# UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

## FACULTAD DE ESTUDIOS SUPERIORES "CUAUTITLÁN"

REDES DE COMPUTADORAS

# "TÉCNICAS CRIPTOGRÁFICAS UTILIZADAS EN LA SEGURIDAD LAN"

**T R A B A J O  D E  S E M I N A R I O**

QUE PARA OBTENER EL TITULO DE:
LICENCIADA EN INFORMÁTICA
P R E S E N T A :

**SILVIA CRUZ CASTILLO**

ASESOR : ING. MIGUEL ÁLVAREZ PASAYE

CUAUTITLÁN IZCALLI, EDO. DE MEX. 1997

VNIVERSIDAD NACIONAL
AVTNOMA DE
MEXICO

**FACULTAD DE ESTUDIOS SUPERIORES CUAUTITLAN**
**UNIDAD DE LA ADMINISTRACION ESCOLAR**
**DEPARTAMENTO DE EXAMENES PROFESIONALES**

U. N. A. M.
FACULTAD DE ESTUDIOS SUPERIORES CUAUTITLAN

DEPARTAMENTO DE
EXAMENES PROFESIONALES

**DR. JAIME KELLER TORRES**
**DIRECTOR DE LA FES-CUAUTITLAN**
**P R E S E N T E .**

**AT'N: ING. RAFAEL RODRIGUEZ CEBALLOS**
**Jefe del Departamento de Exámenes**
**Profesionales de la FES-C.**

**Con base en el art. 51 del Reglamento de Exámenes Profesionales de la FES-Cuautitlán, nos permitimos comunicar a usted que revisamos el Trabajo de Seminario:**

Redes de cComputadoras: Técnicas Criptográficas utilizadas en la Seguridad LAN.

**que presenta la pasante:** Silvia Cruz Castillo
**con número de cuenta:** 8805114-3 **para obtener el Título de:**
Licenciada en Informática.

**Considerando que dicho trabajo reúne los requisitos necesarios para ser discutido en el EXAMEN PROFESIONAL correspondiente, otorgamos nuestro VISTO BUENO.**

**A T E N T A M E N T E .**
**"POR MI RAZA HABLARA EL ESPIRITU"**
**Cuautitlán Izcalli, Edo. de México, a** 13 **de** Octubre **de 19** 97

| **MODULO:** | **PROFESOR:** | **FIRMA:** |
|---|---|---|
| II | Ing. Miguel Álvarez Rosaya | |
| III | M. en I. Gloria Ponce Venegas | |
| III | Ing. Moisés Hernández Duarte | |

**DEP/VOBOSEM**

# AGRADECIMIENTOS

**A mis padres:**

**Elena Castillo Cruz**
**Lorenzo Cruz Morales**

**Por todo el amor, apoyo y cariño que me ofrecieron incondicionalmente, durante mi vida y mi formación profesional.**

**Gracias, espero nunca defraudarlos.**

**Los quiero mucho:**

**Silvia C.C.**

# AGRADECIMIENTOS


A mis hermano(as):

Ma. Elena Cruz Castillo
Ma. Rosario Cruz Castillo
Maricela Cruz Castillo
Lorenzo Cruz Castillo
Pedro Cruz Castillo
J.Luis Cruz Castillo
Gelbis Cruz Castillo

Por que se que no ha sido fácil convivir con alguién como yo, y que en su momento también padecieron mi mal carácter pero apesar de ello siempre recibí su apoyo.

Gracias!

Silvia C.C.


# AGRADECIMIENTOS

A mis maestros:

Por que en cada palabra, expresión y aciertos, esta uno y cada uno de mis profesores y esto no es sino la muestra que dejaron en mí.

Al Ing. Miguel Álvarez Pasaye:

Por su apoyo, paciencia y dirección en la elaboración de este trabajo.

Al Ing. F. Javier Contreras Torres:

Gracias por la paciencia, cariño y comprensión que me has brindado siempre y por estar conmigo en todo momento.

A la UNAM:

Gracias por la estancia dentro de sus aulas todo este tiempo y así como a la FES-Cuautitlán, por formarme como persona y profesionista.

A mis amigos:

Por que incontables, todos dejaron algo o un mucho de bueno en mí, espero aprovecharlo al máximo y tenerlos presentes siempre en mí.

**Gracias!**

# ÍNDICE

# INTRODUCCIÓN

Con el desarrollo de éste trabajo pretendo cubrir un objetivo que se me planteó hace más de un año. Debido a una serie de razones de índole profesional, fue necesario estudiar el problema de la seguridad de la información.

La utilización creciente de redes de computadoras y las tecnologías de computación han hecho posible la "presencia" de las computadoras y el acceso a ellas por todo tipo de personas.

Debido a esto, existen ahora mucho más puntos vulnerables en los sistemas. El administrador ya no tiene tanto control sobre los que sucede y tampoco los usuarios tienen siempre tanta conciencia de lo que están haciendo. Incluso, es muy probable encontrarse con usuarios mal intencionados que aprovecharán cualquier resquicio en la seguridad del sistema para obtener algún beneficio o causar algún daño.

Como en la gran mayoría de los problemas, la mejor solución es prevenir los incidentes de seguridad y no permitir que sucedan. Como siempre, la mejor manera de lograr éste objetivo es mediante la aplicación de técnicas adecuadas y la educación. Lo ideal es inculcar a los usuarios de las computadoras desde sus "inicios" los conceptos básicos de seguridad.

De esta manera se logran varios objetivos :

1.- Los usuarios adquieren conciencia de la importancia de la seguridad.

2.- Al considerar la seguridad como algo "natural" al computo, los usuarios tienen más facilidad para aceptar y aplicar las medidas de seguridad sugeridas, y de hecho por ellos mismos sin esperar a que el administrador las imponga o las proponga.

3.- Los usuarios tendrán mayor conocimiento sobre las técnicas criptográficas que pueden aplicar por ellos mismos, para incrementar la seguridad del sistema y su productividad en el mismo.

4.- El conocimiento de los usuarios propicia un incremento substancial en la seguridad del sistema, por su labor conjuntamente con la del administrador, produce una disminución considerable en los puntos vulnerables del mismo.

Con estas razones fundamentales y otras de tipo personal, nació la idea de difundir las Técnicas de Criptografía.

El contenido de este Trabajo de Desarrollo está estructurado en cuatro capítulos que tratan :

CAPITULO 1 Introducción a las Redes de Área Local.

CAPITULO 2 Introducción a la Criptografía.

CAPITULO 3 Seguridad en comunicación y archivos utilizando criptografía.

CAPITULO 4 Caso Práctico.

# CAPÍTULO 1

# INTRODUCCIÓN A LAS REDES DE ÁREA LOCAL (LAN)

# 1 INTRODUCCIÓN A LAS REDES DE ÁREA LOCAL ( LAN)

En los últimos veinte años, la industria de comunicaciones ha centrado su atención en sistemas que transportan datos a largas distancias. Las redes locales (LAN - Local Area Networks), constituyen un campo relativamente nuevo. La Tecnología en que se basan empezó a adquirir interés a mediados de los setenta, y es en la actualidad uno de los sectores de más rápido crecimiento dentro de la industria de comunicaciones de datos.

Los principales motivos son :

- Proporcionar a los usuarios acceso a varios ordenadores.
- Compartir Archivos
- Compartir Recursos Físicos
- Compartir el acceso a redes de área extensa
- Proporcionar correo electrónico y otros servicios de comunicaciones en sistemas de oficinas.
- Seguridad de los datos

La expansión de la industria de las redes locales durante los últimos seis años ha sido explosivo.

La idea básica de una red local es facilitar el acceso a todos las terminales de la oficina, entre los que encuentra no sólo los ordenadores(personales, miniordenadores, o grandes equipos), sino también otros dispositivos presentes en casi todas las oficinas :impresoras, trazadores gráficos y , cada vez más, archivos electrónicos y bases de datos. Una Red Local se configura de modo que proporcione los canales y protocolos de comunicación necesarios para el intercambio entre servidores y terminales. En este capítulo se ofrece una idea general de las topologías y protocolos de Red Local más comunes. También se estudian algunos de los nacientes estándares para red local emitidos por el IEEE .802, los comités ISO , y la importancia de la Seguridad en las redes( Mediante las técnicas Criptográficas).

## 1.1 PRINCIPALES ATRIBUTOS DE UNA RED LOCAL

Las conexiones entre las estaciones de trabajo suelen tener longitudes comprendidas entre algunos cientos de metros y varios kilómetros.

Una red local transmite datos entre estaciones de usuarios y servidores (También pueden transferir imagen, voz y vídeo)

La capacidad de transmisión de una red local suele ser mayor que la de una red extensa (WAN)[1]; las velocidades de transmisión suelen estar comprendidas entre 1 Mbit por segundo y 20 Mbits por segundo.

El canal de una red local suele ser propiedad de la misma organización que utiliza la red. Las compañías Telefónicas hoy en día proporcionan a los usuarios de redes locales una variedad de opciones como :

Internet[2] e Intranet[3] entre otras.

La tasa de errores de una red local suele ser considerablemente menor que la del canal telefónico orientado a redes extensas. Sin embargo con la utilización creciente de las redes de computadoras y las tecnologías de comunicación han hecho posible la "omnipresencia" de las computadoras y el acceso a ellas por todo tipo de personas. Existen ahora muchos más puntos vulnerables en los sistemas .

El administrador ya no tiene tanto control sobre lo que sucede y tampoco los usuarios tiene siempre tanta conciencia de lo que están haciendo. Incluso, es muy probable encontrarse con usuarios malintencionados que aprovecharán cualquier resquicio en la seguridad del Sistema para obtener algún beneficio o causar algún daño. Como en la gran mayoría de los

[1] WAN (Wide Area Network ;Red de Área Amplia).Conjunto de computadoras y otros dispositivos comunicados entre sí colocados dentro de un espacio geográfico de amplias dimensiones

[2] Internet : La llamada " Red de redes" creada de la unión de muchas redes TCP/IP a nivel internacional y cuyos antecedentes están en la ARPANet . Conexión entre dos o más redes.

[3] Intranet_ : Red de uso privado que emplea los mismos estándares y herramientas de Internet. Es uno de los segmentos del mercado de computación que más impulso está cobrando.

problemas, la mejor solución es prevenir los incidentes de seguridad y no permitir que sucedan.

### 1.1.1 REDES DE BANDA ANCHA Y REDES DE BANDA BASE

En las redes locales existen sistemas de banda ancha y de banda base, las redes de banda ancha se caracterizan por operar con tecnologías analógicas : utilizan un módem para enviar en el medio de tranamisión señales portadoras, que son después modificadas (moduladas) por una señal digital.

Debido a su naturaleza analógica, las redes de banda ancha suelen estar multiplexadas por división en frecuencia (FDM), lo cual permite transportar múltiples portadoras y subcanales por un mismo camino. El ancho de banda es un indicativo de la cantidad de información que puede ser transmitida por un medio.

La denominación de banda ancha se debe a que trabajan en una banda de frecuencia de radio de alta frecuencia (entre 10 y 400 Mhz) .No todas las redes analógicas trabajan en frecuencias tan elevadas. Las que no cumplan esta característica no se consideran de banda ancha.

Las redes de banda base utilizan tecnología digital. El canal que recibe esta señal se comporta como un mecanismo de transporte a través del cual se propagan estos impulsos digitales. El acceso es mediante multiplexado por división en el tiempo (TDM). Las redes locales de más de 100 estaciones suelen utilizar técnicas de banda ancha.

El sistema de banda ancha puede transmitir datos, voz e imágenes.

Todo canal de transmisión tiene su ancho de banda característico, el cual debería ser bastante mayor que la banda de frecuencias de las señales a pasar por él.

## 1.2 ESTÁNDARES DE RED LOCAL DEL IEEE (THE INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERING)

En 1980, en un intento de introducir una estandarización en las redes de área local, el instituto de Ingenieros Eléctricos y Electrónicos (IEEE) ha establecido seis subcomites.

Todos los grupos reciben la denominación colectiva de comités de Normalización de redes locales IEEE 802 :

802.1 Gestión y Niveles Superiores

802.2 Control Lógico del Enlace (LLC)

802.3 (CSMA/CD)[4] (Método de acceso y especificación del nivel físico)

802.4 Token Bus (Paso de testigo en bus)

802.5 Token Ring (Paso de testigo en anillo)

802.6 Redes Metropolitanas (MAN)[5]

La norma 802.1 da una introducción al conjunto de normas y define las primitivas de Interface.

La norma 802.2, describe la parte superior de la capa de enlace (LLC)

Las normas 802.3, 802.4 y 802.5 , para redes de tipo Lan, es decir, las normas CSMA/CD, Paso de testigo en bus y paso de testigo en anillo respectivamente cada norma cubre los protocolos[6] de la capa física y la subcapa MAC[7] [ 3 ]

[4] CSMA/CD : Carrier Sensing Multiple Access / Colition Detection - Acceso Múltiple de sentido de transporte / Detección de Colisiones.
[5] MAN : Redes de Área Metropolitana
[6] Protocolo : Reglas que establecen la comunicación de un host a host (nodo a nodo).
[7] MAC : Medium Access Control - Control de acceso al medio.

**Las normas IEEE 802 han sido adoptadas por :**

**ANSI (Instituto Nacional Americano de Normalización) , como una norma Nacional Americana ; NBS (Oficina Nacional de Normas) , como una norma gubernamental y ISO (Organización Internacional de Normas) , como una norma internacional (conocida como ISO 8802).**

## 1.3 LAS NORMAS ISO[8] 8802

El modelo OSI[9] (en castellano este modelo recibe las siglas ISA - Interconexión de Sistemas Abiertos). Este estándar es apoyado por los principales organismos de normalización, administraciones de telecomunicación y empresas.

El modelo OSI tiene siete capas (ver fig. 1). Los principios aplicados para el establecimiento de siete capas fueron los siguientes :

- Una capa se creará en situaciones en donde se necesita un nivel diferente de abstracción.
- Cada capa deberá efectuar una función bien definida.
- La función que realizará cada capa deberá seleccionarse con la intención de definir protocolos normalizados internacionalmente.
- Los límites de las capas deberán seleccionarse tomando en cuenta la minimización del flujo de información a través de las interfaces.
- El número de capas deberá ser los suficientemente grande para que funciones diferentes no tengan que ponerse juntas en la misma capa y , por otra parte, también deberá ser lo suficientemente pequeño para que su arquitectura no llegue a ser difícil de manejar.

| | |
|---|---|
| NIVEL DE APLICACIÓN | 7 |
| NIVEL DE PRESENTACIÓN | 6 |
| NIVEL DE SESIÓN | 5 |
| NIVEL DE TRANSPORTE | 4 |
| NIVEL DE RED | 3 |
| NIVEL DE ENLACE | 2 |
| NIVEL FÍSICO | 1 |

**FIGURA 1** Estructura del modelo de referencia ISA (OSI, en inglés).

[8] ISO : International Standard Organization. Esta organización ha definido los protocolos de comunicaciones conocidos como ISO.
[9] OSI : Open Systems Interconnect - Interconexión de Sistemas Abiertos (ISA). Conjunto de protocolos normalizados por la organización Internacional para la normalización, ISO.

**Nivel Físico :**

Las funciones incluidas dentro de este estrato se encargan de activar , mantener y desactivar un circuito físico entre un ETD[10] Y ECD[11]. Para el nivel físico se han publicado bastantes estándares. Entre otros el RS-232-C (Interfaz entre equipos terminales de datos y equipos de comunicación de datos mediante intercambio de datos binarios en serie) y el V-24 (Lista de definiciones para los circuitos de intercambio entre equipos terminales de datos y equipos de terminación del circuito de datos(ETCD)).

**Nivel de Enlace :**

Es el responsable de la transferencia de datos por el canal. Proporciona a los datos la sincronización necesaria para delimitar el flujo de bits del nivel físico. También garantiza la identidad de los bits, encargándose de que los datos lleguen sin errores al ETD receptor. Se ocupa de controlar el flujo de datos para impedir que el ETD se desborde en ningún momento. Una de sus funciones más importantes consiste en detectar errores en la transmisión y en recuperar, por distintos mecanismos, los datos perdidos, duplicadas o erróneas.

Por lo tanto asegura la compatibilidad de los protocolos del nivel de enlace que proporcionan una transmisión libre de errores, así como el acceso al medio de comunicaciones.

Entre sus funciones incluyen:

- Establecimiento y liberación del Enlace.
- División en paquetes y sincronización, incluyendo los medios para distinguir los datos de los indicadores.
- Control de secuencia.
- Detección de los errores de transmisión.
- Retransmisión y otras formas de corrección de los errores de transmisión.

[10] ETD : Equipo Terminal de Datos.
[11] ECD : Equipo de Conmutación de Datos.

- Control del flujo.
- Identificación e intercambio de parámetros.
- Supervisión de la conexión física.
- Gestión del nivel de enlace.
- Control de acceso para las redes de área local.

