia de que Masel computers, Inc. cotizó más bajo que los otros competidores en la licitación de un contrato con el gobierno federal de los Estados Unidos, por ejemplo, tendría, evidentemente, más significado para un grupo determinado de personas que para otro. La noticia de la oferta ganadora llevó la misma cantidad de información a todos los que se enteraron de ésta, pero poseía un significado diferente en cada caso. El término información carece, por lo tanto, de todo valor, salvo el que le asigna quien la recibe. Pero información no es eso, sino un termino inherente cuantitativo, que se mide por el grado con que aclara lo desconocido; un hecho que pueda predecirse totalmente no contiene información, se analizará el valor cuantitativo de la misma en oposición a su valor emocional.

Los párrafos que siguen revelarán con exactitud cuanta información contenía la noticia de que se había adjudicado el contrato. La comprensión de este concepto resultará útil durante el estudio de la eficiencia, los esquemas de codificación y el control de errores.

En la Teoría de la Información se entiende por mensaje simplemente la salida de una fuente informativa. Si la fuente fuese un transmisor telefónico, el mensaje estaría constituido por las tensiones analógicas aplicadas a la línea. Si la fuente fuera una tele-

impresora, el mensaje podría ser un carácter, uno de los bits que integran un carácter o de una palabra. En consecuencia, la composición de un mensaje puede variar y éste debe ser definido o comprendido de acuerdo con su uso dentro de un sistema.

El valor cuantitativo de un mensaje se basa en varios factores. En primer lugar, debe establecerse cuánto se sabía del contenido del mensaje antes de que fuera recibido. Si se conocía que Masel era la única compañía involucrada, la noticia de que había ganado la licitación no hubiera sido ninguna sorpresa y el contenido de información del mensaje hubiera sido cero. No obstante, un mensaje que proporcionara el valor del contrato firmado contendría cierta cantidad de información: se sabía que Masel intervenía en la licitación, pero se desconocía exactamente el importe especificado en la oferta.

En segundo lugar, para poder definir aún más la cantidad de información de que es portador un mensaje, debemos conocer cuántos mensajes componían el conjunto del cual aquél fue seleccionado. Si tres compañías compiten por un contrato, para identificar a la ganadora habrá que enviar uno de los tres mensajes posibles. Si las compañías ofertantes son diez, el mensaje debe ser elegido de un grupo de diez y tendría que portar más información para identificar a la ganadora.

En tercer lugar, para ser más exactos, habría que conocer la probabilidad de cada suceso que el mensaje podría describir. Si cada una de las diez compañías intervinientes tuviese exactamente el mismo volumen de ventas, el mensaje con el nombre de la ganadora llevaría todo lo que se puede saber sobre el resultado de la licitación. Si los volúmenes de ventas de cada compañía fuesen distintos, tendríamos cierta información sobre el desenlace antes de conocer los resultados y, por lo tanto, el mensaje llevaría esa misma cantidad de información de menos.

El cálculo del contenido de información de mensajes con probabilidades distintas resulta muy complejo.

En consecuencia, para contribuir a la clarificación de este análisis supondremos que la información es enviada en forma fortuita y, por consiguiente, que todos los mensajes son equiprobables.

ENTROPÍA

En general, podemos decir que la información posee la propiedad de disminuir la incertidumbre de una situación. La incertidumbre se denomina entropía (H) y existe en la medida en que se carece de información (información + entropía = 100%, o en forma abreviada, 1 + H = 1). Si la entropía de una situación es reducida, sólo se requiere una pequeña cantidad de información para clarificarla. Si la entropía es grande, se necesitará mucha más información antes de que la incertidumbre sea reemplazada por un grado aceptable de claridad.

Si hubiese competido únicamente con Riqo Inc., la cantidad de entropía hubiera sido pequeña; intervendrían tan solo dos fabricantes con el mismo volumen de ventas. Si hubiese pujado contra diez competidores, la entropía hubiera sido grande, porque no

solo habría habido un número mayor de compañías, sino que cada una de ellas habría tenido una probabilidad distinta de adjudicarse el contrato.

Algunos códigos han sido concebidos para disminuir la entropía hasta el punto en que los errores cometidos durante la transmisión pueden ser no sólo descubiertos y localizados, sino también corregidos. Estudiaremos este tema más adelante.

TRANSMISIÓN DE DATOS

El término datos, se refiere a la información que pudo haber sido tomada de documentos originales: como pedidos de venta, tarjetas de tiempo trabajado, registro de producción, etcétera; de algún medio de almacenamiento, como son las cintas magnéticas, o de la memoria de una computadora. El traslado de estos datos entre máquinas situadas a cierta distancia es la transmisión de datos. Las máquinas que se emplean en la comunicación de datos son muy diversas, y los lenguajes que se usan son códigos (generalmente binarios) muy variados, que pueden ser interpretados directamente por la máquina.

En la década de los cincuenta, los estudios efectuados por los Laboratorios Bell y otros, revelaron que si los impulsos eléctricos generados por las máquinas comerciales eran convertidos en tonos audibles de una gama semejante a la de la voz humana, dichos tonos podían ser transportados por la misma red y equipos que se utilizaban para las conversiones telefónicas ordinarias. Con el objeto de ejecutar la función de conversión, se crearon y construyeron dispositivos denominados conversores de datos (data sets), y las máquinas comenzaron a "conversar" entre sí a través de la red telefónica. De esta manera evoluciona el concepto de la transmisión de datos hasta concretarse así: datos (información en el lenguaje de máquina) transmitidos por las líneas telefónicas existentes, pero con la alternativa de poder establecer comunicaciones orales utilizando el mismo equipo, en caso necesario.

Quien estudie transmisión de datos deberá conocer ciertos principios fundamentales acerca de ellos que son: cómo se miden y cómo se diferencian de otros tipos de información.

EL SISTEMA NUMÉRICO BINARIO

El sistema numérico binario es el verdadero lenguaje de los datos, pues la mayoría de los medios electromecánicos y electrónicos que operan con estos tiene dos estados; si o no, más o menos, etcétera. Se necesita un conocimiento básico del sistema binario para poder llegar a entender la comunicación de datos.

Todos los sistemas de numeración presentan varios puntos en común:

1. La base es la que da su nombre al sistema y (viceversa) es igual a la cantidad de dígitos que lo integran.
2. El valor máximo de un dígito del sistema no excede nunca del valor de la base

menos 1.
3. El 0 denota que se ha llegado al término del sistema básico.
4. Las potencias sucesivas de la base indican los valores posiciónales del sistema.

Apliquemos estas reglas al sistema binario de numeración:
1. El término binario indica que el sistema está compuesto por dos dígitos y que, por ende, su base es 2.
2. El valor más elevado que puede tomar un dígito del sistema es una unidad menos que el valor de la base. Puesto que la base es 2, el dígito máximo es 1. El otro digito, naturalmente debe ser 0.
3. Empezando a contar en binario partiendo de 1 como la base es 2, el número siguiente tiene que ser el último de nuestro sistema básico de contabilidad y esta situación se indica mediante el uso del 0. Por lo tanto, el segundo número, después de uno, es 10.

DEFINICIÓN DE "BIT"

La condición binaria es la que posee una cualidad biestable. Por consiguiente, puede existir uno de dos estados: encendido o apagado, si o no, marca o espacio, magnetizado o desmagnetizado, y así sucesivamente. En el sistema numérico binario esas dos condiciones están representadas por los dígitos 1 y 0. Era inevitable que alguien abreviara la expresión "Binary digit" (dígito binario) y, en consecuencia, surgió el término "bit".

Obsérvese que ambos estados binarios se denominan bits, y no sólo el bit "1". Esto se debe a que los dos son portadores de la misma cantidad de información; la presencia de uno significa la ausencia del otro. Comparando con el sistema decimal: la presencia del número ocho, pongamos por caso, posee un significado preciso, ¡pero la mera ausencia de ese guarismo podría tener una variedad de significados!

MEDICIÓN DE LA INFORMACIÓN

Una vez que se ha establecido que la información es un término cuantitativo, se debe determinar cómo medirla con exactitud. Para el caso en que Masel compitiera con Riqo Inc., para designar al ganador existía la elección entre dos mensajes. Casualmente, una propiedad fundamental del bit binario (ya se trate de 1 o 0) es la de poder reducir a la mitad la incertidumbre de la situación. Puesto que sólo dos compañías competían por ese contrato, podría haberse utilizado el "1" binario para significar que había ganado Masel, y el "0" para indicar que la victoria era de Riqo Inc., de modo que la noticia sobre el triunfo de Riqo llevaba un bit de información.

Con el propósito de establecer una comparación: ¿cuánta información o cuántos bits son necesarios para indicar el ganador de un contrato, en cuya indicación intervienen ocho compañías? Si se colocan las compañías en orden y se especifica que el bit "1" indica

la mitad superior de la lista y el bit "0" la mitad inferior, podemos enviar una serie de bits para señalar la oferta ganadora. Puesto que la firma vencedora es Masel y se encuentra en la mitad inferior de la nomina, el primer bit será 0:

Después de que se ha eliminado la parte superior, Masel se encuentra en la mitad superior del resto de la lista, de manera que enviemos un "1":

El bit siguiente fue 0, pues Masel está en la parte inferior de las compañías restantes. Por lo tanto, se han utilizado tres bits (010) para definir una posibilidad entre ocho. Cualquiera que hubiese sido la firma oferente ganadora, sólo tres bits habrían sido necesarios para señalarla. Básicamente, se ha formulado una serie de preguntas (¿la mitad superior?) y las respuestas han sido "si" o "no". Con este ejemplo hemos ilustrado una propiedad fundamental del bit; no solo constituye la partícula más pequeña de información, sino que es también la máxima cantidad de información posible en una elección de si o no.

Con este conocimiento podemos determinar cuantos bits se necesitan para definir una elección entre varias posibles. Recordando que un bit puede ser 1 o 0, podemos utilizarlo para definir una elección entre dos; dos bits definen una elección entre cuatro, tres bits una elección entre ocho, y así sucesivamente. Cada bit agregado duplica el número de elecciones posibles; las elecciones aumentan en potencias de dos.

Un bit:	$2^1 = 2$ elecciones
Dos bits:	$2^2 = 4$ elecciones
Tres bits:	$2^3 = 8$ elecciones
	.
	.
	.
	etcétera

Si se conoce el número de elecciones se puede determinar cuántos bits se requieren para identificar una de ellas. Si en una licitación intervienen ocho compañías, entonces $8 = 2^3$, de modo que se necesitan tres bits, como hemos visto en el ejemplo anterior. Si sólo se hubiesen presentado cuatro compañías, entonces $4 = 2^2$, y con dos bits hubiera bastado. ¿Cómo sería en el caso de que en la licitación hubiesen participado seis compañías?. Seis es menor que 2^3, pero mayor que 2^2, de manera que sería preciso un mínimo de tres bits para identificar al ganador.

En cuanto a la formula $2^3 = 8$, el 8 era conocido (el número de compañías licitadoras) y el 2 también era conocido (con una situación binaria), pero queríamos encontrar el valor desconocido 3, la cantidad mínima de tres bits para identificar una de las ocho compañías. Operando con los valores conocidos (8 y 2), el problema podría haberse enfocado hallando el logaritmo de 8 con respecto a la base 2 lo que se escribe $\log_2 8$. Sinónimo de logaritmo es exponente, de modo que en realidad, estamos buscando el exponente de

2 que de 8 puesto que $2^3 = 8$, entones $\log_2 8 = 3$.

El número de bits que se necesitan para identificar determinada elección en un grupo de N elecciones posibles es $\log_2 N$, siempre que todas ellas tengan igualdad de oportunidades para ser elegidas:

$$I = \log_2 N$$

Un código común de comunicaciones posee 32 caracteres. ¿Cuántos bits debe tener por carácter? Respuesta: $\log_2 32 = 5$ bits. ($2^5 = 32$). ¿Cuántos bits se requieren para un código que describa sin repeticiones los 26 caracteres del alfabeto?. Respuesta: $\log_2 16 < \log_2 26 < \log_2 32$, de manera que se necesitan $\log_2 32$, o sea, 5 bits. Si una pregunta tiene una sola respuesta posible, el contenido de información de esa repuesta es 0: I (información) = $\log_2 I = 0$. Si la pregunta tuviese ocho respuestas posibles, como en los resultados del concurso mencionado, entonces la respuesta contiene I= $\log_2 8 = 3$ bits.

El ejemplo siguiente puede servir para aclarar aún más este concepto. El número de maneras diferentes en que pueden colocarse las cartas de una baraja completa es ¡52! (52! Se lee "factorial 52", y significa 52x51x50x.....x3x2x1). Utilizando la fórmula general, hallamos que el número de bits que puede ser representado por el orden de las cartas después de un baraje (el orden podría ser un "mensaje") es:

$$I = \log_2 52! = 225.7 \text{ bits.}$$

Durante una mezcla cualquiera se divide la baraja en dos mazos aproximadamente iguales, A y B. Las partes A y B representan una situación binaria y la baraja tiene un total de 52 cartas, de manera que A y B pueden combinarse en 2^{52} secuencias posibles. Podemos utilizar la fórmula de información para encontrar el número máximo de bits que un baraje puede producir:

$$I = \log_2 2^{52} = 52 \text{ bits} \quad (\log_2 2^{52} = 52 \log_2 2 = 52 \text{ x } 1 = 52)$$

Entonces, 225.7 dividido entre 52 es igual a 4.3, de modo que se requiere un mínimo de cinco barajes para tener la certeza de que las 52 cartas están dispuestas al azar. ¡Recuérdelo durante su próxima partida de póquer!

De lo que hemos visto hasta aquí, podría suponerse que todos los bits son portadores de información. Sin embargo no es así, y debemos distinguir con claridad los bits informativos de aquellos otros que no lo son.

Un dígito binario puede ser o no portador de información. Una regla empírica, que la mayoría de las veces da resultado, dice que si no es posible predecir con exactitud el valor del bit (1 o 0), contiene información. En cambio si su valor puede vaticinarse en forma precisa, está cumpliendo una función que no es la de llevar información. Por lo tanto, los bits informativos se combinan para formar códigos que representan letras, números y funciones especiales; los bits no informativos se utilizan para que el juego de equipos del sistema (hardware) pueda discriminar dónde termina un carácter o comienza el próximo,

para tener un medio de descubrir y corregir errores, y a fin de que los equipos situados en los dos extremos del circuito alcancen y mantengan la sincronización. Esta distinción debe tenerse presente, pues aclarará más adelante los estudios sobre codificación, control de errores y eficiencia del sistema.

CODIFICACIÓN DE LA INFORMACIÓN

En esta parte analizaremos la forma y el contenido de información de las señales transmitidas por las máquinas comerciales. Con estos conocimientos abordaremos el estudio de los códigos que permiten a las máquinas comunicarse.

Símbolos

Hasta este momento hemos estudiado en términos muy generales el contenido de la información de los mensajes. Definimos el mensaje como la salida de una fuente de información, pero, más concretamente, podría ser un símbolo o un grupo de símbolos: bits, letras del alfabeto, números o caracteres especiales. Además de esos caracteres, también pueden considerarse símbolos el sincronismo y el esparciamiento entre caracteres, e incluso el propio espacio.

Definición de carácter

Por carácter se entiende, según el diccionario, "el símbolo que se emplea en un sistema de escritura...". Podría ser una letra, un número o un símbolo con significado especial, como el periodo o espacio. La codificación de caracteres, para adaptarlos a un sistema de transmisión o procesamiento de la información, consiste en asignarle una combinación discreta de bits.

El carácter puede tener un número variable de bits, según el sistema de codificación empleado (como los códigos Baudot y ascii, de cinco y ocho bits, respectivamente), pero dentro de un sistema todos los caracteres poseen el mismo número de bits.

Codificación

La cantidad de información que puede llevar un símbolo depende del número de símbolos que integran el conjunto del cual fue seleccionado. Ya lo hemos ejemplificado anteriormente, cuando se requerían tres bits para definir un símbolo entre ocho, mientras que para identificar una letra del alfabeto se necesitaban por lo menos cinco. Esta conversión de un conjunto de números en otro se denomina codificación. Si un símbolo complejo se convierte en un grupo de símbolos más simples, o si se pasa de un grupo de símbolos a otro mayor, la codificación es ascendente. Un ejemplo de ello lo constituye la transformación de una letra del alfabeto en cinco bits del código Baudot. En la codificación descendente

la cantidad de símbolos es menor, pero cada uno contiene más información.

Codificación reversible

Se considera que la técnica de codificación, sea ascendente o descendente, es reversible si cada mensaje (carácter, símbolo, grupo de código, etcétera) está codificado de manera distinta a la de cualquier otro mensaje dentro del mismo sistema. En el código Morse, por ejemplo, la letra V se halla representada por tres puntos y una raya. Si la letra Y estuviese formada de la misma manera, la forma de codificación no sería reversible, pues el decodificador tendría que optar arbitrariamente entre Y y V. Para que al decodificar los mensajes se pueda obtener la misma forma que tenían antes de transmitirlos es imprescindible que el esquema de codificación usado sea totalmente reversible.

La unidad de información más pequeña

El estudio de la Teoría de la Información revela que el bit (ya sea el 1 o el 0) es la unidad de información más pequeña, de la misma manera que el átomo es la partícula más diminuta de la materia.

En los medios magnéticos, como la cinta o los discos, los bits 1 y 0 se hallan representados por puntos magnetizados o no magnetizados, respectivamente.

Para formar los caracteres, los bits se combinan de acuerdo con diversos esquemas, proceso que se denomina codificación. En los párrafos siguientes se explican los códigos de uso más comunes.

ERRORES Y PARIDAD

En la transmisión de datos se ha producido un error si la secuencia de los bits recibidos no es igual a la secuencia en que fueron transmitidos. Tal condición es consecuencia de los bits perdidos o con un valor u orden distinto al que tenían. Los factores que dan origen a esos trastornos se analizan más adelante, pero aquí la cuestión es que no pueden impedirse. En consecuencia, siempre existe la posibilidad de que ocurran errores durante la transmisión de datos.

Puesto que la exactitud es de primordial importancia en el tratamiento de la información, se necesita un método para determinar si los datos han conservado, durante el procesamiento, la transmisión o el almacenamiento, el valor o la forma deseados. En los códigos para cinta de papel se agrega un bit de paridad a los bits de información, como medio para controlar errores. El bit de paridad es un bit de verificación que indica que el número total de dígitos binarios "1" de un carácter o palabra (excluido el bit de paridad) es impar o par. Si el bit de paridad indica que el número de dígitos "1" es impar, entones el bit "0" señala que ese número es par. Si el número de bits "1" incluido el de paridad, es

siempre par, se dice que es un sistema de paridad par. En un sistema de paridad impar, el número total de bits "1", incluido el bit de paridad, es siempre impar.

CÓDIGO ASCII

Debido a que el número de combinaciones posibles con el código Baudot está limitado y, lo que es más importante, porque carece de un esquema lógico o secuencial, se han desarrollado nuevos códigos, más flexibles que se prestan fácilmente a la computación.

A la ascii, sigla de American Standard Code for Información Interchange (Código Standard Norteamericano para el Intercambio de Información) también se le denomina código ansi y código para el Intercambio de Datos. Se trata de un código de siete canales a los que se suma un octavo de paridad par.

La configuración de bits del código asciise muestra en la figura 1.1. Los caracteres gráficos (imprimibles) y de control (funciones) han sido encolumnados dentro de líneas dobles. Encabeza cada columna la configuración de bits de orden superior correspondiente a los caracteres o funciones de esa columna. A la izquierda de cada fila se da la configuración de los cuatro bits de orden inferior que representan los caracteres o funciones de esa fila. Codificando la letra F = 1 0 0 0 1 1 0 = orden superior y orden inferior.

EL ESPECTRO DE FRECUENCIAS

Las frecuencias tienen una gama de variación muy amplia: empiezan en 0 y aumentan gradualmente a través del espectro acústico, de radio, infrarrojo (calor), de luz, ultravioleta, de rayos X, rayos gama y rayos cósmicos. La gama audible va de 20 Hz a 20, 000 Hz aproximadamente y es muy variable de una persona a otra. La banda de radiofrecuencias se extiende desde los 14 kHz hasta más de 10 millones de kHz.

La Fig.1.2 ilustra la disparidad entre las frecuencias perceptibles por el oído humano y aquellas que pueden ser transmitidas por un canal telefónico. La voz humana (100 a 1100 Hz), sin embargo, cae casi en su totalidad dentro de los límites impuestos por el circuito de telefonía.

FRECUENCIA DE UNA SEÑAL DIGITAL

La señal con la que se efectúa la comunicación de datos está compuesta por una gama de frecuencias. La frecuencia de la señal, en un momento determinado, depende de la composición del código que se transmite. Para ilustrar esto supongamos que se transmite un carácter cuya representación binaria es 11110000. Si los unos binarios son una tensión positiva y los ceros una tensión negativa, sólo se habría transmitido un ciclo durante el tiempo requerido por un carácter: la tensión de línea habría ido de cero a una tensión positiva (durante los bits "1") y luego habría variado a una tensión negativa pasando por cero mientras se transmitían los "0".

Por otra parte, si se transmitiera un carácter cuyo equivalente binario fuese 10101010, se producirían cuatro ciclos de corriente durante el mismo tiempo requerido. En realidad,

la transmisión del segundo carácter hubiera dado lugar a la máxima frecuencia posible para esa señal en particular, pues se habría producido el mayor número de transiciones de un estado de la señal (positivo) al otro (negativo). Por lo tanto, el número de bits de que puede ser portador un canal de transmisión por unidad de tiempo está directamente relacionado con el límite superior de su rango de frecuencias utilizable.

FRECUENCIAS DE CORTE

Visto que en los medios de comunicación se suponen muchas conversaciones simultáneas (u otra información), es necesario restringir cada una de ellas a su propio canal. Los filtros eléctricos que se utilizan para tal fin forman una banca que deja pasar las frecuencias comprendidas dentro de cierta gama y bloquea aquellas que no lo están. Los puntos situados en los extremos superior e inferior de la banda pasante se denominan frecuencias de corte (véase la figura 1.3).

Si fuera posible transmitir la señal por un canal perfecto, llegaría al destino exactamente como fue enviada. Canales de este tipo, sin embargo, sólo existen en teoría; por lo tanto, las señales se distorsionan durante la transmisión.

Hemos dicho con anterioridad, que el ruido es una fenómeno imprevisible que puede describirse mejor estadísticamente. La distorsión, en cambio, afecta a la señal en forma permanente y es función de cada canal en particular. Existen tres tipos de distorsión que un canal puede transmitir a una señal: distorsión de retardo, distorsión por atenuación e inestabilidad.

TIPOS DE RUIDO

El ruido de un canal está integrado por impulsos eléctricos aleatorios que provienen de varias fuentes y, por lo general, hay muchos tipos de ruido: blanco, térmico, rosa, atmosférico, etcétera.

RUIDO PARÁSITO

El ruido parásito es causado generalmente por el funcionamiento de máquinas y llaves,

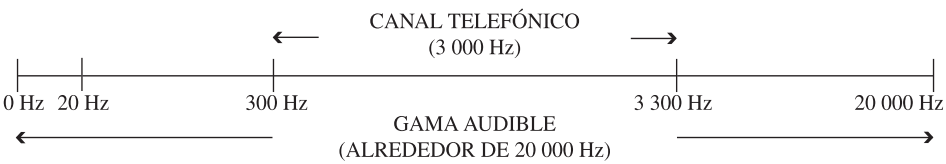


Figura 1.2 Disparidad entre el oído humano y un canal telefónico

BITS	b_7 ——————————→ b_6 ——————————→ b_5 ——————————→					0 0 0	0 0 1	0 1 0	0 1 1	1 0 0	1 0 1	1 1 0	1 1 1
BITS	b_4	b_3	b_2	b_1	Columna Fila	0	1	2	3	4	5	6	7
	0	0	0	0	0	NUL	DLE	SP	0	@	P	'	p
	0	0	0	1	1	SOH	DC1	!	1	A	Q	a	q
	0	0	1	0	2	STX	DC2	"	2	B	R	b	r
	0	0	1	1	3	ETX	DC3	#	3	C	S		s
	0	1	0	0	4	EOT	DC4	$	4	D	T	d	t
	0	1	0	1	5	ENQ	NAK	%	5	E	U	e	u
	0	1	1	0	6	ACK	SYN	&	6	F	V	f	v
	0	1	1	1	7	BEL	ETB	'	7	G	W	g	w
	1	0	0	0	8	BS	CAN	(	8	H	X	h	x
	1	0	0	1	9	HT	EM	)	9	I	Y	i	y
	1	0	1	0	10	LF	SUB	*	:	J	Z	j	z
	1	0	1	1	11	VT	ESC	+	;		[	k	{
	1	1	0	0	12	FF	FS	,	<	L	\	l	
	1	1	0	1	13	CR	GS	-	=	M	]	m	}
	1	1	1	0	14	SO	RS		>	N	^	n	~
	1	1	1	1	15	SI	US	/	?	O	—	o	DEL

Figura 1.1 Tabla de código ASCII

así como por tormentas eléctricas. Se caracteriza por su intensidad, corta duración y está confinado a una parte restringida del espectro de frecuencias. Dentro de la gama de audio es perceptible como chasquidos bruscos o ráfagas de estática (figura 1.4).

RUIDO BLANCO (RUIDO GAUSSIANO)

La energía del ruido blanco, por el contrario, está repartida en una amplia región del espectro de frecuencias y se escucha familiarmente como soplido de fondo en radio o telefonía. Se debe a la inducción de las líneas de fuerza, la intermodulación de circuitos adyacentes y un conglomerado de otras señales aleatorias. Una explicación del uso del adjetivo "blanco" para describir este tipo de ruido es que origina la "nieve" visible en la pantalla de TV cuando la señal es débil.

El ruido se hace molesto cuando su magnitud es más de la mitad de la que tiene un elemento positivo del código. A esto se debe que se tomen muestras de una señal y si el ruido supera el nivel de decisión se interpreta como una señal positiva. (figura 1.5). Se analizará con detalle estos aspectos oportunamente.

EFECTO DEL RUIDO SOBRE LA CAPACIDAD DE UN CANAL (SHANNON)

Puesto que las señales que son ruido poseen muchas de las características de una señal portadora de información, debemos buscar alguna forma de distinguirlas con claridad. Por fortuna, el nivel de potencia (intensidad) del ruido es bastante bajo en la mayoría de los circuitos. Si la potencia de la señal informativa está muy por encima de la potencia de ruido, el equipo receptor puede diferenciarlas con más facilidad. A medida que la señal y el ruido alcanzan un nivel de potencia similar, en tanto que el ancho de banda del canal permanece constante, cada una de las condiciones o estados discretos de la señal deben estar presentes durante periodos más prolongados, para que el equipo de recepción

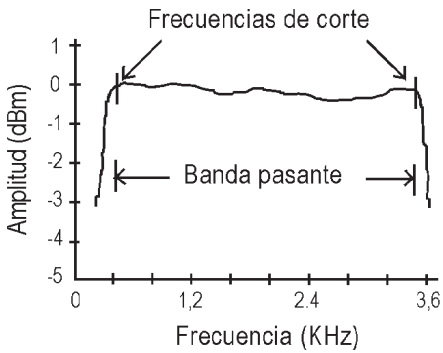


Figura 1.3 Banda pasante formada con filtros

pueda discriminar entre ellos y los estados aleatorios del ruido.

C. E. Shannon fue un precursor en este campo y en 1949 desarrolló una teoría según la cual el régimen máximo de bits, C, que se puede enviar por un canal con un ancho de banda BW y una relación señal/ruido S/N (donde S = intensidad de la señal y N = intensidad del ruido) está determinada por la fórmula siguiente:

$$C=BW\log_2(1+S/N)$$

Esta relación de potencia S/N indica la intensidad relativa de la señal con respecto a la del ruido en el canal, y es expresada en forma proporcional (10^3:1, o en decibeles (dB). Una relación de potencias S/N de $10^{2:}$ 1 sería igual a 20 dB, y así sucesivamente.

Si tuviésemos un canal perfecto, con un ancho de 3000 Hz y una relación S/N de 10^3 : 1 podríamos utilizar la fórmula antedicha y calcular el régimen máximo de bits del canal:

C=BWlog2(1+S/N)
=3000log2(1+103)
=3000log2(1001)
=3000x10(aprox.)
=30.000…bits/seg

Obsérvese que no se describen los métodos de codificación y modulación; son casi imposibles de lograr y, en verdad, no resultarían económicos.

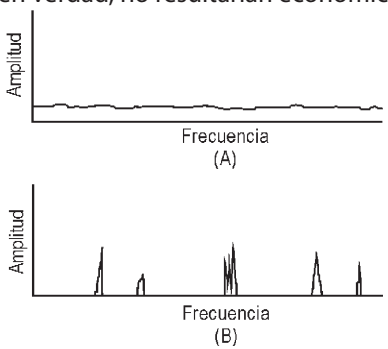


Figura 1.4 Distribución en amplitud y frecuencia (A) del ruido blanco y (B) del ruido parásito de corta duración.

ELEMENTOS DE CÓDIGO CON MÚLTIPLES NIVELES

En presencia de ruido, una señal binaria se percibe más exacta y fácil que otra en la cual se emplean varios bits por elemento de código. A medida que aumenta el contenido de bits (número de niveles) de un elemento de código, debe producirse un incremento

proporcional en la relación S/N para que los resultados de la detección de una señal binaria sigan siendo los mismos. La fórmula antes citada puede modificarse para obtener la relación S/N que se necesita como mínimo para un régimen de bits y un ancho de banda conocido.

$$S/N=2^{C/BW}$$

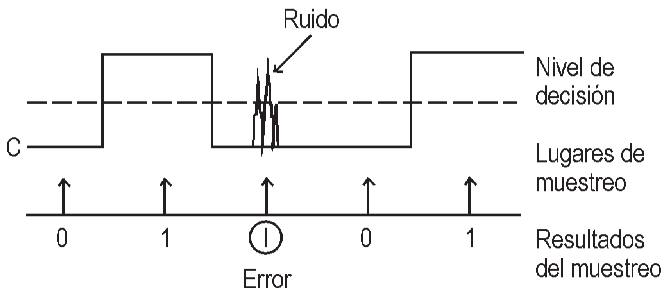


Figura 1.5 Efectos del ruido sobre una señal binaria.

La aplicación de esta fórmula a señales binarias y de niveles múltiples indicará la medida de la desventaja de ruido requerida para permitir la transmisión de varias señales de niveles múltiples.

Primero debe calcularse la relación S/N de una señal binaria, para que sirva de referencia. Suponiendo un canal perfecto de 3000 Hz, puede utilizarse la velocidad establecida por Nyquist, de 6000 bps, con lo que se obtiene una relación S/N de 3 : 1 como mínimo:

$$S/N=2^{C/BW}-1$$
$$S/N=2^{6000/3000}-1=22-1=3$$

El equivalente en decibeles de una relación S/N de 3:1 es:

$$dB=10\log S/N$$
$$=10\log 3=10(4,8)=4,8$$

En contraste con el sistema binario mencionado, en un sistema ternario (de tres niveles) se necesitaría una relación de potencia S/N superior. La velocidad máxima en bits de un sistema ternario a través de un canal ideal de 3000 Hz es:

$$bps = 2BW(\log_2 3)$$

$$= 6000(1,58) = 9500$$

y la relación S/N necesaria será:

$$S/N=2C/BW-1$$
$$=2^{9500/3000}-1$$
$$=2^3-1=7\ldots(\text{aprox.})$$

El equivalente en decibeles de una relación S/N de 7 es:

$$dB=10\log 7=8,5$$

La desventaja de ruido de un sistema ternario con respecto a uno binario (en un canal ideal) es, pues, 8,5-4,8 = 3.7 dB. Un sistema cuaternario requiere una diferencia mínima de 11,7 entre los niveles de la señal y de ruido. Por lo tanto, tiene una desventaja de ruido de 11,7 – 4,8 = 6,9 dB por encima del binario. Estos son los requisitos mínimos de un canal perfecto en cualquier otro sentido, y los ilustramos aquí para indicar el límite de la desventaja de ruido que se requiere para aumentar la velocidad de la señal en un canal determinado.

Además del límite que el ancho de banda y ruido de un canal (reducida relación señal-ruido) imponen sobre su capacidad portadora de bits, otras imperfecciones del canal y las limitaciones de los equipos actuales obligan a un mínimo práctico de la relación S/N del orden de 10^2: 1 (20 dB) o más.

REDES BLUETOOTH

Hoy día, un sinnúmero de personas utilizan cuantiosos dispositivos portátiles en sus actividades profesionales y privadas tales como ordenadores, teléfonos móviles, pda y reproductores mp3. Para la mayoría, estos dispositivos se usan por separado, esto es sus aplicaciones no interactúan. Sin embargo, en el caso que pudiesen interactuar directamente, los participantes de una reunión podrían compartir documentos o presentaciones; las tarjetas de visita irían automáticamente al registro de direcciones en un ordenador portátil y el número se registraría en un teléfono móvil. A medida que los viajeros salen de un tren cercano, sus ordenadores portátiles podrían permanecer en línea; de la misma manera, ahora el correo electrónico entrante podría ser derivado a sus pda; finalmente, al entrar a la oficina, toda la comunicación podría ser encaminada automáticamente a través de la red inalámbrica corporativa.

Estos ejemplos de comunicación inalámbrica espontánea, ad hoc entre dispositivos podrían ser definidos de manera informal como un esquema, al que a menudo se denomina formación de redes ad hoc, que permite a los dispositivos establecer la comunicación, en cualquier momento y en cualquier lugar, sin la ayuda de una infraestructura central. En realidad, la formación de redes ad hoc como tal no es nueva, sino la configuración, el uso y

los participantes. En el pasado, la noción de redes ad hoc se asociaba con frecuencia con la comunicación en los campos de combate y en los emplazamientos de zonas desastrosas; en la actualidad, al materializarse nuevas tecnologías tales como Bluetooth, es probable que cambie el escenario de la formación de redes ad hoc, así como su importancia.

A continuación se describe el concepto de la formación de redes ad hoc proporcionando sus antecedentes y presentando algunos de los retos técnicos que plantea. Además, se indican algunas de las aplicaciones que se pueden contemplar para la formación de redes ad hoc.

FORMACIÓN DE REDES BLUETOOTH

En todo el mundo, la industria ha mostrado mucho interés en técnicas que proporcionen conectividad inalámbrica de corto alcance. En este contexto, la tecnología Bluetooth se ve como el componente clave. Sin embargo, la tecnología Bluetooth debe ser capaz de operar en redes ad hoc que puedan ser autónomas, o parte del mundo "de la red ip", o una combinación de las dos cosas.

El principal propósito de Bluetooth es sustitur los cables entre dispositivos electrónicos, tales como los teléfonos, los pda, los ordenadores portátiles, las cámaras digitales, las impresoras, y las máquinas de fax, usando un chip de radio de bajo costo. La conectividad de corto alcance también encaja muy bien en el contexto del área amplia, en que puede extender la formación de redes ip al dominio de la red de área personal, como se discutió con anterioridad.

Bluetooth debe ser capaz de transportar ip eficientemente en una pan, ya que las pan estarán conectadas a Internet a través de umts o lan corporativas, y contendrán anfitriones con capacidad para ip. En términos generales, una buena capacidad para transportar ip daría a las redes Bluetooth una interfaz más amplia y más abierta, lo que con toda certeza impulsaría el desarrollo de nuevas aplicaciones para Bluetooth.

PRINCIPIOS BÁSICOS DE BLUETOOTH

Bluetooth es una tecnología de comunicación inalámbrica que usa un esquema de saltos de frecuencia una banda Industrial–Científica–Médica (Industrial–Scientific –Medical–ism) a 2,4 GHz que no necesita licencia. Dos o más unidades Bluetooth que comparten el mismo canal forman una pico red (figura 1.6). Dentro de una pico red, una unidad Bluetooth puede representar uno de dos papeles: maestro o esclavo. Cada pico red solamente puede contener un maestro (y siempre debe haber uno) y hasta siete esclavos. Cualquier unidad Bluetooth puede llegar a ser maestra en una pico red.

Además, dos o más pico redes pueden ser interconectadas, formando lo que se denominan una red dispersa (scatternet) (figura 1.7). El punto de conexión entre dos pico redes consta de una unidad Bluetooth que es miembro de ambas pico redes. Una unidad Bluetooth puede ser simultáneamente un miembro esclavo de múltiples pico redes, pero sólo maestro en una. Asimismo, debido a que una unidad Bluetooth únicamente puede transmitir y recibir datos en una pico red a la vez, su participación en múltiples pico redes

ha de ser en régimen de multiplexación por división de tiempo.

El sistema Bluetooth proporciona transmisión dúplex basada en duplicación por división de tiempo TDD (time-división duplex) con intervalos, donde la duración de cada intervalo es de 0.625 ms. No hay transmisión directa entre esclavos en una pico red Bluetooth, sólo de maestro a esclavo y viceversa.

La comunicación en una pico red está organizada de manera que el maestro interroga a cada esclavo de acuerdo con un esquema. Un esclavo sólo tiene permiso para transmitir después de haber sido interrogado por el maestro. El esclavo comenzará su transmisión en el intervalo de tiempo esclavo-a-maestro inmediatamente después de haber recibido un paquete del maestro. El maestro puede o no incluir datos en el paquete usado para interrogar a un esclavo. Sin embargo, es posible enviar paquetes que cubran múltiples intervalos. Estos paquetes multiintervalo pueden tener una longitud de bien tres o bien cuatro intervalos.

