DIVISION DE ESTUDIOS DE POSGRADO

Facultad de Ingeniería

# ESTUDIO COMPARATIVO DE ALGORITMOS CRIPTOGRAFICOS PARA SEÑALES DE VOZ Y PROPUESTA DE UN ESQUEMA

JAIME AYALA PEREZ

## T E S I S

PRESENTADA A LA DIVISION DE ESTUDIOS DE POSGRADO DE LA

FACULTAD DE INGENIERIA
DE LA
UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

COMO REQUISITO PARA OBTENER EL GRADO
DE
MAESTRO EN INGENIERIA ELECTRICA
( OPCION : COMUNICACIONES)
CIUDAD UNIVERSITARIA


**UNAM – Dirección General de Bibliotecas Tesis Digitales Restricciones de uso**

# AGRADECIMIENTOS


## AL Dr. Rogelio Alcántara Silva

Por toda la paciencia, ayuda y motivación constante en la realización de este humilde y sencillo trabajo.

## AL Dr. Sergio Rasjbaun

Por todas sus enseñanzas en la realización de este trabajo y mostrarme nuevos horizontes donde desenvolverme.

## AL Dr. Francisco J. Garcia Ugalde

Por su inapreciable ayuda y facilidades en la realización de este trabajo.

## AL M. en I. Fernando Lepe Casillas

Por toda su ayuda y sus apreciables consejos y comentarios en la realización de este trabajo.

## A MIS CONPAÑEROS DE LA DEPFI Y DE GENERACION

Por su amistad y apoyo incondicional en la elaboración de este humilde y sencillo trabajo.

## A mis padres

## Roberto Ayala R. y Francisca Pérez H. de Ayala

Por su amor, compresión y apoyo incondicional que siempre me brindan, y con la promesa de seguir adelante.

## A todos mis hermanos y familiares.

Porque sin su apoyo no sería posible la realización de este trabajo, porque este logro también es suyo, y

**gracias por creer en mí,**

**gracias por confiar en mí.**

# TESIS : ESTUDIO COMPARATIVO DE ALGORITMOS CRIPTOGRAFICOS PARA SEÑALES DE VOZ Y PROPUESTA DE UN ESQUEMA

JAIME AYALA PEREZ

RESUMEN

La información puede valorarse de muy diferentes maneras. Por ejemplo, podría tener un costo financiero, político, militar o comercial. Un intruso podría interceptarla para modificarla e influir así en la toma de decisiones logrando con ello ciertos objetivos o saçando provecho del contenido de dicha información. Esto puede suceder cuando la información no está físicamente asegurada, es decir, cuando se le transmite por medios de comunicación de acceso compartido (los cuales se consideran inseguros), entre los que se cuentan las líneas telefónicas (que pueden ser intervenidas), la transmisión por radio (microondas, que puede ser interferida), etc. Por lo anterior, el valor de la información puede llegar a tener un valor incalculable.

Es posible, que aún por canales de comunicación considerados como inseguros, la información que se transmita resulte incomprensible para una persona que no tenga derecho a recibirla, siempre y cuando a dicha información se le un tratamiento de proteción, para que únicamente las personas autorizadas pueden recobrar la información original. Una medida de protección a la información empleada contra la adulteración o la inyección de información es la utilización de la Criptología, ya sea aplicando algún algoritmo criptográfico de clave privada o algún algoritmo criptográfico de clave pública.

En este trabajo de tesis, simulamos y comparamos algunos algoritmos criptográficos de clave pública aplicados a señales de voz. Dichos algoritmos se aplicarón a señales de voz para poder realizar el cifrado en el dominio del tiempo, en el dominio de la frecuencia, en la Amplitud y en la manipulación de sus parámetros característicos (parámetros LPC).

En esta tesis, cada algoritmo de ciframinto estudiado, es la combinación de un esquema de ciframiento y de un sistema de comunicación entre diversos usuarios. Además, tomando en cuenta las ventajas y desventajas de los algoritmos de ciframiento, se proponen algunas modificaciones realizadas a el esquema de ciframiento RSA realizado en forma matricial, a la vez que se propone un nuevo sistema de comunicación entre diversos usuarios.

# CONTENIDO


INTRODUCCION 1

CAPITULO I

SISTEMA DE COMUNICACION

I.1 Introducción. 1
I.2 Un Sistema de Comunicación. 1
I.3 Elementos de un Sistema de Comunicación Digital. 3
I.3.1 Elementos de un Sistema de Comunicación Digital : El Transmisor. 3
I.3.2 Elementos de un Sistema de Comunicación Digital : El Receptor. 6
I.3.3 Elementos de un Sistema de Comunicación Digital : El Canal de Comunicación. 7

CAPITULO II

PROCESAMIENTO DIGITAL DE LA SEÑAL EN UN SISTEMA DE COMUNICACION DIGITAL

II.1 Introducción. 9
II.2 Clasificación de las señales. 9
II.3 Características de las señales. 12
II.3.1 Señales de Audio. 12
II.3.2 Señales de Voz. 14
II.3.3 Señales de Video. 16
II.4. Representación de los Sistemas Discretos Lineales Invariantes en el Tiempo. 18
II.4.1 Representación de un Sistema en el Dominio del tiempo. 19
II.4.2 Representación de un Sistema en el Dominio de la Frecuencia. 20
II.5 Filtros Digitales. 20
II.5.1 Clasificación de filtros digitales relacionados mediante su función de transferencia. 21
II.5.2 Clasificación de filtros digitales relacionados mediante su realización física. 22
II.5.2.1 Filtros Transversales. 22
II.5.2.2 Filtros en Escalera. 25
II.6 La Transformada de Fourier. 26
II.6.1 Transformada Rápida de Fourier. 27
II.6.2 Espectro de Fourier en Frecuencia. 31

| | | |
|---|---|---|
| II.7 | Técnicas de Estimación Parámetrica. | 31 |
| II.7.1 | Codificación por Predicción Lineal. | 31 |
| II.7.2 | Algoritmo Levinson-Durbin. | 36 |
| II.7.3 | Autocorrelación. | 38 |
| II.7.4 | Método de Análisis de Leroux-Gueguen. | 39 |


CAPITULO III

PRINCIPIOS BASICOS DE LA CRIPTOLOGIA


| | | |
|---|---|---|
| III.1 | Introducción a la Criptología. | 43 |
| III.2 | Definición de Criptología. | 44 |
| III.2.1 | Objetivos de un Sistema Cifrador. | 44 |
| III.3 | Necesidad de la Criptología. | 45 |
| III.3.1 | Ataques Criptoanáliticos. | 45 |
| III.4 | Elementos de la Criptología. | 47 |
| III.5 | Sistema cifrador de un solo paso. | 49 |
| III.5.1 | Seguridad Perfecta. | 50 |
| III.5.2 | Confusión y Difusión. | 52 |
| III.6 | Cifradores de bloques. | 55 |
| III.6.1 | Cifrador para Datos Estandar DES. ( Data Encryption Standard ). | 57 |
| III.6.1.1 | Descripción del DES. | 58 |
| III.7 | Cifradores de Flujo (cifradores de cadenas). | 61 |
| III.7.1 | Registros de Corrimiento Lineal. | 62 |
| III.8 | Sistema Cifrador de Clave Pública. | 65 |
| III.8.1 | Introducción a la Criptología Moderna. | 65 |
| III.8.2 | Sistema Cifrador de Clave Pública. | 66 |


CAPITULO IV

ALGORITMOS CRIPTOGRAFICOS DE CLAVE PUBLICA PARA SEÑALES DE VOZ


| | | |
|---|---|---|
| IV.1 | Introducción. | 69 |
| IV.2 | Criptografía en el Dominio del Tiempo. | 71 |
| IV.2.1 | Introducción a la Criptografía en el Dominio del Tiempo. | 71 |
| IV.2.2 | Algoritmo de ciframiento en el dominio del Tiempo. | 75 |
| IV.2.2.1 | Descripción del esquema RSA. | 76 |
| IV.2.2.2 | Aplicación del esquema RSA a el método de Reordenación de Muestras en el Dominio del Tiempo. | 77 |
| IV.2.3 | Sistema de Comunicación entre diversos usuarios. | 79 |
| IV.2.3.1 | Descripción del método propuesto por Diffie-Hellman. | 79 |
| IV.3 | Criptografía en la Amplitud. | 81 |
| IV.3.1 | Introducción a la Criptografía en la Amplitud. | 81 |
| IV.3.2 | Algoritmo de ciframiento en la Amplitud. | 81 |
| IV.3.2.1 | Aplicación del esquema RSA para el ciframiento de señales de voz en Amplitud. | 82 |
| IV.3.3 | Sistema de Comunicación entre diversos usuarios. | 84 |
| IV.3.3.1 | Realización de la clave común por elevación exponencial. | 84 |

| | | |
|---|---|---|
| IV.4 | Criptografía en el Dominio de la Frecuencia. | 86 |
| IV.4.1 | Introducción a la Criptografía en el Dominio de la Frecuencia. | 86 |
| IV.4.2 | Algoritmo de ciframiento en el Dominio de la Frecuencia. | 91 |
| IV.4.2.1 | Descripción del esquema propuesto por Elgamal T. | 92 |
| IV.4.3 | Sistema de Comunicación entre diversos usuarios basado en un Sistema de Identificación de Información. | 93 |
| IV.4.3.1 | Descripción del Sistema de Identificación de información propuesto por Okamoto E. | 94 |
| IV.5. | Manipulación de los parámetros de la señal de Voz. | 98 |
| IV.5.1 | Introducción. | 98 |
| IV.5.2 | Algoritmo de ciframiento de clave pública para la manipulación de los parámetros LPC. | 98 |
| IV.5.2.1 | Descripción del esquema propuesto RSA-Rabin-Williams. | 100 |
| IV.5.3 | Sistema de Comunicación entre diversos usuarios. | 101 |
| IV.5.3.1 | Sistema de Comunicación entre diversos usuarios realizado en Forma Matricial. | 101 |

CAPITULO V

PROPUESTA DE UN ALGORITMO DE CIFRAMIENTO PARA SEÑALES DE VOZ

| | | |
|---|---|---|
| V.1 | Introducción. | 104 |
| V.2 | Presentación del algoritmo propuesto. | 104 |
| V.2.1 | Descripción del esquema propuesto. | 104 |
| V.2.2 | Aplicación del esquema propuesto para la manipulación de parámetros LPC. | 108 |
| V.3 | Sistema de Comunicación entre diversos usuarios. | 112 |
| V.3.1 | Sistema de Comunicación entre diversos usuarios realizado en Forma Matricial. | 112 |

CAPITULO VI

PRESENTACION DE RESULTADOS Y COMPARACION DE ALGORITMOS DE CIFRAMIENTO

| | | |
|---|---|---|
| VI.1 | Introducción. | 114 |
| VI.2 | Resultados correspondientes al esquema de ciframiento de permutación de muestras en el tiempo. | 115 |
| VI.2.1 | Esquema de ciframiento RSA. | 115 |
| VI.2.1.1 | Presentación de resultados Gráficos correspondientes al método 1. | 116 |
| VI.2.1.2 | Ventajas y desventajas del esquema de ciframiento. | 118 |
| VI.2.1.3 | Ventajas y desventajas del Sistema de Comunicación entre diversos usuarios propuesto por Diffie-Hellman. | 119 |
| VI.2.2 | Complejidad en el tiempo. | 119 |
| VI.2.3 | Pruebas de seguridad. | 120 |
| VI.2.3.1 | Factorización de R. | 120 |
| VI.2.3.2 | Cálculo de $\Phi(R)$ sin factorizar R. | 121 |
| VI.2.3.3 | Determinación de d sin factorizar R. | 122 |

| | | |
|---|---|---|
| VI.3 | Resultados correspondientes al esquema de ciframiento en Amplitud. | 123 |
| VI.3.1 | Esquema de ciframiento RSA. | 123 |
| VI.3.1.1 | Presentación de resultados Gráficos correspondientes al método 2. | 123 |
| VI.3.1.2 | Ventajas y desventajas del esquema de ciframiento. | 125 |
| VI.3.1.3 | Ventajas y desventajas del Sistema de Comunicación entre diversos usuarios realizado en forma exponencial. | 125 |
| VI.3.2 | Complejidad en el tiempo. | 126 |
| VI.4 | Resultados correspondientes al esquema de ciframiento en el dominio de la Frecuencia. | 127 |
| VI.4.1 | Método de permutación de Coeficientes de la DFT. | 127 |
| VI.4.1.1 | Presentación de resultados Gráficos correspondientes al método 3. | 127 |
| VI.4.1.2 | Ventajas y desventajas del esquema de ciframiento. | 129 |
| VI.4.1.3 | Ventajas y desventajas del Sistema de Comunicación entre diversos usuarios. | 129 |
| VI.4.2 | Complejidad en el tiempo. | 130 |
| VI.4.3 | Prueba de Seguridad. | 130 |
| VI.5. | Resultados correspondientes al esquema de ciframiento de permutación de parámetros LPC basado en el esquema propuesto por RSA-Williams-Rabin. | 131 |
| VI.5.1 | Método de permutación de parámetros LPC. | 131 |
| VI.5.1.1 | Presentación de resultados Gráficos correspondientes al método 4. | 131 |
| VI.5.1.2 | Ventajas y desventajas del esquema de ciframiento. | 133 |
| VI.5.1.3 | Ventajas y desventajas Sistema de Comunicación entre diversos usuarios. | 133 |
| VI.5.2 | Complejidad en el tiempo. | 134 |
| VI.5.3 | Prueba de seguridad. | 134 |
| VI.6 | Resultados correspondientes al esquema de ciframiento de manipulación de parámetros LPC basado en el esquema RSA realizado en Forma Matricial. | 137 |
| VI.6.1 | Manipulación de los parámetros LPC. | 137 |
| VI.6.1.1 | Presentación de resultados Gráficos correspondientes al método 5. | 137 |
| VI.6.1.2 | Ventajas y desventajas del esquema de ciframiento. | 139 |
| VI.6.1.3 | Ventajas y desventajas del Sistema de Comunicación entre diversos usuarios. | 140 |
| VI.6.2 | Complejidad en el tiempo. | 141 |
| VI.6.3 | Prueba de seguridad. | 144 |
| VI.7 | Comparación de algoritmos de ciframiento. | 148 |
| VI.8 | Comparación de resultados de los diferentes esquemas de ciframiento. | 154 |
| VI.8.1 | Inteligibilidad residual. | 154 |
| | **Conclusiones** | 155 |
| | **Bibliografía** | 159 |

La información puede valorarse de muy diferentes maneras. Por ejemplo, podría tener un costo financiero, político, militar o comercial. Un intruso ( criptoanalista ) podría interceptarla para modificarla e influir así en la toma de decisiones logrando con ello ciertos objetivos o sacando provecho del contenido de dicha información. Esto puede suceder cuando la información no está físicamente asegurada, es decir, cuando se le transmite por medios de comunicación de acceso compartido (los cuales se consideran inseguros), entre éstos se cuentan las líneas telefónicas (que pueden ser intervenidas), la transmisión por radio (microondas, que puede ser interferida), etc. Por lo anterior, el valor de la información puede llegar a tener un valor incalculable.

Es posible, que aún por canales de comunicación considerados como inseguros, la información que se transmita resulte incomprensible para una persona que no tenga derecho a recibirla, siempre y cuando a dicha información se le dé un tratamiento de protección, para que únicamente las personas autorizadas puedan recobrar la información original.

Las dos principales razones para proteger la información (el contenido de un mensaje) son : (1) **Privacidad** y (2) **Autenticidad.** La privacidad en un Sistema de Comunicación que utiliza un canal público, consiste en evitar a usuarios no autorizados escuchar la conversación que se efectúa entre el emisor y el receptor. La autenticidad previene que personas no autorizadas extraigan, alteren, inyecten o modifiquen la información que se transmite a través de un Canal de Comunicaciones Público, de tal manera que se consiga "engañar" al receptor. La privacidad se logra aplicando algún esquema de ciframiento y la autenticidad se logra empleando algún Sistema de Comunicación entre diversos usuarios.

Una medida de protección a la información empleada contra la adulteración o la inyección de información es la utilización de la **Criptología.** Podemos decir que la aplicación de técnicas criptográficas es una de las soluciones universalmente aceptadas para evitar actos que puedan vulnerar la información. Estos actos pueden clasificarse en alguno de estos grupos : robo, corrupción, alteración de palabra clave y en general cualquier utilización no autorizada de información.

Por estas consideraciones, la Criptología ha sido de gran importancia en las comunicaciones militares, diplomáticas y recientemente en el ámbito comercial.

La protección del contenido de la información, se lleva a cabo aplicando algún algoritmo de cifrамiento Simétrico o Asimétrico. Simmons [1] clasifica a los Algoritmos de Cifrамiento, para su estudio, en *Algoritmos de Cifrамiento Simétricos* (de una sóla clave) y *Algoritmos de Cifrамiento Asimétricos* (de dos claves). Simmons define a los *Algoritmos Simétricos* (también llamados Algoritmos de Cifrамiento de clave privada), como aquellos algoritmos en los cuales el proceso de cifrado **E**, y el proceso de descifrado **D**, se realiza por medio de una sóla clave, dicha clave se guarda en secreto por cada usuario $U_i$. El conocimiento de dicha clave por parte de un intruso, le permite a éste conocer el contenido del mensaje cifrado.

Los *Algoritmos de Cifrамiento Asimétricos* también llamados Algoritmos de Cifrамiento de Clave Pública son aquellos en los cuales el proceso de cifrамiento **E** se realiza con una clave pública **e**, mientras que el proceso de descifrado **D** se realiza con una clave privada **d**. En este tipo de algoritmos cada usuario $U_i$ da a conocer ( pública ) su clave pública **e** en un **Directorio Público de claves públicas.** El conocimiento o cálculo de la clave **d** a partir de la clave pública **e**, no compromete en nada la seguridad del sistema de cifrамiento, ya que el cálculo de la clave privada **d** a partir de la clave pública **e** es intratable desde el punto de vista de Teoría de la Complejidad, es decir, no importa que tanta cantidad de recursos en espacio y tiempo este dispuesto a utilizar el intruso ( criptoanalista ).

El objetivo ( *general* ) de este trabajo de tesis es realizar un estudio comparativo de diversos algoritmos de cifrамiento de clave pública aplicados a señales de voz. Dicho estudio comparativo se llevó a cabo simulando y comparando entre sí diversos algoritmos de cifrамiento. Cabe aclarar que cada algoritmo de cifrамiento estudiado es el resultado de la adaptación de un *Esquema de Comunicación entre diversos Usuarios* a un *Esquema de Cifrамiento de clave pública* con la finalidad de lograr **Privacidad** y **Autenticidad** como una medida de protección de la información que se transmite entre diversos usuarios.

La simulación de estos algoritmos se llevó a cabo mediante programas realizados en lenguaje C. Tal simulación permitió hacer la evaluación de 4 algoritmos de cifrамiento en cuanto a su velocidad de cifrамiento y descifrамiento, para de esta manera proponer un nuevo algoritmo de cifrамiento.

A continuación se hace un pequeño resumen del contenido de cada capítulo de esta tesis.

En el primer capítulo se describe de manera muy breve un Sistema de Comunicación Digital, así como los elementos que lo constituyen. Se hace hincapié en la importancia que tienen las etapas de ciframiento y desciframiento en dicho Sistema de Comunicación. En el capítulo dos se presentan los fundamentos y algoritmos para el Procesamiento Digital de Señales en un Sistema de Comunición Digital. En el capítulo tres se presentan los fundamentos de la Criptología, las ventajas de utilizar la Criptología moderna con respecto de la Criptología Clásica (antigüa). En el capítulo cuatro se presenta el análisis y la implementación de diversos Algoritmos Asimétricos para señales de voz. En el capítulo cinco se presentan los resultados de la simulación de un nuevo Algoritmo de Ciframiento de Clave Pública para señales de voz. Este capítulo puede considerarse como la aportación más importante de este trabajo de tesis ( *objetivo particular* ), ya que en él se presentan las modificaciones realizadas a un Esquema de ciframiento de clave pública realizado en forma matricial [30] y la propuesta de un Sistema de Comunicación entre diversos usuarios como una forma de cifrar las señales de voz para su transmisión a través de un Canal de Comunicación Público. Finalmente, en el capítulo seis se muestran las comparaciones entre los diversos algoritmos de ciframiento mencionados en el capítulo cuatro, con respecto al algoritmo presentado en el capítulo cinco.

CAPITULO

U N O

# S I S T E M A  D E  C O M U N I C A C I O N

## I.1 INTRODUCION.

La voz es la forma más común de comunicación en nuestra sociedad. Generalmente, el objetivo principal en un Sistema de Comunicación es transmitir un mensaje en forma rápida, precisa y al menor costo posible.

Existe un gran número de situaciones en las que el contenido del mensaje que se transmite a través de un Canal Público de Comunicación es confidencial y donde el interceptor podría beneficiarse y sacar provecho a partir de la información obtenida. Para evitar que la información contenida en el mensaje sea entendible, por parte del interceptor, una de las medidas de protección contra la intercepción de un mensaje a través de un Canal de Comunicación Público es empleando la *Criptología.*

La criptología forma parte de un Sistema de Comunicación (ver sección I.3 ) y tiene como finalidad proteger el contenido del mensaje, así como evitar la comprensión del mensaje por parte de un interceptor.

## I.2 UN SISTEMA DE COMUNICACION.

Se define a la comunicación como el proceso por medio del cual un mensaje *(información)* se transfiere en espacio y tiempo de un punto llamado fuente, a otro punto que es el receptor.

Se entiende por un *Sistema de Comunicación* a la totalidad de mecanismos [2] que proporcionan el enlace para la transferencia de mensajes entre fuente y receptor ( ver Fig.1.1 ).

La Fig.1.1 muestra los elementos funcionales de un Sistema de Comunicación. Por conveniencia, los hemos aislado como entidades distintas, aunque en los sistemas reales la separación no puede ser tan obvia. Como se indica en la Fig. 1.1, existen algunos factores no deseados, los cuales inevitablemente forman parte de un Sistema de Comunicación.

El mensaje producido por una fuente no es eléctrico y por lo tanto, es necesario un transductor de entrada. Este transductor convierte el mensaje en una señal eléctrica, tal como un voltaje o una corriente. Similarmente, otro transductor en el receptor convertirá la señal de salida en una forma apropiada de mensaje. En lo sucesivo, los términos señal y mensaje se usarán indistintamente, puesto que tanto la señal como el mensaje son una representación de la información.

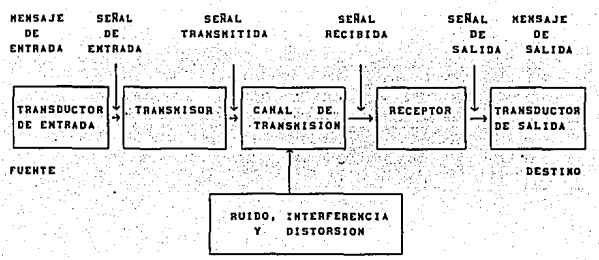



Fig. 1.1 Elementos de un Sistema de Comunicación ([2] fig. 1.1).

Además de los transductores, en un Sistema de Comunicación, existen tres elementos esenciales, éstos son : El *Transmisor*, el *Canal de Comunicación* y el *Receptor*. Cada uno de los elementos anteriores tienen su función característica, la cual se describe a continuación.

**Transmisor.** El transmisor conduce el mensaje al Canal de Comunicación en forma de señal. Para lograr una transmisión eficiente y efectiva, se deben desarrollar varias operaciones de procesamiento de la señal. Una de las más importantes es la *Modulación*.

**Canal de Comunicación.** El Canal de Comunicación o medio es el enlace eléctrico entre el transmisor y el receptor. El Canal de Comunicación puede ser : El espacio libre o Atmósfera, un par de alambres, un cable coaxial, etc.

**Receptor.** La función del receptor es extraer del Canal de Comunicación la señal deseada y entregarla al transductor de salida. Como las señales son frecuentemente muy débiles, como resultado de la atenuación, el receptor tiene varias operaciones de procesamiento de la señal y una de ellas es la Amplificación. Una etapa importante en el receptor es la *Demodulación* ( o Detección ), que es el caso inverso del proceso de la Modulación realizada en el transmisor, con este proceso vuelve la señal a su forma original.

## I.3 ELEMENTOS DE UN SISTEMA DE COMUNICACION DIGITAL.

En el inciso anterior se hizo referencia a un Sistema de Comunicación de manera muy general, en este inciso se describirán de manera muy breve las etapas que constituyen específicamente a un Sistema de Comunicación Digital DSC (de las siglas en inglés) [3], así como de las perturbaciones que afectan al Canal de Comunicación en dicho DSC.

Un diagrama a bloques de un DSC se muestra en la Fig.1.2, los bloques superiores constituyen el Transmisor y los bloques inferiores constituyen al receptor.

Se puede mencionar también, que en varios puntos del DSC la señal, $s[n]$, es modificada por una señal de ruido y se considera que en el receptor se tiene una estimación de la señal original, $\hat{s}[n]$.

### I.3.1 Elementos de un Sistema de Comunicación Digital : El Transmisor.

Los bloques que constituyen al transmisor son :

**Formateo** ( Format ).
El primer paso de la señal en un DSC, es el Formateo y consiste en hacer compatible la señal de la fuente con el procesamiento digital, es decir, transforma la información producida por la fuente en símbolos digitales.

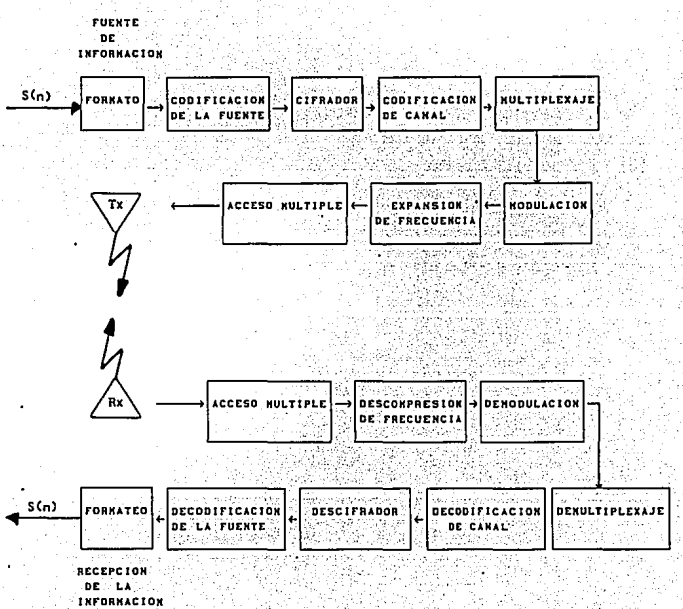



Fig. 1.2 Sistema de Comunicación Digital ([3] fig. 1.2).

**Codificación de Fuente** ( Source Coding ).
La codificación de fuente produce una conversión analógica digital (A/D) (para fuentes analógicas) y elimina la redundancia de información en el mensaje.

**Ciframiento** ( Encription )
Evita que los usuarios no autorizados entiendan el contenido del mensaje que se transmite a través del Canal de Comunicación, también evita inyección falsa de mensajes en un DSC.

**Codificación de Canal** ( Channel Coding ).

Para una conocida relación de datos, la codificación de canal permite reducir los requirimientos de ancho de banda de la Relación Señal a Ruido (**SNR**) o la probabilidad de error **Pe** en un DSC, según la necesidad del ancho de banda o la complejidad del codificador.

En la codificación de canal la responsabilidad es para el codificador, ya que él realiza un mapeo de todos los ingresos (señales, datos, etc.) del **DSC** hacia la entrada del canal. De la misma manera, el decodificador realiza un mapeo de la salida del canal hacia la salida del **DSC**, con esto, se logra que el efecto del ruido en el canal sea mínimo.

La combinación de la codificación de canal y el decodificador proporcionan una comunicación fidedigna sobre un canal con ruido. Esto se logra introduc iendo redundancia.

**Multiplexaje** (Multiplex)

Produce una combinación de señales que pueden existir en un un solo canal, ya que dichas señales tienen diferentes características y son producidas por diferentes fuentes, de esta manera las señales comparten una porción del medio de comunicación.

**Modulación** ( Modulate ).

La modulación es la alteración sistemática de una forma de onda, conocida como *portadora*, de acuerdo a las características de otra forma de onda, *la señal moduladora* o *mensaje*. El objetivo fundamental es producir una onda modulada que conduzca información, y cuyas propiedades sean las más adecuadas al trabajo de comunicación dado.

La modulación, es un proceso que se distingue por el acoplamiento de la señal transmitida, a las propiedades del canal, por medio de una onda portadora.

**Compresión de Frecuencia** ( Frequency Spread ).

. Produce una señal que es menos vulnerable a interferencias (a la interferencia natural e intencional) y puede usarse para incrementar la privacidad de los comunicadores.

**Acceso Múltiple** ( Multiple Access ).

El término de "acceso múltiple", se refiere a los métodos de acceso a un mismo recurso, es decir, compartir un mismo recurso de comunicación por partes iguales.

Existen tres técnicas básicas de acceso múltiple : División en frecuencia (FDMA), división en tiempo (TDMA) y división de código (VDMA). Estas técnicas difieren en la utilización de la potencia del satélite, tiempo y frecuencia (ancho de banda). Estas técnicas pueden usarse para cualquiera de las tres siguientes formas de operación : preasignación, asignación en tiempo y asignación por demanda.

### I.3.2 Elementos de un Sistema de Comunicación Digital : El Receptor.

Los bloques que constituyen el receptor son :

**Acceso Múltiple** ( Multiple Access ).
En esta etapa se reliza el proceso inverso a la etapa de acceso múltiple realizada por el transmisor, es decir, el transpondedor de un Satélite de Comunicación permite la interconexión de forma rápida y eficiente, ésto es, la comunicación con uno o varias estaciones en tierra y de esta manera lograr una comunicación en tiempo real.

**Descompresión de Frecuencia** ( Frequency Despread ).
Devuelve las características (en frecuencia) de la señal antes de la compresión de las señales.

**Demultiplexaje** ( Demultiplex ).
Realiza la separación de las diferentes señales que se transmiten en un solo canal.

**Decodificación de Canal** ( Channel Decode ).
La decodificación del canal simplemente ejecuta el proceso inverso a la codificación de canal, es decir, por medio de esta se consigue entregar al destinatario una reproducción de la fuente digital original de salida. Las ventajas más importantes de usar la codificación y decodificación de canal son :(1) Se logra reducir los requerimientos del ancho de banda, (2) Se tiene un control sobre la redundancia del mensaje.

**Demodulación** ( Demodulate ).
La demodulación o detección, es el proceso, realizado en el receptor, por medio del cual se recupera el mensaje de la onda modulada.

**Desciframiento** ( Decryt ).
Descifra la información que se transmite de un usuario hacia otro a través de un Canal de Comunicación, empleando para ello su clave privada.

**Decodificación de Fuente** ( Source Decode ).
Realiza la conversión D/A de la señal (para señales analógicas).

**Formateo** ( Format ).
Representa la señal eléctrica como resultado de la conversión Digital/Analógico a un formato especifico, como bits, caracteres, etc.

**Sincronización** (Syncronization)
Este bloque es uno de los más importantes en un DSC, ya que permite la interacción entre cada uno de los bloques que componen el DSC.

## I.3.3 Elementos de un Sistema de Comunicación Digital : El Canal de Comunicación.

El DSC tiene diferentes formas, siendo quizá la más empleada, la conexión que existe entre la antena transmisora de la radioemisora comercial y la antena receptora del equipo de radio. En este DSC, el canal de comunicación es la Atmósfera o el espacio libre, ya que la señal transmitida se propaga a través de la atmósfera, hasta llegar a la antena receptora. En este tipo de canal, como en general en los diferentes tipos de canales de comunicación, la señal sufre de cierta degradación (perturbación) ya sea en el Trasmisor, en el Receptor o en el mismo Canal de Comunicación. Entre los tipos de perturbaciones que ocurren durante la transmisión de la señal se encuentran : Atenuación, Distorsión, Interferencia y Ruido.

**Atenuación.-** Todos los medios de transmisión eléctricos se caracterizan por la *atenuación*, que es la disminución progresiva de la potencia de la señal conforme aumenta la distancia. Por lo tanto, la atenuación reduce la **intensidad** de la señal. La magnitud de la atenuación debe de ser pequeña. Cuando es grande, es un factor a considerar, debido a que puede producir alteraciones a la información. Sin embargo, son más serios la distorsión, la interferencia y el ruido, los cuales se manifiestan como atenuaciones de la **forma** de la señal.

**Distorsión.-** Es la alteración de la señal debido a la respuesta imperfecta del sistema a ella misma. A diferencia del ruido y la interferencia, la distorsión desaparece cuando la señal deja de aplicarse. El diseño de sistemas perfeccionados o redes de compensación reducen la distorsión. En teoría es posible lograr una compensación perfecta. En la práctica debe permitirse cierta distorsión, aunque su magnitud debe estar dentro de ciertos límites tolerables.

**Interferencia.-** Es la contaminación por señales extrañas, generalmente artificiales y de forma similar a las de la señal. El problema es particularmente común en estaciones de radio, donde pueden ser captadas dos o más señales simultáneamente por el receptor.

**Ruido.-** Por ruido se debe entender a las señales aleatorias e impredecibles de tipo eléctrico originadas en forma natural dentro o fuera del sistema. Cuando estas variaciones se agregan a la señal portadora de la información, pueden quedar en gran parte ocultas en el mensaje. El mantener el ruido entre ciertos intervalos permitidos es uno de los problemas básicos que la comunicación eléctrica trata de resolver.

Este trabajo de tesis, se enfocará a los bloques de *ciframiento y deciframiento* para señales digitales, como una medida de protección al contenido de la información que se va a transmitir a través de un Canal de Comunicación Público.

CAPITULO

D O S

# PROCESAMIENTO DIGITAL DE LA SEÑAL EN UN SISTEMA DE COMUNICACION DIGITAL

## II.1 INTRODUCCION.

Existen muchas clases de fuentes de información, por éso, los mensajes aparecen en muchas formas : una secuencia de símbolos o letras discretas (por ejemplo: palabras escritas en una forma telegráfica); una magnitud sencilla variando con el tiempo (por ejemplo; la presión acústica producida por la voz o la música); varias funciones del tiempo y otras variables (ejemplo, la intensidad de la luz y el color de un escena de televisión). Pero, sea cual fuere el mensaje, el objetivo de un Sistema de Comunicación es proporcionar una réplica aceptable de él a su destino.

## II.2 CLASIFICACION DE SEÑALES.

Existen diversas maneras de clasificar a las señales, como son las siguientes ([3], pag. 11) :

1.) Señal determinística y señal aleatoria.

Una *señal determinística*, es aquella para la cual no hay incertidumbre respecto a su valor para cualquier instante de tiempo.

Una *señal aleatoria*, es aquella para la cual hay un cierto grado de incertidumbre antes de que la señal ocurra. Para este tipo de señales no es posible escribir una expresión explícita. Sin embargo, si se examina sobre un periodo largo de tiempo, lo cual nos lleva a lo que es un proceso aleatorio, se pueden expresar en términos de probabilidades o promedios estadísticos.

## 2.) Señales periódicas y aperiódicas.

Una señal x(t) es llamada *periódica* si existe una constante T > 0 tal que :

$$x(t) = x(t + T), \qquad -\infty < t < \infty, \quad T > 0 \tag{2.1}$$

Un valor pequeño de T que satisface la ecuación (2.1), es llamado el período de la señal. Una señal para el cual el valor de T ( para T > 0 ) no satisface la ecuación (2.1), es llamada no *periódica* o *aperiódica*.

## 3.) Señales Analógicas y Discretas

Una señal es *Analógica* cuando tiene valor en cualquier instante de tiempo y se representa como :

$$x(t) \qquad |t| < \infty$$

Una señal es *Discreta* [4] cuando toma valores sólo en ciertos intervalos de tiempo y se representa como :

$$x[nT] \quad \text{ó} \quad x[n]$$

donde n = conjunto de todos los enteros, y
T = intervalo de tiempo entre muestras.

La notación x[n] se empleará para designar una secuencia de números reales o complejos definidos para todo número entero **n**. La secuencia x[n] será denominada *señal discreta* y el índice **n** *tiempo discreto*.

Emplearemos a menudo el siguiente caso especial :

Señal Impulso Unitario ó Secuencia Delta

$$\delta[n] = \begin{cases} 1, & n=0 \\ 0, & n\neq 0 \end{cases}$$

Empleando la Señal Impulso Unitario, una secuencia arbitraria x[n], se representa como una sumatoria de impulsos unitarios apropiadamente desplazados y multiplicados por los valores de la secuencia x[n].

$$x[l] = \sum_{n=-\infty}^{\infty} x[n]\delta[l-n]$$

## 4.) Señales de Energía y Señales de Potencia.

Una señal eléctrica puede representarse por un voltaje v(t) o por una corriente i(t) proporcionando una potencia instantánea a través de una resistencia R definida por :

$$p(t) = \frac{v^2(t)}{R} , \qquad \text{potencia instantánea}$$

o bien por :

$$p(t) = R\, i^2(t)$$

En un Sistema de Comunicación la potencia se normaliza, suponiendo R = 1 [ohms].

Entonces independientemente de si la forma de onda es voltaje o corriente, la potencia instantánea se puede representar como :

$$p(t) = x^2(t)$$

donde x(t) es una señal de corriente o voltaje.

La energía disipada durante el intervalo (-T/2 a T/2) por una señal real se puede escribir como ([3], ec. 1.5) :

$$E_x^T = \int_{T/2}^{T/2} x^2(t)\, dt \quad ;$$

La potencia promedio disipada durante un periodo de tiempo es ([3], ec. 1.6) :

$$P_x^T = \frac{1}{T} \int_{T/2}^{T/2} x^2(t)\, dt$$

Clasificaremos x(t) como una *señal de energía*, si y solo si, x(t) tiene una energía diferente de cero pero finita ( $0 < Ex < \infty$, para toda $t$), y que además su potencia es igual a cero ($P(t)=0$), y esta dado como ([3], ec. 1.7) :

$$Ex = \lim_{T \to \infty} \int_{T/2}^{T/2} x^2(t)\, dt \quad = \hat{E}x = \int_{-\infty}^{\infty} x^2(t)\, dt$$

En la práctica siempre se transmiten señales que tienen energía finita. Sin embargo para describir a las señales periódicas, los cuales por definición existen para todo tiempo y por lo tanto tienen energía infinita y con el propósito de mantenernos con las señales aleatorias que tienen energía infinita, entonces es conveniente definir una clase de señales de potencia.

Una señal x(t), es una *señal de potencia* si y solo si, ésta tiene potencia diferente de cero pero finita, ($0 < P_x < \infty$ para toda t), y además tienen $E = \infty$ y esta dada como ([3], ec. 1.8) :

$$P = \lim_{T \to} \frac{1}{T} \int_{-T/2}^{T/2} x^2(t)\, dt$$

Esta clasificación es mutuamente exclusiva en el siguiente sentido.

Una señal de energía, tiene energía finita pero potencia promedio cero.

Mientras que :
Una señal de potencia tiene, una potencia promedio finita pero energía infinita.

Como regla general :

* Las señales periódicas y las señales aleatorias están clasificadas como señales de potencia, es decir, tienen energía infinita.

* Las señales que sean a la vez tanto determinísticas y no periódicas se les clasifica como señales de energía y tienen energía finita.

## II.3 CARACTERISTICAS DE LAS SEÑALES.

Otra forma de clasificar las señales en general es en función de su ancho de banda. En este inciso a las señales las clasificamos como : Señales de Audio, Señales de voz y Señales de Televisión, que presentamos a continuación brevemente.

### II.3.1 Señales de Audio.

En general, las señales de audio (señales acústicas) se clasifican en señales primarias y señales secuendarias [5]. Las señales primarias se originan por instrumentos musicales, el canto, el habla, así como las señales de ruidos, que sirven de acompañamiento de fondo para las emisiones musicales y artísticas (ruido de tren, chirrido de grillos, etc).

Al valorar los canales de radioemisión y de telecomunicación se considera que cada señal acústica, por lo general, es una señal aleatoria. Aunque considerables trozos de este tipo de de señales aleatorias pueden tener un caracter periódico, al analizarlas en grandes intervalos. Las señales como por ejemplo, el pitido de una sirena, el zumbido de una bocina y otros, son una excepción de esta consideración.

Las señales acústicas secundarias se reproducen por medio de dispositivos electroacústicos, o sea, son señales primarias que han pasado a través de canales electroacústicos de telecomunicaciones, en los que sus parámetros han sido modificados convenientemente.

La señal secundaria ideal debe reproducir exactamente la primaria, pero esta exigencia no es determinante, ya que el oído humano no puede percibir su disparidad. Además, en la práctica, a menudo es imposible, o muy costoso, conseguir que estas señales sean iguales.

Por otra parte, el ancho de banda de una señal acústica se encuentra entre 10Hz y 25.4khz. La composición y forma del espectro de la señal acústica de cada una de las fuentes primarias del sonido que se emplean en los sistemas de radiodifusión y telecomunicaciones, como regla general, varían continuamente. Se distinguen espectros de altas y bajas frecuencias, discontinuos y continuos. El espectro de cualquier fuente de sonido, aunque ésta sea de un mismo tipo (por ejemplo, violines de una orquesta), tiene sus rangos característicos denominado *timbre* del sonido. Son de uso común los conceptos de timbre del violín, del trombón, del órgano, etc, así como del timbre de la voz: sonoro, cuando se acentúan las componentes de frecuencias altas: apagado, cuando estas frecuencias están atenuadas.

Saposhrov detalla las bandas de frecuencias en Hz para algunas de las fuentes primarias de señales acústicas ([5], pag.45 ) :

| Fuente | Rango [Hz] |
|---|---|
| Conversación | 70 - 7000 |
| Violín | 250 - 15000 |
| Triángulo musical | 1000 - 16000 |
| Bajo (instrumento) | 50 - 6000 |
| Órgano | 20 - 15000 |
| Orquesta sinfónica | 30 - 15000 |

## II.3.2 Señales de Voz.

El sonido familiar de la voz humana es una señal acústica extremadamente compleja [5]. Y esto de esperarse, ya que la señal eléctrica la cual resulta a partir de un micrófono es también muy compleja.