Entre los servicios que proporciona el nivel de red incluyen :

- Transmisión de los datos en las unidades de servicio del nivel de enlace.
- Provisión de un identificador de extremo del enlace de datos.
- Control de secuencia.
- Notificación de la transmisión de errores.
- Control de flujo.
- Indicación de la calidad de servicio

**Nivel de Red :**

Define la interfaz entre el ETD de usuario y a la Red de conmutación de paquetes, además de la interfaz de un ETD con otro a través de esta Red.

Específica también las operaciones de encaminamiento por la red, la comunicación entre distintas redes. Es un nivel muy detallado, y con una amplia variedad de funciones. En este nivel está incluida las especificaciones X.25.

Entre las funciones de nivel de red se encuentran :

- Seleccionar las rutas primarias y alternativas para establecer los circuitos virtuales correspondiente.
- Seleccionar las conexiones con la Red direccionando nodos intermedios.
- Multiplexar las conexiones de red.
- Construir bloques de datos y segmentos y reconstrucción en su destino.

- Detectar y corregir errores.
- Control de flujo y secuencia.
- Garantizar una transmisión satisfactoria de los datos.
- Inicialización de las conexiones de Red.
- Selección de Servicios.
- Gestión del nivel de enlace y comunicaciones con los niveles adyacentes.
- Establecimiento de conexiones entre redes (internetworking).

Entre los servicios que proporciona el nivel de Red se encuentran :

- Provisión de direcciones de Red.
- Provisión de conexiones de Red.
- Identificación de los puntos terminales de la Red.
- Transferencia de unidades de datos de servicio de Red.

**Nivel de Transporte :**

Proporciona la interfaz entre la Red de comunicación de datos y los tres niveles superiores. Es el nivel que permite al usuario elegir entre diversas opciones de calidad dentro de una misma Red ( es decir, dentro del nivel de red). Está diseñado para mantener al usuario al margen de algunos aspectos físicos y funcionales de la red de paquetes. Se encarga además de la facturación entre dos extremos.

Las funciones de la capa de transporte incluyen :

- Establecer una conexión de transporte sin prestar atención a los nodos intermedios.
- Transmisión de datos, detección de errores y retransmisión (extremo a extremo) cuando sea necesario.
- Liberación de la conexión de transporte.
- Gestión del nivel de transporte y comunicación con las capas adyacentes.
- Asignación de direcciones a los usuarios (los usuarios pueden cambiar de rutas)

- Control de la calidad de servicio.

Los servicios que presta a la capa de sesión incluyen :

- Transmisión de datos.
- Establecimiento y liberación de las conexiones de transporte.
  - Conexiones con una tasa de errores residual aceptables (Errores no detectados en el nivel Red o detectados pero no corregidos).
  - Conexiones con una tasa de errores residuales aceptable (Con una tasa de errores de señalización inaceptable)
  - Conexión con una tasa de errores residual inaceptable para el usuario del servicio de transporte.

**Nivel de Sesión :**

Funciona como interfaz del usuario con el nivel de transporte. Ofrece un mecanismo organizado de intercambio de datos entre usuarios. Cada usuario puede seleccionar el tipo de control y de sincronización que desea de la red.

Las funciones de la capa de sesión incluyen :

- Asignación de sesiones con conexiones de transporte.
- Control de flujo para la sesión.
- Intercambio de datos entre tareas.
- Apertura , terminación y restablecimiento de las conexiones de sesión.
- Gestión de la capa de sesión y comunicación con las capas adyacentes.
- Control del diálogo (quién, cuándo, duración, half[12] o full-duplex[13])
- Recuperación frente a problemas de comunicación durante una sesión sin pérdida de datos.

[12] Half - Duplex ( Semidúplex) : Comunicación bidireccional, donde no hay cruce de información en la línea. La información circula en un sentido o en otro, pero no en los dos a la vez.
[13] Full- Dúplex ( Dúplex) : La comunicación se puede producir en ambos sentidos simultáneamente.

Entre los servicios que proporciona a la capa de presentación se incluyen :

- Establecimiento y terminación de la sesión.
- Realización de las transferencias de datos.
- Control del diálogo.
- Sincronización de la conexión de la sesión.
- Notificación de los errores irrecuperables.

**Nivel de Presentación :**

Asigna una sintaxis a los datos, es decir, determina la forma de presentación de los datos según este modelo, sin preocuparse de su significado o semántica. (Aceptar tipos de datos - Caracteres, enteros, etc.- procedentes del nivel de Aplicación y negociar con el nivel homólogo del otro extremo la sintaxis escogidas(ASCII)[14]). El nivel de presentación es capaz de crear visualizaciones de terminales virtuales.

Las funciones de la capa de presentación incluyen :

- Peticiones de apertura , cierre e implementación de una sesión.
- Intercambio de datos.
- Coordinación de los perfiles sintácticas y de presentación.
- Traducción sintáctica de juegos de caracteres, cadenas de texto, formatos de presentación, gráficos y tipos de datos.
- Traducción del perfil de presentación.
- Cifrar[15] y Descifrar[16] (Técnicas de Criptografía[17] (Encriptamiento)), los datos , si es necesario.
- Compresión de los datos , si es necesario.

[14] ASCII : American Standard Code for Information Interchange - Código Americano Estándar para intercambio de información.
[15] Cifrado (Encriptación): Se llama a una transformación del texto original (Criptograma→ Documento cifrado).
[16] Descifrado (Desencriptación): Proceso que permite recuperar el texto original apartir del texto cifrado.
[17] Criptografía :" Arte de enviar mensajes en clave secreta", "Ciencia que estudia los procesos de cifrado y descifrado de los mensajes, así como el análisis de los criptogramas para descubrir la clave y texto original"

Entre los servicios que proporciona la capa de aplicación se encuentran :

- Formateo de los datos.
- Selección de la sintaxis.
- Traducción de la sintaxis.
- Selección del perfil de presentación.
- Encriptamiento de los datos.

**Nivel de Aplicación :**

Se encarga de entender al proceso de aplicación del usuario final. A diferencia del nivel de presentación, este nivel tiene en cuenta la semántica de los datos. Contiene varios elementos de servicio capaces de gestionar procesos de aplicación tales como la gestión de trabajos, el intercambio de datos financieros, sentencia send/receive (enviar - recibir) de distintos lenguajes de programación ; y el intercambio de datos comerciales, además este nivel maneja los conceptos de terminal virtual y archivo virtual.

Comprobación de passwords, base de datos distribuidos, transferencia de documentos o archivos, conexión al sistema y comprobación de acceso a archivos.

La capa de aplicación puede proporcionar entre otros los siguientes servicios a los procesos de aplicación :

- Identificación de las partes implicadas en la comunicación y determinación de su estado de disponibilidad.
- Comprobaciones de autorización y validez.
- Asignación de costos.
- Agrupación de los recursos disponibles.
- Servicios de admisión.
- Aplicaciones de sincronización.
- Corrección de errores.

- Selección del diálogo.
- Comprobación de la identidad de los datos.
- Peticiones de acceso a archivos y transferencia de archivos.
- Carga de programas a través de líneas de comunicaciones.
- Procedimientos Gráficos.
- Acciones sobre bases de datos, consultas, inserciones y eliminaciones.
- Servicios de terminales virtuales.
- Control y entrada remota de trabajos.
- Correo electrónico.

El modelo de referencia de 7 niveles del OSI aplicado a dos sistemas interconectados ; ilustrando las funciones básicas y los estándares de ISO para cada capa (ver fig. 2).

| | | | |
|---|---|---|---|
| 7 NIVEL DE APLICACIÓN | PROTOCOLO PARA APLICACIONES ESPECIFICAS | 7 NIVEL DE APLICACIÓN | CCITT / ISO<br>CCITT X400<br>ISO 8571 (FTAM)<br>ISO 8650 (CASE) |
| 6 NIVEL DE PRESENTACIÓN | Mensajes, traducción de formatos, códigos y lenguajes ; ENCRIPTACIÓN. | 6 NIVEL DE PRESENTACIÓN | ISO 8823<br>ISO 8823 |
| 5 NIVEL DE SESIÓN | Diálogo extremo a extremo entre procesadores, conexiones 1 a 1 (sin multiplexación) funciones contables y fact. | 5 NIVEL DE SESIÓN | ISO 8327 |
| 4 NIVEL DE TRANSPORTE | Transporte seguro de mensajes extremo a extremo. Control de flujo y multiplexación. Secuenciación de mensajes. | 4 NIVEL DE TRANSPORTE | ISO 8073<br>CLASE 0 a CLASE 4 |
| 3 NIVEL DE RED | Conmutación y direccionamiento de mensajes. Ordenación de los paquetes. | 3 NIVEL DE RED | ISO 8473<br>Nivel de paquete de la X25 del CCITT<br>(ISO 8200 |
| 2 NIVEL DE ENLACE | Envío y recepción de paquetes.<br>Detección y corrección de errores.<br>Acceso a los medios. | 2 NIVEL DE ENLACE | ISO 8802/2<br>(IEEE 802.2 LLC)<br><br>ISO (HDLC)<br>X 25 LAP |
| 1 NIVEL FÍSICO | Transmisión y recepción de bits.<br>Compatibilidad eléctrica, mecánica y funcional | 1 NIVEL FÍSICO | ISO 8802/3 (IEEE 802.3)<br>ISO 8802/4 (IEEE 802.4)<br>ISO 8802/5 (IEEE 802.5) |
| | MODO DE INTERCONEXIÓN 0 | | |

**FIGURA 2** Modelo de referencia de 7 niveles del OSI.

## 1.3.1 RECOMENDACIONES ISO RELATIVAS A LA SEGURIDAD :

El Organismo Internacional de Normalización (ISO) recomienda establecer el cifrado en el nivel de presentación de la configuración según el modelo ISA. Estas son las razones que aduce el ISO para ello :

- Es algo comúnmente admitido que servicios de cifrado han de colocarse en un nivel superior de red, con el fin de simplificar el cifrado de extremo a extremo. El nivel de transporte es el nivel más bajo en el que existen servicios de extremo a extremo ; por tanto, el cifrado ha de realizarse en el nivel cuarto o en uno superior.

- Sin embargo, los servicios de cifrado han de encontrarse en un nivel superior al de transporte si se quiere minimizar la cantidad de programas a los que ha de confiarse el texto legible. Es decir, cuantos menos programas manejen el texto legible vulnerable, mejor. Este razonamiento nos lleva a trasladar los procesos de cifrado a un nivel superior al de transporte.

- El cifrado ha de establecerse por debajo del nivel de aplicación. ya que de lo contrario las transformaciones sintácticas sobre los datos cifrados serían bastante difíciles. Además, si en el nivel de presentación se llevan a cabo transformaciones sintácticas, éstas han de tener lugar antes de que realice el cifrado.

- Puesto que es deseable poder aplicar la protección de forma selectiva (es posible mejor que no todos los campos necesiten ser cifrados), el organismo ISO cree que donde mejor puede hacerse esta selección es en el nivel 4 de presentación o en uno superior, ya que por debajo de este nivel no existe constancia de la división en campos de la corriente de datos.

- Aunque el cifrado puede efectuarse en cualquier nivel, la protección adicional que obtienen los datos de usuarios puede no compensar la sobrecarga de trabajo que supone el cifrado.

Los servicios de seguridad se asignarán a nivel OSI particulares, donde pueden ser implementados si se desea. Los niveles más altos podrán hacer uso de los servicios de seguridad si estos se implementan en niveles más bajos.[ 11 ]

El objetivo del estándar OSI es asegurar que un sistema de seguridad que utilice los protocolos de comunicaciones OSI no sea menos seguro que un servidor o una terminal.

Los tipos de servicios de seguridad que pueden requerir son (ver fig. 3):

- Confidencialidad : ( Protección de los datos transmitidos contra su revelación a personas no autorizadas).
- Integridad : (Seguridad de que los datos recibidos no contienen, duplicados, insecciones , modificaciones o sustituciones).
- Verificación de la identidad de pareja : ( La identificación de entidades remotas , eliminando la posibilidad de que se repitan secuencias de verificación previas).
- Control de acceso : (Limitaciones y control del acceso a ordenadores principales mediante enlaces de comunicaciones).
- Seguridad en el flujo de tráfico : (Modelos de enmascaramiento u ocultamiento de tráfico ).
- No rechazo (Seguridad de que el receptor de los datos no puede negar que los ha recibido , ni el remitente y que los ha enviado).
- Verificación del origen de los datos : (Seguridad de que la fuente de los datos es la requerida).

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Verificación de identidad de pareja | | | o | o | | o | |
| Control de acceso | | | o | o | | o | o |
| Confidencialidad | o | | o | o | | o | |
| Seguridad del flujo de tráfico | o | | o | | | | o |
| Integridad | | | o | o | | o | |
| Verificación del origen de los datos | | | o | o | | o | |
| No rechazo | | | | | | o | |

**FIGURA 3** Asignación de servicios de seguridad a niveles OSI.

## 1.4 TOPOLOGÍAS Y PROTOCOLOS DE REDES LOCALES

La forma en que están conectados los nodos es lo que se conoce como topología de una red.

En redes locales existen tres tipos básicos de topologías a saber :

- Estrella
- Bus
- Anillo

**Topología en estrella :** En este tipo de conexión, el elemento central es el SERVER con sus periféricos. En la arquitectura de estrella todos los nodos[18] se juntan en un solo punto conocido como nodo central o eje (ver fig. 4). El nodo central puede ser un dispositivo activo o pasivo. En este caso el nodo central se encarga de establecer todas las rutas de los mensajes dentro de la red o dicho de otra forma, el nodo central se mantiene preguntando constantemente a cada estación de trabajo (Host) mediante comunicación exclusiva y por turno, si se desea transmitir información ; de ser afirmativo, el nodo central la atiende y al terminar prosigue su rutina sobre los siguientes nodos. Esta rutina es permanente.

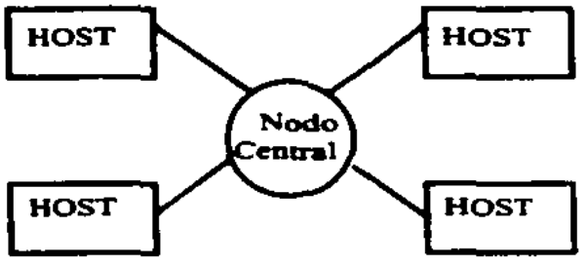



**FIGURA 4** Topología en estrella.

[18] Nodos : En general, se le llama nodo a cualquier ordenador conectado a una red.

**Topología de Bus :** Esta conexión se considera que es la más sencilla de todas, donde los nodos incluyendo al SERVER están enlazadas por un mismo cable (coaxial o par trenzado), y la información viaja en ambos sentidos, por lo que es necesario prevenir las colisiones (ver fig. 5).

Para ello el protocolo apropiado es CSMA/CD (Carrier Sense Multiple Acces / Collisión Detection).

Con este protocolo la RED transmite y espera a que se confirme que la información fue recibida correctamente, de otra forma, detecta la posible colisión y espera un tiempo apropiado para que el canal se encuentre desocupado y así poder retransmitir la información nuevamente.

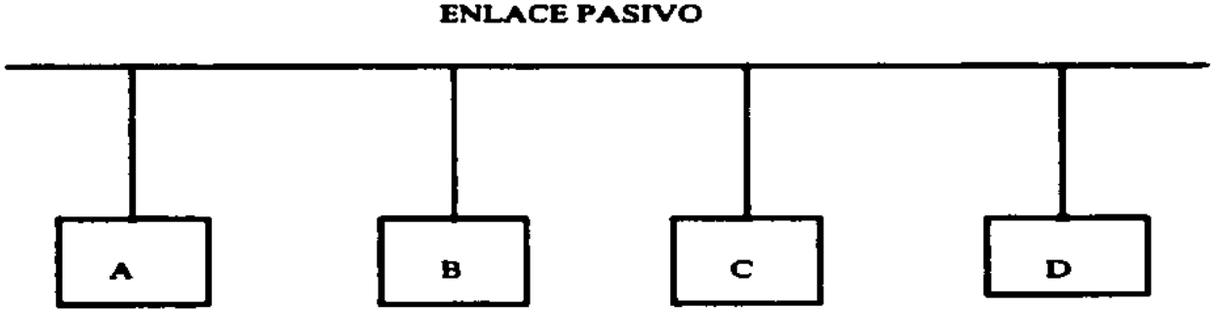



**FIGURA 5** Topología de bus.

**Topología de Anillo :** En esta conexión la información viaja ordenadamente con un solo sentido a través de un solo cable y describiendo un ángulo de 360° en cuyo anillo imaginario están conectadas en serie las estaciones de trabajo y el SERVER (ver fig.6).

Una señal llamada TOKEN (Receptáculo a modo de estafeta), va calculando por la RED y pasando por cada estación, en donde tenemos por ejemplo, que si la primera resulto ser la solicitante con previa identificación entrega la información, en caso contrario la deposita en un "sobre cerrado", para que esta a su vez la envíe a la siguiente estación, llevando consigna de entregarla hasta identificar al solicitante.

un "sobre cerrado", para que esta a su vez la envíe a la siguiente estación, llevando consigna de entregarla hasta identificar al solicitante.