Aplicaciones

Las redes de paquetes de radio ad hoc han sido tomadas principalmente para usos militares, para una operación descentralizada.

En el sector comercial, los equipos para informática inalámbrica móvil representan un alto costo, y no es atractivo para el público. Pero conforme aumente la capacidad de los ordenadores móviles, también aumentará la formación de redes, y éstas se utilizarán en donde no haya ninguna infraestructura fija o celular.

Para operaciones de rescate en zonas remotas o para aumentar la cobertura local de modo rápido en sitios en construcción. A nivel local, las redes ad hoc pueden enlazar ordenadores portátiles para difundir y compartir información entre los participantes en una conferencia. También para redes domésticas, tal como audio, video, alarmas, actualizaciones de configuración y, en un fututo, redes más o menos autónomas de robots domésticos interconectados para limpieza, vigilancia, etcétera. Redes de salto múltiple (redes sensóras) para monitores del medio ambiente.

Ruido ambiental y laboral

El ruido es uno de los contaminantes más sutiles con que el ser humano inunda el mundo. No se ve, no tiene olor ni color, no deja rastro. Pero generar molestia, problemas de salud, y sobre todo sordera en las personas sometidas a ruido constante o excesivo. Es imperativo conocer los riesgos que el ruido puede producir para evitar consecuencias que pueden ser irreparables. La seguridad ocupacional pretende la inexistencia de riesgos para la vida y la salud del trabajador, y la legislación exige que se evite la generación de riesgos así como disminuir los ya existentes. Conservar la audibilidad es responsabilidad

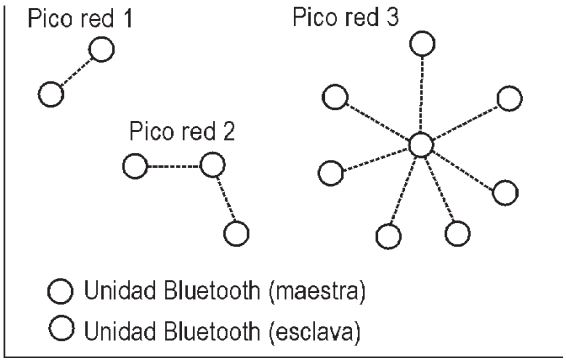


Figura 1.6 Ejemplos de pico redes Bluetooth

tanto de trabajadores como de empresarios, aunque toca a los últimos adoptar las medidas correspondientes.

Sortear el ruido industrial tiene como objetivo principal proteger a los trabajadores de las exposiciones excesivas de ruido, con lo que pueden presentarse pérdidas auditivas.

Esta es una prioridad que incluye la promulgación de leyes, indicando los límites de nivel máximo de ruido permisible en la maquinaria y equipos empleados en la industria, así como la formulación de recomendaciones para su ubicación, aislamiento, y la elaboración de rutinas adecuadas de trabajo.

La medición básica del nivel de ruido se realiza en dB (A), y son de gran importancia los valores de nivel instantáneo, nivel mínimo, nivel máximo, además de la dosis de ruido que incide en los oídos del personal en su horario completo de trabajo. El análisis de frecuencia y el de ubicación de las fuentes sonoras, son de gran utilidad para conocer mejor el ruido y buscar la forma más práctica y económica de atenuarlo.

El ruido industrial incluye todos los sonidos que se producen en una fábrica o instalación industrial, como son: motores, ventiladores, cajas de engranes, maniobras de carga y descarga, etcétera; asimismo el ruido generado en el proceso de producción. El nivel de ruido puede medirse en cualquier momento, pero hay que tomar en cuenta que con frecuencia hay variaciones de nivel de un momento a otro, por lo que la medición momentánea en dB (A) no es suficiente.

Se puede hacer gráficas continuas de la fluctuación del nivel de ruido, pero son difíciles de analizar e interpretar, por lo que se han desarrollado descripciones más sencillas, y la más empleada en ruido industrial es el l_{eq} o Nivel Sonoro Continuo Equivalente en dB (A), que es el promedio de energía del ruido en el tiempo que dura la medición.

El ruido puede ser continuo o estable, como en el caso de un motor eléctrico, o

de carácter fluctuante o intermitente, como en el caso de maquinaria de velocidad o proceso variables. Todos ellos pueden medirse en leq para determinar el posible riesgo de daño al oído.

La reglamentación a su vez establece mediciones por bandas de frecuencias con el objeto de caracterizar correctamente al ruido, en su caso, instalar el aislamiento adecuado o identificar con facilidad la fuente probable, para el caso de reducción de ruido. Las bandas empleadas con frecuencia son las de octava y 1/3 de octava.

Las mediciones de ruido estacionario se realizan con un medidor de nivel sonoro con ponderación A, y con respuesta lenta o rápida del indicador. El ruido debe medirse en la posición de la cabeza del trabajador. Esta es prácticamente una medición de ruido ambiental, en la máquina que opera el trabajador será sólo una de las fuentes de ruido, y no necesariamente la más importante, por lo que la respuesta del micrófono debe ser omnidireccional, de tal manera que se asegure la correcta medición del ruido generado por todas las fuentes involucradas.

Muchos trabajadores son expuestos a un cierto número de niveles de ruido con duración variable, lo que puede deberse al ciclo de trabajo de la maquinaria o del propio trabajador, desplazándose de un departamento a otro. Los códigos de ruido establecen procedimientos para sumar una serie de dosis parciales a las que son sometidos estos trabajadores. Por ejemplo, iso (Organización Internacional de Normalización) fija para ocho horas de trabajo y un nivel de ruido de 90 dB (A), la dosis de 100%, y para el mismo periodo de tiempo, pero con un nivel de 93 dB (A), la dosis es de 200%, por lo que si un trabajador permanece cuatro horas a un nivel de 90 dB (A) y las otras cuatro horas a un nivel de 93 dB (A), se dice que ha recibido una dosis de 150%. Es necesario tener presente que se fija el nivel de 105 dB (A) como el máximo nivel de ruido al que un trabajador puede ser sometido, y nunca más de 15 minutos al día. La osha establece una diferencia de 5 dB para duplicar el porcentaje de exposición, y actualmente usa 85 dB (A)/8 horas como base para el 100%.

Cuando el nivel de ruido fluctúa en forma impredecible, éste puede representarse por el nivel Sonoro Continuo Equivalente, el cual tiene la misma energía acústica que un ruido estable del mismo valor en un periodo de tiempo igual. Este principio de igual energía ha sido adoptado por iso, como por las normas mexicanas.

Los dosímetros de ruido de uso personal se usan para medir directamente en porcentaje la dosis recibida por un trabajador, sometido a niveles de ruido con fluctuaciones aleatorias en un periodo normal de ocho horas de trabajo. En caso de requerir la realización de mediciones en menos tiempo, por ejemplo, cuando se efectúan muestreos o en los sitios en que prácticamente el ruido no fluctúa, siempre es posible calcular el valor correspondiente a ocho horas, aunque para el cumplimiento de las normas nunca se aceptan mediciones de menos de dos horas, y en los casos críticos, es indispensable medir las ocho horas. Sólo para la determinación del Nivel Sonoro Continuo Equivalente, se han normalizado procedimientos que reduzcan el tiempo de medición por motivos de eficiencia, pero haciendo un muestreo por periodos cortos a lo largo de jornadas

enteras.

Para el caso de ruidos impulsivos no existe un criterio de índole mundial aceptado, en algunos países simplemente se suma 10 dB al nivel equivalente medido para compensar por la generación súbita de los ruidos impulsivos, ya que no permiten que actúen las defensas normales del aparato auditivo. En otros, se mide el nivel de los sonidos impulsivos y se marca un máximo de impulsos de dicho nivel por día. En cualquier caso se prohíbe que los ruidos impulsivos o de impacto superen el nivel de 140 dB "pico".

Debido a la falta de uniformidad en los criterios de evaluación de los ruidos impulsivos, los trabajadores sometidos a este tipo de ruido deben ser observados cuidadosamente desde el inicio de sus actividades, a través de programas de conservación auditiva, los cuales en algunos países son obligatorios en los sitios en donde existen niveles de ruido por encima de los 85 dB.

Con frecuencia, se requiere que los datos generados por las mediciones de ruido sean utilizados como referencia para futuras mediciones, o para determinar atenuaciones o incrementos después de cierto tiempo, o para cualquier otro tipo de comparación, incluyendo aspectos legales, de ahí que convenga realizar reportes suficientemente detallados. El control de ruido no necesariamente tiene que ser costoso, existen muchos ejemplos de bajo costo. Cuando el control de ruido no es práctico, la rotación de personal en zonas ruidosas contribuye a reducir el riesgo de pérdida auditiva, siempre y cuando el resto de la jornada suceda en ambientes de bajo ruido. En ocasiones, se requiere asilar la maquinaria ruidosa con barreras parciales o totales, las cuales se seleccionan de acuerdo al tipo de ruido. Los protectores auditivos reducen la cantidad de ruido que realmente entra al oído; esta solución deberá considerarse permanentemente en la fuente, o se aísla la maquinaria. En los casos en que lo anterior no es posible, es indispensable adiestrar adecuadamente al personal que tendrá que usar los protectores.

La planeación de la construcción futura de instalaciones industriales o su modernización, debe prestar especial atención a minimizar la generación de ruido. Resulta menos costoso diseñar y construir una fábrica silenciosa, que realizar acciones de control de ruido una vez que está en operación.

En el caso del ruido ambiental, el problema rara vez consiste en la pérdida de audición. Típicamente se trata de un asunto de confort, y para ello existen varias normas que establecen los niveles máximos de ruido que se pueden producir por vehículos, por fábricas y talleres en el lindero de sus predios, y, en general, por comercios y centros de diversión, incluyendo casa-habitación.

Por tal razón se marcan zonas en las ciudades de acuerdo al uso único o mayoritario que tengan éstas: habitacional, semiindustrial o industrial.

El control de ruido constituye en sí mismo un problema técnico de cierta complejidad, pero aunado a ello, existen otros que dificultan el control, tales como los de carácter económico, en algunos casos legislativos, falta de conocimiento o de interés por parte de las personas involucradas en la generación de ruido, ignorancia y/o negligencia por parte de los trabajadores sujetos a protección personal, falta de personal capacitado para realizar las instalaciones necesarias, etcétera.

UNIDAD II
MODELO DEL PROCESO DE COMUNICACIÓN

Un diagrama a bloques de un sistema general de comunicación se muestra en la figura 2.1 y su equivalente binario (on/off) es mostrado en la 2.2 se realizará un examen de las distintas partes del sistema, así como el proceso de codificación y decodificación.

FUENTE DE INFORMACIÓN

La fuente de información selecciona símbolos (letras, números, palabras, sonidos, etcétera) de un alfabeto (o conjunto) de símbolos posibles. El alfabeto del cual los símbolos son seleccionados es fijo e independiente de los procesos de comunicación. Las combinaciones de símbolos seleccionados sucesivamente (secuencialmente) forman los mensajes que serán transmitidos sobre un sistema de comunicación, la selectiva y estadística naturaleza de la fuente es una característica principal de la Teoría de Comunicaciones moderna.

FUENTE CODIFICADORA DE LA SEÑAL

La fuente codificadora de la señal transforma los símbolos seleccionados sucesivamente dentro de distintas señales físicas, estas señales deben tomar la forma de pulsos de voltaje como en sistemas telegráficos o voltaje continuo/funciones de tiempo como en sistemas de radio y teléfono. Es importante notar la distinción entre símbolos (que son seleccionados por algún alfabeto predeterminado) y las señales (como son representadas físicamente por los símbolos seleccionados).

Decodificador de señal a recipiente

Este decodificador opera inversamente a la fuente decodificadora de la señal. Convierte señales físicas dentro de símbolos adecuados para su uso por el recipiente. Es típico que las salidas de la señal a decodificar sean de teleimpresores, de radio y teléfono. Es importante notar que las señales que constituyen la entrada de la señal al decodificador de recipiente son dependientes de las decisiones previas hechas al medio para el decodificador de recipiente.

Codificador de señal a señal

El codificador de señal a señal, convierte la señal representando un símbolo dentro de otro de forma más compleja. El proceso de conversión involucra sumando redundancia a las señales y es esa parte del sistema la que emplea el codificador necesario cuando emplea códigos detectores de error o correctores de error.

Decodificador de señal a señal

El codificador de transmisión de señal a señal opera inverso al codificador de señal a señal (los compartimientos de transmisión son convenientes para la salida del codificador de señal a señal) y produce una señal que idealmente deberá corresponder directamente a la salida del codificador de la fuente a la señal.

CODIFICADOR DE TRANSMISIÓN AL MEDIO

El codificador de transmisión al medio (o modulador) opera en las señales codificadas que representan símbolos de información, convirtiéndolos en una forma apropiada para la transmisión, siempre que el médio esté conectado al transmisor y al receptor. Por lo general, hay restricciones en las señales enviadas al término de la transmisión al medio. Estas restricciones pueden tomar formas limitadas en la potencia, ancho de banda y duración de las señales eléctricas usadas, y el codificador de transmisión al medio debe ser diseñado para producir señales adecuadas.

DECODIFICADOR DEL MEDIO AL RECEPTOR

El decodificador del medio al receptor (o detector) opera inversamente al codificador de

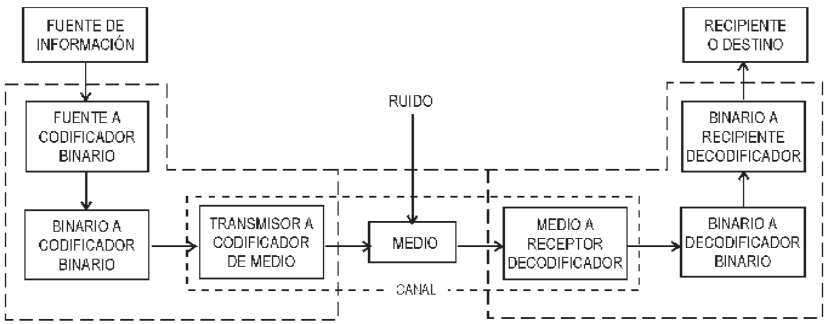


Figura 2.1 Diagrama de un sistema de comunicación

transmisión al medio. Éste convierte las señales moduladas que son recibidas en señales similares a las de la salida del codificador de señal a señal. El dispositivo a menudo actúa como una decisión primaria al hacer en un sistema binario, debe decidir en todo caso si el pulso recibido es binario 1 o 0. Las señales de salida provenientes del decodificador al medio y al receptor son usados en la parte decodificadora de éste último.

CANAL

El canal es el medio y la terminal fija del equipo que enlaza al transmisor y al receptor. El término "equipo terminal fijo" es necesario para la elaboración desde la aplicación de la Teoría de la Información que requiere una definición cuidadosa de cómo construir un canal. Las figuras 2.1 y 2.2 muestran el codificador de transmisión al medio y de éste al decodificador del receptor como parte del transmisor y del receptor. Sin embargo, si los procesos de modulación y demodulación son fijos en el sentido que el diseñador está sujeto a cualquiera de los dos, incapaz de tener cambios, entonces aquellos pueden formar parte de un canal. En general, en la aplicación del teorema de Shannon, el canal representa qué parte del sistema el diseñador no puede ni podrá cambiar, e incluye los procesos de decisión llevándolos a la salida del demodulador.

FUENTES DE INFORMACIÓN DISCRETA Y CODIFICACIÓN BINARIA DE SALIDAS

Las fuentes de información generan mensajes haciendo selecciones sucesivas de un alfabeto de símbolos posibles. Las fuentes pueden ser discretas o continuas.

Una fuente de información discreta es aquella que selecciona símbolos de una

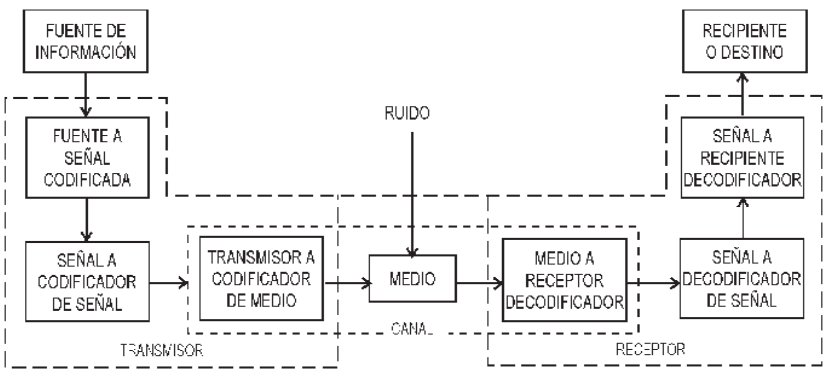


Figura 2.2 Diagrama de un sistema de comunicación binario

serie finita de x1, x2, ..., x3 de acuerdo a las reglas de probabilidad. La telegrafía es un ejemplo simple de una fuente discreta y de un sistema de transmisión.

Una fuente de información continua es aquella que hace selecciones de un alfabeto que es continuo dentro de su rango. Un ejemplo de la salida de una fuente continua es la posición tomada por el apuntador de un instrumento usado para medir la amplitud de algunas variables, que pueden tomar algún valor dentro de los límites de un cierto rango.

Esta unidad considera sólo aquellas fuentes conocidas matemáticamente como fuentes ergodic. Una fuente ergodic es aquella en la cual cada secuencia de símbolos producidos por la fuente es la misma en propiedades estadísticas.

Si ésta es observada lo suficiente, dicha fuente producirá, con una probabilidad aproximada a la unidad, una secuencia de símbolos que es típica. En términos simples significa que si una secuencia es lo suficientemente grande, contendrá casi con toda certeza números de símbolos y combinaciones de símbolos que son independientes de la secuencia particular.

Se dice que una fuente de información no tiene memoria o tiene memoria cero, si los símbolos sucesivos generados por la fuente son estadísticamente independientes. Esto es, una fuente tiene una memoria cero si cada símbolo es seleccionado sin la influencia de todas las selecciones previas. Si los símbolos previamente seleccionados influyen en la selección de un símbolo, entonces, se dice que la fuente posee memoria. Si la selección de símbolos está influenciada sólo por el símbolo que la precede inmediatamente, la fuente es conocida matemáticamente como una fuente Markov. Si la selección está influenciada por los m símbolos previamente seleccionados, la fuente posee memoria y a veces es llamada una fuente "Markov" de "m-ésimo orden'".

UNA MEDIDA DE INFORMACIÓN Y FUNCIÓN DE ENTROPÍA

Definición. Si un evento Xi ocurre con una probabilidad P(xi) entonces la cantidad de información asociada con la ocurrencia conocida del evento está definida por:

$$I(xi)=\log_x[p(xi)]^{-1}$$

Si, en la definición, los logaritmos son base 2, las unidades de información están en bits (una forma acortada de dígitos binarios). Si los logaritmos son tomados con base e, las unidades de información están en «nats» (una forma acortada de unidades naturales). Y si los logaritmos son tomados con base 10, las unidades de información están en «Hartleys» (después rvl Hartley).

1 hartley = 3.322 bits.

1 nat = 1.443 bits.

Una medida de información obtenida de una fuente de memoria cero: si una fuente

de memoria cero selecciona símbolos de un alfabeto x1, x2, ..., xn, y las probabilidades de seleccionar los símbolos son p(x1), p(x2), ..., p(x)n, respectivamente, entonces (de la definición de arriba) la información generada cada vez que se selecciona un símbolo xi es:

$$\log 2[p(xi)]^{-1} \text{ bits} \quad \ldots\ldots\ldots\ldots\ldots\ldots \quad 2.1$$

El símbolo Xi será seleccionado, en promedio, NP(xi) veces en un total de N selecciones, la cantidad promedio de información H´ obtenida de N selecciones es:

$$H' = NP(x_1)\log_2[p(x_1)]^{-1} + \ldots + NP(x_n)\log_2[p(x_n)]^{-1} \text{bits.}$$

Por lo tanto, la cantidad promedio de información por selección de símbolo es:

$$H' / N = H = p(x_1)\log_2[p(x_1)]^{-1} + \ldots + p(x_n)\log_2[p(x_n)]^{-1}$$

Esto es:

$$\text{bits / símbolo} \quad \ldots\ldots\ldots \quad 2.2$$

La cantidad H dada por 2.2 es llamada función de entropía. Este término es usado debido a que la forma de la ecuación 2.2 es la misma que se deriva de la mecánica estadística, para la cantidad de entropía termodinámica.

Nota: la información asociada con N selecciones de la serie estadísticamente independiente es, en promedio, igual a N veces la información por selección.

Una medida de información obtenida de una fuente con memoria, cuya memoria se extiende más allá de m símbolos, la dependencia sobre las selecciones previas puede ser expresada matemáticamente en términos de una probabilidad condicional.

Esto da la probabilidad de que la fuente seleccionará xi, dado que las m selecciones previas fueron $x_{11}, x_{12}, \ldots, x_{1m}$, donde x_{1m} es el símbolo seleccionado inmediatamente antes de la selección de xi, y x_n es el símbolo seleccionado m símbolos antes de la selección de Xi. Esta probabilidad condicional puede ser escrita:

$$p(xi/x_{il}, x_{i2}, \ldots x_{im})$$

Deberá ser entendido aquí que x_{li}, i=1,2, ..., m, puede ser cualquiera ser de los n símbolos fuente posibles; $x_1, x_2, \ldots, x_n$.

Una fuente cuya memoria se extiende más allá de m símbolos se dice que está en el estado $(x_{11}, x_{12}, \ldots, x_{1m})$ cuando los m símbolos previamente seleccionados fueron x_{11}, $x_{12}, \ldots, x_{1m.}$

Claramente, para una selección de un alfabeto de n símbolos posibles, y con una memoria extendida más allá de m símbolos, hay un máximo de n^m posibles estados, oscilando desde el estado $(x_1, x_1, \ldots, x_1)$ hasta el estado (x_n, x_n, x_n).

Se puede ver que la ecuación 2,1 para una fuente en el estado $(x_{11}, x_{12}, \ldots, x_{1m})$, la

información generada por la selección de un símbolo Xi es:

$$\log_2\{p[xi(x_{i1}, x_{i2}, \ldots, x_{im})]\}^{-1} \text{ bits.}$$

Y debido a que la fuente puede seleccionar cualquiera de los símbolos; x1, x2, ... , xn. la cantidad promedio de información generada por selección cuando la fuente esta en el estado ($x_{11}, x_{12}, ..., x_{1m}$) es:

bits.....2.3

La función $H[xl(x_{i1}, x_{i2}, \ldots, x_{im})]$ es llamada la "entropía condicional" y es una medida de la cantidad promedio de información generada por una fuente en el estado ($x_{11}, x_{12}, ..., x_{1m}$) cuando se selecciona un símbolo fuente.

Debido a que la fuente puede estar en cualquiera de los n^m estados posibles, esto sigue que, si la probabilidad está en el estado "i" es denotado por $p(x_{11}, x_{12}, ..., x_{1m})$, entonces las cantidades promedio de información generadas por la fuente en la selección de un símbolo es:

Por lo tanto, usando el teorema de Bayes, éste puede ser reescrito por:

La información generada por la fuente en la selección de N símbolos es H´= NH.

PROPIEDADES E INTERPRETACIÓN DE LA FUNCIÓN DE ENTROPÍA.

La función de entropía tiene un número de propiedades que son consideradas como una medida razonable de información. Algunas de estas propiedades son las siguientes:

A) es continuo en P(xi)

B) Si las probabilidades P(xi) son iguales [p(xi) = 1/n] entonces H= log n, y es por lo tanto, una función que se incrementa con el aumento de n. Esta es una propiedad razonable de una medida de información debido a que, entre más símbolos disponibles haya para la selección, hay una incertidumbre inicial más grande, y de aquí que haya un mayor cambio que va de un estado de incertidumbre a uno de certidumbre asociado con la selección de un símbolo particular.

C) H = 0 si y solo si todas las P(xi) son cero excepto una que es la unidad. Esta es, otra vez, una propiedad razonable de una medida de información, debido a que si el resultado de una selección es conocido antes, de que la selección sea hecha, entonces cuando se haga, no se aprenderá algo de eso.

D) Para una n dada, esto es, un número dado de símbolos fuente, H es un máximo e igual al log n cuando todas las P(Xi) sean iguales [p(xi) = 1/n]. Esta es también una propiedad razonable debido a que es la situación que intuitivamente tiene mayor elección o incertidumbre asociada con éste.

Si una fuente de información selecciona de un alfabeto sólo dos símbolos, entonces se dice que es una fuente binaria, si la probabilidad de la ocurrencia de los símbolos es P y q (=1 - P), respectivamente, la función de entropía para una fuente de memoria cero es:

$$H=-p\log_2 p-(1-p)\log_2(1-p)$$

Esta función es mostrada en la figura 2.3.

La salida de una fuente binaria está en dígitos binarios "binits". La distinción entre el binit que es una medida de información, y el bit que es un símbolo binario de salida, deberá ser cuidadosamente notificado. La figura 2.3 muestra que en promedio, las cantidades de información proporcionadas por una fuente binaria son siempre igual o menores que 1 bit/binit. La fuente binaria proporciona un bit de información para cada símbolo seleccionado sólo cuando los dos símbolos son equiprobables.

Sin considerar si una fuente posee memoria o no, la función de entropía puede ser interpretada como la cantidad promedio de información proporcionada por la fuente por símbolo seleccionado o alternativamente, como la cantidad promedio de información necesaria para especificar qué símbolo ha sido seleccionado. Si se permite que una fuente pueda seleccionar n símbolos donde n es un número largo, entonces seleccionará con alta probabilidad sólo $2^{n/f}$ secuencias de símbolos diferentes, cada uno y teniendo una probabilidad de ocurrencia igual a $1/ 2^{n/f}$. Esta es una interpretación física directa de H. Lo cual significa que, teóricamente, una muy larga secuencia de n símbolos seleccionados por la fuente pueden ser codificados y retransmitidos usando solo nH dígitos binarios, llevando cada dígito un bit de información.

CODIFICACIÓN BINARIA DE UNA FUENTE DE INFORMACIÓN

Cuando un símbolo es seleccionado por una fuente de información, se pone en acción una cantidad enorme de información igual a H. Ello implica la posibilidad que se use como un codificador fuente a binaria en cada modo para transmitir el símbolo seleccionado. Usando únicamente dígitos binarios H (H es el límite inferior). El límite inferior puede, en general, ser obtenido por la codificación en bloques más grande de una fuente de símbolos. Después, en la práctica algunos otros dígitos son más usados que los teóricamente

necesarios. En esta sección son discutidos dos métodos para la codificación de salida de una fuente, así como el uso y aplicación cuando usamos un número reducido de dígitos binarios. La importancia práctica de la codificación de este tipo es lo que limita, desde la redundancia general (innecesaria en los dígitos binarios).

La interferencia del ruido es corregida en los códigos de lectura, el error de detección y error de corrección, con el uso de redundancia. Sin embargo, existen circunstancias particulares cuando los errores ocasionales no son demasiados serios o cuabdo la interferencia del ruido no es muy considerable, ésta puede ser aprovechada en forma de dígitos binarios y es posible especificar y transmitir un símbolo seleccionado.

En el procedimiento de codificación Shannon-Fano, los símbolos son dispuestos en orden de probabilidad decreciente y luego divididos en dos grupos con probabilidad casi igual como sea posible. El dígito binario cero es asignado a cada símbolo en el grupo inferior. El proceso se repite dividiendo cada uno de los grupos en dos subgrupos de probabilidad casi igual. El cero binario es asignado a cada símbolo en el subgrupo superior de cada grupo y un uno binario para cada símbolo en el subgrupo inferior de cada grupo. El proceso se continúa hasta que cada subgrupo contenga solo un símbolo.

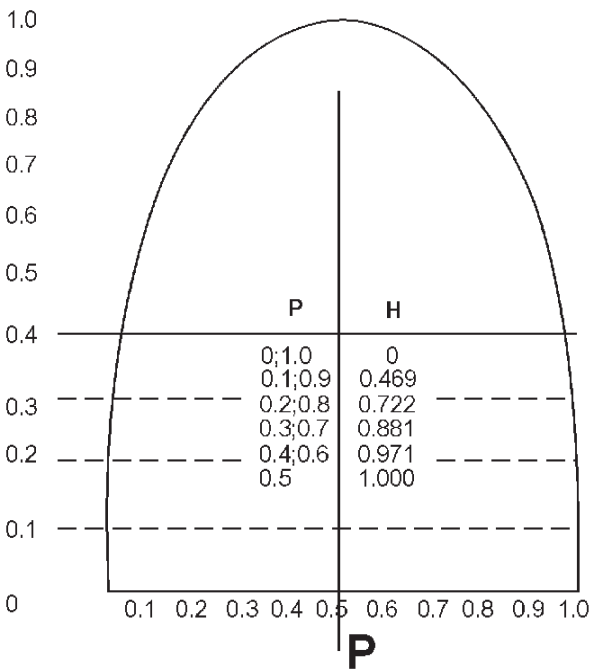


Figura 2.3 La función de entropía; $H=Plog_2(1-p)$

Este proceso de codificación (tabla 2.1) tiene importantes propiedades de comienzo económico en el uso de dígitos binarios, permitiendo la codificación sin ambigüedad en un símbolo-por-símbolo básico.

La tabla 2.2 es un método alternativo de construcción de código de palabras.

Código de Huffman. Aunque el método de codificación de Shannon-Fano es satisfactorio, no garantiza que el número promedio de dígitos binarios usados para representar un símbolo fuente será tan pequeño como el número promedio usado cuando es codificado por algún otro esquema. Un procedimiento de desarrollo codificado por Huffman (tabla 2.3) es como sigue:

Etapa 1. El símbolo es colocado en probabilidad de orden descendente (primera colocación).

Etapa 2. Los dos símbolos de menos probabilidad son combinados para formar un símbolo simple tal, que su probabilidad es la suma de dos símbolos constituyentes.

Etapa 3. Un nuevo conjunto de símbolos es formado después del conjunto original, con los símbolos combinados reemplazando estos dos símbolos constituyentes en la lista. El nuevo conjunto de símbolos es el promedio en orden descendente (segunda colocación).

Etapa 4. Se repite la etapa 2.

Etapa 5. Se repite la etapa 3.

Etapa 6. Las etapas 1 y 5 son repetidas hasta que un símbolo simple de unidad probable se obtiene.

Etapa 7. Cuando, alguna vez, dos símbolos son combinados para formar un nuevo símbolo, un cero binario es asignado a un símbolo bajo en la combinación. El código de palabra completo por una fuente de símbolo particular es la secuencia de dígitos binarios avanzando después del símbolo unidad-probable-final regresa a través de varios símbolos junto al símbolo fuente en cuestión.

Nota: El número promedio de dígitos binarios necesarios para representar un símbolo fuente, puede ser reducido hacia el límite de entropía, H, si una de las dos técnicas Shannon-Fanon o Huffman es usada para codificar bloques de símbolos fuente, más bien al contrario como fuente de símbolos individuales.

ENTROPÍA RELATIVA Y REDUNDANCIA

La razón de la entropía como una fuente al máximo valor de entropía, que se puede tomar por el mismo conjunto de símbolos de fuente, es llamada entropía relativa.

La Redundancia R es igual a 1 menos la entropía relativa

$$R = 1 - H/ Hmax$$

Cuando H es la entropía y Hmax el máximo valor de la entropía.

Símbolo fuente	Probabilidad P(Xi)	Palabras código representando cada símbolo					
X1	0.4	0					Palabra Código 1
X2	0.2	1	0				Palabra Código 2
X3	0.2	1	1	0			Palabra Código 3
X4	0.1	1	1	1	0		Palabra Código 4
X5	0.07	1	1	1	1	0	Palabra Código 5
X6	0.03	1	1	1	1	1	Palabra Código 6
Promedio de longitud código-palabra= (1x0.4)=(2x0.2)=(3x0.2)=(4x0.1)=(5x0.07)=(5x0.03)= 2.3 dígitos binarios / símbolo							

Tabla 2.1 Ejemplo de codificación Shannon-Fano

CANAL DE COMUNICACIÓN

Los canales de comunicación son clasificados por la naturaleza de las entradas y salidas, y la naturaleza de la probabilidad condicional relativas a sus entradas y salidas.

Si la entrada de un canal es discreta y la salida es discreta, se dice que el canal es discreto. Si las entradas y las salidas son ambas continuas, se dice que el canal es continuo. Si la entrada es discreta y la salida es continua se dice que el canal es discreto a continuo. El canal puede ser continuo a discreto si la entrada es continua y la salida discreta.

Si las probabilidades condicionales relativas a los símbolos de entrada y los símbolos de salida siguen alterando los símbolos que son transmitidos sucesivamente, se dice que el canal es constante o de menos memoria. Si esas probabilidades dependen en que ocurran los eventos de entrada y de salida, se dice que el canal posee memoria.

REPRESENTACIÓN DE UN CANAL

Después de que un símbolo o un mensaje ha sido seleccionado por una fuente de información, y la probabilidad codificada (por la técnica de Huffman, o como la técnica de co-

Símbolo fuente	Probabilidad P(Xi)	Palabras código representando cada símbolo				
X1	0.4	0	0			Palabra Código 1
X2	0.2	0	1			Palabra Código 2
X3	0.2	1	0			Palabra Código 3
X4	0.1	1	1	0		Palabra Código 4
X5	0.07	1	1	1	0	Palabra Código 5
X6	0.03	1	1	1	1	Palabra Código 6
Promedio de longitud código–palabra= (2x0.4)+(2x0.2)+(2x0.2)=(3x0.1)+(4x0.07)=(4x0.03)= 2.3 dígitos binarios / símbolo La entropía de esta fuente es cero–memoria H=0.4log0.4+0.2log0.2+0.2log0.2+0.1log0.1+0.07log0.07+0.03log0.03= 2.21 bits / símbolo						

Tabla 2.2 - Método alternativo de codificación Shannon - Fano

rrección-error), esto es, la alimentación del canal de comunicación. En el final del receptor de un mensaje se toma una decisión de un símbolo o mensaje que fue transmitido; lo cual constituye la salida del canal porque de varias formas de interferencia pueden ser tomadas decisiones incorrectas tiempo a tiempo y la salida de un canal puede diferir de su entrada.

La decisión hecha por el detector al tomar decisiones, hace que parte del canal pueda ser relacionado a a los símbolos de entrada por un arreglo de probabilidad condicional. Si el arreglo de símbolos de n entradas es denotado, como x1, x2, ..., xn, y el arreglo de k salidas como y1, y2, ...yn, entonces, el canal incluye la decisión al transmitir el proceso-creación en el receptor final, que puede ser representado por el diagrama presentado en la figura 2.4, o por un canal como se muestra debajo de ésta.

$$y_1 \ldots\ldots\ldots\ldots y_2 \ldots\ldots\ldots\ldots\ldots\ldots y_i \ldots\ldots\ldots\ldots\ldots\ldots y_k$$

$$P(y_1/x_1)\ \_P(y_2/x_1)\ldots\ldots\ldots P(y_i/x_1)\ldots\ldots\ldots\ldots P(y_k/x_1) \qquad x_1$$
$$P(y_1/x_2)\ \_P(y_2/x_2)\ldots\ldots\ldots P(y_i/x_2)\ldots\ldots\ldots\ldots P(y_k/x_2) \qquad x_2$$
$$.$$
$$.$$

Arreglo										
Símbolo fuente	1st		2na		3ra		4th		5th	
									0.60	1.0
X1	0.40	—	0.40	—	0.40	—	0.40	—	0.40	
X2	0.30	—	0.30	—	0.30	—	0.30			
X3	0.20	—	0.20	—	0.20	—	0.30			
			0.06	—	0.10					
X4	0.04	—	0.04							
X5	0.04									
X6	0.02									

Fuente símbolo:	Código palabra
X1	1
X2	00
X3	010
X4	0111
X5	01100
X6	01101

Promedio longitud de código palabra=2.06 dígitos binarios/símbolo
La entropía de la fuente=1.999 bits / símbolo

Tabla 2.3 - Ejemplo de codificación Huffman

.

$P(y_1/x_j)$ _ $P(y_2/x_j)$.....$P(y_i/x_j)$.....$P(y_k/x_j)$ x_1

.

.

$P(y_1/x_n)$ _ $P(y_2/x_n)$.....$P(y_i/x_n)$.....$P(y_k/x_n)$ x_n

Figura 2.4. Diagrama de un canal discreto

En el diagrama y la matriz, las representaciones del canal P(yi/xi) son llamadas probabilidades de adelanto, P(yi/xi) que se refieren a la probabilidad de una decisión, la cual puede ser tomada en los resultados de un símbolo de salida yi, cuando en realidad el símbolo transmitido fue xj. Claramente, desde que un símbolo de entrada particular en decisión puede ser alcanzada u observado en un símbolo de salida:

.....2.5

La probabilidad de obtener un símbolo yi, como salida de un canal es:

De la regla de Bayes mostramos la probabilidad de que un símbolo xj fue trans-

mitido, dado que la salida del canal es yi:

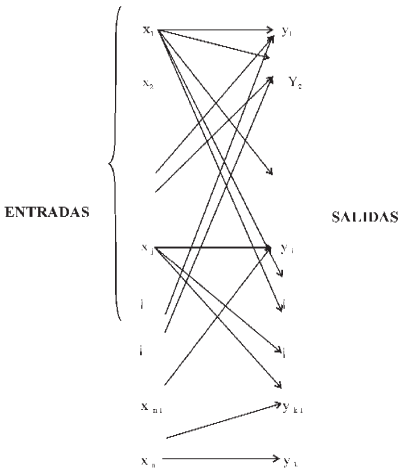
.....2.6

Y por lo tanto:

.....2.7

P(xj/yi) es llamada probabilidad para atrás o de reversa.