En la Fig.2.1, se muestra un espectro típico de voz. Una observación muy importante, es que la Densidad de Potencia cae rápidamente para componentes de frecuencia mucho mayores que 3.5 Khz y menores que 300 Hz. Consecuentemente las mismas componentes de frecuencias altas contribuyen muy poco a la reconstrucción de la señal de voz.

Esta observación es importante por lo siguiente, podemos considerar como una señal de voz a aquellas señales que se encuentran en el intervalo entre 300 a 3300 Hz. Esto es importante para la reproducción de una señal de voz, ya que nos interesa las señales que están dentro de este intervalo. El diseñador de un cifrador de voz necesita ser capaz de poder reconstruir la señal de voz en el receptor a partir de este intervalo de frecuencia.

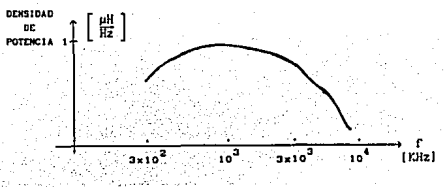



Fig.2.1 Espectro típico de voz ([6], fig. 2.17).

Las características principales de una señal de voz son ([7], pag. 33) :

-- Potencia de la voz.
-- Espectro de frecuencia de la voz.
-- Frecuencia fundamental de voz.

1.) Potencia de la voz ([7], pag. 31).

El nivel efectivo promedio de tiempo largo varía dependiendo de cada individuo, así como también de las condiciones de pronunciación. En un medio ambiente tranquilo, un valor promedio

efectivo de tiempo largo de una medición de voz a partir de diferentes individuos es aproximadamente de 58.2 dB. La distribución de un nivel efectivo promedio para voces de hombres y mujeres es aproximadamente gaussiano, con una desviación estandar de aproximadamente 3.8 dB.

2.) Espectro de frecuencia de la voz ([7], pag. 33).

Las componentes de voz también cambian continuamente, de acuerdo a la intensidad de la voz. Un espectro en frecuencia promedio de tiempo largo se realiza a partir de la medición del nivel de energía en cada banda por medio de un banco de filtros paso bajas (FPB) cubriendo el rango de frecuencias por completo de una señal de voz. El espectro promedio de tiempo largo de individuos japoneses (hombres y mujeres) se muestra en la Fig.2.2. La sola diferencia entre las voces de un hombre y una mujer aparecen en la banda de las frecuencias bajas que es aproximadamente 0.13Khz, donde la energía de la voz de la mujer es casi nula. Una medición similar de voces de Mujer y Hombres americanos también se muestra en dicha figura.

En esta figura, las componentes de frecuencia menores que 0.8 khz ocupan al menos el 80% de toda la energía. De esta manera, se obtiene un espectro aproximado, usando un espectro plano hasta 0.8 Khz y con una pendiente de -10dB/oct a partir de 0.8 Khz.

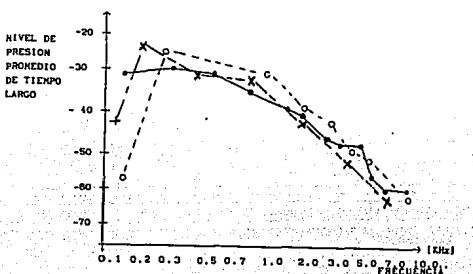



Fig.2.2. Espectro de frecuencia de voz : (x--) Mujer Americana, (*--)Hombre japonés, (o--)Mujer Japonesa ([7], fig.3.3).

3.) Frecuencia fundamental de voz ([7], pag. 34).

Un forma de onda consiste de dos partes: la parte de ruido (noiselike), en el cual la amplitud varía aleatoriamente, y la parte periódica, la cual se repite al menos la misma forma de onda ciclicamente. El periodo repetitivo es llamado un periodo fundamental y el recíproco de el periodo es llamado la frecuencia

fundamental. La forma de onda de la señal de voz, produce componentes de frecuencia en relación a todas las armonicas; Las frecuencias bajas representan la frecuencia fundamental que corresponde a las vibraciones de las cuerdas vocales.

La frecuencia fundamental de las formas de onda en una conversación, varía de una forma continua y lenta en el tiempo. La desviación promedio y estandar para diferentes individuos se muestra en la Fig.2.3. La desviación para una voz femenina es cuando mucho dos veces mayor que la de la voz de un hombre.

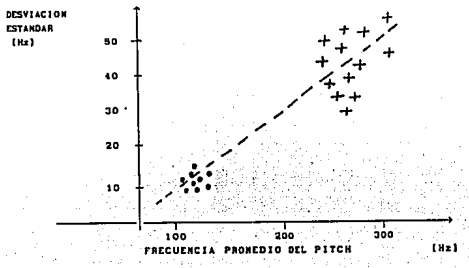



Fig.2.3 Media y Desviación estandar de la frecuencia del pitch de voz: (*) Hombre ,(x) Mujer ([7], fig.3.4).

### II.3.3 Señales de Video.

Los sistemas de televisión, son sistemas de transmisión de imágenes, con un mensaje patrón bidimensional, y por lo tanto, función de dos variables. Los sistemas televisivos [1] se basan en el traslado de una escena, a una serie de pequeños puntos llamados pixeles, los cuales se obtienen al barrer sucesivamente una imágen con un haz de electrones con intensidad modulada por el brillo relativo de la imágen. Como resultado, se obtiene una variación de voltaje proporcional al brillo instantáneo, siendo este voltaje función de la variable tiempo **t**.

Para que la transmisión de imágenes se realice de manera satisfactoria, un sistema de televisión requiere adquirir y reproducir fielmente ciertas características de los objetos observados como son : su forma, brillo relativo, movimiento, sonido y color.

En el mundo actual existen varias normas para la transmisión de televisión, cada una con sus propias características e incompatibilidades con los demás sistemas, siendo los principales

el norteamericano y el europeo. El sistema norteamericano emplea para las transmisiones en blanco y negro la norma FCC (Federal Communications Commission) y para color la norma NTSC (National Television Standars Committe) ver tabla 2.1. En México el sistema utilizado es el norteamericano.

| | |
|---|---|
| Ancho de banda del canal de transmisión | 6.0 Mhz |
| Ancho de banda de la señal de video | 4.2 Mhz |
| Desviación de audio en FM | 25.0 Khz |
| Localización de la portadora de imágen | 11.25 Mhz desde el extremo inferior |
| Localización de la portadora de color | 3.58 Mhz desde la portadora de imagen. |
| Relación de aspecto | 4/3 |
| Líneas de barrido | 525 por cuadro |
| Entrelazado | 2 :1 |
| Frecuencia de barrido vertical | 15.75 KHz |
| Frecuencia de barrido horizontal | |
| Tiempo de línea | 63.5. µseg. |
| Tiempo de retrazo horizontal | 10.0 µseg. |

Tabla 2.1 Norma NTSC ([2], Tabla C.1).

Finalmente el ancho de banda del canal para la norma NTSC es de 6 Mhz (ver Fig. 2.4).

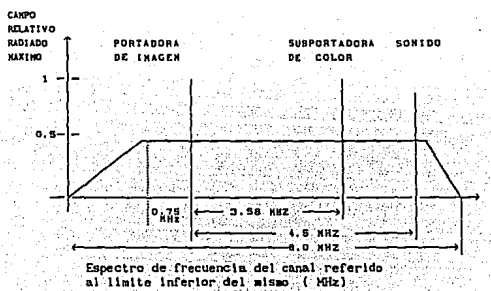



Fig. 2.4 Espectro de la Señal de Video NTSC ([2], fig. C.6).

## II.4 REPRESENTACION DE LOS SISTEMAS DISCRETOS LINEALES INVARIANTES EN EL TIEMPO.

Para modelar un fenómeno físico, biológico, económico, etc., se usan las nociones de señales y sistemas [4]. Un sistema se puede definir como un conjunto de elementos inter-relacionados entre sí que responden a una excitación (señal de entrada) con una respuesta (señal de salida), como se ve en la Fig.2.5, donde las señales de entrada y salida son funciones del tiempo discreto, n.

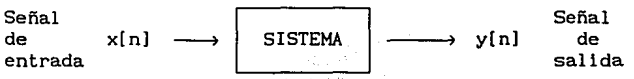



Fig. 2.5 Representación de un fenomeno por medio de señales y sistemas

La relación entre las señales x[n] y y[n] con el sistema se puede escribir como :

$$\mathbb{T}\{ x[n] \} = y[n] \qquad (2.2)$$

donde $\mathbb{T}\{ x[nt] \}$ es la transformación ocurrida a la señal de entrada por la acción del sistema.

Como ejemplos de señales podemos mencionar señales de voz, audio, imágenes, radar, bioeléctricas, etc. y entre las transformaciones que pueden sufrir están la eliminación del ruido y distorsiones, la modificación (corrección) de características de una señal, etc.

Finalmente, consideramos cualquier sistema como : Discreto lineal e Invariante en el tiempo si cumple con :

Un sistema es discreto en el tiempo cuando sólo reciba entradas y genera salidas en ciertos momentos (por ejemplo en ciertas horas, cada segundo, etc.)

Un sistema es lineal cuando cumple las propiedades de superposición y escalonamiento ;

-- Superposición $\mathbb{T}\{a_1x_1[n]+a_2x_2[n]\} = a_1\mathbb{T}\{x_1[n]\} + a_2\mathbb{T}\{x_2[n]\}$
-- Escalonamiento $\mathbb{T}\{a_1x[n]\} = a_1y[n]$

donde $x_1[n]$, $x_2[n]$ son señales de entrada, y
$a_1$, $a_2$ son constantes.

Un sistema es causal, si su salida para todo instante de tiempo **n**, depende únicamente de los valores de la entrada en instantes presentes y pasados.

Un sistema es invariante en el tiempo cuando

$$T\{x[n-\tau]\} = y[n-\tau]$$

para cualquier $\tau$. Es decir, un corrimiento en el tiempo a la entrada resulta en un corrimiento igual a la salida.

### II.4.1 Representación de un Sistema en el Dominio del Tiempo.

En la Fig.2.6 se muestra la representación de un sistema discreto donde x[n] es la señal discreta de entrada, y[n] es la señal discreta de salida y a h[n] se le llama respuesta al impulso del sistema [4]. Las letras "sombreadas" indican otra manera de representar la señal en el dominio de la frecuencia (ver sección II.4.2).

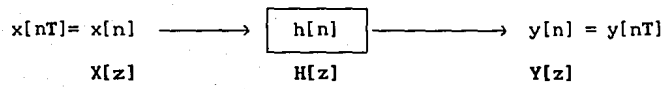



Fig.2.6 Sistema discreto (representación en Tiempo y en Frecuencia) ([3], fig. 1.9).

donde h[n] es la respuesta del sistema a una señal $\delta[n]$ (impulso discreto) definida como :

$$\delta[n] = \begin{cases} 1, & n = 0 \\ 0, & n \neq 0 \end{cases} \qquad (2.3)$$

Por lo tanto, la respuesta de un sistema discreto, lineal e invariante en el tiempo a cualquier entrada x[n] es :

$$y[n] = \sum_{l=-\infty}^{\infty} x[l]h[n-l] = \sum_{l=-\infty}^{\infty} x[n-l]h[l] = x[n]*h[n] \qquad (2.4)$$

donde a x[n]*h[n] se le llama convolución entre x y h. Es decir, la salida de un sistema discreto, lineal e invariante en el tiempo es igual a la convolución de la señal de entrada con la respuesta al impulso del sistema.

## II.4.2 Representación de un Sistema en el Dominio de la Frecuencia.

Otra manera de representar la relación entre señales de entrada, salida y sistema, es en el dominio de la frecuencia como se puede ver en la Fig.2.6 (letras sombreadas).

En el caso discreto, se define la transformada Z de una señal como:

$$Z\{x[n]\} = \sum_{n=-\infty}^{\infty} x[n]Z^{-n} = X(Z) \qquad (2.5)$$

y la Transformada Discreta de Fourier (TDF), ver sección II.6 como:

$$F\{x[n]\} = \sum_{n=-\infty}^{\infty} x[n]\, e^{-j2\pi nkT/N} = X[k] \qquad (2.6)$$

donde **T** es el periodo de muestreo y **N** es el número de muestras que se tienen.

Por medio de estas transformaciones, se puede trasladar el problema al dominio de la frecuencia. La ventaja es que en este dominio, según el teorema de convolución [3], la respuesta puede expresarse como :

$$Y(z) = X(z)H(Z) \qquad (2.7)$$

Es decir, una convolución en el tiempo, ecuación (2.4), equivale a una multiplicación en frecuencia, ecuación (2.7), lo que facilita los cálculos. Otra definición importante es la función de transferencia de un sistema, que representa la relación entre la señal de salida y la señal de entrada en el dominio de la frecuencia, la cual está dada por :

$$H(Z) = \frac{Y(Z)}{X(Z)} = Z\{h[k]\} \qquad (2.8)$$

## II.5 FILTROS DIGITALES.

En el Procesamiento Digital de Señales (PDS) se requiere muchas veces transformar una señal de acuerdo con ciertas especificaciones (por ejemplo eliminación de un rango de frecuencias). Esto se hace por medio de filtros digitales. El término filtro se usa para describir un sistema que puede realizar cualquiera de las tres siguientes operaciones [8]:

1. Filtrado, que significa la extracción de la información de una señal a partir de otra señal.

2. Suavizado (smoothing), que difiere con el filtraje en que la cantidad de interés no necesita estar disponible al tiempo, t (hay un retraso al producir el resultado de interés).

3. Predicción, que consiste en derivar información acerca de la cantidad de interés a un tiempo $t+\tau$ usando datos medidos hasta ese tiempo t.

## II.5.1 Clasificación de Filtros Digitales relacionados mediante su Función de Transferencia.

Existen 2 tipos importantes de filtros [9] :

Filtros RIF (Respuesta Impulso Finita), en los que la respuesta al impulso (h[n]) del filtro es finita. Es decir, si x[n] es la entrada al filtro y y[n] es la señal de salida, a partir de la ecuación (2.4) :

$$y[n]= \sum_{l=0}^{p} h[l]x[n-l] = \sum_{l=0}^{p} a[l]x[n-l] \qquad (2.9)$$

donde a **p** se le llama orden del filtro.

Filtros RII (Respuesta Impulso Infinita), en los que la respuesta al impulso del filtro es infinita.

$$y[n] = \sum_{l=0}^{\infty} h[l]x[n-l] \qquad (2.10)$$

Una manera de eliminar la sumatoria infinita de la ecuación (2.10) es con una ecuación de recurrencia, en la que los valores de y[n] se hacen dependientes de los valores de y[n-1], los valores de y[n-1] dependientes de los valores de y[n-2] y así sucesivamente, por lo que en lugar de la ecuación (2.10) podríamos escribir :

$$y[n] = \sum_{l=0}^{p} a[l]x[n-l] - \sum_{l=1}^{q} b[l]y[n-l] \qquad (2.11)$$

donde a **a[l]** y **b[l]** se les llama coeficientes del filtro y **p** y **q** son los órdenes del filtro.

De esta manera, las funciones de transferencia de los dos tipos de filtro quedarían como sigue:

RIF $$H(Z) = Z\{h[n]\} = \sum_{n=0}^{p} a[n]z^{-n} \qquad (2.12)$$

$$\text{RII} \qquad H(Z) = \frac{Y(Z)}{X(Z)} = \frac{\sum_{n=0}^{p} a[n]z^{-n}}{1 + \sum_{n=1}^{q} b[n]z^{-n}} \qquad (2.13)$$

## II.5.2 Clasificación de Filtros Digitales relacionados mediante su realización física.

Hay 2 tipos importantes de filtros (en cuanto a su estructura física); Tranversales y en Escalera ("lattice" en inglés).

### II.5.2.1 Filtros Transversales.

Un filtro transversal es un dispositivo cuya salida se forma como una combinación lineal de valores derivados en etapas [9] ("Taps") retardadas en el tiempo.

La realización de un filtro transversal de respuesta al impulso infinita se basa en los coeficientes de a[1] y b[1] de la ecuación (2.11). La llamada forma directa I se muestra en la Fig.2.7. En este tipo de estructura [9] se necesitan p+q elementos de retraso ($z^{-1}$) que equivalen a otras tantas localidades de memoria para guardar los valores pasados de x[n] o y[n].

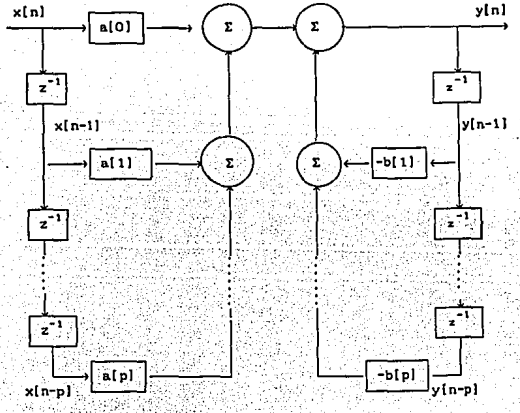



Fig.2.7 Forma directa I de un Filro RII ([36], fig. 7.13).

El lado izquierdo de la Fig.2.7 representa Σa[1]x[n-1] y el lado derecho Σb[1]y[1-n]. La resta de las dos dá y[n] (ver ecuación (2.11)).

La forma directa II o forma canónica requiere max(p,q) unidades de retraso como se muestra en la Fig.2.8.

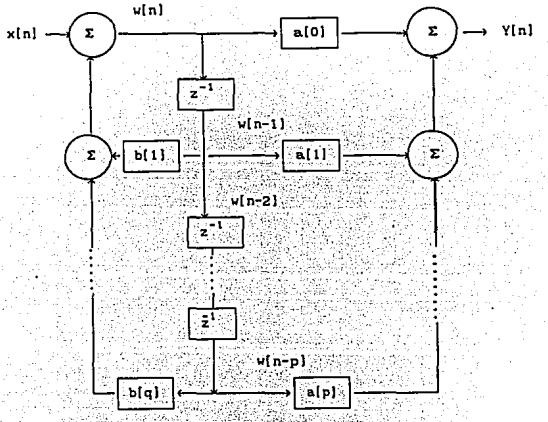



Fig. 2.8 Forma Directa II. Realización canónica de un filtro RII ([36], fig. 7.14).

En este tipo de estructura se utiliza una variable intermedia w[n] cuya relación con x[n] y y[n] es la siguiente:

$$y[n] = -\sum_{l=0}^{q} b[l]w[n-l]$$

$$w[n] = \sum_{l=1}^{p} a[l]w[n-l]+x[l]$$

Cuando los órdenes del filtro en forma directa (**p** y **q**) son grandes, la precisión de las variables que intervienen debe ser grande, es decir, se les debe asignar un gran número de bits a los coeficientes del filtro y a los resultados del filtro de las multiplicaciones. De otra manera, los resultados del filtro no serían tan exactos.

Para evitar estas imprecisiones, hay otras formas no directas de implementar filtros digitales : en cascada y en paralelo.

En la forma de cascada, un filtro de orden grande con función de transferencia H(z) se factoriza en filtros de orden menor (generalmente de orden 2) :

$$H(z) = \prod_{i=1}^{N} H_i(z)$$

y

$$H_1(z) = \frac{A_{01} + A_{11} z^{-1}}{1 + B_{11} z^{-1} + B_{21} z^{-2}}$$

El diagrama a bloques se muestra en la Fig.2.9.

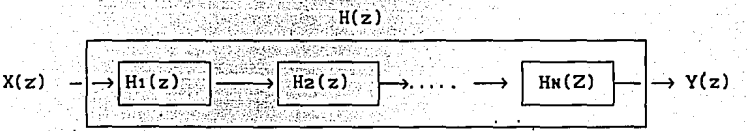



Fig.2.9 Filtros en Cascada ([36], fig. 7.20).

En la forma paralelo, H(z) se descompone en una suma de funciones de transferencia obtenidas por fracciones parciales:

$$H(z) = \sum_{i=1}^{N} H_i(z) + C$$

donde C es una constante y

$$H_1(z) = \frac{A_{01} + A_{11} z^{-1}}{1 + B_{11} z^{-1} + B_{21} z^{-2}}$$

El diagrama a bloques se muestra en la Fig.2.10.

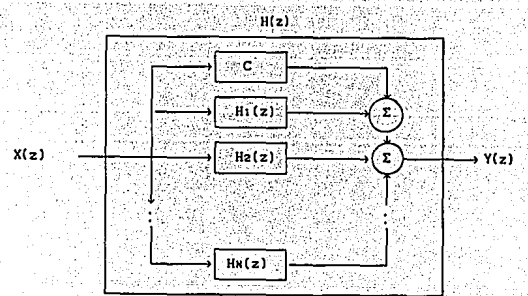



Fig.2.10 Filtro en Paralelo ([36], fig. 7.21).

El error debido a la precisión en estos filtros es menor (para órdenes grandes) al de los implantados en forma directa. La magnitud de este error depende de las factorizaciones hechas, del orden en que se ponen las funciones de transferencia $H_i(z)$ y del acoplamiento entre el numerador y denominador de cada función.

### II.5.2.2 Filtros en Escalera ("lattice") .

Estos filtros combinan los llamados errores directos y retrógrados [8] $E^f[n]$ y $E^b[n]$ en una sola estructura mostrada en la Fig.2.11 (para un filtro RIF).

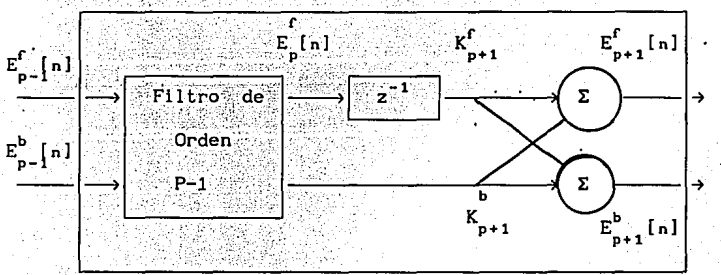



Fig.2.11 Filtro en escalera (" Lattice") de orden p.

Estos filtros son recursivos en orden. Si se quiere hacer un filtro de orden **p** se necesita un filtro de orden p-1, un elemento de retrazo $z^{-1}$ y los coeficientes de reflexión [12] $K^b$ y $K^f$. La ventaja de estos filtros es que son numéricamente estables (dado que los coeficientes de reflexión son menores a $\mp 1$ y son modulares (a partir de un filtro de orden **p**, es decir, se puede construir un filtro de orden **p+1** a partir de un filtro de orden **p**, y así sucesivamente, ver sección II.7.2).

## II.6 TRANSFORMA DE FOURIER.

Muchas veces es conveniente expander una secuencia de duración finita en una serie discreta de Fourier [10]. La expansión que se obtiene es una secuencia de duración finita. Tal representación se conoce como la transformada Discreta de Fourier **DFT** (de las siglas en inglés) [9] de la secuencia. De esta manera, si x[n] es una secuencia definida solamente sobre el intervalo definido a partir de 0 hasta N-1, la **DFT** X[k], de **x**[n] es definida en el intervalo de 0 hasta N-1 por ([9], ec. 6.11) :

$$X[k]=\sum_{n=0}^{N-1} x[n]\exp(-jkw_0n) \quad 0\le k\le N-1 \qquad (2.14)$$

donde $w_o = 2\pi/N$.

La inversa de la Transformada Discreta de Fourier **IDFT** (de las siglas en inglés) [9] de la secuencia X[k], esta dada como una secuencia **x**[n] definida en el intervalo de 0 hasta N-1 por ([9], ec. 6.12):

$$x[n] = \frac{1}{N} \sum_{k=0}^{N-1} X[k]\exp(jkw_0n) \qquad (2.15)$$

Las ecuaciones (2.14) y (2.15) constituyen el par de Transformadas Discretas de Fourier y algunas veces son reescritas en términos de $W_N$ como sigue ([9], pag. 263) :

$$X[k]=\sum_{n=0}^{N-1} x[n]\, W_N^{kn} \qquad 0 \le k \le N-1 \qquad (2.16)$$

$$x[n]= \frac{1}{N} \sum_{k=0}^{N-1} X[k]W_N^{-kn} \qquad 0 \le n \le N-1 \qquad (2.17)$$

donde $W_N= \exp(-j2\pi/N)$

Si se considera x[n] para valores complejos, la ecuación (2.16) puede reescribirse en términos de su parte real como imaginaria de la siguiente manera ([9], ec. 6.20) :

$$X[k]=\sum_{n=o}^{N-1}\left\{ Re[x[n]] + j\ Im[x[n]]\right\}\ \left\{ Re[W_n^{kn}] +j[\ Im[W_n^{kn}]\right\}$$

$$= \left\{ \sum_{n=o}^{N-1} Re[x[n]]xRe[W_N^{kn}] - \sum_{n=o}^{N-1} Im[x[n]xIm[W_N^{kn}] \right\}$$

$$+j\left\{\sum_{n=o}^{N-1} Re[x[n]]xIm[W_N^{kn}] + \sum_{n=o}^{N-1} Im[x[n]Re[W_N^{kn}]\right\}$$

## II.6.1 Transformada Rápida de Fourier.

Existen muchos métodos para reducir el número de multiplicaciones y el número de adiciones en el cálculo de la DFT. La técnica más importante es la de Cooley-Turkey y se basa en la descomposición de la transformada en pequeñas transformadas para una conocida transformada total. Cooley-Tukey demostraron que la decimación se puede realizar tanto en el dominio del tiempo como en el dominio de la Frecuencia [10].

En esta sección presentamos la decimación en el tiempo y suponemos que el número de puntos es una poténcia de 2, esto es, $N = 2^v$. Esta decimación en el tiempo consiste en dividir la transformada de N-puntos en dos transformadas de (N/2) puntos, luego divididiendo cada transformada de N/2 puntos en dos transformadas de N/4 puntos, y continuando este proceso hasta obtener transformadas de dos puntos.

Dada una secuencia, x[n], definida como :

$x[n] = x[0]x[1]x[2]...x\left[\frac{N}{2}-1\right]...x[(N-1]$, y donde la secuencia par ( índice par) es : x[0]x[2]x[4]...x[N-2] , y la secuencia impar (índice impar) es : x[1]x[3]x[5]...X[N-1].

A partir de la definición de la DFT, ecuación (2.16), la sumatoria es representada en dos partes, una para el índice par y otra para el índice impar, por lo que tenemos :

$$X[k]=\sum_{\substack{n=0\\ n=par}}^{N-2} x[n]\, W_N^{kn} + \sum_{\substack{n=1\\ n=impar}}^{N-1} x[n]\, W_n^{nk} \qquad (2.18)$$

En la ecuación (2.18), si colocamos n = 2r en la primera sumatoria y n = 2r + 1 en la segunda sumatoria, entonces la ecuación (2.18) se puede escribir como ([9], ec. 6.22) :

$$X[k] = \sum_{r=0}^{N/2-1} x(2r)W_N^{2rk} + \sum_{r=0}^{N/2-1} x(2r+1)W_n^{(2r+1)k} \qquad (2.19)$$

Reagrupando cada parte de X[k] en dos transformadas de N/2 puntos, y usando

$$W_N^{2rk} = \left[W_N^{2}\right]^{rk} = \exp(-j\,\frac{2\pi}{N}\,2rk) = \exp(-j\,\frac{2\pi}{N/2}\,rk) = W_{N/2}^{rk}$$

Entonces la transformada de Fourier de x[n] esta dada como sigue([9], ec. 6.24) :

$$X[k] = \sum_{r=0}^{N/2-1} x(2r) W_{N/2}^{rk} + Wn \sum_{r=0}^{N/2-1} x(2r+1) W_{N/2}^{rk}$$

DFT de N/2 puntos de la secuencia indexada par

DFT de N/2 puntos de la secuencia indexada impar.

Si G[k] y H[k] representa la DFT de N/2 puntos de la secuencia indexada par e impar, entonces X[k] puede reescribirse para k = 0 hasta N/2-1 como ([9], ec. 6.25a) :

$$X[k] = G[k] + W_N^k H[k] \quad k = 0,1,..,N/2-1 \qquad (2.20)$$

Este es el primer paso en la decimación de la transformada en dos transformaciones de N/2 puntos como se muestra en la Fig.2.12.

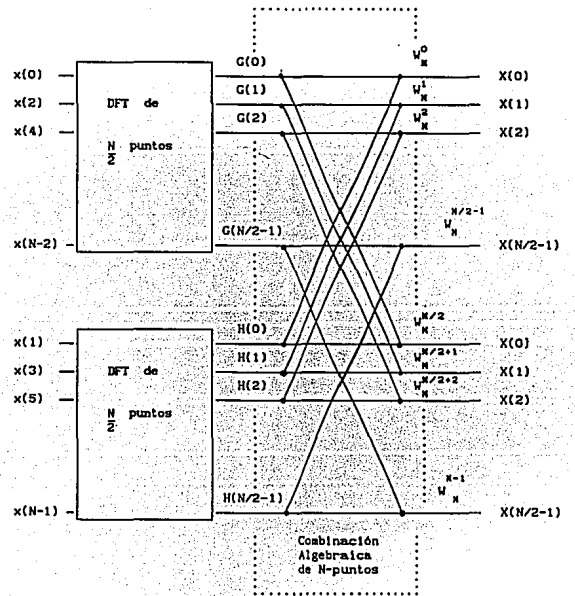



Fig. 2.12 Primera etapa de la descomposición para la decimación en el tiempo para la Transformada de Fourier Rápida ([9], fig. 6.5).

En la evaluación de la ecuación (2.20) para k = N/2 hasta N, G[k] y H[k] se consideran periódicas con período N/2; Por lo tanto, para k ≥ N/2, X[k] es conocida por ([9], ec. 6.25b) :

$$X[k] = G[k-N/2] + W_N^k \, H[k-N/2] \qquad \text{para } N/2 \le k \le N-1$$

Cada una de las secuencias de N/2 puntos genera dos secuencias de longitud N/4 como se muestra en la Fig.2.12. Cada una de las combinaciones algebraicas son gobernadas por la siguiente ecuación, asumiendo la periocidad necesaria de G[k] y H[K] ([9], ec. 6.26) :

$$X[k] = G'[k] + W_{N/2}^k \, H'[k] \qquad k = 0,1,..,N/2-1$$

$$= G'[k] + W_N^{2k} \, H'[k]$$

Continuando con este proceso cada transformada de N/4 puntos se divide en dos DFT de (N/8) puntos, etc., este proceso puede continuarse hasta que exista v o $\log_2$ N etapas como se muestra en la Fig.2.13.

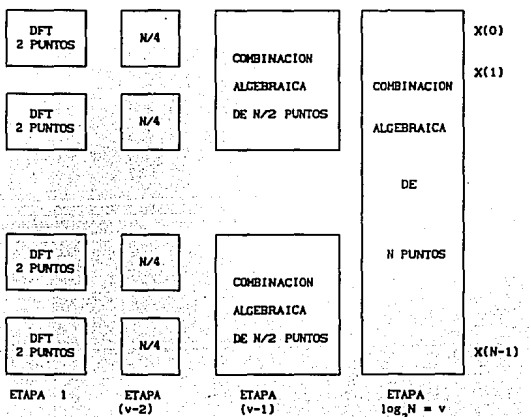



Fig. 2.13 Descomposición Conceptual final para la decimación en el tiempo FFT ([9], fig. 6.7).

A partir de la Fig.2.13, se pueden realizar varias observaciones importantes.

1.) La entrada de datos puede ser camufleada. El dato de entrada aparece en el orden llamado "bit reverse", ilustrado abajo para N = 8.

| Posición | Patrón de bits de la secuencia | Bit inverso | Indice de la secuencia |
|---|---|---|---|
| 0 | 000 | 000 | 0 |
| 1 | 001 | 100 | 4 |
| 2 | 010 | 010 | 2 |
| 3 | 011 | 110 | 6 |
| 4 | 101 | 001 | 1 |
| 5 | 101 | 101 | 5 |
| 6 | 110 | 011 | 3 |
| 7 | 111 | 111 | 7 |

2.) El bloque básico computacional de cálculo en el diagrama se llama "mariposa" (ver Fig.2.15).

Si se usa *m* para representar la *m*-enésima etapa, y **a p y q** para representar la posición de los números en la etapa *m*, cada mariposa en la Fig.2.13, puede ser representada como se muestra en la Fig.2.14.

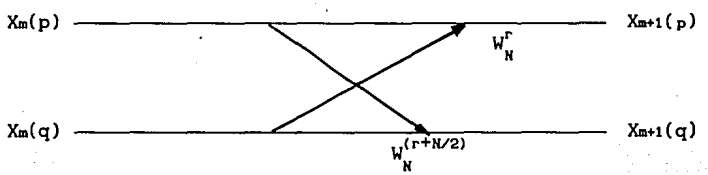



Fig.2.14 Mariposa de 2 puntos ([9], fig. 6.9).

donde

$$X_{m+1}(p) = X_m(p) + W_N^r X_m(q)$$

$$X_{m+1}(q) = X(p) + W_N^{r+N/2} X_m(q)$$

La potencia, r, de $W_n$ es variable y depende hasta la última posición de la mariposa. También notamos que $X_{m+1}(p)$ y $X_{m+1}(q)$, son las salidas de la mariposa en la etapa m+1, éstas se calculan en términos de Xm(p) y Xm(q), el valor correspondiente a la m-enésima etapa, y no de las otras entradas.

### II.6.2 Espectro de Frecuencia.

Generalmente, X[k] es una función compleja. Esta función se escribe en forma de su parte real e imaginaria como :

$$X[k] = Re[X[k] + jImX[k]]$$

En el caso de una señal real x[n], las partes real e imaginaria de X[k] son respectivamente conocidas por :

$$Re = [X[k]] = \sum_{n=-\infty}^{\infty} x[n]\cos 2\pi ft$$

y

$$Im = [X[k]] = -\sum_{n=-\infty}^{\infty} x[n]\text{sen } 2\pi ft$$

Las ecuaciones anteriores se pueden escribir en función de su Amplitud y de su Fase de la siguiente manera :

$$X[k] = | X[k] | e^{j\arg[X(k)]}$$

El factor X[k], es llamado espectro de amplitud, y expresa la distribución en frecuencia de la magnitud de x[n]. El factor $\Theta_x[k] = \arg[X[k]]$, es llamado el espectro de fase y contiene la distribución de frecuencia de la fase de x[n]. Finalmente, el factor $| X[k] |^2$ es llamado el espectro de energía que representa la distribución en frecuencia de la energía de x[n]. Y esto se denota por $\Phi_x[k]$.

## II.7 TECNICAS DE ESTIMACION PARAMETRICA.

### II.7.1 Codificación por Predicción Lineal.

Un problema importante en el área de las comunicaciones es el de utilizar un canal de la mejor manera posible. Una manera de hacer esto es "comprimiendo" la información a mandar y después "restaurando" la señal en el receptor. En el caso de la voz humana, esto se hace generalmente con el método llamado **LPC** (de las siglas en inglés) [12]. Recientemente, la técnica de predicción lineal es usada para el análisis y síntesis de señales de voz.

El método LPC consiste en que el valor presente de la muestra de una señal de voz s[n] puede ser predecible a partir una sumatoria ponderada de sus valores previos, es decir,

$$s[n] = a_1 s[n-1] + a_2 s[n-2] + a_3 s[n-3] + \ldots + a_p s[n-p]$$

Esto se puede escribir como :

$$\hat{s}[n] = \sum_{k=1}^{p} a[k]\ s[n-k] \qquad (2.21)$$

donde las a[k] son los coeficientes del filtro.

De esta manera un predictor de orden p, requiere p parámetros ai's y las últimas p muestras de la señal de voz.

En la Fig.2.15 se muestra un Sistema de Análisis y Síntesis de señales de voz basado en el método LPC [13]. La sección del analizador, consiste de un muestreador para señales de voz, s[n]. La función principal del analizador, es extraer un conjunto de parámetros a[k], los cuales proporcionan información de la señal de voz, así como de la energía de una *trama* particular de voz previamente analizada. En esta etapa también se extrae el período del pitch, además de realizar una decisión entre sonidos de voz ("voiced") y sonidos de no voz ("novoiced") para una *trama* particular de voz.

En la sección del sintetizador, se realiza la síntesis de la señal de voz a partir de los coeficientes de predicción a[k], el período del pitch y de una factor de ganancia G.

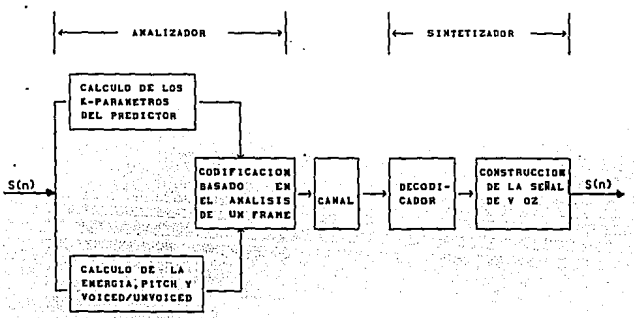



Fig.2.15 Sistema de Análisis y Síntesis de voz.

En la Fig.2.16 se presenta la etapa del sintetizador más detallada para la síntesis de señales de voz. El modelo consiste de un filtro que es excitado ya sea por un tren periódico de impulsos o por una fuente de ruido. La fuente periódica produce sonidos "de voz" ("voiced") como las vocales y sonidos nasales, y la fuente de ruido produce sonidos "no de voz" ("unvoiced" o "fricativo") tales como las producidas al pronunciar las letras f, s, sh.

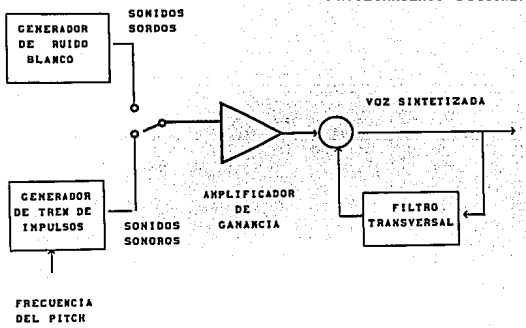



Fig.2.16 Modelo LPC de la Síntesis de Señales voz ([12],fig.5.1).

Existen dos casos de interés especial :

1. Modelo de ceros : $a(k) = 0$ $\quad 1 \leq k \leq p$
2. Modelo de polos : $b(l) = 0$ $\quad 1 \leq l \leq q$

El modelo de ceros se conoce como movimiento promedio (**MA**), y el modelo de polos como autoregresivo (**AR**).

Este último modelo es el más empleado, debido a que el problema se reduce a encontrar los coeficientes a[k]. El cálculo de los coeficientes a[k], se lleva a cabo resolviendo un sistema algebráico de ecuaciones lineales, dicho sistema de ecuaciones depende de la entrada y la salida de la función de transferencia del sistema.

Aquí explicaremos el modelo de sólo polos, debido a que es el modelo que se utilizará en la síntesis de voz (ver sección **IV.5.2**). El filtro generalmente se supone sólo con polos ("all-poll model") o modelo auto-regresivo (AR) de tal manera que ([13], ec.4) :

$$s[n] = -\sum_{k=1}^{p} a[k]s[n-k] + Gu[n] \qquad (2.22)$$

donde G es un factor de ganancia y la función de transferencia del filtro mostrado en la Fig.2.16 es ([13], ec.5):

$$H(Z) = \frac{G}{1 + \sum_{k=1}^{p} a[k]\, z^{-k}}$$

Dada una señal particular s[n], el problema consiste en determinar a[k] y G de tal manera que $\Sigma|e[n]|^2$ sea mínimo [13], donde e[n] representa el error en el tiempo n dado por :

$$e[n] = s[n] - \hat{s}[n] = s[n] + \sum_{k=1}^{p} a[k]\, s[n-k] \qquad (2.23)$$

Encontrando $\frac{\partial Error}{\partial a[k]}$ e igualando a cero se obtiene las ecuaciones :

$$\sum_{k=1}^{p} a[k]\ R[i-k] = -\ R(i)$$

llamadas, las ecuaciones "normales" donde R[i] es la función de autocorrelación de s[n]. La solución de estas ecuaciones está dada por las funciones de recurrencia de Durbin (ver sección II.7.2).

De esta manera, en lugar de tener muestras de 10 milliseg. de voz, se tendrán $p$ parámetros (generalmente $p$ = 10), 1 bandera (para saber si se tratan de sonidos de voz "voiced" o no voz "unvoiced"), un factor de ganancia G y un periodo de "pitch".

Para la estimación de los parámetros a[k] de una señal de voz s[n], utilizando la función de transferencia H[z], se emplean los siguientes métodos : Método de Mínimos cuadrados y el Método de autocorrelación.

A. Método de mínimos cuadrados ([13], pag.7).

Este método asume que la entrada u[n] es desconocida, lo cual es cierto en muchas aplicaciones, con esto se tiene que la señal s[n] es una aproximación lineal de los valores anteriores de s[n] y está dada por ([13], ec.6):

$$\hat{s}\,[n] = -\sum_{k=1}^{p} a[k]\ s[n-k]$$

Entonces el error entre valor actual s[n] y el valor predecible s[n] está dado por ([13], ec.7) :

$$e[n] = s[n]-\hat{s}\,[n] = s[n] + \sum_{k=1}^{p} a[k]s[n-k]$$

En este método, los coeficientes a[k] se obtienen al minimizar la suma de los errores al cuadrado, para cada uno de los parámetros a[k]. El análisis puede realizarse, suponiendo a la señal s[n], como : a.) Determinística, b.)Una realización de un proceso aleatorio.

a.) Señal Determinística.