Sin embargo con una topología en anillo los mensajes podrían permanecer en circulación indefinidamente si no son absorbidos por alguna de las estaciones. Por lo tanto podemos decir que la topología en anillo trabaja las señales cerrando ciclos "Circulares" ; por ello el protocolo apropiado para este caso se conoce como TOKEN PASSING.

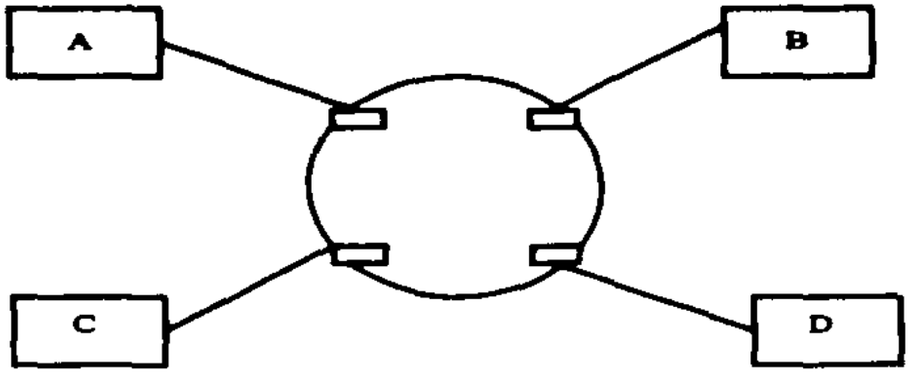



**FIGURA 6** Topología de anillo.

### 1.4.1 PROTOCOLOS TCP/IP (TRANSMISSION CONTROL PROTOCOL / INTERNET PROTOCOL)

Todas las redes de comunicaciones están basadas en protocolos o reglas, las cuales definen como prepara un mensaje ; como se establece un canal de comunicaciones y como se controla la comunicación una vez establecida.

Existen muchos protocolos de redes a saber : TCP/IP, IPX, Netbios,Netbevi,etc. Cada uno tiene diferentes características. El tipo de red determinará el protocolo a utilizarse (Por ejemplo :Novell - IPX ; IBM - Netbios ; Macrosoft - Netbeui ;UNIX - TCP/IP). El protocolo TCP/IP se forma por la unión de dos protocolos, el protocolo de transmisión (TCP) y el protocolo de interconexión de redes (IP). Estos protocolos de nivel superior se encuentran como estándares en las máquinas conectadas a Internet.[ 9]

## 1.5 SEGURIDAD EN LAS REDES (MEDIANTE LAS TÉCNICAS CRIPTOGRÁFICAS)

Las redes de área amplia son claramente unos medios de comunicación potencialmente inseguras, por lo que existe una amplia gama de contramedidas para combatir las amenazas.

Las redes de área local (LAN) son, sin embargo frecuentemente consideradas como menos vulnerables, debido al menor territorio que cubren. Pero en realidad las LAN generan muchas de las vulneravilidades de un sistema de ordenador. Los problemas particulares incluyen :

a) La mayoría de las LAN utilizan el método de transmisión de difusión, el cual genera que todos los datos estén disponibles para todos los dispositivos conectados a la LAN.

b) Puede utilizarse el mismo medio de comunicaciones para aplicaciones diferentes, y por tanto, con requerimientos de seguridad distintos.

c) Las LAN están conectadas frecuentemente por puertas de acceso a redes de área amplia, haciendo que se pueda acceder a los datos desde lugares remotos.

La seguridad de red presenta una multitud de nuevos problemas que no se encuentran en una implementación de un solo sistema.

### 1.5.1 REQUISITOS DE SEGURIDAD

La seguridad de una red incluye tres requisitos :

- SECRETO : Requiere que la información en un sistema computacional sea accesible para la lectura solo por partes autorizadas. Este tipo de acceso incluye impresión, desplegado y otras formas de divulgación e incluso la simple revelación de la existencia de un objeto.

- **INTEGRIDAD :** Requiere que el contenido del sistema computacional pueden modificarlo solo las partes autorizadas. La modificación incluye escritura, cambio de estado, borrar y crear.

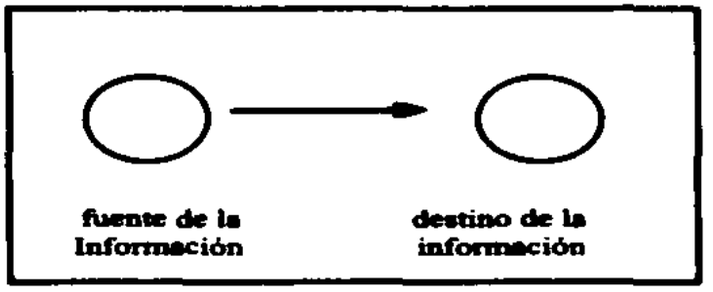
- **DISPONIBILIDAD :** Requiere que el contenido del sistema computacional este disponible para las partes autorizadas.

Los tipos de amenazas a la seguridad de una red se identifican mejor observando la función del Sistema Computacional que va a proporcionar información. En general, existe un flujo de información desde una fuente a un destino. Este flujo normal está descrito en la figura 7a. El resto de la figura muestra cuatro categorías generales de amenazas que son :

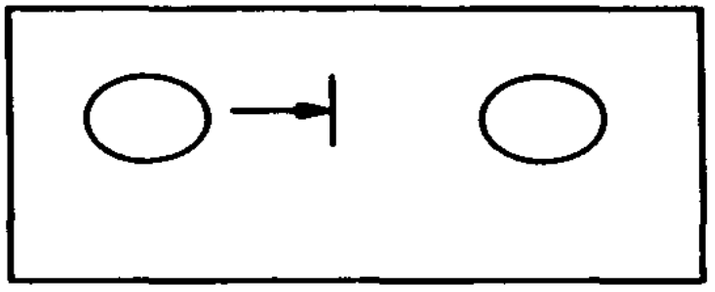
- INTERRUPCIÓN : Una parte del contenido del programa se destruye, se torna inutilizable o ya no esta disponible. Esta es una amenaza a la disponibilidad. Algunos ejemplos incluyen la destrucción de una pieza del hardware tal como un disco duro, el rompimiento de una línea de comunicación o la deshabilitación del sistema de administración de archivos (ver fig. 7b).

- INTERCEPCIÓN : Una parte no autorizada consigue accesar el contenido del sistema. Esto es una amenaza al secreto. La parte no autorizada podría ser una persona, un programa o una computadora. Los ejemplos incluyen intervención de las conexiones para captura, datos en una red y la copia ilícita de archivos o programas. (ver fig. 7c).

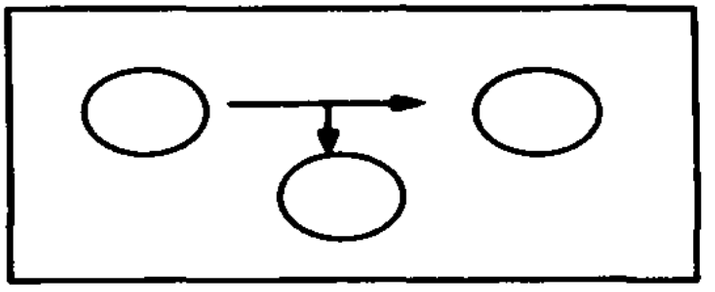
- MODIFICACIÓN : Una 'parte no autorizada no solo consigue accesar sino que altera en forma indebida una parte del contenido del sistema. Esta es una amenaza a la "Integridad". Los ejemplos incluyen cambiar valores en un archivo de datos, al alterar un programa de manera que se ejecute de manera diferentes modificar el contenido de mensajes que se transmiten en una red (ver fig. 7d).



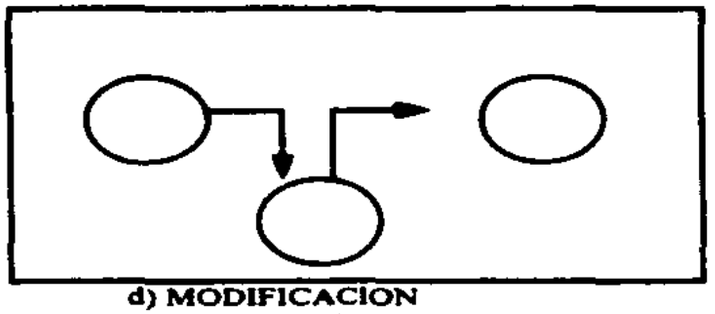

a) FLUJO NORMAL



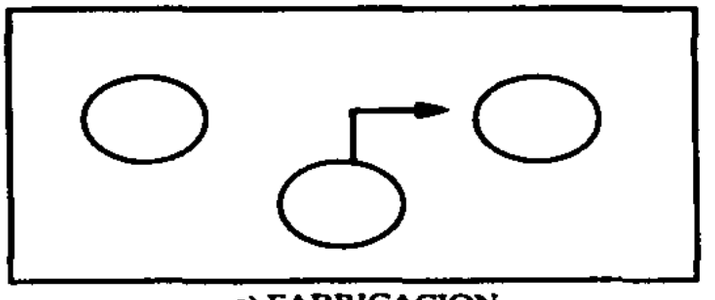
b) INTERRUPCION
(Disponibilidad)



c) INTERSECCION
(Secreto)



d) MODIFICACION
(Integridad)



e) FABRICACION
(Integridad)

**FIGURA 7** Amenazas a la seguridad.

- **FABRICACIÓN :** Una parte no autorizada inserta objetos falsificados en el Sistema. Esta es también una amenaza a la Integridad. Los ejemplos incluyen la inserción de mensajes impuros en una red o la adición de registro a un archivo (ver fig. 7e).

El contenido en un sistema computacional puede clasificarse en hardware, software, datos y líneas de comunicación y redes (ver fig. 8).[ 17 ]

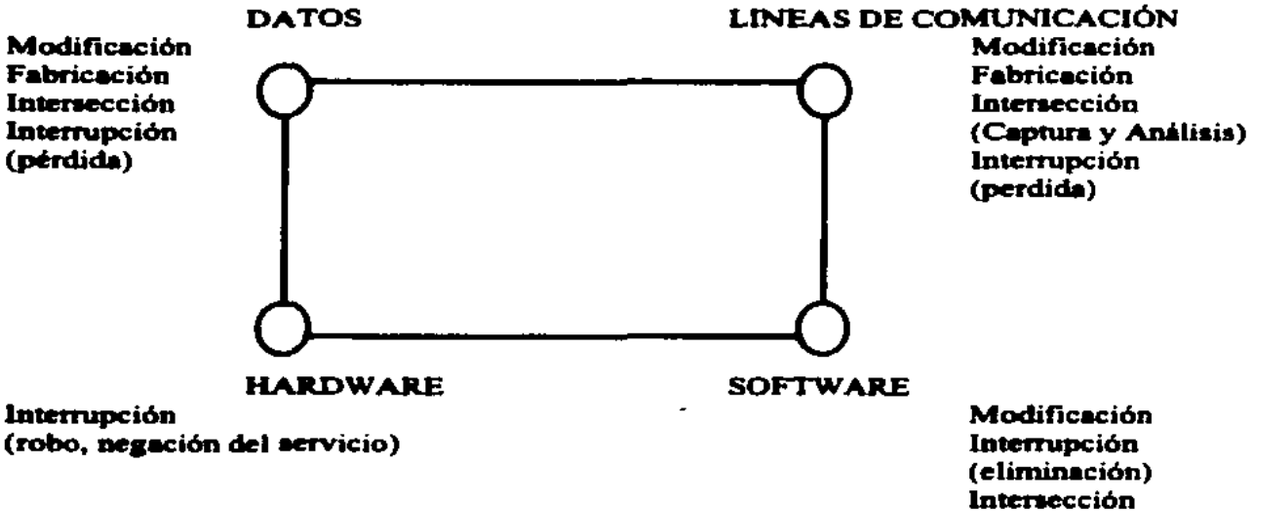



**FIGURA 8** Amenazas a la seguridad y ventajas del sistema computacional.

El enfoque más eficiente y más común para enfrentar las amenazas destacadas en el análisis es el encriptado. Si se usa el encriptado para enfrentar estas amenazas, entonces necesitamos decidir que encriptar y donde debe localizarse el mecanismo de encriptado.

# CAPÍTULO 2

# INTRODUCCIÓN A LA CRIPTOGRAFÍA

# 2 INTRODUCCIÓN A LA CRIPTOGRAFÍA

Una de las herramientas automatizadas más importantes para la seguridad computacional es la CRIPTOGRAFÍA (Encriptado). El encriptado es un proceso que oculta el significado cambiando mensajes legibles a mensajes que otros no pueden entender.

El encriptado puede hacerse por medio de un código, una cifra. Un sistema de código usa una tabla predefinida o diccionario para sustituir una palabra o frase sin sentido para cada mensaje o parte de un mensaje . El código mas simple consiste en sustituir una letra por otra diferente del mismo alfabeto. Una cifra usa un algoritmo computable que puede traducir cualquier flujo de bits de mensaje en un criptograma no legible , como las técnicas de cifra se presentan con facilidad a la automatización, estas son las técnicas que usan las computadoras contemporáneas y las instalaciones de seguridad de red. Este capitulo sólo analiza técnicas de encriptado.

Empezaremos observando el enfoque tradicional de encriptado ahora conocido como encriptado de clave privada. Después veremos una técnica nueva bastante útil conocida como encriptado de clave pública.

## 2.1 SISTEMAS CRIPTOGRÁFICOS DE CLAVE PRIVADA (Simétricos)

Cuando las claves de descifrado y la de cifrado coincidan o al menos sea posible deducir la clave de descifrado a partir de la clave de cifrado, se habla entonces de cifrado simétrico o de clave secreta.

En los cifrados de clave simétricos, la seguridad depende de un secreto compartido exclusivamente por emisor y receptor.[ 20 ]

### 2.1.1 CIFRADO POR SUSTITUCIÓN

La sustitución es la forma más sencilla de cifrado. Casi todos hemos utilizado alguna vez esta técnica en alguna de nuestras actividades personales, o incluso como un juego de niños. Consiste en reemplazar una letra o un grupo de letras del original por otra letra o grupo de letras. El esquema sustitucional más sencillo es el esquema de Cesar. En éste mecanismo, cada letra del alfabeto se sustituye simplemente por otra. Por ejemplo :

| | |
|---|---|
| Texto legible : | ABCDEFGHIJKLMNOPQRSTUVWXYZ |
| Letras de sustitución : | FGQRASEPTHUIBVJWKLXYZCONMD |

Este tipo de cifrado se conoce como sustitución monoalfabética, ya que cada una de las letras se sustituye por otra del mismo alfabeto. Aunque éste método ofrece $4x10^{26}$ claves distintas, la propia clave puede revelar bastante sobre la legibilidad del mensaje. Si no se conocen las claves, o si estas no presentan ninguna regularidad, se calcula que un ordenador tendría $10^{13}$ años en probar con todas las claves, si dedica un microsegundo a probar con cada clave. Sin embargo, los lenguajes presentan ciertas propiedades que permiten descifrar mucho más de prisa.

Por ejemplo, las vocales son mucho más frecuentes que las consonantes : (hola, tuna, etc ; fácil de descifrar). Además, existen algunas combinaciones de dos letras (diagramas) que aparecen muy a menudo ( por ejemplo , en español, de, en, in, etc.). En muchos idiomas también son frecuentes determinadas combinaciones de tres letras (trigramas, como por ejemplo, en español, des, con, que, etc.).

La tarea del criptoanalista consiste en estudiar las apariencias de cada letra individual, los diagramas, trigramas y palabras más frecuentes, puede generar un intento de texto legible basándose en los datos decodificados .

Existen otros métodos de cifrado sustitucional,. Por ejemplo, algunos sistemas utilizan la sustitución polialfabética, en la cual existen varios alfabetos de cifrado que se emplean en rotación. Una variación del cifrado sustitucional consiste en utilizar una clave más larga que el texto legible . Se usa como clave una secuencia aleatoria de bits, que se cambia periódicamente.

La principal desventaja de todas las estructuras basadas en una clave privada es que todos los nodos de la Red han de conocer cuál es la clave común. La distribución de las claves acarrea algunos problemas administrativos y logísticos. Hasta hace poco, la idea de una clave privada era el esquema de cifrado predominante en las redes. Hoy en día las redes cambian la clave periódicamente ; que bien puede ser, cada 24 horas, o incluso , si es necesario cada minuto.