UNA MEDIDA DE LA INFORMACIÓN TRANSMITIDA SOBRE UN CANAL



Antes de la salida de un canal, la probabilidad de un símbolo es obtenida como xj, en el canal de entrada es P(xj), la entropía asociada con los símbolos de entrada es por lo tanto:

bits / símbolos 2.8

Esto es una propiedad de la entropía que puede ser interpretada como el promedio de bits de información portada por un símbolo de entrada o como el número promedio de bits necesarios para especificar un símbolo de entrada.

ENTRADAS

Después de recibir una salida yi, la probabilidad asociada con el símbolo de entrada es:

Y la entropía asociadas con el conjunto de entradas: x 1, x2…, xn es

bits

Tomando el promedio de todas las posibles salidas:

H(X/Y) es llamada entropía posterior o equivocada y puede ser interpretada como: el número promedio de bits de información de la portadora por un símbolo, después de que el símbolo ha sido recibido en el canal de salida, o como el número promedio de los bits necesarios para especificar un símbolo de entrada, después de que el símbolo ha sido recibido en la salida del canal. H(X/Y) es una medida de la incertidumbre asociada con la entrada después de que la salida ha sido recibida. Esta incertidumbre es causada por el ruido del canal.

La diferencia entre una priori y una entropía posterior es, I= H(X) - H(X/Y). Llamada algunas veces información mutua y con más frecuencia, el índice de información. La interpretación de H(X) y H(X/Y) es una medida de la cantidad de información ganada por el receptor como resultado de la observación de la salida en el canal.

bits / símbolo.....2.10

PROPIEDADES DE LA INFORMACIÓN MUTUA Y LA ENTROPÍA ASOCIADA

La información mutua I tiene un número importante de propiedades, y la entropía asociada para satisfacer un número importante de relaciones. Algunas propiedades relacionadas son:

A) El valor de I es equivalente a 1 o más grande que cero. Esto significa que el monto promedio de información recibida a través de un canal es negativo.

B) L a única condición bajo la cual I=0 es cuando el canal de entrada y el canal de salida son estáticamente independientes, por ejemplo, cuando:

Esta es una propiedad razonable, puesto que hay independencia estática entre el canal de entrada y el canal de salida, significa que nada se aprende del canal de entrada, sin conocimiento en el canal de salida.

C) Para un canal sin ruido, una vez que un símbolo de entrada se ha observado, y que no hay incertidumbre como en el símbolo de entrada que fue transmitido; se tiene por lo tanto H= (X/Y) = 0 y I = H(X), la entropía del canal de entrada. Las siguientes relaciones son mostradas para su veracidad:

A)

donde

B)

donde

C)

La igualdad en cada caso ocurre si y solo si «X» y «Y» son estáticamente independientes

CAPACIDAD DEL CANAL

La capacidad del canal está definida como el máximo valor al cual la información puede ser transmitida por un canal. Como puede verse de 2.8, 2.9 y 2.10; la información mutua o información valuada, depende no solamente en el arreglo de probabilidades condicionales relacionadas al canal de entrada y salida, sino también en las probabilidades con las cuales los diversos canales de símbolos de entrada son escogidos. Para un apropiado proceso de codificación, los símbolos de salida de la fuente pueden ser usados como formas en que los P(x)´s gobiernen el canal de símbolos de entrada, maximizando el valor de transmisión para un determinado arreglo de probabilidades condicionadas. El proceso de codificación es, algunas veces, referido como un arreglo estático de la fuente y el canal.

Aunque el cálculo de la capacidad del canal está, en general, un poco comprometido algebraicamente, presenta dificultades no fundamentales, y en ciertos casos el cálculo llega a ser relativamente simple.

ALGUNOS CANALES SIMPLES

Canal simétricamente binario. El canal mostrado en la figura 2.5 es conocido como canal simétricamente binario, los canales de entrada y salida son binarios y las probabilidades son simétricas.

bits / símbolos.....2.12

Canal de borrado. El canal mostrado en la figura 2.6 es conocido como canal de borrado. Puede ser interpretado como el modelo de un canal el cual toma la decisión al final del receptor del canal, e imprime un borrado, si la razón de una probabilidad posterior asociada con el canal de símbolos de entrada no es suficientemente grande.

La capacidad de canal es:

bits / símbolo

Para incrementar el valor de borrado, la probabilidad de una decisión incorrecta puede ser reducida a un valor despreciable (figura 2.7). Este canal es conocido como canal de borrado binario y tiene una capacidad de:

bits / símbolo 2.13

Canal de desvanecimiento de Rayleigh. Pierce ha considerado un canal en el cual la información es transmitida por llaves de cambio de frecuencia (fks) en la presencia de atenuación de Rayleigh y ruido Gausiano. En el sistema considerado por Pierce hay dos receptores, uno para cada símbolo transmitido y es usado sobre la detección. La señal transmitida para que sea asociada con el receptor, dando la salida más grande. La atenuación de baudios sucesiva es supuesta, para ser independiente estadísticamente, como es el ruido aditivo en los receptores. Se supone también que ocurren cambios de fase y amplitud durante cada baudio. Pierce ha mostrado que un sistema posee estas propiedades y satisface las suposiciones, y puede ser representado como un canal simétrico binario con cruce probable de:

Donde SO es el promedio de potencia del transmisor, T la duración de baudio y No el ruido portencia/hertz en cada receptor. El canal es mostrado en la figura 2.8 y la función:

Está dada en la figura 2.9, para varios valores de relación señal a ruido. La capacidad del canal, para varios valores de SO, T y No pueden ser derivados de la ecuación 2.12.

Canal binario con ruido gaussiano. Si la información es transmitida sobre un canal binario como una serie de pulsos positivos y negativos con la amplitud V/2 y el canal es perturbado por un ruido aditivo Gaussiano con promedio de N(=σ2) la probabilidad de potencia de paso es:

erf = función de error
erfc = función de error complementario

Para un punto transmitido en el rango de Nyquist y duración (1/2W) segundos, (V/2)2 es igual a P, la potencia promedio. La probabilidad de cruce puede ser escrita como:

Y la capacidad del canal como

Donde

Y W es el canal de banda base. En la figura 2.10, C/W es trazado como una función de P/N.

Nota: Si la información fue transmitida como una serie de pulsos ON/OFF, de amplitud V y cero respectivamente, la probabilidad de cruce podría tener una ganancia de:

En este caso la potencia promedio es V2/2, y por lo tanto, tres decibeles más son requeridos en el sistema ON/OFF para alcanzar la misma capacidad del canal.

Comportamiento de la capacidad del canal

Son varias las formas de perturbación que causan errores en la transmisión de información a través de un canal de comunicación. Los efectos de las perturbaciones incluyen fenómenos de; distorsión, así como de amplitud, distorsión o lineal, desvanecimiento debido a la transmisión de multicanales y ruido. El ruido puede ser impulsivo o Gaussiano, o podría tener características estadísticas completamente diferentes.

Existen técnicas, y se desarrollan otras, para la reducción de los efectos indeseables de varias perturbaciones. Estas técnicas incluyen: el uso de ecualización, de frecuencia y la diversidad del espacio, mejorar los métodos de modulación, el diseño de señales, y mejorar los procesos de decisión, estas modificaciones del canal llevan una reducción en las probabilidades de error y un acrecentamiento consecuente en la capacidad del canal.

TEOREMA FUNDAMENTAL DE LA TEORÍA DE LA INFORMACIÓN.

La información mutua, I= H (X) H(X/Y), es una medida de la suma promedio de la información transmitida a través de un canal. Sin embargo, esto no significa que la salida del canal es libre de error o que un receptor podría estar seguro de la entrada del canal conociendo la salida del mismo. Conociendo la salida del canal simplemente quiere decir que, la entrada del canal podría estar codificada usando H(X) - H(X/Y) menos dígitos binarios. La medida I, y particularmente su máximo valor C (capacidad del canal) ha sido definida, sin embargo, en términos de transmisión libre de error en un teorema atribuido a Shannon. El teorema, que es conocido como: el segundo teorema de Shannon, el teorema del canal de ruido codificado, o teorema fundamental que se puede enunciar como: "Si una fuente de información tiene una entropía H y un canal ruidoso de capacidad C, entonces teniendo H> C, la salida de la fuente se puede transmitir a través del canal y

recuperarse con una probabilidad pequeña de error".

Nota: En el teorema H y C se miden en bits/seg=(bits/símbolo) por (símbolo/seg).

Al alcanzar la transmisión libre de error, es necesario que los mensajes de la fuente sean codificados usando sucesiones largas de n símbolos del canal, el teorema de Shannon indica que: con un canal de capacidad C, es posible transmitir con una arbitrariamente pequeña probabilidad de error cualquiera de $M=2^{n(c-\lambda)}$ mensajes equiprobables de la fuente, usando una sucesión de n símbolos de canal. La probabilidad de error se puede hacer arbitrariamente pequeña, nula o tan pequeña como pequeño sea, haciendo n lo suficientemente grande.

La razón de que la probabilidad de error baje con n creciente es de importancia considerable, siendo más largo el retraso introducido por codificación y la más compleja de las operaciones de codificación y decodificación. Trabajo que muestra que por varios canales la probabilidad de error decrece exponencialmente (o casi exponencialmente) con incrementos de n, Fano, ha mostrado que la probabilidad de error de un canal con memoria finita tiene una forma general.

Donde k es una función variante de n y la transmisión proporcional R´, el coeficiente a, que es positivo para R´< C, es independiente de n pero e una función de R´ y las características del canal. También Shannon ha derivado en forma supero y bajos límites para la probabilidad de error en canales con ruido aditivo Gaussiano que son usados en la codificación y decodificación óptima.

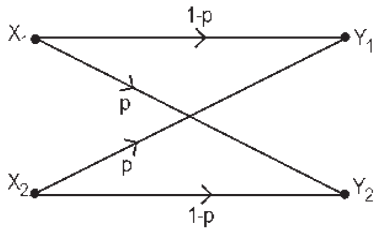


Figura 2.5 Canal simétrico binario

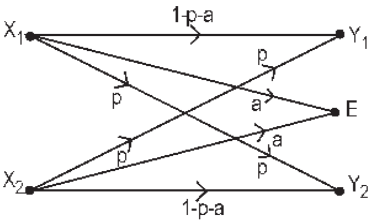


Figura 2.6 Canal de borrado

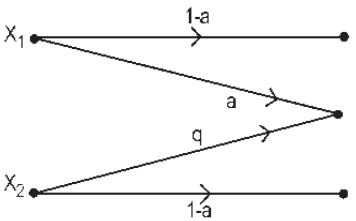


Figura 2.7 Canal de borrado binario

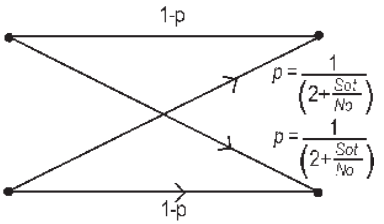


Figura 2.8 Canal con desvanecimiento de Rayleigh con ruido Gaussiano adicional

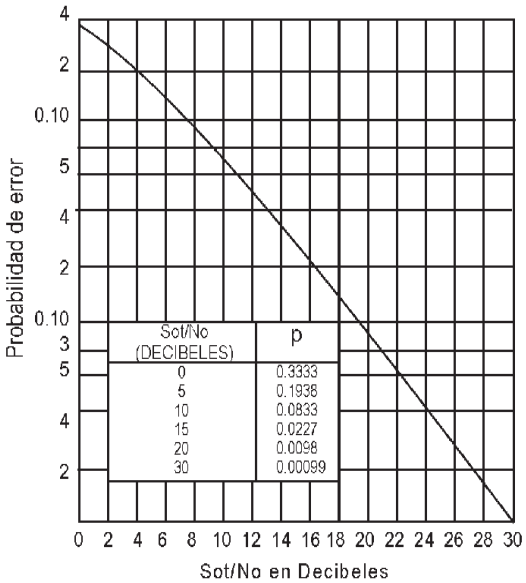
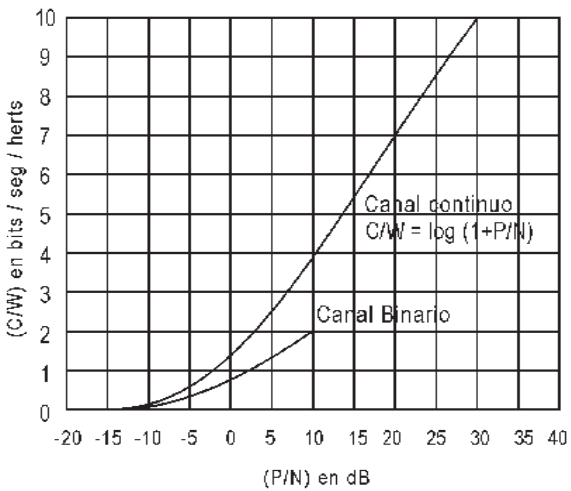


Figura 2.9 Canal con probabilidad de error por sobreposición en un desvanecimiento de Rayleigh



P/N dB	C/W Canal binario	C/W Canal continuo
-20	0.0092	0.01
-15	0.0288	0.04
-10	0.0897	0.13
-5	0.271	0.40
0	0.738	1.00
5	1.537	2.06
10	1.982	3.46
15	1.999	5.03
20	2.000	6.66
25	2.000	3.31
30	2.000	9.97
35	2.000	11.63

Figura 2.10 Capacidad del canal en bits/seg/Hz con ruido Gaussiano

UNIDAD III
SISTEMAS CONTINUOS DE INFORMACIÓN

Una fuente de información discreta genera información a una proporción finita,mientras que la función de entropía es una medida de información generada. En el caso de una fuente continua de información la situación es más complicada. Las complicaciones se incrementan porque una cantidad continuamente inconstante puede asumir cualquier número infinito de dígitos binarios para su especificación exacta. Una consecuencia inmediata de lo anterior, es que, para transmitir la salida de una fuente continua de información y recobrarla con exactitud, se requiere de un canal de capacidad infinita. En la práctica, un canal continuo es perturbado por ruido y por eso tiene una capacidad finita(como se mostrará más adelante), no es posible transmitir la salida de una fuente continua a través de un canal ruidoso y recobrarla exactamente.

Las dificultades fundamentales asociadas con fuentes continuas se pueden evitar desde la transmisión y recuperar fielmente la información (donde ésta representa la salida de la fuente exactamente como se desea). Shannon ha mostrado que si se especifica la salida de una fuente continua dentro de ciertos límites de tolerancia, es posible, en muchos casos, asignarle un valor definido, en razón de que la información es generada por la fuente. Se puede transmitir esta información por un canal y la probabilidad de error en la recuperación hacerlo pequeño, con tal de que la razón de generación sea menor que la capacidad del canal.

TEOREMA DEL MUESTREO

El teorema del muestreo es una ayuda importante en el estudio y análisis de sistemas de la comunicación, involucra el uso de funciones continuas en tiempo de ancho de banda limitada. El teorema declara que: si una función de tiempo f (t) no contiene frecuencias más altas que W hertz, está determinada completamente por los valores dados de la función a una serie de puntos espaciados 1/2 W segundos.

Si f (t) no contiene frecuencias más grandes que W hertz, entonces se puede expresar como:

Donde:

Es importante entender que el teorema no hace ninguna mención al origen del tiempo de las muestras. El origen del tiempo es insignificante; sólo el espacio entre líneas de las muestras es lo que interesa. Si la función f (t) es substancialmente cero al exterior del intervalo de tiempo T y no contiene frecuencias más altas que W hertz, puede ser especificado por 2TW ordenadas.

ENTROPÍA DE UNA DISTRIBUCIÓN CONTINUA

La entropía de una variable continua x con función de densidad de probabilidad p(x) se define como:

.....3.1

Con una función de densidad n-dimensional p (x1, x2,...., xn) la entropía se define como:

.....3.2

En el caso de dos variables "x" y "y", la juntura (unión) y (condicional) definen estas entropías como:

Como en el caso discreto:

Con igualdad si, y solo si, "x" y "y" son independientes.
Las dificultades se encuentran con respecto a:

Como el caso del límite de

Se discute en Goldman la función de entropía: en el caso continuo está dependiente en el sistema de la coordenada (ver Shannon), y cualquier cambio en las coordenadas dará lugar a un cambio en la función de entropía. La función de entropía es importante en el caso continuo como en el discreto; los conceptos de información mutua y capacidad del cauce depende de la diferencia de dos entropías, y la diferencia absoluta e independiente de los sistemas de la coordenada.

DISTRIBUCIÓN MÁXIMA DE ENTROPÍA

Si x es una variable continua con función de densidad de probabilidad p(x) y varianza σ, la forma de p(x) para máxima entropía es de forma Gaussiana, esto es, de forma:

Es un máximo si

La entropía de una distribución Gaussiana unidimensional con varianza $\sigma 2$ es:

.....3.3

ENTROPÍA DE UN CONJUNTO DE FUNCIONES

Del teorema del muestreo, es sabido que se puede representar totalmente una función continua de tiempo por muestras tomadas a intervalos separados de 1/2 W segundos. Si se saca una muestra a una forma de onda a n puntos, la distribución de la probabilidad por las amplitudes de muestras sucesivas es de la forma general p(x1, x2, …, xn) y la entropía del juego de funciones de tiempo posibles es dada por

Se define la entropía por muestra:

La entropía por segundo es:

y, desde n = 2WT, esto dice que H(X) = 2WH1(X)

Si el conjunto de posibles formas de onda tiene las características de ruido blanco Gaussiano de potencia promedio N (=s2), entonces las muestras son independientes, y

La entropía por segundo es:

POTENCIA DE ENTROPIA

Un concepto a destacar en sistemas de información continua es la potencia de entropía. La potencia de entropía de un conjunto fijo de señales dado, es definida al ser la potencia de ruido blanco limitado al mismo ancho de banda, como las señales originales y teniendo la misma entropía como señales.

Si un grupo de señales tiene una entropía H1, la potencia de ruido blanco tiene la misma entropía y se da por:

.....3.4

El potencial N1 es la potencia de entropía de las señales.

Se debe notar que el ruido blanco tiene la entropía máxima para una potencia dada, la potencia de entropía de cualquier ruido es menor o igual que su potencia real.

CAPACIDAD DE UN CANAL CONTINUO

Si la entrada a un canal continuo está en la forma de funciones de tiempo continuas, la salida será una versión perturbada de estas señales, y las señales de entrada y salida siendo limitadas a un ancho de banda W, se pueden representar durante un intervalo de tiempo T por n =2TW muestras. Las funciones de la densidad de probabilidad para la entrada, salida, y para la relación condicional entre entrada y salida, son:

y

respectivamente.

La razón de transmisión I de información a través de un canal continuo se define en cierto modo análogo por el caso discreto.

La capacidad del canal es definida como el máximo valor de I con respecto a todos los posibles conjuntos de señales de entrada.

.....3.5

Capacidad de un canal, en que el ruido es aditivo e independiente de la entrada.

La razón a que se trasmite, a través del canal de información es:

Donde la salida Y es relacionada a la entrada X por Y= X+n, n es el ruido, y dado que X y n son estadísticamente independientes, H (Y/X) pueden ser mostradas al ser igualadas a H (n), la entropía de ruido. La razón de transmisión de información por lo anterior es:

Y se encuentra la capacidad por llevar hasta el máximo H(Y) con respecto a la entrada:

.....3.6

Capacidad de un canal continuo perturbado por ruido blanco aditivo Gaussiano.

De la capacidad del canal dada por:

Si el ruido es ruido blanco Gaussiano, la entropía del mismo se da por:

bits / seg.

Donde W es el ancho de banda del canal, y N es la potencia promedio de ruido.

Si la potencia promedio transmitida se limita a P, la potencia promedio recibida es P+N, la distribución P(X) tiene entropía máxima para una potencia dada P+N ($=s^2$), es Gaussiana y tiene entropía:

bits / seg.

La capacidad del canal es por lo tanto:

Esto significa que, por usar señales codificadas suficientemente largas, tienen la propiedad de ruido blanco Gaussiano, esto se debe, posiblemente, al transmitir información a través del canal de una razón menor o igual a C, con la probabilidad arbitrariamente pequeña de error.

La función $C/ W= \log_2 (1+P/N)$ se traza para varios valores de P/N.

CAPACIDAD DE UN CANAL PERTURBADO POR UN TIPO DE RUIDO ARBITRARIO

Cuando se trata de perturbaciones arbitrarias de ruido, el problema asociado con la determinación de capacidad del canal no se puede resolver explícitamente. De cualquier modo, los límites superior e inferior se puede determinar por C en términos del ancho de banda del canal, la potencia promedio transmitida, la potencia media de ruido, y la potencia de entropía del ruido.

La capacidad C, en bits/segundo, se limita por las desigualdades:

Donde W= ancho de banda, P= potencia promedio transmitida, N= potencia media de ruido, y N1= potencia de entropía de ruido.

CÓDIGOS DE CORRECCIÓN DE ERROR

Como se mencionó anteriormente, el teorema fundamental de la Teoría de la Información supone que es posible transmitir cualquiera de $M = 2^{nR}$ de n dígitos binarios y que si R es menor que la capacidad del canal C, entonces la probabilidad de error puede ser disminuida arbitrariamente con la condición de que n sea suficientemente grande.

Lo cual significa que de los n dígitos binarios transmitidos, el equivalente de sólo nR son dígitos llevando un mensaje, el residuo de n(1-R) son redundantes en el sentido de que no llevan información en el mensaje. La razón nR/n es llamada razón de transmisión de información o simplemente razón y es medida en bits/digitos binarios.

En esta prueba del teorema fundamental, Shannon evita la parte difícil y hasta ahora, problema sin resolver, de especificar un código que satisfaga las condiciones del teorema. Él consideró la probabilidad de error promedio en todos los códigos elegidos al azar de longitud n y ha demostrado que este promedio tiende a cero cuando n tiende a infinito. Este es el problema de producir sistemáticamente un código que satisfaga las condiciones del teorema fundamental, antes de seleccionar uno al azar y esperando que éste sea uno bueno, que ha sido el tema de considerable atención desde la publicación inicial de la teoría de Shannon.

Básicamente, el concepto de codificación de información para transmisión consiste de dos operaciones. La primera es una operación de codificación en la cual nR dígitos de información son convertidos y representados por un gran bloque de n dígitos. Los n dígitos son transmitidos sobre el canal, y en el receptor la segunda operación (una operación de decodificación) es llevada a cabo.

En la decodificación los n dígitos recibidos son usados en el receptor y una decisión es hecha para nR dígitos de información originales que fueron transmitidos desde la fuente. Si el concepto de bloque codificado es considerado nuevo, un problema fundamental encontrado en intentos prácticos para transmitir de acuerdo con el teorema de

Shannon queda en claro.

Para realizar la operación de codificación, las facilidades deben de estar disponibles para que la secuencia de nR bits de información puedan ser convertidos a una secuencia de n binits, con una correspondencia de uno a uno entre las dos secuencias. Esto podría parecer a primera vista, que el codificador podría tener que almacenar cada uno de 2^{nR} secuencias posibles de n binits y seleccionar la secuencia apropiada en la recepción de n R dígitos de información en lo que se refiere a decodificación, y una cantidad similar de almacenamiento podría parecer necesaria.

Durante la transmisión, ocurren errores, así que recibir secuencias de n binits pueden ser cualquiera de un conjunto de 2^n, y el receptor tiene la tarea de comparar cada una de las 2^{nR} posibles secuencias transmitidas con la secuencia recibida antes de tomar una decisión acerca de cuál fue la secuencia transmitida más parecida. La posibilidad de tener un equipo de codificación y de decodificación en el cual aumente en complejidad exponencialmente con n, es extremadamente prohibitiva en la práctica y se han hecho intentos para facilitar el problema de almacenamiento.

Una aproximación adoptada es con una estructura algebraica, y la teoría de grupo en particular es empleada. Esto puede mostrar que la codificación puede ser realizada con equipo cuya complejidad aumenta solo linealmente con n y que el almacenamiento necesario en el decodificador son secuencias de $2^{n(1-R)}$ binits.

En una segunda aproximación, con probabilidad esencialmente, una técnica secuencial ha sido empleada en un intento de reducir el almacenamiento para la operación de decodificación. La codificación algebraica es considerada al detalle más adelante en esta sección y serán proporcionados ejemplos de unos códigos importantes, además, el problema de la síntesis sistemática de los códigos eficientes de corrección de múltiples errores son mencionados y una clase importante de estos códigos, considerados e ilustrados con ejemplos.

GRUPO DE CÓDIGOS, CÓDIGOS DE CHEQUEO DE PARIDAD

Como se ha dicho, la información puede ser transmitida usando bloques de n dígitos binarios. En cualquier sistema efectivo de codificación, no todas las posibles 2^n n–binit secuencias son usadas. El subconjunto de secuencias usadas en la codificación y cada miembro de los subconjuntos es llamado un código de Palabra (código Word)

Si la codificación y decodificación utilizan distintas secuencias n–bini, entonces como se menciono, el código se dice que es un código de bloques. En ciertos casos se emplean los términos alternativos como: códigos lineales, grupos de códigos y códigos de chequeo de paridad. El término código lineal se usa en un código, como el conjunto de secuencias desde el código Word que, generalmente, satisface las condiciones de asociación de álgebra lineal. Asimismo el grupo de códigos es utilizado desde el estudio de código de bloques, que puede ser desarrollado haciendo uso de la teoría de grupos. Y el término código de chequeo de paridad es usado desde el código Word, que por

lo general consiste en dígitos de información y de redundantes que se refieren a dígitos de chequeo de paridad.

CÓDIGOS SISTEMÁTICOS

El código Word es construido para que se sume a los dígitos de información, ellos contienen un número de dígitos "redundantes". Esos dígitos "redundantes" están e formados por combinaciones lineales de los dígitos de información y son llamados códigos de chequeo de paridad.

Si, dentro de un código, el primer dígito k en cada código Word es el dígito de información y los siguientes m (= n–k) dígitos son los dígitos de chequeo, entonces los códigos son llamados códigos sistemáticos.

CÓDIGOS DE DETECCIÓN DE ERROR

Los códigos de chequeo de paridad mencionados, forman la base de los códigos de detección y corrección de error. Un código de detección de error es aquel cuya estructura de código de Word es tal, que la presencia de un error o errores en la secuencia recibida pueden ser detectados pero no corregidos. en cambio un código de corrección de error es aquel cuya estructura de código Word es tal, que la presencia de un error o errores pueden ser detectados, localizadas la posición o posiciones y necesariamente corregidos.

Ejemplo: una muestra de una detección de error elemental es que un simple dígito de chequeo de paridad es usado para detectar la presencia de un número impar de errores en una secuencia. El dígito adicional es escogido para que el número total de 1´s en la palabra sea un número par. Esta manera de checar llamada un chequeo de igual paridad y se ilustra más adelante. Si los dígitos de información son 01011, y se usa en chequeo de igual paridad, la secuencia transmitida es 010111, y la presencia de 1, 3 o 5 errores pueden ser detectados pero no corregidos.

Módulo 2 aritmético

Él módulo 2 aritmético juega un papel importante en el estudio de códigos binarios. Las reglas de módulo 2 aritmético son las siguientes:

El signo ⊕, es a veces usado para denotar el módulo 2 adicional.

Patrones de Error

Si la secuencia transmitida es V y la secuencia recibida es U, la secuencia U–V es llamada patrón de error. Claramente, el patrón de error es el patrón que sumando al código Word transmitido, resulta en la secuencia recibida. Por ejemplo: si 011011 es transmitido y 101101 es recibido, entonces el patrón de error es 011011–101101, que es igual a 011011+101101 en módulo 2 aritmético. El patrón de error se ve como 110110.

Distancia de Hamming

La distancia de Hamming entre dos secuencias de n–dígitos binarios es el número de dígitos en que aquéllos difieren. Por ejemplo; si la secuencia es 1010110 y 1001010, la distancia de Hamming es 3.

Mínima distancia decodificada

En la mínima distancia decodificada, una secuencia recibida es comparada con todas las secuencias transmitidas, siendo la secuencia escogida del acortamiento de distancia desde la secuencia mínima recibida. Para los errores, esto es independiente del dígito binario a digito binario, la mínima distancia decodificada lleva al probablemente error más pequeño por encima de todo, y es equivalente de la máxima probabilidad decodificada.

Relación entre la distancia de Hamming y detección de error.

Si la distancia entre cualquiera de dos palabras de un código es igual a e +1, entonces es posible detectar la presencia de cualquier e, o algunos errores en una secuencia recibida.

Si la distancia de Hamming entre cualquiera de 2 palabras de un código es igual a 2e + 1, entonces es posible corregir cualquier e, o algunos errores ocurridos en una secuencia recibida.

ELEMENTOS DE CODIFICACIÓN DE COMPROBACIÓN DE PARIDAD

Un código de comprobación de paridad o código de grupo, puede ser definido únicamente en términos de una matriz de comprobación de paridad. Una secuencia v (= v_1, v_2, … v_n) es una palabra código si y solo si, ésta satisface la ecuación de matriz H v^T= 0, donde H es la matriz de comprobación de paridad, y v es la transformada de la matriz de la fila v = v_1, v_2 …v_n).

Si la matriz de comprobación de paridad es tomada para que sea de la forma general,

entonces el requisito de que una palabra código satisface la ecuación de matriz de arriba y la palabra satisface el siguiente grupo de m ecuaciones simultaneas

.....3.9

Si el grado de la fila de la matriz de comprobación de paridad es m, esto significa que m filas de la matriz son linealmente independientes y, por lo tanto, resolviendo las ecuaciones, que n-m de los elementos $v_1, v_2, \ldots v_n$ de la palabra código pueden ser elegidos arbitrariamente. Los restantes m dígitos son determinados en términos de estos dígitos elegidos, por la solución de los n-m dígitos escogidos arbitrariamente y son los dígitos de información y los restantes m dígitos determinados por la solución del grupo de ecuaciones simultáneas son los dígitos de comprobación de paridad.

La matriz de comprobación de paridad es usada en las dos operaciones, codificación y decodificación, y puede ser guardada, en alguna forma, en ambos, el codificados y decodificador.

La operación de decodificación puede ser ilustrada con un ejemplo en el cual la matriz de comprobación de paridad es tomada así:

Entonces esta matriz tiene un grado de fila 4, las palabras código vistas contienen 4 dígitos de comprobación de paridad y 2 dígitos de información. Los dígitos de comprobación de paridad C_1, C_2, C_3, C_4 pueden ser determinados de los dígitos de I1 e I2 usando la ecuación de la matriz de arriba. Si la palabra código v es arbitrariamente elegida tomada de la forma $C_1, C_2, C_3, C_4, I_1, I_2$, entonces los dígitos de comprobación de paridad deben satisfacer el grupo de ecuaciones simultáneas:

Las palabras código resultantes para este ejemplo son vistas para ser 000000, 0111111, 101110 y 110001.

En la decodificación, la matriz de comprobación de paridad es multiplicada por la transformada de la secuencia recibida $v' (= v'_1, v'_2, \ldots v'_n)$ y una secuencia de m dígito es llamada el corrector o síndrome obtenido. Siguiendo la determinación del síndrome, una corrección puede entonces ser hecha, asumiendo que un síndrome particular siempre ocurre por un resultado de la presencia de un error patrón particular.

El síndrome c es relacionado a la secuencia recibida y la matriz de comprobación de paridad por la ecuación de la matriz.

Claramente, si la secuencia recibida es la misma tal como una posible secuencia transmitida, entonces el síndrome es cero y la secuencia recibida puede ser asumida como correcta. Si de cualquier modo, los errores ocurren durante la transmisión y para convertir la secuencia transmitida dentro de una secuencia que corresponde a otra secuencia de

transmisión permisible, el síndrome no será cero. En este caso la secuencia recibida v' es igual a la suma de la secuencia transmitida v y el patrón de error x, y el síndrome es:

Puede verse que el síndrome es de hecho igual al módulo 2, la suma de las columnas de la matriz cuyas posiciones corresponden a las posiciones de unos en el modelo de error x. Dado que es posible que un número del modelo de error resulte en el mismo síndrome, es claro que cualquier decodificador práctico no puede corregir todos los modelos de error. El decodificador que examina todos los modelos de error resulta en un síndrome particular, y selecciona como error de transmisión ese modelo de error que contiene la menor cantidad de unos, es un decodificador de distancia mínima.

El siguiente ejemplo ilustra al decodificador de distancia mínima, basado sobre estas ideas. Asumamos que la matriz de chequeo de paridad es de la forma:

La tabla muestra las palabras clave, los modelos error, y las consecuencias recibidas, junto con los síndromes calculados usando la matriz H. Puede verse, en la tabla, que todos los errores simples y algunos errores dobles pueden corregirse, pero no pueden corregirse errores de modelo 3 o de más. Se notará que para efectuar la operación de decodificación de distancia mínima a un código de grupo, es necesario almacenar sólo la matriz de paridad, junto con el síndrome de 2^m y sus modelos de error asociados a éste.

De las ideas y ejemplos arriba presentados, se aclarará que un código debe ser tal que cualquier modelo de errores e, o menos, es corregible, luego cada modelo de error tal debe conducir a un nivel más alto de síndrome. Lo cual significa que ningún doble set de columnas e de la matriz de paridad tendrá el mismo módulo suma 2, o expresado alternativamente, que cada set de columnas 2e de la matriz de paridad será linealmente independiente si el código es capaz de corregir cualquier modelo de errores e o menores.

Para una longitud dada de palabra n, el problema de producir sistemáticamente la matriz de chequeo de paridad con cada set de columnas 2e linealmente independientes, es uno de los más difíciles de la teoría de codificación. Un método general de sintetizar tal matriz es el método de Sacks. Este método que puede usarse como prueba del límite Varsharmov-Gilber-Sacks, es muy laborioso e ineficiente, dado que los rangos (el rango de dígitos de información a lo largo de la palabra) no son tan altos como los obtenidos por otros métodos de síntesis. Un número muy importante de procesos de síntesis continúa y se ilustran con ejemplos.

El ligamento de Varsharmov-Gilbert-Sacks es menos seguro en el sentido de que el código de chequeo de paridad, capaz de corregir cualquier e o menos errores, y teniendo códigos de palabras de longitud n, siempre pueden ser construidos si el número de dígitos de chequeo es igual a o mayor que m, donde m es el entero menor que satisface la condición.

.....3.10

El ligamento de Varsharmov.Gilber-Sacks es una condición suficiente, pero no es

necesaria, desde que m = m´ es el entero menor para que la siguiente condición

sea satisfecha, luego es ciertamente posible construir un código (con palabras de longitud n) capaces de corregir cualquier patrón de e o menos errores. Sin embargo, también es posible, en muchos casos, construir un código capaz de corregir cualquier e errores con menos de m´ digitos de chequeo.

Tabla 3.1 Distancia mínima de decodificación

CÓDIGO DE CORRECION DE ERROR SIMPLE

Desde el procedimiento teórico se pudo observar que, si queremos corregir todos los errores simples que pueden ocurrir dentro de una secuencia de n dígitos, se necesita solamente ordenar la matriz de chequeo de paridad, donde sus n columnas no son cero y son distintas. De este modo, un código binario de corrección de error simple, con códigos de palabras de longitud n puede ser construido si éste contiene M dígitos de chequeo, donde M es el entero más pequeño que satisface la condición $2^m \geq N+1$. Si la matriz de chequeo de paridad está ordenada de tal forma que, el binario contenido en cada columna (cuando es convertido a su equivalente decimal) indica la posición de la columna dentro de la matriz y las posiciones de los dígitos de chequeo, dentro del código de palabra están ordenados para coincidir con esas columnas dentro dela matriz que contiene solamente un uno, el código es conocido como un código de error simple de Hamming. Este orden particular de la matriz de chequeo de paridad, mientras que no posea propiedades adicionales de corrección de error comparado con algún otro orden de la misma clase de columnas, tiene las siguientes ventajas:

A) Cada dígito de chequeo puede ser determinado directamente por los dígitos de información independiente de los otros dígitos de chequeo.

B) La posición de un error puede ser determinada, simplemente, convirtiendo el síndrome resultante a su equivalente decimal, este número es la localización del error.

Ejemplo: considere la construcción de un código de corrección de error simple de Hamming para palabras de longitud N=15, en este caso la condición $2^m \geq 15+1$ puede ser satisfecha y un código de corrección de error simple puede, por lo tanto ser construido con palabras que contegan 11 dígitos de información y 4 dígitos de chequeo. La matriz H de chequeo de paridad es:

y la estructura del código de palabras es: $C_1\ C_2\ I_1\ C_3\ I_2\ I_3\ I_4\ C_4\ I_5\ I_6\ I_7\ I_8\ I_9\ I_{10}\ I_{11}$.