Para el caso donde la señal s[n] es determinística, el valor medio cuadrático está dado por ([13], ec. 8) :

$$E = \sum_{n} e^2[n] = \sum_{n} \left[e[n] + \sum_{k=1}^{p} a[k]s[n-k]\right]^2 \qquad (2.24)$$

minimizando E se tiene $\dfrac{\partial E}{\partial a[i]} = 0$ para $1 \le i \le p$

de donde se obtiene ([13], ec. 10) :

$$\sum_{k=1}^{p} a[k] \sum_{n} s[n-k]s[n-i] = -\sum_{n} s[n]s[n-i] \qquad 1 \le i \le p \qquad (2.25)$$

este sistema se conoce como *ecuaciones normales*.

El mínimo error cuadrático total, denotado por $E_p$, se obtiene al desarrollar las ecuaciones (2.24), sustituyendo el resultado en la ecuación (2.25) se obtiene la siguiente expresión ([13], ec.11) :

$$Ep = \sum_{n} s[n]^2 + \sum_{k=1}^{p} a[k] \sum_{n} s[n]s[n-k]$$

B. **Método de Autocorrelación** ([13], pag.7).

Para el caso donde la señal s[n] es un proceso aleatorio, el error se minimiza en el rango de duración infinita $-\infty < n < \infty$, y las ecuaciones (2.24) y (2.25) se reducen a :

$$\sum_{k=1}^{p} a[k]R[i-k] = -R[i] \qquad 1 \le i \le p \qquad (2.26)$$

$$Ep = R[0] + \sum_{k=1}^{p} a[k]R[k] \qquad (2.27)$$

donde

$$R[i] = \sum_{n=-\infty}^{\infty} s[n]s[n+i]$$

que es la autocorrelación de la señal s[n]. Note que la senal R[i] es una función par de *i*, es decir, R[-i] = R[i].

En la práctica, la señal s[n] se conoce sólo durante un intervalo finito, si nuestro interés es analizar un intervalo menor de la señal, esto se realiza por la multiplicación de la señal s[n] por una ventana w[n], con lo cual se obtiene una nueva señal s[n] que es igual a cero fuera de un intervalo $0 \le n \le N-1$, como se define a continuación :

$$\hat{s}[n] = \begin{cases} s(n)w(n) & 0 \leq n \leq N-1 \\ 0 & C.O.C \end{cases}$$

Con esta señal la función de autocorrelación está dada por ([13], ec. 17):

$$R[i] = \sum_{n=0}^{N-1-i} \hat{s}[n]\,\hat{s}[n+i] \qquad i \geq 0$$

**II:7.2 Algoritmo Levinson-Durbin.**

La recursión Levinson-Durbin permite calcular los coeficientes de un filtro de orden p+1 a partir de un filtro de orden p, además de la potencia del error de predicción $P_p$, resolviendo la ecuación normal aumentada [8].

El cálculo de estos coeficientes se puede realizar de dos maneras ([8], pag. 153) :

1.) A través de un Predictor Lineal Progresivo (**FLP** de las siglas, en inglés), en el cual el conjunto de muestras x[n-1], x[n-2],...,x[n-p] se usan para realizar una predicción de x[n].

$$x[n] = -\sum_{k=1}^{p} a_p[k]x[n-k]$$

donde $a_p$ son los coeficientes de predicción.

2.) Por medio de un Predictor Lineal Regresivo (BLP de las siglas en inglés), en el cual el conjunto de muestras x[n], x[n-1],..,x[n-p-1] se usa para realizar una predicción de x[n-p].

$$x[n-p] = -\sum_{k=0}^{p-1} b_p[k]x[n-k]$$

En ambos casos, la predicción se optimiza a través de la minimización del valor cuadrático medio del error de predicción.

El filtro de escalera ("Lattice") es un método para la implantación de predicción lineal que combina a los filtros de predicción progresiva y los filtros de predicción regresiva en una sola estructura.

La recursión de Levinson-Durbin, se inicia suponiendo que conocemos la solución a un conjunto de ecuaciones normales, para el caso del predictor lineal progresivo de orden **p**, y requerimos utilizarlo para resolver un predictor lineal progresivo de orden **p+1** (es decir, un orden más alto). Si, en verdad tenemos la solución recursiva para ese problema, podemos iniciar con el caso elemental de orden **p** igual a cero, usamos este resultado para calcular la solución para el orden p+1 igual a 1, y continuamos de esta manera hasta alcanzar el valor deseado para el orden del predictor.

Las características de Levinson-Durbin son :

1.) A partir de la siguiente ecuación ([8], ec.7.16) :

$$K_{p+1} = a_{p+1}(p+1) \qquad (2.28)$$

se establece que el último valor de $K_{p+1}$ es simplemente igual al último coeficiente $a_{p+1}(p+1)$ del filtro predictor de error de orden **p** + 1.

2). A partir de la siguiente ecuación ([8], ec.7.15) :

$$P_{p+1} = P_p \quad (1-K^2_{p+1}) \qquad (2.29)$$

donde $P_p$ es la potencia del error de la señal de entrada.

Los valores de $K_{p+1}$ son comunmente conococidos como *los coeficientes de reflexión.* Los valores negativos de $K_{p+1}$ se conocen como *los coeficientes de correlación parcial* (**parcor**). La ecuación (2.29) establece que dados los coeficientes de reflexión $K_{p+1}$ y la potencia promedio del error de predicción progresiva en la salida del filtro de orden **p**, se evalúa la potencia promedio de el error de predicción progresiva en la salida correspondiente del filtro de orden **p+1**. Note que si la potencia promedio de el error de predicción progresiva se decrementa (o al memos es la misma) el orden de la predicción se incrementa, esto es, $P_{p+1} \leq P_p$, entonces requerimos que $|K_{p+1}| \leq 1$ para toda **p**.

3). A partir de la relación recursiva de la ecuación siguiente ([8], ec.7.12).

$$a_{p+1}(m) = a_p(m) \; K_{p+1} a_p(p-m+1) \quad m = 0,1,2,\ldots,p+1 \qquad (2.26)$$

se establece que dados los coeficientes de reflección $K_{p+1}$ y los coeficientes de el filtro de predicción de error de orden **p**, es posible calcular los coeficientes de la correspondiente etapa del filtro predictor de error de orden **p+1**. Esta relación recursiva se llama recursión Levinson-Durbin.

Para iniciar la recursión, iniciamos con el caso elemental de un filtro de predición de error de orden $p = 0$. Si ponemos $p = 0$ en la siguiente ecuación ([8], ec.7.1) :

$$\sum_{m=0}^{p+1} a_{p+1}(m)R_x(m-k) = \begin{cases} P_{f,p+1} & k = 0 \\ 0 & k=1,\ldots, p+1 \end{cases}$$

reconocemos que $a_0(0) = 1$, e inmediatamente calculamos $P_0 = R_x(0)$, donde $R_x(0)$ es la función de autocorrelación del filtro de entrada con un retrazo de cero. Para las condiciones encontradas de la recursión Levinson-Durbin se tiene que

$$a_0(0) = 1$$
$$a_0(1) = 0$$
$$P_0 = R_x(0).$$

4.) El conocimiento de los coeficientes de reflexión $K_1, K_2, \ldots, K_p$ es suficiente para determinar completamente los coeficientes del filtro predictor de error de orden p. Inversamente, dados los coeficientes del filtro predictor de error $a_p(1), a_p(2), .., a_p(p)$ se determinan los coeficientes de reflexión $K_1, K_2, \ldots, K_p$. La recursión inversa Levinson-Durbin queda establecida como ([8], ec.7.18) :

$$\left\{K_1 K_2 K_3, \ldots, K_p\right\} \Leftrightarrow \left\{a_p(1),\ a_p(2), \ldots, a_p(p)\right\} \qquad (2.31)$$

5.) Para una entrada estacionaria, la potencia promedio del error de predicción para un predictor de orden p, se calcula a partir de la secuencia de los coeficientes de reflexión $K_1, K_2, \ldots, K_p$ de la siguiente manera ([8], ec.7.19) :

$$P_p = P_0 \prod_{K=1}^{p} (1-K_K^2) \qquad (2.32)$$

donde $P_0$ es la potencia promedio de la señal de entrada.

### II.7.3 Autocorrelación.

En el PDS es común comparar dos señales. Esto se puede realizar de varias maneras. Una posibilidad usada comunmente es el desplazamiento de una señal con repecto a otra señal, esto sirve para medir la similitud entre ambas funciones. Matemáticamente, esta operación se representa por :

$$R_{xy}[\tau] = \sum_{l=-\infty}^{\infty} x[n]y[n+\tau] = \sum_{l=-\infty}^{\infty} x[n-\tau]y[n] = R_{yx}[-\tau]$$

donde se supone que al menos una de las señales es real; es decir, tiene energía finita.

La señal $R_{xy}[\tau]$ es la llamada función de correlación cruzada de x[n] y y[n]. Si estas dos señales son idénticas, la señal $R_{xy}[\tau]$ es la función de autocorrelación de x[$\tau$]. La función $R_{xy}[\tau]$ es una medida de la similitud entre x[n] y y[n], y ésta alcanza su valor máximo cuando x[n] y y[n] son idénticas.

Los diferentes pasos y operaciones en el cálculo de una función de autocorrelación son :

* La señal y[n] se recorre a partir de una cantidad conocidad $\tau$.
* El producto x[n]y[n+$\tau$] se calcula muestra por muestra para todas los valores de n.

### II.7.4 Método de Análisis de Leroux-Gueguen.

El método de Levinson-Durbin es una forma eficiente para determinar los coeficientes de reflexión $K_i$. Pero en el caso de necesitar los parámetros $a_i$'s, se tiene que realizar una conversión de parámetros, es decir, pasar de $K_i$'s a $a_i$'s. Le Roux-Gueguen resolvieron este problema introduciendo las cantidades ([12], ec.5.35)

$$e^{j}(i) = R_x(i) + a_1^{(j)} R_x(i-1) + a_2^{(j)} R_x(i-2) + \ldots + a_j^{(j)} R_x(i-j) \qquad (2.33)$$

donde $R_x(i)$ son los coeficientes de autocorrelación. De esta manera se calculan los coeficentes de reflexión $K_i$'s de manera directa, además de calcular los coeficentes $a_i$'s como cantidades intermedias.

Entonces, los coeficientes de reflexión se calculan a partir de las siguientes relaciones ([12], pag. 126) :

$$K_j = \frac{-e_{(j)}^{j-1}}{e_{(0)}^{j-1}} \qquad j = 1,\ldots,p \qquad (2.34)$$

$$e^{j}(i) = e^{j-1}(i) + K_{j-1}\, e^{j-1}(j-1) \qquad i = -p+j,\ldots,p \qquad (2.35)$$

con la condición inicial

$$e^{0}(i) = R_x(i) \qquad i = -p,\ldots,p \qquad (2.36)$$

donde $R_x(-i) = R_x(i)$.

Entonces, la energía residual es

$$E(i) = e^{i}(0) \qquad (2.37)$$

En la ecuación (2.35), los valores $e^{j}(i)$, $i = 1,\ldots j$ son cero, por lo que no es necesario calcularlos. Un resultado importante de estas formulaciones, es que la secuencia de autocorrelación esta normalizada, es decir, $R_x[0] = 1$, por lo tanto todas las cantidades $e^{j}(i)$ se encuentran entre -1 y +1.

El conjunto de parámetros $K_i$, $i = 1,...p$ (coeficientes de reflexión) juegan un papel central en el método LPC y tienen las siguientes propiedades ([12], pag. 123) :

1.) Los coeficientes Ki's, son equivalentes a los coeficientes del filtro, $a_i$. Es decir, a partir de las $K_i$'s se pueden obtener las $a_i$'s y viceversa, de acuerdo a las siguientes relaciones

Ki's a ai's :

$$a_i^{(i)} = K_i$$

$$a_j^{(i)} = a_j + K_i \, a_{i-j}^{(i-1)} \qquad \begin{cases} i = 1, \ldots, p \\ j = 1, \ldots, i-1 \end{cases}$$

De las ai's a Ki's :

$$K_i = a_i^{(i)}$$

$$a^{(i-1)} = \frac{a_j^{(i)} \; a_i^{(i)} \; a_{i-j}^{(i)}}{1 - K_i^2} \qquad \begin{cases} i = p, \ldots, 1 \\ j = 1, \ldots, i-1 \end{cases}$$

2.) Se tiene un filtro estable, es decir, todos los polos se encuentran dentro del círculo unitario.

$$-1 < k_i < 1 \qquad i = 1,...p$$

Esta condición es muy importante, ya que si nos aseguramos que las Ki's están en el intervalo entre -1 y +1 podemos garantizar la estabilidad del filtro.

3.) Con el fin de implantar el filtro H(z) del tracto vocal no es necesario convertir los Ki's a ai's y después usar alguna forma del filtro predictor. En lugar de ello, es posible implementar el filtro en forma de escalera usando los coeficientes de reflexión directamente. Las ecuaciones para implantar el filtro de escalera son ([12], pag. 125) :

$$f^{(i-1)}[n] = f^{(i)}[n] - K_i \; b^{(i-1)}(n-1) \qquad (2.38)$$

$$b^{(i)}[n] = K_i \, f^{(i-1)}[n] + b^{(i-1)}[n-1] \qquad (2.39)$$

con

$$f^{(p)}[n] = Gu[n] \qquad (2.40)$$

donde u[n] es la señal de excitación.

El superíndice indica la etapa en el filtro de escalera, mientras que el argumento es el índice de tiempo. Entonces, la salida es ([12], ec. 5.30) :

$$s[n] = f^{(0)}[n] \tag{2.41}$$

Las ecuaciones anteriores introducen las cantidades que son llamadas error progresivo $f^{(i)}[n]$ y error regresivo $b^{(i)}[n]$. Estas ecuaciones se escriben de la forma siguiente ([12], pag. 125) :

$$f^{(i)}[n] = f^{(i-1)}[n] + K_i \; b^{(i-1)}[n-1] \tag{2.42}$$

$$b^{(i)}[n] = b^{(i-1)}[n-1] + K_i \; f^{(i-1)}[n] \tag{2.43}$$

que representan el filtro inverso **A**(z) en la Fig. 2.16.

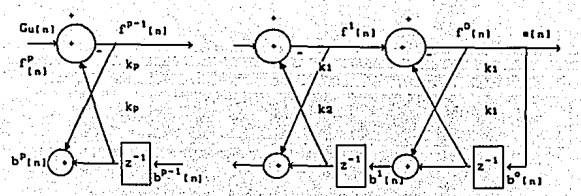



Fig. 2.17 Filtro de escalera para sintetizar voz a partir de la excitación Gu[n] y de los coeficientes de reflexión $K_i$'s, ([12], fig. 5.9).

Cuando la entrada al filtro es la señal s[n], la salida es la señal de error residual e[n]. Este filtro se implanta como se muestra en la Fig.2.18.

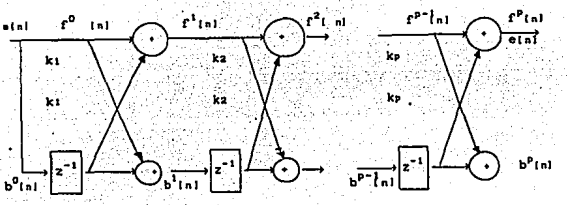



Fig.2.18 Implantación en Escalera ("Laticce") del filtro inverso LPC. La entrada es la señal de voz s[n] y la salida el error residual ([12], fig. 5.10).

Donde el error progresivo $f^{(i)}[n]$ y el error regresivo $b^{(i)}[n]$ (para i = 0) se define como ([12], pag. 125) :

$$f^{(o)}[n] = s[n] \qquad (2.44a)$$

$$b^{(o)}[n] = s[n] \qquad (2.44b)$$

y la salida se define como ([12], ec. 5.34) :

$$e[n] = f^{p}[n] \qquad (2.45)$$

Obsérvese que si la señal de error residual e[n] se alimenta al filtro de síntesis de la Fig.2.17, la salida será la misma señal de entrada s[n]. Es decir, se puede usar la señal de error residual e[n] como excitación al filtro del tracto vocal.

CAPITULO

T R E S

# PRINCIPIOS BASICOS DE LA CRIPTOLOGIA

## III.1 INTRODUCCION A LA CRIPTOLOGIA.

La *seguridad*, en un caso general, debe entenderse como una medida de protección o prevención a los *bienes* o *valores* contra el robo. En un DSC (ver Fig.1.2), *la seguridad* es una medida de protección a la información transmitida a través de un Canal de Comunicación.

Las *amenzas o ataques* [17] que sufre cualquier DSC se clasifican en dos grupos :

a). *Deliberadamente a propósito .*
Gente que voluntariamente es enemigo.
-- Ladrones.
-- Terroristas.
-- Espías.
-- Venganza de gente.

b). *Accidentalmente gente/naturaleza.*
Gente que involuntariamente es enemigo o algún fenómeno de la naturaleza que afecta al DSC.
-- Errores de gente.
-- Accidentes.
-- Problemas del medio ambiente.
(Inundaciones, terremotos, descargas electrostáticas, etc.)

Una *medidad de seguridad* o *protección* a los *bienes* empleada contra el robo, la adulteración o la inyección de información es la utilización de la *Criptología*. Por lo tanto, la criptología forma parte de la seguridad en un DSC.

## III.2 DEFINICION DE CRIPTOLOGIA.

La etimología de la palabra *Criptología* es :
**Kriptos** ( escondido ) y **logos** ( palabra ).

Podemos entender por Criptología :

" Escritura secreta realizada mediante clave, de manera que sea imprescindible conocer la clave para descifrar la escritura".

La Criptología estudia los procesos de *cifrado* y *descifrado* de los mensajes [16], así como el análisis de los mensajes cifrados ( criptogramas ) para descubrir la clave y el mensaje original.

La Criptología se divide en dos ramas que son [ 3 ] :

La *Criptografía*, la cual se refiere al estudio de los diferentes métodos para cifrar y descifrar mensajes y el *Criptoanálisis*, que se refiere a las técnicas de ataque para violar el secreto de la clave y del mensaje cifrado.

Así, al diseñador del sistema criptográfico se le denomina criptográfo, y al sistema que diseña, sistema criptográfico (criptosistema). Su oponente es el criptoanalista, que trata de romper el secreto del sistema.

Además, la Criptología también comprende el estudio de las vías para cifrar o descifrar mensajes, así como para evitar intercepciones de información no autorizadas. El término *cifrador* se refiere a la transformación de cifrado que sufre o se realiza al *mensaje original* en el transmisor, dando como resultado un *mensaje cifrado* o *criptograma* y el término *descifrador* se refiere a la transformación de descifrar el *mensaje cifrado* que se realiza en el receptor, para recuperar el mensaje original.

### III.2.1 Objetivos de un Sistema Cifrador.

Los requerimientos para un buen sistema criptográfico pueden establecerse como sigue ([3], pag. 671) :

1). Proporcionar un medio fácil y barato de cifrado y descifrado para usuarios autorizados en posesión de la clave apropiada.

2). Proporcionar al criptoanálista o a personas no autorizadas una tarea difícil de análisis y un gasto enorme de recursos (en tiempo y/o espacio de memoria) para la recuperación del mensaje original, con base a que tienen cierta información del criptograma, de la clave o de ambos.

Tomando en cuenta lo anterior, los sistemas criptográficos pueden clasificarse como : Computacionalmente seguros (Condicionalmente) e Incondicional seguros.

Un sistema criptográfico se dice que es *computacionalmente seguro,* si al criptoanalista, (con base en que tiene cierta información de el criptograma, de la clave o de ambos), le llevaría un tiempo no menor de **x** unidades de tiempo el poder conocer el mensaje original que se transmitió.

Un sistema criptográfico, se dice que es *incodicionalmente seguro,* si al criptoanalista, (con base a que tiene cierta cantidad de información útil del criptograma, de la clave o de ambos, no le es suficiente para determinar el contenido del mensaje original que se transmitió, no importa cuanto tiempo o recursos este dispuesto a dedicar.

## III.3 NECESIDAD DE LA CRIPTOLOGIA.

Las dos principales razones para cifrar un mensaje son las siguientes ([3], pag. 669) :

1.) **Privacidad.** La privacidad en un sistema de comunicación utilizando un canal público, consiste en evitar a usuarios no autorizados que escuchen la conversación que se esté efectuando entre el emisor y el receptor.

2.) **Autenticidad.** Para prevenir que personas no autorizadas extraigan, alteren, inyecten o modifiquen la información que se transmite a través de un Canal de Comunicación Público, de tal manera que se consiga "engañar" al receptor.

Podemos decir que la aplicación de técnicas criptográficas es una de las soluciones universalmente aceptadas para evitar los actos que puedan vulnerar la información.

### III.3.1 Ataques Criptoanaliticos.

Un sistema criptográfico puede sufrir una infinidad de ataques [16] por parte del criptoanalista, estos ataques pueden clasificarse en tres niveles en función de la información que le proporcionen al criptoanalista (ver Fig.3.1) quien tiene el propósito de poder encontrar la clave y el mensaje original que se está transmitiendo hacia un receptor determinado.

**Nivel I : Ataque al mensaje cifrado.**

El nivel I, le permite al criptoanalista conocer el contenido del mensaje cifrado. Esto ocurre frecuentemente en la práctica. En este caso, el criptoanalista utiliza solamente el conocimiento de las propiedades estadísticas del lenguaje usado, por ejemplo, la frecuencia de letras de un lenguaje (ejemplo, en inglés la letra E ocurre 13%), y conocimiento de ciertas palabras probables (ejemplo, diptongos, triptongos, sílabas, palabras más comunes : (que, cual, etc.). Es la amenza más débil a la que un sistema puede estar sujeto, y cualquier sistema que sucumba a esto se considera totalmente inseguro.

**Nivel II : Ataque al mensaje original conocido.**

Este nivel le da a conocer al criptoanalista, además del contenido del criptograma, de que mensaje proviene, es decir, su objetivo se reduce a averiguar la clave. Un sistema que es seguro contra este tipo de ataques libera a los usuarios de las necesidades de mantener los mensajes pasados en secreto o de parafrasearlos antes de desecharlos. Aunque un ataque de mensaje original conocido no es siempre posible, su ocurrencia es muy frecuente y un sistema que no puede resistir esto, no se considera seguro.

**Nivel III : Ataque de mensaje en claro elegido.**

El nivel III le ofrece al criptoanalista una mayor oportunidad para determinar la clave, ya que este nivel le permite elegir el mensaje original que se cifrará y por lo tanto, elegir su correspondiente criptograma. Este tipo de ataque es difícil de llevar a cabo en la práctica, debido a que se aproxima a la determinación de la clave, pero puede ser aproximado.

Una aproximación a este tipo de ataque, es la designación de un criptoanalista, dicho criptoanalista es parte del equipo del diseñador del criptosistema, aunque dicho criptoanalista puede ser el propio diseñador del sistema, el cual se encargara de hacer todas pruebas necesarias para la determinación de la clave **K**, a partir del mensaje original **M**, y del mensaje cifrado **C** seleccionado. Un sistema que está seguro del ataque al mensaje original elegido, puede evitar que sus usuarios se preocupen porque sus oponentes puedan colocar mensajes en su sistema.

En la práctica, la seguridad de los sistemas cifradores más comunes no depende, en general, del desconocimiento del algoritmo cifrador, sino que depende de la facilidad que se tenga para deducir la clave $K_i$ que se usó en el algoritmo cifrador, ya que el algoritmo cifrador puede recibir como entrada una clave $k_i$ de $i$-caracteres, donde $i$ es un número muy grande.

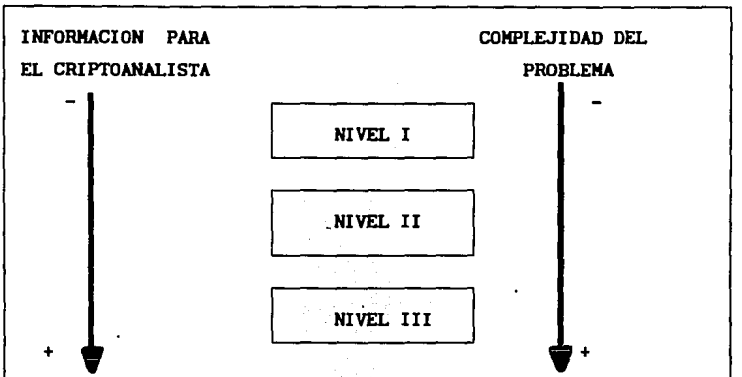



Fig.3.1 Clasificación de ataques con base a la información que proporcionan al criptoanalista.

## III.4 ELEMENTOS DE LA CRIPTOGRAFIA.

Un sistema de comunicación que permite que la información sea confidencial y ésta no sea entendida por personas no autorizadas se denomina, *sistema cifrador*. En un sistema cifrador se pueden reconocer los siguientes elementos, ver Fig.3.2 ([3], pag. 669).

*Mensaje* **M** ( Plain-text) .
Es la información confidencial que se desea hacer llegar desde el transmisor hasta el receptor.

*Algoritmo Cifrador.*
Es el conjunto de reglas que con una cierta clave **K**, convierten el mensaje original **M**, en un mensaje cifrado ( criptograma ) **C**.

*Mensaje cifrado o Criptograma.*
Es el mensaje que se enviará a través de un Canal de Comunicación Público, desde el transmisor hasta el receptor, pero que previamente se le aplicó un algoritmo criptográfico. Debe ser imposible, o muy difícil, que el intruso obtenga información acerca del mensaje original a partir del criptograma.

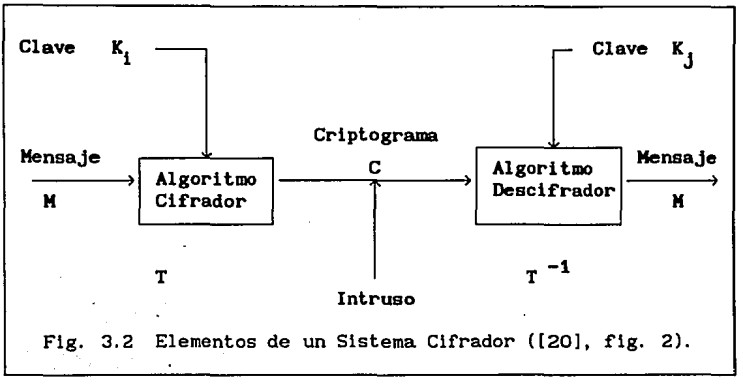



Fig. 3.2 Elementos de un Sistema Cifrador ([20], fig. 2).

*Intruso* o *Criptoanalista.*

Es la persona que desea conocer el mensaje original y que no está autorizada para ello, no es un elemento del sistema cifrador, pero se incluye aquí, ya que éste da la razón de existencia a los sistemas cifradores.

*Algoritmo descifrador.*

Es el conjunto de reglas que con una cierta clave **K**, convierten un criptograma **C** en el mensaje original **M**.

La función de cifrado **E**, es tal que combina de alguna manera el mensaje original **M**, con la clave $K_i$, para obtener el criptograma **C**. Consecuentemente, la función de descifrado **D**, combina el criptograma **C**, con la clave $K_j$, para obtener el mensaje original **M**.

De este funcionamiento se deducen al menos dos cosas :

1). Las funciones **E** y **D** provocan transformaciones en los mensajes, siendo inversas una de la otra.

2). La clave empleada en la función de descifrado, puede ser la misma o puede depender de la clave que se utilizó en la función de cifrado. Por lo tanto, al utilizar un sistema criptográfico donde hay un emisor y un receptor, éste último debe poseer la clave de descifrado, habiéndola recibido mediante algún sistema no interceptable.

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

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

Análogamente, designando a **D** como función de descifrado:

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

De esta manera toda la seguridad reside en mantener el secreto de la clave **K**, que es el elemento que efectúa el cifrado y el descifrado. En algunos casos, los esquemas de cifrамiento empleados en los sistemas criptográficos (por ejemplo, sistemas criptográficos de clave privada [17]), envían las claves (a su vez cifradas) con otra clave denominada **clave maestra**, como precaución necesaria para la distribución de las claves.

## III.5 SISTEMA CIFRADOR DE UN SOLO PASO.

Este es un sistema particular que tiene gran influencia sobre sistemas cifradores modernos con *seguridad perfecta*, y se conoce como un sistema de un sólo paso (one-time pad), ver Fig.3.3 [19]. Un cifrador de un sólo paso es aquel en el que el criptograma se obtiene en un sólo tiempo, es decir, para obtener el criptograma respectivo no se necesitan más etapas de cifrамiento.

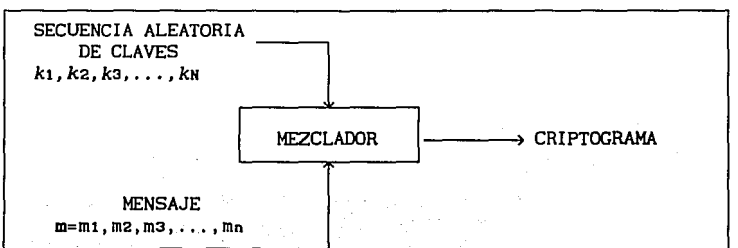



Fig. 3.3 Sistema Cifrador de un sólo paso ([3], fig.12.15).

Sea el mensaje **M** = $m_1, m_2, m_3, \ldots, m_n$ el mensaje a ser cifrado. (En este mensaje cada $m_i$ es un carácter de un alfabeto y **M** es una palabra de dicho alfabeto). En este sistema, para cada pareja $(k_i, m_i)$ el mezclador o algoritmo cifrador produce un carácter $c_i$ del criptograma **C**. Las funciones del mezclador son del tipo :

a). $c_i = m_i + k_i \pmod{25}$ Sumador módulo 25, para un alfabeto de 25 caracteres donde cada uno de estos caracteres se representa por un entero del 0 al 25.
$c_i$ { 0...25}
$k_i$ { 0...25}

b). $c_i = m_i + k_i \pmod{2}$ Sumador módulo 2, para mensajes codificados en forma binaria.

Además, entre las características adicionales de un criptosistema de un sólo paso están : Seguridad Perfecta, Confusión y Difusión.

### III.5.1 Seguridad Perfecta.

La mayor influencia que tiene la criptografía moderna se debe a los trabajos realizados por Shannon [18]. Shannon observó que la clave $K_1$, en la Fig.3.4, determina una transformación del conjunto de todos los posibles mensajes al conjunto de todos los posibles criptogramas. Estos dos conjunto son denominados respectivamente : *espacio del mensaje* y *espacio del criptograma.*

La definición para un sistema cifrador, de acuerdo a Shannon es: Un sistema cifrador es un conjunto de transformaciones **T** sobre un conjunto finito del espacio del mensaje **M**, que dan como resultado un conjunto finito del espacio del criptograma **C**.

Un requerimiento fundamental en los sistemas cifradores es, que conociendo el criptograma, el algoritmo cifrador y la clave empleada, se puede obtener el mensaje original que es único. Es decir :

$C = t ( M )$ El mensaje **M** se transforma en el criptograma **C** por la transformación **t**.

$M = t^{-1} ( C )$ El mensaje **M** puede determinarse por la transformación inversa de **t** sobre el criptograma **C**.

De lo anterior y observando la Fig.3.4, se determina que la transformación **t** depende del algoritmo cifrador y de la clave $K_1$, mientras que la transformación inversa $t^{-1}$ depende del algoritmo descifrador y de la clave $K_2$.

Si el receptor conoce C y t, está habilitado para deducir M, mientras que el criptoanalista conoce C y las probabilidades de varias $t_s$, con dichos elementos se espera que el criptoanalista no pueda deducir M, teniéndose así **seguridad perfecta** en el sistema cifrador.

Un código perfectamente seguro es aquel que a cada mensaje le puede corresponder cualquier criptograma con igual probabilidad, independientemente de la clave utilizada. Un sistema perfectamente seguro deberá distribuir el espacio de mensajes originales sobre sí mismo de modo aleatorio, de tal forma que un criptoanalista, al interceptar un criptograma, tiene que considerar todos los mensajes de M como candidatos igualmente probables, para seleccionar el mensaje original.

Un esquema de cifrado perfecto es equivalente a una matriz, en donde las columnas corresponden a los mensajes originales, las filas a los criptogramas y las entradas a las claves como se muestra en la Fig.3.4.

| | $M_1$ | $M_2$ | $M_3$ | $M_4$ | ..... | ..... | $M_{N-2}$ | $M_{N-1}$ | $M_N$ |
|---|---|---|---|---|---|---|---|---|---|
| $C_1$ | $K_1$ | $K_2$ | $K_3$ | $K_4$ | ..... | ..... | $K_{N-2}$ | $K_{N-1}$ | $K_N$ |
| $C_2$ | $K_n$ | $K_1$ | $K_2$ | $K_3$ | ..... | ..... | ..... | $K_{n-2}$ | $K_{n-1}$ |
| $C_3$ | $K_{N-1}$ | $K_N$ | $K_1$ | $K_2$ | ..... | ..... | ..... | ..... | $K_{N-2}$ |
| $C_4$ | ..... | $K_{N-1}$ | $K_N$ | $K_1$ | $K_2$ | ..... | ..... | ..... | ..... |
| ..... | ..... | ..... | $K_{n-1}$ | $K_n$ | $K_1$ | ..... | $K_3$ | $K_4$ | ..... |
| ..... | ..... | ..... | ..... | ..... | ..... | ..... | ..... | ..... | ..... |
| ..... | ..... | ..... | ..... | $K_{N-1}$ | $K_N$ | ..... | $K_2$ | $K_3$ | $K_4$ |
| $C_{U-2}$ | $K_4$ | | | | $K_{N-1}$ | | $K_1$ | $K_2$ | $K_3$ |

Fig.3.4 Esquema del Cifrado Perfecto([35], fig. 46).

Considere un sistema cifrador con espacio finito de N mensajes $M = \{ M_0, M_1, \ldots\ldots, M_{N-1} \}$ y un espacio finito de U criptogramas $C = \{ C_0, C_1, \ldots, C_{U-1} \}$. Para un $M_i$, la probabilidad de que $M_i$ se transmita es $P( M_i )$; sabiendo que $C_j$ es el mensaje recibido, la probabilidad a posteriori de que el mensaje $M_i$ se transmita es $P (M_i / C_j)$.

Un criptosistema tiene seguridad perfecta si, para todo mensaje $M_i$ y todo criptograma $C_j$, la probabilidad a posteriori es igual a la probabilidad a priori, como lo muestra la ec.(3.1).

$$P( M_i / C_j ) = P ( M_i ) \qquad ( 3.1 )$$

De esta forma, para un sistema con "seguridad perfecta", un criptoanalista que intercepta $C_j$ no obtiene información para determinar de cuál mensaje $M_j$ proviene $C_j$.

En un sistema cifrador en el cual el número de mensajes, el número de claves, y el número de criptogramas son todos iguales, se obtiene seguridad perfecta si y sólo si posee las dos condiciones siguientes :

1). Existe una sóla clave que transforme cada mensaje original en un único criptograma.

2). Todas las claves tienen la misma probabilidad de ser usadas.

Si estas condiciones no son satisfechas, se tendría que para algún mensaje $M_i$, tal que para un $C_j$ dado, no hay clave que pueda descifrar $C_j$ a $M_i$, implicando que $P(M_i / C_j ) = 0$ para algún i y j.

$$P (C_j / M_i) = P (C_j) \qquad (3.2)$$

### III.5.2 Confusión y Difusión.

Un análisis estadístico, basado en la frecuencia de ocurrencia de un carécter individual o las combinaciones de caracteres, puede ser utilizado para solucionar muchos sistemas criptográficos. Shannon [18] sugiere dos conceptos de ciframiento para frustar el esfuerzo estadístico de un criptoanalista. Estos conceptos son :

- -- Confusión
- -- Difusión.

**Confusión :**

El concepto de confusión pretende que por medios estadísticos el criptoanalista no descarte un gran número de claves, debido a que existe una relación muy extrecha entre la clave **K** y el criptograma **C**, (ver, Fig.3.5), debido a que el cifrado se efectúa por la aplicación de cada bit de la clave $k_i$ sobre todo el criptograma.

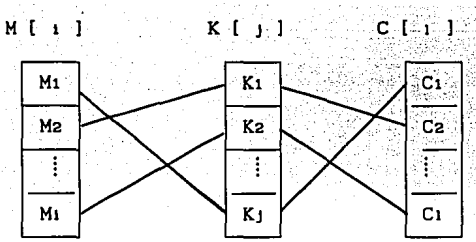



Fig. 3.5 Concepto de Confusión.

Asimismo, la confusión asegura que la relación entre un criptograma y su clave correspondiente es compleja; por lo tanto, el objetivo es hacer más difícil el análisis estadístico de las características de la clave. Para asegurar esto, es deseable que el cifrado de todos los caracteres del mensaje dependan de la clave.

**Difusión :**

Asegura una relación compleja entre el mensaje y el criptograma, esto sirve para extender las estadísticas del mensaje sobre grandes porciones del criptograma. La idea es asegurar que el criptoanalista necesite interceptar una gran parte del criptograma, antes de que pueda descifrarlo estadísticamente.

La difusión, en un alfabeto de 26 letras, se utiliza para transformar una secuencia de caracteres $M = M_0, M_1, \ldots$ en una nueva secuencia de caracteres $Y = Y_0, Y_1, \ldots$, mediante la ecuación (3.3) ([3], pag. 683).

$$Y_n = \sum_{i=0}^{s-1} M_{n+i} \text{ módulo } - 26 \qquad (3.3)$$

donde:

- $Y_n$ Es la secuencia determinada por la ecuación. (3.3).
- n Es el número de caracteres que constituyen el mensaje.
- s Es cualquier entero.

El nuevo mensaje $Y_n$ tiene la misma redundancia que el mensaje original, **M**, pero la frecuencia de los caracteres del mensaje $Y_n$ es más uniforme que los caracteres del mensaje **M**. El criptoanalista necesita, para decifrar el mensaje original, una secuencia más larga del mensaje, de la que anteriormente necesitaba y un análisis estadístico más exhaustivo. En resumen, se busca que esta curva sea lo más uniforme posible, con el objeto de no darle mayor información al criptoanalista.

Un ejemplo de difusión se muestra a continuación. Supóngase el siguiente mensaje original a transmitir :

*ESTE SALUDO ES PARA ALGUIEN MUY ESPECIAL,*
*TRABAJADOR, HUMILDE, SENCILLO,...*

Su correspondiente criptograma, a partir de un corrimiento s = 4 es :

*IWXI WEPYHS IW TEVE EPKYMIR QYC IWTIGMEP,*
*XVEFENEHSV, LYQMPHI, WIRGMPPS,...*

Si se realiza una gráfica de la "ocurrencia" de cada una de las letras vocales del criptograma, tendríamos lo siguiente, (ver Fig.3.6).

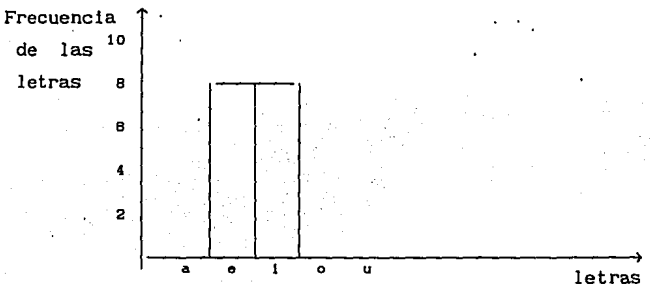



Fig.3.6 Ejemplo del Concepto de Difusión.

Se puede observar que la mayor "ocurrencia" de cada una de las letras vocales (en este caso, la letra *e* y la letra *i*), proporcionan al criptoanalista información acerca del mensaje transmitido. Esto es, combinando cada una de las letras con mayor ocurrencia, permiten al criptoanalista formar parte o el total del mensaje transmitido.

Por otra parte, a partir de un sistema cifrador de un sólo paso, hay esencialmente tres tipos de sistemas cifradores modernos [17] :

A). Cifradores de bloques.
B). Cifradores de cadenas.
C). Cifradores de Claves Públicas.

## III.6 CIFRADORES DE BLOQUES.

El cifrado en bloque trabaja con grupos de bits de longitud fija denominados bloques. Cada bloque se trata por separado, con lo que cada bloque del mensaje se cifra únicamente en base a él mismo, a la clave de cifrado y en algunos casos utilizando el criptograma que se está generando. El cifrado en bloque se utiliza de dos maneras ([35], pag. 136).

1). Cifrado en bloque propiamente dicho, que responde al esquema de bloques separados.

2). Cifrado en bloques encadenados, en el que se sigue cifrando la información en base a grupos o bloques de bits, pero cada bloque se forma con dos porciones de mensaje, una con mensaje en claro, y la otra con una parte del criptograma correspondiente al bloque anteriormente cifrado, o del mensaje en claro del bloque anterior. Esto da lugar a tres tipos de cifrado en bloque encadenado :

2a). Cifrado encadenado modalidad criptograma.

2b). Cifrado encadenado modalidad mensaje original.

2c). Existe también una tercera que es una mezcla de ambos, en el que cada bloque de entrada al proceso de cifrado se compone de una parte de mensaje original correspondiente al bloque en curso, otra parte correspondiente al bloque de mensaje original anterior, y otra correspondiente al último criptograma obtenido, generalmente relacionados con alguna función de tipo lógica como es la suma módulo dos, o simplemente concatenados.

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

Las expresiones para los distintos modos en bloque, usando las funciones de concatenación $\odot$ y suma módulo dos $\oplus$, siendo $C_K$ la función de cifrado con la clave K, se pueden expresar de la siguiente manera ([36], pag. 140) :

Cifrado en bloque puro :

$$C_i = C_K ( M_i ) \qquad \text{para toda } i$$

Función de concatenación $\ominus$ :

Cifrado en bloque encadenado modalidad criptograma:

$$C_i = C_K ( M_i \ominus C^*_{i-1} ) \qquad \text{para } i \geq 1$$

Cifrado en bloque encadenado modalidad mensaje original:

$$C_i = C_k ( M^*_i \ominus M_{i-1} ) \text{ para } i \geq 1$$

Cifrado en bloque encadenado modalidad mixta:

$$C_i = C_K ( M_i \ominus M^*_{i-1} ) \quad \text{para } i \geq 1$$

donde * significa " una porción de " y para el caso concreto de i = 1, se usa la palabra clave PW.