## 2.1.2 CIFRADO POR TRANSPOSICIÓN

Un método criptógrafico más sofisticado es el cifrado por transposición, en el que las claves de las letras se reordenan, pero no se disfrazan necesariamente. La clave utilizada en este caso es "S E M I N A R I O" (ver fig.9), en donde, la clave se emplea para enumerar

las columnas. La columna 1 se coloca bajo la letra de la clave más próxima al comienzo del alfabeto, es decir, A,B,C..., etc. Si la clave incluye alguna letra repetida , puede adoptarse el criterio de numerar de izquierda a derecha. A continuación se escribe el texto legible como una serie de renglones que se colocan debajo de la clave . Después se lee el texto cifrado por columnas, empezando por aquella columna cuya letra clave sea la más próxima al principio del alfabeto. Así, la frase "Nunca seré un obstáculo para mi misma " quedará como sigue :

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| S | E | M | I | N | A | R | I | 0 |
| 9 | 2 | 5 | 3 | 6 | 1 | 8 | 4 | 7 |
| N | U | N | C | A | S | E | R | E |
| U | N | O | B | S | T | A | C | U |
| L | O | P | A | R | A | M | I | M |
| I | S | M | A | A | B | C | D | E |

**FIGURA 9** Cifrado por transposición.

Y el texto cifrado será el siguiente :

"STABUNOSCBAARCIDNOPMASRAEUMEEAMCNULI "

## 2.1.3 CIFRADO DE DATOS ESTÁNDAR (DES)

El 15 de enero de 1997, el Departamento de Comercio y la Oficina Nacional de Estándares de Estados Unidos publicaron la norma DES( Data Encryption Standard) Estándar de cifrado de datos. El algoritmo DES es un sistema monoalfabético que fue desarrollado en colaboración con IBM y se presentó al público con la intención de proporcionar un algoritmo de cifrado normalizado para redes de ordenadores.

DES se basa en el desarrollo de un algoritmo de cifrado que modifica el texto con tantas combinaciones que el criptoanalista no podría deducir el texto original aunque dispusiese de numerosas copias.

El algoritmo criptográfico suministra seguridad entre dos nodos de un sistema de proceso de datos, si los dos nodos de un sistema de proceso de datos, tienen instalado el algoritmo , sea con tecnología hardware, como obliga la norma de utilización estándar en USA, o con tecnología Software, como se diseñe. Es preciso además que ambos nodos tengan exacto conocimiento de la clave utilizada.

Es importante anotar que para una buena seguridad en los datos solamente se necesita mantener en secreto la clave, pueden ser públicos los detalles del algoritmo. La clave criptográfica , por lo tanto es considerada con un nivel de seguridad análogo a la combinación de una caja fuerte.

### 2.1.3.1 DESCRIPCIÓN DEL ALGORITMO DES

El cifrado comienza con la función de permutación (Función P- ver fig. 10 ); en este caso la entrada a la función P de 8 bits. Como se ve en el interior del recuadro , la sustitución de los bits sigue una serie de reglas lógicas. La salida esta formada por los mismos bits

cambiados de orden . La caja P puede estar controlada por un programa con el fin de llevar a cabo diversos tipos de permutaciones.

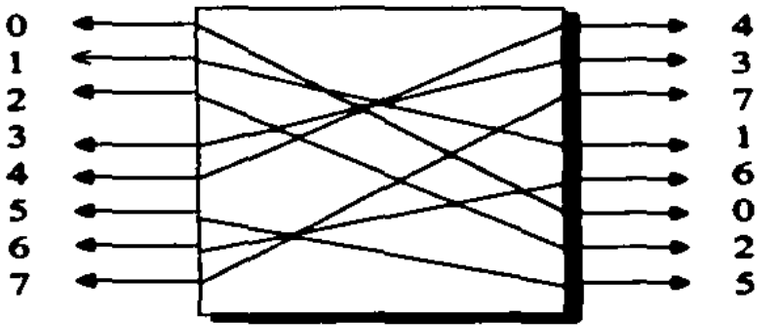



**FIGURA 10** CAJA P (Permutación ).

La segunda función , la de sustitución , esta representada en la fig. 11. En este caso , una entrada de 5 bits selecciona una de las ocho posibles líneas que entran en la caja S (Decodificador ). La función S lleva a cabo la sustitución de las líneas, con lo cuál las 8 líneas vuelven a convertirse en 5 al traspasar por el Codificador.

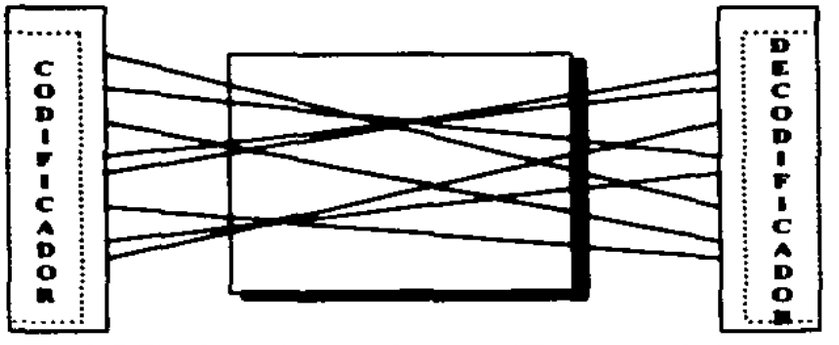



**FIGURA 11** CAJA S (Transposición).

La filosofía del DES consiste en llevar acabo múltiples etapas de permutación y sustitución, como se observa en la fig. 12. DES cifra un bloque de texto original de 64 bits en un bloque de texto cifrado de 64 bits bajo el control de una clave criptográfica de 64 bits de los cuales 56 son usados directamente por el algoritmo y 8 son utilizados para la detección de errores. [ 3 ]

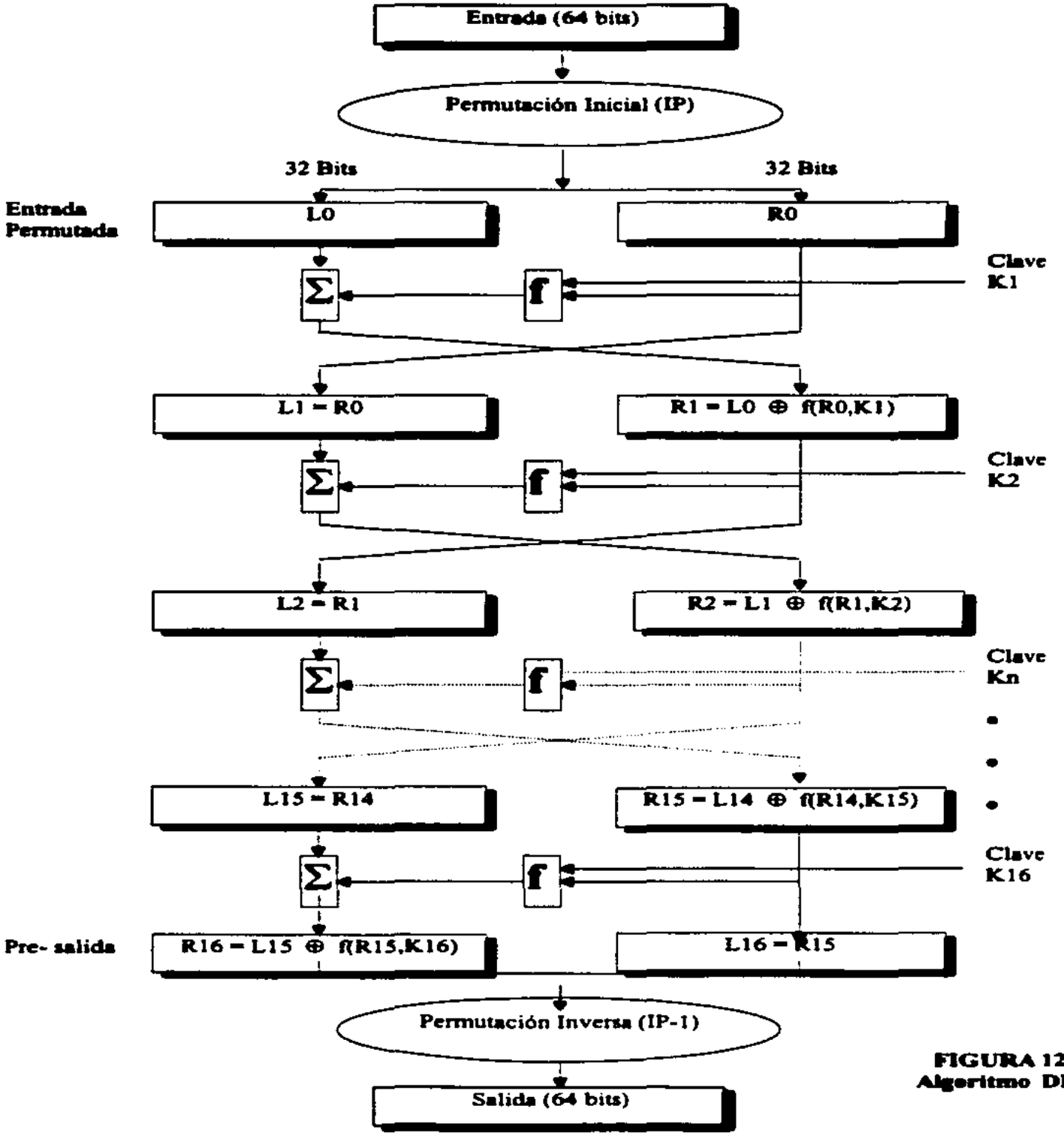



**FIGURA 12**
**Algoritmo DES**

El descifrado convierte los datos a su forma original si se usa su misma clave (ver fig. 13).

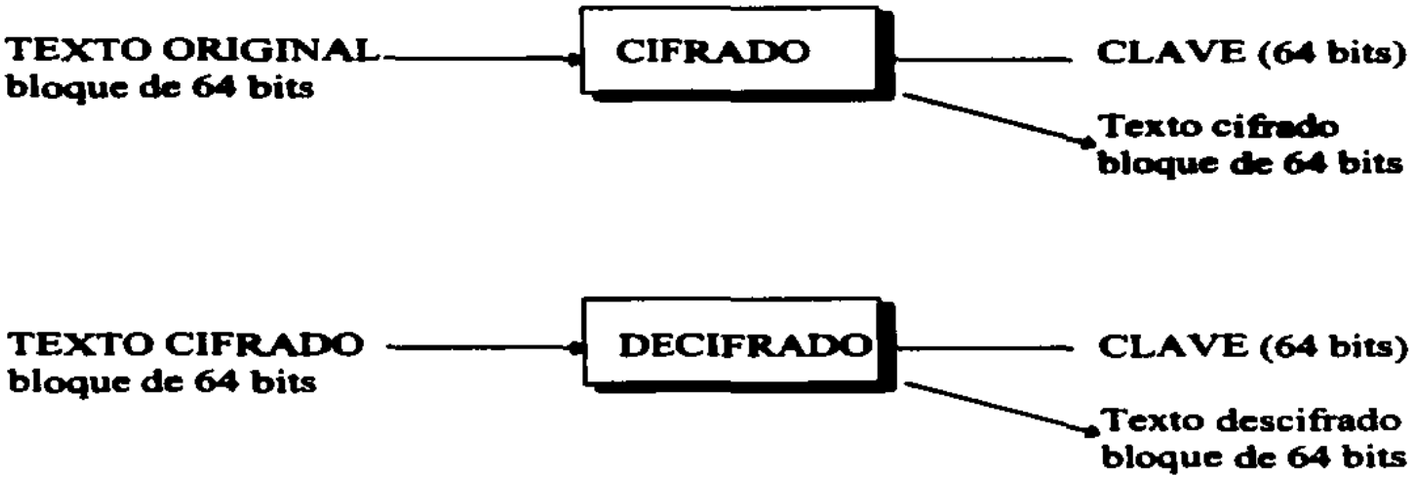



**FIGURA 13** Cifrado y Descifrado.

La clave es generada de tal modo que 56 bits de los 64 son usados por el algoritmo y 8 son usados como bits de paridad impar de cada byte de 8 bits, es decir existe un número impar de bits 1 en cada byte.[ 9 ]

Existen unos setenta mil billones (70,000,000,000,000,000) de claves posibles de 56 bits. Sin embargo esto no quiere decir que sea imposible romper una clave semejante. Los ordenadores de alta velocidad, mediante análisis estadístico, no necesita emplear todas las posibles combinaciones para romper la clave. El objetivo principal de DES no es proporcionar una seguridad absoluta, sino únicamente un nivel razonable para las redes orientadas a aplicaciones comerciales.

Otra forma de analizar el algoritmo DES es por medio de tablas :

Ver figura 14 , en el método DES el texto legible que debe ser cifrado se somete a una permutación inicial (IP) con un bloque de entrada de 64 bits que se permuta de la siguiente forma :

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

**FIGURA 14** Tabla (Permutación Inicial-IP).

Ahora bien, estas tablas se leen de izquierda a derecha y de arriba abajo, de manera que, la entrada permutada tiene como primer bit 58 del original (64 bits), como segundo bit el bit 50, y así sucesivamente, hasta llegar al último bit, que corresponderá al bit 7 del texto sin cifrar. Entre las transposiciones inicial y final, el algoritmo realiza 16 iteraciones de una función "f" que combina una sustitución y una transposición.

A continuación , el resultado final se somete a la siguiente permutación, que es la inversa de la permutación inicial (IP -1) (ver fig. 15)

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

**FIGURA 15** Tabla (Inversa de la permutación inicial (IP-1)).

Las 16 etapas emplean los dos bloques (L y R) de 32 bits para generar dos bloques de 32 bits de salida c/u, es decir L = 32 y R= 32. 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 o - exclusivo[19] ( ver fig. 16 , + denota la suma bit a bit).[ 9 ]

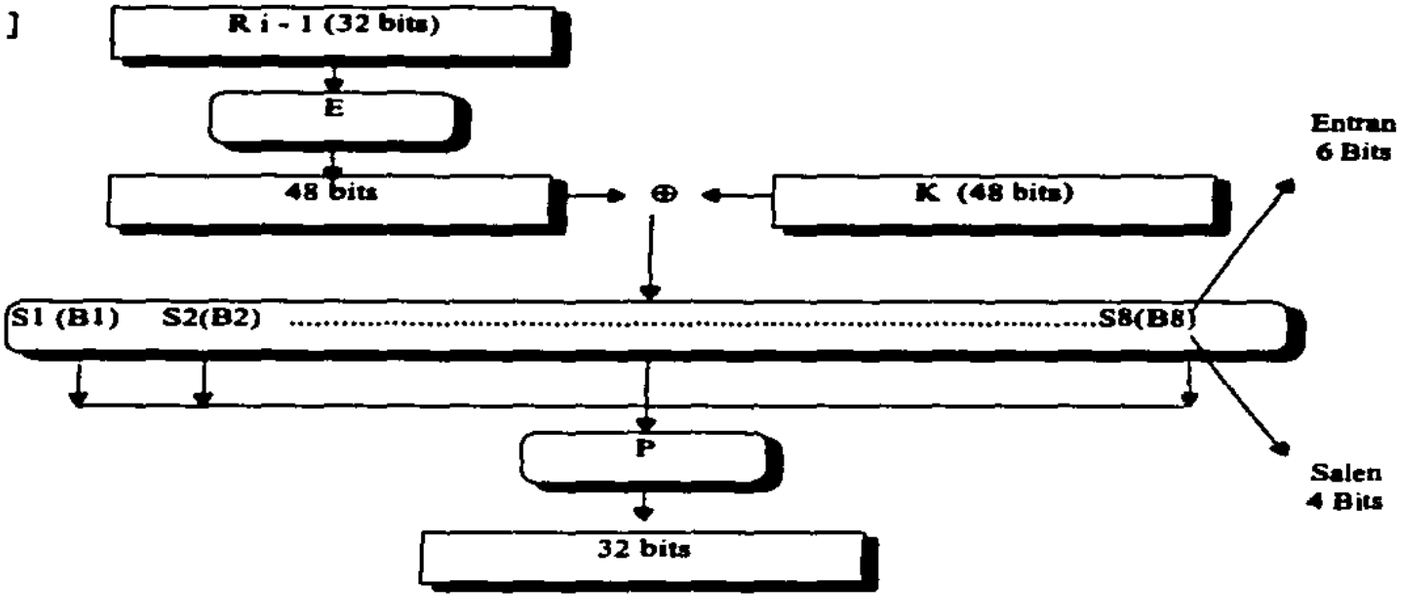



**FIGURA 16** Función "f" , f(Ri - 1,K1).

1.- La mitad derecha 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 **o - exclusivo**. En cada etapa se escoge un bloque 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.

Apesar de toda la complejidad, DES es básicamente un cifrador de sustitución monoalfabética que utiliza 8 caracteres de 64 bits.

[19] o - exclusivo es : una compuerta (enrutador de selección)

## 2.1.4 ATAQUES A DES

DES ha disfrutado de un uso cada vez más amplio. Sin embargo, el Algoritmo DES ha sido motivo de controversia desde su concepción, parte de esta polémica se debe al secreto que rodeo a su desarrollo.

Para desarrollar DES, IBM trabajo en colaboración con la Agencia Nacional de Seguridad de Estados Unidos, y ambas organizaciones se unieron para guardar en secreto los aspectos de diseño del algoritmo. Las principales críticas se concentran en los 56 bits de longitud de la clave, la cual algunos observadores consideran demasiado corta.