Donde C_1 es i-esimo dígito de chequeo e I_j es el j-esimo dígito de información. Para este código los dígitos de chequeo pueden ser observados para ser determinados de:

Si se desea transmitir los dígitos de información 10101010101, después de los dígitos de chequeo (los cuales pueden ser determinados de las ecuaciones anteriores) se encuentra que son $C_1 = 1, C_2 = 0, C_3 = 1, C_4 = 0$ y el código de palabras transmitido cuyo resultado se observó que es: 1011010001010101.

Como una ilustración de decodificación se permite asumir que la secuencia recibida es 1001010010100101. para esta secuencia recibida el síndrome encontrado es:

0
0
1
1

La cual tiene un equivalente decimal de $1x2^0 \div 1x2^1 \div 0x2^2 \div 0x2^3 = 3$, indicando que el error está dentro del tercer dígito de la secuencia recibida. Si la secuencia recibida fue 1010100101001000 entonces el síndrome es:

1
1
1
1

El cual tiene un equivalente decimal de 15, indicando que el error está dentro del quinceavo dígito de la secuencia recibida.

CÓDIGOS DE CORRECCIÓN DE ERROR DE REED-MULLER

Los códigos de Reed-Muller son una clase de códigos de corrección de error múltiple, que tiene una gama de razones de información y habilidad de corrección de error. Estos códigos son semejantes, tal que para algunos enteros r y s, donde r es menor que s, hay un código con palabras de longitud $n = 2^s$ que contiene $m = 1 - {}^sC_1 - {}^sC_2 - \ldots - {}^sC_{s-r-1}$ dígitos de chequeo capaces de corregir algún patrón de $2^{s-r-1} - 1$ o menos errores.

Proceso de codificación. En la operación de codificación, la secuencia transmitida $f(=f_0, f_1, \ldots, f_{n-1})$ es obtenida de los dígitos de información n-m por medio del uso de una expresión de grado r-esimo de la siguiente forma general:

En esta expresión, los coeficientes $g_0, g_1, \ldots, g_{1,2,3}, \ldots$, etcétera, son dígitos de información, y las secuencias $x_1, x_2, \ldots x_s$ son vectores base de longitud n teniendo la forma de:

Ejemplos que ilustran el proceso de codificación:

Caso 1: Considere el caso donde s=4 y r=1. Bajo estas circunstancias la expresión general de codificación será:

$$F = g_0 \bullet x_0 \div g_1 \bullet x_1 \div g_2 \bullet x_2 \div g_4 \bullet x_4$$

Y los códigos de palabras son generados por medio del uso de g_i´s como dígitos de información. Las palabras de este código son de longitud $n = 2^s = 2^4 = 15$, y el código es capaz de corregir algún patrón de $2^{s-r-1} - 1 = 3$ o menos errores.

Como forma de ilustración, se desean transmitir los dígitos de información 10100. para este ejemplo, la secuencia transmitida $f(= f_0, f_1 \ldots, f_{15})$ se observo que:

Caso 2: Como una segunda ilustración, considere el caso cuando s = 4 y r = 2. Bajo estas circunstancias será:

Patrones de error		Código de palabras		Síndrome Transpuesto para cada secuencia recibida	
	000000	011111	101110	110001	
000000	000000	011111	101110	110001	0000*
100000	100000	111111	001110	010001	1000*
010000	010000	001111	111110	100001	0100*
001000	001000	010111	100110	111001	0010*
000100	000100	011011	101010	110101	0001
000010	000010	011101	101100	110011	1011*
000001	000001	011110	101111	110000	1100*
110000	110000	101111	011110	000001	1100*
101000	101000	110111	000110	011001	1010*
100100	100100	111011	001010	010101	1001*
100010	100010	111101	001100	010011	0011*
100001	100001	111110	001111	010000	0100*
011000	011000	000111	110110	101001	0110*
010100	010100	001011	111010	100101	0101*
010010	010010	001101	111100	100011	1111*
010001	010001	001110	111111	100000	1000*
001100	001100	010011	100010	111101	0110*
001010	001010	010101	100100	111011	1001*
001001	001001	010110	100111	111000	1110*
000110	000110	011001	101000	110111	1010*
000101	000101	011010	101011	110100	1101*
000011	000011	011100	101101	110010	0111*

Este código, que tiene palabras de longitud $2^s=2^4=16$, contiene $1+{}^4C_1=5$ dígitos de chequeo y 11 dígitos de información y es capaz de corregir cualquier error que ocurre en una secuencia recibida.

De la expresión anterior de codificación, la secuencia transmitida correspondiente a la secuencia de información 01000100001 es:

y como:

y

la secuencia transmitida se observó que es

0100010001001011

Proceso de decodificación. Un algoritmo general de decodificación para estos códigos ha sido elaborado por Reed. El algoritmo permite cualquier patrón de 2^{s-r-1} - 1 o menos errores para corregirse.

En operación de decodificación, cada digito de información es calculado un número de veces en términos de ciertas subclases seleccionadas de los elementos $f_0, f_1, \ldots f_{n-1}$ de la secuencia recibida, y una decisión de mayoría es hecha para saber si el dígito de información en cuestión es 1 o 0. En la decodificación, los coeficientes de r-esimo grado (g_{12}, g_{13}, …, g_{34} en el caso 2) son primero obtenidos, y después una nueva secuencia recibida es calculada adicionando nuevamente los términos de r-esimo orden encontrado ($g_{12} \cdot x_1 \cdot x_2$, …, $g_{34} \cdot x_3 \cdot x_4$ en el caso 2) a la secuencia original, esta nueva secuencia recibida es después usada, y los coeficientes de (r – 1)-esimo grado extraídos en la misma forma que los coeficientes de r-esimo grado. El proceso es repetido hasta que el mensaje es extraído u ocurra una indeterminación.

Un esquema general para determinar cuál subclase de los elementos $f_0, f_1, \ldots, f_{n-1}$ debe ser usado en el chequeo de los dígitos de información $g_i, \ldots, g_{ij}, \ldots g_{ijk}$, etétera, es el siguiente:

Ordenar los vectores base de acuerdo a como se muestra en la figura 3.1 y para cada vector x asociar el j-esimo 0 con el j-esimo 1 como está indicado. Cada par de elementos asociados está condicionado a su par en juego.

La subclase 2^{s-1} de dos elementos usados para determinar g_1 son 2^{s-1} pares en juego en el vector base x_i. Cada una de las subclases 2^{s-2} de cuatro elementos usados para determinar g_{ij} es obtenido un par, en juego de componentes en x_i junto con los pares asociados en xj. De la misma manera, cada una de las dos 2^{s-3} subclases de 8 elementos usados para determinar gijk es obtenido tomando un par en juego x asociado con este

un par en juego xj y 4 componentes en juego en xk. El esquema puede ser extendido en una forma sencilla para obtener las relaciones de chequeo para coeficientes de orden más alto.

Ejemplo que ilustra el proceso de decodificación. Este permite considerar el caso donde s=4 y r=2, como se hizo anteriormente y se asume que se deseo transmitir la secuencia de información 10000000001. la secuencia transmitida para ésta, en particular es 0111111111110000.

Usando el esquema descrito anteriormente y como se observó en la figura 3.1 las relaciones de chequeo son:

Y sustituyendo los valores del elemento recibido dentro de las relaciones de chequeo para los coeficientes g_i, los siguientes valores son obtenidos:

$g_{12} = 1; g_{12} = 0; g_{12} = 0; g_{12} = 0 \quad \therefore g_{12} = 0$ decisión de mayoría.
$g_{13} = 1; g_{13} = 0; g_{13} = 0; g_{13} = 0 \therefore g_{13} = 0$ decisión de mayoría.
$g_{14} = 1; g_{14} = 0; g_{14} = 0; g_{14} = 0 \therefore g_{14} = 0$ decisión de mayoría.
$g_{23} = 1; g_{23} = 0; g_{23} = 0; g_{23} = 0 \therefore g_{23} = 0$ decisión de mayoría.
$g_{24} = 1; g_{24} = 0; g_{24} = 0; g_{24} = 0 \therefore g_{24} = 0$ decisión de mayoría.
$g_{34} = 0; g_{34} = 1; g_{34} = 1; g_{34} = 1 \therefore g_{34} = 1$ decisión de mayoría.

En estas seis etapas los dígitos de información han sido decodificados.
La nueva secuencia recibida, $f' = g_0 \bullet x_0 + g_1 \bullet x_1 + g_2 \bullet x_2 + g_3 \bullet x_3 + g_4 \bullet x_4$
Puede ser calculada ahora sumando la secuencia
para f

La secuencia f´ se encontró que es 0111111111111111, y usando estos nuevos elementos en las relaciones de chequeo para g_1, g_2, g_3 y g_4 los siguientes valores son obtenidos para los dígitos de información g_1, g_2, g_3 y g_4.

$g_1 = 1; g_1 = 0; g_1 = 0; g_1 = 0; g_1 = 0; g_1 = 0; g_1 = 0; g_1 = 0$
$g_2 = 1; g_2 = 0; g_1 = 0; g_1 = 0; g_1 = 0; g_1 = 0; g_1 = 0; g_1 = 0$
$g_3 = 1; g_3 = 0; g_3 = 0; g_3 = 0; g_3 = 0; g_3 = 0; g_3 = 0; g_3 = 0$
$g_4 = 1; g_4 = 0; g_4 = 0; g_4 = 0; g_4 = 0; g_4 = 0; g_4 = 0; g_4 = 0$

Por decisiones de mayoría de g_1, g_2, g_3 y g_4, son tomados como 0, 0, 0, 0, respectivamente.

Sumando $g_1 \bullet x_1 + g_2 \bullet x_2 + g_3 \bullet x_3 + g_4 \bullet x_4$ a la secuencia f´, la secuencia correspondiente a $g_0 \Sigma x_0$ es obtenida. Esta secuencia se encontró que es 0111111111111111 y como x_0 es 1111111111111111111, g_0 puede ser igual a 1 por decisión de mayoría. La secuencia de información decodificada es 100000000001, lo cual es correcto.

CÓDIGOS DE PRODUCTO O ITERADOS.

Es posible usar códigos sistemáticos simples para producir códigos más poderosos con habilidad de corrección de error aumentada. Estos códigos son llamados iterados o códigos de producto.

Como un ejemplo de código de producto o iterados, considere el código formado por un código sistemático simple, en el cual un dígito de chequeo simple es sumado luego de ser formado como un medio de detección, un número impar de errores en un código de palabras. Los dígitos de información están ordenados en dos dimensiones (o dimensiones más altas) ordenadas como se muestra en la figura 3.2, y un digito de chequeo de paridad par es sumado a cada región y a cada columna. En la suma los chequeos son también llevados sobre los dígitos de chequeo.

El código específico se expone en la figura 3.2, que es claramente más poderoso que los códigos originales delos cuales fueron construidos.

La posición de un error está localizada como el elemento del renglón y la columna, los cuales checan si falta paridad. Los códigos de producto pueden ser resumidos de forma que los renglones del orden pueden ser tomados de un tipo de código sistemático, mientras que las columnas son tomadas de un tipo diferente de un código sistemático.

CÓDIGOS BOSE-CHAUDHURI

En años recientes, algunos de los avances más importantes en el desarrollo de los códigos de corrección de error múltiple han sido de mucho interés junto con una gran clase de códigos conocidos como códigos cíclicos. Estos códigos son de extrema y práctica importancia debido a la facilidad con la que pueden ser sintetizados, así como codificados y decodificados utilizando un registro de desplazamiento de retroalimentación.

Para poder entender en forma clara los códigos cíclicos, es necesario tener conocimientos de álgebra abstracta, lo cual está fuera del alcance de esta unidad. Por ello se propone considerar, sólo en forma breve las clases más importantes de códigos de Bose-Chaudhuri. Las propiedades de los códigos Bose-Chaudhuri, así como un método de construcción de matriz de chequeo de paridad (parity check matriz) para la corrección de errores múltiples son aplicados a lo largo de éste, por otra parte también se discutirán métodos prácticos para la codificación y de codificación de los mismos.

Los códigos de Bose-Chaudhuri son una clase de códigos cíclicos particularmente efectivos en la detección y corrección de errores múltiples que ocurren en el número entero positivo, hay un código con n= 2-1 de largo, este código contiene más de m dígitos de chequeo de paridad y es capaz de corregir algún patrón de error e o menor.

La matriz de chequeo de paridad, H, para un código Bose-Chaudhuri que tiene palabras de n =2exp.m -1 de largo y capaz de corregir algún patrón de error e o menor puede ser derivado como se muestra a continuación:

A) Tome una matriz de m x m, z de la forma

Y seleccione los dígitos binarios μ0, μ1, μ2, …, μ(m-1) de manera que el polinomio

no se reduzca y no se divida entre X-1 para cualquier K menor a 2-1

B) Tome algún vector sin ningún cero X de m elementos.

C) Forme la matriz de chequeo de paridad, H, como sigue:

En esta matriz Zexp.i es la matriz Z multiplicada por sí mismo i veces, y Zexp. ix es la matriz obtenida al multiplicar la matriz Zexp.i por la matriz X.

La matriz [illegible] puede contener

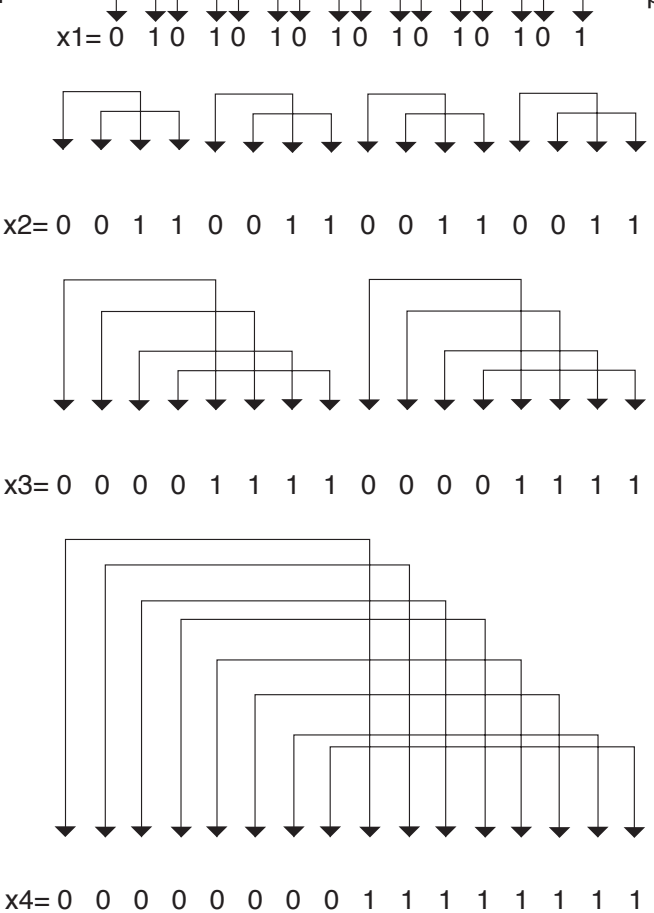


Fig3.1- Esquema del símbolo de paridad para uso en decodificación del código Reed – Muller.

también un número de filas repetidas. Obviamente, las filas de este tipo no tienen valor durante el chequeo de paridad, por lo que deben ser anulados de la matriz H.

Una vez eliminadas estas filas independientes, H es igual al rango de filas de la matriz y, como se explico anteriormente, esto es igual al número de dígitos de chequeo.

El rango de la matriz H se puede determinar de manera directa como sigue:

Si f(x), para i= 1, 3, 2e-1, es un polinomio con ceros y unos como coeficientes, y es tal que el mínimo grado del polinomio para el cual la ecuación de la matriz fi(x= Zexp.i)= 0 se satisface; entonces el polinomio f(x), es el mínimo común múltiplo de las fi(x)´s, es decir, es el polinomio de grado más bajo, que es un múltiplo de cada fi(x) y se conoce como "polinomio generador" del código Bose-Chaudhuri. El grado del polinomio generador es igual al rango de la matriz H.

Ejemplo: considere la síntesis del código Bose-Chaudhuri para la corrección de un triple error para el cual m=4 y e=3. Este código tiene palabras de n=(2exp.4–1)= 15 de largo. Asumiremos que:

y que la matriz Z es

Para esta elección de Z, el polinomio característico

Queda de la siguiente manera

El cual no se puede reducir y no se divide entre x- I para alguna k menor a 15.

A) Ejemplo General de un Código Iterado

B) Especificaciones de un ejemplo de código iterado

Figura 3.2 Ejemplos de códigos iterados

Por medio de una multiplicación de matrices se observa que:

Y por lo tanto

Continuando con multiplicación de matrices.

La matriz H de chequeo de paridad es:

Esta matriz tiene una fila de puros ceros y 2 filas idénticas. Si la fila de ceros se elimina junto con una de las dos filas idénticas, la matriz resultante se obtiene como la matriz de paridad de chequeo para el código.

Esta matriz tiene 10 filas independientes y es, por lo tanto, de rango 10, también podemos observar que cada 6 columnas, la matriz es linealmente independiente, el código puede corregir todos los patrones de errores de 3 o menores.

El rango de la matriz anterior se ha obtenido directamente del hecho de que los poli-

nomios mínimos f(x), f3(x), y f5(x) son $1+x+x^4$, $1+x+x^2+x^3+x^4$, y $1+x+x$ respectivamente.

Por lo tanto:

Tiene grado igual a 10 y el rango de H es por lo tanto 10.

El polinomio g(x) es el polinomio generador para un código Bose-Chaudhuri, con información 5 y 10 dígitos de chequeo.

La codificación y decodificación del código de Bose-Chaudhuri, puede ser fácilmente mecanizado utilizando registros de desplazamiento de retroceso.

Los procedimientos de decodificación y codificación se entienden de mejor forma en términos de polinomios de código. Cualquier palabra de código puede ser expresada como polinomio y los coeficientes del mismo son los elementos de la palabra de código.

Por ejemplo: si una palabra de código es 1011001, esta puede ser representada por un polinomio como sigue:

Los códigos cíclicos tienen la propiedad importante de que cualquier palabra de código es un múltiplo de polinomio generador. Por lo tanto, cualquier polinomio de palabra de código T (x) se relaciona con el polinomio generador por la expresión:

$$T(x) = P(x).\ g(x)$$

Donde P(x) es un polinomio multiplicador. Si las palabras de código son de duración n y el número de dígitos de chequeo es m=n-k, entonces el polinomio T(x) es de grado igual o menor a n-I y como g(x) es grado m. La operación de codificación puede ser considerada como una simple multiplicación del polinomio generador con polinomio P(x), el cual es de grado k-I o menor y tiene como coeficientes dígitos de información k.

Un esquema de un registro de desplazamiento de retroceso para la multiplicación de un polinomio compuesto:

Un polinomio: se muestra en la figura 3.3

El sistema contiene n-k estados de registro de desplazamiento, el contenido inicial de estos es puesto a cero. La operación de multiplicación se puede llevar a cabo con este circuito alimentando una secuencia de dígitos n dentro del registro y observando la salida en la posición indicada en la figura 3.3, la secuencia de entrada consiste de k dígitos de información, los cuales se introducen primero en el registro de alto orden, y de n/k ceros, que son introducidos en el registro después de los dígitos de información.

Después de la transmisión en un canal, el mensaje codificado posiblemente puede contener algún error. Si el patrón de error es representado por el polinomio E(x), en la misma forma que las palabras de código, entonces la secuencia recibida es:

Y dado que E(x), no es un múltiplo de g(x), la presencia de algún error en R(x) puede ser detectado simplemente dividiendo R (x) por g(x).

En la ausencia de errores, g(x) dividirá a R(x) en forma exacta (no habrá residuo), pero si ha ocurrido algún error de g(x) no dividirá a R(x) en forma exacta, y por lo tanto, existirá un residuo. La presencia o ausencia de residuo se puede usar para determinar si ha ocurrido algún error. Se debe observar que si E(x)=q(x). g(x) entonces dividirá a R(x) en forma exacta y el error no podrá ser detectado.

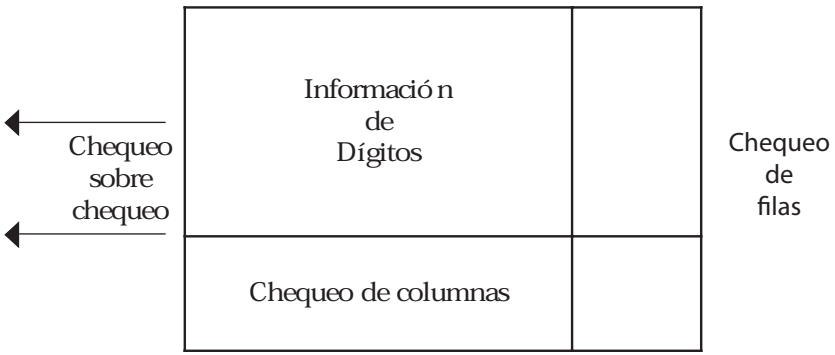
Esto no debe preocupar puesto que:

Corresponde a una secuencia de palabras de códigos permisible, y el decodificador debe asumirlo como tal. El circuito de la figura 3.4 sirve para dividir un polinomio:

Por un polinomio

En la división los contenidos de registro inicialmente se ponen en cero y los dígitos r(n-1), …, r1 son desplazados dentro del registro en el orden en que son recibidos. Después de un total de n–1 desplazamientos, el contenido de los registros es igual al residuo después de dividir R(x) por g(x).

Además de las aproximaciones algebraicas para la codificación, y aspectos importantes que se mencionaron anteriormente, la aproximación probabilística también ha sido investigada y tiene la promesa de ser un método económico para la transmisión de la información con una pequeña probabilidad de error, en rangos cercanos a la capacidad del canal.



Información de dígitos

	1	0	1	1	0	1	0
Filas de Chequeo	0	1	1	1	0	1	0
	1	0	1	0	0	1	1
	1	0	0	0	1	1	1
Chequeo de Chequeo	0	0	1	1	0	1	1
	1	0	1	1	1	0	0
	0	1	1	0	0	1	1

Columnas de Chequeo

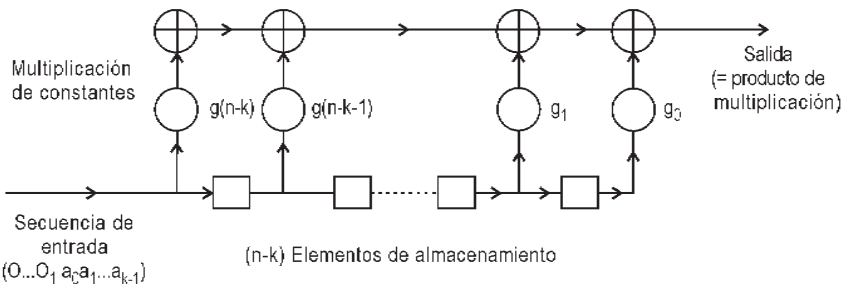


Figura 3.3 Circuito para multiplicar el polinomio $g(X)=g_0+g_1 \cdot x+\ldots g_{n-k} \cdot x^{n-k}$ por el polinomio $P(x)=a0+a \cdot x+\ldots+a^{k-1} \cdot x^{k-1}$

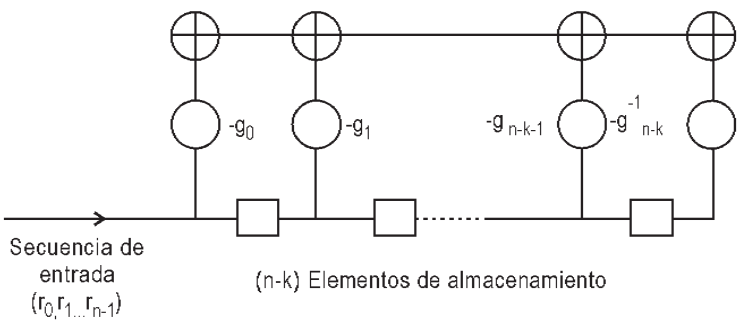


Figura 3.4 Circuito para dividir el polinomio $R(X)=g_0+g_1 \Diamond x+\ldots+h^{n-1} \Diamond x^{n-1}$
Entre el polinomio $g(x)=g_0+g_1 \Diamond x+\ldots+g^{n-k} \Diamond x^{n-k}$

UNIDAD IV
TRANSMISIÓN DE DATOS DIGITALES

Cuando la información es transmitida digitalmente, el ancho de banda es especificado en bits por segundo (o capacidad de transmisión), y existe una relación directa con el ancho de banda análogo; enseguida se analizará la respuesta en frecuencia de los pulsos digitales.

Se tiene, idealmente que, el filo de un pulso es perfectamente perpendicular con altura infinita y el tope (duración del pulso) de transmisión con un ancho de banda infinito para transmitir información digital en forma.

Por supuesto, esto no es necesario, debido a que los pulsos no necesitan ser perfectamente rectangulares cuando llegan al receptor. La cuestión es que los pulsos sean detectados como unos y ceros.

En la figura 4.1 se observa un tren de pulsos representando información digital, y el espectro de frecuencia de un tren de pulsos periódicos se muestra como un tren de componentes de frecuencia, y proporciona una idea de por qué se requiere el ancho de banda en Hertz para transmisión.

El espacio entre los componentes de frecuencia es siempre igual para la frecuencia fundamental del tren de pulsos y la amplitud es siempre cero en la frecuencia, donde tp es la duración del pulso.

RAZÓN DE ERROR DE BIT (BER)

Mediante el envío de un patrón de bits conocido y contando el número de bits recibidos incorrectamente en el receptor, se puede medir la calidad de la conexión, el parámetro de calidad de la red digital es la razón de error de bit (BER, BIT ERROR RATIO) expresado como el promedio de bits recibidos incorrectamente al número total de bits transmitidos.

En una transmisión de voz sobre una conexión digital de 64Kb/s, la razón de error es de 10^{-6} o menos en un tiempo arbitrario, y no hay degradación de la calidad. Si es 10^{-5} la calidad para voz es legible y si es 10^{-4} se tiene disturbio considerable, y con una razón de error de 10^{-3} la degradación de la calidad es severa.

Para otros servicio, una razón de error de bit aceptable son, para datos de 10^{-7} -10^{-8}, telex 10-4, fax 10^{-5}-10^{-6}, videophone 10^{-6} -10^{-7} y correo electrónico 10^{-5}-10^{-6}.

En la práctica, los errores de bit ocurren normalmente en "bursts".

El itu-t, recomendación G-821 define los siguientes parámetros para conexión de

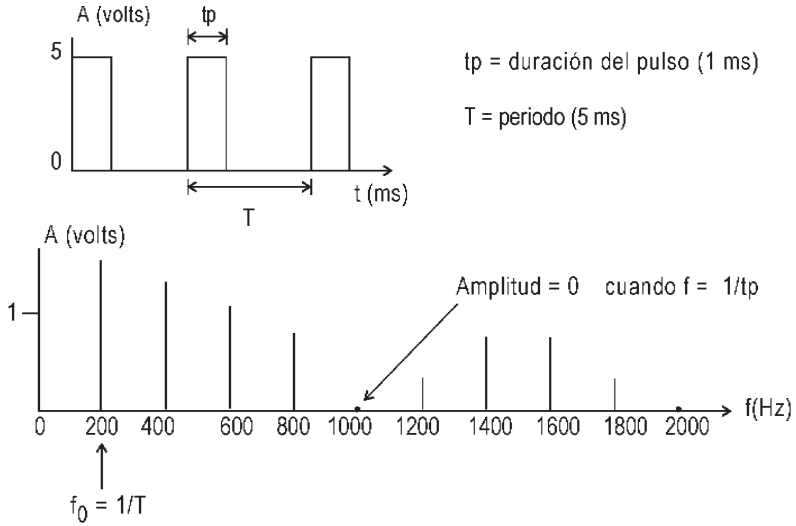


Figura 4.1 un tren de pulsos y su espectro de frecuencia

64 Kb/s entre 2 suscriptores.

- Degradación por minuto (dm) menos de 10%, en un intervalo de un minuto se tiene un ber de $1X10^{-6}$ o peor.
- Errores por segundo (es) menos de un 8% de un número, en un intervalo de un segundo se tienen bits alterados.
- Errores por segundo severos (ses), menos de 0.2% de un número, en un intervalo de un segundo. Tienen un ber de $1X10^{-3}$ o peor.

DISTORSIÓN DE CUANTIZACIÓN

Antes de que la red de telecomunicaciones se digitalice completamente, ésta tiene en sus principios, una mezcla de equipo análogo a digital; cada transición de equipo analógico a digital involucra una cuantización, ésta proporciona una cierta distorsión de la curva de la voz, por tener un cierto número limitado de intervalos de cuantificación usados para describir la información. La unidad utilizada para medir la distorsión de cuantización es el qd (quantizing distortion) en una conexión.

Un qd es igual a la distorsión producida por una conversión A/D.

El itu-t recomienda un máximo de 14 qd en tráfico internacional, y el objetivo es que no se exceda de 5qd en redes parciales, y cuando las redes sean completamente digitalizadas 7qd será el valor permisible en interfaces internacionales.

RUIDO

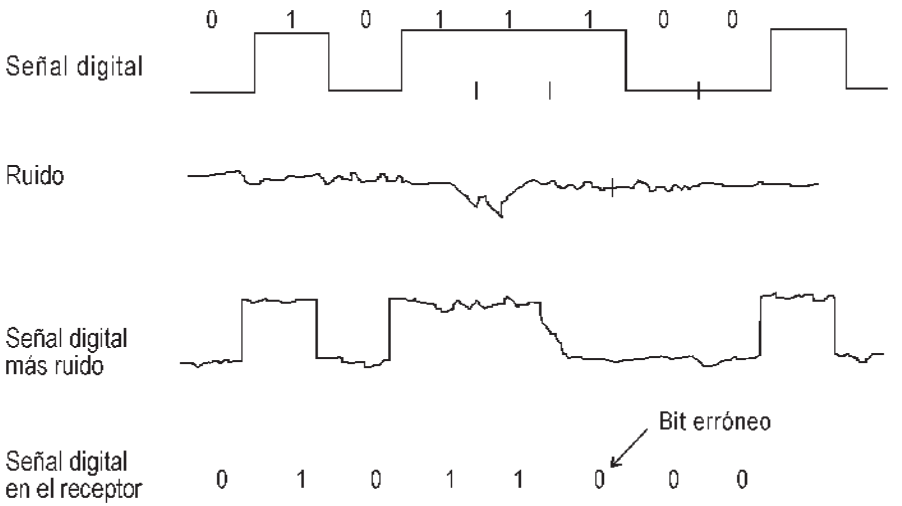


Figura 4.1 Transmisión de datos digitales más ruido

El ruido es la causa predominante de errores en los bits en conexiones digitales. A los datos digitales transmitidos se les agrega el ruido, y el resultado es una señal mal interpretada en el receptor.

Por medio del espectro de frecuencias se distingue dos tipos de ruido: ruido blanco y ruido 1/f.

El ruido blanco se caracteriza porque la potencia es constante para todas las frecuencias, al contrario del ruido 1/f donde la potencia es más grande a bajas frecuencias y decrece al aumentar la frecuencia.

Se tiene además, el ruido térmico que ocurre porque las cargas eléctricas están en constante movimiento, y éste es más fuerte cuando se incrementa la temperatura, y en el cero absoluto no habría este movimiento. Este ruido causa variaciones aleatorias en el voltaje, por ejemplo, de un resistor, además de que se tiene un incremento del ancho de banda.

El ruido de disparo ocurre en semiconductores y es causado por los portadores de cargas individuales (huecos o electrones) que provocan la corriente eléctrica, para semiconductores (diodos, transistores), se realiza la suposición de que se tienen corrientes constantes.

En un transistor bipolar, la corriente es distribuida en la base de modo aleatorio, y la misma distribución también ocurre en el electrodo compuerta de un fet, este tipo de ruido es llamado ruido de partición.

Eco

El eco en sistemas digitales en forma semejante a la transmisión analógica, degrada la

información cuando se tienen retardos de tiempo grandes.

JITTER

Los sistemas de transmisión pueden causar constantemente cambios de fase llamados Jitter, éste es especificado por la desviación de fase en el tiempo (grados o intervalos de unidad, ui) y como frecuencia, o como el número de cambios de fase por segundo. Es medido por medio de una señal de prueba enviada a través de la conexión para investigar los cambios de fase en el receptor. Las conexiones de datos que utilizan psk son sensitivas al Jitter, y éste ocurre en sistemas análogos y digitales; también sucede cuando se tiene la transmisión desde una alta razón de bits multiplexados a una razón de bit más baja (figura 4.2).

SCRAMBLING

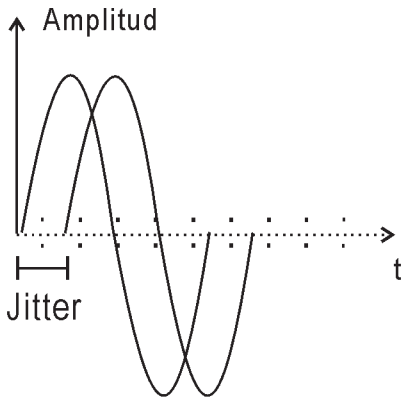


Figura 4.2 Generacion de Jitter.

Cambiar la señal bit a bit de acuerdo a una secuencia repetitiva separada. En la figura 4.3 produce Scrambling, se muestran los pasos en la secuencia de cómo manejar los bits en la señal antes de ser codificados, en cada paso, un cero cualquiera significa "guardar el valor", o un uno significa "invertir el valor".

El código Inversión de Dígitos Alternados (adi), es una forma de Scrambling, la secuencia repetitiva separada es: (0,1), que significa "invertir cada segundo bit".

Las secuencias de diferentes algoritmos de Scrambling, son diferentes en longitud (la longitud normal son cientos de pasos).

Para el diseño, el Scrambler consiste de un registro de corrimiento retroalimentado y es descrito por medio de un polinomio, por ejemplo, el Scrambler para una señal sdh de 155 Mbits/s, utiliza un polinomio de x^7+x^6+1.

El receptor hace uso de la misma secuencia de Scrambling, para decodificar la señal empleada por el transmisor, teniendo ambas sincronizadas para obtener una de-

codificación.

Se evita con el Scrambling grandes series de unos y ceros, y garantiza lo mismo

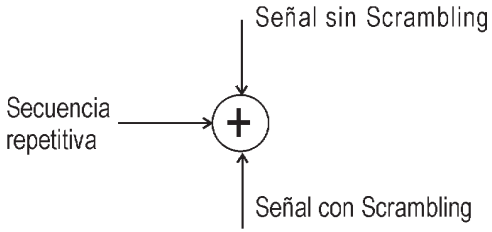


Figura 4.3 Scramling

que el código hdb_3 y no se afecta el ancho de banda, también la razón de bit es la misma antes y después del Scrambling.

TRANSMISIÓN DIGITAL DE INFORMACIÓN

La modulación hace posible la transmisión de información en forma binaria (1,0) sobre portadoras analógicas, en este proceso un bit o grupo de bits pueden ser trasladados en rápidos cambios de estado, tal como la amplitud o corrimiento de fase, estos métodos

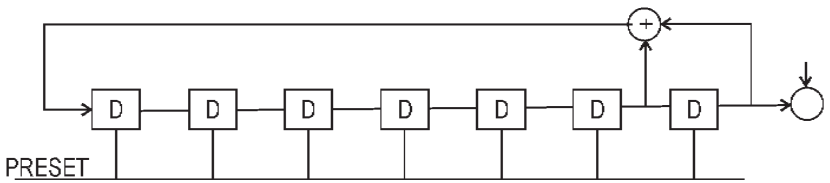


Figura 4.4 Scrambling de acuerdo al polinomio X^7+X^6+1

básicos de modulación son:

ask- Amplitude-Shift

esk- Frecuency- Shift Keying

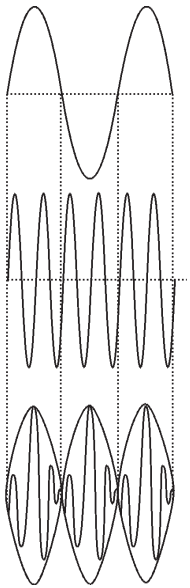
psk- Phase shift Keying

En el caso de transmitir información analógica, los cambios se efectúan continuamente (transmisiones suaves).

Para am de doble banda lateral sin portadora y con portadora de potencia se muestran en la figura 4.5, las formas de realizar diferentes modulaciones analógicas.

Al transmitir información digital sobre portadoras analógicas, el propósito es transmitir la mayor cantidad de bits por Hertz como sea posible, en la figura 4.6 se presentan las diferentes formas de realizar este proceso.

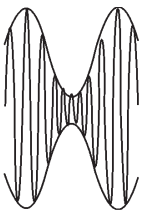
En psk, la fase es cambiada diferencialmente de acuerdo a una fase previa, +90ª para 0 y +270ª para 1 o absolutamente, donde cada estado de modulación es representado



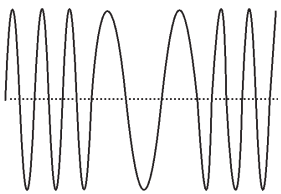
Señal modulante de información o de banda base limitada a fm Hertz

Señal portadora de frecuencia fc>>fm

Señal de am de dbl - P con B=2fm



Señal de am de dbl - pp con B=2fm



Señal de frecuencia modulada fm con ancho de banda B= $2\Delta\omega+4\omega_m$

Figura 4.5 Tipos de modulación analógica

con una fase específica para un 1, las variaciones diferenciales permiten equipo de modulación menos complicado.