Función suma módulo dos $\oplus$ :

Cifrado en bloque encadenado modalidad criptograma:

$$C_i = C_K ( M_i \oplus C_{i-1}) \qquad \text{para } i \geq 1$$

Cifrado en bloque encadenado modalidad mensaje original:

$$C = C_i ( M_K \oplus M_i )_{i-1} \qquad \text{para } i \geq 1$$

Cifrado en bloque encadenado modalidad mixta:

$$C_i = C_K ( M_i \oplus M_{i-1} \oplus C_{i-1} ) \qquad \text{para} \geq 1$$

Donde la relación es cierta para todos los bloques i, teniendo en cuenta la excepción del caso i = 1, que usará una palabra clave para suplir la ausencia del correspondiente componente.

Las operaciones de descifrado para el cifrado en bloque encadenado usando la función suma módulo dos son ([36], pag. 141) :

Descrifrado para la modalidad criptograma:

$$( M_i \oplus C_{i-1} ) = C_K^{-1} (C_i); \quad M_i = ( M_i \oplus C_{i-1}) \oplus C_{i-1}$$

Descifrado para la modalidad mensaje original:

$$(M_i \oplus M_{i-1}) = C_k^{-1} (C_i) ; \quad M_i = (M_i \oplus M_{i-1}) \oplus M_{i-1}$$

Descifrado para la modalidad mixta :

$$(M_i \oplus M_{i-1} \oplus C_{i-1}) = C_K^{-1} (C_i) ;$$

$$M_i = (M_i \oplus M_{i-1} \oplus C_{i-1}) \oplus M_{i-1} \oplus C_{i-1}$$

Una propiedad muy importante de los cifrados en bloque encadenados, es su fuerte dependencia intersímbolos de naturaleza no lineal, en la que cualquier tipo de corrupción afecta a uno o más bloques de criptogramas, según el tipo de cifrado encadenado utilizado.

Como ejemplos prácticos de los cifradores en bloques se puede mencionar : El sistema Cifrador Lucifer [21]. El sistema Cifrador DES [22], etc. Aquí mencionaremos el Sistema Cifrador DES.

### III.6.1 Cifrador de Datos Estandar DES (Data Encryption Standard).

El algoritmo DES es un sistema monoalfabético y fue presentado con el fin de proporcionar un algoritmo normalizado para redes de computadores [22 ]. El DES se basa en el desarrollo de un algoritmo de cifrado que modifica el mensaje original, con tantas combinaciones, que el criptoanalista no podría deducir el mensaje original aunque dispusiese de numerosas copias.

Un algoritmo como el DES puede considerarse como un número grande de procedimientos matemáticos llamados transformaciones, dichas transformaciones actúan sobre secuencias de datos (bits) no inteligibles que representan un mensaje y que dan como resultado secuencias de bits que aparentemente son ruido a hombres o máquinas. La clave criptográfica se mantiene en secreto y generalmente es corta, además se forma por una secuencia de bits que identifica las tranformaciones a realizar. Ya que el DES es un algorimto estandar y cuenta con las siguientes ventajas :

a). Si un circuito integrado o un conjunto de circuitos integrados se diseñan para implementar el estandar, los costos se reducen.

b). La existencia de un estandar incrementa el número de usuarios del criptosistema, ya que al convertirse un algoritmo cifrador en estandar, dan confiabilidad a la seguridad del sistema.

c). Existe una compatibilidad entre diversos sistemas de comunicación que emplean el criptosistema DES.

Es importante notar, que para una buena seguridad en los datos, solamente se necesita mantener en secreto la clave pudiendo ser públicos los detalles del algoritmo.

### III.6.1.1 Descripción del Algoritmo DES.

La filosofía de **DES** consiste en llevar a cabo varias etapas de permutación y sustitución, como se muestra en la Fig. 3.7. El **DES** utiliza una clave de 64 bits, de los cuales 56 se utilizan directamente por el algoritmo **DES** y los 8 restantes se emplean para la detección de errores.

Como se muestra en la Fig.3.7, en el método **DES** el mensaje original que debe cifrarse se somete a una permutación inicial **IP** con un bloque de entrada de 64 bits, que se permuta de acuerdo a la tabla 3.1. :

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 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 | 38 | 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 3.1 Permutación Inicial ( IP )

La entrada permutada tiene como primer bit, el bit 58 del mensaje original, como segundo bit, el bit 50 del mensaje original, y así sucesivamente, hasta llegar al último bit, que corresponderá al bit 7 del mensaje original. A continuación, el bloque de entrada permutado sirve de entrada a un complejo cálculo, dependiendo de la clave, que consiste de 16 etapas. El funcionamiento de cada etapa es el mismo, pero la función de cifrado de la clave **K** se realiza de distintas formas.

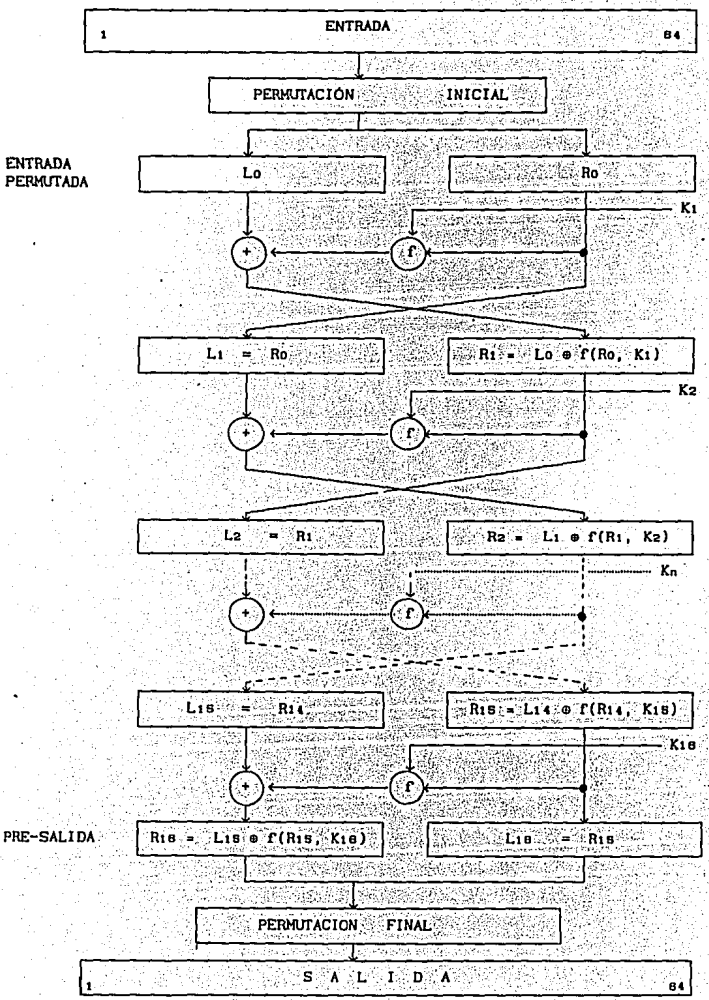



Fig.3.7 Algoritmo DES (Data Encrytion Standard).

Las 16 etapas emplean los dos bloques ( **L** y **R** ) de 32 bits para generar dos bloques de 32 bits de salida. Las copias derecha e izquierda se intercambian antes de cada etapa. La función **F** lleva a cabo cuatro pasos sobre la salida derecha, mediante una transposición basada en la operación or-exclusivo ( $\oplus$ ) que denota la suma bit a bit.

1). La mitad derecha **R** de 32 bits se convierte, mediante una regla de transposición y duplicación, en el número **E**, de 48 bits.

2). **E** y **K** se combinan mediante un or-exclusivo. En cada etapa se escoge un bloque de **K** de bits dentro de la clave de 64 bits.

3). Los 48 bits generados en la etapa 2 se dividen en ocho grupos de 6 bits que se introducen en sendas cajas **S**, cada una de las cuales produce 4 bits de salida.

4). Los 32 bits restantes se introducen en una caja **P**.

A continuación, el resultado final se somete a la siguiente permutación, de acuerdo a la tabla 3.2, que es la inversa de la permutación inicial.

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 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 3.2 Permutación Final ( $IP^{-1}$ )

## III.7 CIFRADORES DE FLUJO (Cifradores de cadenas).

Un sistema cifrador de flujo [19] típico se muestra en la Fig.3.8. La principal característica de este tipo de cifradores, reside en que el cifrado de cada bit de datos es independiente del resto del mensaje original.

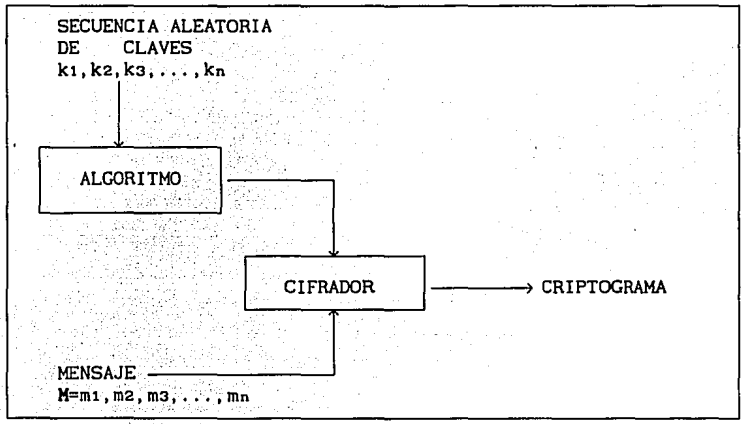



Fig.3.8 Cifrador de Cadenas

En este sistema la clave se alimenta en el algoritmo, usando éste la clave para generar una secuencia infinita (idealmente) de bits. Se hace referencia al algoritmo como el generador de cadena de llaves. Los generadores de cadenas de llaves producen una sucesión de dígitos pseudoaleatorios. Una sucesión de dígitos pseudoaleatoria es una sucesión de dígitos en los que no hay una relación obvia entre ellos.

Un cifrado en flujo no trata los caracteres o símbolos del lenguaje original independientemente, sino en función del estado del algoritmo de cifrado, que a su vez, depende de los símbolos que hayan llegado al cifrado y de la clave utilizada. Después de cifrar cada caracter, cambia de estado de acuerdo con alguna regla determinada. Esto impide que dos símbolos idénticos sean cifrados produciendo idéntico símbolo en el criptograma. Generalizando, dos secuencias de dígitos binarios que sean idénticos producen distinta secuencia de dígitos binarios en el criptograma.

El cifrado en flujo produce un símbolo o carácter por cada operación de cifrado, pero en realidad pueden alimentarse como un símbolo (una secuencia de bits de longitud predeterminada, generalmente ocho bits). Su comportamiento es tal que la longitud de la salida es igual a la longitud de la entrada, por lo que si ésta es pequeña habrá que hacer un número de operaciones de cifrado mucho mayor.

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

$$\frac{L}{I} = N$$

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

### VI.7.1 Registros de Corrimiento Lineal.

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

Un registro de corrimiento lineal con retroalimetación [23] es un arreglo de registros en serie, donde cada registro es capaz de almacenar cualquier dígito 1 (on) ó 0 (off). Un pulso de reloj regula el comportamiento del sistema, el cual trabaja de la siguiente manera :

Supongase que el sistema tiene **n** registros $R_1,\ldots,R_n$ como se muestra en la Fig.3.10, y que $X_1(t)$ denota el contenido del registro $R_1(t)$ en el tiempo **t**. Inicialmente definimos el sistema conociendo su configuración

$$\overline{x}\ (0) = (\ X_1(0),\ldots,X_n(0)\ ).$$

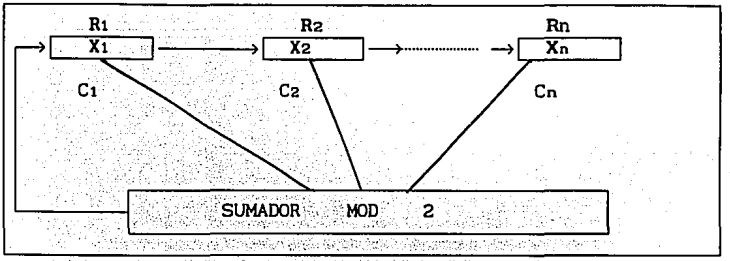



Fig.3.10 Registro de corrimiento de n-bits con Retroalimentación Lineal ([3], fig.12.13).

Si $x(t) = (X_1(t),\ldots,X_n(t))$ denota el estado del registro en el tiempo t, el estado del registro en el tiempo t+1 está dado por las reglas siguientes ([23], pag 127) :

$$X_i(t+1) = X_{i-1}(t) \qquad (2 \le i \le n) \qquad (3.4)$$

$$X_1(t+1) = C_1X_1(t)+\ldots+CX_n(t) \qquad (3.5)$$

donde $C_i$ $(1 \le i \le n)$ son constantes del sistema, las cuales toman valores 0 y 1 y la aritmética en la ecuación (3.5) se realiza en suma módulo 2. Está claro, por tanto, que el sistema está completamente especificado por :(1) Un vector inicial x(0), y por (2) El conjunto de constantes $C_1,\ldots,C_n$.

Asumimos que $C_n \neq 0$, de otra forma está fuera del registro $R_n$. La manera que el sistema trabaja, al recibir un dato (bit), permite a cada registro hacer dos cosas :

1). Pasar su contenido hacia adelante, es decir, hacia el vecino del lado derecho. (En el n-ésimo registro, no se realiza esta operación).

2). Aquellos registros $R_i$ para los cuales $C_i=1$, también pasan su contenido hacia el sumador. Esto opera al pasar el resultado hacia el registro $R_1$.

Una vez que el conjunto del vector inicial sea leido, el registro de corrimiento puede ser rearreglado como la fuente de la cadena finita de digitos binarios

$$X_0(0),X_1(1),X_2(2),\ldots,$$

y de esta forma, obtenemos el contenido sucesivo del primer registro. De esta manera las secuencias de los registros de corrimiento tienen dos propiedades principales y son : (1) Periodicidad, y (2) Longitud de la secuencia.

Periodicidad.

La secuencia ($y_i$: $0 \leq i < \infty$) se denomina *periódica* con período **p**, si **p** es un entero tal que $y_{i+p} = y_i$ para toda **i** y, además **p** es el entero más pequeño con esta propiedad. De esta manera, si la secuencia ($u_i$: $0 \leq i < \infty$ tiene período **p**, esto se puede escribir de la siguiente forma ([23], pag. 128) :

$$y_0, y_1, y_2, \ldots, y_{p-1}, y_0, y_1, y_2, \ldots, y_{p-1}, y_0, y_1, y_2, \ldots, y_{p-1}$$

En otras palabras, una secuencia con período **p** es justo una secuencia de repeticiones de un bloque finito de longitud **p**.

Longiud de la secuencia.

La secuencia de salida de un registro de corrimiento lineal es periódica, si hay **n** registros y su máximo período es $2^n-1$.

Por otra parte, definimos la característica polinomial del registro de corrimiento para el polinomio ([23], pag. 129) :

$$P_n(x) = C_nx + \ldots + C_2x + C_1x + 1$$

Con $C_n \neq 0$, donde los coeficientes de retroalimentación $c_i$ del registro son cualquier valor 0 ó 1. Este polinomio es *primitivo* si : (a) El polinomio no tiene factores no-triviales apropiados, y (b) $P_n(x)$ no puede ser dividido por $x+1$ para cualquier $d < 2^n-1$.

Finalmente, esto nos lleva decir que la secuencia de salida de un registro de corrimiento lineal para una entrada diferente de cero tiene período máximo si, y solamente si su característica polinomial es primitiva.

## III.8 SISTEMA CIFRADOR DE CLAVE PUBLICA.

### III.8.1. Introducción a la Criptología Moderna.

Desde la década de los sesenta, con la utilización masiva de los computadores y la gran potencia de cálculo aportada por estos, se empezaron a utilizar métodos criptográficos basados en técnicas que se denominan computacionales, cuyo fin es hacer altamente improbable la vulnerabilidad del sistema mediante el empleo de métodos con una elevadísima complejidad computacional, incluso con la técnicas actuales, es necesario mucho tiempo de cálculo para hacer "seguro" al sistema criptográfico. El esfuerzo reside concretamente en la complejidad computacional para resolver ciertos problemas matemáticos con los métodos actualmente conocidos.

Por otra parte, Shannon [18] especificó cinco criterios para un sistema secreto perfecto en un entorno de comunicaciones mediante el uso de la Criptología. Dada la fecha en que fueron enunciados (en 1949 fecha de su publicación), no se contempló la posibilidad de que un computador fuese el sistema que realizase el proceso de cifrado y descifrado, así como de diferentes modos de representación codificada de la información; esto obliga a efectuar una revisión de los criterios de Shannon para actualizarlos al sistema computacional actual transformandose en los siguientes criterios ([35], pag. 210) :

Uno : La cantidad de seguridad deseada, determina la cantidad de trabajo y tiempo de cálculo necesarios para vulnerar el mensaje cifrado.

Dos : Las claves utilizadas deben ser de fácil construcción, lo más cortas posibles, fáciles de alimentar, modificar y consecuentemente que ocupen poca memoria.

Tres : Las operaciones de cifrado y descifrado, conociendo la clave, deben implicar la menor cantidad de cálculo posible.

Cuatro : Las claves y el sistema de cifrado deben ser tales que destruyan los parámetros estadísticos del lenguaje, o bien su estructura natural.

Cinco : Los errores de transmisión en los criptogramas, no deben originar ambigüedades o pérdida del sentido en la información original, haciéndola inútil.

Seis : La necesidad de almacenamiento para los criptogramas no debe ser mayor que la necesaria para los mensajes en claro equivalentes.

Siete : El análisis de un criptograma al tratar de vulnerarlo debe necesitar una cantidad de cálculo tal, que sea considerado como un problema intratable, incluso con computador como apoyo.

### III.8.2 Sistema Cifrador de Clave Pública.

El concepto de sistemas criptográficos de clave pública empezó a manejarse por Diffie y Hellman [20], que proponen un sistema de comunicación privada que emplea un directorio de claves públicas, de tal modo que cada usuario fija un procedimiento **E** para que sea usado por otros usuarios cuando cifren sus mensajes que vayan dirigidos a él, mientras que guarda en secreto su propio procedimiento **D** de descifrado.

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

Los sistemas de clave pública utilizan dos diferentes claves, una para cifrar y la otra para descifrar. En los sistemas criptográficos de clave pública, no sólo el algoritmo cifrador, sino también la clave de cifrado pueden ser publicados sin comprometer la seguridad del sistema. Este hecho es parecido a un directorio telefónico público, el cual contiene todas las claves de ciframiento de todos los suscriptores. Solamente la clave del descifrado se mantiene en secreto. La Fig.4.10, ilustra este tipo de sistema criptográfico.

Como se muestra en la Fig.4.10, si el suscriptor **A** desea enviar un mensaje **M**, hacia el suscriptor **B**, entonces el suscriptor **A** selecciona la clave publica del suscriptor **B** a partir del directorio de claves público y aplicando el algoritmo cifrador **E**, obtiene el criptograma $C_B = E(M)$, el cual se transmite a través de un Canal Público de Comunicación. Solamente el subscriptor **B** puede descifrar $C_B$ por la aplicación de el algoritmo descifrador y de su respectiva clave privada $D_B$, para obtener el mesaje original **M**, $M = D(C_B)$.

Las características más importantes de un sistema criptográfico de clave pública son las siguientes :

1). El algoritmo cifrador **E**, y el algoritmo descifrador **D**, son transformaciones invertibles del mensaje original **M** o del mensaje cifrado **C**, definido por la clave **K**, esto es, que para cada **K** y **M**, si $C = E(M)$, entonces $M = D(C) = D[E(M)]$.

2). Para cada **K**, las transformaciones **E** y **D** son fáciles de evaluar.

3). Para cada **K**, el cálculo de **D** desde **E**, es computacionalmente intratable, es decir, el conocimiento público de **E** no implica el conocimiento ni perdida de seguridad de **D** , o lo que es igual, la obtención de **D** a partir de **E** es un problema intratable desde el punto de vista de Teoría de Cálculo.

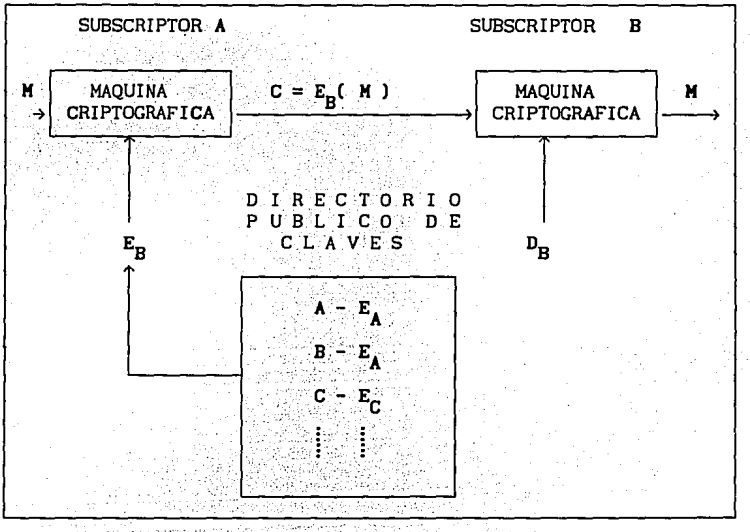



Fig. 4.10 Sistema Criptográfico de Clave Pública ([3], fig.12.17).

Estos esquemas de cifrамiento son computacionalmente seguros y sirven para aumentar la privacía; además, al compararlos con los esquemas de cifrамiento de clave privada tienen las siguientes ventajas [17]:

1.) En un esquema criptográfico de clave privada, el transmisor necesita enviar la clave por un canal seguro. En cambio, en un sistema de clave pública, mandar a publicar la clave en el archivo público podría resultar mucho menos costoso.

2.) En un esquema criptográfico de clave privada, la seguridad del sistema depende mucho de la seguridad del canal seguro, ese canal puede ser supuestamente seguro, o sea que existe la inseguridad.

En un esquema criptográfico de clave pública, no se necesita usar ningún canal seguro, aunque la seguridad del sistema no es incondicional, sino es computacional, es decir, nadie puede encontrar la clave secreta a partir de la clave pública, aún usando las computadoras. Con que se logre esto, es suficiente para proteger las comunicaciones en cuanto a su privacía.

3.) Enviar la clave por una canal seguro causa retardos para las comunicaciones. Esto es, mientras que la clave sea distribuida, el transmisor de mensajes tiene que esperar o mandar la clave de antemano, y en los sistemas de clave pública no existe este problema. Las claves ya están publicadas, será cuestión de buscarla en el archivo público de claves, lo cual reduce el retardo.

4.) En un sistema de clave privada, el transmisor tiene que mandar la clave a los receptores uno a uno, mientras en un esquema de clave pública, con sólo publicar la clave, la obtienen (la saben) todos, lo cual es más eficiente y requiere menos esfuerzo.

5.) Cuando las claves están comprometidas, deben ser cambiadas fácilmente. Cambiar la clave pública en un archivo público es más fácil que cambiar la clave y mandarla de nuevo por un canal seguro.

CAPITULO

C U A T R O

# ALGORITMOS CRIPTOGRAFICOS DE CLAVE PUBLICA PARA SEÑALES DE VOZ

El objetivo principal de este capítulo es implantar diversos algoritmos criptográficos aplicados a señales de voz. Cada uno de los algoritmos criptográficos implantados, es una combinación de un esquema de cifrамiento de clave pública y de un sistema de comunicación entre diversos usuarios. Cabe mencionar también, que en este capítulo el *autor de este trabajo de tesis* propone un sistema de comunicación entre diversos usuarios (ver inciso **IV.5.3**).

## IV.1 INTRODUCCION.

El cifrамiento de una señal de voz se puede realizar modificando la forma de onda de la señal de voz en su **Amplitud**, en el dominio del **Tiempo**, en el dominio de la **Frecuencia** [6], o por la modificación de sus características paramétricas (por ejemplo, manipulación de los parámetros **LPC** [14], ya sea aplicando algún Algoritmo de Cifrамiento Simétrico (Algoritmo de una sóla clave), o aplicando algún Algoritmo de Cifrамiento Asimétrico (Algoritmo de Cifrамiento de dos claves).

Simmons [1] clasifica a los Algoritmos de Cifrамiento en general en : (1) Algoritmos de Cifrамiento Simétricos (también llamados Algoritmos de Cifrамiento de clave privada) y (2) Algoritmos de Cifrамiento Asimétricos (también llamados Algoritmos de Cifrамiento de clave pública). Los algoritmos Simétricos emplean una sola clave tanto para el proceso de cifrамiento, **E**, así como para el proceso de descifrамiento, **D**. El conocimiento de la clave por parte de un intruso permite el conocimiento del mensaje cifrado.

Los algoritmos Asimétricos emplean dos claves, una clave **e**, para cifrar el mensaje original **M** y así obtener el criptograma **C** respectivo y otra clave **d**, para descifrar el criptograma **C** y de esta manera recuperar el mensaje original **M** transmitido. En este tipo de algoritmos cifradores la clave para cifrar el mensaje **e**, se hace pública en un directorio público de claves, mientras la clave para descifrar **d**, se guarda en secreto. El hecho de que la clave para cifrar sea publicada no compromete en nada la seguridad del sistema cifrador, ya que es difícil o intratable calcular la clave de descifrar **d**, a partir del conocimiento de la clave para cifrar **e**.

## IV.2 CRIPTOGRAFIA EN EL DOMINO DEL TIEMPO.

### IV.2.1 Introducción a la Criptografía en el Dominio del Tiempo.

Las técnicas de cifrамiento en el dominio del tiempo [6] son : (1) Inversión de segmentos en el tiempo. (2) Reordenamiento de muestras en el tiempo. (3) Permutación de bloques en el tiempo. Los cuales se describirán a continuación en forma breve.

**Inversión de segmentos en el tiempo.**

En este tipo de cifradores ([6], pag. 153), las muestras del mensaje de voz se agrupan en segmentos de tiempo que se almacenan en memoria, cada vez que se completan las muestras de un segmento, éstas se entregan al convertidor D/A en un orden invertido, obteniéndose de esta forma las correspondientes muestras del criptograma (ver Fig. 4.1).

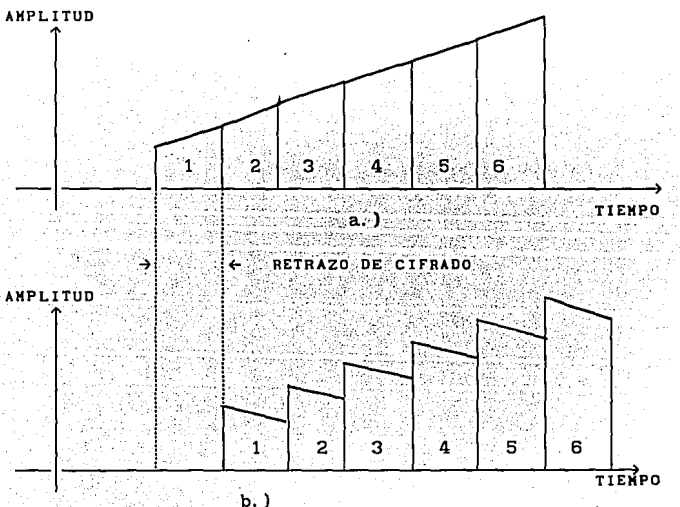



Fig. 4.1 Inversión de segmentos en el tiempo ([6], fig. 5.1). a.) Mensaje de voz; b.) Criptograma de voz.

En esta técnica de ciframiento el tamaño de los segmentos se adecúa de acuerdo a los requerimientos del sistema, evidentemente los segmentos grandes causan grandes retrasos de tiempo, pero en contraste proveen bajos residuos de inteligibilidad "comprensión del mensaje".

Esta técnica no contiene ninguna llave, pero se puede introducir una llave para obtener una variación en el tamaño de los segmentos, además, el tamaño de la memoria restringe los posibles tamaños de los segmentos y de esta forma, las longitudes de los segmentos se limitadan a un rango pequeño. Esta técnica ofrece una seguridad relativa.

**Reordenamiento de muestras en el Tiempo.**

Esta técnica de ciframiento de voz se muestra en la Fig.4.2 y funciona de la manera siguiente ([6], pag.. 186) :

1.) Se recibe el mensaje analógico de voz.

2.) A través de un convertidor A/D se obtiene el mensaje digital de voz.

3.) El mensaje digital de voz se transforma en el criptograma digital, esto se realiza reordenando las muestras de cada bloque del mensaje.

4.) A través de un convertidor D/A, se obtiene el criptograma analógico a transmitir.

Las dos principales inconvenientes para adoptar este método son :

1.) El acompañamiento de la extensión del ancho de banda.

2.) La integridad de las muestras individuales.

Para contrarrestar el primer inconveniente, a esta técnica de ciframiento se le adiciona una etapa de pre-filtrado para evitar que el ancho de banda de la señal procesada se expanda.

Para el segundo inconveniente, con esta técnica, conservar la integridad de las muestras es más difícil. Para un canal de comunicaciones real, es casi inevitable que la señal sea distorsionada. Estos niveles de distorsión llegan a ser significativamente más perceptibles cuando se presentan las discontinuidades en la operación inversa del reordenamiento.

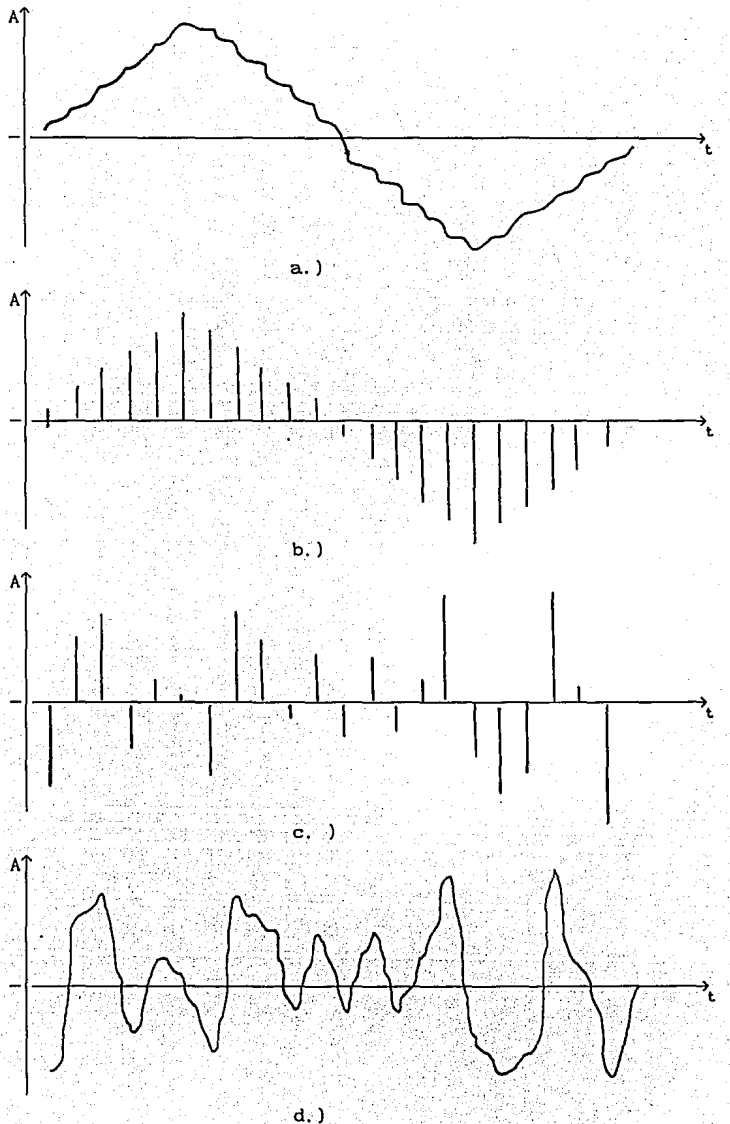



Fig. 4.2 Reordenamiento de Muestras en el Tiempo.

**Permutación de bloques en el Tiempo.**

En esta técnica de ciframiento ([6], pag. 156), la señal analógica se divide en períodos iguales de tiempo, llamados marcos. Cada marco es entonces sub-dividido en pequeños períodos de tiempo denominados segmentos, y el criptograma se obtiene permutando internamente los segmentos pertenecientes a un mismo marco (ver Fig.4.3).

En esta técnica de ciframiento se tienen tres parámetros importantes : (1) Longitud del segmento, (2) Longitud del marco y (3) Tipo de permutador.

1.) Longitud del segmento.

La longitud del segmento debe ser lo suficientemente pequeña para que no contenga más de un fonema, pero entre más pequeño sea el segmento, habrá mayores discontinuidades en la señal recuperada, lo cual provoca una expansión del ancho de banda, ya que estos súbitos cambios implican componentes de alta frecuencia.

2.) Longitud del marco.

La longitud del marco afecta el retraso entre el mensaje de voz analógico transmitido y el mensaje de voz recibido. En general, el tiempo de retraso total para un sistema con s segmentos por marco con una longitud por marco de T seg, es 2sTseg.

Desde el punto de vista de seguridad son aconsejables longitudes de marcos grandes, ya que si tenemos s segmentos por marco, entonces tenemos s! permutaciones posibles. Si s! permutaciones son pocas, evidentemente facilitamos la labor del criptoanalista.

3.) Tipo de Permutador.

Se puede tener una clave, la cual selecciona una permutación fija, esta permutación se usa para transmitir todos los marcos de voz del criptograma.

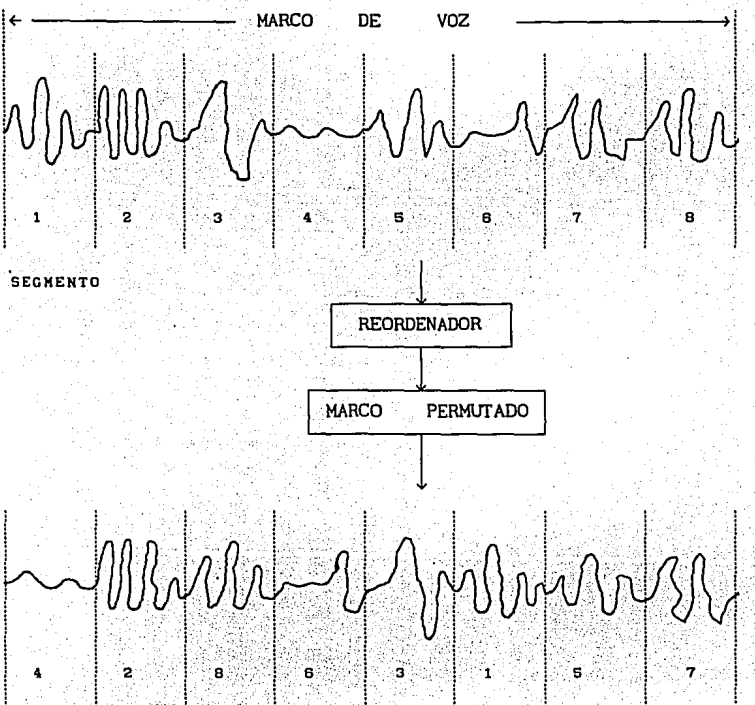



Fig. 4.3 Permutación de segmentos pertenecientes a un mismo marco de voz ([6], fig.5.5).

### IV.2.2 Algoritmo de Ciframiento en el Dominio del Tiempo. (Reordenación de muestras en el dominio del Tiempo).

El algoritmo de ciframiento para señales presentado en este inciso se basa en el método de reordenación de muestras en el tiempo de la señal de voz (ver Fig. 4.2), y utiliza el esquema de ciframiento RSA [15], además de un sistema de comunicación entre diversos usuarios basado en el método propuesto por Diffie-Hellman [20]. En el inciso IV.2.2.1 explicaremos el esquema RSA, y en la sección V.2.3, explicaremos el método de comunicación entre diversos usuarios.

### IV.2.2.1 Descripción del Esquema RSA.

El esquema de ciframiento RSA (Rivest, Shamir y Adleman [15]) utilizado para cifrar y descifrar el mensaje **M**, consiste de los siguientes pasos :

1.) El usuario **A** elige dos números primos **p** y **q** de diferente longitud cada uno de ellos.

2.) El mismo usuario **A**, calcula $R_A$ y $\phi(R_A)$ de la siguiente manera:

$$R_A = p\,q \qquad (4.1)$$

$$\phi(R_A) = (p-1)\,(q-1) \qquad (4.2)$$

donde $R_A$ Es el número de elementos en el campo.
$\Phi(R_A)$ Es el número de elementos "primos relativos" a $R_A$.

3.) El usuario **A** elige un número primo **e** y procede a calcular el el número **d**, con el auxilio del Algoritmo Extendido de Euclides [24], de tal manera que la siguiente congruencia cumpla con los valores de **e** y **d**.

$$ed \equiv 1 \pmod{(p-1)(q-1)} \qquad (4.3)$$

donde **d** se encuentra en el rango $1 \leq d \leq (p-1)(q-1)$.

En el caso de que el valor calculado **d**, además de los valores seleccionados, **p**, **q** y **e** no satisfagan la expresión (4.3), no se garantiza el correcto proceso de desciframiento del mensaje cifrado ( vease el ejemplo en la pag. 106).

4.) El usuario **A** forma su clave privada como la pareja de números $(d, \phi(R_A))$ la cual guarda en secreto. Además, el mismo usuario **A** forma su clave pública como la pareja de números $(e_A, R_A)$ y la pública en un directorio público de claves.

5.) Se representa el mensaje **M** por su equivalente en números enteros, es decir, el mensaje que va a ser cifrado se representa como un entero en el rango $\{1, \ldots, R-1\}$.

6.) Si el usuario **B** desea enviarle un mensaje cifrado al usuario **A**, el usuario **B** emplea la clave pública del usuario **A** para enviarle un mensaje cifrado a partir de la siguiente relación.

$$C \equiv M^{e_A} \bmod R_A \qquad 0 < C < R_A \qquad (4.4)$$

donde

**C** Es el criptograma resultante que se envía al usuario **A**.
**M** Es el mensaje original que es cifrado por el usuario **B**.
$(e_A, R_A)$ La clave pública del usuario **A**.

7.) Una vez que el usuario **A** tenga el mensaje cifrado, éste procede a descifrar el criptograma con la ayuda de su clave privada $d_A$ y a partir de la siguiente ecuación :

$$M \equiv C^{d_A} \bmod R_A \qquad 0 < M < R \qquad (4.5)$$

donde

**M** Es el mensaje descifrado que le envía el usuario **B**.

**C** Es el criptograma resultante cifrado por el usuario **B**, y enviado al usuario **A**.

$(d_A, \Phi(R_A))$ La clave privada del usuario **A**.

### IV.2.2.2 Aplicación del Esquema RSA para el ciframiento de Señales de Voz.

El algoritmo de ciframiento de señales presentado en este inciso, se basa en el esquema RSA y se aplica al método de reordenación de muestras en el dominio del tiempo y consiste de los siguientes pasos :

1.) Se escogen los valores de **p** = 5 y **q** = 11.

2.) Se escoge un bloque de $R_A$ muestras. La longitud del bloque $R_A$, se calcula de la siguiente manera :

$$R_A = p\ q = (5)(11) = 55$$

3.) El usuario **A** elige número primo **e** y enseguida procede a calcular su clave privada, **d**. En este caso **e** = 7 y **d** = 23.

4.) El usuario **A** forma su clave privada como la pareja de números ($d = 157, \Phi(n) = 2668$) la cual la guarda en secreto. Además, el mismo usuario **A** forma su clave pública como la pareja de numeros ($e = 17$, $n = 2773$) y la pública en un directorio público de claves.

5.) A cada una de las posiciones de las muestras de cada bloque se le aplica la ecuación (4.4) del esquema RSA.

$$C_i \equiv M_i^{e_A} \bmod R_A \qquad 0 < C < R_A$$

donde

$C_i$ Es la posición i-ésima de la muestra en el bloque cifrado.

$M_i$ Es la posición i-ésima de la muestra en el bloque a cifrar.

$(e_A, R_A)$ La clave pública del usuario **A**.

6.) El usuario **A** descifra el mensaje que le enviaron por medio de su clave privada $d_A$, utilizando la ecuación (4.5) del esquema RSA

$$M_i \equiv C_i^{d_A} \mod R_A \qquad 0 < M < R_A$$

donde

$C_i$ Es la posición i-ésima de la muestra en el bloque a descifrar.

$M_i$ Es la posición i-ésima de la muestra descifrada.

$(d_A, \Phi(R_A))$ La clave privada del usuario **A**.

El número de operaciones realizadas en el transmisor, si consideramos un bloque de $R_A$ muestras es el siguiente :

No. de operciones para el proceso de ciframiento $= R_A \times 2 \times \log_2 (e)$

donde

$R_A$ Es el número de muestras en el bloque a cifrar.

**e** Es el valor numerico de la clave utilizada para cifrar.

El número de operaciones realizadas en el receptor, si consideramos un bloque de $R_A$ muestras es el siguiente :

No. de operciones para el proceso de desciframiento $= R_A \times 2 \times \log_2 (d)$

donde

$R_A$ Es el número de muestras en el bloque a descifrar.

**d** Es el valor número rico de la clave utilizada para descifrar.

### IV.2.3. Sistema de Comunicación entre diversos usuarios.

En la segunda parte de este método se presenta un esquema de comunicación entre dos o más usuarios a partir de una clave común, tomando en cuenta las claves públicas y claves privadas de ambos usuarios.

En este sistema, dos usuarios **A** y **B** se ponen de acuerdo en una clave que se llama *clave común* a través de un Canal de Comunicación Público. O sea, que el usuario **A** calcula la clave común utilizando la clave pública del usuario **B** y su propia clave privada; mientras que el usuario **B** también usa la clave pública del usuario **A** y su clave privada propia. Haciendo operaciones con esas claves cada usuario, llegan al mismo resultado, esto es, la clave común de los dos usuarios. Ambos utilizan esa clave común para cifrar sus mensajes y su inversa para descifrarlos. Cualquier otra persona que no conozca alguna de las claves privadas de **A** o de **B** no puede calcular la clave común utilizando las claves públicas de ambos.