El diseño original de IBM incluía una clave de 128 bits, que habría hecho radicalmente imposible romper la clave, incluso con los ordenadores más rápidos hoy en día. Hay quien piensa que el gobierno ésta dispuesto a poner al alcance del público una clave completamente inviolable.[ 3 ]

Hoy en día la digitalización de voz es algo que ya incorporan algunos aparatos telefónicos. Utilizando la tecnología de semiconductores, no sería demasiado difícil instalar dentro del propio teléfono, junto con la circuitería de digitalización, un circuito integrado capaz de calcular y descifrar cualquier transmisión de sus ciudadanos, con el fin de proteger la seguridad nacional y combatir el crimen. Así pues, la cuestión radica en posturas políticas, y no sólo en aspectos técnicos.

Cuando la digitalización de la voz y el cifrado entre de lleno en nuestra ciudad, la codificación de las conversaciones teléfonicas se convertirá en un asunto polémico.

De manera básica, existen dos maneras de romper un texto encriptado :

Una manera es explotar las propiedades de cualesquier función matemática que forman la base del algoritmo de encriptado para hacer un ataque criptoanálitico sobre ellas. Por lo

general, se supone que el DES es inmune a tales ataques, el papel de la NSA ( National Security Agency) en la formación de los estándares DES finales dejo amplias dudas.

La otra manera es un ataque de fuerza bruta en la cual prueba todas las claves posibles en una búsqueda exhaustiva. Esto es, usted intenta descifrar el texto encriptado con cada clave posible de 56 bits, hasta que surge algo legible . Con sólo 56 bits en la clave DES, existen $2^{56}$ claves diferentes ( un número tan pequeño que resulta incomodo y que se está volviendo más pequeño a medida que las computadoras se vuelven más rápidas).

Diffie y Hellman demuestran que el nivel de seguridad del DES no es adecuado , porque utilizando el método de criptoanálisis más básico (búsqueda exhaustiva de las claves) estiman una tardanza de 112 horas en romperlo con una máquina de grandes prestaciones.

Concluyen que, ya que con el paso de los años dicha máquina resultará menos costosa, los datos almacenados que hayan sido cifrados con DES corren peligro a largo plazo :

Por un lado, el tamaño de la clave es demasiado pequeño, por lo que se facilita un ataque por búsqueda exhaustiva y por otro lado, la Tecnología.

## 2.2 SISTEMAS CRITOGRÁFICOS DE CLAVE PÚBLICA (Asimétricos)

Si es imposible obtener la clave de descifrado mediante la clave de cifrado, se trata de un cifrado Asimétrico ó de clave pública.

La criptografía de clave pública utiliza dos claves, la privada (conocida solamente por su dueño) y la pública (que puede ser conocida por cualquier persona.).

REMITENTE → CIFRA / CLAVE PÚBLICA (del destinatario)
DESTINATARIO → DESCIFRA /CLAVE PRIVADA (del destinatario)[ 19 ]

### 2.2.1 CRIPTOSISTEMAS RSA (RIVEST, SHAMIR Y ALDEMAN)

Antes de discutir las implementaciones de criptografía pública, es necesario hacer un breve paréntesis histórico. Desde su invento, la criptografía ha sido una poderosa herramienta para el espionaje y la guerra. Por ello los EUA imponen restricciones para la exportación de software que incorpore criptografía avanzada. Rivest, Shamir y Adelman desarrollaron, en 1977, un algoritmo extremadamente seguro y simple para criptografía de llave pública , al cual se le conoce como RSA .

A pesar de presiones por parte del gobierno de EUA para evitarlo, el algoritmo fue publicado en 1977 y en 1978. En 1983, el MIT (- Massachusets Institute of Technology) obtuvo la patente sobre el algoritmo. Esta patente es inválida fuera de EUA y Canadá , pues, excepto en este país , al publicarse el algoritmo, éste se vuelve del dominio público y por lo tanto no es patentable (en EUA hay un período de gracia de hasta un año después de su publicación).

Más tarde, MIT cede la patente en un grupo llamado Public Key Partner (PKP) , que incluye a RSA Data Security, la cual es también dueña de otras patentes que cubren otros

algoritmos de criptografía . En esencia, la patente da a PKP el derecho a ser un monopolio que controla la criptografía de llave pública en EUA y Canadá por

17 años, el periodo de duración de las patentes. En 1991, Phil Zimmermann autoriza publicar en múltiples servidores de información y foros de USENET[20] un programa de dominio público llamado Pretty Good Privacy (PGP), que incluye una implementación del algoritmo de RSA, pero basándose en la información pública que se hizo disponible 10 años antes.

RSA amenaza con demandarlo, por lo que para evitarlo , Zimmermann promete no continuar con el desarrollo de PGP . Sin embargo, programadores en diversas partes del mundo continúan con su desarrollo , portándolo a múltiples arquitecturas y Sistemas Operativos. Por si fuera poco el código de PGP puede ser obtenido desde cualquier país por lo que el gobierno de los EUA inició una investigación para decidir si Zimmermann violó las restricciones de exportación.

Apenas en enero pasado Zimmermann es notificado que se decidió no continuar la investigación . MIT decide negociar con Zimmermann y RSA una licencia para el uso no comercial de PGP , y nace así la versión 2.5 , la cual no puede ser exportada. Sin embargo, las secciones no relacionadas con criptografía si pueden ser exportadas, y en ellas se basa Stale Schumacher para crear la versión internacional de PGP , la cual es, a partir de ese momento, compatible con la de MIT.[ 21 ]

RSA es el sistema de cifrado con clave pública más utilizado ; sus aplicaciones adecuadas están en el correo electrónico, donde una determinada "firma" verificando un determinado directorio de claves públicas, y en comunicaciones de datos para la autentificación y secreto. Las elevadas necesidades de proceso de los sistemas de cifrado con clave pública ha restringido su utilización comercial a unas cuantas aplicaciones de banca y a la distribución de claves para el DES.

[20] USENET : Otro nombre que se le da a los grupos de noticias. (Foros de discusión que permiten a individuos concertar acerca de temas de interés común). Ftp//sri.com/netinfo/interest.groups.txt

RSA utiliza bloques de datos grandes, normalmente de 512 bits, y el cifrado requiere el equivalente a tres millones de multiplicaciones de 16 bits por bloque. La implementación del Software requiere aproximadamente 45 segundos para procesar un bloque de 512 bits en un PC IBM , mientras que las implementaciones de hardware tardan al menos de 0 a 1 segundos. Con esos procesos tan elevados , RSA no resulta atractivo para muchas necesidades de los sistemas de comunicación de datos de alta velocidad.

Las claves de RSA son palabras de 200 bits. La clave de codificación es el producto de dos números primos secretos, cada uno de 100 bits, y la clave de descifrado puede calcularse a partir de dichos números. Para obtener los números primos secretos podría factorizarse la clave, pero ello llevaría, para una clave de 200 bits, 3800 millones de años suponiendo que se realiza una operación por microsegundo.

El mensaje original se convierte primero en un bloque de datos de hasta 512 bits de longitud. El cifrado del bloque de texto original, utilizando la clave de cifrado, produce una clave de texto cifrado del mismo tamaño. El proceso de descifrado es el inverso del cifrado, pero utilizando la clave de descifrado.

El algoritmo de cifrado RSA está basado en una función de un solo sentido que permitirá que un número **U** se transforme en un número **V**, pero que hará que la transformación inversa sea computacionalmente inviable. Una "trampa" (trapdoor) es un método de derivar **U** a partir de **V** con una información especial.

Se han producido sistemas de cifrado híbrido en los cuales un sistema de cifrado con clave pública se combina con un sistema de cifrado con clave privada, como DES, para aprovechar la rapidez y fiabilidad de los chips VLSI (Integración a muy grande escala). Un sistema así es mucho más rápido que un sistema de criptografía con clave pública, ya que por mensaje se requieren muchos más cifrados con clave privada que con clave pública.

**Para transmitir los datos , el remitente genera primero una clave aleatoria que es utilizada en un algoritmo rápido de cifrado con clave privada . La clave aleatoria se cifra entonces utilizando el método de clave pública, y tanto la clave cifrada como el texto cifrado con DES se transmiten al receptor. El receptor primero descifra la clave, y la emplea para descifrar el texto cifrado. Se puede utilizar un segundo paso para comprobar la autenticidad del texto.[ 14 ]**

## 2.2.3 ALGORITMO PGP (PRETTY GOOD PRIVACY)

PGP es el programa más utilizado en el mundo para criptografía de llave pública. La versión más actual es la 2.6.3i , donde la i identifica a la versión internacional. Es ilegal en México utilizar la versión del MIT (2.6.3) no porque viole la patente, sino porque contiene código protegido por derecho de autor, además que es ilegal exportar desde EUA una copia de 2.6.3. PGP 2.6.3i es gratuito para fines no comerciales , pero es necesario pagar una licencia para su uso comercial (debido a que utiliza un algoritmo llamado IDEA(International Data Encryption Algorithm), patentado por Ascom Systec, en Suiza) ; su precio es relativamente barato : US $ 15 , por usuario Contrariamente a lo que mucha gente supone.

PGP es tan seguro como su contraparte estadounidense. ViaCript pública una versión comercial de PGP que sólo puede ser exportada a compañías transnacionales estadounidenses que cumplan con ciertos requisitos. Existen paquetes que permiten *conectar* PGP con programas de correo electrónico para firmar, autentificar, encriptar y desencriptar mensajes electrónicos.[ 21 ]

Netscape Communications utiliza RSA para autentificar conexiones a nivel de sockets[21]. El protocolo es llamado Secure Sockets Layer (SSL) . Netscape Navigator, utiliza SSL para realizar transacciones comerciales entre él y Netscape Commerce Server.

Debido a restricciones de exportación de los EUA, la versión internacional de Nestcape permite solamente llaves de 128 bits. Netscape asegura que se necesitan 64 MIPS (Millones de Instrucciones Por Segundo) - años para romper una llave de 40 bits. Si la información vale la pena, puede ser decodificada. Esto no pasaría con una llave de 128 bits (con una llave de 256 bits sería virtualmente imposible lograrlo aun utilizando toda la energía del universo).[ 21 ]

[21] Socket :Son algoritmos orientados para establecer la comunicación entre el servidor y el cliente. Utilizan los protocolos TCP/IP y UDP(User Datagram Protocol).

PGP usa una clave dividida en dos, para cifrar los mensajes, la privada (conocida solamente por su dueño) y la pública (que puede ser conocida por cualquiera). Un mensaje que se desea enviar debe ser encriptado utilizando la llave publica del destinatario. Al recibirlo, el destinatario utilizará su llave privada para desencriptarlo.

El sistema de llave pública tiene las siguientes ventajas :

a) Es muy seguro si las llaves son suficientemente grandes
b) Por cada persona es necesaria solo una pareja de llaves
c) La llave pública de una persona puede ( y debe ) ser publicada.

En cambio, el sistema de llave única requiere que cada pareja de corresponsales comparta una llave única, y que ésta se mantenga siempre en secreto. Sin embargo encriptar un mensaje con el sistema de llave pública es lento.

PGP realiza los siguientes pasos para cifrar un mensaje :

- Comprime el mensaje
- Genera una clave de sesión de forma aleatoria, usando un algoritmo conocido como sistema estándar para cifrar información ( IDEA- International Data Encryption Algorithm).
- Usando la clave de sesión, PGP cifra el mensaje comprimido.
- La clave de sesión se cifra mediante la clave pública del receptor y puesta en la parte frontal del mensaje cifrado.

Para descifrar el mensaje PGP debe realizar los siguientes pasos :

- Reconoce la clave de sesión pública, que se encuentra dentro del mensaje cifrado, para después solicitar al usuario por la parte privada de la clave.
- Con la parte privada de la clave se descifra la clave de sesión.
- Usando la clave de sesión, PGP descifra el mensaje.
- Finalmente descompacta el mensaje.

Además PGP ofrece el servicio de identificación de usuarios, para realizar esto usa el concepto de firma digital , dicha firma digital se agrega al documento , el cual es enviado. El destinatario separa la firma digital del mensaje. Posteriormente decodifica con la llave pública de X la firma digital del mensaje y la compara con la calculada. Si son diferentes entonces, o bien el contenido del mensaje fue modificado después de ser firmado, o X no lo envío. Este tipo de transacciones son de especial utilidad para el cierre de contratos por medios electrónicos.

PGP permite al usuario elegir el tamaño de la parte pública. Esta puede ser de 512, 768 ó 1024 bits. La parte pública de la clave se forma mediante el nombre del usuario y su clave de correo electrónico, por ejemplo :[ 8 ]

csilvia<csilvia@fes.cuautitlan2.unam.mx>

## 2.2.4 EL SISTEMA DE AUTENTIFICACIÓN DE KERBEROS

Fue desarrollado en 1983 por el proyecto Athena del Instituto Tecnológico de Massachusetts( MIT - Massachusets Institute of Technology) en colaboración con las compañías IBM y Digital Equipment Corporation . Desde entonces , Kerberos ha sido adoptado por otras organizaciones para sus propias necesidades. Muchos desarrolladores de aplicaciones de otras firmas incluyen el soporte para la autentificación del sistema Kerberos en sus productos.

Kerberos es un sistema de autentificación (es un sistema que valida la identidad de un *principal*). Un *principal* puede ser un usuario o un servicio :[ 16 ]

- Nombre primario ( Identificador del registro de x persona)
- Instancia (Es nula, 0 ó contiene información particular respecto al usuario )
- Reino (Para distinguir entre diferentes dominios de autenticación, distintos servidores Kerberos )

En la terminología Kerberos , a esto se le llama un *trio* y se le ilustra en seguida :

<nombre primario, instancia, reino>

Los *principales* Kerberos obtienen boletos para servicios de un servidor especial conocido como servidor despachador de boletos.

Este es un sistema intermediario, su objetivo es establecer un mecanismo para realizar la identificación mutua, entre máquina y usuario. Cada uno de los usuarios, de las máquinas y de los servicios tienen una contraseña, la cual se encuentra almacenada en una base de datos centralizada manejada mediante Kerberos. Las contraseñas sirven para identificar a los usuarios y a las máquinas, para evitar que estas puedan ser robadas mediante el monitoreo del tráfico de la red, la transmisión de información entre los diferentes entes de la Red se hace de forma cifrada.

El acceso a los servicios se proporciona mediante boletos, la administración de los boletos es responsabilidad de kerberos. A la máquina que se encarga de la administración de los boletos se conoce como "centro de distribución de claves" (Key Distribution Center - KDC) (ver fig. 17).

| |
|---|
| Clave de Sesión |
| Nombre del usuario |
| Dirección |
| Nombre del servicio |
| Tiempo de vida |
| Fecha y tiempo de creación (estampilla) |

**FIGURA 17** Estructura de un boleto de Kerberos.

La principal ventaja con el sistema Kerberos es que cada boleto tiene un tiempo de vida específico. Después de que dicho tiempo termina, debe solicitarse un nuevo boleto, el cual será emitido por el servidor despachador de boletos.

La principal desventaja : La clave se almacena en memoria por lo tanto es posible que los usuarios no autorizados puedan obtener las claves.

# CAPÍTULO 3

# SEGURIDAD EN COMUNICACIÓN Y ARCHIVOS UTILIZANDO CRIPTOGRAFÍA

# 3 SEGURIDAD EN COMUNICACIÓN Y ARCHIVOS UTILIZANDO CRIPTOGRAFÍA

La fig.18 , describe en forma genérica , las medidas que se toman para controlar el acceso en un sistema de procesamiento de datos. Caen en dos categorías : las asociadas con el usuario y las asociadas con los datos.[ 17 ]

El control de acceso por el usuario se denomina algunas veces autentificación.

## 3.1 USO DE CONTRASEÑAS

Un ejemplo bastante común de control de acceso por el usuario, en un sistema de tiempo compartido, es el inicio de una sesión por el usuario, la cual requiere un identificador de usuario (ID) y una contraseña. El sistema permitirá a un usuario iniciar una sesión sólo si conoce el identificador de ese usuario y si el usuario conoce la contraseña asociada por el sistema con ese identificador.

El sistema IDENTIFICADOR/CONTRASEÑA es un método poco fiable de control de acceso del usuario. Los usuarios pueden olvidar sus contraseñas y pueden accidental o intencionalmente revelar su contraseña . Los piratas han resultado muy hábiles en adivinar identificadores para usuarios especiales, tales como control del sistema y personal de administración del sistema. Por último, el archivo IDENTIFICADOR/CONTRASEÑA está sujeto a intentos de invasión.