En sistemas de telefonía móvil, se utilizan mezclas de modulación digital, al combinar ask con luz on, (amplitud completa) o un 0 con luz off (sin amplitud), figura 4.7.

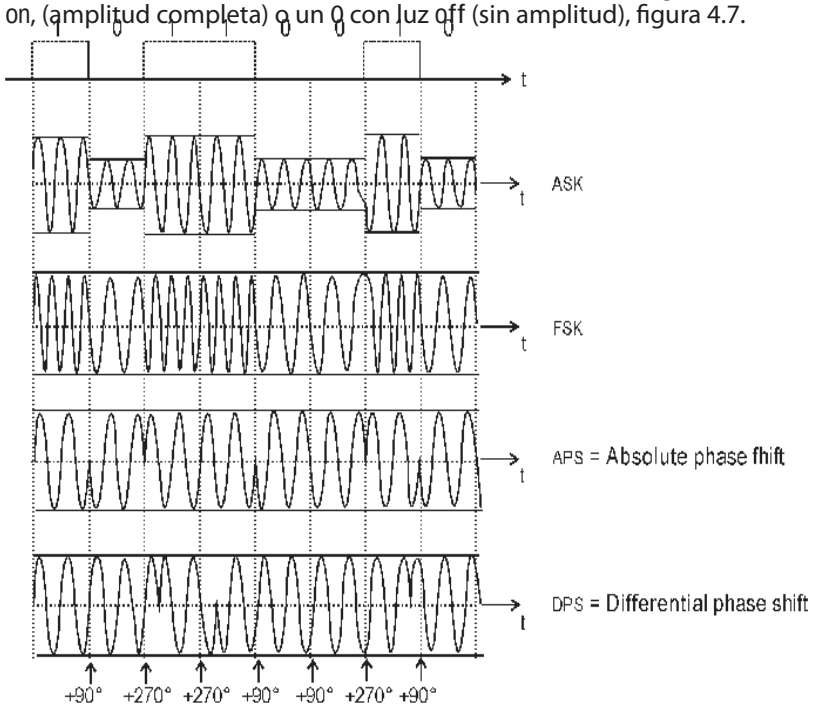


Figura 4.6 Información digital sobre portadoras analógicas

y psk se obtiene la llamada Quadrature Amplitude Modulation (qam) que permite más bits por Hertz que otros métodos.

En la figura 4.8 se presenta qam con 16 estados de modulación, con 8 estados de psk y 8 de ask.

Los módems Quadrature Amplitude Modulation (qam) se utilizan para conexiones en radio enlaces y para líneas telefónicas analógicas, para módems con 19.2 Kb/s y 256

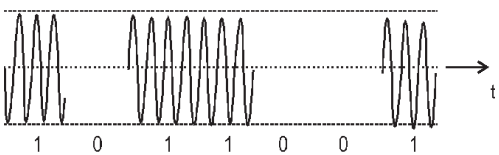


Figura 4.7 Transmisión binaria en fibra óptica

estados de modulación, se tiene que

19.200/8=2400 bauds
y la "densidad de información" es .

RAZÓN DE MODULACIÓN

La razón de modulación especifica el número de posibles cambios de estado por unidad

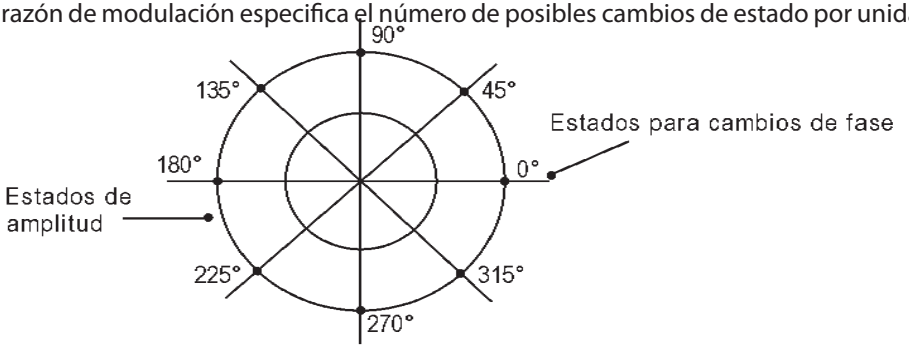


Figura 4.8 Modulación de amplitud en cuadratura

de tiempo, la unidad baud es usada para razón de modulación.

Si se utiliza un método de modulación que comprende cuatro diferentes estados, cada estado puede representar una combinación de 2 bits, cubriendo todas las combinaciones (00,01,10,11) véase figura 4.9.

Debido a que cada cambio de estado representa 2 bits, el valor de baud es la mitad del valor de bits/s, luego para 1200 bauds, se tiene que equivale a la razón de bit de 2400 bits/s.

En módems de 2400 bits/s se utilizan cuatro diferentes estados de corrimiento de fase, la frecuencia de portadora es de 1800 Hz.

Para 16 diferentes estados de modulación, o 4 bits por estado, y con la misma razón de bit de 2400 bits/s, la razón de modulación es de 600 bauds.

La razón de bit (el ancho de banda digital) está especificada por la unidad bits/s, el número de unos y ceros transmitidos por segundo, incluyendo los pulsos redundantes para detectar errores.

TRANSMISIÓN EN BANDA BASE

Cuando se envía información codificada en líneas físicas sin modulación se llama transmisión en banda base, se utiliza por ejemplo en lan, enlaces públicos de pcm. Las dos técnicas de transmisión que hacen mejor uso del cobre son adsl y hdsl.

hdsl (High Bit Rate Digital Suscriber Line)

Está técnica permite PCM de 2 Mbits/s, la principal ventaja es la distancia, la cual

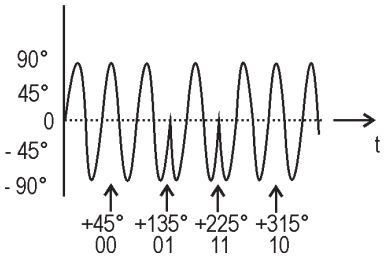


Figura 4.9 Señal con cuatro estados por corrimiento de fase

es de 1.5Km a aproximadamente 4Km. (cobre con diámetro de 0.5mm), reduciéndose la necesidad de regeneración, costos de operación y mantenimiento.

hdsl está basada en dos métodos para reducir el ancho de banda de la señal, mediante división de la transmisión en diferentes pares de alambres con full-duplex en cada par y mediante el uso de líneas codificadas que mueven la distribución espectral de la señal de información hacia frecuencias más bajas.

ADSL

Para una conexión simétrica, la capacidad de transmisión es la misma en ambas direcciones, pcm y hpsl son simétricas.

Asymmetrical Digital Suscriber Line (adsl) es asimétrica, lo que significa que la capacidad de transmisión es mayor en una dirección que en la otra, permitiendo la transmisión de video sobre líneas telefónicas tradicionales, además de que el ancho de banda es más eficiente para servicios interactivos que no requieren la misma capacidad en ambas direcciones.

SEÑALES, ESPECTROS Y FILTROS

Debido a que los conceptos de frecuencia se utilizan ampliamente en las telecomunicaciones, se revisarán los espectros de frecuencia para diferentes señales periódicas y aperiódicas mediante el análisis de series de Fourier y Transformada de Fourier.

Pulsos periódicos y su respectivo espectro.

Para una serie de Fourier que describe a una señal f(t) periódica del tiempo, con periodo T se tiene la siguiente expresión:

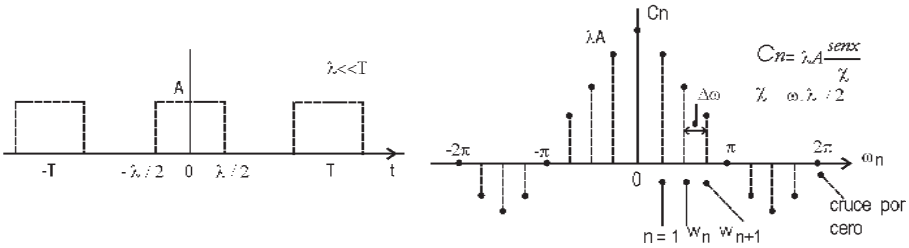
donde y

o bien

y

la separación entre componentes de frecuencia es:

El ancho de banda para los pulsos periódicos. Si se especifica como la banda de frecuencia que va desde la frecuencia cero hasta el primer cruce por cero.



Señal del tiempo y su espectro

la potencia de señales periódicas es:

La potencia promedio se obtiene sumando la contribución de potencia de todas las frecuencias, y para los pulsos rectangulares de la figura 4.10, se tiene.

IMPULSOS PERIÓDICOS UNITARIOS

Para los pulsos rectangulares, si se hace que el ancho del pulso λ tienda a cero y la amplitud tienda a ∞, se obtienen funciones impulsos de área unitaria, ancho cero y altura infinita.

Si el área Aλ tiene el valor k para un impulso de área unitaria y centrada en t = λ es , y el "ancho de banda" tiende a infinito, debido a que λ→0, su ancho de banda

INTEGRAL DE FOURIER

Las señales periódicas no llevan información, aunque se utilizan para pruebas en sistemas de comunicación, en la práctica, se hace una aproximación más adecuada al utilizar señales aperiódicas en el tiempo. Para obtener la representación en el dominio de la

frecuencia se hace que para una señal periódica el periodo sea mayor, y en el límite, se obtiene la integral de Fourier.

Transformada inversa de Fourier

Transformada directa de Fourier

F(ω) es en general una función compleja de ω y se denota como sigue:

El espectro de frecuencia de las señales aperiodicas es un espectro continuo a diferencia de las periódicas que tienen un espectro de líneas, a continuación se muestran funciones típicas y su espectro.

Para f(t) se tiene lo siguiente.

luego

PULSO TRIANGULAR

El pulso triangular y su espectro siguen la misma relación inversa tiempo-frecuencia de las señales anteriores, esto es, a medida que el ancho del pulso disminuye, el ancho de banda B medido hasta el primer cruce por cero aumenta de acuerdo a 1/T.

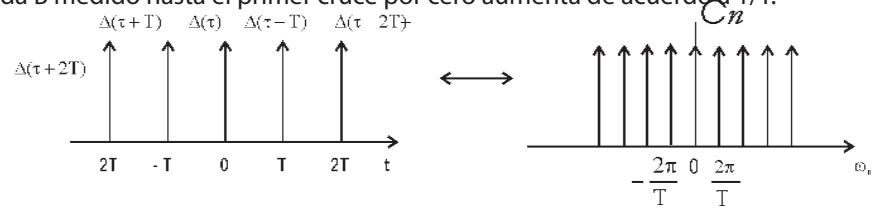


Figura 4.11 Impulsos periódicos y su espectro de frecuencia

PULSO GAUSSIANO

T = es una posible medida del ancho del pulso, y el ancho de F(ω) es entonces 1/T.

DISTRIBUCIÓN GAUSSIANA O NORMAL

Al analizar la estadística del ruido en sistemas de comunicación, es muy común recurrir a la función de densidad Gaussiana, que para una variable está dada por la siguiente expresión:

Como la curva f(x) es simétrica alrededor de x= a, la mitad del área está incluida entre -∞ y a, y la probabilidad de que x ≤ a, es entonces 0.5

La función de distribución acumulativa, o la probabilidad de que la variable sea menor que algún valor de x es:

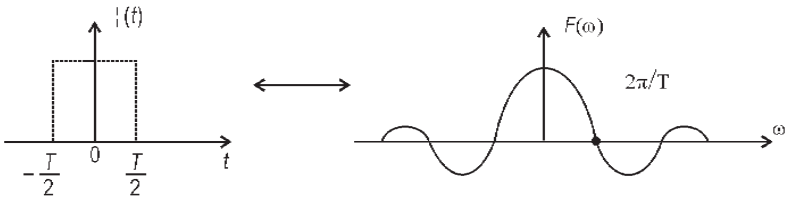


Figura 4.12 Pulso rectangular y su espectro

Luego F(a) = 0.5 = mediana de la distribución estadística.

Y el punto de probabilidad 0.5 se llama la mediana de la distribución estadística, y para la función Gaussiana la mediana, o valor promedio y el punto modal (pico de f(x)) coinciden.

RUIDO EN SISTEMAS DE COMUNICACIÓN

Las consideraciones sobre el ancho de banda (B) constituyen en elemento importante en la determinación del comportamiento de los sistemas de comunicación, además de que es un requisito para que las señales pasen relativamente sin distorsión desde el transmisor hasta el receptor.

Cuando se introduce distorsión, al transmitirse por canales de banda limitada, los efectos que se producen en las señales transmitidas tienen que ser determinadas.

Al analizar la transmisión de señales por un sistema, el ruido se agrega a la señal que se mueve desde el transmisor hasta el receptor, en algunos casos se encuentra des-

vanecimiento de la señal, interferencia de otras señales y otros efectos adversos. El ruido siempre se encuentra en los sistemas, poniendo limitaciones en el rendimiento, tal como la relación señal a ruido y la probabilidad de error.

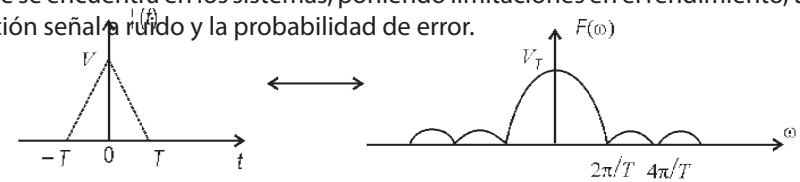


Figura 4.13 Pulso triangular y su espectro

Fuentes de ruido
- Atmósfera
- Disipación en cables de transmisión
- Movimiento aleatorio de los portadores de corriente
- Acoplamiento electromagnético
- Vibraciones mecánicas

A continuación se analiza el ruido aditivo, que consiste en sumar el ruido a la señal que se propaga por el canal de comunicación.

El ruido es aleatorio, y no es posible especificar por adelantado valores específicos

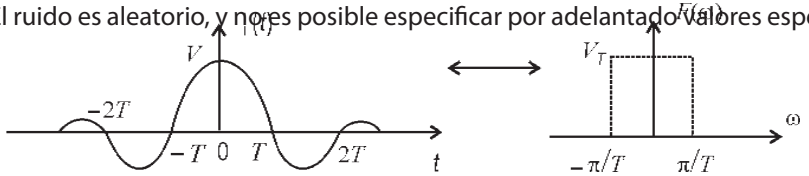


Figura 4.14 Pulso y su espectro

de voltaje en función del tiempo, pero se conoce la estadística del ruido, y en particular se tiene una función de densidad de probabilidad Gaussiana con E(n)=0 que es el valor esperado o valor promedio de n.

Si el ruido se muestra en un momento t_1, la probabilidad de que la muestra obtenida $m(t_1)$ esté dentro del intervalo n a n+dn está dada por f(n).

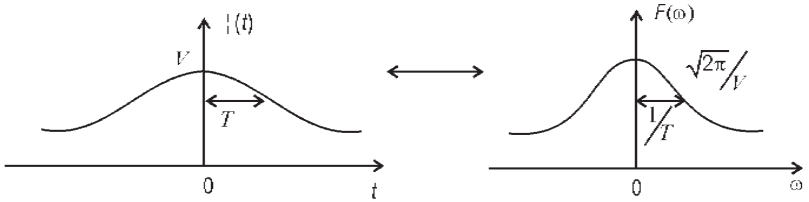


Figura 4.15 Pulso Gaussiano y su espectro

Donde n = voltaje de ruido
σ^2 = variación del ruido, potencia de ruido (λ grande).

σ = desviación estándar, valor rms del ruido.

La probabilidad de que los valores de n sean superiores a varias veces σ, es en forma decreciente exponencial con n^2, además, es igualmente probable que el ruido tenga valores positivos y negativos.

Si en un sistema de comunicaciones se están recibiendo señales binarias de pulsos, el ruido n(t) se agrega al grupo de pulsos que llega al receptor y se tiene la posibilidad de que este ruido provoque un error en la decodificación de la señal.

La distribución de probabilidad del ruido es de forma Gaussiana, de modo que el valor promedio es cero volts, y la curva es simétrica con respecto al origen, siendo σ el valor rms del ruido.

A continuación se obtiene la probabilidad de que el voltaje de ruido sea menor que un valor Kσ con K como constante.

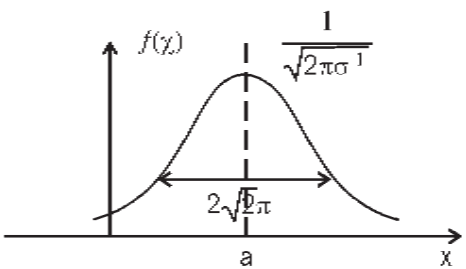


Figura 4.16 Función de densidad espectral Gaussiana

Si X representa el voltaje instantáneo de ruido. Se obtiene la probabilidad de:

para valores positivos y negativos del voltaje de ruido.
Para valores esta integral, se tabula (anexo A)
haciendo, y con la simetría de f(x).
Se obtiene:

Esta integral se llama función de error y se denota ó

Luego
Y
Consultando la función de error tabulada, se tiene que para K=1
Para K = 2 fer

Luego, la probabilidad de que el voltaje de ruido sea menor que σ volts es 0.68, y

la probabilidad de que el voltaje sea menor que el doble del voltaje rms de ruido (2σ) es 0.95.

Para una posible secuencia de pulsos binarios de amplitud A, más ruido, se determinará la probabilidad de error Pe en forma cuantitativa, haciendo que primero se transmita un cero; esto es, no hay pulso presente en la decodificación, y la probabilidad de error es la probabilidad de que exceda los A/2 volts (tomando como nivel de decisión para un 0 o un 1 a A/2 volts) para que el cero sea interpretado como 1 y si v(t)=n(t) si hay un cero presente, la probabilidad de error es la probabilidad de que v(t) aparezca con un valor comprendido entre A/2 e ∞, y la función de densidad para v, si hay un cero presente es:

y la probabilidad de error Pe_0, para este caso con

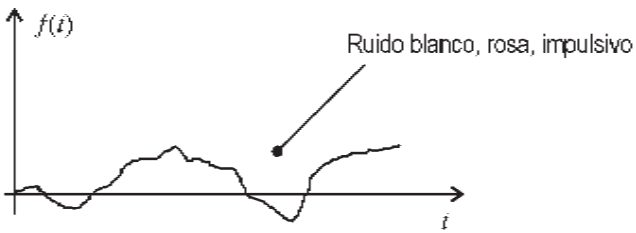


Figura 4.17 Forma de onda aleatoria para voltaje de ruido a(t)

entre A/2 e ∞

Para el caso en que se transmite un 1, la variable v(t) será de A+n(t), y la cantidad de A sirve para desplazar el nivel del ruido desde el nivel cero volts hasta el valor de A volts, la variable n fluctúa alrededor de A volts, y la función de densidad es Gaussiana con valor promedio A, y se tiene:

Estas funciones se presentan en la figura 4.19 y la probabilidad de error es que la muestra esté por debajo de A/2 volts para que el uno sea interpretado erróneamente como 0, y es el área bajo la curva de que está entre -∞ y A/2.

Las dos probabilidades anteriores son mutuamente excluyentes, el 0 impide que aparezca un 1 y viceversa, y las probabilidades se pueden sumar a la vez; ambas probabilidades son condicionales, la primera supone un 0 presente y la segunda un 1 presente, eliminando la condicionalidad al multiplicar por la probabilidad de ocurrencia, si la probabilidad de transmitir un cero y un uno es conocida, se tiene:

la probabilidad total de error es:

$P(0_T)$ = Probabilidad de transmitir un 0.

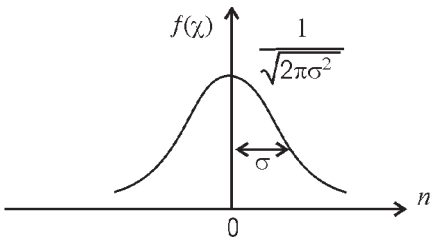


Figura 4.18 Funciones de densidad de probabilidad Gaussiana

$P(1_R/0_T)$ = Probabilidad de recibir un 1 cuando se ha transmitido un 0.
$P(1_T)$ = Probabilidad de un 1transmitido.
$P(0_R/1_T)$ = probabilidad de recibir un 0 cuando se ha transmitido un 1.
Luego
Las dos probabilidades Pe0 y Pe1 son iguales para pulsos binarios, y si 0 y 1 pueden ocurrir igualmente , entonces la Pe es igual a P_{e0} o a P_{e1}, luego Pe está dada por:

siendo

Pe depende de A/σ, la razón entre la amplitud de la señal y la desviación estándar del ruido. O bien a σ se le llama también ruido rms.

Y el cociente A/σ es la relación señal a ruido rms. También se tiene la función de error complementario.

y también

Ejemplo 1: El voltaje de ruido rms de salida de un sistema lineal está dado por 2mV, y el ruido es de tipo Gaussiano ¿cuál es la probabilidad de que el voltaje de ruido instantáneo a la salida del sistema esté entre -4 y +4mV?

El valor del ruido rms es 2mV = σ de luego la

entonces K vale 2
lo que indica que el 95% del tiempo la señal está variando entre -4 y +4 mV.
Si ahora se agrega al ruido de salida un voltaje de cc de 2mV, ¿cuál será la nueva

probabilidad?

Ejemplo 2: En un sistema de transmisión digital binario que transmite 400000 bits/seg, la amplitud de la señal de información es de 2mV y el valor rms del ruido es de 1mV, calcular el tiempo promedio entre errores.

y A=2mV

luego

si 158 es proporcional a 1000
luego en 400000 bits/seg se tendrán 63200 errores/seg.
Y 1 error ocurre cada 15.8 μseg.

Aumentando la señal a 4mV (amplitud)

en 400000 bits/seg se tendrán 9000 errores/seg, y un error ocurre cada 111.1seg.

Aumentando a 6mV la Pe es ahora.

y un error ocurre cada 1.9mseg.
y para A = 8mV

la fer = 0

La gráfica para la Pe comparada con A/σ en decibeles se muestra en la figura 4.20, se observa que para $A / \sigma = 7.4$ (17.4dB) la Pe es 10^{-4}, que indica que se tendrá 1 bit de error para cada 104 transmitidos.

Al aumentar la relación A/σ disminuye la Pe, y para módems comerciales es usual utilizar probabilidades de 10^{-8} a 10^{-12}.

Enseguida se muestra un generador de ruido blanco seudo-aleatorio, debido a que estas secuencias binarias son de gran utilidad donde se requiere una señal que siendo determinística y reproducible, presente a la vez características de señal aleatoria, siendo la diferencia entre una señal seudo-aleatoria y una aleatoria, el período; la primera tiene período finito y la segunda es aperíodica.

Los registros de corrimiento proporcionan secuencias seudo-aleatorias, siendo las

propiedades para una secuencia binaria las siguientes:

A) Para un período, el número 0 o 1 difieren, a lo más en la unidad.

B) En las series de unos consecutivos y ceros consecutivos, en un período, la mitad de las series de cada tipo es de longitud uno, un cuarto de longitud 2, un octavo de longitud 3, etcétera.

En el caso de utilizar un registro con n-etapas, la longitud de un período de la secuencia seudo-aleatoria es de 2^n-1.

Una configuración que permite generar una secuencia pseudo-aleatoria consta de un registro de corrimiento unidireccional (figura 4.21), y de un circuito combinatorio lineal que

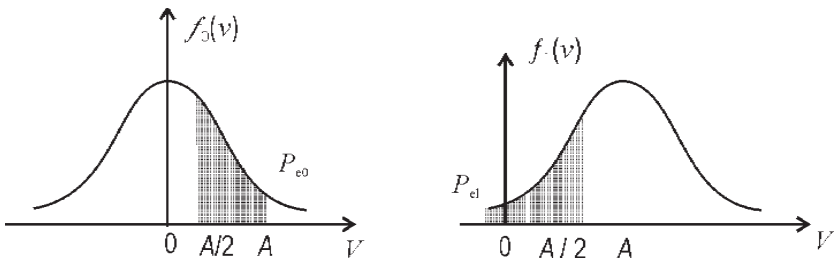


Figura 4.19 Densidad de probabilidad para 0 y 1

genera la señal que alimenta a la primera etapa del registro, esta señal que se retroalimenta es función lógica de los niveles lógicos presentes, en otras etapas, la operación or exclusiva se utiliza para la desunión de los niveles lógicos.

Siempre se busca que la secuencia tenga una longitud máxima, tan larga como la secuencia del registro pueda permitirlo, y se tiene longitud máxima=2n-1, si n=30, la longitud máxima=230-1=1073215489.

La aplicación del generador de ruido blanco es en:

- Pruebas de sistemas de audio.
- Música aleatoria.
- Criptografía.
- Sistemas de seguridad.

Si se adiciona un filtro a la salida se dice que "colorea" al ruido blanco, pudiendo resultar "rosa", "azul" etcétera.

Si la información saliente de una computadora se modula con una seudo-secuencia aleatoria, a fin de que la resultante sea inmune al ruido, y así pasar por lugares ruidosos, para recuperar la información correcta se demodula con una copia idéntica de la seudo-secuencia aleatoria.

Del circuito de la figura 4.21 la compuerta OR-exclusiva en la retroalimentación da la longitud máxima, aunque esta configuración no es la única para tal fin. Si se cierra el interruptor se cortocircuita el inversor, ocasionando que de entre las 2^N combinaciones posibles de las salidas de los N biestables, la que contiene exclusivamente ceros no apa-

rece en la secuencia, si el registro tuviera únicamente ceros, se estaría paseando un cero, y ninguna secuencia sería posible.

Si el circuito se deja abierto, entonces la secuencia de puros unos está prohibida, iniciando el circuito con solo ceros, se obtiene la secuencia siguiente:

Si se tuvieran 31 etapas, el registro de corrimiento tendría una secuencia de longitud = 2147483647 estados, y si se tiene un reloj de 1MHz, la secuencia se repetirá cada 2147.5 segundos, y para una frecuencia de 100KHz la secuencia se repetirá cada 5 horas aproximadamente, es decir, la secuencia se repetirá cada 2^{n-1} ciclos de reloj.

El circuito anterior (31 etapas) a frecuencias bajas tendrá un período tan largo que no se notará la diferencia entre una señal aleatoria y la no-aleatoria, el cálculo de las condiciones de retroalimentación para cada longitud del registro, permite obtener una secuencia de período máximo y es muy complejo, sólo resta transformar la secuencia en señal analógica y digital.

NIVELES DE DECISIÓN

Al ser las señales (uno o cero) igualmente probables, se ha elegido arbitrariamente el nivel de decisión A/2 para la secuencia de pulsos unipolares, para el caso polar se ha supuesto el nivel 0 para decisión de 1 o 0. Luego, el decodificador basa su decisión en la amplitud de voltaje de la muestra v(t), y para ajustar Pe se varía la amplitud del nivel al cual se toma la decisión que se llamará d, y éste será igual a cero si los unos y ceros se presentan con mayor frecuencia, y se tendrá $P_0 > P_1$ y d se desplazaría en forma positiva y viceversa, luego d dependerá de P_0 y P_1.

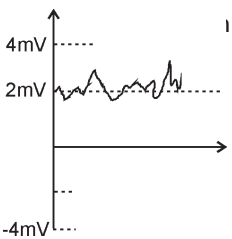
Para obtener un nivel óptimo de d se procede a realizar el siguiente análisis:

En general

suponiendo que hay la misma cantidad de 0 y 1

y

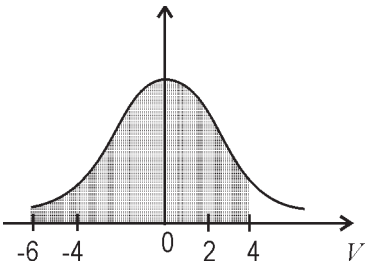
respecto a d para tomar el nivel óptimo.



$$\text{Prob}(-4mV \le u \le 4mV) = \frac{1}{2}\text{Prob}(-6 \le u \le 6) + \frac{1}{2}\text{Prob}(-2 \le u \le 2)$$

$$= \frac{1}{2}\,\text{fer}\,\frac{3}{\sqrt{2}} + \frac{1}{2}\,\text{fer}\,\frac{1}{\sqrt{2}}$$

$$= 0.4987 + 0.3443 = 0.84$$


-6
-4
0
2
4
V

Para señales unipolares el punto d está dado por el punto donde las dos funciones de densidad se intersectan.

Para el caso de señales polares el punto d será igual a cero si.

Cuando , el nivel se desplaza y la expresión para el nivel de decisión será:

y d aumenta positivamente si, y negativamente si .

ANÁLISIS DE RUIDO

Se obtendrá la representación espectral del ruido. Las fuentes que producen ruidoson: resistores, transistores, diodos, etcétera. La forma de onda de una señal aleatoria tal como el ruido sería la de n(t), de la figura 4.24.

Se tiene una función de correlación que proporciona una medida de la semejanza entre una señal y su versión retardada en el tiempo expresada por la siguiente ecuación.

AUTOCORRELACIÓN

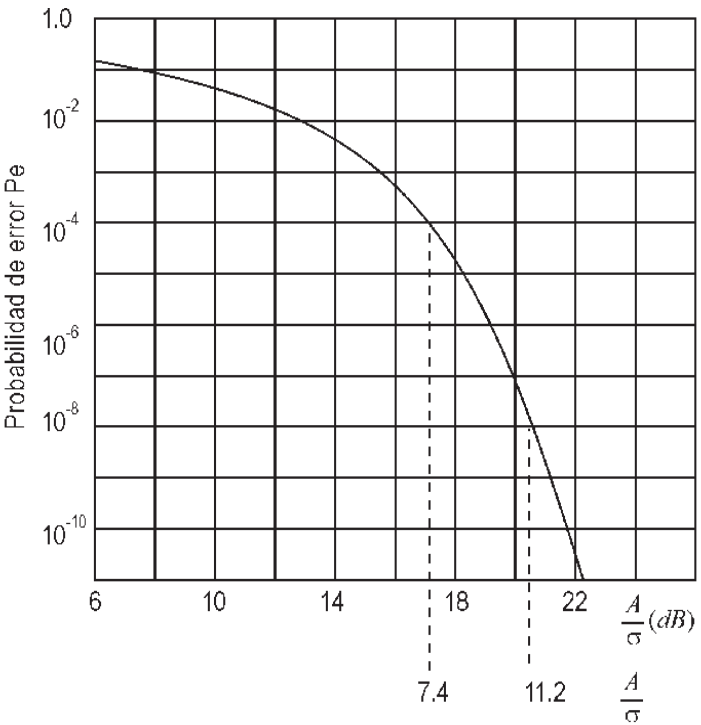


Figura 4.20 Pe comparado con A/s en decibeles

Cuando, la variable aleatoria $n(t_2)$ llega a estar más "cercanamente relacionada" o "más predecible" por $n(t_1)$ luego se define una función de autocorrelación por:

Donde E es el valor esperado o segundo momento estadístico.

Cuando E(n) es independiente del tiempo se denomina proceso estacionario. Para analizar a Rn(t1,t2) se hace que dependa únicamente del intervalo (t2-t1) = (y no del origen del tiempo

la medición de las variaciones en el tiempo del proceso aleatorio, se hacen mediante:

si t = 0

que es la potencia promedio

POTENCIA DEL RUIDO

Relacionar Rn(τ) con el análisis espectral de n(t) y definir un ancho de banda, considerando

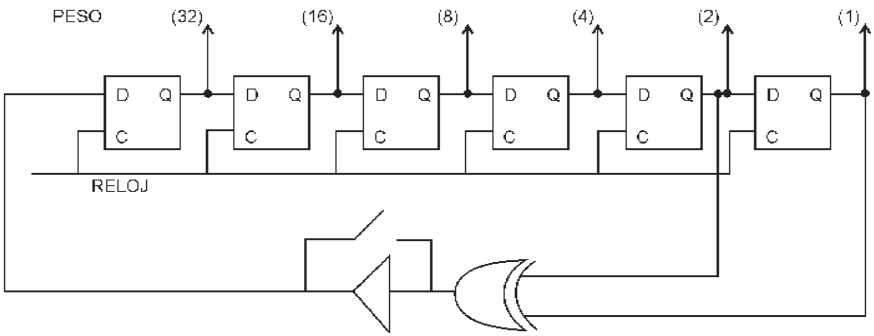


Figura 4.21 Generador de secuencia pseudo-aleatoria

a n(t) una función determinística.

donde

El ruido es una función real

si m = l la integral es igual a T
si m ≠ l la integral es igual a cero

000000-0	011010-26	100101-37
100000-32	001101-13	010010-18
110000-45	000110-6	001001-9
111000-56	000011-3	000100-4
111100-60	100001-33	100010-34
111110-62	010000-16	010001-17
011111-31	101000-40	001000-8
101111-47	110100-52	100100-36
110111-55	111010-58	110010-50
111011-59	011101-29	011001-25
111101-61	001110-14	001100-12
011110-30	000111-7	100110-38
001111-15	100011-35	010011-19
100111-39	110001-49	101001-41
110011-51	011000-24	010100-20
111001-57	101100-44	101010-42
011100-28	110110-54	010101-21
101110-46	011011-27	001010-10
010111-23	101101-45	000101-5
101011-43	010110-22	000010-2
110101-53	001011-11	000001-1
		000000-0 (y se vuelve a repetir la secuencia)

es una variable aleatoria o bien es un proceso estocástico, y los resultados son

totalmente probables.

Densidad espectral de potencia de ruido.

y luego y

y

es la transformada de Fourier de y es la densidad espectral de potencia o espectro de potencia.

RUIDO BLANCO

El ruido blanco tiene un espectro de potencia constante (K) en el dominio del tiempo y la transformada de Fourier es:

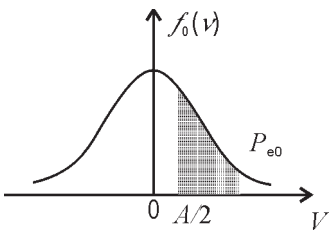


Figura 4.22 Señales con una polaridad

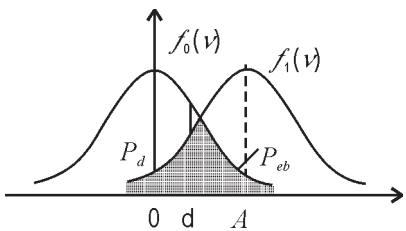


Figura 4.23 Nivel de decisión d en transmisión binaria

Si el ruido blanco se introduce a un filtro pasa-bajas, se obtiene ruido rosa. A continuación se encontrará la autocorrelación del ruido rosa.

luego
De
Y

primer cruce por cero y para 1mseg.

La frecuencia de corte del filtro pasa-bajas es de 1KHz y B = 1KHz

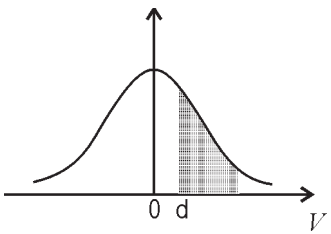
Ejemplo 3: Una señal aleatoria s(t) de valor promedio cero tiene la densidad espectral de la figura 4.28. Determine: a) ¿cuál es la potencia promedio y b) Demuestre que la función de autocorrelación es

a)

potencia promedio

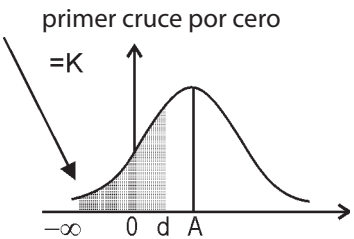
b)

c) Si B = 1MHz y K = 1μV^2/Hz, demuestre que el valor rms de la señal es y que las



muestras espaciadas 1μs no están correlacionadas.

σ = valor rms.



segundo cruce por cero

RUIDO A TRAVÉS DE SISTEMAS LINEALES

En un circuito RC,

Ancho de Banda del sistema lineal (circuito RC)

Ejemplo 4: Una fuente n(t) tiene una función de autocorrelación dada por

a) encuentre y dibuje $Rn(\tau)$ y $Gn(\tau)$ para $a/2n=10^4$ y 10^6, compare las dos familias de curvas y cuál es el ruido en cada uno de los 2 casos.

b) encuentre la potencia del ruido de salida rms.

si

para

para

FILTROS ADAPTIVOS

En las comunicaciones digitales de banda base se tiene ruido blanco agregado a la secuencia de pulsos binarios (figura 4.37) de forma conocida a la entrada del receptor, con la suma compuesta pasando por un filtro lineal; a continuación se hace un muestreo y se toma la decisión para el nivel del pulso del detector. El diseño del filtro previo a la detección deberá maximizar la relación $A/\rho = A/$ a la salida de éste.

Los resultados del análisis siguiente, se aplican tanto para señal de banda base y como para transmisión digital con portadora; por otro lado, la forma de los pulsos no tiene que ser completamente rectangular, lo que interesa es reconocer una señal pulsante en presencia de ruido, enseguida se obtendrá la función de transferencia H(w).

Se tiene lo siguiente:

A: amplitud de la información.