#### IV.2.3.1 Desarrollo del Método Hellman-Diffie.

Esta técnica aprovecha la dificultad de calcular logaritmos sobre un campo finito (campo de Galois) GF(p) con un número **p** de elementos [20]. (Los números $\{0,1,\ldots,(p-1)\}$, cumplen la aritmética módulo **p**).

Cada usuario puede generar su clave $y_i$ para publicarla, a partir de su una clave privada $x_i$, seleccionada en forma aleatoria de la siguiente manera ([20], ec. 4) :

$$y_i \equiv a^{x_i} \left[ \bmod p \right], \quad \text{para} \quad 1 \leq x_i \leq p-1, \qquad (4.6)$$

donde **a** es un elemento primitivo fijo de GF(**p**), (esto es, que el rango de las potencias de **a** está entre los elementos diferentes de cero de GF(**P**), o sea $\{1,2,\ldots,(p-1)\}$.

El cálculo de **y** a partir de **x** es computacionalmente fácil empleando el método de elevación exponencial cuadrática [24].

Así, el esfuerzo para calcular **y** a partir de **x** (que es el esfuerzo del usuario legítimo) a lo más es de $2\lfloor \log_2 p \rfloor$ multiplicaciones (recuerde que $1 \leq x \leq p-1$), donde $\lfloor \log_2 p \rfloor = \lceil \log_2 p \rceil + 1$, o sea la parte entera de $(\log_2 p)$ más 1.

Pero calcular **x** a partir de **y** (que es el esfuerzo del criptoanalista) es equivalente a calcular un logaritmo sobre el campo de Galois, o sea

$$x = \log_a y \qquad \text{sobre } GF(p),$$

y esto puede ser mucho más difícil. Para ciertos valores de **p** cuidadosamente seleccionado se pueden requerir del orden de **p** operaciones aún usando el mejor algoritmo que se conoce [25].

Entonces, cuando dos usuarios **i** y **j** se quieren comunicar en forma privada, ellos pueden calcular la clave común en forma independiente usando las claves privadas $x_i$, $x_j$, y las claves públicas $y_i$, $y_j$ respectivante. Esto es equivalente a que el usuario **i** busque la clave pública del usuario **j**, $y_j$, y usando su propia clave privada $x_i$ calcula la clave común $k_{ij}$ por medio de ([20], ec. 7) :

$$k_{ij} \equiv \left( y_j^{x_i} \mod p \right)$$

El usuario **j** calcula $k_{ji}$ del mismo modo, o sea :

$$k_{ji} \equiv \left( y_i^{x_j} \mod p \right)$$

Se puede ver que $k_{ij}$ es igual a $k_{ji}$, esto es,

$$k_{ij} \equiv \left( y_j^{x_i} \mod p \right) \equiv \left( a^{x_j} \right)^{x_i} \left( \mod p \right)$$

$$k_{ij} \equiv a^{x_j x_i} \left( \mod p \right) \equiv \left( a^{x_i} \right)^{x_j} \left( \mod p \right)$$

$$k_{ij} \equiv \left( y_i^{x_j} \mod p \right) \equiv k_{ji}$$

Una vez que encuentren la clave común $k_{ij}$ o $k_{ji}$, la pueden utilizar como la clave para cifrar, la inversa de $k_{ij}$, $k_{ij}^{-1}$, como la clave para descifrar, esto es, la pueden utilizar como clave para un sistema criptográfico de clave pública convencional.

## IV.3 CRIPTOGRAFIA EN AMPLITUD.

### IV.3.1 Introducción a la Criptografía en Amplitud.

El método de ciframiento que se presenta en este inciso, consiste en un algoritmo de ciframiento de clave pública en amplitud basado en el esquema **RSA**, (ver sección IV.2.2.1). Este método de ciframiento se divide en dos partes : (1) El algoritmo de ciframiento en amplitud, y (2) Un sistema de comunicación entre diversos usuarios.

Este método de ciframiento presenta ciertas modificaciones, con respecto al esquema de ciframiento propuesto en ([6], pag. 192), que fueron realizadas por el *autor de este trabajo de tesis* y son:

1.) Este esquema de ciframiento, utiliza un esquema de ciframiento de clave pública para el ciframiento de una señal.

2.) El ciframiento en **Amplitud** realizado en este inciso, consiste en dividir el valor de la muestra $M_i$ a cifrar en **nc** sub-bloques y posteriormente aplicar el esquema de ciframiento de clave pública a cada uno de estos sub-bloques $m_i$ para obtener el mensaje cifrado $c_i$ respectivo. Para posteriormente unir cada sub-bloque $c_i$ cifrado y formar la muestra $C_i$ cifrada. La finalidad de dividir la muestra a cifrar en nc sub-bloques es lograr un mejor ciframiento de la señal de voz.

### IV.3.2 Algoritmo de Ciframiento en la Amplitud.

El algoritmo de ciframiento propuesto en este inciso lo propone *el autor de este trabajo de tesis* para el ciframiento de una señal de voz en Amplitud.

El transmisor, para cifrar la señal en amplitud realiza los siguientes pasos :

1.) Se tiene un bloque de muestras de voz de tal manera que cada valor de la muestra está dentro de un intervalo de $-1 \leq x \leq 1$.

2.) Se toma una muestra de la señal de voz del bloque de muestras, de tal manera que esa muestra se pasa a un número entero.

3.) Se divide el valor de la muestra en $m_i$ sub-bloques de **nc** (número de cifras) cifras, de tal manera que cada sub-bloque $m_i$ sea menor que $R_A$.

4.) A cada sub-bloque de **mi** cifras se le aplica la ecuación (4.4) del esquema **RSA** (ver pag. 75), hasta cifrar el último **mi** sub-bloque de la muestra.

5.) El valor de la muestra durante el ciframiento es un número entero de **nc** cifras, que se pasa a un número fraccionario para poder transmitir el mensaje.

6.) Los pasos del 1.) a 5.), se aplican a cada una de las restantes muestras de la señal de voz y de esta manera obtenemos el mensaje cifrado.

Los pasos del algoritmo de descifrамiento (realizado en el receptor) son los siguientes :

1.) Se toma una muestra del mensaje cifrado que es un valor que se encuentra dentro de un intervalo de $-1 \leq x \leq 1$.

2.) El valor de la muestra se pasa a un valor entero y además para ese valor de la muestra se divide en **mi** sub-bloques de **nc** cifras.

3.) A cada uno de estos sub-bloques de las muestras se le aplica la ecuación (4.5) del esquema RSA (ver pag. 76).

4.) El valor de la muestra durante el descifrамiento es un número entero de **nc** cifras, que se pasa a un número fraccionario dentro del intervalo $-1 \leq x \leq 1$, con la finalidad de recuperar la muestra de la señal original de voz .

5.) Los pasos del 1.) a 4.) se aplican a cada una de las restantes muestras del mensaje cifrado de tal manera que se obtiene el mensaje descifrado.

### IV.3.2.1 Aplicación del Sistema RSA para el ciframiento de Señales de Voz en Amplitud.

El algoritmo de ciframiento de señales de voz en Amplitud presentado en este inciso se basa en el esquema RSA y consiste de los siguientes pasos :

1.) El usuario **A** elige los valores de $p = 47$ y $q = 59$.

2.) Se escoge un bloque de $R_A$ muestras. La longitud del bloque $R_A$, se calcula de la siguiente manera :

$$R_A = p\ q = (47)\ (59) = 2773$$

3.) El usuario **A** elige un número primo **e** y enseguida procede a calcular su clave privada, **d**. En este caso $e = 17$ y $d = 157$.

4.) Se selecciona un número de muestras $R_A$ a cifrar, además del número de dígitos a cifrar nc, de tal manera que el número de dígitos a cifrar sea menor que el número de dígitos de $R_A$.

5.) Si se tiene la siguiente muestra de señal de voz perteneciente a un bloque de $R_A$ muestras de longitud con una amplitud de

x(t)= 0.000310979462181776756.

La muestra se divide en sub-bloques de nc cifras.

6.) A cada sub-bloque de la muestra se le aplica la ecuación (4.4) del esquema RSA (ver pag 75) hasta terminar con el último $M_i$ sub-bloque de la muestra.

$$C_i \equiv M_i^{e_A} \bmod R_A \qquad 0 < C < R_A$$

donde

$C_i$ Es el i-ésimo sub-bloque de la muestra cifrada.
$M_i$ Es el i-ésimo sub-bloque de la muestra a cifrar.
$(e_A, R_A)$ La clave pública del usuario A.

7.) Se concatenan cada una de los sub-bloques de la muestra y se pasa a un número fraccionario para posteriormente transmitirlo.

8.) Se repiten los pasos 5.) al 7.) para el ciframiento de las muestras restantes del bloque de la señal de voz.

Los pasos para el desciframiento (realizados en el receptor) son los siguientes :

1.) Se toma una muestra del mensaje cifrado.

$x_c(t)$ = 0.000015532073066183334

2.) Como el valor de la muestra es un número fraccionario, se divide la muestra en sub-bloques y cada sub-bloque se pasa a un número entero.

$x_c(t)$ = 0.0000 1553 2073 0660 1833 34

3.) A cada uno de estos sub-bloques se les aplica la ecuación 4.5 (ver pag. 76) con la cual se obtiene la muestra descifrada, que es :

x(t) = 00 03 10 97 94 ( muestra descifrada )

4.) Se concatenan cada uno de los sub-bloques de tal manera que se tenga un sólo bloque de números

$x(t) = 0.0003109794$

5.) Se repiten los pasos 1.) a 4.) para cada una de las demás muestras del bloque.

El número de operaciones realizadas en el transmisor, si consideramos un bloque de $R_A$ muestras y un número nc de dígitos a cifrar es el siguiente :

No. de operciones para el proceso de ciframiento $= R_A \times nc \times 2 \times \log_2 (e)$

donde

- $R_A$ Es el número de muestras en el bloque a cifrar.
- e Es el valor número de la clave utilizada para cifrar.
- nc Es el número de dígitos en que se divide cada muestra a cifrar.

El número de operaciones realizadas en el receptor, si consideramos un bloque de $R_A$ muestras y un número de m-c de dígitos a descifrar es el siguiente :

No. de operaciones para el proceso de desciframiento $= R_A \times m\text{-}c \times 2 \times \log_2 (d)$

donde

- $R_A$ Es el número de muestras en el bloque a descifrar.
- d Es el valor numerico de la clave utilizada para cifrar.
- m-c Es el número de dígitos en que se divide cada muestra a cifrar.

### IV.3.3 Comunicación entre varios usuarios.

#### IV.3.3.1 Realización de la clave común por elevación exponencial.

Una vez que los usuarios i y j obtienen su clave común $k_{ij}$, la pueden utilizar para cifrar sus mensajes. Si denotamos a M, $k_{ij}$ y C como el mensaje original, la clave, y el criptograma respectivamente, con las siguientes restricciones :

$$1 \leq M \leq p-1$$
$$1 \leq C \leq p-1$$
$$1 \leq k_{ij} \leq p-2$$

y

$$\gcd(k_{ij}, p-1)=1$$

donde p es un número primo grande (recuerde que $\Phi(p) = p-1$, si p es un número primo).

La primera restricción sirve para que se pueda aplicar el Teorema de Euler [24], en donde **M** tiene que ser un primo relativo con respecto a **p**. La segunda restricción se cumple para realizar las operaciones módulo **p**. La tercera y cuarta restricción sirven para que la inversa de $k_{ij}$ exista, donde $k_{ij}$ tiene que ser primo relativo con respecto a $\Phi(p)$, que es la última restricción, obviamente que $k_{ij}$ tiene que ser menor que **p-1**; esto es, que $k_{ij}$ tiene que ser menor o igual a **p - 2**.

Entonces, el mensaje original se cifra de la siguiente manera

$$C \equiv M^{k_{ij}} (\text{mod } p)$$

El receptor del mensaje, al recibir **C**, lo puede descifrar con la inversa de la clave común, $k_{ij}^{-1}$, y aplicando el Teorema de Euler.

$$M \equiv C^{k_{ij}^{-1}} \left[\text{mod } p\right] \equiv \left[ M^{k_{ij}} \right]^{k_{ij}^{-1}} (\text{mod } p) \equiv M \left[ \text{mod } p \right]$$

donde

$$k_{ij}\ k_{ij}^{-1} \equiv 1 \bmod \Phi(p) = 1$$

## IV.4 CRIPTOGRAFIA EN EL DOMINIO DE LA FRECUENCIA.

### IV.4.1 Introducción a la Criptografía en el Dominio de la Frecuencia.

Una alternativa para realizar el cifrado de señales de voz es llevarlo a cabo en el dominio de la frecuencia. Existen varios métodos de ciframinto de señales de voz en la frecuencia [6] como son : (1) Inversión en frecuencia. (2) Reordenadores de bandas. (3) Reordenadores de Espectro de frecuencia utilizando DFT [6]. A continuación se describirán brevemente cada uno de ellos.

**Inversión en Frecuencia :**

La inversión en frecuencia ([6], pag.21), como literalmente se especifica, es mover las componentes de frecuencias altas de la señal de voz a las correspondientes frecuencias bajas, y las componentes de frecuencias bajas a las correspondientes frecuencias altas (ver Fig. 4.6). Este sistema de ciframinto presenta un nivel bajo de seguridad.

En un principio se pensaría que para obtener la frecuencia invertida de una señal discreta de **n** muestras, primero se obtendría la DFT de las **n** muestras de una señal de voz, la cual nos daría **n** componentes de frecuencia y después se realizaría el proceso de inversión de la siguiente manera :

| No de componentes en frecuencia | Nueva posición de la inversión |
|---|---|
| 0 | N-1 |
| 1 | N-2 |
| 2 | N-3 |
| ⋮ | ⋮ |
| N-3 | 2 |
| N-2 | 1 |
| N-1 | 0 |

Pero la acción anterior no tiene el efecto esperado, esto se comprueba a partir de las dos siguientes aseveraciones :

a) La inversión de la DFT de una señal, excluyendo la primera componente, causa una correspondiente inversión en el tiempo de la señal, excluyendo la primera muestra.

b.) La inversión de la señal analógica se obtiene si las muestras impares de la señal de voz son multiplicadas por -1.

Por lo tanto, la inversión de la DFT de una señal no tiene algún uso para el cifrамiento de voz. Ya que no representa la inversión de la frecuencia analógica.

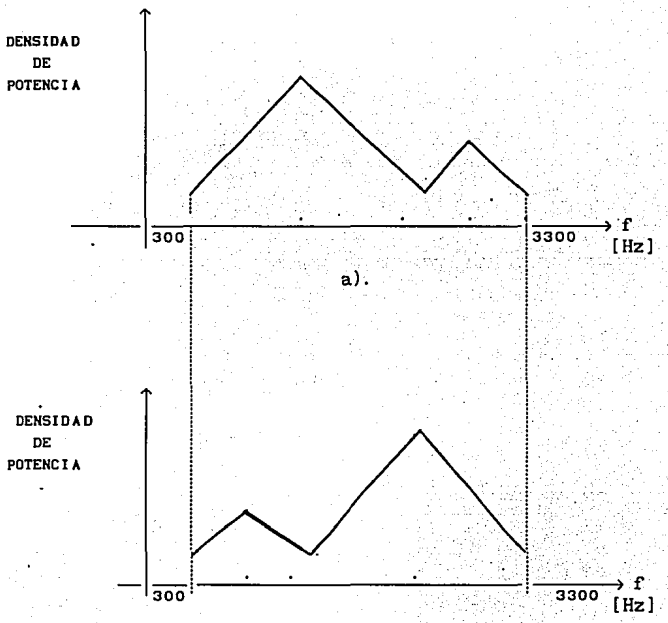



Fig. 4.6 Inversión en Frecuencia ([6], fig. 4.1).
a)Densidad espectral de potencia de la señal de voz original, y
b)Densidad espectral de potencia del mensaje cifrado (señal con con frecuencia invertida).

A continuación se analizará cómo es posible representar la inversión de la freceuncia analógica de una señal real através de la DFT.

Sea una señal periódica x[n] de **N** muestras, además de

**N** = número de muestras de la señal por período.
**Ns** = número de muestras por segundo.
**T** = **N/Ns** período de la señal.
**f** ≥ **Ns/N** frecuencia fundamental de la señal.

Entonces, a partir del Teorema del muestreo, nuestra señal de banda limitada tendrá el rango de 0 a **Ns/2** Hz, y la componente de frecuencias más alta de la DFT corresponde a la armónica **Ns/N**, la cual ocurre a **1/2Ns** Hz. Dividiendo el ancho de banda entre la frecuencia fundamental, resulta :

$$(Ns/2)/(Ns/N) = N/2$$

donde **N/2** es la armónica de mayor frecuencia y a la vez el pivote de simétría :

X(0) Corresponde a la componente espectral de 0 Hz.
X(1) Corresponde a la componente espectral de **Ns/N** Hz.
X(N/2) Corresponde a la componente espectral de **Ns/2** Hz.

Por lo tanto, la inversión de frecuencia analógica de una señal de n muestras se obtiene al realizar una permutación cíclica a la derecha de **N/2** muestras en la DFT (ver Fig. 4.7).

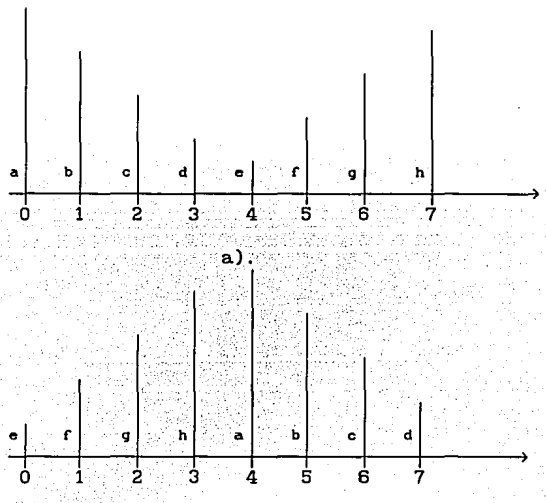



Fig. 4.7 Inversión de Frecuencia analógica utilizando la DFT. a.) DFT con n = 8 para una señal real ([6], fig. 4.4), y b.) Inversión de frecuencia de a.) ([6], fig. 4.5).

**Reordenadores de bandas.**

En este tipo de sistemas cifradores ([6], pag.135), para obtener el espectro de frecuencia del bloque del mensaje de voz a cifrar, se divide en sub-bandas la señal de voz, las cuales se reordenan para obtener el espectro del correspondiente bloque del criptograma. En este método se permite una modificación algo "sofisticada" para algunas de las sub-bandas que deben ser invertidas (ver Fig. 4.8).

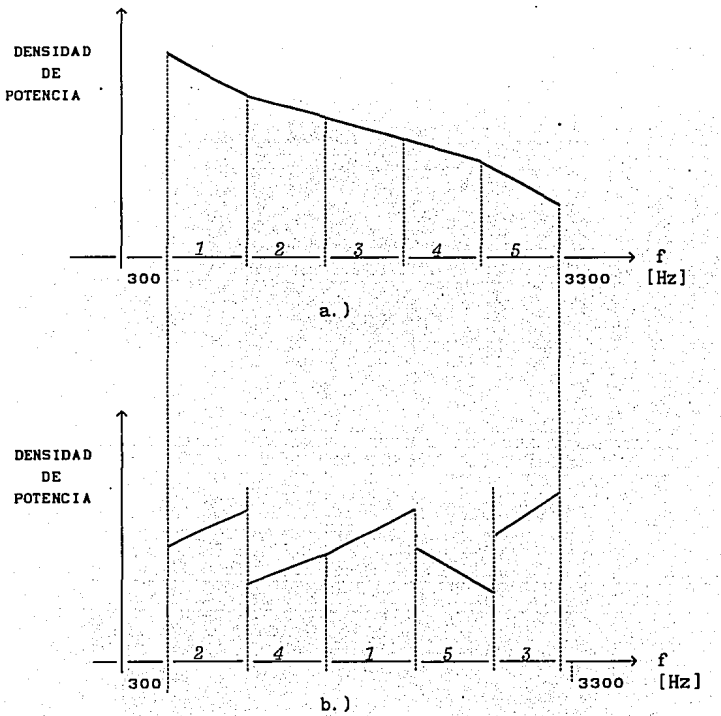



Fig.4.8. División en bandas. Espectro de voz dividido en 5 sub-bandas ([6], fig. 4.10).
a) Orden de las sub-bandas. b) Espectro re-ordenado.

**Reordenadores de Espectro de Frecuencia utilizando DFT.**

Con este tipo de cifradores se realiza un procesamiento digital de señales muy rápido y son considerados como la generalización de los sistemas reordenadores de bandas ([6], pag. 124). Estos sistemas cifradores, dada la velocidad que requieren para un procesamiento en tiempo real, necesitan de recursos de cómputo especializados para el procesamiento digital de señales.

El principio de funcionamiento de los sistemas reordenadores de espectro es el siguiente :

1.) Se tiene un bloque de mensaje (señal de voz) de n muestras.
2.) Se le aplica la DFT.
3.) Se permutan los coeficientes de la DFT. La permutación de los coeficientes de la **DFT** se realiza aplicando el esquema de cifrамiento de clave pública propuesto por Elgamal, T. [26], a los coeficientes de la parte real o a los coeficientes de la parte imaginaria o ambos coeficientes.

4.) A la DFT reordenada se le aplica IDFT para obtener el criptograma a transmitir.

Como se sabe, una señal de voz (mensaje a transmitir) x[r] es una señal real, al aplicar la DFT a la señal x[r] se obtiene una parte real Re{X(r)} y una parte imaginaria Im{X(r)}, que son par e impar respectivamente, si aplicamos la transformacion de cifrado $\mathbb{T}$ a la parte real de la DFT "$\mathbb{T}${Re{X(r)}", dicha transformación debe ser par, enseguida aplicamos la inversa de la $DFT^{-1}$ tanto a la parte real como a la parte Imaginaria $DFT^{-1}\{\mathbb{T}[Re\{X(r)\}$ y Im{X[r]}}, con la finalidad de obtener una "senal física".

Como se sabe la DFT de una señal real cumple con las reglas de simetría :

siendo
x[r] el conjunto de muestras de la señal, y
X[r] el conjunto de muestras de la DFT de x[r] para r=0,1,...,N-1.

$$|X(r)|=|X(N-r)| \text{ y}$$

Entonces, para la DFT reordenada (permutada) se deben de seguir cumpliendo estas reglas.

### IV.4.2 Algoritmo de Ciframiento de clave Pública en la Frecuencia. (Reordenador de espectro de frecuencia utilizando DFT).

El algoritmo de ciframiento presentado en este inciso se basa en el método del Reordenador de Espectro. Este método de ciframiento se divide en dos partes : (1) El algoritmo del Reordenador de Espectro basado en el esquema Elgamal T.y (2) Un Sistema de Comunicación entre diversos usuarios basado en identificación de información.

El transmisor, para reordenar el espectro, realiza los pasos siguientes :

1.) Obtiene un bloque del mensaje de **n** muestras.

2.) Aplica la **DFT** (FFT) al bloque de la señal de voz.

3.) Permuta los coeficientes de la **DFT** (FFT).
La permutación de los coeficientes de la FFT se lleva a cabo aplicando el esquema de ciframiento de clave pública propuesto por Elgamal, T. [26] a los coeficientes de la **FFT**.

4.) Aplica la $\mathbf{DFT}^{-1}$ (IFFT) al bloque de la señal de voz y de esta manera se obtiene el mensaje cifrado analógico a transmitir.

El receptor, para recuperar el mensaje original, realiza los siguientes pasos :

1.) Toma un bloque del mensaje cifrado de **n** muestras.

2.) Aplica la **DFT** (FFT) al bloque de la señal de voz cifrada.

3.) Permuta los coeficientes de la **DFT** (FFT).
La permutación de los coeficientes de la FFT se lleva a cabo por medio del algoritmo de desciframiento propuesto por Elgamal, T. [26] (ver *proceso de descifrado* ).

4.) Aplica la $\mathbf{DFT}^{-1}$ (IFFT) al bloque de la señal de voz y de esta manera se obtiene el mensaje original transmitido.

**IV.4.2.1 Descripción del Esquema propuesto por Elgamal T.**

**A.) Inicialización del Sistema Criptográfico.**

1.) Todos los usuarios del sistema son informados de un número primo **p** "grande" junto con una *raiz primitiva* **a modulo p.** De esta manera **a** es un entero menor que **p**, y cumple con las propiedades siguientes ([23], pag. 193) :

$$a^{p-1} \equiv 1 \pmod{p}.$$

Además,

$$a^{d-1} \not\equiv 1 \pmod{p}$$

Para cualquier **d**, con $1 < d < p$ .

2.) El usuario **B** selecciona de manera aleatoria su clave privada, $x_B$, de tal manera que cumpla con la condición siguiente :

$$1 \leq x_B \leq p-1$$

3.) La clave pública de **B** es el entero $y_B$ calculado a partir de la ecuación siguiente :

$$y_B = a^{x_B} \pmod{p}.$$

**B.) Proceso de Ciframiento.**

Suponga ahora que el usuario **A** envía al usuario **B** un mensaje **M**, donde **M** se encuentra en el intervalo $1 \leq M \leq p-1$.

Para cifrar el mensaje **M**, el usuario **A** procede como sigue ([23], pag. 194) :

1.) Selecciona de manera aleatoria el entero $k_b$ tal que

$$1 \leq k_b \leq p-1.$$

2.) Calcula su "clave"

$$K_B = y_B^{k_b} \pmod{p}$$

3.) Cifra el mensaje **M** como el par de enteros $(C_1, C_2)$, definidos como :

$$C_1 = a^{k_b} \pmod{p}, \quad C_2 = K_B M \pmod{p}$$

De esta manera, el proceso de cifrамiento **E**, es el mapeo

$$E(M) \longrightarrow C = (C_1, C_2)$$

Con lo cual se tiene el doble de longitud del mensaje a cifrar.

**C.) Proceso de Descifrамiento.**

Para descifrar el mensaje cifrado recibido $(C_1, C_2)$, el receptor (usuario B) procede como sigue ([23], pag. 194) :

1.) Algoritmo de descifrамiento

Paso 1: Recupera la clave $K_B$ por la regla

$$K_B = y_B^{kb} = a^{XBkb} = \left[ a^{kb} \right]^{XB}$$

$$= C_1^{XB} \pmod{p}$$

donde toda la aritmética es módulo **p**.

Esto es fácil para el usuario B, dado que $x_B$ es su clave privada.

Paso 2 : Recupera el mensaje **M** dividiendo $C_2$ por $K_b$.

$$M \equiv \frac{C_2}{K_b} \mod p$$

### IV.4.3 Sistema de comunicación entre diversos usarios basado en Identificación de información.

Un sistema de distribución de claves con identificación de información ID-KDS (de las siglas en inglés) se presenta en este inciso. Este ID-KDS utiliza una identificación de información indiviual de cada uno de los usuarios (por ejemplo, nombre, dirección, etc.) en lugar del archivo público usado en el esquema Hellman-Diffie (ver sección IV.2.3.1.).

La implantación de criptosistemas aparentan una gran dificultad debido al complicado manejo de claves. Si cada usuario tiene que guardar tantas claves como sea el número de usuarios, entonces es necesario un gran espacio de memoria. Para decrementar los costos de memoria, surge la idea de involucrar un centro de distribución de claves. Cada usuario necesita solamente mantener la clave maestra de cifrамiento para usarse entre él y la central. Cuando el usuario requiere una palabra clave, el centro conoce la palabra clave cifrada con la clave maestra de cifrамiento.

Este esquema **ID-KDS**, se puede realizar de dos maneras que son: **A.**) Fase de Comunicación con Autentificación Indirecta, y **B)** Fase de Comunicación con Autentificación Directa, como se describirá en la fase de comunicación (ver pag. 94).

### IV.4.3.1 Descripción del Sistema de Identificación de Información.

El sistema **ID-KDS** tiene dos fases: 1.) Fase de emisión de carnet's, 2.) Una fase de comunicación. En la primera fase, es el control distribuido de carnet's para usuarios. En la segunda fase, los usuarios generan las claves empleadas y se comunican secretamente con otro usuario usando el carnet.

**A). Fundamentos del sistema ID-KDS.**

**1.) Fase de Emisión de carnet's :**

i.) El sistema **ID-KDS** realiza la emisión de carnet's en base a la elección de dos números primos **p q**.

ii.) Selecciona un número primo **e** y procede a calcular el número entero **d** con el auxilio del algoritmo extendido de Euclides de tal manera que satisfaga la siguiente ecuación ([27], ec. 1) :

$$e\,d \ (\mathrm{mod}\ (p-1)\ (q-1)) = 1 \qquad (4.14)$$

donde ambos numeros **e** y **d**, son menores que $n = pq$.

Si el valor calculado **d**, no satisface la expresión (4.14), no se garantiza que el proceso inverso de identificación del usuario se realice de manera correcta.

iii.) El sistema **ID-KDS** también determina un entero **g**, el cual es un elemento primitivo en **GF(p)** y **GF(q)**.

iv.) Para cada usuario **i**, cuya información de identificación es $ID_i$, la oficina de control calcula el entero $S_i$ ($i = 1,2,\ldots$) ([27], ec. 2) :

$$s_i = ID_i^{-d} \ (\mathrm{mod}\ n) \qquad (4.15)$$

y la oficina de control almacena el conjunto de enteros (**n, g, e,** $S_i$) en el carnet para los diversos usuarios **i**, a la vez que lo distribuye hacia los demas usuarios.

Las ecuaciones (4.14) y (4.15) indican ([27], ec. 3) :

$$s_i^e \ ID_i \ (\mathrm{mod}\ n) = 1 \qquad (4.16)$$

Por lo tanto, **d** se guarda en secreto por cada usuario **i**. Además $S_i$ es conocido solamente por el usuario **i**, y **n**, **g** y **e** son comunes para todos los usuarios. La Fig. 4.10a, ilustra la fase de emisión de carnet.

**2) Fase de Comunicación.**

**A.) Fase de Comunicación con Autentificación Indirecta.**

i.) Cuando los usuarios **i** y **j** desean conseguir la clave común de de trabajo $W_{ij}$, el usuario **i** genera un número aleatorio $r_i$ y envía al usuario **j** el entero **x** ([27], ec. 4 ) :

$$x_i = s_i \; g^{r_i} \pmod{n} \qquad (4.17)$$

ii.) El usuario **j** también genera un número aleatorio $r_j$ y envía al usuario **i** el entero $x_j$ ([27], ec. 5 ) :

$$x_j = s_j \; g^{r_j} \pmod{n} \qquad (4.18)$$

iii.) Entonces, los usuarios **i** y **j** calculan cada uno su clave común de trabajo $WK_i$ y $WK_j$, respectivamente, como sigue ([27], ec. 6 ) :

$$WK_i = (x_j^e \; ID_j)^{r_i} \pmod{n} \qquad (4.19)$$

$$WK_j = (x_i^e \; ID_i)^{r_i} \pmod{n} \qquad (4.20)$$

Las ecuaciones (4.19) y (4.20) llevan al hecho de que las claves comunes empleadas son iguales ([27], ec. 7 ) :

$$WK_i = WK_j = g^{e \times r_i \times r_j} \pmod{n} \qquad (4.21)$$

Este sistema **ID-KDS** autentifica usuarios en forma indirecta, es decir, el receptor no tiene algún tipo de dato del emisor.

La Fig. 4.10b muestra la fase de comunicación para un sistema **ID-KDS**.

**B.) Fase de Comunicación con Autentificación Directa.**

i.) El usuario i genera un número aleatorio $r_i$ y envía al usuario j los enteros $x_i$, $y_i$ :

$$x_i = g^{e \times r_i} \pmod{n} \qquad (4.22)$$

$$y = s_i \; g_i^{c_i \; r_i} \pmod{n} \qquad (4.23)$$

donde $c_i$ es un número cuyo valor está en función de $x_i$, de la dirección del usuario j, código postal del usuario i, tiempo, etc. ([27], ec. 11 ):

$$c_i = \text{hash}(x_i, ID_i, ID_j, \text{Tiempo}_i) \qquad (4.24)$$

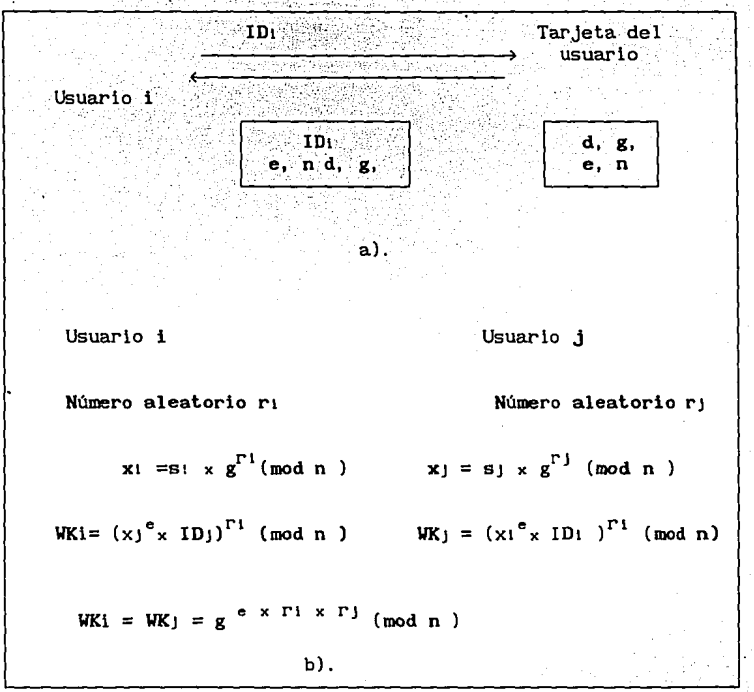



Fig. 4.10 Sistema de Identificación de información ([27], fig.1). a.) Fase emisión de carnet. b) Fase de Comunicación.

ii.) El usuario j también genera un número aleatorio $r_j$ y envía al usuario i, $x_j$, $y_j$, satisfaciendo ([27], pag. 482 ) :

$$x_j = g^{e\, r_j} \pmod{n} \qquad (4.25)$$

$$y_j = s_j \; g^{c_j \; r_j} \pmod{n} \qquad (4.26)$$

$$c_j = \text{hash}(x_j, ID_j, ID_i, \text{Tiempo}_j) \qquad (4.27)$$

iii.) El usuario i puede autentificar al remitente si la siguiente ecuación se cumple ([27], ec.15 ) :

$$ID_j = \frac{x_j^{c'j}}{y_j^{e}} \pmod{n} \qquad (4.28)$$

donde c'j es el número calculado por el usuario i en (4.27). Con esto se obtiene la autorización directa. Si $x_j$ es cambiada hacia otro número por usuarios no-autorizados, $c_j$ no es de igual valor que $c_j$ y por lo tanto no se cumple. Esta es la razón por la cual $c_j$ es dependiente de $x_j$. El usuario i coloca la clave empleada $WK_i$ ([27], ec. 16) :

$$WK_i = x_j^{r_i} \pmod{n} \qquad (4.29)$$

El usuario j puede autentificar al usuario i y obtener la clave empleada $WK_j$ de la misma manera. Ambas claves de trabajo empleadas $WK_i$ y $WK_j$ son iguales a la ecuación (4.21).

## IV.5 CIFRAMIENTO DE LA SEÑAL DE VOZ A TRAVES DE LA MANIPULACION DE LOS PARAMETROS LPC.

### IV.5.1 Introdución.

Sambuer y Jayant [14] proponen varios métodos para la manipulación de los parámetros **LPC** (de las siglas en inglés) y de esta manera lograr el ciframiento de una señal de voz. Específicamente, proponen el rearreglo temporal o permutación de la secuencia de los parámetros **LPC**. Esto último hace pensar que con este método se tiene un mayor potencial de ciframiento que con las técnicas de ciframiento temporal (ver inciso **IV.2, IV.3** Y **IV.4**), en términos del tiempo necesario para "violar la seguridad de la clave".

En este inciso se propone un nuevo método de ciframiento de los parámetros **LPC**. El método de ciframiento propuesto es una combinación de :1.) Un algoritmo de ciframiento de clave pública basado en el esquema RSA-Williams, y (2) De un Método de Comunicación entre diversos usuarios realizado en forma matricial dicho método de comunicación fue *realizado por el autor de este trabajo de tesis.*

### IV.5.2 Algoritmo de ciframiento de clave pública para la manipulación de los parámetros LPC .

El método **LPC** se emplea para la comprensión de señales de voz. En el método **LPC**, la señal de voz se modela como la salida de un filtro de "solo polos" (All-pole) H(z), y se excita por una secuencia de pulsos separados por el período del pitch para sonidos "de voz" (voiced) o ruido pseudo-aleatorio para sonidos de "no voz" (unvoiced). Estas suposiciones implican que para una determinada trama de voz, la secuencia de salida de la voz se obtiene a través de ([14], pag. 1375) :

$$s[n] = \sum_{k=1}^{p} a[k]\, s[n-k] + G u[n]$$

donde **p** Es el número de polos para representar el modelo.
**u[n]** Es la señal apropiada de excitación de entrada,
**G** Es la ganancia del filtro, y
**a[k]'s** Son los coeficientes que caracterizan el filtro. (Coeficientes de Predicción Lineal).

La generación de voz en este modelo requiere de un conocimiento del pitch, de los parámetros del filtro (coeficientes a[k]'s ó ki's) y la ganancia G del filtro (amplitud de excitación) en cada *trama* de voz.

El ciframiento de los parámetros se aplica directamente sobre los coeficientes de reflexión $K_i$'s o sobre los coeficientes de correlación parcial **parcor** (de las siglas en inglés) $-k_i$'s, o sobre los coeficientes **log-area** $g_i$, dado que todos estos coeficientes mantienen la estabilidad del filtro de predición lineal **H(z)**, además de que este filtro es extremadamente sensible para pequeñas perturbaciones de cualquiera de estos coeficientes.

Los coeficientes **log-area** se relacionan no-linealmente con los coeficientes **parcor** de la siguiente manera ([14], pag. 1376) :

$$g_i = \log \frac{1 + k_i}{1 - k_i}$$

donde los $k_i$'s son denominados coeficientes de **parcor**.

Si denotamos $a_i^{(j)}$ como el i-ésimo coeficiente de predición lineal para el j-ésimo polo del modelo de preción lineal, entonces (ver pag. 40)

$$k_i = a_i^{(j)}$$

Los coeficientes de parcor tienen la siguiente propiedad :

$$| k_i | < 1, \quad i = 1,\ldots,p$$

es decir, los valores de $k_i$ están normalizados y con esto se garantiza que el filtro de predicción lineal es estable. Esto es, una pequeña variación en los coeficientes de **parcor** o en los coeficientes de **log-area** no afectan la estabilidad del filtro modelado.

Sambuer y Jayant [14], también proponen la siguiente medida de distancia para cuantificar la similitud entre el valor de los parámetros a cifrar y los valores de los parámetros descifrados.

**Medida de Distancia**

La medida de distancia LPC se define como ([14] pag. 1381) :

$$d_n = \ln (a_n V a_n / b_n V b_n)$$

donde

$a_n$ Es el vector de coeficientes originales LPC $(1, a1, \ldots, ap)$ correspondientes a la n-ésima trama de la señal de voz.

$b_n$ Es el vector de coeficientes LPC determinados después de la manipulación de los parámetros correspondientes a la n-ésima trama.

y

$$V = [v(|i-j|)], \quad (i, j = 0, 1, \ldots, p)$$

donde v(i) son los coeficientes de correlación normalizados que se calculan directamente a partir de $b_n$.

La medida $d_n$ es muy empleada en problemas de reconocimiento de voz, reconocimiento de parlantes, etc. Gray and Markel [20], han demostrado que la medida $d_n$ es muy parecida a la raíz cuadrada del valor medio del cuadrado de la diferencia de los espectros **rms espectral.**

**IV.5.2.1 Descripción del Esquema propuesto por RSA-Rabin-Willians.**

El algoritmo de ciframiento consiste de los pasos siguientes :

**A.) Inicialización del Sistema.**

1). El usuario selecciona un par de números primos **p** y **q**, grandes pero de diferente longitud los cuales guarda en secreto y calcula el valor de **R** como ([33], pag. 358 ) :

$$R = p \times q .$$

**B.) Proceso de Ciframiento.**

1.) Si el usuario $U_i$ desea enviar el mensaje **M**, como es usual $0 < M < R$, hacia el usuario $U_j$, lo realiza empleando la siguiente congruencia ([33], pag. 358 ) :

$$C \equiv M^2 \pmod{R} \qquad (4.30)$$

donde $0 < C < R$.

Entonces el usuario $U_i$ envía el mensaje cifrado **C** hacia el usuario $U_j$.

**C.) Proceso de Descifrado.**

El receptor $U_j$, recupera el mensaje **M** a partir del mensaje cifrado **C**, resolviendo las congruencias siguientes ([33], pag. 358) :

$$\begin{aligned} x^2 &\equiv C \pmod{p} \\ y^2 &\equiv C \pmod{q} \end{aligned} \qquad (4.31)$$

para **x** y **y**.

El usuario $u_j$ recupera el mensaje original **M**, a partir del mensaje cifrado **C**, resolviendo las congruencias $M \equiv \pm x^2 \pmod p$ y $M \equiv \pm y^2 \pmod q$, empleando el teorema del residuo chino [29]. Además **M** debe tener algún género de redundacia interna, para poder seleccionar el mensaje **M** correcto a partir de los cuatro posibles candidatos.

Existen dos dificultades con este esquema :

i). Aunque si bien hay $O(\log p)$ métodos probabilísticos para resolver la congruencia cuadrática.

$$x^2 \equiv M \pmod p$$

donde **p** es un número primo.

ii) Existe una ambigüedad 4:1 en la selección correcta del mensaje descifrado, y esto es un problema, especialmente si la redundacia interna en el mensaje **M** es minimizada. Es decir, no se sabe con exactitud cual de las cuatro valores que satisfacen la ecuación (4.31) es el mensaje correcto. Además la solución de la ec. (4.31) y el subsecuente uso del teorema del residuo Chino consumen demasiado tiempo.