Pueden tomarse varias medidas para mejorar la seguridad del esquema de contraseña y establecer tres requisitos :

1.- Debe haber un número grande de combinaciones de contraseña posibles. Esto reduce las oportunidades que tiene un extraño de adivinar con éxito los códigos o usar una computadora para hacer repetidos intentos por la fuerza con el control de programas. Es útil

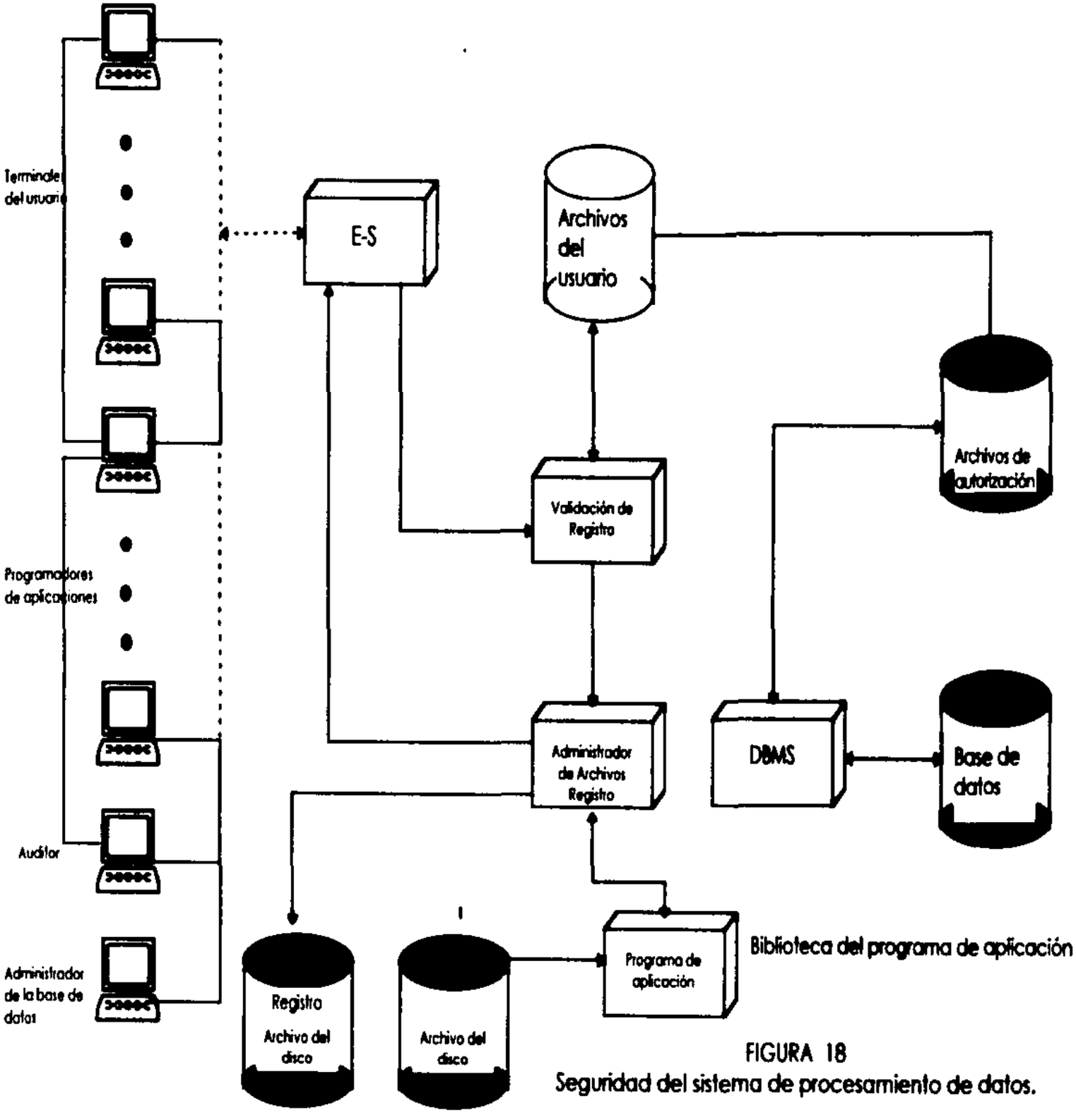



FIGURA 18
Seguridad del sistema de procesamiento de datos.

restringir las contraseñas a caracteres alfanuméricos y usar combinaciones pronunciables de caracteres, de tal manera que los usuarios puedan recordarlos con facilidad y evitar escribirlos.

2.- Debe haber desconexión automática de la línea terminal de llegada después de que se han hecho unos cuantos intentos de contraseñas no válidas. El límite usual es tres a cinco intentos. Esto hace que un atacante espere y vuelva a marcar después de unos pocos intentos, aumentando el tiempo requerido para ejecutar una invasión a varios años. Así, el ataque programado que prefieren los piratas se vuelve inútil.

3.- El sistema debe registrar y comunicar intentos inválidos de conexión y otros "eventos" que tengan implicaciones de seguridad. Estos podrían incluir, por ejemplo, una persona no autorizada que intenta correr programas de aplicación delicados , tales como sistemas de recursos humanos o que usa programas de utilería poderosos del sistema para copiar o modificar archivos. Esta característica revelará si están ocurriendo intentos de vandalismo computacional.

Un aspecto relacionado interesante es el de quién está autorizado para crear contraseñas. Algunos administradores de seguridad sienten que no se debe permitir a los usuarios asignar sus propias contraseñas (información fácil de averiguar) .Otros sienten que obligar a los usuarios a utilizar contraseñas seleccionadas por el sistema provoca que escriban la contraseña , lo cuál implica un mayor riesgo.

El problema del control de acceso del usuario se complica con una red de comunicación (Transmisión de datos). El diálogo de inicio de sección debe ocurrir en el medio de comunicación y la escucha a escondidas es una amenaza potencial.

El control de acceso del usuario en una ambiente distribuido puede ser centralizado o descentralizado. En un enfoque centralizado, la red proporciona un servicio de inicio de sesión para determinar a quién se le permite usar la red y con quién se permite conectar al usuario.

El control de acceso de usuario descentralizado trata a la red como un enlace de comunicación transparente y el procedimiento usual de inicio de sesión lo realiza la computadora destino. Por supuesto, todavía deben considerarse los aspectos de seguridad para la transmisión de contraseñas por la red.

En muchas redes, pueden usarse dos niveles de control de acceso. Pueden darse a los anfitriones individuales una opción de inicio de sección para proteger los recursos específicos de la computadora principal y la aplicación. Además, toda la red puede proporcionar protección para limitar el acceso a ella a usuarios autorizados. Este dispositivo de dos niveles es deseable para el caso común en el cual la red conecta anfitriones diferentes y simplemente proporciona un medio conveniente de acceso a TERMINAL/COMPUTADORA PRINCIPAL. En una red más uniforme de anfitriones, podría imponerse una política de acceso centralizado en un centro de control de red.

Se han propuesto técnicas más elaboradas que una simple contraseña de identificación para reconocer al usuario. Técnicas exóticas como registro de voz, huellas digitales y análisis de la geometría de la mano pueden ser más seguras pero en el presente, se consideran demasiado caras.[ 4 ]

## 3.2 EL ARCHIVO DE CONTRASEÑAS

Si se eligen las contraseñas con cuidado, si los propietarios de contraseñas toman conciencia de la importancia de la seguridad y si las medidas de seguridad de red impiden la lectura de las contraseñas transmitidas , entonces están cerradas la mayoría de las avenidas de ataque . No obstante, para que las contraseñas sean utilizables , el sistema operativo debe mantener un archivo de contraseñas, listar contraseñas legales y los privilegios asociados con cada contraseña. Si un pirata tiene éxito en obtener acceso a ese archivo, entonces el sistema ha sido vencido.

El archivo de contraseñas puede protegerse usando encriptado (ver fig.19). En este caso, todas las contraseñas en la tabla de contraseñas se almacena en forma encriptada. Cuando un usuario introduce una contraseña, esa contraseña es encriptada y comparada las contraseñas encriptadas en la tabla para una coincidencia. Note que con esta técnica , las contraseñas en el archivo de contraseña nunca son descifradas.[ 2 ]

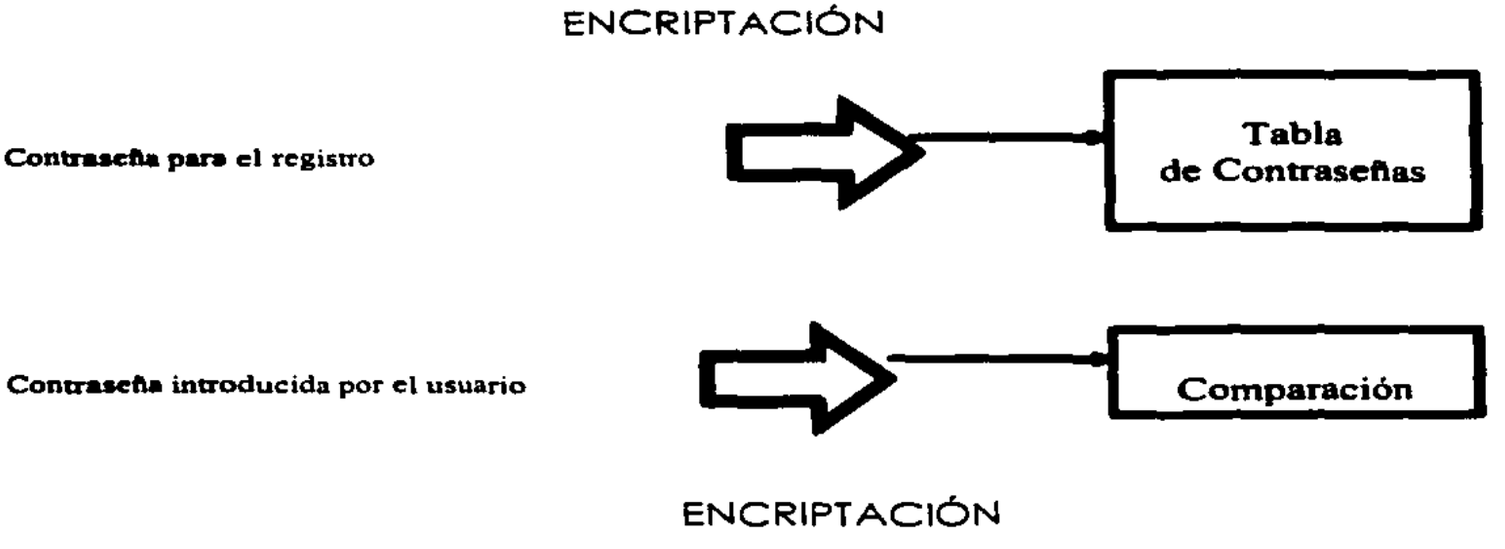



**FIGURA 19** Encriptado con contraseñas.

La ventaja de este enfoque es que la tabla de contraseña misma no necesita estar protegida, a menos que el atacante conozca la clave de descifrado, la tabla no es de utilidad. Además, si se usa una técnica de encriptado asimétrico, en la cual la clave de encriptado y las claves de descifrado son diferentes, entonces la clave de descifrado no necesita estar almacenada en el sistema computacional o en ninguna otra parte (Clave pública).

## 3.2.1CONTROL DE ACCESO ORIENTADO A DATOS

Después de un inicio de sesión exitoso, se otorga acceso al usuario a un conjunto de anfitriones y aplicaciones o a una sola de ellas. Por lo general, esto no es suficiente para un sistema que incluye datos delicados en su base de datos. Por medio del control del procedimiento para el control de acceso del usuario, el sistema puede identificar a un usuario. Asociado con cada usuario puede haber un perfil de usuario, el cual especifica las operaciones permisibles y los accesos al archivo.

El sistema operativo puede después imponer reglas basadas en el perfil del usuario. No obstante, el sistema de administración de base de datos debe controlar el acceso a registros específicos o incluso a parte de los recursos. Por ejemplo, puede permitirse para cualquiera en la administración tener una lista del personal de la compañía, pero sólo individuos seleccionados pueden tener acceso a información de salarios. El asunto es sólo uno de los que se encuentra a nivel de detalle.

Cada vez que el sistema operativo puede conceder un permiso de usuario para accesar un archivo o usar una aplicación, después del cuál no existen comprobaciones de seguridad, el sistema de administración de la base de datos debe decidir con respecto a cada intento de acceso individual. Esta decisión dependerá no sólo de la identidad del usuario sino también de las partes específicas de los datos que se están accesando e incluso de la información ya divulgada al usuario.

Un modelo general de control de acceso, según lo ejerce un archivo o sistema de administración de base de datos es la **matriz de acceso** ( ver fig.20a). Los elementos básicos del modelo son los siguientes :[ 2 ]

SUJETO : Una entidad capaz de accesar objetos. Por lo general , el concepto de sujeto se iguala con el proceso. Cualquier usuario o aplicación en realidad obtiene acceso a un objeto por medio de un proceso que representa a ese usuario o aplicación.

OBJETO : Todo a lo que se controla el acceso. Los ejemplos incluyen archivos, partes de archivos, programas y segmentos de memoria.

DERECHO DE ACCESO : La manera en la que un sujeto accesa un objeto. Los ejemplos son leer, escribir y ejecutar.

**FIGURA 20** Estructuras de control de acceso.

A) Matriz de acceso

| | PROGRAMA 1 | * * * | SEGMENTO A | SEGMENTO B |
|---|---|---|---|---|
| PROCESO 1 | lectura<br>ejecución | | lectura<br>escritura | |
| PROCESO2 | | | | lectura |
| *<br>*<br>* | | | | |

B) Lista de capacidades

| |
|---|
| Lista de control de acceso para el programa 1 :<br>Proceso 1 (lectura, ejecución) |
| Lista de control de acceso para el segmento A :<br>Proceso 1 (lectura, ejecución) |
| lista de control de acceso para el segmento B :<br>Proceso 2(lectura) |

C) Lista de capacidades

| Lista de capacidades para el proceso 1 :<br>Programa 1 (lectura, ejecución)<br>Segmento a (lectura, escritura) |
|---|
| Lista de capacidades para el proceso 1 :<br>Segmento b (lectura) |

Un eje de la matriz consiste en sujetos identificados que pueden intentar el acceso de datos. Por lo general, esta lista consta de usuarios individuales o grupos de usuarios, aunque el acceso puede controlarse por terminales, anfitriones o aplicaciones, en lugar de o además de usuarios.

El otro eje lista los objetos que se pueden accesar. En el nivel de detalle más grande, los objetos pueden ser campos de datos individuales. Más agrupamientos de totales, tales como registros, archivos o incluso la base de datos completa, también pueden ser objetos en la matriz. Cada entrada en la matriz indica los derechos de acceso de un sujeto para un objeto.

En la práctica, una matriz de acceso por lo general es poco densa y se implementa por descomposición, en una o dos maneras. La matriz puede descomponerse por columnas , generando **listas de control de acceso** (ver fig. 20b). Por lo tanto , para cada objeto, una lista de control de acceso muestra los usuarios y sus derechos de acceso permitidos.

La lista de control de acceso puede contener una entrada por omisión o pública. La entrada por omisión permite que tengan derechos especiales los usuarios que no están listados en forma explícita y les da un conjunto de derechos por omisión. Los elementos de la lista pueden incluir usuarios individuales y grupos de usuarios.

La descomposición por renglones da **boletos de capacidad** (ver fig.20c). Un boleto de capacidad especifica los objetos y operaciones autorizados para un usuario. Cada usuario tiene

varios boletos y puede ser autorizado con la finalidad de prestarlos y darlos a otros. Cómo los boletos pueden dispersarse por el sistema, representan un mayor problema para la seguridad que hacer listas de control de acceso. En particular, el boleto no debe olvidarse. Una manera de hacerlo inolvidable es hacer que el sistema operativo contenga todos los boletos a favor de los usuarios. Los boletos deben conservarse en una región de la memoria inaccesible para los usuarios.

Las consideraciones de red para el control de acceso orientado a datos son paralelas a las de control de acceso orientado a usuario. Si se permite sólo a ciertos usuarios accesar ciertos ítems de datos, entonces puede necesitarse el encriptado para proteger esos ítems durante la transmisión a usuarios autorizados. Por lo general, el control de acceso orientado a datos está descentralizado, esto es, lo controla el sistema de administración de bases de datos basado en la computadora principal. Si existe un servidor de la base de datos de red en el sistema, entonces el control de acceso de datos se convierte en una función de red.