N: la potencia del ruido.
E: energía de la información.
relación de potencia de la señal a potencia del ruido
E = constante

si es máxima → la probabilidad de error es mínima, y la

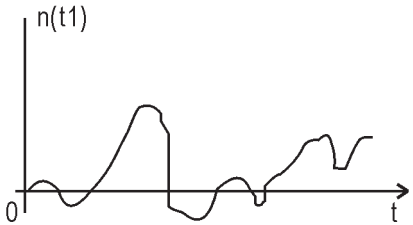


Figura 4.24 Señales de ruido n(t)

El filtro tiene una función de transferencia
S(w) es la salida del filtro, y se obtiene para el dominio del tiempo;

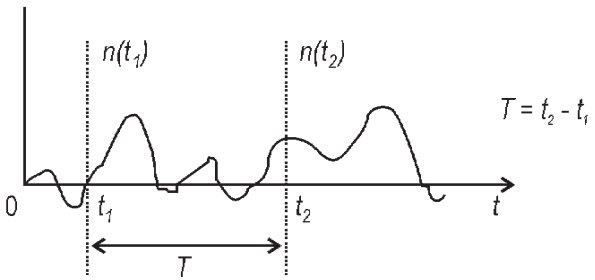


Figura 4.25 Función de autocorrelación

Tenemos a la entrada e interesa a la salida.

Tenemos la energía de la señal como:

Desigualdad de Shwartz

ocurre que es máxima cuando se cumple la igualdad. Y si el numerador es igual al denominador, luego de la demostración de la desigualdad se tiene:

la igualdad sucede cuando:

El filtro sólo reconoce la forma de la señal de entrada, y los filtros que tienen la característica de la ecuación anterior se conocen como filtros adaptados o acoplados. La relación señal a ruido es una función de la energía de la señal y de la densidad espectral del ruido blanco, y si se tienen dos señales diferentes en la entrada del filtro adaptado, pueden proporcionar la misma probabilidad de error en presencia de ruido blanco aditivo, siendo la energía de la señal la que proporciona la capacidad de detección del filtro en presencia de ruido.

Ejemplo5: Un pulso rectangular de amplitud V volts y ancho T segundos se aplica a un filtro adaptado, demuestre que la salida es un pulso de forma triangular y el valor máximo de este pulso.

Demostración:

Del teorema de corrimiento en tiempo se tiene lo siguiente:

Tomando el conjugado, se tiene la expresión para el filtro adaptado:

si la entrada es
Y la salida es

La transformada inversa es una forma de pulso triangular desplazado un tiempo, de amplitud. Verificar que la transformada inversa es un pulso triangular.

RUIDO DE BANDA ANGOSTA

En la transmisión de señales binarias con portadoras analógicas, se debe tener un criterio para seleccionar un tipo en particular, así como el método de detección en particular, ya sea en forma síncrona o por detección de envolvente. En el caso de

sistemas psk con detección síncrona ofrece mejoras en la relación señal a ruido y una probabilidad de error menor que los demás métodos, y se prefiere siempre y cuando se mantenga la coherencia de fase. Cuando se utiliza detección de envolvente, el método recomendado es fsk sobre a ook aunque los circuitos sean complejos, aquí la coherencia de fase no es posible.

En la detección de fm y am la relación señal a ruido que presenta fm es superior a am, a continuación se analiza la representación de banda angosta del ruido, considerando el ruido n(t) en la salida de un filtro de banda angosta o estrecha, y si Gn(f) es la densidad espectral centrada alrededor de f0 y ancho de banda 2B<<f0, el ruido oscilará alrededor de la frecuencia f0 como se muestra en la figura 4.42.

Para una señal de am se tiene la conocida expresión siguiente;

=g(t)

Por analogía se tiene ahora una envolvente aleatoria r(t), con portadora aleatoria y se tiene

donde es una fase aleatoria

Potencia de ruido total

Se tiene que

y para el espectro discreto se tiene;

Se tiene que todos los dobles productos son cero, debido a que dos cosenos de diferentes frecuencias son ortogonales y por lo tanto igual a cero-

y también

y solo queda la integración de

Gn(t) … (es medible)

haciendo la analogía siguiente:

donde

x(t) y y(t) son términos de baja frecuencia.

El modelo de ruido de banda angosta sirve para cualquier modem, ya sea de fsk, ask y psk.

DETECCIÓN DE SEÑALES BINARIAS

Con la representación de ruido de banda angosta se compara la relación S/N de ask psk y ook, y se tienen los siguientes métodos:

1) Detección síncrona (coherente).

2) Detección de envolvente (asíncrona-incoherente).

Para señales ask ook y psk se utiliza detección síncrona como se observa en la figura 4.46

Para un voltaje de ask se tiene A=1 y B =0

La probabilidad de error de ask es: figura 4.48 Pulso para ASK

Para señales psk

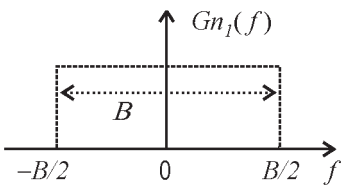


Figura 4.26

Para fsk

Ejemplo 6: se tiene que, demuestre lo siguiente, y bosqueje ambas.
Obteniendo la transformada de Rn(T)

tenemos que:

y con el Teorema de la modulación

y la transformada de una constante es:

luego se tiene que; 1.....

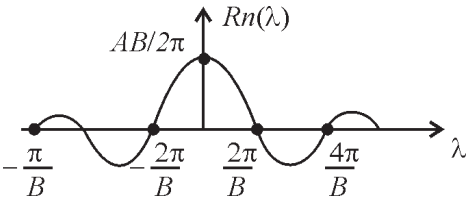


Figura 4.27

y gráficamente a Rn(T) en la figura 4.50

Ejemplo 7: Para una señal aleatoria dada , siendo θ una variable uniformemente distribuida, demuestre que:
cuando se promedia sobre la variable aleatoria θ.

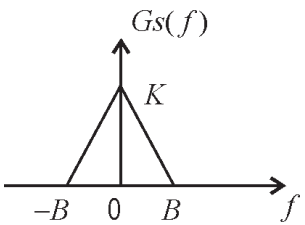


Figura 4.28

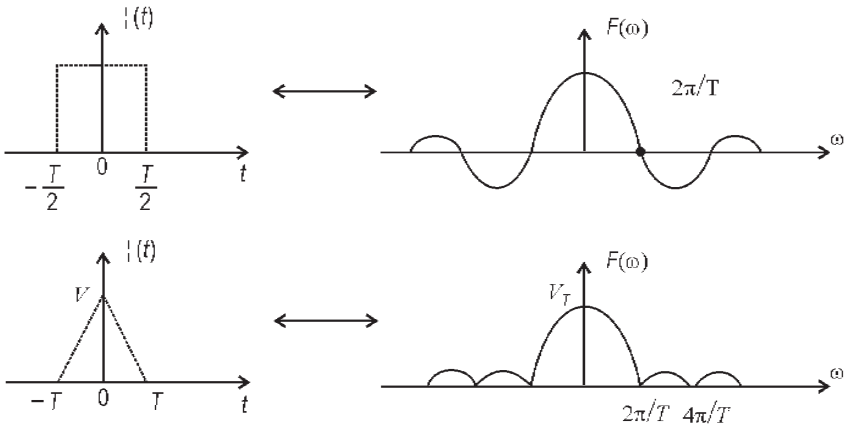


Figura 4.29

Figura 4.30

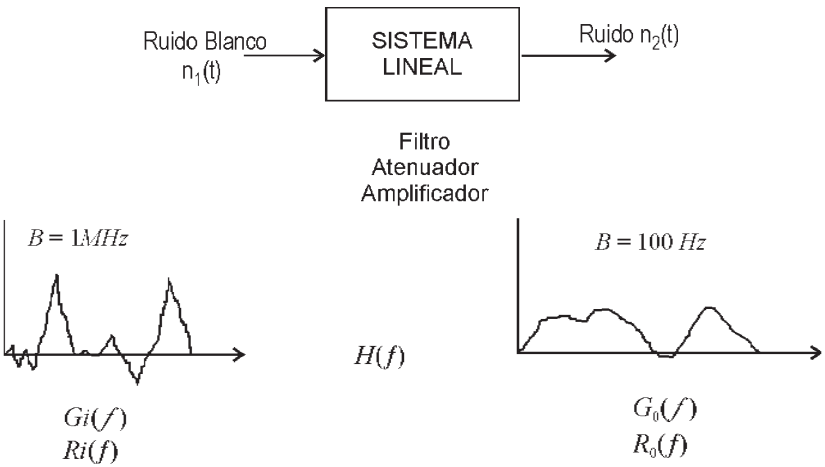


Figura 4.31

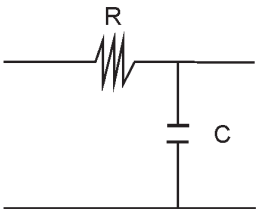


Figura 4.32

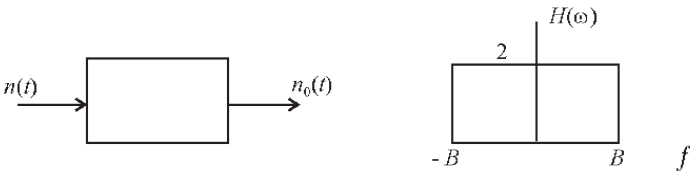
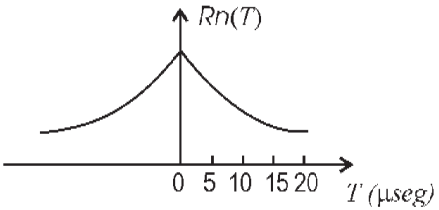


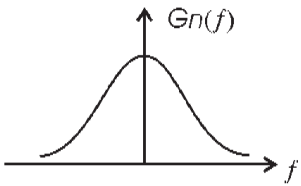
Figura 4.33

$$Gn(f) = \frac{1}{3}\frac{2a}{(2\pi)^2\left[\left(\frac{a}{2\pi}\right)^2 + f^2\right]} = \frac{1}{3\pi}\frac{a/2\pi}{\left(\frac{a}{2\pi}\right)^2 + f^2}$$

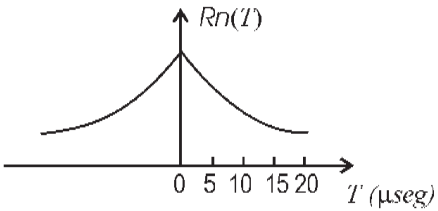
$$Gn(f) = \frac{1}{3\pi}\frac{a/2\pi}{\left(\frac{a}{2\pi}\right)^2 + f^2} =$$



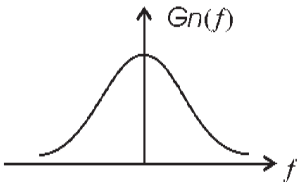
$$\text{para}\frac{a}{2\pi} = 10^4$$



$$\text{para}\frac{a}{2\pi} = 10^4$$



$$\text{para}\frac{a}{2\pi} = 10^6$$



$$\text{para}\frac{a}{2\pi} = 10^6$$

Figura 4.34

Figura 4.35

$$N_{no} = \int_{-\infty}^{\infty} G_{no}(f)\,df = \int_{-B}^{B} G_{no}(f)\,df$$

$$= 4\frac{(a/2\pi)}{3\pi}\left[\frac{1}{\left(\frac{a}{2\pi}\right)^2}\,tg^{-1}\,\frac{f}{\frac{a}{2\pi}}\right]_{-B}^{B}$$

$$N_{N\,o} = \frac{4}{3\pi}\left|\frac{\pi}{4} + \frac{\pi}{4}\right| = \frac{4}{6} = 0.667$$

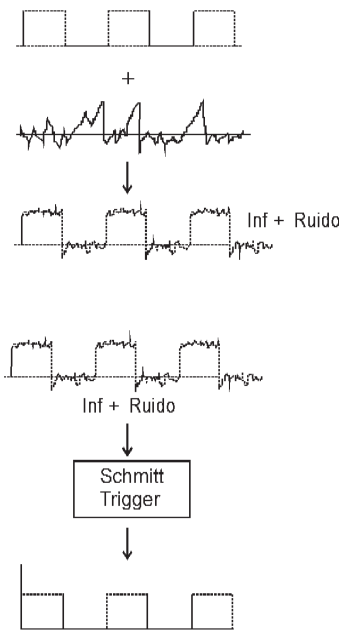


Figura 4.37

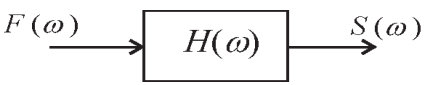


Figura 4.38

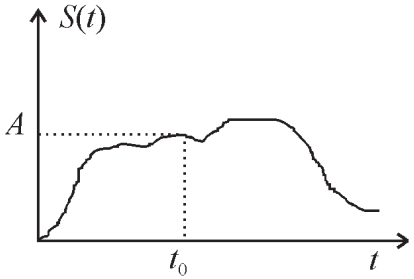


Figura 4.39

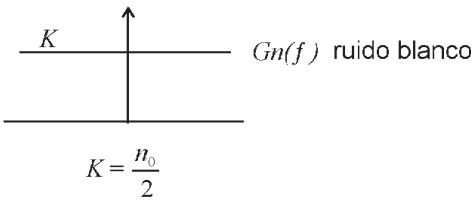


Figura 4.39

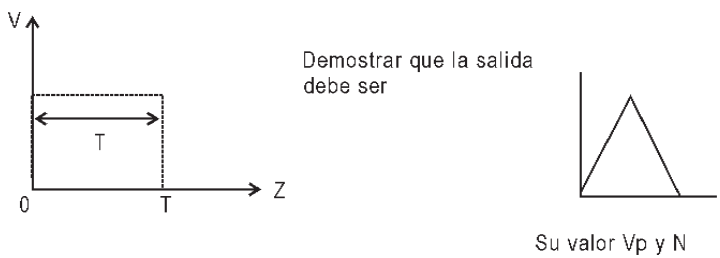


Figura 4.40 señal rectangular a través de un filtro adaptado

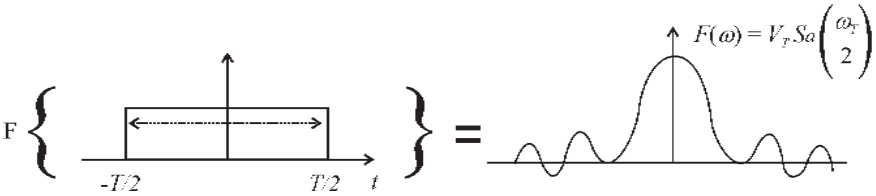


Figura 4.41 Transformada del pulso rectangular

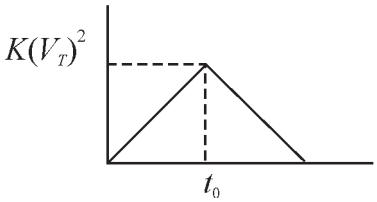
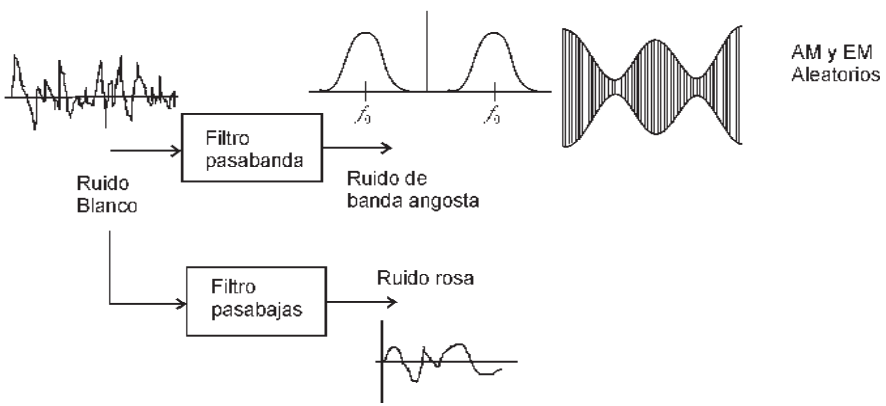


Figura 4.42



4.42 Obtención de ruido de banda angosta, y si la señal contiene dos bandas laterales se tiene señal de am

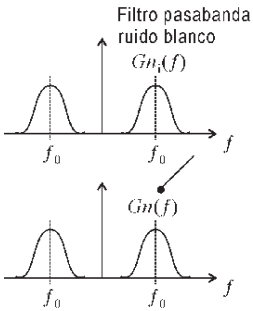


Figura 4.43 Densidad espectral del ruido

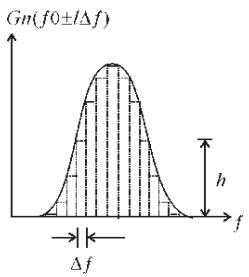
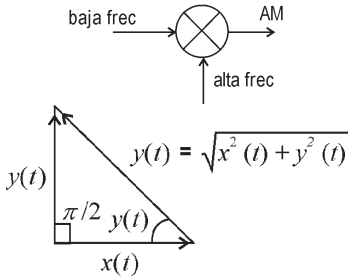


Figura 4.44 Equivalente discreto de la densidad espectral



$$\theta(t) = \tan^{-1} \frac{y(t)}{x(t)}$$

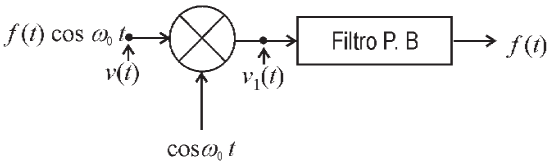


Figura 4.46 Detección síncrona

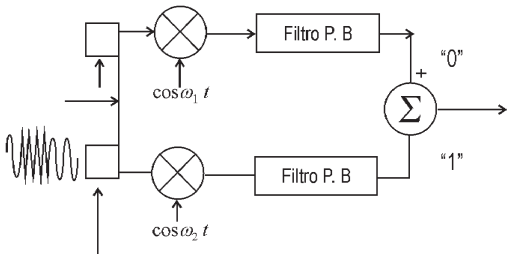


Figura 4.47 Detección síncrona de esk

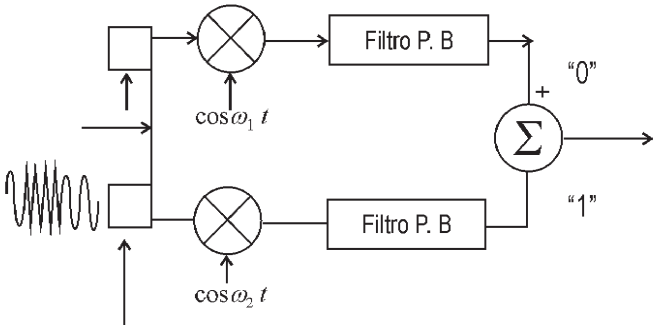


Figura 4.49 Detección de fsk

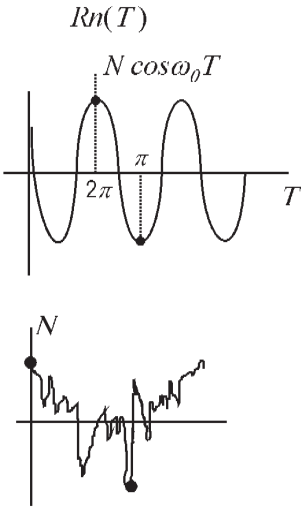


Figura 4.50 Gráfica de Rn(T)

CAPITULO V
ENCRIPTAMIENTO DE DATOS

Las intituciones financieras; en la época de la computación no escaparon al uso de este instrumento, e inevitablemente con ello el mal uso de las computadoras también triunfó. El problema era que, con conocimientos elementales y una terminal de computadora, culquier usuario podía transferir fondos a su propia cuenta, utilizar la tarjeta de alguien más, u obtener dinero de un cajero automático.

International Bussines Machine (ibm) comprendió esta situación rápidamente y, a finales de los años sesenta, preparó un grupo de investigación para desarrollar un código de cifrado conveniente para proteger datos. Los trabajos arrojaron como resultados en 1971, el llamado código Lucifer, mismo que fue vendido a Lloyds de Londres para un sistema dispensador de efectivo.

LUCIFER

Lucifer tuvo éxito pero tenía algunas debilidades. ibm invirtió aproximadamente tres años para refinarlo y fortalecerlo. El código se analizó muchas veces por expertos en criptología y resistió los sofisticados ataques ciptoanalíticos. En 1974 estavo listo para comercializarse.

Al mismo tiempo, el National Bureau Standars (nbs), responsable desde 1965 de las normas, en vías de desarrollo, para la compra de equipo computacional por el gobierno federal estadounidense, comenzó un estudio sobre seguridad informática. El nbs vio la necesidad de crear un método de encriptado, y solicitó un algoritmo de encriptamiento conveniente para el almacenamiento y transmisión de datos clasificados.

En respuesta a esta solicitud, ibm propuso su cifrador Lucifer. Este cifrador consistió en un algoritmo sumamente complejo incluido en una estructura de ic. Básicamente, la clave o llave del cifrador entra en una serie de ocho bloques "S", fórmulas matemáticas complejas que encriptan y desencriptan datos con la clave apropiada. El cifrador Lucifer inicial tenía una clave de 128 bits, antes de que se presentara el cifrador a nbs, ibm lo acortó quitando más de la mitad de la clave.

PARTICIPACIÓN DE NSA

Por su parte la Agencia de Seguridad Nacional (nsa) había mostrado un marcado interés en el proyecto Lucifer; por lo que prestó ayuda a ibm en el proceso de las estructuras de bloques "S".

Durante años, la nsa dependio, en cuanto a comunicaciones de los datos internacionales como los relacionados con Medio Oriente para las transacciones de petróleo, mensajes; las actividades comerciales de América latina, Europa y el Este lejano. Así como los vinculados al ejército e inteligencia diplomáticos. Con ello logró obtener mucha información sobre los países comunistas y no-comunistas.

Ahora, el desarrollo de un dispositivo de encriptado de datos barato, muy seguro, amenazó causar un problema serio a la nsa; investigadores externos podían hacer encriptado con los métodos de la nsa.

Las reuniones entre la nsa e ibm produjo un acuerdo por el cual ibm reducía su clave de 128 bits a 56 bits y clasificaba ciertos detalles sobre la selección de los ocho bloques "S" para el cifrador.

El nbs le pasó este cifrador a la nsa para su análisis. Ésta certificó el algoritmo como libre de cualquier debilidad matemática o estadística y lo recomendó como el mejor candidato para el estándar de encriptado de datos nacionales (Data Encryption Standard, des). La sugerencia de nuevo se criticó. ¿Era el cifrador lo suficientemente grande para impedirles a los indiscretos corporativos penetrarlo o muy corto para que la nsa rompiera el código rápidamente?

La agencia se ocupó, vanamente, con las criticas de los bloques "S", y por consiguiente insistió que ciertos detalles fueran clasificados. La razón citada para ello era simple: los des podrían estar disponibles comercialmente permitiendo el uso extranjero de un cifrador irrompible. Las debilidades encontradas en el cifrador permitían a la agencia penetrar cada canal y banco de datos usando el des. Los violadores de código del nsa quisieron estar seguros de que ésta podría romper el cifrador. Como resultadode la situación se alcanzó un compromiso burocrático. La parte del bloque "S" del cifrador se fortaleció, y la clave, que era dependiente de los usuarios de código, se debilitó.

Sin embargo, los expertos en computación defendieron la posición de que sería posible construir una computadora que usara un millón de especiales "chips de búsqueda" que podría probar un millón de posibles soluciones por segundo; por consiguiente, en 72,000 segundos (20 horas), todas las posibles combinaciones podrían probarse. Habría un 50% de probabilidad de que en 10 horas de ensayo-tiempo romperían el código (con 56 bits, hay 2^{56} combinaciones). Semejante computadora costaría alrededor de 20 millones de dólares y, prorrateando a más de cinco años, esto significaría aproximadamente 10,000 dólares por día. Si se utilizara cada 24 horas, cada código promediaría aproximadamente 5000 dólares para romperlo. Cuando la tecnología derrumbó los costos, estas figuras podrían ser divididas con un factor de 10 o 100.

EL LUCIFER ORIGINAL

¿Y si la clave de 128 bits del Lucifer original se hubiera sometido a consideración? hay 2^{128} soluciones que es igual a $34.03x10^{37}$. Este número es astronómico e incomprensible para la mayoría de las personas. Si pudieran probarse 1 billón de soluciones por segundo, tomaría $34x10^{25}$ segundos, no más, o alrededor de 1.08×10^{19} años. Éste es un tiempo bastante largo. El universo conocido existe aproximadamente $2.6 x10^{10}$ (26 billones) años. Por consiguiente, el código Lucifer de ibm, al presente, probablemente es irrompible.

des

El 15 de junio de 1977, el des se volvió el cifrador oficial del gobierno norteamericano; en la actualidad se utiliza ampliamente, y uno de los usuarios principales es hbo con su sistema de VideoCipher II. Con aumentos en las velocidades de la computadora, nuevas tecnologías, y costos más bajos, la seguridad del cifrador desaparecerá lentamente. Algunas autoridades le dan cinco años o diez. El advenimiento del VideoCipher II enfocó más aún la atención en el des y más pronto o más tarde será derrotado; mientras tanto, los nuevos métodos de Scrambling reemplazarán probablemente al VideoCipher II.

EXTRACTOS DEL DES

Los des especifican un algoritmo para ser implementado en dispositivos de hardware electrónico y usado para la protección criptográfica de datos de la computadora. Las publicaciones acerca de esta norma mantienen una descripción completa de un algoritmo matemático, el encriptado (enciphering) y desencriptado (deciphering) de información codificada en binario. Los datos encriptados se convierten a una ininteligible forma llamada un cifrador. Desencriptar un cifrador convierte los datos otra vez a su forma original. El algoritmo descrito en esta norma especifica ambas operaciones; cifrado y descifrado, los cuales están basados en un número binario llamado la clave. La clave consiste de 64 dígitos binarios (ceros o unos), de los cuales 56 bits son usados directamente para el algoritmo y 8 bits para la detección de error.

Los datos codificados en binario pueden ser criptográficamente protegidos usando el algoritmo des junto con una clave; es decir, la clave es generada de modo que cada uno de los 56 bits usados por el algoritmo sea aleatorio y el octavo bit, detector de error está puesto para que cada byte (en su bit 8) sea para la clave impar, esto es, hay un número impar de unos en cada byte. Cada miembro de un grupo de usuarios autorizados de datos encriptados de computadora, debe tener la clave para cifrar los datos. Esta clave, que tiene cada miembro en común, es utilizada para descifrar cualquier dato recibido en forma cifrada de otros miembros del grupo. El algoritmo de encriptamiento especificado en esta norma es conocido por todos aquellos que la emplean. La clave única escogida

para uso en aplicaciones particulares hace que los resultados del encriptador sean únicos, la selección de una clave diferente causa importantes diferencias en la salida del cifrador. La seguridad criptográfica depende de la seguridad proporcionada por la clave para cifrar y descifrar los datos.

MODOS ALTERNATIVOS DE USAR EL DES

La publicación 74 de Guidelines for Implemnentig and Using the nbs Data Encryption Standard" fips, describe dos modos diferentes para usar el algoritmo descrito en esta norma. Pueden introducirse bloques de datos que contienen 64 bits directamente en el dispositivo que genera bloques de 64 bits de cifrado bajo el control de la clave. Esto se llama el modo del libro de código electrónico (ecb).

Alternativamente, el dispositivo puede usarse como un generador binario para producir aleatoriamente bits binarios, con los que, entonces, se combinan datos limpios (desencriptado) que usan una operación or exclusiva lógica. Para asegurar que se sincronizan el dispositivo del cifrador y el dispositivo descifrador, sus entradas siempre se ponen a los 64 bits anteriores de cifrado transmitidos o recibidos. Este segundo modo de usar el algoritmo del encripción se llama el modo de cifrado retroalimentado (cfb).

El ecb genera bloques de 64 bits de cifrado. El cfb genera un cifrado que tiene el mismo número de bits como el texto llano. Cada bloque de cifrado es independiente de otros cuando se usa el ecb, mientras que cada byte (grupo de bits) de cifrado depende de los 64 bits previos del cifrado cuando se usa el cfb.

El algoritmo criptográfico especificado en esta norma, transforma un valor binario de 64 bits en un único valor variable de 56 bits. Si la entrada completa de 64 bits se utiliza y si la variable de 56 es elegida aleatoriamente, ninguna otra técnica probará todas las posibles claves, usando una entrada y salida conocida por el des, garantizará encontrar la clave elegida. Como se tienen más de 70.000,000,000,000,000 posibles claves de 56 bits, la posibilidad de derivar una clave particular de esta manera es sumamente improbable de que "amenace" los sistemas. Y si la clave frecuentemente se cambia, el riesgo de que este evento pase disminuye en mayor proporción.

Sin embargo, los usuarios deben ser concientes de que teóricamente es posible encontrar la clave en menos intentos y debe avisarse para cambiar la llave tan a menudo como sea posible. Los usuarios deben cambiar la clave y proporcionar un alto nivel de protección para minimizar los riesgos potenciales del uso no autorizado del equipo de cómputo. La viabilidad de conocer la clave correcta puede cambiar con adelantos en la tecnología.

METODOS DE ENCRIPTADO DE DATOS

El encriptado es la transformación de datos de su forma inteligible original a una forma de cifrado ininteligible. Pueden usarse dos transformaciones básicas: permutación y

substitución. La permutación cambia el orden de los símbolos individuales que forman los datos. En la substitución, los símbolos son reemplazados por otros símbolos. Durante la permutación los símbolos retienen sus identidades pero pierden sus posiciones. En la substitución los símbolos retienen su posición pero pierden sus identidades originales.

El conjunto de reglas para una transformación particular se expresa en un algoritmo. La transformación básica puede combinarse para formar una transformación compleja. En aplicaciones computacionales, la transformación encriptada de permutaciones reordena los bits de los datos. La transformación encriptada de substitución reemplaza un bit con otro o un byte con otro.

Cifrado de bloque

Un cifrado producido mediante la transformación simultánea de un grupo de bits del mensaje en un grupo de bits del cifrador se llama un cifrador de bloque. En general, los grupos son del mismo tamaño.

Cifrador producto

Combinando las transformaciones básicas de permutación y substitución producen un término complejo llamado cifrador producto. Si se aplican permutación y substitución a un bloque de datos, el cifrado resultante se llama un cifrador producto de bloque.

ALGORITMO ENCRIPTADOR DE DATOS

El algoritmo es diseñado para cifrar y descifrar bloques de datos que consisten en 64 bits bajo el control de una clave de 64 bits d. El descifrado debe ser acompañado usando la misma clave pero con la condición de direccionar la clave con los bits alterados, tal que el proceso de descifrado es lo contrario del proceso de cifrado.

Un bloque para ser cifrado está sujeto a una permutación inicial (ip), entonces el cálculo depende de una clave compleja, y finalmente de una permutación que es el inverso de una permutación inicial(IP^{-1}). La clave dependiente de la computación puede definirse en términos de una función f, llamada la función de cifrado y una función ks, llamada la clave del programa. Una descripción del cómputo se da al inicio, junto con los detalles de cómo se usa el algoritmo para el cifrado, enseguida, se describe el algoritmo para el descifrado, finalmente, una definición de la función de cifrado f es dada, en términos de la función primitiva, la cual es llamada la función de selección S_j, y la función de permutación P.

La anotación siguiente es conveniente: dado dos bloques (L Y R) de bits, L y R denotan los bloques consistentes de los bits de L seguidos de los bits de R. Debido a que la concatenación es asociativa, B1, B2,… B3, por ejemplo, denota el bloque que consiste de los bits de $B_{1,}$ seguido de los bits de B_2 … seguido delos bits de B_8.

CIFRADO

Un esquema de cifrado en computación se muestra en la tabla 1, con más detalle se puede consultar en las publicaciones fips 46 y 74.

Los 64 bits del bloque de entrada para que sea cifrado, está sujeto a la siguiente permutación llamada permutación inicial ip. Esto es, la entrada permutada tiene el bit 58 como el primer bit, el bit 50 como el segundo bit, y el bit 7 como el último bit.

El bloque de entrada permutado es la entrada de la clave compleja calculada, la salida de este cálculo, llamada la presalida, es seguida de la permutación IP^{-1}, la cual es la inversa de la permutación inicial; esto es, la salida del algoritmo tiene al bit 40 del bloque de presalida como el primer bit, el bit 8 es el segundo bit y así sucesivamente hasta el bit 25 del bloque de presalida como el último bit de la salida.

El cálculo que utiliza el bloque de entrada permutada como su salida produce el bloque de presalida, pero para un intercambio final de bloques, de las 16 iteraciones de un cálculo que se describirá en términos de la función de cifrado f, la cual opera en dos bloques (uno de 32 bits y uno de 48bits) y produce un bloque de 32 bits.

IP							
58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

Tabla 1 Permutación inicial IP.

Se permite que los 64 bits del bloque de entrada para una iteración conste de un bloque L de 32 bits, seguido de bloque R de 32 bits, el bloque de entrada es LR.

Si K es un bloque de 48 bits, y $L' = R$ e la clave de 64 bits, entonces la salida L'R', de una iteración con entrada LR, está dada por:

$$R' = L\{PC\}f(R, K) \qquad \text{(Eq.5. 1)}$$

Donde {PC} denota la adición bit a bit módulo 2.

La entrada de la primer iteración del cálculo es el bloque de entrada permutado. A cada iteración, un bloque K diferente de los bits de la clave, es elegido desde la clave de 64 bits designada por key. Se describen enseguida las iteraciones; si ks es una función

IP^{-1}							
40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

Tabla 2 Permutación IP^{-1}

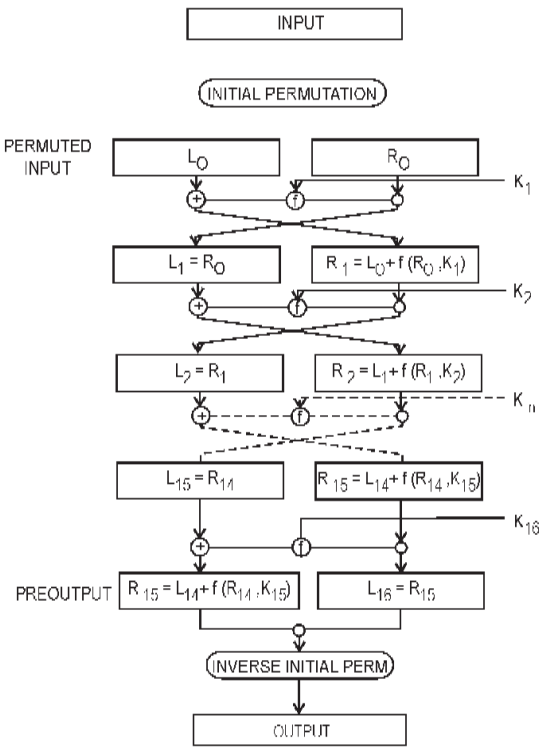


Fig. 5.1. - El cálculo del cifrado.

que toma un entero n, en el rango de 1 a 16 y un bloque key de 64 bits como entrada y produce como salida un bloque Kn de 48 bits, que es una selección permutada de bits desde key. De modo que:

$$K_n = KS(n, KEY) \qquad \text{(Eq5. 2)}$$

Con Kn determinado por los bits en 48 posiciones de bit distintos de KEY. KS es llamada la clave de programa porque el bloque K, usado en la iteración n-sima de la ecuación 5.1, es el bloque Kn determinado por la ecuación 5.2. Como antes, el bloque de entrada permutado es LR. Finalmente Lo y Ro, son respectivamente L y R, y Ln y Rn, son respectivamente L'y R' de la ecuación 5.1 cuando L y R son L_{N-1} Y R_{N-1}: esto es, cuando n está en el rango de 1 a 16;

$$L_n = R_{n-1}$$
$$R_n = L_{n-1}\{PC\}f(R_{n-1}, K_n) \qquad \text{(Eq. 5.3)}$$

El bloque del preoutput es entonces R_{16} L_{16}.
La clave del programa produce el 16Kn requerido para el algoritmo.

DESCIFRADO

La permutación IP^{-1} aplicada al bloque del preoutput es el inverso de la permutación inicial, ip, aplicado a la entra $R = L'$ 5.1) se sigue que:

$$L = R'\{PC\}f(L', K) \qquad \text{(Eq. 5. 4)}$$

Consecuentemente, para descifrar, es necesario aplicar el mismo algoritmo que para un bloque de mensaje cifrado. Tomando cuidado de que, a cada iteración del cálculo, el mismo bloque de bits de la clave K, es usado durante el descifrado como el cifrado del bloque, expresando por l $R_{n-1} = L_n$

$$L_{n-1} = R_n\{PC\}f(L_n, K_n) \qquad \text{(Eq. 5)}$$

Donde R_{16} I_{16} es el bloque de entrada permutado para el cálculo de descifrado y LoRo es el bloque de presalida, esto es, para el cálculo de descifrado, con R_{16} I_{16} como la entrada permutada, K_{16} es usada en la primer iteración, K_{15} en la segunda y así sucesivamente, con K_1 usado en la última iteración.