## IV.5.3 Sistema de Comunicación entre diversos usuarios.

### IV.5.3.1 Sistema de comunicación entre diversos usuarios realizado en forma Matricial.

El sistema de comunicación entre diversos usuarios consiste de los siguientes pasos :

1.) El usuario $U_i$ define una matriz $A_i$ orden $n \times n$, en donde los elementos de la matriz $A_i$ son elementos primitivos de GF(p). La matriz $A_i$ se dá a conocer públicamente.

2.) El mismo usuario $U_i$ define una matriz $X_i$ de orden $n \times n$, en donde los elementos de la matriz $X_i$ se eligen de manera aleatoria. La matriz $X_i$ se guarda en secreto.

3.) Cada usuario $U_i$ genera su clave pública $Y_i$, donde $Y_i$ es una matriz de orden $n \times n$ que tiene sus elementos definidos por :

$$y_{ij} \equiv a_{ij}^{x_{ij}} \pmod p, \quad i,j = 1,2,\ldots,n$$

y se denota como :

$$Y_1 \equiv A_1^{X_1} \pmod p$$

Este usuario publica su matriz $Y_1$.

Cualquier otra persona no puede calcular **X** a partir de **Y** por la dificultad de calcular logaritmos sobre GF(p).

4.) Cuando dos usuarios $U_1$ y $U_2$ se quieren comunicar privadamente, ellos calculan su clave común de la siguiente manera :

$$K_{12} \equiv Y_2^{X_1} \pmod p = Y_1^{X_2} \pmod p$$

donde $Y_1$, $Y_2$ son las matrices públicas de los usuarios $U_1$ y $U_2$.
$X_1$, $X_2$ son las matrices privadas de los usuarios $U_1$ y $U_2$ respectivamente.

La matriz de la clave $K_{12}$ es de la misma dimensión que la matriz **Y** que a su vez es de dimensión nxn.

5.) El ciframiento del mensaje es de forma matricial, es decir, si $k_{12}$ es no singular, se puede cifrar un mensaje original **M** que tiene forma matricial de orden nxr, multiplicando **M** por $k_{12}$ y de esta manera obtenemos la matriz de criptograma **C** de orden nxr :

$$C = K_{12}M$$

Para que se puedan multiplicar las matrices **K** y **M**, la matriz **M** tiene que tener dimensión adecuada, es decir, **M** tiene que ser de dimensión nxr, donde n es el orden de la matriz cuadrada **K**. Esto es que **M** tiene nxr elementos. Si el número de elementos de la matriz **M** es menor que nxr, o sea que este número es igual a nxr-s (donde s<n)), entonces se asignan números aleatorios a los s elementos que no tienen información.

6.) Para descifrar el criptograma **C**, se premultiplica a la matriz C, por la matriz inversa de $K_{12}$, $K_{12}^{-1}$, y de esta manera se obtiene **M** :

$$M \equiv K_{12}^{-1} C = K_{12}^{-1} ( K_{12} M) = M$$

En este caso, la matriz de clave común $K_{12}^{-1}$, tiene también la restricción de que $K_{12}$ tiene que ser no singular para que $K_{12}^{-1}$ exista.

Sin embargo, esta restricción es mucho más fácil de cumplir comparada con la restrición de que $gcd(K_{ij},(p-1)) = 1$ para el caso de la realización de la clave común por elevación exponencial descrita en la sección IV.3.3.1 de este trabajo. Esto, es debido a que la posibilidad de que el determinante de $K_{12}$ sea igual a cero es demasiado pequeña (casi nula) comparada con la posiblidad de que el determinante de $K_{12}$ sea cualquier número diferente de cero, para una matriz $K_{12}$ que tiene los elementos calculados a partir de otros elementos seleccionados aleatoriamente.

CAPITULO

C I N C O

# PROPUESTA DE UN ALGORITMO DE CIFRAMIENTO PARA SEÑALES DE VOZ

## V.1 INTRODUCCION.

En este capítulo se propone un nuevo algoritmo de ciframiento de clave pública para señales de Voz. Este nuevo algoritmo se aplica para el ciframiento (manipulación) de los parámetros LPC. Dicho método de ciframiento propuesto es una combinación de : 1.) Un Algoritmo de Ciframiento de Clave Pública basado en el esquema **RSA**, que se realiza en forma matricial, y 2.) De un Sistema de Comunicación entre diversos usuarios realizado en forma Matricial.

La propuesta de este nuevo algoritmo de ciframiento se basa en que el *autor de esta tesis* realiza varias modificaciones al Esquema de Ciframiento de Clave Público **RSA** realizado en forma matricial, además de que propone un sistema de comunicación entre diversos usuarios en forma matricial. Cabe mencionar que las modificaciones realizadas al esquema de ciframiento de clave pública **RSA** en forma matricial, así como el sistema de comunicación entre diversos usuarios realizados por el autor de este trabajo de tesis está escrito en itálicas.

## V.2 PRESENTACION DEL ALGORITMO PROPUESTO.

### V.2.1 Descripción del esquema propuesto.

El algoritmo propuesto se basa en el esquema RSA [15] se realiza en forma matricial [30] y consiste de los siguientes pasos.

**A.) Inicialización del esquema.**

**A.1)** *Se define el orden de la matriz* **A** *a cifrar (descifrar). El orden de la matriz* **A** *es común para todos los usuarios* $U_i$.

**A.2)** Se define la colocación de los datos "*camufleados*" en la matriz **A** de ciframiento (desciframiento), es decir, los datos a cifrar se colocan en la parte superior o en la parte inferior de la diagonal principal de la matriz **A** a cifrar (descifrar).

**A.3)** *Todos los usuarios* $U_i$ *son informados de las siguientes funciones,* **r**, **g()** y **f()** de un *sólo sentido. Las funciones* **g()**, **f()** modulo **S** *son comunes para todos los usuarios, debe mencionarse que el valor del módulo* **R** *debe ser mucho mayor que el modulo* **S**.

**A.4)** Cada usuario $U_i$, selecciona dos números primos grandes $p_i$ y $q_i$ de diferente longitud y calcula $R_i = p_i q_i$.

**A.5)** Cada usuario $U_i$, selecciona un número primo grande, $e_i$, como parte de su clave pública, tal que $0 < e_i < (p_i-1)(q_i-1)$, además, $e_i$ es un número primo relativo a $(p_i-1)(q_i-1)$.

**A.6)** Cada usuario $U_i$, calcula su clave privada $d_i$, empleando el Algoritmo Extendido de Euclides de tal manera que se cumpla la siguiente congruencia

$$d_i e_i \equiv 1 \pmod{(p_i-1)(q_i-1)} \qquad (5.1)$$

En caso de que la expresión (5.1) no se cumpla para el valor calculado $d_i$, no se garantiza que la operación de desciframiento se efectúe correctamente.

**A.7)** El usuario $U_i$ forma su clave privada como el par de números $(d_i, (p_i-1)(q_i-1))$, la cual guarda en secreto, a la vez que forma su clave pública como el par de números $(e_i, R_i)$, la cual la da a conocer en un directorio público de claves.

**A.8)** El usuario $U_i$ define los *n-elementos* $a_{ii}$, que componen la diagonal principal, y que se seleccionan de manera aleatoria, dichos elementos son diferentes entre sí, y además son primos relativos con respecto a $R_i$.

**A.9)** *Los elementos* $a_{ii}$ *seleccionados por el usuario* $U_i$, *son cifrados por la función* $u() = a_{ii}^{x} \bmod S$. *Dichos valores se publican en un directorio de claves público. La finalidad de utilizar la función* **u()** *es de que* los datos $u()_{ii}$ *sean comunes tanto para el usuario* $U_i$ *e* $U_j$.

**A.10)** El usuario $U_i$ forma el siguiente sistema de ecuaciones simultáneas y procede a calcular los coeficientes $C_i$, $i = 0,1,\ldots,n-1$, guardando el valor de dichos coeficientes de la matriz **A** en secreto.

$$
\begin{aligned}
u()_{11}^{e_i} &\equiv c_{n-1}^{e_i}\, u()_{11}^{n-1} + c_{n-2}^{e_i} u()_{11}^{n-2} + \ldots + c_o^{e_i} \\
u()_{22}^{e_i} &\equiv c_{n-1}^{e_i}\, u()_{22}^{n-1} + c_{n-2}^{e_i}\, u()_{22}^{n-2} + \ldots + c_o^{e_i} \\
&\vdots \qquad\qquad \vdots \qquad\qquad \vdots \\
u()_{nn}^{e_i} &\equiv c_{n-1}^{e_i}\, u()_{nn}^{n-1} + c_{n-2}^{e_i}\, u()_{nn}^{n-2} + \ldots + c_o^{e_i}
\end{aligned}
\qquad (5.2)
$$

donde $u()_{ii}, i = 1,2,\ldots,n$ denota el i-enésimo elemento de la diagonal principal.

**A.11)** *El usuario* $U_i$ *cifra los coeficientes* $C_i^{e_i}$ *a través de una función de un sólo sentido* $u() = \left[ C_i^{e_i} \right]^{x_i} \bmod S$, *a la vez que los publica en un directorio de claves público.*

**B.) Ciframiento.**

Los pasos de ciframiento son los siguientes :

**B.1)** *El usuario* $U_i$ *define a* $r = U_i$, *o define una nueva función para calcular el valor de* r, *y evalua la función de g(r).*

**B.2)** a.- El usuario $U_i$ define $i = 1$ y $j = 2$.

b.- Calcula $f(r)$ usando el número r.

c.- Calcula $f(r) \circledcirc m_{ij}$.

donde $m_{ij}$ es el mensaje a cifrar, y el resultado de dicha operación se coloca en el $(i, j)$-ésimo elemento de la matriz **A**.

$\circledcirc$ Denota la operación or-exclusiva bit a bit.

d.- Se Actualiza $r = r + 1 \bmod R$ y $j = j + 1$.
Y se repiten los pasos (B.4.b), (B,4.c) hasta $j = n$.

e.- Se designa $i = i + 1$ y $j = j + 1$. Y se repiten los pasos (B.4.b) y (B.4.c) hasta $i = n - 1$.

**B.3)** A partir de los coeficientes calculados en el paso **(A.11)** y empleando el Teorema de Cayley-Hamilton [31] se realiza el cifrado de la matriz **A**.

$$\mathbf{A}^{e} = C_{n-1}\mathbf{A}^{n-1} + C_{n-2}\mathbf{A}^{n-2} + \ldots + C_{0}\mathbf{I}$$

**B.4)** Se coloca **r** ≡ **r** + 1 (mod R) y se repiten los pasos (B.2) y (B.3) hasta cifrar todo el mensaje original.

**C. Desciframiento.**

Después de que el usuario $U_j$ recibe las matrices cifradas, procede a recuperar el mensaje original a partir del mensaje cifrado realizando los siguientes pasos :

**C.1)** *Recibe los datos* $u()_{ii}$, *y los descifra. Esta operación permite recuperar los datos* $a_{ii}$ *y compararlos con los suyos (previamente almacenados).*

**C.2)** *Recibe los datos* $C^{kij(ei)}_{ii}$, *y los descifra. Esta operación nos permite recuperar los coeficientes* $C_i^{ei}$, *y compararlos con los suyos, previamente almacenados.*

*Si los pasos* **C.1** *y* **C.2** *no se cumplen, no se garantiza que el proceso de descifrado se efectue correctamente.*

**C.3)** Forma el siguiente sistema de ecuaciones y procede a calcular los coeficientes $C_i^{di}$, i = 0,1,...,n-1 para posteriormente almacernarlos en secreto.

$$\begin{aligned}
a_{11}^{ei\,di} &\equiv c_{n-1}^{di}\, a_{11}^{ei(n-1)} + c_{n-2}^{di}\, a_{11}^{ei(n-2)} + \ldots + c_{o}^{di} \\
a_{22}^{ei\,di} &\equiv c_{n-1}^{di}\, a_{22}^{ei(n-1)} + c_{n-2}^{di}\, a_{22}^{ei(n-2)} + \ldots + c_{o}^{di} \\
&\vdots \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \vdots \\
a_{nn}^{ei\,di} &\equiv c_{n-1}^{di}\, a_{nn}^{ei(n-1)} + c_{n-2}^{di}\, a_{nn}^{ei(n-2)} + \ldots + c_{o}^{di}
\end{aligned} \qquad (5.3)$$

donde $a_{ii}^{ei}$, i,1,2,...,n denota el i-ésimo elemento de la diagonal principal a partir de la matriz recibida.

C.4) Emplea los coeficientes calculados $C_i$ en el paso (C.3), y aplica el Teorema de Cayley-Hamilton [30] para descifrar la matriz recibida.

$$A^{d_i} = C_{n-1}A^{n-1} + C_{n-2}A^{n-2} + \ldots + C_0 I$$

C.5) *Define el número* r, *o define una nueva función para calcular el valor de* r, *en este caso se seleccionó* $r = U_i$.

C.6) a.- Define $i = 1$ y $j = 2$.

b.- Calcula la función f(r) usando el número r.

c.- Recupera el mensaje original a partir de la siguiente ecuación

$$f(r) \otimes a_{ij} \equiv f(r) \otimes \left[ f(r) \otimes m_{ij} \right] \equiv m_{ij} \bmod R$$

donde $a_{ij}$ Es la (i,j)-ésima entrada de la diagonal principal de la matriz recibida.

d.- Actualiza $r \equiv (r + 1) \bmod R$ y $j = j + 1$. Y repite los pasos (C.4.b) y(C.4.c) hasta $j = n$.

e.- El usuario $U_j$ coloca $i = i + 1$ y $j = i + 1$.
Y repite los pasos (C.2) a (C.4) hasta descifrar todos los mensajes recibidos.

*Solamente* e, R y *las funciones f() y g(), así como los coeficientes* $u()_{ii}$ y $C_i^{k_{ii}}$ *son hechas públicas. El valor de* d, r, $a_{ii}$, $i = 1,2,\ldots,n$ *y los números primos* $p_i$ *y* $q_i$ *se guardan en secreto.*

La eficiencia computacional de este nuevo algoritmo, depende de la dimensión de la matriz a cifrar. La implantación más eficiente, es el caso en el cual la matriz es de dimensión 2x2, ya que para el proceso de ciframiento y desciframiento consiste de una simple multiplicación mod R, además de la evaluación de una función de una sóla vía. En este caso, este criptosistema de clave pública tiene el potencial de una rápida implantación.

### V.2.2 Aplicación del esquema propuesto para la manipulación de parámetros LPC.

**A.) Inicialización del sistema.**

A.1) El usuario $U_i$ selecciona dos números primos grandes, de diferente longitud. En este caso, el usuario $U_i$ selecciona $p = 47$ y $q = 59$ y calcula R de la siguiente manera :

$$R = p \times q = 47 \times 59 = 2773$$

A.2) El usuario $U_1$, selecciona su clave pública $e_1$, de forma aleatoria. Tal que $0 < e_1 < (p-1)(q-1)$ y que el número $e_1$, es un número primo relativo a $(p-1)(q-1)$. En este caso $e_1 = 17$.

A.3) El usuario $U_1$, calcula su clave privada, $d_1$, con el auxilio del Algoritmo Extendido de Euclides. Este caso el valor de $d_1$ es 157.

A.4) El usuario $U_1$ define el tamaño de la matriz **A** que en este ejemplo es de orden 2x2 e inicia la construcción de la matriz **A** seleccionado los elementos de la diagonal principal. En este caso se selecciona $a_{11} = 19$ y $a_{22} = 23$ y donde $a_{11}$ y $a_{22}$ son primos relativos a **R**.

A.5) El usuario $U_1$ selecciona el mensaje a cifrar M. En este ejemplo el mensaje **M** está formado por $m_1 = 37$ y $m_2 = 23$.

**B.) Ciframiento de la señal de Voz.**

Los pasos de ciframiento son los siguientes :

B.1) El usuario $U_1$ selecciona los elementos de la diagonal principal en forma aletoria, de tal manera que cumplan el paso A.4, y forma la matriz **A** de tamaño *mxn*, por la selección de $a_{11} = 19$ y $a_{22} = 23$ como sus elementos de la diagonal principal.

B.2) El usuario $U_1$ forma el sistema de ecuaciones de acuerdo a la ecuación (2), en este caso, el sistema de ecuaciones es el siguiente :

$$19^{17} \equiv 2824 \equiv C_o^e + 19\, C_1^e \mod 2773$$

$$23^{17} \equiv 1581 \equiv C_o^e + 23\, C_1^e \mod 2773$$

y procede a calcular los coeficientes ( $C_o$ y $C_1$ ) de dicho sistema de ecuaciones. La solución a este sistema de ecuaciones es $C_o = 54$ y $C_1 = 2116$

B.3) Calcula el valor de r definido como una función de un sólo sentido. En este ejemplo, r se calcula como :

$$r \equiv (a_{11} + a_{22}) \bmod R$$

En este ejemplo como el mensaje a cifrar es de longitud = 2, es decir, solamente se tienen dos bloques de mensaje, la secuencia de r, es la siguiente :

$r_o = 42 \mod 2773$
$r_1 = 43 \mod 2773$

B.4) Este paso depende de la función f() y del valor r calculado previamente, dicha función f(), se define como :

$$f(r_1) = r_1^{e_1} \mod R.$$

B.5) Primero se calcula $f(r_1) \oplus m_1$ y se coloca el resultado de dicha operación en el lugar $a_{12}$. En este ejemplo el mensaje $m_0$ es 37. El resultado de $(fr_1) \oplus m_1$ es 1465.

$$\begin{array}{rll} & f(r_0) = (1416)_{10} & = (\,1\,0\,1 \quad 1\,0\,0\,1 \quad 1\,1\,0\,0\,)_2 \\ \oplus & m_0 = (37)_{10} & = (\,0\,0\,0 \quad 0\,0\,1\,0 \quad 0\,1\,0\,1\,)_2 \\ \hline & (1465)_{10} & (\,1\,0\,1 \quad 1\,0\,1\,1 \quad 1\,0\,0\,1\,)_2 \end{array}$$

El cifrado del primer bloque del mensaje original se efectúa de la siguiente manera

$$A^{e_1} \equiv A^{17} \equiv 54 \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + 2116 \begin{bmatrix} 19 & 1465 \\ 0 & 23 \end{bmatrix} \mod 2773$$

$$A^{e_1} \equiv A^{17} \equiv \begin{bmatrix} 54 & 0 \\ 0 & 54 \end{bmatrix} + \begin{bmatrix} 1439 & 2499 \\ 0 & 1527 \end{bmatrix} \mod 2773$$

$$A^{e_1} \equiv A^{17} \equiv \begin{bmatrix} 1493 & 2499 \\ 0 & 1581 \end{bmatrix} \mod 2773$$

B.6) El usuario $U_1$ aplica de nuevo los pasos (B.1) a (B.5) al resto del mensaje original. En este ejemplo se aplican los pasos (B.1) a (B.4) al bloque $m_1$.

El segundo bloque de mensaje es $m_1 = 23$ y realizando la operación $f(r_1) \oplus m_1$ es 1327.

$$\begin{array}{rll} & f(r_0) = (1336)_{10} & = (\,1\,0\,1 \quad 0\,0\,1\,1 \quad 1\,0\,0\,0\,)_2 \\ \oplus & m_0 = (37)_{10} & = (\,0\,0\,0 \quad 0\,0\,0\,1 \quad 0\,1\,1\,1\,)_2 \\ \hline & (1327)_{10} & (\,1\,0\,1 \quad 0\,0\,1\,0 \quad 1\,1\,1\,1\,)_2 \end{array}$$

El cifrado del segundo bloque del mensaje original se efectúa de la siguiente manera :

$$A^{e_1} \equiv A^{17} \equiv 54 \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + 2116 \begin{bmatrix} 19 & 1327 \\ 0 & 23 \end{bmatrix} \mod 2773$$

$$A^{e} \equiv A^{17} \equiv \begin{bmatrix} 54 & 0 \\ 0 & 54 \end{bmatrix} + \begin{bmatrix} 1439 & 1656 \\ 0 & 1527 \end{bmatrix} \mod 2773$$

$$A^{e} \equiv A^{17} \equiv \begin{bmatrix} 1493 & 1656 \\ 0 & 1581 \end{bmatrix} \mod 2773$$

B.7) El usuario $U_1$ transmite la secuencia del mensaje cifrado, que son los valores $a_{12}$ de cada una de las matrices cifradas. En este ejemplo la secuencia del mensaje cifrado es 2499 y 1656.

**C.) Descifrado de la Señal de Voz.**

C.1) El usuario $U_2$ actualiza el sistema de ecuaciones de acuerdo a la forma de la ecuación (5.3) de la manera siguiente :

$$1581^{157} \equiv 23 \equiv C_o^d + 1581\ C_1 \bmod 2773$$

$$1436^{157} \equiv 19 \equiv C_o^d + 1436\ C_1 \bmod 2773$$

y procede a calcular los coeficientes ($C_o$ y $C_1$) de este conjunto de ecuaciones. El valor de los coeficientes es $C_o = 228$ y $C_1 = 612$.

C.2) El usuario $U_2$ procede a descrifrar el primer bloque del criptograma calculando las siguientes ecuaciones

$$\left[A^e\right]^{157} \equiv 228\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + 612\begin{bmatrix} 1581 & 2499 \\ 0 & 1436 \end{bmatrix} \bmod 2773$$

$$\left[A^e\right]^{157} \equiv \begin{bmatrix} 228 & 0 \\ 0 & 228 \end{bmatrix} + \begin{bmatrix} 2568 & 1465 \\ 0 & 2564 \end{bmatrix} \bmod 2773$$

$$\left[A^e\right]^{157} \equiv \begin{bmatrix} 2796 & 1465 \\ 0 & 2792 \end{bmatrix} \bmod 2773$$

C.3) El usuario $U_2$ recupera el primer bloque del mensaje efectuando la operación $f(r) \oplus a_{12}$, que en este caso es $m_1 = 1416 \oplus 1465 = 37$.

$$\begin{array}{rl} f(r_1) & = (1416)_{10} = (\ 1\ 0\ 1\quad 1\ 0\ 0\ 1\quad 1\ 1\ 0\ 0\ )_2 \\ \oplus\ m_1 & = (1465)_{10} = (\ 1\ 0\ 1\quad 1\ 0\ 1\ 1\quad 1\ 0\ 0\ 1\ )_2 \\ \hline & (\ 37\ )_{10} \quad (\ 0\ 0\ 0\quad 0\ 0\ 1\ 0\quad 0\ 1\ 0\ 1\ )_2 \end{array}$$

C.4) Repite los pasos (C.2) y (C.3), y calcula la secuencia de $f(r_1)$ para recobrar el segundo bloque del mensaje original $m_1$ de la siguiente manera :

$$\left[A^{e}\right]^{157} \equiv 228\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix} + 612\begin{bmatrix}1581 & 1656\\ 0 & 1436\end{bmatrix} \bmod 2773$$

$$\left[A^{e}\right]^{157} \equiv \begin{bmatrix}228 & 0\\ 0 & 228\end{bmatrix} + \begin{bmatrix}2568 & 1656\\ 0 & 2564\end{bmatrix} \bmod 2773$$

$$\left[A^{e}\right]^{157} \equiv \begin{bmatrix}2796 & 1327\\ 0 & 2792\end{bmatrix} \bmod 2773$$

El usuario $U_2$ recupera el segundo bloque del mensaje efectuando la operación $f(r) \oplus a_{12}$, que en este caso es $m_1 = 1336 \oplus 1327 = 23$.

$$\begin{array}{rll} & f(r_1) = (1336)_{10} & = (\ 1\ 0\ 1\quad 0\ 0\ 1\ 1\quad 1\ 0\ 0\ 0\ )_2 \\ \oplus & m_1 = (1327)_{10} & = (\ 1\ 0\ 1\quad 0\ 0\ 1\ 0\quad 1\ 1\ 1\ 1\ )_2 \\ \hline & (\ 27\ )_{10} & (\ 0\ 0\ 0\quad 0\ 0\ 0\ 1\quad 0\ 1\ 1\ 1\ )_2 \end{array}$$

## V.3 SISTEMA DE COMUNICACION ENTRE DIVERSOS USUARIOS.

### V.3.1 Sistema de Comunicación entre diversos usuarios realizado en forma Matricial.

*El sistema de comunicación entre diversos usuarios consiste de los siguientes pasos :*

1.) *El usuario* $U_i$ *define una matriz* $A_i$ *orden nxn, en donde los elementos de la matriz* $A_i$ *son elementos primitivos de GF(p). La matriz* $A_i$ *se da a conocer públicamente.*

2.) *El mismo usuario* $U_i$ *define una matriz* $X_i$ *de orden nxn, en donde los elementos de la matriz Xi se eligen de manera aleatoria. La matriz* $X_i$ *se guarda en secreto.*

3.) *Cada usuario* $U_i$ *genera su clave pública* $Y_i$, *donde* $Y_i$ *es una matriz de orden nxn que tiene sus elementos definidos por :*

$$y_{ij} \equiv a_{ij}^{x_{ij}} (\bmod p),\ i,j=1,2,\ldots,n$$

*y se denota como :*

$$Y_i \equiv A_i^{X_i} \ (\bmod p)$$

*Este usuario pública su matriz* $Y_i$.

*Cualquier otra persona no puede calcular* **X** *a partir de* **Y** *en un tiempo breve debido a la dificultad de calcular logaritmos sobre GF(p)* [25].

*4.) Cuando dos usuarios* $U_1$ *y* $U_2$ *se quieren comunicar en forma privada, ellos calculan su clave común de la siguiente manera:*

$$K_{12} \equiv Y_2^{X_1} \pmod p = Y_1^{X_2} \pmod p$$

*donde* $Y_1$, $Y_2$ *son las matrices públicas de los usuarios* $U_1$ *y* $U_2$. $X_1$, $X_2$ *son las matrices privadas de los usuarios* $U_1$ *y* $U_2$ *respectivamente.*

*La matriz de la clave* $K_{12}$ *es de la misma dimensión que la matriz* **Y** *que a su vez es de dimensión nxn.*

*5.) Ciframeinto de un mensaje representado en forma matricial. Si* $k_{12}$ *es no singular, se puede cifrar un mensaje original* **M** *que tiene forma matricial de orden nxr, y de esta manera se obtiene la matriz de criptograma* **C** *de orden nxr :*

$$C = K_{12}M$$

*Para que se puedan multiplicar las matrices* **K** *y* **M**, *la matriz* **M** *tiene que tener la dimensión adecuada, es decir,* **M** *tiene que ser de dimensión* **nxr**, *donde* **n** *es el orden de la matriz cuadrada* **K**. *Esto es que* **M** *tiene* **nxr** *elementos . Si el número de elementos de la matriz* **M** *es menor que* **nxr**, *o sea que este número es igual a* **nxr-s** *(donde* $s<n$*), entonces, se asignan números aleatorios a los* **s** *elementos que no tienen información.*

*6.) Para descifrar el criptograma* **C**, *se premultiplica a la matriz* **C**, *por la matriz inversa de* **K**, $K^{-1}$, *y de esta manera se obtiene* **M** *:*

$$M \equiv K_{12}^{-1} C = K_{12}^{-1} ( K_{12} M) = M$$

*En este caso, la matriz de clave común* $K_{12}^{-1}$, *también tiene la restricción de que* $K_{12}$ *tiene que ser no singular para que* $K_{12}^{-1}$ *exista.*

*Sin embargo, esta restricción es mucha más fácil de cumplir comparada con la restricción de que gcd(*$K_{11}$, *(p-1)) = 1 para el caso de la realización de la clave común por elevación exponencial descrita en la sección IV.3.3.1 de este trabajo. Esto es debido a que la posibilidad de que el determinante de* $K_{12}$ *sea igual a cero es demasiado pequeña (casi nula) comparada con la posiblidad de que el determinante de* $K_{12}$ *sea cualquier número diferente de cero, para una matriz* $K_{12}$ *que tiene los elementos calculados a partir de otros elementos seleccionados aleatoriamente.*

CAPITULO

S E I S

# PRESENTACION DE RESULTADOS Y COMPARACION DE ALGORITMOS DE CIFRAMIENTO

## VI.1 INTRODUCCION.

En este capítulo *se* presentan los resultados obtenidos por la simulación de los diferentes esquemas de ciframiento, así como la complejidad en el tiempo y las pruebas de seguridad para los diversos métodos de ciframiento empleados en este trabajo de tesis. Las simulaciones fueron realizadas en una computadora PC-AT, con el auxilio de una Tarjeta de Adquisición y Reprodución de señales de voz "Sound-Blaster", además de algunos otros recursos requeridos, para que de esta forma se alcanzaran los objetivos que se pretendían en los capítulos IV y V.

Las pruebas que se aplicaron a cada uno de los diferentes esquemas de ciframiento para su validación son :

* Complejidad en el tiempo.
* Pruebas de seguridad.
* Inteligibilidad residual.

Cabe aclarar que las pruebas se realizaron suponiendo un Canal de Comunicación sin ruido.

Los objetivos que se cubrieron fueron los siguientes :

a.) Implementar mediante software diferentes esquemas de ciframiento descritos en el capítulo IV.

b.) Proponer e Implementar mediante software un nuevo esquema de ciframiento de clave pública, descrito en el capítulo V.

c.) Observar la Inteligibilidad Residual de los diferentes esquemas de ciframiento, así como observar su comportamiento, tanto en el dominio del tiempo, como en el de la frecuencia.

## VI.2 RESULTADOS CORRESPONDIENTES AL ESQUEMA DE CIFRAMIENTO DE PERMUTACION DE MUESTRAS EN EL TIEMPO.

### VI.2.1 Esquema de ciframiento de clave pública RSA.

El esquema de ciframiento de clave pública (también llamado Algoritmo de Ciframiento Asimétrico), propuesto por Rivest, Shamir, y Adleman (RSA) [15], y empleado en el *Método de cifrado de permutación de muestras en el tiempo*, se basa esquemáticamente en la complejidad computacional necesaria para factorizar números primos grandes. El mejor algoritmo conocido hasta el momento para encontrar un número primo de $d$ dígitos lo realiza en un tiempo de $O(d^3)$, mientras que obtener sus factores le lleva una complejidad de

$$O\left(n^{\left[\ln(\ln n)\ln n\right]^{1/2}}\right)$$

como lo demuestra Schroeppel [32].

Los resultados correspondientes a la simulación del método 1 se muestran en el inciso VI.2.1.1, las ventajas de este esquema de ciframiento se mencionan en el inciso VI.2.1.2 y las ventajas y desventajas del sistema de comunicación entre diversos usuarios en el inciso VI.2.1.3.

### VI.2.1.1 Presentación de Resultados Gráficos correspondientes al método 1

El aspecto gráfico es un factor muy importante, ya que permite comprobar y observar algunas consideraciones ya mostradas en los capítulos IV y V.

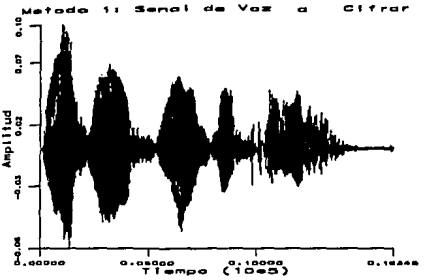
A partir de las propiedades de simetría de la DFT [4] se puede concluir que el rango de frecuencias de una señal discreta en el tiempo está limitada a $0 \leq \omega \leq \pi$, es decir, a la mitad del período.

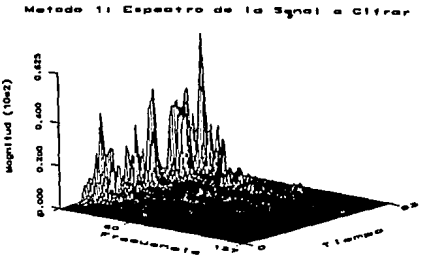
Por lo tanto, la descripción en el dominio de la frecuencia de una señal real y discreta en el tiempo, se especifica completamente por su espectro en el rango de frecuencia de $0 \leq \omega \leq \pi$, y usualmente, podemos trabajar con el intervalo fundamental $0 \leq \omega \leq \pi$, ó $0 \leq F \leq Fs/2$, en términos de Hertz. Donde Fs es la frecuencia de muestreo.

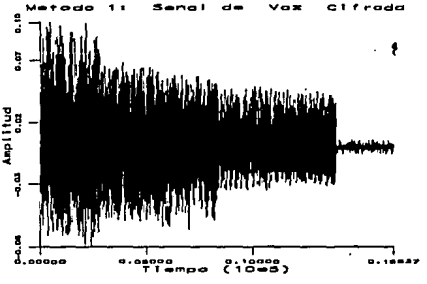
En la Fig. 6.1 se muestran los resultados gráficos del Esquema de ciframiento en el Dominio del Tiempo denominado "Permutación de muestras en el tiempo". En la Fig. 6.1a se presentan las formas de onda de la señal de voz a cifrar, tanto en el dominio del tiempo como en el dominio de la frecuencia.

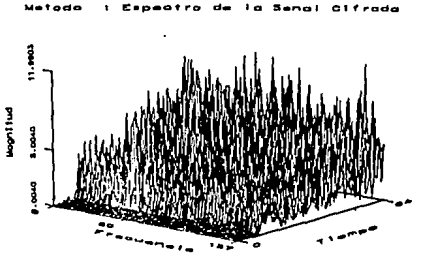
En la Fig. 6.1b se muestran las formas de onda de la señal de voz cifrada -Criptograma-, tanto en el dominio del tiempo, como en el dominio de la frecuencia. Con respecto a la forma de onda en el dominio del Tiempo, la forma de onda de la señal de voz cifrada desaparece y esto permite que el mensaje original no se alcance a percibir por completo, de tal forma que no se logra visualizar ningún lóbulo principal de la señal de voz, mucho menos entender el contenido del mensaje. Con respecto al dominio de la frecuencia, se nota una amplificación de las componentes bajas, medias y altas de la señal de voz cifrada.

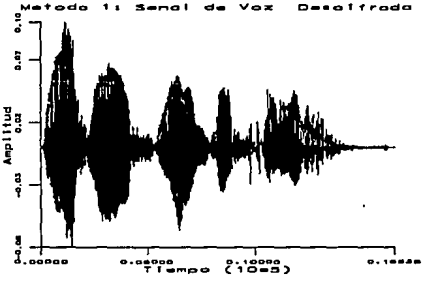
En la Fig.6.1c se muestran las formas de onda de la señal de voz descifrada. En dicha figura se nota que se recupera la misma forma de onda de la señal de voz a cifrar, tanto en el domino del Tiempo, como en el dominio de la Frecuencia, -forma de onda y magnitud-, además, no existe pérdida significativa de energía alguna en la señal descifrada, debido a que únicamente el proceso de cifrado consiste en permutar las muestras en el dominio del tiempo.

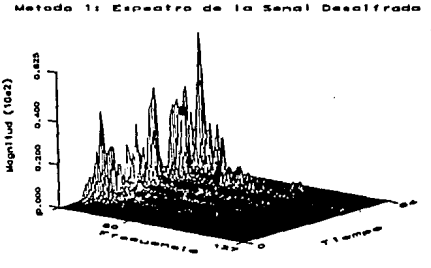

Metodo 1: Senal de Voz a Cifrar
Amplitud
Tiempo (10e5)


Metodo 1: Espectro de la Senal a Cifrar
Magnitud (10e2)
Frecuencia
Tiempo


Metodo 1: Senal de Voz Cifrada
Amplitud
Tiempo (10e5)


Metodo 1 Espectro de la Senal Cifrada
Magnitud
Frecuencia
Tiempo


Metodo 1: Senal de Voz Descifrada
Amplitud
Tiempo (10e5)


Metodo 1: Espectro de la Senal Descifrada
Magnitud (10e2)
Frecuencia
Tiempo

### VI.2.1.2 Ventajas y desventajas del esquema de ciframiento.

Las ventajas del esquema de ciframiento son :

**Ventajas :**

-- Se logra una inteligibilidad residual mayor, cuando se consideran bloques de muestras de tamaño grande.

-- No existe pérdida de información.

-- Este esquema cifrador aprovecha el hecho de que encontrar números primos muy grandes es computacionalmente fácil, pero factorizar el producto de dos números primos es computacionalmente imposible.

**Desventajas :**

-- El esquema cifrador de clave pública RSA tiene como desventaja principal, el manejo de números muy grandes. En este esquema cifrador, cada muestra del mensaje $m$ representa una sucesión de enteros $m_1, m_2, m_3, \ldots, m_i$, y donde $m_i$ es un número entero entre $0 < m_i < R-1$, y donde R es el producto de dos números primos grandes **p** y **q**.

El ciframiento de cada mensaje $m_i$, consiste en elevar cada posición de la muestra $m_i$ a la potencia **e** mod R, siendo **e** mayor o igual que 2, pero menor que o igual a $(p-1)(q-1)-1$, con esto se consigue que el número **R**, sea un número de 100 dígitos (donde **p** y **q** son números primos de aproximadamente 50 dígitos). Además, los números **d** y $(p-1)(q-1)$ que nos permiten comprobar la ec. 4.3 (ver, pag. 75), pueden también llegar a ser de 100 dígitos.

La finalidad de que los números **p**, **q**, **e** y **d** sean : 1.) Números primos, 2.) Sean de longitud grande (de 100 dígitos o más), es para que le sea laborioso al criptoanalista factorizar el valor de **R**, o calcular el valor de la clave privada **d** a partir del valor de la clave pública **e**.

Elevar un número a la potencia **e** es un trabajo muy laborioso aunque se puede aligerar aplicando algún algoritmo de exponenciación rápida [19][24].

-- Una incomodidad de este esquema cifrador, es el manejo de números primos "grandes", es decir, tenemos que hacer operaciónes con números muy grandes (ejemplo, 100 dígitos) y estas operaciones son difíciles de realizar en las microcomputadoras (por ejemplo, una PC-AT ), y usando el lenguaje C, solamente se puede lograr operaciones de suma, resta, multiplicación y división con números enteros que tienen

un máximo de 36 dígitos, utilizando un arreglo llamado "long-integer", pero no es posible aplicar muchas funciones sobre estos números enteros grandes, como por ejmeplo, la función "módulo R" (que se emplea en los algoritmos criptográficos de los capítulos IV y V).

### VI.2.1.3 Ventajas y desventajas del Sistema de Comunicación entre diversos usuarios de ciframiento propuesto por Diffie-Hellman.

Las ventajas y desventajas del Sistema de Comunicación entre diversos usuarios son :

**Ventajas :**

-- Se consigue que tanto el emisor como receptor de un criptograma se "reconozcan" entre sí, es decir, el receptor sabe con exactitud quién le envió el mensaje.

**Desventajas :**

-- En este esquema de comunicación se debe de cumplir que gcd( $K_{ij}$, $R$ ) = 1 (donde $R = pq$ ) para que la clave inversa de $K_{ij}$, $K_{ij}^{-1}$, exista.

### VI.2.2 COMPLEJIDAD EN EL TIEMPO.

Para el algoritmo de permutación de muestras en el tiempo, el número de operaciones realizadas por el transmisor, considerando un bloque de $R_A$ muestras a cifrar es el siguiente :

No. de operciones = $R_A \times 2 ( \log_2 (e) )$
para el ciframiento

donde

$R_A$ Es el número de muestras en el bloque a cifrar.
**e** Es el valor numerico de la clave utilizada para cifrar.

Mientras que el número de operaciones realizadas en el receptor, si considerando un bloque de $R_A$ muestras a descifrar es el siguiente :

No. de operaciones = $R_A \times 2 (\log_2 (d) )$
para el desciframiento

donde

$R_A$ Es el número de muestras en el bloque a descifrar.
**d** Es el valor numerico de la clave utilizada para cifrar.

## VI.2.3 PRUEBAS DE SEGURIDAD.

Aunque no existen técnicas para probar que un esquema de ciframiento es seguro, con las pruebas disponibles se puede estimar si alguna persona no autorizada podría ingeniar alguna manera para violarlo.

En este inciso tratamos de mostrar que todos los métodos obvios para violar este esquema de ciframiento son, por lo menos, tan complejos como factorizar R ( R = pq) en sus factores primos, es decir, conocer p y q. Aunque factorizar el producto de dos números primos grandes probablemente no es difícil, ya que es un problema muy conocido [32]. Sin embargo, nadie ha encontrado todavía un algoritmo que puede factorizar un número de 100 dígitos ( o más) en un tiempo razonable (unos minutos o unas horas).

A continuación se muestra la dificultad que tiene un criptoanalista para calcular la clave secreta a partir de la clave pública [15]. Primero considérese que un criptoanalista trata de factorizar la clave pública, R, en su factores primos p y q, y que estos factores secretos se utilizan en la determinación de la clave para descifrar, y con esto comprueba que su esfuerzo es inmensamente grande.

### V.2.3.1. Factorización de R

La factorización de R puede permitir a un criptoanalista romper la seguridad del esquema cifrador. Los factores de R le permiten calcular $\Phi(R)$, (como $\Phi(R) = (p-1)(q-1)$), y de esta manera obtener la clave para descifrar d. Existen varios algoritmos que factorizan un número grande, pero el algoritmo más rápido es de Richard Schroeppel [32]. Este algoritmo puede factorizar un número grande en aproximandamente

$$\exp\left[(1+O(1))\left(\sqrt{\ln(R)*\ln(\ln(R))}\right)\right]$$

pasos.