## 3.3 INTRODUCCIÓN AL CIFRADO DE EXTREMO A EXTREMO

El enfoque más efectivo y más común para enfrentar las amenazas destacadas en el análisis de la fig. 21 es el encriptado. Si se usa el encriptado para enfrentar estas amenazas, entonces necesitamos decidir qué encriptar y dónde debe localizarse el mecanismo de encriptado. Como lo indica la fig. 22 existen dos alternativas fundamentales : encriptado de enlace y encriptado extremo a extremo.[ 6 ]

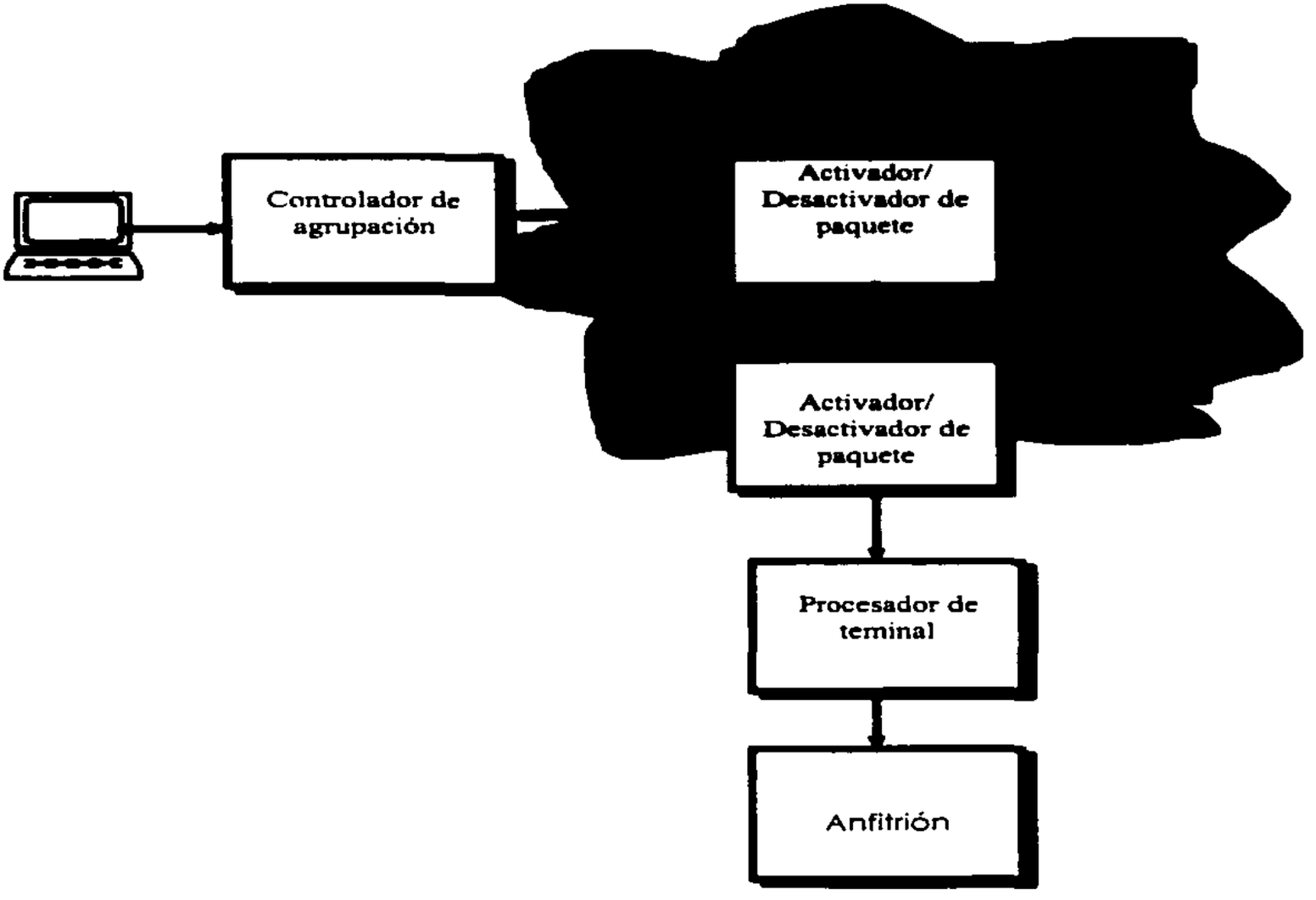
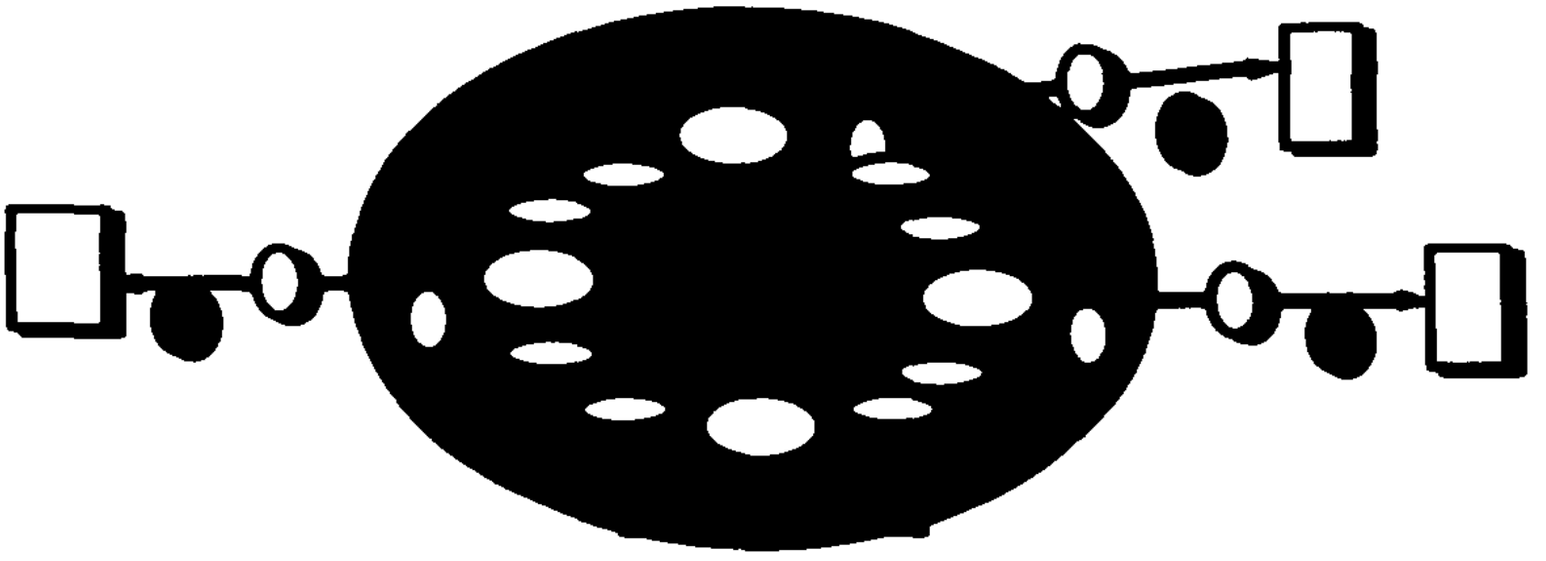



**FIGURA 21** Trayectoria física típica.



Dispositivo de encriptación de extremo a extremo

Dispositivo de encriptación de enlaces

**FIGURA 22** Encriptado por una red de conmutación de paquetes

Con el encriptado de enlace cada enlace de comunicaciones vulnerable está equipado en ambos extremos con un dispositivo de encriptado. Por lo tanto, se asegura todo el tráfico sobre todos los enlaces de comunicaciones. Aunque esto requiere una gran cantidad de dispositivos de encriptado en una red grande, el valor de este enfoque es claro.

Una desventaja es que el mensaje debe descifrarse cada vez que entra en un conmutador de paquete ; el descifrado es necesario por que el conmutador debe leer la dirección (número de circuito virtual) en el encabezado del paquete para dirigir el paquete. Por

lo tanto, el mensaje es vulnerable en cada conmutador. Si es una red pública de conmutación de paquetes, el usuario no tiene control sobre la seguridad de los nodos.

Con un encriptado extremo a extremo, el proceso de encriptado se realiza en los dos sistemas finales. La computadora principal frente o la terminal encriptan los datos. Este enfoque pareceria asegurar la transmisión contra ataques sobre los enlaces o conmutadores de la red. No obstante, todavía existen un sitio débil.

Una computadora principal conectada a una red de conmutación de paquetes, establece un circuito virtual a otra computadora principal y se encuentra preparada para transferir datos a esa otra computadora principal usando encriptado extremo a extremo. Los datos se transmiten por una red en forma de paquetes que tienen un encabezado y algunos datos de usuario. Ahora bien la computadora principal encripta el paquete completo, incluyendo el encabezado .

Esta táctica no funcionará debido a que, recuerde, sólo la otra computadora principal puede ejecutar el encriptado. El nodo de conmutación de paquetes recibirá un paquete encriptado y no será capaz de dirigir el paquete. Por lo tanto, la computadora principal puede encriptar sólo la parte del paquete que contiene los datos del usuario y debe dejar el encabezado sin encriptar para que pueda leerlo la red.

Por lo tanto, con el encriptado extremo a extremo , los datos del usuario están seguros. No obstante, el patrón de tráfico no lo está porque los encabezados del paquete se transmiten sin encriptar. Para alcanzar una mayor seguridad se necesitan el encriptado de enlace y el de extremo a extremo , como está mostrado en la fig. 22.

La fig. 23 ilustra los efectos separados y juntos de las dos formas de encriptado. Cuando se emplean ambas formas, la computadora principal encripta los datos del usuario usando una clave de encriptado extremo a extremo.

Después, el paquete completo se encripta usando una clave de encriptado de enlace. Cuando el paquete recorre la red, cada conmutador decripta el paquete usando una clave de encriptado de enlace para leer el encabezado y luego encripta el paquete completo otra vez enviándolo en el siguiente enlace. Ahora el paquete completo está seguro excepto durante el tiempo en el que el paquete está en realidad en la memoria de un conmutador de paquetes, tiempo en el cual el encabezado del paquete no está encriptado.[ 17 ]

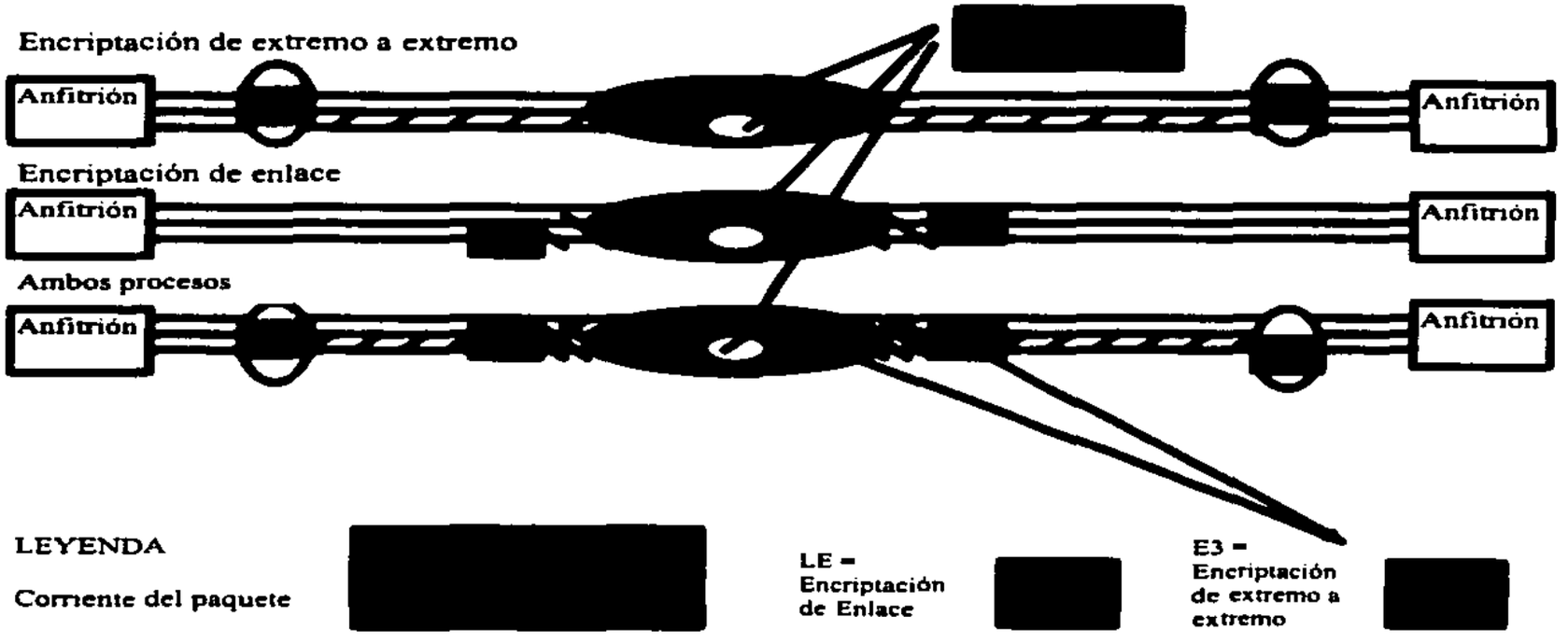



**FIGURA 23** Encriptación de extremo a extremo

## 3.4 DISTRIBUCIÓN DE CLAVES

La distribución de claves puede lograrse de varias maneras.

Para dos partes A y B :

1.- A puede elegir una clave y entregarla de manera física a B.

2.-Un tercero puede seleccionar la clave y entregarla de manera física a A y B.

3.- Si A y B han usado una clave un poco antes, una parte puede y transmitir a la otra la nueva clave, la cual ha sido encriptada usando la clave vieja.

4.- Si A y B cada una tiene una conexión encriptada a un tercero C, este puede entregar una clave por enlaces encriptados a A y B.

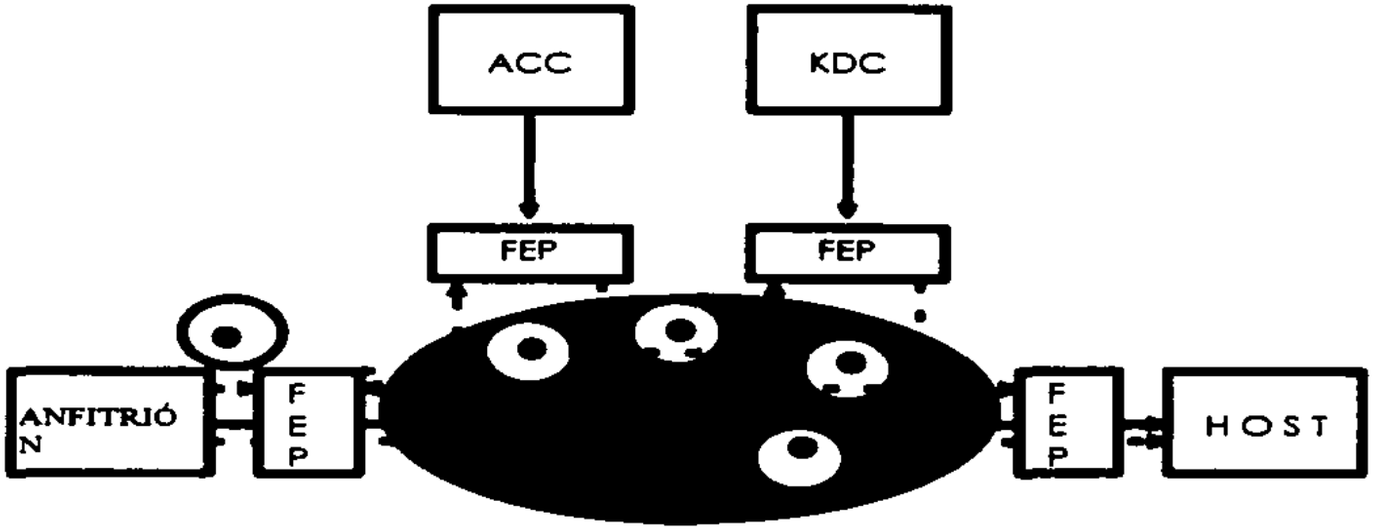
Las opciones 1 y 2 requieren la entrega manual de una clave. Para el encriptado de enlace , este es un requisito razonable debido a que cada dispositivo de encriptado de enlace va estar intercambiando datos sólo con su compañero en el otro extremo del enlace. No obstante , para encriptado extremo a extremo la entrega manual es torpe.

En un sistema distribuido, cualquier computadora principal o terminal dadas puede necesitar ocuparse en intercambios con muchas otras computadoras principales y terminales durante el tiempo. Por lo tanto, cada dispositivo necesita varias claves, proporcionadas en forma dinámica. El problema es en especial difícil en un sistema distribuido a nivel área.

La opción 3 es una posibilidad para el encriptado de enlace o el encriptado extremo a extremo, pero si un atacante tiene éxito en obtener acceso a una clave, entonces se revelan todas las claves subsecuentes. Incluso si se hacen cambios frecuentes a las claves de encriptado de enlace , deben hacerse en forma manual. Con el fin de proporcionar claves para encriptado extremo a extremo, es preferible la opción 4.

La fig. 24 ilustra una implementación que satisface la opción 4 para encriptado extremo a extremo. Se ignora el encriptado de enlace, pero puede añadirse o no, según se requiera. Para este esquema, se identifican dos clases de claves :[ 9 ]

**FIGURA 24** Encriptado extremo a extremo por una red




CLAVE DE SECCIÓN : Cuando dos sistemas extremos (computadoras principales, terminales, etc. ) desean comunicarse, establecen una conexión lógica (por ejemplo, circuito virtual) ; durante esa conexión lógica, todos los datos del usuario se encriptan con una clave de sesión única. Cuando concluye la sesión o conexión , la clave se destruye.

CLAVE PERMANENTE : Una clave permanente es una clave usada entre entidades para distribuir claves de sesión.

La configuración consiste en los siguientes elementos :

CENTRO DE CONTROL DE ACCESO : El centro de control de acceso determina a cuáles sistemas se les permite comunicarse uno con otro.

CENTRO DE DISTRIBUCIÓN DE CLAVE : Cuando el centro de control de acceso otorga el permiso para que los sistemas establezcan una conexión, el centro de distribución de clave proporciona una clave de una sesión única para esa conexión.