La funcion de cifrado f

Un bosquejo del cálculo de f(R.K) se da en la figura 5.2, donde E denota una función que toma un bloque de 32 bits como entrada y produce un bloque de 48 bits como salida, de tal modo que se pueden escribir como bloques de 6 bits cada uno, obteniéndose selectivamente los bits en la entrada ordenadamente, de acuerdo a lo siguiente:

Tabla de selección del bit E					
32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29

Así, l de R, mientras los últi

Cada -bits como entrada y p la tabla 4 contenien

Selección de la función S_1																
	Columna No.															
fila No.	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	0	0	6	13

Tabla 4, La función S_1

Si S_1 es la función definida en esta tabla 4, y B es un bloque de 6 bits, entonces $S_1(B)$ está determinado como sigue; el primer y último bit de B representan, en base 2, un número en el rango de 0-3. si ese número es i. La mitad de cuatro bits de B representa en base 2, un número en el rango de 0-15, y ese número es j. En la tabla observe el número en la fila i y en la columna j, es un número en el rango de 0-15 y es únicamente representado por un bloque de 4 bits. Ese bloque es la salida $S_1(B)$ de S_1 para la entrada B, por ejemplo, para la entrada 011101, la fila es 01(esto es, la fila 1) y la columna está determinada por 1101, la columna 13, luego en la fila 1, la columna 13 aparece como 5, tal que la salida es 0101.

La función de permutación P, produce una salida de 32 bits desde una entrada de 32 bits, permutando los bits del bloque de entrada, de modo que una función se define como sigue:

La salida P(L) para la función P, definida por la tabla 6, es obtenida desde la entrada

tomando el bit 16 de L como el primer bit de P(L), el bit 7 como el segundo bit de P(L), y así hasta el bit 25 de L, que es tomado como el bit 32 de P(L).

Si ahora $S_1,\ldots, S_8$ son ocho distintas funciones de selección, y P es la función de permutación, y E se define como antes, para definir f(R,K), primero se define $B_1 \ldots B_8$

Función de permutación P			
16	7	20	21
29	12	28	17
1	15	23	26
5	18	31	10
2	8	24	14
32	27	3	9
19	13	30	6
22	11	4	25

Tabla 5. Permutación P

hasta tener bloques de 6 bits cada uno, para lo cual:

$$B_1 B_2 \ldots B_8 = K\{PC\}E(R) \qquad \text{(Eq.5. 6)}$$

El bloque f (R,K) se define entonces como:

$$P[S_1(B_1)S_2(B_2 \ldots S_8(B_8)] \qquad \text{(Eq.5. 7)}$$

Así, K{PC} E{R} es primero dividido en los ocho bloques, como se indicó en la ecuación

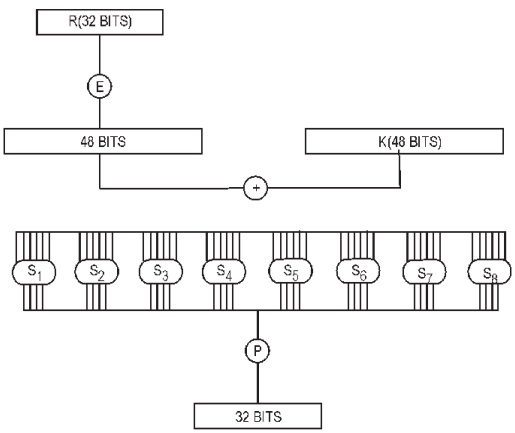


Figura 5.2 Calculation of F(R, K)

(5.6), entonces cada B_i se toma como una entrada a S_i y los ocho bloques $S_1(B_1)$,$S_2(B_2)$ … $S_8(B_8)$ de 4 bits cada uno es consolidado en un solo bloque de 32 bits los cuales forman la entrada de P. La ecuación de salida (5.7), es entonces la salida de la función f para las entradas R y K.

CARACTERÍSTICAS DEL ALGORITMO des

Las claves del des son vectores binarios de 64-bits que consisten de 56 bits de información independiente y 8 bits de paridad. Los bits de paridad están reservados rara detección de error y no son usados para el algoritmo de encripción. Los 56 bits de información son usados para la operación de cifrado y descifrado y se refiere a ellos como la clave activa. Las claves activas son generadas (seleccionadas al azar de todas las posibles claves) por cada grupo de usuarios autorizados de un sistema de computo particular o conjunto de datos.

En el cálculo de encripción, los 64 bits de entrada están divididos en dos partes, cada uno de 32 bits, una mitad es usada como entrada a una compleja función no-lineal, y el resultado es la operación or exclusiva con la otra mitad figura 5.3 después de cada iteración, o recorrido las dos mitades de los datos están intercambiadas y la operación es realizada otra vez. El algoritmo des usa 16 recorridos para producir un cifrado producto de bloque recirculado. El cifrado producido por el algoritmo despliega sin correlación a la entrada. Cada bit de la salida depende de cada bit de la entrada y de cada bit de la clave activa

La seguridad proporcionada por el algoritmo des está basada en el hecho de que si la clave es desconocida, un destinatario desautorizado de datos encriptados, conociendo algo de los datos de entrada, puede realizar una cantidad de intentos para descifrar otros datos encriptados o recobrar la clave, y aun teniéndola toda, si un bit de la clave no es correcto, el resultado es un dato inteligible. El único modo de conocer la clave con certeza es consiguiendo emparejar texto cifrado y texto sencillo y probar exhaustivamente las claves cifrando el texto sencillo conocido con cada clave y comparando el resultado con el texto cifrado conocido. Debido a que los 56 bits independientes son usados en una clave des, 2^{56} pruebas son requeridas para garantizar encontrar una clave particular.

El número de pruebas necesario para recobrar la clave correcta es 2^{55}, a un microsegundo por prueba, se requerirán 1 142 años. Bajo ciertas condiciones, los intentos esperados podrían reducirse a 571 años, y la posibilidad de 2^{56} claves, hace que adivinar o calcular cualquier clase de clave es muy improbable, siguiendo las recomendaciones para generar y proteger la clave. Por supuesto, se puede reducir el tiempo requerido para cualquier criptoalgoritmo teniendo varios dispositivos trabajando en paralelo, el tiempo se reduce pero el costo inicial se incrementa.

Una característica importante del algoritmo des es su flexibilidad para usarse en varias aplicaciones de proceso de datos. Cada bloque de cifrado es independiente de los otros, permitiendo encriptado o desencriptado de un simple bloque en un mensaje

o estructura de datos. El acceso aleatorio para encriptar datos por lo tanto es posible. El algoritmo puede ser utilizado en este modo sencillo para formar un bloque cifrado o alternativamente con encadenamientos, en los cuales la salida del algoritmo depende de previos resultados. La primer técnica es llamada el modo de libro de código electrónico ecb que ya se mencionó y la técnica encadenada tiene dos ejemplos llamados el modo de cifrado de bloque encadenado y el cifrado retroalimentado, en resumen, des puede ser utilizado en el modo de salida retroalimentada para generar un flujo seudoaleatorio de bits que es una operación or exclusiva para los bits del texto simple y formar un cifrador.

El algoritmo des es matemáticamente una proyección uno a uno de los 2^{64} posibles bloques de entrada sobre todos los 2^{64} posibles bloques de salida, debido a que hay 2^{64} posibles claves activas, hay 2^{64} posibles proyecciones, seleccionando una clave, se selec-

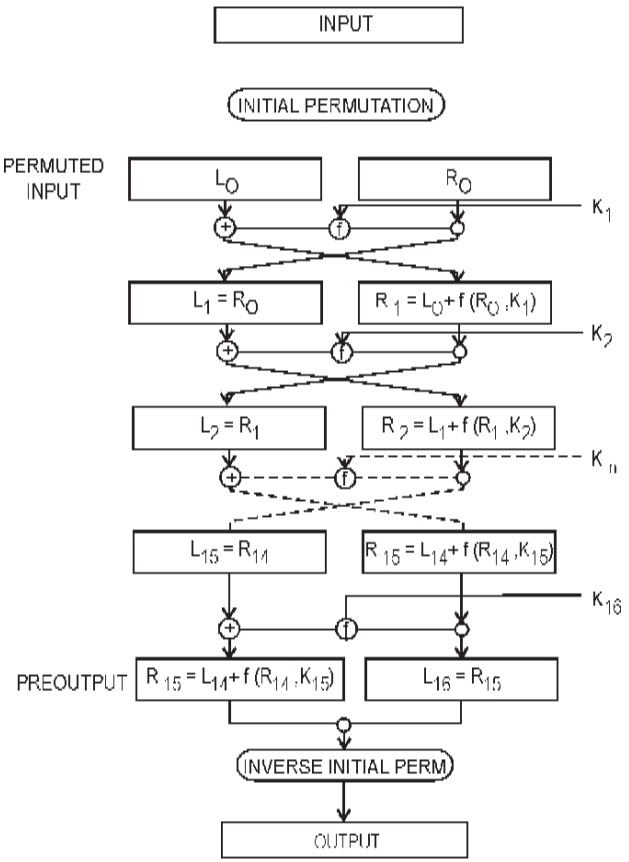


Fig. 5.3 Cálculo de cifrado en el libro de código electrónico.

ciona una de las proyecciones.

La entrada para el algoritmo es bajo la completa especificación del diseñador del sistema criptográfico y el usuario del sistema. Cualquier patrón de 64 bits es aceptable para el algoritmo, y el formato del bloque de datos puede ser definido por cada aplicación. En el ecb, los subcampos de cada bloque pueden ser definidos para incluir uno o más casos; un número de secuencia de bloque, el número de secuencia de bloque del último recibido del transmisor, códigos de detección-corrección de error, información de control información de dato y tiempo, información de autentificación del usuario o terminal, o un campo en el cual los datos aleatorios están colocados para asegurar que, los campos de datos idénticos en diferentes bloques de entrada resultará en diferentes bloques cifrados. Se recomienda que no más de 16 bits sean usados para conocer valores constantes, por ejemplo, el mismo valor de identificación de terminal de 32 bits no debe ser usado en cada bloque, si se desea que el bloque de datos en el modo de ecb despliegue una secuencia dependiente, una porción del último bloque enviado o recibido puede ser incorporado dentro del bloque, como un subcampo u operación or exclusiva en el bloque mismo.

El algoritmo des está compuesto de dos partes: la operación de cifrado y la de descifrado, los algoritmos son funcionalmente idénticos, excepto que la porción de la clave usada para las rutinas 1, 2,…, 16 durante la operación de encriptado son usadas en el orden 16, 15, …, 1 para la operación de desencriptado. El algoritmo utiliza dos registros de 28 bits llamados C y D para retener la clave activa de 56 bits. La clave de programa del algoritmo circula recorriendo los registros C y D independientemente, izquierdo para encriptado y derecho para desencriptado. Si los bits del registro C son todos ceros o unos (después de elegir la permutación 1 aplicada a la clave), y los bits del registro D son todos ceros o unos, entonces, el desencriptado es idéntico al encripitado. Esto ocurre para cuatro claves conocidas; 0101010101010101, FEFEFEFEFEFEFEFE, 1F1F1F1F0E0E0E0E y E0E0E0E0F1F1F1F1, (notar que los bits de paridad de la clave son conjuntos tales que cada byte tiene paridad impar). Es probable que en otros casos, los datos encriptados dos veces con la misma clave no resultará en texto simple, esta característica es benéfica en algunas aplicaciones de procesos de datos en que niveles críticos de cifrado pueden ser utilizados en una red, considerando que algunas de las claves usadas puedan ser las mismas.

Si un algoritmo es su inverso, entonces un número constante de encripciones bajo la misma clave resultará en texto simple. Hay ciertas claves, tal que para cada clave K, existe una clave K' para la cual el encriptado con K es idéntico al desencriptado con K', y viceversa, K y K' son llamadas claves duales. Las claves duales fueron encontradas examinando las ecuaciones que deben mantener dos claves para tener claves de programa contrarias. Las claves que tienen duales son aquellas que producen puros ceros o unos, o patrones alternados de ceros y unos en los registros C y D, después de que ha operado elección de permutación 1 sobre la clave, estas claves son las que se presentan en la tabla 6.

Las primeras seis claves tienen duales diferentes de sí mismas, cada una es a la vez una clave y un dual, dando 12 claves con el dual. Las últimas cuatro claves son iguales a sus duales y son llamadas las claves duales de sí mismas. Estas cuatro claves son las ante-

riormente tratadas, para las cuales la doble encripción es igual al no tener encripción, esto es el mapeo idéntico. El dual de una clave se forma dividiendo la clave en dos mitades de ocho caractere cada mitad entre dos caracteres, nc es.

Los datos pu rlos (antes de que se encripte y desi simple puede ser encriptado varias eces con la misma clave, resultando n ser encriptados sucesivamente pc las mismas claves para producir los o son mantenidas en el orden aprop exto simple con la clave 1 y luego de simple", entonces lo siguiente es cie

1. $E_1(D_1(P)) = P$
2. $E_1(E_1(P)) = P$ ...para..claves..duales.de.si..mismas
3. $D_1(D_1(E_1(E_1(P)))) = P$
4. $E_1(E_1(D_1(D_1(P)))) = P$
5. $D_1(D_2(E_2(E_1(P)))) = P$
6. $D_1(D_2(...(D_j(E_j...(E_2(E_1(P)...) = P$
7. $E_1(E_2(...(E_j(D_j...(D_2(D_1(P)...) = P$
8. $E_2(E_1(P)) = P$..para..claves.duales
9. $D_2(D_1(P)) = P$..para.claves.duales

Pero, en general, lo siguiente no es verdad:

$$1.D_2(D_1(E_2(E_1(P)))) = P$$

MODO DE LIBRO DE CÓDIGO ELECTRÓNICO

El modo más simple de funcionamiento, citado en oportunidades anteriores el libro del código electrónico (Electronic Code Book,) ecb, es el algoritmo de des especificado en fips, publicación 46. El modo de ecb se muestra en las figuras 5.1 a 5.3 en el modo de operación ecb, el algoritmo es independiente del tiempo y es llamado un sistema sin memoria. Dando el mismo dato y la misma clave, el resultado de cifrado siempre será el mismo. Esta característica debe ser considerada cuando se diseñe un sistema criptográfico usando el modo ecb. El bloque de salida O_t no es dependiente de cualquiera de las entradas previas $I_1, I_2, \ldots, I_{t-1}$. Es importante hacer notar que los 64 bits de O_t deben estar disponibles para obtener la entrada original I_t. Una recomendación para usar el des en este modo, es que todas las posibles entradas deben ser permitidas y usadas cada vez que sea posible. Debido a que la seguridad de los datos en este modo está basada en el número de entradas en el libro de código, este número debe ser maximizado cuando sea posible. En particular, este modo nunca debe ser usado para cifrar caracteres simples (es decir, cifrando caracteres ascii de 8 bits introduciéndolos en posiciones fijas de 8 bits y llenando los otros 56 bits con un número fijo). En este modo, 2^{64} entradas son posibles, y un subconjunto lo más grande como sea posible debe ser usado. Información aleatoria debe ser usada para rellenar pequeños bloques y desecharla cuando el bloque es descifrado.

Los datos deben ser introducidos en el registro de entrada, tal que el primer carácter de entrada aparece en la izquierda, el segundo carácter a la derecha de el, y el

Clave	Dual
1.B001E001F101F101	01B001B001F101F1
2.FE1FFE1FFE0EFB0E	1FFE1FFB0EF B0EFE
3.B01FB01FF10EF10E	1FE01FB00EF10E F1
4.01FB01F B01FE01FE	FB01FB01F B01FE01
5.011F01 1F010 B010E	1F011F01 0B010 B01
6.B0FEB0F EF1FEF1F E	FEE0FEB0F EF1FEF1
7.010101010101 01 01	010101 010101010101
8.F EFEFEFEFEF EFEFE	FEFEF EFEFEFEF EFE
9.B0B0E 0B0F1F 1F1F1	B0 B0B0 B0F1F1F1 F1
10.1F1F1F1F 0B0E0B0E	1F1 F1F1F0E0B0E0E

Tabla 6 Claves duales

último más a la derecha. Usando tecnología de registros de corrimiento, los caracteres deben ser introducidos sobre la derecha y correrlos a la izquierda, hasta que el registro esté completo. En forma similar, la salida del des debe ser tomado de izquierda a derecha cuando se ha transmitido los caracteres en modo serial, los caracteres deben salir desde la izquierda y el recorrido del registro debe realizarse hasta que esté vacío.

MODO DE CIFRADO DE BLOQUE ENCADENADO

El modo de cifrado de bloque encadenado es un método para usar el algoritmo des en el cual los bloques de cifrado son encadenados juntos; en la figura 5.5 se presenta como el modo Cipher Block Chaining (cbc) es usado para encriptar un mensaje. La entrada del des a un tiempo t es definido para que la or exclusiva (representada por pc) del dato al tiempo t y el cifrador al tiempo t-1. El cifrador al tiempo 0 es definido para que sea una cantidad llamada vector inicialización o IV. El modo cbc requiere bloques completos de 64 bits hasta que el bloque final es cifrado. El bloque de datos final de un mensaje puede no contener exactamente 64 bits cuando se procesa en el modo cbc, cuando esto ocurre, cualquier bloque terminal debe ser rellenado para tener 64 bits, o bien, el bloque terminal debe ser cifrado de modo que se tenga el mismo número de bits en la entrada. La primer técnica se llama relleno y la segunda truncado.

Cuando una secuencia de caracteres está siendo cifrada y el bloque terminal contiene menos que el máximo número de caracteres (ocho en el caso de caracteres de 8 bits), el relleno deber ser usado para formar el bloque de entrada final. Suponiendo que caracteres de relleno P son necesarios para llenar el bloque externo, si P es igual a 1, el carácter representando el número 1 debe ser colocado en la última posición del byte. Si P es más grande que 1, el carácter representando el número 1 debe ser colocado

en el último byte y los ceros deben ser colocados en la posición del byte remanente P-1 (figura 5.5).

En la mayoría de esquemas codificadores, los últimos tres bits del carácter representando un dígito son los mismos de la representación binaria del dígito. Es decir, la representación ascii del carácter 4 en hexadecimal es 34. Un bit cualquiera puede ser usado en el encabezado del bloque del mensaje empaquetado, que significa un mensaje rellenado (es decir, el bloque final del paquete está relleno) o algún otro método debe ser concebido.

El truncado puede ser usado en el modo cbc cuando el número de bits cifrados debe ser el mismo que el número de bits de entrada. Puede ser necesario que una cinta de cifrado contenga el mismo número de grabaciones y el mismo número de caracteres por grabación como la cinta de descifrado. Esto requiere que ocurra también, en algunos sistemas de conmutación de mensajes, en donde la longitud de grabación es fija, en estos casos, el método siguiente puede ser usado para cifrar el bloque terminal que no contiene 64 bits.

El bloque terminal corto es cifrado mediante el encriptado del bloque de cifrado previo en el modo ecb y la operación or exclusiva resultante hacia el bloque de datos terminal (figura 5.6). El receptor debe detectar el bloque cifrado corto y mantener la misma operación, ello es, encriptar el bloque cifrado completo previo y mantener operación or exclusiva para obtener el bloque de texto simple original. Si un bloque terminal corto contiene B bits, entonces los B bits más a la izquierda del bloque cifrado se utilizan. Esta técnica normalmente proporciona seguridad adecuada para el bloque final, pero debe notarse que, si los últimos B bits de texto simple son conocidos para una activa intercepción, el o ella puede alterar los últimos B bits de cifrado, tal que desencriptaran cualquier texto simple, ello es porque si sólo los últimos son alterados, el mismo valor estará en la operación or exclusiva para el bloque de cifrado corto en el desencriptado.

Uno o más bits erróneos dentro de un bloque cifrado simple, afectará el desencriptado de dos bloques (el bloque en que el error ocurre y el bloque sucesivo). Si los errores ocurren en el bloque de cifrado t, entonces cada bit del bloque de texto simple t tendrá una razón de error promedio del 50 %. El bloque de texto simple (t + 1) tendrá sólo aquellos bits erróneos que correspondan directamente a los bits erróneos cifrados, y el bloque de texto simple (t + 2) será correctamente desencriptado, además, el modo cbc sincroniza asimismo un bloque después el error.

MODO DE CIFRADO RETROALIMENTADO

El modo de operación de cifrado retroalimentado (cfb) mencionado oportunamente, puede ser usado en aplicaciones que requieren encadenamiento para prevenir substituciones o donde bloques de 64 bits no pueden ser usados eficientemente. La mayoría de datos de computadora son para ser transmitidos o almacenados, codificados en códigos de 6 a 8 bits. En algunos protocolos de comunicación, las unidades de datos son bits o carac-

teres más que bloques. El modo de cifrado retroalimentado utiliza el des que satisface un requerimiento para encriptar elementos de datos de longitud K, donde 1≤K≤64.

El modo cfb de operación se expone en la figura 5.7, la entrada para el algoritmo des no es el dato mismo, más bien, son los 64 bits previos de cifrado. El primer encriptado emplea un vector inicialización IV como su entrada I_0. En el modo cfb, ambos, transmisor y receptor de datos, utilizan solamente la operación de encriptado del des. La salida en el tiempo t es el bloque del bit 64 O_t, el cifrado al tiempo t es producido por la operación or exclusiva de los K bits del texto simple P_t, para los K bits más a la izquierda de O_t. Este cifrado C_t, es transmitido y también introducido en el lado derecho del registro de entrada, después de que la entrada previa es recorrida K bits posiciones a la izquierda. La nueva entrada es utilizada para el siguiente cifrado. Un IV de 64 bits es generado en el tiempo 0 y colocado dentro del registro de entrada. De ese tiempo, el cifrado del texto dependerá de su entrada inicial. Para llenar el registro de entrad del receptor, uno de dos eventos debe ocurrir:

1. El receptor independientemente debe generar el llenado inicial idéntico.

2. El transmisor debe transmitir suficientes datos para llenar el registro de entrada del receptor.

La explicación es que el transmisor genera un número seudoaleatorio (48-64 bits) y lo transmite como el IV. El transmisor y el receptor usa este número (con los bits de más alto orden de la entrada del des de 64 bits, rellenos con los bits "0" si es necesario) como el IV de 64 bits. Usando un número muy alto de bits proporciona alta seguridad, pero también resulta transmisión por encima del máximo. No es deseable que dos mensajes cifrados con la misma clave utilicen el mismo IV. El des puede ser usado como un generador de números seudoaleatorios para tener el IV. Los dispositivos de comunicación start/stop (asíncronos) transmiten el IV como caracteres con los bits start/stop apropiados adjuntos.

En el modo cfb, los errores dentro de una unidad de K-BIT de cifrado afectará el desencriptado del cifrado, y de los sucesivos, hasta que los bits de error hayan sido corridos fuera del bloque de entrada del des. La primer unidad K-BIT afectada de texto simple será incomprensible en exactamente aquellos lugares donde el cifrador tiene errores.

Los sucesivos desencriptados de texto simple tendrán una razón de error promedio del 50 % hasta que todos los errores hayan sido corridos fuera del bloque de entrada.

Suponiendo que no se encuentran errores adicionales durante este tiempo, se obtendrá el correcto texto simple, además, el modo cfb se autosincroniza. El modo cfb de operación también es útil para el encriptado de datos almacenados. Para máxima eficiencia se utilizan elementos de datos de 64 bits. Si el bloque de datos terminal no contiene un dato completo de 64 bits, los bits remanentes son rellenados antes del encriptado, asimismo, el bloque cifrado puede ser truncado, tal que sólo los bits de cifrado correspondientes a los bits sin relleno son usados, en este caso, el número de bits de cifrado será igual al número de bits de datos. Cuando se usa el modo de cfn de K-BIT, los últimos bits K del cifrador pueden ser alterados por un intruso que conoce los últimos bits K del texto simple. Esta es la misma amenaza que se tiene en el modo cbc con termi-

nal de bloque truncado. Si es una amenaza significativa, se recomienda que el final de los bits K del texto simple sea una función de los bits de texto simple previo, es decir, un chequeo de paridad o suma.

MODO DE SALIDA RETROALIMENTADA

El modo de salida retroalimentado (Output Feedback Mode ofb), como el modo cfb, opera

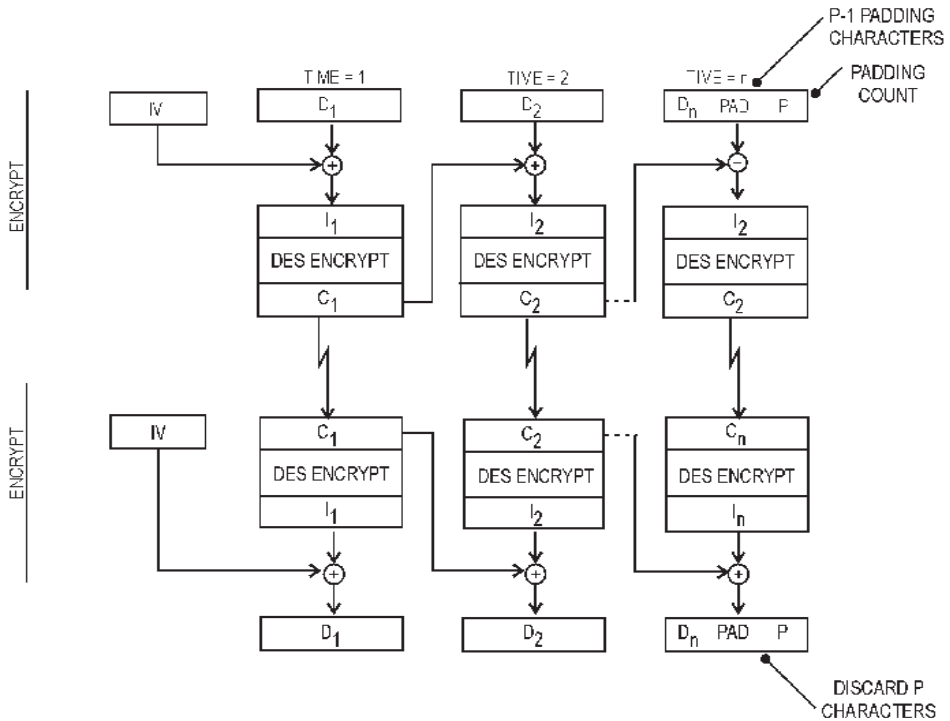
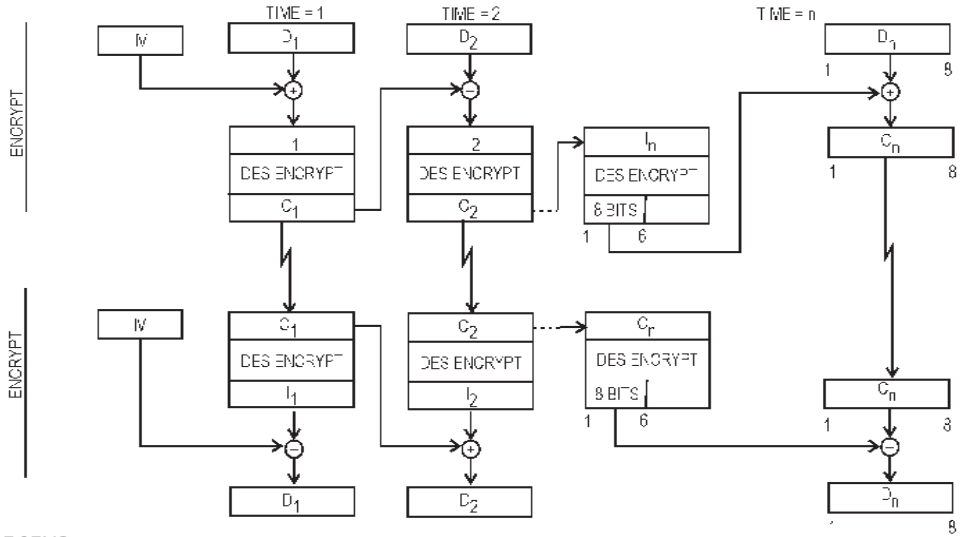


Figura 5.5. Cipher block chaining (cbc) mode, with terminal block

sobre unidades de datos de longitud K, donde K es un entero de 1 a 64, asimismo, el modo ofb no encadena el cifrado de una vez. Un bit de error en texto cifrado causa sólo un bit de error del texto simple desencriptado. Por otro lado, éste modo puede ser usado en aplicaciones donde se requiere propagación sin errores. La figura 5.8 ilustra el modo ofb.

La primera encripción utiliza un vector de inicialización como su entrada I_0, y ambos, el transmisor y receptor usan solamente la operación de encripción del des. El cifrado al tiempo t es producido por los K bits de la operación or exclusiva del texto simple hacia

los K bits más a la izquierda de la salida O_t. Los mismos K bits del bloque de salida del des son retroalimentados hacia el lado derecho del registro de entrada, después de que la entrada previa es recorrida K-BIT posiciones a la izquierda, y la nueva entrada es empleada para el siguiente cifrado. La salida del modo ofb es independiente del cifrado y el texto



LEGEND
D1=DATA VLOCK AT TIME
I1=ENCRYPTION INPUT BLOCK AT TIME
C1=CIPHER BLOCK AT TIME
IV=INITIALIZATION VECTOR
+=EXCLISIVE - OR

Figura 5.6. cipher block chainnig (cbc) mode, with terminal block truncation

simple. Asimismo, el modo ofb carece de la propiedad de autosincronización de los modos cbc y cfb. Si la sincronización se pierde, entonces un nuevo IV debe ser establecido entre el transmisor y receptor.

RELACIÓN DE CBC Y CFB DE 64 BITS

Como el cbc, el modo de operación cfb puede ser usado para encriptar bloques de 64 bits. En este caso, los 64 bits de O_t son operados en or exclusiva con los 64 bits de texto simple al mismo tiempo del encriptado. Esto es llamado el modo de operación cfb de 64 bits. Sea M1 una máquina cfb de 64 bits con clave de programa de $KR=(K_1, K_2, \ldots, K_{16})$, sobre cada uno de los 16 recorridos de encripción.

En el modo cfb el mismo programa es también usado para desencriptado. Sea M2

una máquina cbc con una clave de programa de KR=(K_{16}, K_{15}, …, K_1) para encriptado (es decir, la operación descifrado des). Si M1 encripta los bloques de 64 bits de texto simple P_1, P_2 y P_3 con vector de inicialización IV para formar el cifrado C_1, C_2 y C_3, entonces M2 encriptará P_3, P_2, y P_1 con vector de inicialización C_3 para formar el cifrado C_2, C_1, IV, de

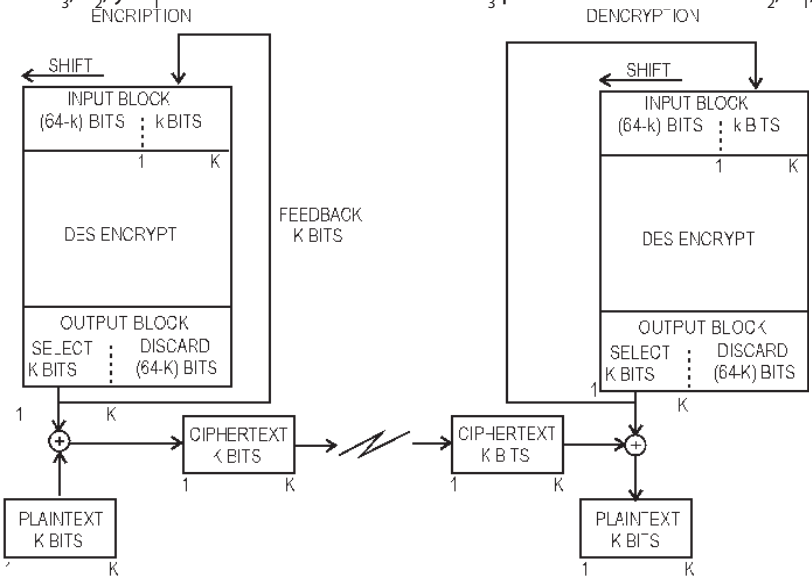


Figura 5.7. K-bit cipher feedback (cfe) mode

forma similar, mientras M1 desencripta C_1, C_2 y C_3 (usando vector de inicialización IV) para P_3, P_2, y P_1, M2 desencriptará C_2, C_1, y IV (usando vector de inicialización C_3) para P_3, P_2, y P_1, además lo contrario de (IV, C_1, C_2, C_3) para (C_3, C_2, C_1 ,IV) puede formar el cifrado desencriptado por M1 con M2.

Para ver si las afirmaciones anteriores son ciertas, sea E(S)(X) representando el encriptado de X en el modo ecb usando la clave de programa S, y sea D(S)(X) el desencriptado ECB de X bajo el programa S. Notar que S es la clave de programa y no clave misma. En desencriptado usar la cl $P_1 \oplus E[KS](IV) = P_1 \oplus O_1 = C_1$ rso de encriptado, además E(KS)(X)= D(KR)(X). El encrip $P_2 \oplus E[KS](C_1) = P_2 \oplus O_2 = C_2$ o IV, puede ser descrito por tres ecuaciones:

$$P_3 \oplus E[KS](C_2) = P_3 \oplus O_3 = C_3$$

O_1, O_2 y O_3 representan el encriptado ecb, con la clave de programa ks, de entradas IV, C_1, y C_2 respectivamente. El símbolo matemático (P⊕C) es un operador or exclusivo de 64 bits. El encriptado de P_3, P_2, y P_1 por M1, usa C_3 como el vector de inicialización, puede ser descrito también por tres ecuaciones:

$$E[KR](P_3 \oplus C_3) = E[KR](O_3) = D[KS](O_3) = C_2$$
$$E[KR](P_2 \oplus C_2) = E[KR](O_2) = D[KS](O_2) = C_1$$
$$E[KR](P_1 \oplus C_1) = E[KR](O_1) = D[KS](O_1) = IV$$

Invirtiendo la clave de programa, las entradas, y las salidas, se obtienen máquinas equivalentes. Ecuaciones similares pueden ser derivadas para desencripción, y las relaciones se mantienen para un flujo de longitud arbitraria de bloques de texto simple de 64 bits.

CONDICIONES DE SECRETO PERFECTO

Shannon definió sus condiciones de secreto perfecto partiendo de dos hipótesis básicas:

1. La clave secreta se utilizará solamente una vez, a diferencia de lo que sucedía en los métodos clásicos, en los que la clave era fija.

2. El enemigo criptoanalista tiene acceso sólo al criptograma; luego está limitado a un ataque sobre texto cifrado únicamente.

Basadas en estas dos hipótesis, Shannon enunció sus condiciones de secreto perfecto que pueden, sintetizarse tal y como sigue.

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

$$P(X = x / Y = y) = P(X = x)$$

Para todos los posibles textos fuente $x = (x_1, x_2 \ldots, x_M)$ y todos los posibles criptogramas $y = (y_1, y_2, \ldots y_M)$; es decir, la probabilidad de que la variable aleatoria X tome el valor x es la misma con o sin conocimiento del valor tomado por la variable aleatoria Y. En términos más sencillos, esto equivale a decir que la información sobre el texto claro aportada por el criptograma es nula. Por lo tanto, el enemigo criptoanalista no puede hacer una mejor estimación de X con conocimiento de Y, que la que haría sin su conocimiento, independientemente del tiempo y recursos computacionales de los que dispongan para el procesado del criptograma.

Asimismo, y basado en el concepto de entropía, Shannon determinó la menor cantidad de clave necesaria para que pudieran verificarse las condiciones de secreto perfecto. En efecto, la longitud de la clave K tiene que ser, al menos, tan larga como la longitud del texto claro M:

$$K \geq M$$

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

Una vez establecidas las condiciones de secreto perfecto, cabe preguntarse si existen cifradores perfectos. La respuesta es afirmativa. Tal y como se verá a continuación.

Se considera un método de cifrado en el que el texto claro, criptograma y clave tomen valores en un alfabeto L-ario {0,1,...,L-1} y en el que la longitud de la calve K, criptograma N y texto claro M coincidan entre si K = N =M. En este caso, el número de posibles textos simples, criptogramas y claves son iguales entre sí e iguales a L, se supone que:

a) La calve se elige de forma completamente aleatoria, es decir;

$$P(Z = z) = L^{-M} \qquad (6)$$

para todos los L^M posibles valores z de la clave secreta.

b) La transformación de cifrado es

$$Y_i = X_i \oplus Z_i, i = 1, \ldots M \qquad (7)$$

Donde $\oplus$ denota la adición módulo L, elemento a elemento.

Fijado un texto fuente X = x, a cada posible valor de la clave $Z = z_j$, (j=l, …, L^M), le corresponde unívocamente un criptograma $Y=y_j$, (j = 1, ..., L^M). Entonces, de acuerdo con la condición a), es fácil ver que a un mismo texto claro X = x le puede corresponder con igual posibilidad cualquiera de los L posibles criptogramas; luego

$$P(Y = y) = P(Y = y \mid X = x) = L^{-M} \qquad (8)$$

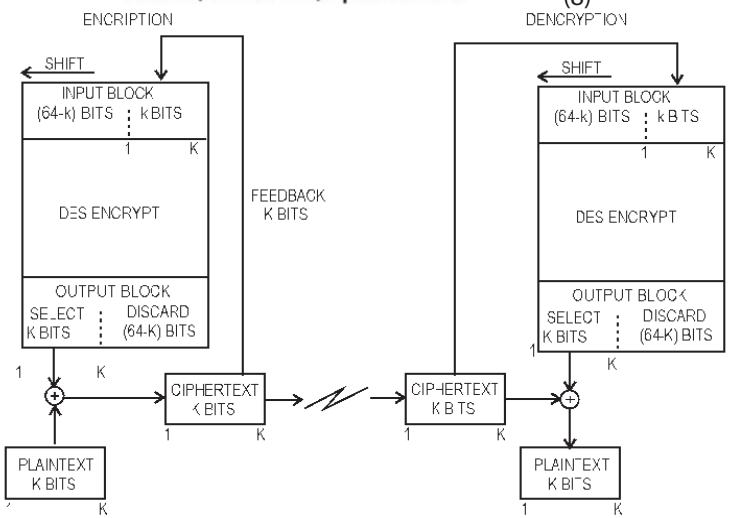


Figura 5.8 Modo OFB

Por ello, la información aportada por el criptograma sobre el texto claro es nula, X e Y son estadísticamente independientes y la transformación modulo L verifica las condiciones de secreto perfecto. Cuando L= 2, se tiene simplemente el cifrado Verman.