La tabla 6.1 muestra el número aproximado de operaciones necesarias para factorizar R con el método de Schroeppel, y el tiempo que se requiere si cada operación tarda un microsegundo para diferentes longitudes del número R (en dígitos decimales).

| Dígitos | Número de operaciones | Tiempo |
|---|---|---|
| 50 | $1.4x10^{10}$ | 3.9 horas |
| 75 | $9.0x10^{12}$ | 104 días |
| 100 | $2.3x10^{15}$ | 74 años |
| 200 | $1.2x10^{23}$ | $3.8x10^{25}$ años |
| 300 | $1.5x10^{29}$ | $4.9x10^{15}$ años |
| 500 | $1.3x10^{39}$ | $4.2x10^{25}$ años |

**Tabla 6.1**

Con esto se comprueba la dificultad de factorizar R para un criptoanalista, pero éste quizás trate de determinar $\Phi(R)$ sin factorizar R para calcular la clave para descifrar, d. En seguida mostramos que ésto no es más fácil que factorizar R.

### VI.2.3.2. Cálculo de $\Phi(R)$ sin factorizar R.

Si un criptoanalista puede calcular $\Phi(R)$, entonces puede violar la seguridad del esquema cifrador calculando la clave para descifrar d, como la inversa multiplicativa de e ( la clave para cifrar, la cual está publicada) utilizando el Algoritmo Extendido de Euclides [24]. Sin embargo, calcular $\Phi(R)$ sin factorizar R es, por lo menos, igual de complicado que factorizar R. Enseguida se muestra la razón de esto.

Primero vemos que una vez que se conoce $\Phi(R)$, es posible factorizar fácilmente R.

$$\Phi(R) = (p-1)(q-1) = pq - p - q + 1$$
$$\therefore \quad p+q = R - \Phi(R) + 1$$

además p-q es la raíz cuadrada de $(p-q)^2$, y $(p-q)^2$ se puede calcular así :

$$(p-q)^2 = p^2 + q^2 + 2pq - 4pq = (p+q)^2 - 4R$$

$$q = \frac{(p+q) - (p-q)}{2}$$

Como este camino para factorizar R no ha resultado práctico, puede decirse que calcular $\Phi(R)$ sin factorizar R no es menos complicado que factorizar R.

Ahora condieremos que el criptoanalista trata de calcular la clave para descifrar **d** directamente, sin factorizar R. En el siguiente inciso se muestra que calcular **d** sin factorizar R tampoco es más fácil que factorizar R.

### VI.2.3.3 Determinación de d sin factorizar R.

Desde luego, **d** debe ser seleccionado de un conjunto suficientemente grande para que una búsqueda directa sea ineficiente.

Demostraremos que calcular **d** no es más fácil para un criptoanalista que factorizar R, puesto que una vez conocida **d**, R podría factorizarse fácilmente. Sin embargo, este método para factorizar R tampoco ha resultado fructuoso. Hasta hoy en día, nadie a dado a conocer los resultados que indican que se puede calcular el valor de **d** factorizando R.

Suponiendo una **d** conocida, la cual permite que R sea factorizada de la siguiente manera: 1.) Se calcula **ed**-1, lo cual es un múltiplo de $\Phi(R)$, recordando que **ed** = k $\Phi(R)$ + 1, donde k es un entero. 2.) Utilizando el múltiplo de $\Phi(R)$ se puede factorizar R. Por lo tanto, si R es grande, un criptoanálista no puede determinar **d** más fácilmente que factorizar R.

## VI.3 RESULTADOS CORRESPONDIENTES AL ESQUEMA DE CIFRAMIENTO EN AMPLITUD.

### VI.3.1 Esquema de ciframiento RSA.

El esquema de ciframiento asimétrico propuesto por Rivest, Shamir, y Adleman (RSA), empleado en el *Método de cifrado en Amplitiud*, se basa esquemáticamenteen la complejidad computacional necesaria para encontrar números primos grandes. Por lo tanto, el esquema de cifrado asimétrico propuesto, basa su seguridad en la dificultad de factorizar R en p y q, así como de una selección cuidadosa de los números primos p y q.

En el inciso siguiente **VI.3.1.1** se presentan los resultados correspondientes al método 2. Las ventajas y desventajas de este esquema de ciframiento se mencionan en el inciso **VI.3.1.2** y en el inciso **VI.3.1.3** se presentan las ventajas y desventajas del sistema de comunicación entre diversos usuarios.

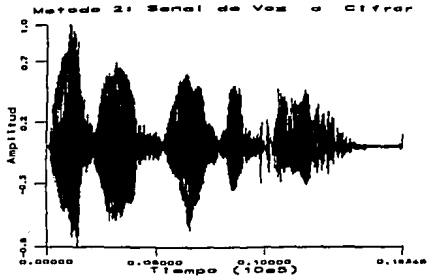
#### VI.3.1.1 Presentación de Resultados Gráficos correspondientes al método 2

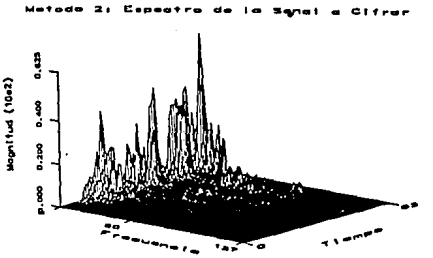
Los resultados de la simulación del esquema de Ciframiento en Amplitud se muestran en la Fig.6.2. En el lado izquierdo de dicha figura se presentan las formas de onda de la señales de voz a cifrar, cifrada y descifrada en el dominio del tiempo. Mientras que el lado derecho de la figura muestra el espectro de dichas señales.

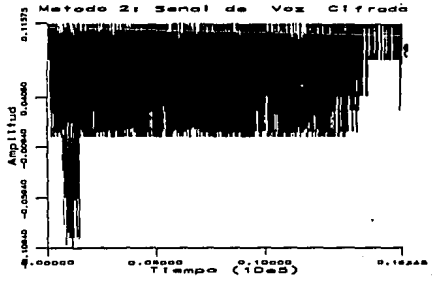
En la Fig.6.2b se muestra la forma de onda de la señal de voz cifrada, cabe hacer notar que en general todas las muestras de la señal de voz cifrada son de una misma Amplitud. Además, en dicha figura se observa que en el dominio del tiempo la forma de onda de la señal original se destruye, de tal forma que no se logra visualizar algún lóbulo principal de la señal de voz.

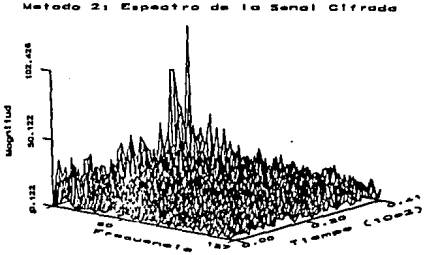
Para el método 2, el espectro de la señal cifrada se muestra en la Fig. 6.2b, en dicha figura se muestra una uniformidad en magnitud de las componentes medias y altas de las diferentes *tramas*.

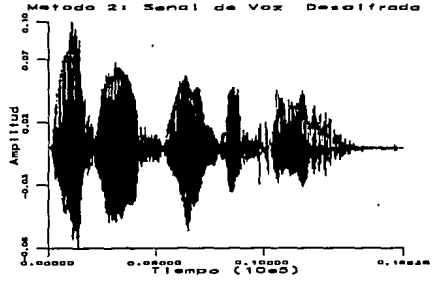
En la Fig.6.2c se observa que los resultados del proceso de descifrado, en dicha figura se observa que, el proceso de descifrado recupera la misma forma de onda de la señal de voz original, tanto en el dominio del Tiempo, así como en el dominio de la Frecuencia, es decir, la señal descifrada conserva las mismas propiedades que la señal original -forma de onda y amplitud-.

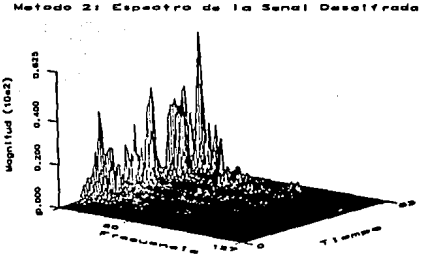

Metodo 2: Senal de Voz a Cifrar
Amplitud
Tiempo (10e5)


Metodo 2: Espectro de la Senal a Cifrar
Magnitud (10e2)
Frecuencia
Tiempo


Metodo 2: Senal de Voz Cifrada
Amplitud
Tiempo (10e5)


Metodo 2: Espectro de la Senal Cifrada
Magnitud
Frecuencia
Tiempo (10e3)


Metodo 2: Senal de Voz Descifrada
Amplitud
Tiempo (10e5)


Metodo 2: Espectro de la Senal Descifrada
Magnitud (10e2)
Frecuencia
Tiempo

### VI.3.1.2 Ventajas y desventajas del esquema de ciframiento.

Las ventajas y desventajas del esquema de ciframiento son :

**Ventajas :**

-- Se obtiene un mayor grado de inteligibilidad si se agrupan sub-bloques de dígitos de tal manera que el número de dígitos (nc) sea menor al número de dígitos de $R_A$.

-- No se requiere de una gran capacidad de memoria para efectuar el ciframiento y desciframiento de la señal, ya que se procesa una sola muestra a la vez.

-- Este esquema de ciframiento presenta la posibilidad de que la señal cifrada se escuche como ruido blanco, además de la gran cantidad del número de amplitudes del ruido pseudoaleatorio que se puede generar.

**Desventajas :**

-- Se pierde precisión al descifrar la señal.

-- Existe una pérdida significativa en la relación señal-ruido en el receptor, debido a que parte de la energía, se pierde en el receptor debido al ruido que se transmitió.

-- Este esquema de ciframiento no puede operar con números grandes cuya longitud sea superior a 100 bits.

### VI.3.1.3 Ventajas y desventajas del Sistema de Comunicación entre diversos usuarios realizado en forma exponencial.

Las ventajas y desventajas del Sistema de Comunicacón entre diversos usuarios son :

**Ventajas :**

-- Si suponemos que un criptoanalista tiene la ventaja de conocer la pareja de mensaje original-criptograma, o sea una pareja correspondiente de **M** y **C**, y quiere calcular la clave común, $k_{ij}$, tiene que hacer la siguiente operación :

$$k_{ij} \equiv \log_M C, \qquad \text{sobre } GF(p)$$

lo cual es un cálculo de logaritmos sobre el campo de Galois GF(p), ya se había mencionado que es un cálculo muy dilatado, aún usando el mejor algoritmo para ello.

**Desventajas :**

-- Los valores de $k_{ij}$ y p-1 tienen que ser primos relativamente para que la inversa de la clave común, $k_{ij}$, (que es la clave para descifrar) exista.

Esta condición quizás no se cumple para $k_{ij} \equiv y_j^{x_i} \pmod p$ calculada, a partir de una $y_j$ dada en el archivo público y además de una $x_i$ fija (note que se había escogido $x_i$ aleatoriamente para calcular $y_i$, pero una vez que $y_i$ está publicada, $x_i$ ya está fija). Una forma de proceder es que el usuario i seleccione una $x_i$ de tal manera que gcd(k, p-1) = 1, para un valor dado de $y_j$, y después publica la $y_i$ calculada con la $x_i$ así elegida. Pero esto significa que el usuario i tiene que publicar una nueva $y_i$. Esto implica que para distintos usuarios con quien desea comunicarse el usuario i, tiene que elegir diferentes $x_i$, calcular su $y_i$ correspondientes y publicarlas.

## VI.3.2 COMPLEJIDAD EN EL TIEMPO.

En este algoritmo de ciframiento de clave pública el número de operaciones realizadas en el transmisor, si consideramos un bloque de $R_A$ muestras y un número nc de dígitos a cifrar es el siguiente :

No. de operaciones = $R_A \times nc \times 2 \times \log_2(e)$
para el ciframiento

donde

- $R_A$ Es el número de muestras en el bloque a cifrar.
- e Es el valor numérico de la clave utilizada para cifrar.
- nc Es el número de dígitos en que se divide cada muestra a cifrar.

Mientras que el número de operaciones realizadas en el receptor, si se considera un bloque de $R_A$ muestras y un número de m-c de dígitos a descifrar, es el siguiente :

No. de operaciones = $R_A \times m\text{-}c \times 2 \times \log_2(d)$
para el desciframiento

donde

- $R_A$ Es el número de muestras en el bloque a descifrar.
- d Es el valor numérico de la clave utilizada para cifrar.
- m-c Es el número de dígitos en que se divide cada muestra a cifrar.

## VI.4 RESULTADOS CORRESPONDIENTES AL ESQUEMA DE CIFRAMIENTO EN EL DOMINIO DE LA FRECUENCIA.

### VI.4.1 Método de permutación de Coeficientes de la DFT.

El esquema de ciframiento asimétrico propuesto por Elgamal,T [26], empleado en el *Método de permutación de coeficientes de la DFT*, basa su seguridad principalmente en la dificultad del cálculo de logaritmos sobre el campo de Galois, **GF(p)**. Si este cálculo es computacionalmente fácil, entonces la seguridad del esquema de ciframiento se puede romper rápidamente. Sin embargo, si se elige cuidadosamente el número primo **p**, ni con el mejor algoritmo que se conoce se puede hacer este cálculo fácilmente [32].

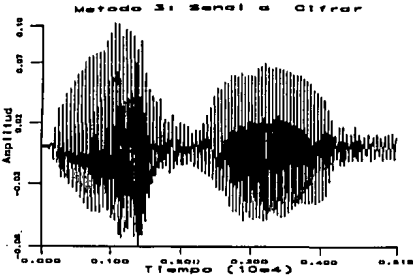
Los resultados correspondientes a la simulación del método 3 se muestran en el inciso **VI.4.1.1**, las ventajas y desventajas de este esquema de ciframiento se mencionan. en el inciso **VI.4.1.2**, mientras que las ventajas y desventajas del sistema de comunicación en el inciso **VI.4.1.3** .

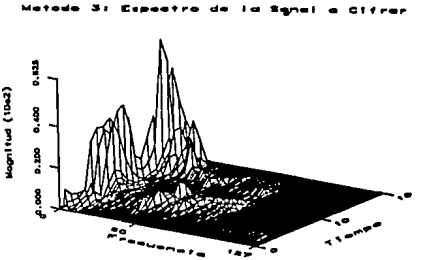
#### VI.4.1.1 Presentación de Resultados Gráficos correspondientes al método 3

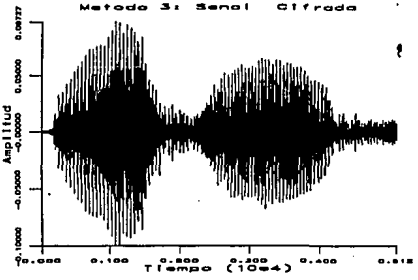
En la Figura 6.3 se muestran las formas de onda de la simulación del esquema de ciframieto de permutación de los coeficientes de la DFT. En la Fig. 6.3a se muestran la forma de onda en el dominio del tiempo, así como en el dominio de la Frecuencia.

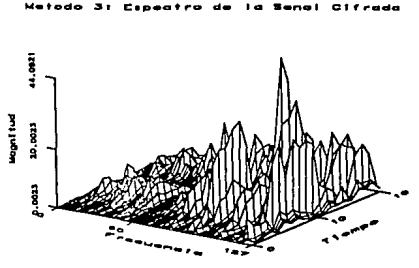
En la Fig.6.3b se muestran las formas de onda de la señal cifrada en el dominio del tiempo, así como en el dominio de la frecuencia, cabe hacer notar que en dicha figura, no existe una distorsión total de la forma de onda de la señal de voz. Además, para ciertos valores pequeños, los amplifica -zona sombreada de la figura-, es posible escuchar el contenido del mensaje a cifrar. Con respecto al espectro de la señal de voz cifrada, dicho espectro presenta una atenuación en las componentes de baja frecuencia y una amplificación de las componentes medias y altas. Además, el espectro de la señal descifrada presenta una atenuación de las componentes de baja frecuencia, además de una amplificación de las componentes medias y altas.

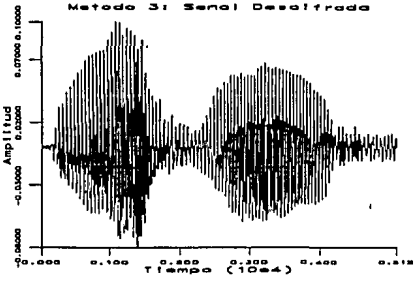
En la Fig.6.3c se muestran las formas de onda del proceso de descifrado, en dicha figura se puede observar que se recuperan las mismas formas de onda del mensaje original en el dominio del tiempo.

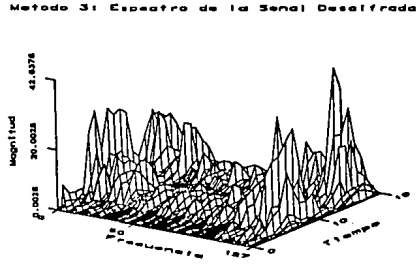

Metodo 3: Senal a Cifrar
Amplitud
Tiempo (10e4)


Metodo 3: Espectro de la Senal a Cifrar
Magnitud (10e2)
Frecuencia
Tiempo


Metodo 3: Senal Cifrada
Amplitud
Tiempo (10e4)


Metodo 3: Espectro de la Senal Cifrada
Magnitud
Frecuencia
Tiempo


Metodo 3: Senal Descifrada
Amplitud
Tiempo (10e4)


Metodo 3: Espectro de la Senal Descifrada
Magnitud
Frecuencia
Tiempo

### VI.4.1.2 Ventajas y desventajas del esquema de cifrамiento.

Las ventajas y desventajas del esquema de cifrамiento son :

**Ventajas :**

-- Se tiene un bloque fijo de muestras a cifrar para todos los usuarios.

-- La operación de multiplicación para $C_2$ en el proceso de cifrado del mensaje **M** puede reemplazarse por cualesquier otra función invertible, tal como una adición mod **p**.

**Desventajas :**

-- El mensaje cifrado (criptograma) **C**, es el doble ( $C = 2M$) del mensaje a cifrar **M**.

### VI.4.1.3 Ventajas y desventajas del Sistema de Comunicación entre diversos usuarios.

Las ventajas y desventajas del Sistema de Comunicación entre diversos usuarios son :

**Ventajas :**

-- Se consigue que tanto el emisor como receptor de un criptograma se "reconozcan" entre sí, es decir, el receptor sabe con exactitud quién le envió el mensaje **M**.

**Desventajas :**

-- En este esquema de comunicación se debe de cumplir que $\gcd(K_{ij}, R) = 1$ (donde $R = pq$) para que la clave inversa de $K_{ij}$, $K_{ij}^{-1}$ exista, el cálculo de $K_{ij}^{-1}$ es un trabajo muy dilatado.

## VI.4.2 COMPLEJIDAD EN EL TIEMPO.

El número de operaciones realizadas por el transmisor para cifrar un mensaje [15] es de :

No. de operciones = $4 \log_2 (p)$, en **GF(p)**
para el ciframiento

donde

**p** Es un número primo definido en **GF(p)**.

Mientras que el número de operaciones realizadas en el receptor para recuperar el mensaje **M**, a partir del mensaje cifrado **C**, es de :

No. de operaciones = $4 \log_2 (p)$, en **GF(p)**.
para el desciframiento

donde

**p** Es un número primo definido en GF(p).

## VI.4.3 PRUEBA DE SEGURIDAD.

Este esquema de cifrado de clave pública hace uso de la dificultad de calcular logaritmos sobre un campo finito **GF(q)** con un número primo de elementos $0,1,2,\ldots,q-1$, trabajando en módulo **q**.

Dada la función siguiente :

$$y = a^x \bmod q, \qquad 1 \leq x \leq q-1$$

siendo **a** un elemento fijo primitivo de **GF(q)**, o sea una potencia del rango **a** sobre los elementos $1,2,\ldots,q-1$ de GF(q), **x** representa el logaritmo base a de **y** sobre **GF(q)**

$$x = \log_a y \quad \text{sobre GF(q)} \qquad 1 \leq y \leq q-1$$

El cálculo de **y** a partir de **x** es fácil, tomando un máximo de **2** $(\log_2 q)$ multiplicaciones.

Sin embargo, el cálculo de **x** a partir de **y** es mucho más difícil, presentando para determinados valores de **q** escogidos a propósito, un número de operaciones del orden de $q^{1/2}$, según uno de los mejores algoritmos conocidos, [25].

## VI.5. RESULTADOS CORRESPONDIENTES AL ESQUEMA DE CIFRAMIENTO DE PERMUTACION DE PARAMETROS LPC BASADO EN EL ESQUEMA PROPUESTO POR RSA - WILLIAMS - RABIN.

### VI.5.1 Método de permutación de parámetros LPC.

El esquema de ciframiento asímetrico propuesto por **Rabin-Willins-RSA**, empleado en el *Método de cifrado permutación de parámetros LPC*, basa su seguridad en el problema de factorizar **R**, donde **R = pq**, así como en la solución de una congruencia de segundo grado [26][33].

Los resultados correspondientes a la simulación del método 4 se muestran en el inciso **VI.5.1.1**, las ventajas y desventajas de este esquema de ciframiento se mencionan en el inciso **VI.5.1.2**, y en el inciso **VI.5.1.3** se mencionan las ventajas y desventajas del sistema de comunicación entre diversos usuarios.

#### VI.5.1.1 Presentación de Resultados Gráficos correspondientes al método 4

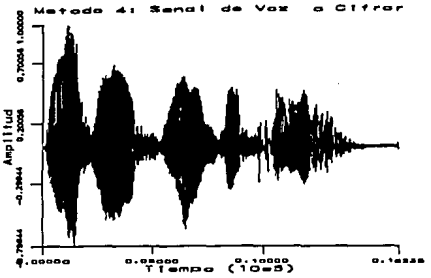
En la Figura 6.4 se muestran los resultados de la simulación del esquema de ciframiento 4, que consiste en la permutación de los parámetros LPC. En dicha figura se muestran las formas de onda del mensaje de voz a cifrar en el dominio del tiempo, así como en el dominio de la frecuencia.

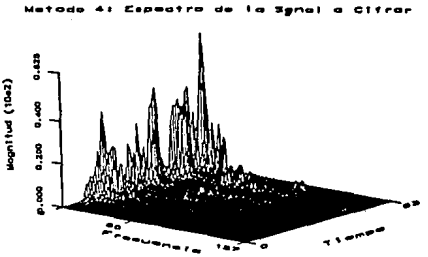
En la Fig.6.4b se muestran los resultados prácticos del esquema de ciframiento que consiste en la permutación de los parámetros LPC, en dicha figura, se muestra la señal cifrada en el dominio del tiempo.

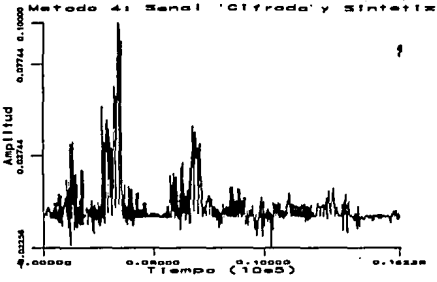
Para este método, la Fig.6.4b representa el espectro en magnitud de la señal cifrada, en ella existe una casi uniformidad de las magnitudes de las diferentes *tramas* que componen dicha señal, es decir, se aprecia una atenuación notable de las componentes bajas y medias de la señal cifrada.

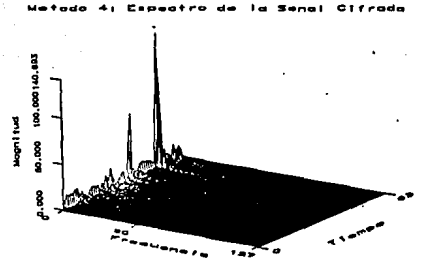
En la Fig.6.4c se muestra la señal descifrada y sintetizada a partir de los parámetros LPC. En dicha figura se nota que la señal reconstruida no es igual a la señal a sintetizar, pero conserva las cualidades de la señal original. También se nota que en la parte inferior de la figura descifrada no se reconstruye totalmente la forma de onda de la señal de voz original.

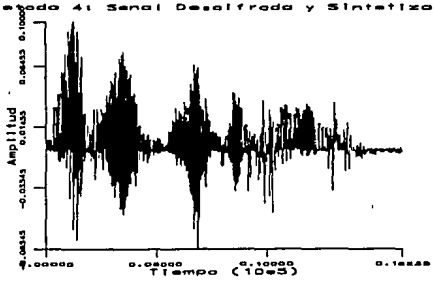
La figura 6.4c representa el espectro en magnitud de la señal descifrada. En dicha figura se logra percibir una similitud con respecto a la señal de voz a cifrar, es decir, se recuperan las componentes de frecuencia baja y media .

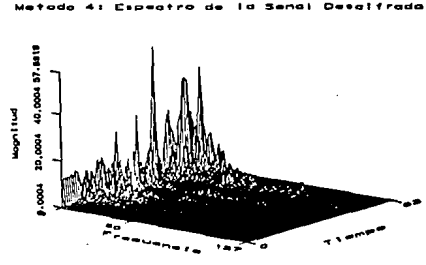

Metodo 4: Senal de Voz a Cifrar
Amplitud
Tiempo (10e5)


Metodo 4: Espectro de la Senal a Cifrar
Magnitud (10e2)
Frecuencia
Tiempo


Metodo 4: Senal 'Cifrada' y Sintetiza
Amplitud
Tiempo (10e5)


Metodo 4: Espectro de la Senal Cifrada
Magnitud
Frecuencia
Tiempo


Amplitud
Tiempo (10e5)


Metodo 4: Espectro de la Senal Descifrada
Magnitud
Frecuencia
Tiempo

### VI.5.1.2 Ventajas y desventajas del esquema de cifrамiento.

Las ventajas y desventajas del esquema de cifrамiento son :

**Ventajas :**

-- Existe una ambigüedad de 4 : 1 para que el criptoanalista seleccione el valor correcto **M**, a partir del criptograma **C**. Es decir, seleccionar el mensaje **M** correcto a partir de 4 valores posibles.

**Desventajas :**

-- A cada mensaje $m_i$ a cifrar hay que agregarle un cierto grado de redundancia, para que de esta manera el receptor pueda recalcular el mensaje original, **M**, a partir del criptograma **C**.

### VI.5.1.3 Ventajas y desventajas Sistema de Comunicación entre diversos usuarios.

Las ventajas y desventajas del Sistema de Comunicación entre diversos usuarios son :

**Ventajas :**

-- La matriz de clave común $K_{ij}$ tiene la restricción de que tiene que no ser singular para que su inversa, $K_{ij}^{-1}$, exista. Sin embargo, esta restricción es mucho más fácil de cumplir comparada con la restricción de que $\gcd(K_{ij}, p-1) = 1$ para el caso de la realización de la clave común por elevación exponencial descrita en el inciso **IV.4.2**. Esto se debe a que la probabilidad de que el determinante de $K_{12}$ sea igual a cero es demasiado pequeña (casi nula) comparada con la posibilidad de que el determinante de $K_{ij}$ sea cualquier número diferente de cero, para la matriz $K_{ij}$ que tiene elementos calculados a partir de otros elementos seleccionados aleatoriamente.

**Desventajas :**

-- La matriz de clave común $K_{ij}$ tiene la restricción de que no debe ser singular para que $K_{ij}^{-1}$ exista.

### VI.5.2 COMPLEJIDAD EN EL TIEMPO.

Para el algoritmo de permutación de parámetros LPC, el número de operaciones realizadas por el transmisor, si consideramos un bloque de *p* parámetros para **nf** frames a cifrar, es el siguiente :

No. de operaciones = **nf** x *p* x 2 ( $\log_2$ (e) )
para el ciframiento

donde
*p* Es el número de parámetros LPC a cifrar por "frame".
**nf** Es el número de frames a cifrar.

Mientras que el número de operaciones realizadas en el receptor, si consideramos *p* parámetros por "trama" a descifrar, es el siguiente :

No. de operaciones para el desciframiento = $4 \left[ nf \times p \times 2 (\log_2(e)) \right]$

donde
*p* Es el número de parámetros LPC a cifrar por "frame".
**nf** Es el número de frames a cifrar.

### VI.5.3 PRUEBA DE SEGURIDAD.

La seguridad de este esquema de ciframiento se basa en dos aspectos muy importantes que son :

1.) La dificultad de factorizar el producto de dos números primos, R = pq, donde p y q son números primos de diferente longitud cada uno de ellos.

2.) La dificultad de buscar una solución rápida para resolver una congruencia de segundo grado.

En este inciso se muestra únicamente la dificultad que existe en encontrar la solución rápida a una congruencia de segundo orden, ya que la dificultad de factorizar el producto de dos números primos se analizó detalladamente en el inciso VI.2.3.

Primeramente, el emisor, para enviar el mensaje **M**, de manera segura, lo hace empleando la ecuación

$$C \equiv M^2 \bmod R$$

y, envía el mensaje cifrado **C** hacia el receptor.

El criptoanalista, al igual que el receptor, debe determinar el mensaje correcto **M**, a partir del mensaje cifrado **C**, resolviendo la congruencia siguiente ([33], ec. 1) :

$$M \equiv C^2 \bmod R$$

El criptoanalista, con el auxilio de los siguientes lemas simplifica la congruencia anterior de la siguiente manera :

**Lema 5.1** : Una solución a la congruencia

$$M \equiv C^2 \bmod R \qquad (1.i)$$

puede obtenerse, sustituyendo la congruencia anterior, por las siguientes congruencias([33], pag. 358 )

$$x^2 \equiv C \bmod p \qquad y^2 \equiv C \bmod q \qquad (1.ii)$$

y, la solución de **x** y **y** a partir de las congruencias (1.ii), se obtiene por medio del Teorema del Residuo Chino.

A partir de las congruencias anteriores, es posible notar, que para que el criptoanalista conozca o determine el mensaje **M** a partir del criptograma **C**, primero debe de factorizar el valor de **R**, en sus factores primos **p** y **q**, lo cual es dilatado como se mostró en el inciso V.2.3, y posteriormente seleccionar un valor único a partir de 4 posibles, es decir,

$$M \equiv \pm x^2 \bmod p \qquad M \equiv \pm y^2 \bmod q$$

**Lema 5.2** : Resolver la congruencia ([23], pag. 189 )

$$x^2 \equiv C \bmod p \qquad (2.i)$$

es equivalente a resolver

$$y^2 \equiv C \bmod q \qquad (2.ii)$$

si consideramos el problema de resolver ([23], pag. 190 )

$$y^2 \equiv d \bmod q \qquad (2.iii)$$

Primero notese que, en general, las ecuaciones (2.i) y (2.ii), no tienen una solución única. Los enteros **d** para los cuales la congruencia (2.iii), tienen una única solución son llamados *residuos cuadráticos módulo* **p** [29], y la solución fundamental para este tipo de ecuación es conocida a partir del criterio de Euler [29].

**Teorema 5.1** ([23], pag. 190) :

Un entero **a** en el rango $1 \leq a \leq p-1$ es un **residuo cuadrático modulo p**, para el número primo impar **p**, sí y solamente si

$$a^{(p-1)/2} \equiv 1 \mod p$$

con este resultado se prueba el lema siguiente.

**Lema 5.3** : Si **p** es un número primo de la forma 4k-1, y **d** es un residuo cuadrático de **p**, una solución de la congruencia

$$y^2 \equiv d \mod p \qquad (3.i)$$

está dada por

$$y \equiv d^k \mod p \qquad (3.ii)$$

De la expresión ( 3.ii ), y partiendo de que **d** es un residuo cuadrático módulo **p**, y además empleando el criterio de Euler, se tiene que

$$d^{(p-1)/2} \equiv 1 \mod p$$

Dado que $k = (p + 1)/4$, se tiene

$$d^{(p+1)/4}\ d^{(p+1)/4} = d^{(p+1)/2} = d^{(p-1)/2}\ d$$

$$= d \pmod p$$

y, con esto se prueba que los números primos **p** y **q** son ambos congruentes a 3 módulo 4, y que el procedimiento de calcular estos números se realiza en un tiempo polinomial.

## VI.6 RESULTADOS CORRESPONDIENTES AL ESQUEMA DE CIFRAMIENTO DE MANIPULACION DE PARAMETROS LPC BASADO EN EL ESQUEMA RSA REALIZADO EN FORMA MATRICIAL.

### VI.6.1 Manipulación de los parámetros LPC.

El esquema de ciframiento de clave pública propuesto en el capítulo V, es una extensión del esquema de ciframiento **RSA** realizado en forma matricial [30] y se emplea en el *Método de cifrado de los coeficientes LPC.* Este esquema de cifrado basa su seguridad en : (1) La complejidad computacional necesaria para factorizar números primos grandes. Si dichos factores, que en este caso son **p** y **q**, se seleccionan cuidadosamente, ni con el mejor algoritmo conocido es posible calcularlos [32]. (2) En una función $f(.)$ de un sólo sentido [17].

Los resultados correspondientes a la simulación del método propuesto se muestran en el inciso **VI.6.1.1,** las ventajas de este esquema de ciframiento se mencionan en el siguiente **VI.6.1.2** y las ventajas y desventajas del Sistema de Comunicación entre diversos usuarios se presentan en el inciso **VI.6.1.3.**

#### VI.6.1.1 Presentación de Resultados Gráficos correspondientes al método 5

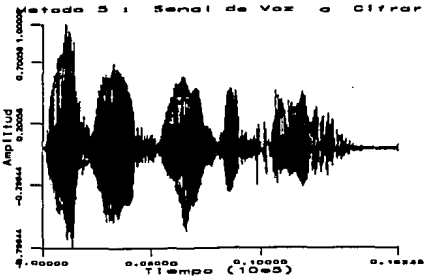
En la Figura 6.5 se representan los resultados de la simulación del esquema de ciframiento propuesto. En la parte izquierda de dicha figura, se encuentran las formas de onda en el dominio del tiempo y en la parte derecha se encuentran las formas en el dominio de la frecuencia.

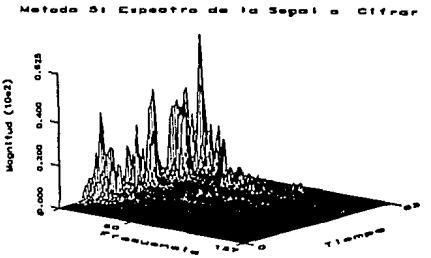
En la Fig.6.5a se muestra la forma de onda de la señal a cifrar, así como su respectivo espectro en magnitud.

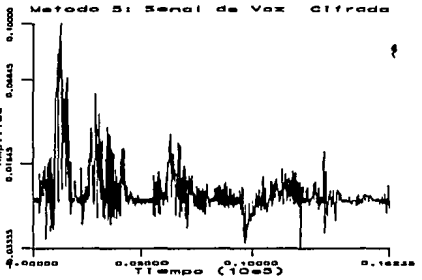
En la Fig.6.5b, se muestra la forma de onda de la señal cifrada,así como su espectro en magnitud. En dicha figura se observa que en el dominio del tiempo, la forma de onda de la señal original se destruye, de tal forma que no se logra visualizar ningún lóbulo principal de la señal de voz. En el dominio de la frecuencia se observa una uniformidad en la magnitud de todas las *tramas*, es decir, existe una atenuación de las componentes bajas y medias.

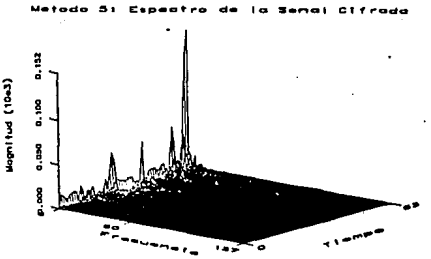
En la Fig.6.5c se muestra la señal descifrada y sintetizada a partir de los parámetros LPC. En dicha figura se observa que la señal sintetizada no es idéntica a la señal original a cifrar por *trama* de la señal a sintetizar.

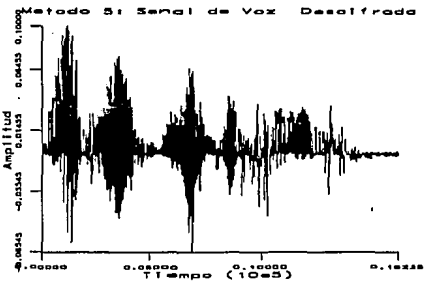
Como se puede observar, en la Fig.6.5c, el espectro de la señal sintetizada, recupera las frecuencias fundamentales -bajas y medias- por *trama* de la señal de voz original.

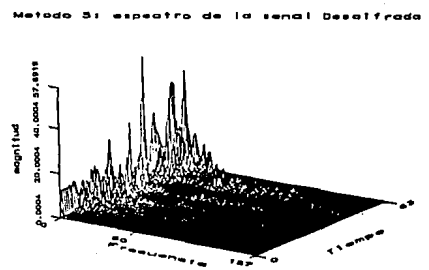

Metodo 5 : Senal de Voz a Cifrar
Amplitud
Tiempo (10e5)


Metodo 5: Espectro de la Sepal a Cifrar
Magnitud (10e2)
Frecuencia
Tiempo


Metodo 5: Senal de Voz Cifrada
Amplitud
Tiempo (10e5)


Metodo 5: Espectro de la Senal Cifrada
Magnitud (10e3)
Frecuencia
Tiempo


Metodo 5: Senal de Voz Descifrada
Amplitud
Tiempo (10e5)


Metodo 5: espectro de la senal Descifrada
magnitud
Frecuencia
Tiempo

### VI.6.1.2 Ventajas y desventajas del esquema de ciframiento.

Las ventajas y desventajas del esquema de ciframiento son :

**Ventajas :**

-- Se tiene un esquema rápido de ciframiento y de desciframiento, ya que no requiere elevar un arreglo de mensajes **M**i a la e (mod R).

-- Tanto el emisor como receptor pueden definir cualquier función de un sólo sentido, f().

-- Únicamente se necesitan elevar *n* elementos a la potencia e mod R. Esto reduce notablemente el número de operaciones tanto en el proceso de cifrado como en el proceso de descifrado.

-- Para que el criptoanálista pueda recuperar o conocer el mensaje **M**, a partir del mensaje cifrado **C**, tiene que realizar los pasos siguientes. 1.) Resolver un sistema de ecuaciones de *n* x *n*. 2.) Determinar los elementos de la diagonal principal. 3.) Evaluar una función de un sólo sentido en "sentido inverso".

-- Los algoritmos de ciframiento y desciframiento basan su velocidad en el Teorema de Cayley-Halmilton. Además, la velocidad de ambos algoritmos depende de la dimensión de la matriz **A** y la capacidad de evaluación de la función de un sólo sentido. La implantación más eficiente es el caso en el cual ambas operaciones (ciframiento y desciframiento) emplean una operación sencilla de multiplicación y la evaluación de una función simple de un sólo sentido.

-- Se obtiene un mayor grado de inentigibilidad si se agrupan sub-bloques de dígitos de tal manera que el número de dígitos (nc) sea menor al número de dígitos de RA.

-- No se requiere de una gran capacidad de memoria para efectuar el ciframiento y desciframiento de la señal, ya que se procesa un solo parámetro a la vez.

**Desventajas :**

-- Se pierde precisión al descifrar la señal.

-- Una incomodidad de este esquema cifrador, es el manejo de los números primos grandes, es decir, se tienen que hacer operaciones con números muy grandes (ejemplo, 100 dígitos) y estas operaciones son difíciles de realizar en las microcomputadoras (por ejemplo, una PC-AT), y usando el lenguaje, C, solamente se puede lograr operaciones de suma, resta, multiplicación y división con números enteros que tienen un máximo de 36 dígitos, utilizando un arreglo llamado "long-integer", pero no es posible aplicar muchas funciones sobre estos números enteros grandes, como por ejemplo, la función "módulo R" (que se emplea en todos los algoritmos criptográficos de los capítulos IV y V).

-- Otra desventaja de este esquema es la pérdida significativa en la relación señal-ruido en el receptor, debido a que parte de la energía, se pierde en el receptor debido al ruido que se transmitió.

-- Este esquema de cifrамiento no puede operar con números grandes cuya longitud sea superior a 100 bits.

### VI.6.1.3 Ventajas y desventajas del Sistema de Comunicación entre diversos usuarios.

Las ventajas y desventajas del Sistema de Comunicación entre diversos usuarios son :

**Ventajas :**

-- La matriz de clave común $K_{ij}$ tiene la restricción de que tiene que ser no singular para que su inversa, $K_{ij}^{-1}$, exista. Sin embargo, esta restricción es mucho más fácil de cumplir comparada con la restricción de que gcd( $K_{ij}$, p-1 ) = 1 para el caso de la realización de la clave común por elevación exponencial descrita en el inciso **IV.4.2.** Esto se debe a que la posibilidad de que el determinante de $K_{12}$ sea igual a cero es demasiado pequeña (casi nula) comparada con la posibilidad de que el determinante de $K_{ij}$ sea cualquier número diferente de cero, para la matriz $K_{ij}$ que tiene elementos calculados a partir de otros elementos seleccionados aleatoriamente.

**Desventajas :**

-- La matriz de clave común $K_{ij}$ tiene la restricción de que no debe ser singular para que $K_{ij}^{-1}$ exista.

## VI.6.2 COMPLEJIDAD EN EL TIEMPO.

El principal aporte del esquema de ciframiento propuesto en el capítulo V, consiste en mostrar que los procedimientos de ciframiento y desciframiento utilizados, por el esquema de ciframiento RSA en forma matricial, son por mucho, más rápidos, que los algoritmos de ciframiento y desciframiento realizados por el esquema RSA [30]. La velocidad de los procedimientos empleados por el esquema de ciframiento RSA en forma matricial, se basan en el tamaño de la matriz **A**, es decir, la rápidez para evaluar la matriz **A** a la e-ésima potencia durante el proceso de cifrado, ó a d-ésima potencia durante el proceso de desciframiento.

Los procedimientos de ciframiento y desciframiento se dividen dos partes. La primera parte consiste en calcular los coeficientes $C_i^e$ y $C_i^d$ a partir de las ecuaciones (6.1) y (6.2). La segunda parte consiste en elevar la matriz **A** a la e-ésima potencia como se explica a continuación.