Hay que resaltar que este tipo de cifrado módulo L, ofrece una total seguridad respecto a la estadística del texto claro, lo cual es una cualidad muy deseable, puesto que sería extraordinariamente peligroso que la seguridad de un método de cifrado dependiera de la naturaleza estadística del lenguaje utilizado en el mensaje a cifrar.

A la luz de las condiciones de secreto perfecto de Shannon, podemos evaluar los métodos criptográficos referenciados anteriormente.

Cifrado de César: utiliza una clave, es fija y se emplea continuamente para cada nueva letra del mensaje a cifrar. Claramente, este procedimiento no verifica las condiciones de Shannon, por lo que la operación módulo 21 deja al descubierto en el criptograma la frecuencia de aparición de las letras del texto fuente.

Cifrado de Vigenere: utiliza una clave más larga que el método anterior, pero, en cualquier caso, más corta que la longitud del mensaje. La clave no es una secuencia aleatoria, sino una palabra del lenguaje, sometida a sus reglas y características, que se reutiliza sucesivas veces. De acuerdo con las condiciones de Shannon, no se trata de un método de cifrado perfecto, por lo que, aunque sea con mayor dificultad que el cifrado previo, el criptoanalista termina por encontrar alguna artimaña (método Kasiski) que le permite determinar la estadística del texto claro, a partir del criptograma y, posteriormente, romper el criptosistema.

Cifrado Vernam: utiliza una clave de longitud igual a la del texto claro siendo ésta una secuencia perfectamente aleatoria que, además, se emplea solamente una vez. Verifica pues, las condiciones de secreto perfecto de Shannon. En este caso, la suma módulo 2 con una secuencia aleatoria ofrece un perfecto enmascaramiento del contenido y estadística del texto claro. Dentro del panorama criptográfico actual, el cifrado Vernam es el único procedimiento incondicionalmente seguro o procedimiento con seguridad probada matemáticamente.

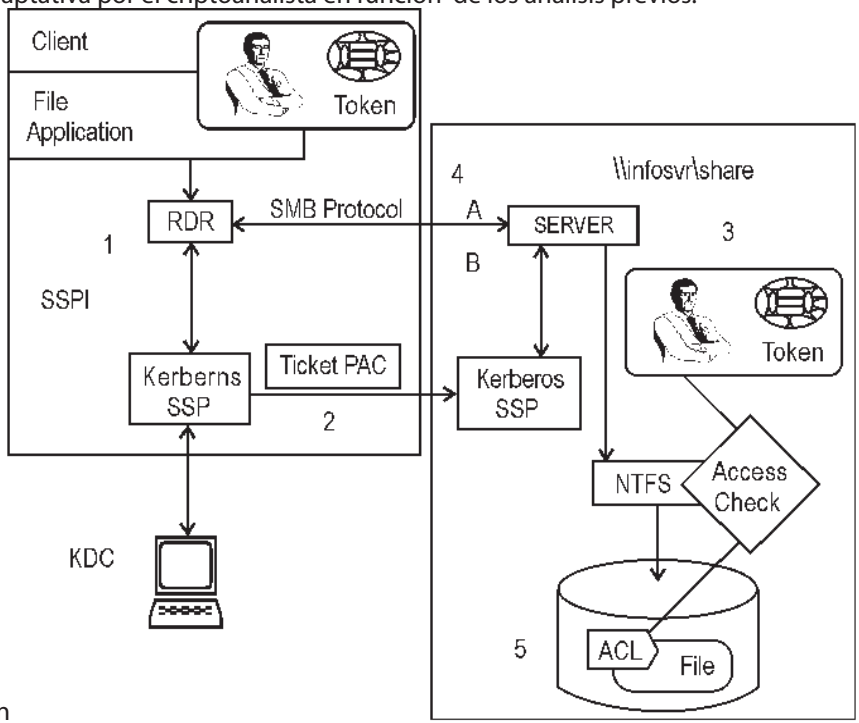
Un criptosistema se puede atacar de muchas formas; la más directa sería la que hace uso únicamente del análisis del mensaje cifrado o criptograma. Se trata de un análisis pasivo. Pero en la realidad se pueden producir más ataques, apoyados en cierto conocimiento adicional o bien cierto grado de intervención, en cuyo caso estaremos frente a un ataque activo.

Los posibles ataques, citados de mayor a menor dificultad, serían:

1. Sólo se conoce el criptograma.
2. Sólo se conoce el criptograma, pero éste va salpicado con partes en claro sin cifrar.
3. Se conocen varios criptogramas diferentes correspondientes al mismo texto claro cifrados con claves diferentes.
4. Se conocen el criptograma y el texto claro correspondiente. Incluye el caso de que

no se conozca enteramente el texto claro.

5. Se conoce el texto descifrado correspondiente a un criptograma elegido por el criptoanalista.
6. Se conoce el criptograma correspondiente a un texto claro escogido por el criptoanalista.
7. Se conoce el texto descifrado correspondiente a un criptograma elegido de forma adaptativa por el criptoanalista.
8. Se conoce el criptograma correspondiente a un texto claro escogido de forma adaptativa por el criptoanalista en función de los análisis previos.



9Secon

oce la clave o al menos se puede limitar el espacio de claves posibles.

Todos estos caos pueden estar modulados por el hecho de que se conozca o no el criptosistema en uso.

SEGURIDAD INFORMATICA

A continuación, se da una serie de reglas ideales de funcionamiento para la administración de una red de equipos de datos dotada de criptografía que deben seguirse dentro de lo posible:

1. Seguridad física:

Habrá un control permanente para seguridad física del sistema informativo que

impida manipulaciones y sabotajes. Se prestará atención a las visitas de servicio técnico: los técnicos ajenos estarán bajo observación permanente de un técnico propio y de un oficial de seguridad. Se controlará cuidadosamente las piezas nuevas que se instalen, las viejas defectuosas se destruirán en el acto y no serán entregadas a los técnicos ajenos. Se plantea un problema importante con los registros magnéticos averiados: aunque no se puede escribir, ni leer, ni borrar información de ellos mientras permanezca la avería, una vez reparados pueden ser perfectamente accesibles al reparador.

2. Duplicación de información:

Al final de cada jornada de trabajo, se duplicará toda la información residente en la memoria del sistema (back up) en cintas magnéticas removibles, que se guardarán en la caja fuerte de un archivo seguro, con las características anteriormente descritas. Antes de borrar un juego de cintas se habrá grabado el juego siguiente con información posterior.

3. Separación de cometidos:

Serán personas diferentes las encargadas de la gestión de claves, de la programación y del uso del sistema.

4. Puestos de confianza compartidos:

Las tareas que exijan la mayor confianza serán responsabilidad compartida de varias personas. Cada una realizará una parte de la tarea. El conocimiento del sistema monopolizado por una de las personas será insuficiente para violar la seguridad de éste.

5. Acceso restringido

Cada usuario sólo tendrá acceso a los archivos de la base de datos que le competan. Los programadores tendrán acceso a las bases de datos. Los usuarios no tendrán acceso a las libretas de programas, los gestores de claves solo tendrán acceso a la instalación de éstas.

6. Control de presencia permanente del usuario:

Cada terminal accederá al sistema sólo si el usuario se ha identificado plenamente mediante la tarjeta y un Personal Identification Number pin. La tarjeta deberá permanecer introducida en el terminal mientras dure la sesión de trabajo. Para evitar que la tarjeta se abandone en el terminal, sería recomendable que se desempeñase, además, la función de tarjeta de identificación de solapa, con fotografía.

7. Los terminales no dispondrán de memoria permanente:

No será posible para el usuario ni para el programador almacenar información de forma permanente en su terminal, ya sea en medios fijos o móviles,. Por lo tanto, los terminales no dispondrán de discos duros o flexibles, casetes o cintas magnéticas, cintas de papel ni ningún otro medio de almacenamiento masivo de información.

8. Se prefieren terminales no inteligentes:

Los terminales con capacidad de proceso de información autónomas son peligrosos, porque se pueden usar como arma de asalto al sistema. Los PC son especialmente peligrosos, pero si se estimase indispensable su uso, debe cumplirse el apartado anterior.

9. Trabajo en la entidad:

Se prohibirá formalmente llevarse trabajos a casa, así como sacar listados de programas o datos del local de trabajo.

10. Asignación de memoria virtual:

El sistema operativo no permitirá el acceso a un área de memoria real en la que puede haber restos de datos, sólo se asignarán áreas de memoria virtual

11. Inspección de programas

Todos los programas nuevos deben ser inspeccionados cuidadosamente por un programador diferente del autor en busca de caballos de Troya. Puertas falsas y gusanos.

12. Criptografía

Se protegerá criptográficamente todo el sistema informático:

- Los archivos se almacenarán cifrados.
- Las comunicaciones se realizarán cifradas bajo la clave de sesión.
- El acceso de los usuarios se controlará mediante tarjeta + pin.
- Los pin se almacenan cifrados

13. Claves jerarquizadas:

Existirá una jerarquía piramidal de claves que permita compartir las diferentes operaciones criptográficas y evitar el descubrimiento de una clave que comprometa la seguridad del sistema.

14. Claves secretas:

No se almacenará ninguna clave en claro fuera del módulo de seguridad. Las claves se generarán de manera aleatoria. Habrá un local seguro para generación e instalación de claves. En este local se guardará un duplicado de las claves maestras, primarias y secundarias. La clave maestra estará en claro; el resto, cifradas. La clave maestra sólo será accesible ante la presencia conjunta de las personas que compartan la responsabilidad de su custodia.

15. Distribución segura de claves:

La seguridad del sistema de distribución de claves poseerá, al menos, el mismo grado de seguridad que la transmisión de información.

16. Gestión automática de claves:

La gestión de claves será totalmente automática. El usuario no participará en absoluto en su uso.

17. Transparencia del sistema criptográfico:

Una vez que el usuario ha insertado su tarjeta de identificación y tecleado su pin de forma satisfactoria, no se verá involucrado en ninguna operación criptográfica más. Toda la información a la que tenga acceso legal le será presentada automáticamente en versión descifrada.

18. Doble seguridad de acceso a la información:

Si por casualidad, el sistema operativo fallase y proporcionara ilegalmente acceso a un usuario a un archivo no autorizado, la información le llegará de forma cifrada.

19. Seguridad de la información:

La totalidad de la información se guardará y se transmitirá cifrada.

20. Seguridad con independencia del terminal:

Se garantizará la seguridad a nivel del sistema operativo y criptográfico con independencia del tipo de terminal o periférico que se utilice: teclado, pantalla, impresora, plotter, ratón, tableta grafica, etcétera.

21. Información al usuario:

Todos los usuarios deberán estar informados necesariamente de que se encuentran operando en un sistema dotado con protección criptográfica.

22. Vida útil de los equipos:

La vida útil de los equipos de criptografía será mayor que la vida de los terminales a proteger.

EDI

La necesidad de intercambiar información es crítica dentro de la comunidad de negocios, la información puede ser genérica por naturaleza, tal como una orden de compra, factura, o específica a una organización, tales como una relación de clientes. Tradicionalmente las empresas han intercambiado esta información a través de formatos preestablecidos por correo. Por la integración de las computadoras y las comunicaciones de datos dentro de los negocios, las compañías pueden cosechar los beneficios de intercambiar información electrónicamente, reduciendo papeles de trabajo, minimizando costos y mejorando el tiempo de repuesta. Este proceso de intercambio de información estandarizada de negocios de computadora a computadora es llamado edi (intercambio electrónico de datos).

Los negocios tienen tres opciones para implementar un sistema edi:

1. Las compañías y los negocios pueden desarrollar su propio software de edi, esta opción es costosa, consume mucho tiempo, y debido al riesgo que involucra el desarrollo de nuevo software, es desechada, excepto en casos extremos, por ejemplo tener una plataforma de hardware para la cual no hay software de edi comercial disponible.

2. Los negocios pueden utilizar los servicios de un edi con una red compartida, con esta opción una empresa envía sus transacciones de negocios al service bureau, que es el buró de servicios de algún sistema de edi, el cual desarrolla su servicio edi en su propio site. Los honorarios por esta clase de servicios son generalmente altos. Los negocios pueden adquirir su producto edi ya desarrollado, esta alternativa es la más efectiva en cuestión de tiempo y costo para la implementación de algún sistema edi.

Elementos para la implementación de edi

1. Establecer las necesidades para la implementación de edi. Para muchas organizaciones edi será requerido para mantenerse competitivo.

2. Establecer un comité de planeación que sea encabezado por una persona interesada y con conocimientos de edi. El comité deberá incluir representantes de todos los departamentos a ser afectados por este sistema.

3. Desarrollar una auditoría de edi dirigida a procedimientos existentes, disponibilidad de recursos de información de sistemas y procedimientos de comercio y de socios de negocios, disponibilidad de software que pudiera ser examinado.

4. Presentar un plan de acción a los altos niveles de la empresa dirigido a la necesidad de contar con edi, beneficios por anticipado, costos y una agenda de implementación.

5. Una vez que ha sido obtenido el apoyo, decidir el tipo de sistema, esto incluye estándares a ser usados, configuración del sistema y que proveedor externo de red se empleará. En suma, las transacciones, los departamentos, los proveedores a ser utilizados deberán ser colocados en el sistema, debiendo decidirse en ese momento. Se debe realizar una revisión de los procedimientos internos de las áreas afectadas para contar con un conocimiento más amplio del tipo de operaciones y sus repercusiones que tienen al realizar cada una de ellas.

6. Dirigir a través de la capacitación el potencial de los usuarios y socios de negocios, este debería ser un proceso en marcha y comenzar tan pronto sea posible. La capitación es un factor muy importante en reducir la resistencia a implementar edi.

PROYECTO BOLERO

Uno de los retos que afrontan los participantes en el tema de comercio exterior, es el de identificar cómo resolver las exigencias que nos imponen la velocidad con que se quieren atender los cambiantes procesos de negociación y contratación, despacho y recibo de mercancías; y, lo más importante, para los bancos desde el punto de vista de servicios bancarios, cómo crear el ambiente favorable para entender a clientes que, hoy en día demandan una mayor eficiencia a un menor costo.

En el mundo, actualmente, son de papel la mayor parte de los billones de documentos que constituyen el soporte del intercambio comercial. El costo de administrar este ineficiente intercambio de documentos, ha sido estimado por las Naciones Unidas en 7% del valor del comercio mundial, lo que representa más de 400 billones de dólares por año. Los sistemas con base en papel son vulnerables al fraude y no llenan las expectativas crecientes de importadores y exportadores para suprimir las demoras en procesos de justo a tiempo.

Por esta razón, la sociedad cooperativa de bancos internacionales, Society for Woldwide Interbank Financial Telecomunication (swift) y el Through Transport Club TTClub, han desarrollado el proyecto Bolero (Bill of Landing Europe: conocimiento de embarque Europa).

El proyecto Bolero consiste en desarrolar una plataforma de servicios que atienda de manera segura, a toda la industria, con la transferencia electrónica de información comercial mundial. En 1996, inició negociaciones con la asociación Bolero, El TTClub, que representa a transportistas, despachadores de carga y autoridades portuarias, y la swift. El TTClub y la swift han hecho un significativo progreso en llevar a cabo sus planes de conformar una compañía de riesgo compartido, Joint venture, que logre mercadear el concepto Bolero.

La Bolero Association Ltd. (bal) representa a todos los sectores industriales y empresariales que son potenciales usuarios del sistema Bolero.

La BAL es una organización con administración autónoma. Su papel consiste en dar apoyo al Joint venture (val), TTClub y la swift. Al final de los años sesenta, 239 bancos de diferentes países (Austria, Bélgica, Canadá, Dinamarca, República Federal Alemana, Finlandia, Francia, Italia, Holanda, Noruega, Suecia, Reino Unido y Estados Unidos) eran lo que se conoce como swift.

SISTEMA SWIFT

La swift es una asociación interbancaria que crea un sistema en donde se logran satisfacer las necesidades de las instituciones financieras a nivel mundial, se pueden interconectar varios nodos o puntos mundiales y además comunicarse entre ellos para transferirse información financiera, tal como: operaciones de pago (transferencias monetarias), cartas de crédito, acuerdos financieros (crédito) entre empresas y la institución bancaria para lograr la compra, importación o exportación de algún producto, incluye también el manejo de inversiones entre las mismas instituciones financieras a nivel mundial. Asimismo por este sistema se informa sobre el ingreso de un nuevo banco o el cambio del mismo o, en su defecto, su desaparición en el mercado financiero. Este sistema resulta muy efectivo entre el mercado financiero de Europa y Estados Unidos que implementaron 3 centros de comunicación entre los dos continentes. Uno de ellos localizado en Virginia, Estados Unidos, el cual se dedica al chequeo de las comunicaciones del continente americano y los otros dos centros están localizados en Bélgica y Holanda. Siendo el de Bélgica el centro de operaciones de todo el sistema.

Además swift proveé de:

1. Conectividad global.
2. Estandarización de mensajes.
3. Servicios de mensajería electrónica.
4. Transferencia de información.
5. Servicios de información operacional.
6. Acuerdos de niveles de servicios.
7. Interfaces.
8. Entrenamiento a usuario.
9. Estructura que permite acuerdos con proveedores de aplicaciones.

CONEXIÓN DEL SISTEMA swift

Tanto la comunicación y la conexión del sistema swift se realiza por medio del sap (punto de acceso al swift) que será cualquier entidad o institución financiera que se conecte a la red swift con el scc (centro del control de sistema), que da el soporte al continente

americano se encuentra ubicado en el estado de Virginia, Estados Unidos.

La comunicación entre un sap y el sistema swift se realiza mediante la ejecución del comando login, que es la petición de una sesión, de acceso lógico en el sistema y se divide en dos partes:

gpa: aplicación para un propósito general, de acceso a varias funciones del sistema. Su función principal es la petición de un número de sesión para completar el ciclo de conexión al sistema, cada sesión siempre será identificada por cuatro dígitos numéricos y que serán diferentes cada vez que realice una petición de conexión; también la gpa recibe ciertos mensajes, que son informativos tanto del sistema como de algunos cambios realizados por bancos.

A) Itc: control de la terminal lógica donde se ejecuta el comando login y se establece la comunicación entre la institución y swift.

B) apc: control de aplicación que realiza el acceso a los mensajes informativos de reportes o peticiones y ejecuta la selección de control sobre una aplicación específica, mediante el comando select.

C) fin: aplicación fin, esta aplicación se obtiene después de ejecutar el select y se obtiene un número de sesión, que también se define por cuatro dígitos numéricos y que son diferentes cada vez que realiza el select. Esta aplicación prové a los usuarios el uso de los mensajes financieros para recibir o transmitir mensajes.

Al realizar el acceso al gpa y al fin se completa el ciclo de conexión al sistema, tanto los dígitos del apc y del fin operan simultáneamente, si falta alguno de los dos no puede realizarse la comunicación, asimismo al controlar la apertura o cierre de una sesión se controla el acceso y la salida de los mensajes.

Para realizar la desconexión del sistema se realiza un quit (abandonar) en la sesión fin, y posteriormente un logout en la sesión apc donde se completa el cierre de las sesiones y la desconexión de swift.

Para poder realizar la ejecución de login y select es necesario el uso del scr, que es un lector de tarjetas de seguridad. La función de este lector es la integración al sistema de números o claves que están contenidos en tarjeta, las que son enviadas por swift al administrador del sistema de cada institución.

Estas tarjetas pueden ser usadas una sola vez, son responsabilidad del administrador del sistema tenerlas en un lugar seguro, si se extravían, se tiene que reportar al centro de soporte swift para cancelar la funcionalidad de las mismas. La información que contienen las tarjetas hace posible la ejecución de login y la obtención de un número de sesión.

Durante la ejecución del login se obtiene un timeout de un máximo de 90 segundos, si en este transcurso no se da la asignación del número de sesión, se cancelará y se tendrá que realizar la petición mediante el login. Si no se llegaran a tener estas tarjetas y el lector, no es posible conectarse a swift.

Las posibles conexiones por acceso físico, pueden ser distintas, como sería el caso de una conexión dedicada o por la red pública de datos.

KERBEROS: ARQUITECTURA DE SEGURIDAD

Actualmente, las redes de computadoras necesitan una arquitectura diseñada para dar seguridad a las operaciones que en ella se realizan, desde suministrar claves, autorizar o identificar a una persona, o el tipo de aplicación que requiera el equipo, por ejemplo: en operaciones de autenticación, además de ser una operación transparente al usuario, éste se limitará a escribir su password o pin. Todo esto conduce al propósito de utilizar una arquitectura distribuida como la que se analiza a continuación.

Esta arquitectura desarrollada por el Instituto Tecnológico de Massachussets, es un servicio de autenticación con arquitectura cliente/servidor y a continuación se dan algunos conceptos de la versión 5, utilizando el algoritmo de cifrado simétrico (des).

Microsoft Kerberos es un protocolo de la autenticación. Los servidores y servicios de la red necesitan saber que el cliente que pide acceso es un cliente válido y que sus credenciales son correctas. Kerberos proporciona pruebas de que la identidad del cliente no ha sido corrompida.

- Basado en que las credenciales del cliente contiene boletos encriptados con claves compartidas (encriptado simétrico). El cliente tiene una clave basada en la contraseña (password) del usuario guardada en todos los controladores de dominio. De forma semejante, cada servidor tiene una clave en todos los controladores de dominio, debido a que cada clave es única, y sólo el cliente y el controlador de domino tienen copias de la clave del cliente, la habilidad de lograr desencriptar el mensaje proporciona identificación segura. Lo mismo sucede para claves compartidas en servidores de aplicaciones, de impresión, de archivos y los controladores de dominio.
- Las bases para los dominios de confianza transitivos (Kerberos Trusts). Es decir, cuando dos dominios están unidos, una clave entre campos es creada, estos dominios pueden confiar uno en el otro, porque ambas claves tienen su clave de programa.
- Basado en el rfc 1510 y versiones revisadas. Kerberos es un estándar abierto maduro, ampliamente usado, que proporciona interoperabilidad con otras aplicaciones, tal como mit Kerberos versión 5.
- Más eficaz que ntlm. Las confianzas transitivas reemplazan confianzas complicadas "all-way". Los boletos de la sesión renovables reemplazan la autenticación pass-trough.
- La arquitectura de Kerberos extensible. Permite especificar los métodos de seguridad adicionales o alternados. También la clave secreta compartida puede ser suministrada con claves privadas/públicas para el uso de tarjetas inteligentes.

Meta primaria: Identidad del usuario autentificada

Cuando un cliente quiere tener acceso a un servidor, éste necesita verificar la identidad del cliente. El cliente afirma ser por ejemplo: alguien@Microsoft.com. Desde el acceso a los recursos, se basará en los permisos de identidad y asociación. El servidor debe estar seguro de que el cliente es quien afirma ser.

El usuario entrega credenciales seguras en ticket

Windows 2000 crea identificadores únicos (sids) que representan usuarios, grupos,

etcétera. Kerberos también entrega el sid del cliente y el sid de cualquier grupo. El propósito, es que en cualquier paquete de autentificación usado en Windows 2000, se proporcione el sid apropiado al servidor, de modo que se crea la señal de acceso al usuario.

Identidad del usuario empaquetado en un ticket

Kerberos empaqueta los nombres de usuario (User Principal Name, UPN. alguien@microsoft.com) y el sid del usuario en una estructura de datos llamada "ticket". Las metas de Kerberos son modificar la creación y distribución de seguridad de tickets. Un grupo de usuarios con información asociada en un ticket de Kerberos se llama Privilege Attribute Certificate (pac). El pac no debe ser confundido con una clave pública. Kerberos autentifica la identidad del usuario, pero no autoriza el acceso, sólo se verifica la identidad del cliente, y una vez que esto se ha hecho, el Local Security Autthority autorizará o denegará el acceso a los recursos.

Privacidad a través de encriptado. Los mensajes de Kerberos son encriptados con una variedad de claves encriptadas, para asegurar que nadie pueda falsificarlos con los tickets del cliente o con otros datos en un mensaje de Kerberos. Esto no significa que cada elemento es encriptado, en efecto, algunos campos de datos son enviados en texto limpio, porque las claves de encriptado todavía no han sido cambiadas, tal que los datos puedan ser irreconocibles, o porque la posesión de los datos no posee una amenaza.

El ticket del cliente, por ejemplo, es encriptado con una clave conocida sólo por el servidor destino y el Kerberos Key Distributio Center (kdc). EL kdc también crea términos cortos y sesiones simples, usadas para encriptar mensajes de cliente-servidor y servidor-cliente, después de que la identificación y autentificación han sido confirmadas. El kdc y el usuario comparten una clave de encriptado secreta, la cual es usada, por ejemplo, para encriptar el mensaje del cliente conteniendo una clave de sesión.

Kerberos utiliza encriptado simétrico y asimétrico. Debido a que los métodos de encriptado de Kerberos están basados en claves conocidas sólo por el kdc y el cliente, o por el kdc y el servicio de red, se dice que Kerberos usa encriptado simétrico, esto es, la misma clave es usada para encriptar y desencriptar mensajes. También puede hacer uso limitado de encriptado asimétrico, un par de claves privada/pública pueden ser almacenadas en un lector desde una tarjeta inteligente, y usada para encriptar/desencriptar mensajes autentificados desde un cliente de red o servicio de red.

El autenticador Kerberos previene repetición de paquetes

Finalmente Kerberos, también, crea, entrega y autentica, normalmente basado en cronómetros únicos, de acuerdo con el ticket del cliente. El autentificador es único y válido sólo una vez, esto minimiza la posibilidad de que alguien obtenga y reutilice el ticket del cliente, tal vez en un intento para sustraer y usar la identidad del cliente, esto es conocido como "reproducción", y el autentificador lo previene. Excepto por la autentificación de Kerberos los accesos de seguridad son idénticos con los de Windows NT y versiones anteriores.

En el ejemplo de la figura 5.9, el cliente ha solicitado y recibido un ticket para \\infosvir. El cliente quiere acceder a \\ infosvir\share para leer un archivo.

1. El cliente y el servidor negocian un paquete de seguridad para usar autentificación, y eligen Kerberos.

2. El cliente envía un ticket de sesión (conteniendo credenciales de usuario en el pac).
3. Si el servidor acepta el ticket (es decir, se habilita para desencriptar el ticket con su clave secreta) entonces el servidor crea una señal de acceso para el usuario basada en el pac.
4. El cliente redirecciona un mensaje smb solicitando acceso al archivo.
5. La seguridad del servidor compara permisos de archivo con las credenciales del usuario y proporciona o deniega el acceso.

FIRMA DIGITAL

La firma es un documento y un medio de comprometer al firmante a mantener su palabra sin permitir al receptor del mismo su alteración. Por ejemplo, el documento podría ser una letra de cambio.

El protocolo para llevar a cabo la firma digital es como sigue:

1. El firmante calcula el mac del documento bajo clave K0 (se usa el MAC como sustituto condensado del mensaje).

2. Eligen r claves K1, …Kr, al azar que mantiene secretas (r es número par).

3. Elige r palabras X1, ...Xr.

4. Cifra Xn bajo Kn produciendo Yn.

5. Entrega a un notario local Xn e Yn.

6. Cifra el mac r veces bajo Kn, produciendo Zn. El conjunto de los Z1, …, Zr, constituyen la firma digital.

7. Envía al destinatario el documento +K0+MAC+X1,…,Xr+Y1,…Yr+Z1+,…, Zr.

8. El destinatario reclama r/2 claves al firmante.

9. El firmante envía al destinatario las r/2 claves pedidas.

10. El destinatario comprueba que las claves son buenas obteniendo los Yn, cifrando los Xn bajo las Kn recibidas.

11. A continuación, verifica la veracidad del mac al cifrarlo bajo las Kr, obteniendo los Zr.

En caso de reclamación, se llevan ante el juez el mac, la firma y los Kn, Xn e Yn. Si hay r, o menos, elementos de la firma correctos, se da la razón al firmante; si hay r+1 elementos correctos, o más, se da la razón al destinatario.

TARJETAS ELECTRÓNICAS

Las tarjetas magnéticas están sujetas a fraude por la facilidad de duplicación, modificación magnética y falsificación.

Como alternativa, se han desarrollado diversos tipos de tarjetas electrónicas. Las más sencillas consisten en una simple memoria, que puede ser de lectura/escritura o de solo lectura. Pueden usarse como inyector de claves o como tarjetas de identificación

personal. Un paso más avanzado son las tarjetas de seguridad inteligentes (intelligent secure card, chip card o smart card), que contiene en su interior un microprocesador con memoria. Resulta imposible recuperar información secreta contenida en ellas, así como su duplicación. El procesador controla el acceso y las aplicaciones de la tarjeta. Ésta puede realizar operaciones de cifrado y descifrado por software; otras tarjetas más perfeccionadas incluyen un procesador "hardware" tipo des o rsa.

Las tarjetas inteligentes pueden cumplir su cometido de identificación personal incluso en terminales desprovistas de facilidades criptográficas y sin conexión en tiempo presente al ordenador central.

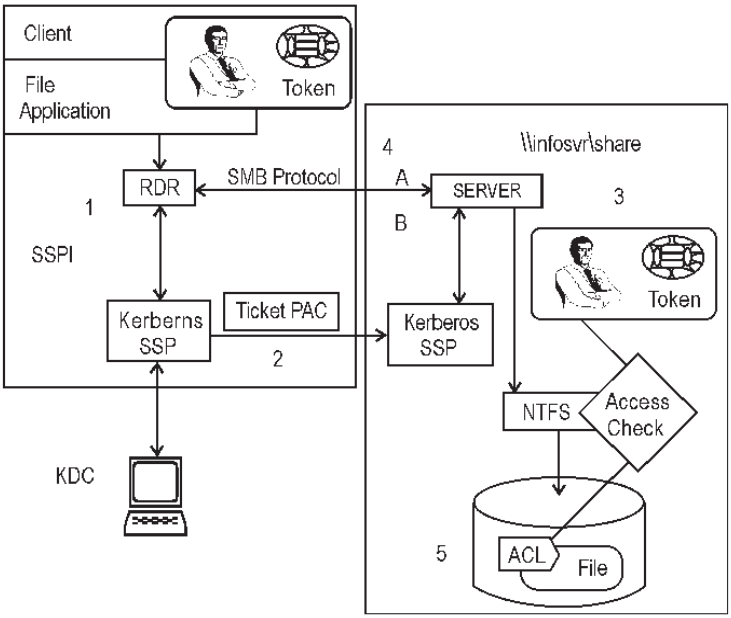


Fig. 5.9 Kerberos y solicitud de autorización remota.

x	0	1	2	3	4	5	6	7	8	9
0,0	0,5000	0,5040	0,5080	0,5120	0,5160	0,5199	0,5239	0,5279	0,5319	0,5359
0,1	0,5398	0,5438	0,5478	0,5517	0,5557	0,5596	0,5636	0,5675	0,5714	0,5754
0,2	0,5793	0,5832	0,5871	0,5910	0,5948	0,5987	0,6026	0,6064	0,6103	0,6141
0,3	0,6179	0,6217	0,6255	0,6293	0,6331	0,6368	0,6406	0,6443	0,6480	0,6517
0,4	0,6554	0,6591	0,6628	0,6664	0,6700	0,6736	0,6772	0,6808	0,6844	0,6879
0,5	0,6915	0,6950	0,6985	0,7019	0,7054	0,7088	0,7123	0,7157	0,7190	0,7224
0,6	0,7258	0,7291	0,7324	0,7357	0,7389	0,7422	0,7454	0,7486	0,7518	0,7549
0,7	0,7580	0,7612	0,7642	0,7673	0,7704	0,7734	0,7764	0,7794	0,7823	0,7852
0,8	0,7881	0,7910	0,7939	0,7967	0,7996	0,8023	0,8051	0,8078	0,8106	0,8133
0,9	0,8159	0,8186	0,8212	0,8238	0,8264	0,8289	0,8315	0,8340	0,8365	0,8389
1,0	0,8413	0,8438	0,8461	0,8485	0,8508	0,8531	0,8554	0,8577	0,8599	0,8621
1,1	0,8643	0,8665	0,8686	0,8708	0,8729	0,8749	0,8770	0,8790	0,8810	0,8830
1,2	0,8849	0,8869	0,8888	0,8907	0,8925	0,8944	0,8962	0,8980	0,8997	0,9015
1,3	0,9032	0,9049	0,9066	0,9082	0,9099	0,9115	0,9131	0,9147	0,9162	0,9177
1,4	0,9192	0,9207	0,9222	0,9236	0,9251	0,9265	0,9279	0,9292	0,9306	0,9319
1,5	0,9332	0,9345	0,9357	0,9370	0,9382	0,9394	0,9406	0,9418	0,9429	0,9441
1,6	0,9452	0,9463	0,9474	0,9484	0,9495	0,9505	0,9515	0,9525	0,9535	0,9545
1,7	0,9554	0,9564	0,9573	0,9582	0,9591	0,9599	0,9608	0,9616	0,9625	0,9633
1,8	0,9641	0,9649	0,9656	0,9664	0,9671	0,9678	0,9686	0,9693	0,9699	0,9706
1,9	0,9713	0,9719	0,9726	0,9732	0,9738	0,9744	0,9750	0,9756	0,9761	0,9767
2,0	0,9772	0,9778	0,9783	0,9788	0,9793	0,9798	0,9803	0,9808	0,9812	0,9817
2,1	0,9821	0,9826	0,9830	0,9834	0,9838	0,9842	0,9846	0,9850	0,9854	0,9857
2,2	0,9861	0,9864	0,9868	0,9871	0,9875	0,9878	0,9881	0,9884	0,9887	0,9890
2,3	0,9893	0,9896	0,9898	0,9901	0,9904	0,9906	0,9909	0,9911	0,9913	0,9916
2,4	0,9918	0,9920	0,9922	0,9925	0,9927	0,9929	0,9931	0,9932	0,9934	0,9936
2,5	0,9938	0,9940	0,9941	0,9943	0,9945	0,9946	0,9948	0,9949	0,9951	0,9952
2,6	0,9953	0,9955	0,9956	0,9957	0,9959	0,9960	0,9961	0,9962	0,9963	0,9964
2,7	0,9965	0,9966	0,9967	0,9968	0,9969	0,9970	0,9971	0,9972	0,9973	0,9974
2,8	0,9974	0,9975	0,9976	0,9977	0,9977	0,9978	0,9979	0,9979	0,9980	0,9981
2,9	0,9981	0,9982	0,9982	0,9983	0,9984	0,9984	0,9985	0,9985	0,9986	0,9986
3,0	0,9987	0,9987	0,9987	0,9988	0,9988	0,9989	0,9989	0,9989	0,9990	0,9990
3,1	0,9990	0,9991	0,9991	0,9991	0,9992	0,9992	0,9992	0,9992	0,9993	0,9993
3,2	0,9993	0,9993	0,9994	0,9994	0,9994	0,9994	0,9994	0,9995	0,9995	0,9995

BIBLIOGRAFÍA

A. FEINSTEIN, FOUNDATIONS OF INFORMATION THEORY, McGRAW-HILL BOOK Co. N.Y.
ABRAMSON, NORMAS, INFORMATION THEORY CODING, PRETINCE HALL.
AMPARO FUSTER, LUIS HERNANDEZ ENCINAS, TÉCNICAS CRIPTOGRÁFICAS DE PROTECCIÓN DE DATOS,RAMA
BERKELAMP, E.R., ALGEBRAIC CODING THEORY, McGRAW HILL.
CASTANO, FUGINI Y MARTELLA, DATABASE SEGURITY, ADDISON-WESLEY.
C.E. SHANONN, COMUNICATION IN PRESENCE OF NOISE, PROC. IRE, 1949, VOL. 37, P.10.
D.A. HUFFMAN, A METHOD FOR THE CONSTRUCTION OF MINIMUM-REDUNDANCY CODES, PROC IRE, SEP. 1952- VOL 40.
* F.G. STREMLER, INTRODUCCIÓN A LOS SISTEMAS DE COMUNICACIONES, ADDISON-WESLEY IBEROAMERICANA.
F.M. REZA, AN INTRODUTION TO INFORMATION THEORY, McGRAW HILL BOOK, N.Y.
HAMMING, RICHARD, CODING INFORMATION THEORY, PRENTICE HALL.
MISCHA SCHWARTZ, TRANSMISIÓN DE INFORMACIÓN MODULACIÓN Y RUIDO, McGRAW HILL .
RUDOLF F. GRAF, WILLIAM SHEETS, VIDEOSCRAMBLING & DESCRAMBLING FOR SATELLITE & CABLE TV, NEWNES
WILLIAM DAVENPORT, COMUNICACIÓN MODERNA DE DATOS, GLEM.
REVISTA, REVIEW, 4/200 Ericsson.
www.ericsson.com
www.bluetooth.com
www.tektronix.com