### 1.) Pre-cálculo de los Coeficientes.

El cálculo de los coeficientes $C_i^{ei}$, en la ec. (6.1), para el proceso de ciframiento tiene exactamente la misma complejidad computacional que el cálculo de los coeficientes $C_i^{di}$, en la ec. (6.2), para el proceso de desciframiento, así que sólo se discutira la complejidad computacional del proceso de ciframiento.

$$
\begin{aligned}
a_{11}^{e} &\equiv c_{n-1}^{e}\, a_{11}^{n-1} + c_{n-2}^{e}\, a_{11}^{n-2} + \ldots + c_{0}^{e} \\
a_{22}^{e} &\equiv c_{n-1}^{e}\, a_{22}^{n-1} + c_{n-2}^{e}\, a_{22}^{n-2} + \ldots + c_{0}^{e} \\
&\;\;\vdots \qquad\quad \vdots \qquad\qquad\quad \vdots \\
a_{nn}^{e} &\equiv c_{n-1}^{e}\, a_{nn}^{n-1} + c_{n-2}^{e}\, a_{nn}^{n-2} + \ldots + c_{0}^{e}
\end{aligned}
\qquad (6.1)
$$

$$
\begin{aligned}
a_{11}^{ed} &\equiv c_{n-1}^{d}\, a_{11}^{e(n-1)} + c_{n-2}^{d}\, a_{11}^{e(n-2)} + \ldots + c_{0}^{d} \\
a_{22}^{ed} &\equiv c_{n-1}^{d}\, a_{22}^{e(n-1)} + c_{n-2}^{d}\, a_{22}^{e(n-2)} + \ldots + c_{0}^{d} \\
&\;\;\vdots \qquad\quad \vdots \qquad\qquad\quad \vdots \\
a_{nn}^{ed} &\equiv c_{n-1}^{d}\, a_{nn}^{e(n-1)} + c_{n-2}^{d}\, a_{nn}^{e(n-2)} + \ldots + c_{0}^{d}
\end{aligned}
\qquad (6.2)
$$

Para la determinación del número de operaciones necesarias para el cálculo de $\hat{C}_i^{ei}$, se requieren realizar las siguientes operaciones :

**a.)** Para evualuar $a_{ii}$ a la **e**-ésima potencia se requiere a lo sumo $2\lfloor \log_2 e \rfloor$ multiplicaciones [24]. De esta manera para evaluar ya sea la ecuación (6.1) o la ecuación (6.2) se requiere a lo sumo ([30], ec. 19) :

$$2n \lfloor \log_2 e \rfloor + n(n-2) \qquad (6.3)$$

multiplicaciones.

Además, existen dos maneras para resolver tanto la ecuación (6.1) ó (6.2), que son : 1.) Utilizando la regla de Cramer, y 2.) Utilizando el algoritmo de Vandermonde.

**b.1)** Si se emplea la regla de Cramer para calcular los coeficientes $\hat{C}_{i1}$, entonces se necesitan a lo sumo ([30], ec. 20) :

$$2n\lfloor \log_2 e \rfloor + n(n-2)+(n+1) \sum_{i=1}^{n-1} \left[ \prod_{j=n-i+1}^{n} j \right] + 15 \lfloor \log_{10} R \rfloor \qquad (6.4)$$

multiplicaciones, y

$$( n+1 ) \sum_{i=1}^{n-1} \left[ \left[ \prod_{j=n-i}^{n} j \right] / \left[ n-i+1 \right] \right] + 10 \lfloor \log_{10} R \rfloor \qquad (6.5)$$

adiciones.

**b.2)** Si se observa detalladamente la ecuación (6.1) ó (6.2) se nota que es un Sistema Vandermonde [31], por lo tanto, el algoritmo Vandermonde puede emplearse para calcular los coeficientes. Este algoritmo tiene distintas ventajas computacionales cuando el tamaño de la matriz **A** es grande (por ejemplo, $n \geq 7$ ). Esta etapa necesita a lo sumo ([30], ec. 22) :

$$2n \lfloor \log_2 e \rfloor + n(n-2) + \frac{n(n-1)}{2} \left[ 15\lfloor \log_{10} R \rfloor + 3 \right] \qquad (6.6)$$

multiplicaciones, y

$$\frac{n(n-1)}{2}\left[10 \lfloor \log_{10} R \rfloor + 3 \right] \qquad (6.7)$$

adiciones.

**2.) Proceso de Ciframiento y Desciframiento.**

Una vez que se conocen los coeficientes $C_i^{ei}$ ó $C_i^{di}$, se procede a evaluar la matriz **A** de ciframiento (desciframiento) a la **k**-ésima potencia empleando el teorema de Caley-Hamilton ([30], ec.1) aplica a la ecuación siguiente :

$$A^k = c_{n-1} A^{n-1} + c_{n-2} A^{n-2} + \ldots + c_0 I = 0 \qquad (6.7)$$

para evaluar $A^k$, solamente se requiere calcular $A^2, A^3, \ldots, A^{n-1}$, multiplicarlas por el correspondiente coeficiente $C_{n-1}^{ei}$ y sumarlas. Este proceso se realiza en ([30], ec. 24 )

$$\frac{n(n+1)(n+2)(n-2)}{6} + \frac{n(n+1)(n-1)}{2} \qquad (6.8)$$

multiplicaciones, y

$$\frac{n(n+1)(n-1)(n-2)}{6} + \frac{n(n+1)(n-2)}{2} \qquad (6.9)$$

adiciones.

## VI.6.3 PRUEBA DE SEGURIDAD.

Existe una forma más rápida de evaluar la matriz **A** a la **k**-ésima potencia utilizando el algoritmo de Vandermonde. Pero la matriz **A** debe de cumplir con : 1.) Los renglones de una matriz **A** de orden $n \times n$ deben de tener la forma $[1 \; a_i \; a_i^2 \; \ldots \; a_i^{N-1}]$. La matriz **A** no cumple con la característica anterior, entonces se emplea el teorema de Caley-Hamilton, para evaluar la matriz **A** a la **k**-ésima potencia.

La seguridad del esquema de ciframiento RSA realizado en forma matricial propuesto en el capítulo **V**, es diferente a la seguridad del esquema **RSA** original. En este inciso se presenta la complejidad de la matriz **A**, cuando **A** se eleva a la **e**-ésima potencia empleando el teorema de Caley-Hamilton. La estructura de $\mathbf{A}^e$ puede establecerse formalmentea partir del siguiente teorema :

**Teorema 6.1** ([30], pag. 145) :

Si definimos una matriz triangular superior de orden $n \times n$. Y denotamos $a_{i,i+j}$ y $a^{e}_{i,(i+j)}$ como la $(i,i+j)$-ésima entrada, y a $(i,i+j)$-ésima entrada después de que la matriz $\mathbf{A}_{(e)}$ se ha elevado a la **e**-ésima potencia, respectivamente. Entonces $a^{(e)}_{i,i+j}$, donde $1 \le i \le n$, $0 \le j \le n-1$, puede representarse como

$$
\begin{aligned}
a^{(e)}_{i,i+j} = a_{i,i+j} \sum_{i_1=1}^{e} & a_{ii}^{e-i_1} \, a_{i+j,i+j}^{i_1-1} \\
+ \sum_{i_1=1}^{j-1} & a_{i,i+i_1} a_{i+i_1,i+j} \sum_{i_1=1}^{e-1} \sum_{i_2=i_1}^{e-1} a_{ii}^{e-1-i_2} \, a_{i+l_1,i+i_1}^{i_2-i_1} \, a_{i+j,i+j}^{i_1-1} \\
+ \sum_{l_1=1}^{j-2} & \sum_{l_2=l_1+1}^{j-1} a_{i,i+l_1} a_{i+l_1,i+l_2} a_{i+l_2,i+j} \\
& \sum_{i_1=1}^{e-2} \sum_{i_2=i_1}^{e-2} \sum_{i_3=i_2}^{e-2} a_{ii}^{e-2-i_3} \, a_{i+l_1,i+l_1}^{i_3-i_2} \, a_{i+l_2,i+l_2}^{i_2-i_1} \, a_{i+j,i+j}^{i_1-1} \\
& \vdots
\end{aligned}
\qquad (6.10)
$$

$$\vdots$$

$$+a_{i,i+1}a_{i+1,i+2}\cdots a_{i+j-1,,i+j}\sum_{i_1=1}^{e-j+1}\sum_{i_2=i_1}^{e-j+1}\cdots\sum_{i_j=i_{j-1}}^{e-j+1}a_{11}^{e-j-1_j+1}\,a_{i+1,i+1}^{i_1-1_{j-1}}\cdots a_{i+j,i+j}^{i_1-1}$$

donde cada término

$$\sum_{i_1=1}^{e-k}\sum_{i_2=i_1}^{e-k}\cdots\sum_{i_{k-1}=i_1}^{e-k}\sum_{i_k=i_{k+1}}^{e-k}a_{11}^{e-k-1_{k+1}}\,a_{i+1_1,i+1_1}^{i_{k+1}-i_k}\cdots a_{i+1_k,i+1_k}^{i_2-i_1}\,a_{i+j,i+j}^{i_1-1}$$

$$=\frac{\displaystyle\sum_{m=i,i+1_1,i+1_2,\ldots,i+1_k,i+j}(-1)^s a_{mm}^e\prod_{\substack{m_1,m_2=i,i+1_1,i+1_2,\ldots,i+1_k,i+j\\ m_1,m_2\neq m\\ i\le m_1<m_2\le i+j}}(a_{m_2m_2}-a_{m_1m_1})}{\displaystyle\prod_{\substack{m_1,m_2=i,i+1_1,i+1_2,\ldots,i+1_k,i+j\\ i\le m_1<m_2\le i+j}}(a_{m_2m_2}-a_{m_1m_1})} \qquad (6.11)$$

donde $k = 1,2,\ldots,j-1$, y

$$s = \begin{cases} k+1, & m = i \\ k+1+subscript(l_{k_1}) & m = i+l_{k_1} \\ 2k+2, & m = i+j \end{cases} \qquad k_1=1,2,\ldots,k$$

Nótese el procedimiento para recuperar la matriz original después de que se ha elevado la matriz **A** a la e-ésima potencia, el denominador de la ecuación (6.11) tiene que ser un primo relativo con respecto a R. La finalidad de que el númerador sea un número primo relativo, es evitar que el criptoanalista pueda factorizar cada elemento a cifrar durante la evaluación de la matriz **A**.

La forma general del numerador de la ecuación (6.11) puede descomponerse y reescribirse en una forma diferente. Esta simplificación puede resumirse formalmente con el lema siguiente.

**Lema 6.4** ([30], pag. 146) :

La forma general del numerador en la ecuación (6.11) puede ser escrito como una combinación no lineal de ecuaciones de menor orden de una misma forma, es decir,

$$\sum_{m=1}^{n} (-1)^{s} a_{mm}^{ed} \prod_{\substack{m_1, m_2 \\ m_1, m_2 \neq m \\ 1 \leq m_1 < m_2 \leq n}} (a_{m_2 m_2} - a_{m_1 m_1}) \qquad , s = n+m$$

$$= \sum_{m=1}^{n} (-1)^{s_1} a_{mm}^{n-2} \left[ \sum_{\substack{m_1=1 \\ m_1 \neq m}}^{n} (-1)^{s_2} a_{m_1 m_1}^{ed} \prod_{\substack{m_2, m_3 = 1 \\ m_2, m_3 \neq m_1 \\ 1 \leq m_2 < m_3 \leq n}}^{n} (a_{m_3 m_3} - a_{m_2 m_2}) \right] \quad (6.12)$$

donde $s_1 = n+m-1$, y

$$s_2 = \begin{cases} n + m_1 & m_1 < m \\ n + m_1 - 1 & m_1 > m \end{cases}$$

En general, los esquemas de cifrамiento son vulnerables al ataque de mensaje en claro seleccionado (ver sección **III.3.1**), este esquema de cifrамiento no es la excepción. Para nuestro caso, el ataque al mensaje en claro seleccionado, se puede llevar a cabo, si se seleccionan y descifran los elementos de la diagonal principal de las diferentes matrices cifradas por parte del criptoanalista. En los elementos de la diagonal principal de la matriz cifrada reside la seguridad de este algoritmo de cifrамiento. Debido a que si el criptoanalista descifra los elementos de la diagonal principal, entonces el criptoanalista tiene cierta información para poder descifrar el mesaje transmitido.

*Una medida de protección para los elementos que pertenecen a la diagonal principal* $a_{ii}$, *propuesta por el autor de este trabajo de tesis, consiste en cifrar los elementos* $a_{ii}$, *por medio de una función de un sólo sentido* $u()$, *y el resultado los publica en un directorio de clave pública.*

De esta manera, los elementos de la diagonal principal son secretos para cada usuario, excepto para el emisor. En este caso, la mejor forma de violar el esquema RSA realizado en forma matricial es buscar la clave de descifrado **d**. Esto formalmente puede establecerse a partir del teorema siguiente :

**Teorema 6.2** ([30], pag. 149) :

Considere el ataque al mensaje original seleccionado con su clave secreta **d**. Si existe un algoritmo de tiempo polinomial el cual calcula la clave de descifrar **d** y viola la seguridad del esquema **RSA** original, entonces, uno puede buscar los elementos de la principal diagonal, así como los elementos de la matriz triangular superior y violar el esquema de ciframiento **RSA** realizado en forma matricial. A la inversa, si existe un algoritmo de tiempo polinomial el cual calcula **d** a partir de las ecuaciones actualizadas de acuerdo al teorema **6.1** y conociendo $0 \equiv a_{ii}^{ed} - a_{ii} \pmod{R}$.

La seguridad de este esquema bajo el ataque al mensaje original seleccionado puede resumirse con el teorema siguiente.

**Teorema 6.3 :**

*Para el caso de un ataque al mensaje original seleccionado, la seguridad del esquema de ciframiento* **RSA** *realizado en forma matricial es cuando* $f(.)$ *es una función de una sóla vía, además* $f(.)$ *satisface la propiedad siguiente :*

**Propiedad 6.1**

*Si se define* $r \equiv \sum_{i=1}^{n} a_{ii} \circledast a_{ii+1} \left[\bmod R\right]$, *entonces, no es posible calcular* $f(r+I \bmod R)$, *conociendo* $f(r+i \bmod R)$ *para* $0 \leq i < I$, *donde* $\circledast$ *es cualquier función suma ó resta modulo* **R**.

*La seguridad de la función* $f(.)$, *consiste en la dificultad y lo dilatado de calcular* **r** *a partir de* $f(.)^{-1}$ , *debido a que requiere de una gran capacidad de memoria, además de mucho tiempo para calcularlo.*

## VI.7. Comparación de Algoritmos de ciframiento

La principal aportación de este trabajo de tesis, es la combinación de dos procesos de cifrado que permiten conseguir **PRIVACIDAD** y **AUTENTICIDAD** con claves independientes una de otra, de tal modo que el criptograma obtenido en un primer cifrado es utilizado como si fuese mensaje original para un segundo cifrado.

La combinación de dos funciones básicas de cifrado, es decir, un doble cifrado, es con el propósito de que el criptograma resultante sea criptográficamente más fuerte y resistente a las vulneraciones o ataques de los criptoanalistas, que cualquiera de los cifrados componentes básicos.

Formalmente podemos decir que se representa como $C_K$ al mensaje cifrado realizado con la clave $K_1$, el doble cifrado se puede expresar del siguiente modo :

$$C = C_{k_2}\left[ C_{K_1}(M) \right] = C_{K_2}(C')$$

$$C' = C_{K_1}(M)$$

donde C' es el criptograma obtenido mediante el cifrado simple (primer cifrado) del mensaje original, **M**, con la clave, $K_1$, y **C** es el criptograma obtenido al cifrar (segundo cifrado) con la clave, $K_2$, el criptograma C'.

La tabla 6.2 muestra una comparación entre los diversos algoritmos de ciframiento investigados y simulados en este trabajo de tesis.

El método 1, denominado *Permutación de muestras en el tiempo* [6], se realiza empleando el esquema RSA [15], así como también la adición de un sistema de comunicación entre diversos usuarios, propuesto por Hellman-Diffie [20], como se muestra en la TABLA 6.2. La adición de un sistema de comunicación, permite la **autentificación** del emisor del mensaje.

Este método de ciframiento no es recomendable ya que su principal inconveniente, es que requiere de un tamaño de memoria **R** variable. El tamaño de memoria **R** depende de los valores seleccionados **p** y **q** (R = pq).

| | METODO 1 | METODO 2 | METODO 3 | METODO 4 | METODO 5 |
|---|---|---|---|---|---|
| ALGORITMO | RSA | RSA | ELGAMAL, T. | RSA-WILLIANS-RABIN | RSA-MATRICIAL |
| | CIFRAMIENTO | CIFRAMIENTO | CIFRAMIENTO | CIFRAMIENTO | CIFRAMIENTO |
| | $C \equiv M^e \pmod R$ | $C \equiv M^e \pmod R$ | $C_1 = a^k \pmod p$<br>$C_2 = KM \pmod p$ | $M \equiv K^2 \bmod R$ | $a_{11} \equiv c_{n-1}^e a_{11}^{n-1} + c_{n-2}^e a_{11}^{n-2} + \ldots + c_0^e$<br>$a_{22} \equiv c_{n-1}^e a_{22}^{n-1} + c_{n-2}^e a_{22}^{n-2} + \ldots + c_0^e$<br>$\vdots$<br>$a_{nn} \equiv c_{n-1}^e a_{nn}^{n-1} + c_{n-2}^e a_{nn}^{n-2} + \ldots + c_0^e$ |
| | DESCIFRAMIENTO | DESCIFRAMIENTO | DESCIFRAMIENTO | DESCIFRAMIENTO | DESCIFRAMIENTO |
| | $M \equiv C^d \pmod R$ | $M \equiv C^d \pmod R$ | $K = C_1^B \pmod p$<br>$M = \frac{C_2}{K} \pmod p$ | $x^2 \equiv K \bmod p$<br>$y^2 \equiv K \bmod q$ | $a_{11}^{mod} \equiv c_{n-1}^d a_{11}^{e(n-1)} + c_{n-2}^d a_{11}^{e(n-2)} + \ldots + c_0^d$<br>$a_{22}^{ed} \equiv c_{n-1}^d a_{22}^{e(n-1)} + c_{n-2}^d a_{22}^{e(n-2)} + \ldots + c_0^d$<br>$\vdots$<br>$a_{nn}^{ed} \equiv c_{n-1}^d a_{nn}^{e(n-1)} + c_{n-2}^d a_{nn}^{e(n-2)} + \ldots + c_0^d$ |
| SISTEMA DE COMUNICACION ENTRE DIVERSOS USUARIOS | DIRECTA<br>$k_{ij} \equiv y_i^{x_j} \pmod p$<br>INVERSA<br>$k_{ji} \equiv y_j^{x_i} \pmod p$ | DIRECTA<br>$k_{ij} \equiv y_i^{x_j} \pmod p$<br>INVERSA<br>$k_{ji} \equiv y_i^{x_j} \pmod p$ | DIRECTA<br>$WK_j \equiv X_j^e ID_j^{r1} \pmod n$<br>INVERSA<br>$WK_j \equiv X_i^e ID_i^{rj} \pmod n$ | DIRECTA<br>$K_{12} \equiv Y_2^{X_1} \pmod p$<br>INVERSA<br>$K_{21} \equiv Y_1^{X_2} \pmod p$ | DIRECTA<br>$K_{12} \equiv Y_2^{X_1} \pmod p$<br>INVERSA<br>$K_{21} \equiv Y_1^{X_2} \pmod p$ |
| COMPLEJIDAD EN EL TIEMPO | CIFRAMIENTO<br>$nA \times 2(\log_2(e))$<br>DESCIFRAMIENTO<br>$nA \times 2(\log_2(d))$ | CIFRAMIENTO<br>$(nA)(n-c)2(\log_2(e))$<br>DESCIFRAMIENTO<br>$(nA)(m-c)2(\log_2(e))$ | CIFRAMIENTO<br>$4 \log_2(p)$, en GF(p)<br>DESCIFRAMIENTO<br>$4 \log_2(p)$, en GF(p) | CIFRAMIENTO<br>$nA \times 2(\log_2(e))$<br>DESCIFRAMIENTO<br>$nA \times 2(\log_2(d))$ | CIFRAMIENTO<br>$2n \lfloor \log_2 e \rfloor + n(n-2)$<br>DESCIFRAMIENTO<br>$2n \lfloor \log_2 d \rfloor + n(n-2)$ |

Un inconveniente, para el sistema de comunicación utilizado en este método de ciframeinto, consiste en que no existe un algoritmo rápido para el cálculo de la clave común inversa, $K^{-1}_{ij}$, dado que la clave común, $k_{ij}$, debe de cumplir con la siguiente condición :

$$\gcd( k_{ij}, p-1 ) = 1.$$

Para el método 2, denominado *Ciframeinto en Amplitud,* la aportación principal es la adición de un sistema de comunicación entre diversos usuarios que permite la **autentificación** del emisor del mensaje. Este sistema de comunicación se *realiza en forma exponencial*, como se muestra en la TABLA 6.2.

La ventaja de utilizar este sistema de comunicación entre diversos usuarios es la dificultad que presenta calcular la clave común, $K_{ij}$, por parte de un criptoanalista como se muestra a continuación :

* El usuario **i** calcula su clave común, $K_{12}$, a partir de la clave pública del usuario j, que se encuentra publicada en un directorio de claves públicas, además de tomar en cuenta la expresión de $y_i$ :

$$K_{ij} \equiv y_j^{x_i} \bmod q = \left[ a \right]^{x_i} \bmod q \equiv a^{x_i x_j} \bmod q$$

Cualquier usuario que desee calcular $K_{ij}$, sólo depende de $y_i$ y de $y_j$, por lo que únicamente puede hacerlo del modo siguiente :

$$K_{ij} = y_i^{(\log_a y_j)} \bmod q$$

Consecuentemente, si **q** es un número primo algo menor que $2^b$. En este caso la exponenciación llevaría 2b multiplicaciones, mientras que tomar logaritmos con el algoritmo [25], llevaría $q^{1/2} = 2^{b/2}$ operaciones. La elección de los valores de **q** para un tamaño adecuado, hará que el número $2^{b/2}$ represente una complejidad intractable hoy día.

Como se ha expuesto, el cálculo de la clave común, $K_{ij}$, es prácticamente imposible sin el conocimiento de una determinada información, y muy fácil si se conoce.

Este método de ciframeinto es recomendable, ya que se puede implantar en tiempo real, en donde se procesa una sola muestra a la vez y por lo tanto no requiere de almacenar una cantidad **N** grande de muestras de la señal a procesar.

Un inconveniente, para el sistema de comunicación utilizado en este método de ciframiento, es que no existe un algoritmo rápido para el cálculo de la clave común inversa, $K^{-1}_{ij}$, a partir de que la clave común, $k_{ij}$, exista.

La principal aportación del método 3, denominado *Permutación de los coeficientes de la DFT* [6], utilizando el esquema de ciframiento propuesto por Elgamal, T. [26]., es la adición de un sistema de comunicación entre diversos usuarios, lo cual permite **autentificar** al emisor del mensaje. Este sistema de comunicación se basa en un *Sistema de Identificación de Información de cada Usuario* propuesto por Tanaka, O. [27], como se muestra en la TABLA 6.2.

Este método de ciframiento no se recomienda porque la calidad en el proceso de cifrado es muy pobre, es decir, existe un alto grado de Intelegibilidad. Además, de que el mensaje cifrado, **C**, ($C_1$ y $C_2$), a transmitir es el doble que el mensaje original, **M**, a transmitir como se muestra en la tabla 6.2.

Una posible sugerencia para este método es sub-dividir el ancho de banda de la señal en B bandas, y permutando cada una de estas sub-bandas, además de aplicar a cada sub-banda la DFT y permutando los coeficientes de la DFT, para que finalmente se aplique la $DFT^{-1}$ a toda la señal a transmitir.

Un inconveniente de los tres métodos anteriores es que se necesita transmitir todo el mensaje cifrado y con esto aumenta la capacidad del Canal de Comunicación. Por lo tanto se buscó primeramente un método de comprensión de señales de voz para poder transmitir pocos datos representativos de esa señal de voz, por lo cual se utilizó el método LPC.

La principal aportación del método 4, denominado *Permutación de los parámetros LPC* y que se basa en el esquema propuesto por Jayant [14], es la adición de un sistema de comunicación entre diversos usuarios realizado en *forma Matricial* al esquema de ciframiento propuesto por Rabin-RSA-Willians [34] como se muestra en la tabla 6.2.

Este método de ciframiento no es recomendable, debido a que el receptor tiene que colocar un cierto grado de redundacia al mensaje, **M**, a transmitir, es decir, con este método, el receptor debe seleccionar un mensaje de 4 mensajes posibles (ver, ecuación de desciframiento en la tabla 6.2) lo cual significa una utilización de mayor tiempo durante el proceso de cifrado.

Un inconveniente del esquema de ciframiento propuesto por Rabin-RSA-Willians, es que no existe una versión rápida del algoritmo del Teorema del Residuo Chino [29], para el cálculo de la solución de las congruencias de desciframiento, como se muestra en la tabla 6.2.

Un ventaja de la utilización de la clave común en este sistema de comunicación, es que para el cálculo de la clave común inversa $k^{-1}_{ij}$, es la matriz inversa de la clave común , $k_{ij}$, y de esta manera nos olvidamos que tanto la clave común, $k_{ij}$, como su inversa, $k^{-1}_{ij}$, cumplan la condición $gcd(k_{ij}, p-1) = 1$ que es más difícil de cumplir.

Tomando en cuenta los resultados de las diferentes simulaciones, además de considerar también las ventajas y desventajas de todos los esquemas de ciframiento, así como de los diferentes sistemas de comunicación entre diversos usuarios, descritos en el capítulo IV de este trabajo de tesis, se propone un nuevo método de ciframiento. Este esquema de ciframiento propuesto, consiste en la adaptación de un sistema de comunicación (*realizado por el autor de esta tesis*), a un esquema de ciframiento de clave pública realizado en forma matricial.

El nuevo método denominado *Manipulación de los parámetros LPC*, se basa en el método propuesto por Jayant [14], pero la manipulación de los parámetros LPC se realiza utilizando el esquema de ciframiento **RSA** [15] realizado en forma matricial [30]. Este método de ciframiento propuesto se basa en :

1.) La utilización de método de análisis y síntesis de voz LPC [12] como un sistema de compresión de voz.

Con este modelo de compresión de señales de voz únicamente se transmiten :

i.) **p** - parámetros LPC (ya sea los parametos $K_i^{(1)}$ ó los $a_i^{(1)}$), que, representan las características del i-enésimo frame.

ii.) Una bandera de *voiced-unvoice*.

iii.) Un valor de ganancia, $G_i$, el cual indica la cantidad de energía en el pitch del i-ésimo frame.

iv.) Un valor correspondiente al período del pitch de la i-enésima *trama*.

en lugar de transmitir toda la *trama* de una señal de voz.

2.) La utilización del esquema RSA realizado en forma matricial [30], es con la finalidad de lograr **PRIVACIDAD**, además de lograr una rápida evaluación tanto de las funciones de cifrado como de descifrado.

Para la evaluación de $\mathbf{A}^k = c_{n-1}\mathbf{A}^{n-1} + c_{n-2}\mathbf{A}^{n-2} + \ldots + c_0 I$ utilizando teorema de Cayley-Hamilton [24] [30], el número de operaciones tanto en el proceso de cifrado, así como también en el proceso de descifrado, se reduce notablemente.

La velocidad de este algoritmo depende tanto de la dimensión de la matriz a cifrar **A**, ( ó a descifrar). La implantación más eficiente, es el caso donde la matriz a cifrar **A**, es de orden 2x2 tanto para el proceso de ciframiento como de desciframiento.

* Una de las modificaciones a este esquema de ciframiento consiste, en que antes de colocar el mensaje, **M**, en la matriz de ciframiento, dicho mensaje, **M**, sufra una operación de pre-cifrado realizado por medio de una función de un sólo sentido, **f(.)**, la cual debe ser común para todos los usuarios.

*El empleo de una función de un sólo sentido, es con la finalidad de logar una mayor dificultad al querer recuperar el mensaje original, **M**, a transmitir por parte de un criptoanalista. La principal característica de las funciones de un sólo sentido, es su facilidad de cálculo en un sentido y la imposibilidad de hacerlo en el otro* [17].

* *Otra modificación más a este esquema de ciframiento es la utilización de los valores* $a_{ii}$, *de manera común tanto para el usuario* **i** *como para el usuario* **j**, *utilizando un sistema de comunicación entre diversos usuarios realizado en forma matricial o por el empleo del método de elevación exponencial.*

* Una vez que los usuarios **i**, e **j** calcularon las $a_{ij}$ comunes, se procede a evaluar el valor de **r**, utilizando una función **g(.)** de un sólo sentido. Esta función **g(.)** debe ser común para todos los usuarios.

3.) La adición de un sistema de comunicación entre diversos usuarios realizado en forma matricial, al esquema de ciframiento **RSA** realizado en forma matricial, con la finalidad de lograr **AUTENTICIDAD** entre diversos usuarios.

En este sistema, la matriz de clave común, $K_2$, tiene la restricción de que tiene que ser no singular para que la clave común inversa, $K_2^{-1}$, exista. Sin embargo esta restricción es mucho más fácil de cumplir comparada con la restricción de la clave común ( $gcd(k_{ij}, p-1) = 1$), $k_{ij}$, de los métodos 1 y 2.

Esto es debido a que la probabilidad de que el determinante de la clave $K_2$, sea igual a cero es demasiada pequeña (casi nula) comparada con la posibilidad de que el determinante de $K_2$ sea cualquier número diferente de cero, para una matriz $k_2$ que tiene elementos calculados a partir de otros elementos seleccionados aleatoriamente.

## VI.8 COMPARACION DE RESULTADOS DE LOS DIFERENTES ESQUEMAS DE CIFRAMIENTO.

### VI.8.1 Inteligibilidad residual.

El término inteligibilidad residual se refiere al grado de reconocimiento del mensaje de voz. la inteligibilidad residual es una medida subjetiva que puede variar de persona a persona. la inteligibilidad residual aumenta y es de poco valor su calificación, si el calificador de ésta conoce el mensaje original. La evaluación de la inteligibilidad residual consitió de dos pruebas, la primera fue reconocer el contenido del mensaje y la segunda reconocer a la persona que hablaba. Nosotros para evaluarla en nuestros diferentes esquemas de cifrамiento, solicitamos a distintas personas que nos hicieran favor de escuchar los diferentes criptogramas, de lo que resulto :

Mayor Inteligibilidad residual ↓

- Esquema de cifrамiento Manipulación - LPC -
- Esquema de cifrамiento Permutación - LPC -
- Esquema de cifrамiento Amplitud.
- Esquema de cifrамiento Tiempo.
- Esquema de cifrамiento Frecuencia.

# CONCLUSIONES

El usuario o responsable de un DSC, está sujeto a una serie de circunstancias críticas que pueden afectar gravemente a la seguridad de la información que se procesa en el DSC, y se transmite por el Canal de Comunicación. Como principales puntos de ataque en un DSC se encuentran : 1.) El transmisor y el receptor, y 2.) El Canal de Comunicación (por ejemplo, las líneas telefónicas de cualquier naturaleza). Respecto a los primeros, el principal peligro es el acceso indebido por parte de personas no autorizadas, que en un DSC pueden tener al alcance de la mano. Respecto a los segundos, los enlaces telefónicos pueden ser intervenidos, o pueden accidentalmente ser "escuchados", introduciendo así otro factor de inseguridad, ya que además no están bajo control del usuario. Una medida de contrarestar estos inconvenientes es la utilización de la Criptología.

El desarrollo de la Criptología, que en un principio tenía únicamente fines bélicos, actualmente, está en una etapa importante en los Sistemas de Comunicaciónes como se menciona en el capítulo I. Al ir cobrando cada vez mayor importancia el Sistema de Comunicación, los esquemas cifradores también la cobran.

Los esquemas de ciframiento de clave pública para señales de voz presentados en los capítulos **IV** y **V**, resuelven los siguientes problemas :

1.) Evitan que personas "escuchen" la conversación.
2.) Evitan que pueden intervenir las líneas telefónicas, y
3.) Permiten la distribución de claves, lo cual siempre ha sido una gran limitación en el uso de la Criptografía convencional (Criptografía de clave privada).

El esquema cifrador que proponemos, puede emplearse en el sistema telefónico, debido a que nuestro esquema cifrador presenta las siguientes ventajas :

1.) El algoritmo propuesto en el capítulo **V** tiene la ventaja de que antes de cifrar el dato, **M**, se realiza un pre-procesamiento con una función de un sólo sentido "one-way function", **f()**, dicha función es común para todos los usuarios.

Con la utilización de esta función de un sólo sentido, **f()**, el mensaje cifrado, **C**, es más resistente contra el ataque al mensaje original conocido -(ver inciso **III.3.1** de este trabajo de tesis). Dicho pre-cifrado no se realiza en ninguno de los otros métodos de ciframiento estudiados en el capítulo **IV**.

2.) Este nuevo esquema de ciframiento propuesto, se aplica para la manipulación de los parámetros LPC utilizando un Esquema de Ciframiento Asimétrico [30], en lugar de un Esquema de Ciframiento Simétrico como lo propone Jayant [14].

La utilización de este Esquema de Ciframiento Asimetrico presenta un alto grado de ciframiento (Inteligibilidad), debido a las ventajas de utilizar un Esquema de Ciframiento Asímetrico mencionadas anteriormente. Además, la utilización de la técnica LPC [7][28] presenta las siguientes ventajas importantes, como son :

únicamente se requieren transmitir :

**p** -parámetros $K_i$'s ( o parametros $a_i$'s)
Una bandera de signo para decidir si *la trama* de voz es voiced ó unvoiced.
Un valor de ganancia, **G**.
Un valor del pitch - período del pitch-, $T_p$.
por *trama*, en lugar de transmtir todo la *trama* de voz.

3.) Al Esquema de Ciframiento propuesto en el capítulo **V**, se le adicionó un sistema de comunicación entre diversos usuarios realizado en forma matricial, el cual permite *autentificar* al emisor del mensaje.

La utilización de este sistema de comunicación se debe a la facilidad de calcular la clave común inversa, $k_{ij}^{-1}$, entre varios usuarios a partir de la clave común, $k_{ij}$, de manera rápida, fácil y sencilla. Ya que es más rápido calcular la matriz inversa a partir de la matriz de la clave común, $k_{ij}$, en lugar de cumplir la condición $gcd(k_{ij},p-1) = 1$, según los métodos 1 y 2, presentados en este trabajo.

4.) Una ventaja más del Esquema de Ciframiento Propuesto, se debe a que tanto para realizar el proceso de ciframiento, como para realizar el proceso de desciframiento, se requiere de un menor número de operaciones, comparado con los métodos presentados en el capítulo **IV**, a la vez que se pueden cifrar - descifrar - varios datos a la vez, cosa que no se puede realizar por ninguno de los métodos anteriores.

El menor número de operaciones se refiere a que se requiere un menor número de multiplicaciones y adiciones para resolver la matriz de ciframiento (descifrамiento) **A**, de onden nxn, que el número de operaciones de multiplicación y adición para elevar el dato **M**, a la potencia **e** mod **R** ( $C \equiv M^e \bmod R$).

Dependiendo del orden de la matriz a cifrar, **A**, se pueden cifrar $(n^2-n)/2$ datos a la vez. Cabe mencionar que una desventaja es que si $n \geq 7$ el esquema de ciframiento no es recomendable debido a que se requiere de un gran número de operaciones de ciframiento y descifrамiento, lo cual hace que el tiempo de ciframiento (descifrамiento) se incremente considerablemente.

Finalmente en la elección del esquema cifrador deben tenerse en consideración los siguientes aspectos :

a.) De quién se debe proteger el Sistema de Comunicación ?.
b.) Que capacidad tiene el criptoanalista de accesar el mensaje cifrado ?
c.) Que alcances tiene el criptoanalista?.
d.) Que consecuencias se tienen si el criptoanalista descifra el mensaje cifrado ?.

Las perspectivas las podemos dividir en tres aspectos principales :

* Criptología Moderna.

- Buscar nuevos algoritmos criptográficos de clave pública, los cuales posean la misma o mayor dificultad al descifrar el criptograma, pero que además se realicen con un número menor de operaciones al cifrar como al descifrar.

- Se pretende que las etapas de cifrado y descifrado las realice un procesador digital de señales DSP (de las siglas en inglés), ya que este tipo de procesadores son elementos de procesamiento muy rápidos.

- Se pretende buscar algoritmos que nos permitan evaluar la funcion $C = M^e \bmod R$ y $M = C^d \bmod R$ de manera rápida, sencilla y práctica para que se permita realizar las operaciones de adición, substración, elevación a un exponente con operandos mayores a 256 bits de longitud.

- Proponer y aplicar diferentes áreas de la criptología moderna como nuevos esquemas de cifrамiento como lo son :
  Pruebas de conocimiento cero ("Zero-Knowledge").
  Firmas digitales.
  Sistemas criptográficos de clave pública basados en curvas elípticas ("Elliptic Curve Key Public Cryptosystem").

* Sistemas de comunicación entre distintos usuarios.

- Buscar nuevos métodos de manejo, distribución generación y control de claves públicas y privadas.

* Métodos de compresión de Voz.

Cuantización Vectorial.

- Se pretende emplear el esquema de compresión de señales de voz denominado "Cuantización Vectorial", para poder transmitir señales de voz a una tasa inferior de 1200 bits/seg. a través de un canal telefónico.

**Bibliografía**

1. Simmons J. G. "A Survey of Information Aunthentication" Proceeding of the IEEE, Vol.76, No.5, May 1988.

2. Carlson, B.Digital Communications System. Prentince-Hall.1987.

3. Sklar, Bernard. Digital Communications : Fundamentals and applications. Prentice - Hall. 1988.

4. Alcántara, S. R. "Apuntes sobre Análisis de señales". UNAM DEPFI 1991.

5. Saposhrov, A.M. Electroacústica. Reverté, S.A.

6. Beker, H. J. Speech Segurity Communications. London Academic. 1985.

7. Saito, Shuzo. Fundamentals of specch Signal Procecessing. Academic Press, Inc. 1985.

8. Haykin, Simon. Adaptive Filter Theory. Prentice Hall 1986.

9. Ludeman C. Lennie. Fundamental of Digital Signal Processing. Prentice-Hall 1988.

10. Brigham Oran E. The Fast Fourier Transform and its Aplications. Prentice-Hall 1989.

11. Le Roux, J., and Gueguen, C. "A Fixed Point computation of Partial Correlation Coefficients". IEEE Transactions on ASSP. June 1997.pp.257-259.

12. Papamichalis, P. Practical aproaches to speech coding. Prentice-Hall Inc. Englewood Cliffs,. 1987.

13. Markhol, John. "Linear Prediction: A Tutorial Review". Proc. IEEE, Vol 63.

14. Jayant, S. and Sambuyer,R. "Speech Encryption by manipulations of LPC Parameters ". The Bell System Technical Journal Vol. 55. No.9. November 1976.

15. Rivest, R.L., Shamir, A., and Adeleman, L.A. "A Method for Obtaining Digital Signatures and Public Key Crytosystems" Communication ACM, Vol.21, No.2.

16. Tilborg, Henk C. An Introduction to Cryptology. 1988.

17. Rajsbaum, S. y Ayala J. " Apuntes sobre Criptología ". UNAM. Inst. de Matemáticas 1993.

18. Shannon, C. " Communications Theory of Secrecy Systems ". Bell Syst. Tech J. Vol 28 1949.

19. Denning, D.E. Cryptography and Data Segurity. Addison Weley Publishing Company, Reading, Mass 1982.

20. Diffie, W.,and Hellman, M. "New Directions in Cryptography", IEEE Trans. Inf. Theory, vol IT22, Nov 1976, pp 644-654.

21. Smith, J. L. " The design of Lucifer, a Criptographic ", Device for Data Communications," IBM Research Rep RC-3326 1971.

22. National Bureau of Standards Federal Information Processing (FIPS). " Data Encryption Standard ". Publication No.46, Jan. 1977.

23. Wersh, Dominic. Codes and cryptography. Oxford. 1991.

24. Knuth, D. E. The Art of Computer Programming, Vol. 2 : Seminumerical Algorithms. Addison-Wesley, Reading, Mass.,1969.

25. Pohling, S.C., and Hellman, M.E. "An Improved Algorithm for Computing, Logarithms en GF(p) and its Cryptographic Significance". IEEE Trans. Inform. Theory, Vol. IT-24, pp. 106-111, Jan. 1978.

26. ElGamal, T. " A Public Criptosystem and Signature Scheme based on discrete Logarithms". IEEE Trans. Inform. Theory, Vol. IT-31, pp. 469-472, July 1985.

27. Tanaka, K., and Okamoto, E. Key Distribution Systema based on Identification Information. Journal on Selected Areas in Communications, Vol 7, No.4 may 1989.

28. Markel, J. D., Gray, Jr. A.H. Linear Prediction of Speech. Springer-Verlag, New York 1976.

29. Niven, I., and Zuckerman, H.S. An introduciton to the Theory of Numbers. Wiley, New York, 1972.

30. Chih-Chwen, C. and Dunhan, J. "Matrix Extension of the RSA algorithm". Advances in Crytology. Advances in Cryptology. Cryptoloy 82, pp .140-155.

31. Ayres, F. Teoría y Problemas de Matrices. Mc-Graw-Hill 1962.

32. Schoroeppel, R., Shamir, A. "A $T.S^2=O(2^n)$ Time/Space trade off for Certain Np-complete problems". MIT Lab. Computing Sci. Rep. 1976.

33. Williams, H. C. "An $M^3$ Public-Key Encryption Scheme". Advances in Cryptology. Cryptoloy 82, Vol 9, No. 2, pp. 359-368.

34. Williams, H.C. "A Modification of the RSA Public-Key Encryption Procedure. IEEE Transactions on Information Theory, Vol. IT/26, No.6. November, 1980.

35. Rodriguez Prieto, A. Protección de la Información. Editorial Paraninfo 1981.

36. Proakis G. John and Manolakis G. Dimitris. Introduction to Digital Signal Processing. Macmillan Publishing Company 1988.