PROCESADOR FRONTAL : El procesador frontal (front-end processor - FEP) ejecuta un encriptado extremo a extremo y obtienen claves de sesión en favor de su computadora principal o terminal.[ 17 ]

Los pasos involucrados en establecer una conexión se muestran en la fig. 24

1.- Cuando una computadora principal desea establecer una conexión con otra, transmite un paquete de solicitud de conexión.

2.- El FEP guarda ese paquete y pide permiso al centro de control de acceso para establecer la conexión.

3.- Se encripta la comunicación entre el procesador frontal y el centro de control de acceso, usando una clave permanente compartida sólo por el centro de control de acceso y el procesador frontal. El centro de control de acceso tiene una clave única tal para cada procesador frontal y para el centro de distribución de claves. Si el centro de control de acceso aprueba la solicitud de conexión, envía un mensaje al centro de distribución de claves, pidiendo que se genere una clave de sesión.

4.- El centro de distribución de claves genera la clave de sesión y la entrega a los dos procesadores frontales apropiados ,usando una clave permanente única para cada frente.

5.- Ahora el procesador frontal que solicita puede liberar el paquete de solicitud de conexión y se establece una conexión entre los dos sistemas finales. Los respectivos procesadores frontales encriptan todos los datos del usuario intercambiados entre los dos sistemas finales usando la clave de sesión única.

La funciones de control de acceso y distribución de clave pueden combinarse en un solo sistema. La separación hace que las dos funciones reinicien y puedan proporcionar un nivel de seguridad un poco mejor. Si deseamos permitir a dos dispositivos cualesquiera comunicase a voluntad, entonces la función de control de acceso no es necesaria del todo,

cuando dos dispositivos desean establecer una conexión, uno de ellos solicita al centro de distribución de clave una clave de sesión.

Por último, las funciones que ejecutaba el procesador frontal no necesitan alojarse en un dispositivo separado sino que pueden incorporarse en el sistema de la computadora principal. La ventaja del procesador frontal es que minimiza el impacto sobre la red. Desde el punto de vista de la computadora principal, el FEP parece ser un nodo de conmutación de paquetes y no se altera la interfaz de la computadora principal a la red. Desde el punto de vista de la red, el FEP parece ser una computadora principal y no se altera la interfaz de conmutación de paquetes para la computadora principal.

El enfoque de distribución de clave automatizado proporciona flexibilidad y características dinámicas necesarias para permitir a varios usuarios terminales accesar varias computadoras principales y para que las computadoras principales intercambien datos una con otra.

## 3. 5 PROTECCIÓN DE CLAVES

El problema del manejo de claves en un sistema criptgráfico abarca la generación , distribución y protección de las claves, necesaria para que en un sistema secreto de comunicaciones, tanto el emisor como el receptor tengan garantizada la seguridad.

Propuesto por (Everton, ), el manejo de claves está basado en un principio simple según el cual, cuando una clave no puede ser físicamente protegida, se debe cifrar bajo otra clave de orden superior.

La ejecución de esto se basa en el establecimiento de una jerarquía de claves en cuya cúspide se encuentran las claves maestras, que son almacenadas en los dispositivos de cifrado (32 bits) y utilizadas para proteger el nivel siguiente inferior de claves , o claves sub - maestras. Estas, a su vez son almacenadas en los nodos, si se trata de una red y son utilizadas para proteger el nivel inmediatamente inferior de claves, que en un entorno transaccional suelen denominarse claves de sesión.

De la idea de Everton se deduce el paralelismo entre la idea jerárquica de una red de comunicaciones (ordenadores , concentradores, nodos, terminales, etc.) y la idea jerárquica de estructura del sistema de claves.

Las claves de sesión son las de más bajo nivel siendo utilizadas únicamente para proteger datos, permaneciendo activas mientras que los datos que han cifrado están en forma de criptograma, significando esto, que las claves de sesión estarán activas solamente mientras dura la sesión de comunicaciones.

Las claves maestra y submaestra son generadas por un responsable de seguridad con la ayuda eventual de un ordenador dedicado a esta tarea. Las claves maestras permanecerán en claro ya que no hay claves de nivel superior a éstas ; sirven para cifrar a las claves submaestras. Cada dispositivo de la red del sistema criptográfico debe tener su propia clave

maestra, y cada nodo, en esta visión estructurada, debe tener las claves submaestras cifradas, tanto la suma como la de los nodos con los que se comunica.

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

Como puede deducirse de este sistema, se propone el montaje de una organización con responsables de seguridad, dependiendo de ésta la correcta distribución secreta y restringida de las claves.

También sugiere que la clave maestra de cada nodo sea introducida en el dispositivo de cifrado en forma clara por el responsable correspondiente. Dicha clave debería destruirse si hay algún fallo de dispositivo o de potencia, permitiéndose reentrada. Las claves de sesión serían producidas por el logical en puntos determinados y transmitidas a los nodos al iniciarse cada sesión, siendo cifrada bajo la clave submaestra local.

Dentro del dispositivo la clave sería descifrada a su forma de presentación en claro, no existiendo ninguna manera de obtener esta clave fuera del dispositivo. Para la transmisión a los otros nodos, la clave se cifrará utilizando la clave submaestra de los nodos de destino.

En conclusión, este procedimiento de Everton es transparente al usuario final, y excepto el responsable de seguridad en cada nodo , no hay nadie que tenga que manipular las claves. Sin embargo , no se recomienda para sistemas de cifrado asimétricos. [ 9 ]

## 3.6 OPERACIONES CRIPTOGRÁFICAS BÁSICAS

***Reglas de Kerckhoffs***

Kerckhoffs, en su trabajo titulado *La Criptografía militar* , recomendó que los sistemas criptográficos cumpliesen las siguientes reglas, efectivamente han sido adoptadas por gran parte de la comunidad criptográfica :

1) No debe existir ninguna forma de recuperar mediante el criptograma el texto inicial o la clave.

Esta regla se considera cumplida siempre que la complejidad del proceso de recuperación del texto original sea suficiente para mantener la seguridad del sistema. No obstante, en muchos casos no es necesario maximizar dicha complejidad, ya que en general la seguridad máxima se paga a la hora del descifrado (principio 5) .

Por otro lado, hay que tener en cuenta la relación existente entre la tecnología y la seguridad de un sistema. Por ejemplo, muchos sistemas con un espacio de claves finito que se consideraban seguros cuando no existían los computadores, resultan ahora completamente inseguros, debido a la posibilidad del examen exhaustivo de todas las claves.

2) Todo sistema criptográfico debe estar compuesto por dos tipos de información :

- Pública, como es la familia de algoritmos que lo definen.
- Privada, como es la clave que se usa en cada cifrado particular.
- La forma de escoger la clave debe ser fácil de recordar y modificar .

3) Debe ser factible la comunicación del criptograma con los medios de transmisión habituales.

4) La complejidad del proceso de recuperación del texto original debe corresponderse con el beneficio obtenido.

El conocido como principio de Kerckhoffs dice que la seguridad de un criptosistema se mide suponiendo que el enemigo conoce completamente ambos proceso de cifrado y descifrado.[ 8 ]

## 3.7 PROTOCOLOS CRIPTOGRÁFICOS

Un algoritmo criptográfico constituye un algoritmo para llevar a cabo comunicaciones entre distintas partes, sean o no adversarios. En general, todo protocolo criptográfico incluye sucesivos intercambios de mensaje. Normalmente, para los protocolos se usan criptosistemas de clave pública.

Ahora bien, es muy difícil comprobar si la seguridad del criptosistemas particular utilizado corresponde también a la seguridad del protocolo. Intuitivamente se puede apreciar que todo protocolo debe ser tan seguro como el criprosistema subyacente, pero también puede ser menos seguro. Normalmente, los protocolos se diseñan para una utilidad específica, tal y como puede observarse en los siguientes ejemplos :[ 8 ] y [ 27 ]

### 3.7.1 ELECCIONES :

Supóngase que se quieren llevar a cabo unas elecciones a través de una Red. Un protocolo que sirva para ello debe cumplir con lo siguientes puntos :

- Prohibir a los votantes no legítimos votar, aunque sean usuarios legales de la Red
- Mantener el secreto de los voto.
- Impedir que nadie pueda votar más de una vez.
- Permitir que cualquier votante pueda verificar si su voto ha sido contabilizado.

Se supone la existencia de dos agencias que intervienen en el proceso. Una agencia X, que revisa la legitimidad de los votantes, y otra agencia Y, que calcula y pública los resultados. La agencia X elabora el conjunto N de todos los números de identificación de quienes han votado y la envía a la agencia Y, que realiza el conteo de los votos incluidos en dicho conjunto.

En esta situación, un protocolo posible para el votante A es :

***Paso1*** : A envía un mensaje a la agencia X para identificarse. Por ejemplo, "hola soy A"

***Paso2*** : Si A es un votante legítimo, X envía su número de identificación i(A) a "A" y quita a " A" de la lista de votantes. Si A no es un votante legítimo, X le en vía un mensaje de rechazo.

***Paso3*** : A escoge una identificación secreta s(A) y envía a Y la 3-UPLA (i(A), v(A), s(A)), donde v(A) es su voto.

***Paso 4*** : La agencia Y comprueba si i(A) está en el conjunto N, en cuyo caso borra i(A) de N y añade s(A) en el conjunto de votantes que han votado por v(A), en otro caso no hace nada.

***Paso 5*** : Cuando acaban las elecciones, Y calcula y publica los resultados y la lista con las identificaciones secretas de quienes han votado por cada opción.

Para añadir seguridad en los tres primeros pasos, se puede usar un criptosistema de clave pública. En ese caso, los mensajes se envía autenticados y cifrados con la clave pública de receptor.

Existe una amplia variedad de elecciones secretas que se pueden realizar usando los protocolos apropiados. Estos protocolos abren nuevos horizontes a la comunicación confidencial. (Elección con derecho a voto)

### 3.7.2 TRANSFERENCIA INCONSCIENTE :

Hay muchas situaciones posibles en las que un cifrado probabilístico es más que suficiente ; es decir, donde un usuario puede cifrar el texto de tal manera que el receptor lo pueda descifrar con una cierta probabilidad.

Supóngase que un usuario A quiere transferir un secreto a B con probabilidad de valor ½, de manera que al finalizar el procedimiento B con seguridad si ha recibido el secreto, pero

A no lo sabe. El protocolo que se requiere en ese caso se conoce por el nombre de transferencia inconsciente o trascordada (oblivius transfer), Protocolo Rabin : La transferencia inconsciente consiste en la transferencia de información en forma probabilística en cuanto a la recepción del mensaje por el destinatario, y en cuanto al conocimiento de la recepción por parte de quién envía el mensaje.

Una aplicación práctica del protocolo de transferencia inconsciente consiste en el lanzamiento de monedas que se explica a continuación.

### 3.7.3 LANZAMIENTO DE MONEDAS ( ÁGUILA O SOL ELECTRÓNICO) :

Otro uso importante de la criptografía de llave pública es el volado electrónico. El problema es el siguiente : ¿ Cómo echar un volado dos personas a través de correo electrónico, asegurando que ninguna de las partes hace trampa ?. Las dificultades son numerosas ¿ Quién arrojará la moneda ? ¿ En que momento la arroja uno y en que momento pide el otro ?. Si ya de por si este es un proceso delicado en persona imagínelo en el mundo de las comunicaciones.[ 21 ]

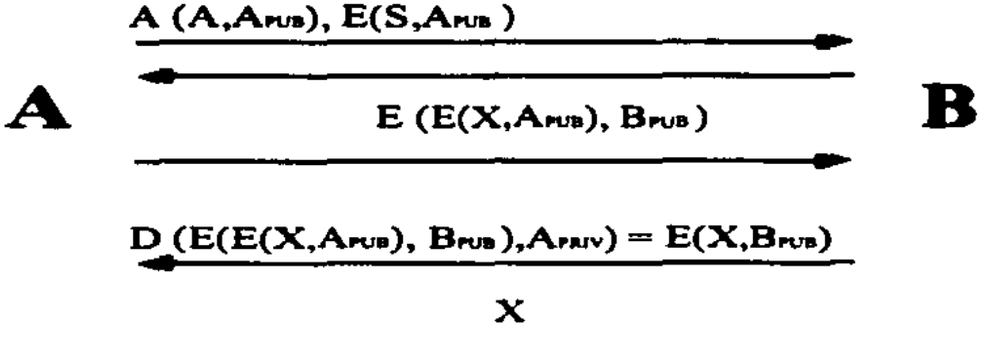



**FIGURA 25** Intercambio de mensajes (A Y B).

El protocolo debe permitir a ambos usuarios comprobar si el otro hizo trampa , existen dos posibles casos de deshonestidad :

El usuario B escoge cara y se lo dice a A. A lanza la moneda obtiene cara y sin embargo comunica " el resultado fue cruz".

El usuario A lanza la monda, B elige cruz y A comunica a B " el resultado es cara ", entonces B le replica "justo el resultado que elegí"

El protocolo funciona de la siguiente manera :

Tenemos A y B a los contendientes. Ambos generan una pareja de llaves públicas y privadas .

B genera dos mensajes, A y S ; cada uno de estos mensajes contendrá una cadena aleatoria , uno águila y el otro sol. (E)ncripa ambos con su llave pública APUB , y envía ambos [E(A,APUB, E(S,APUB)] a B .

B, quién no puede entender ninguno, elige uno al azar, encriptándolo con su llave pública BPUB y enviándolo [E(E(X,APUB), BPUB) donde X es A, o S], de regreso a A.

A, lo "desencripta" utilizando su llave privada APRIV y lo envía a B, esto produce E(Y,APRIV) donde Y es A o S.

B hace lo propio con su llave privada BPRIV, en ese momento el mensaje, efectivamente, es uno de los dos que envió inicialmente, siempre y cuando la cadena aleatoria que utilizó en la primera etapa se mantenga intacta. La fig. 25 muestra el intercambio de mensajes .

B regresa el mensaje a A y ambos intercambian sus llaves públicas y privadas, para verificar que cada mensaje que recibieron fue el correcto.

### 3.7.4 ESQUEMA UMBRAL :

Supóngase que varios usuarios desean compartir una parte de sus secretos , pero no quieren mostrarlos por completo. Éste es el caso, por ejemplo, de dos personas que quieran saber quién es más viejo sin decir las edades.

El protocolo necesario se denomina esquema umbral. Una de sus aplicaciones es la distribución de claves en los sistemas de clave pública donde la clave se divide en dos, una parte pública y otra secreta. Otra aplicación más intuitiva es el planteamiento de las llaves de las cajas de seguridad de un banco. La caja de seguridad en ningún caso se puede abrir con una sola llave, sino que deben usarse las dos de manera simultánea.

En general , cualquier esquema para la protección de información debe ser diseñado teniendo en cuenta la posible pérdida o destrucción de la información o parte de ella. Una manera de guardar la información contra la pérdida o destrucción consiste en hacer varias copias y distribuirlas entre usuarios de confianza. Esto tiene dos inconvenientes obvios. Una pequeña cantidad de copias puede causar la pérdida de la información, mientras que demasiadas copias puede ocasionar que caiga en malas manos.

El esquema umbral, la información se divide en piezas que se distribuyen entre usuarios de confianza, de forma que cuando se reúnan un número fijo y no menos , se logra reconstruir la información. El termino reconstruir de la información se puede reemplazar por *arranque de un programa, acceso a un sistema*, etc.[ 9 ]

### 3.7.5 DEMOSTRACIÓN DE CONOCIMIENTO NULO :

Si una persona A conoce cierta información secreta y debe convencer a una segunda persona B de que posee dicha información, pero sin revelarle absolutamente nada sobre ella, entonces puede usar un protocolo específico conocido como demostración de conocimiento nulo.

Este protocolo debe cumplir las siguientes propiedades :

a) A no puede engañar a B, ya que si en realidad no posee la información entonces la probabilidad de convencer a B es falsa.

b) B no recibe ninguna información a partir de la demostración, salvo la certeza de su existencia.

La idea crucial para la construcción de un protocolo que resuelva este problema y cumpla ambas propiedades es que el protocolo se debe comportar como una caja cerrada : B no puede abrirla porque A tiene la llave y A, se compromete a no modificar el contenido de la caja cuando la abre para enseñárselo a B. Introducir información en la caja significa en términos de criptografía de clave pública, aplicarla para abrir la caja, pero el usuario B no puede.

Este tipo de protocolos resulta muy útil en muchos y variados casos donde la información a esconder es susceptible de copia.

Por ejemplo , si un usuario debe identificarse para acceder a algún servicio. Si para hacerlo debe comunicar su número de identificación y éste puede ser interceptado por un enemigo que puede usarlo más tarde para hacerle pasar por él. Una solución a este problema estaría en que el usuario utilizase un protocolo para las demostraciones de conocimiento nulo, convenciendo de que tiene dicho número sin revelar absolutamente nada de él.[ 8 ]

Ahora bien, algunas de estas aplicaciones están siendo investigadas en forma teórica actualmente, y todavía ni siquiera se han desarrollado de forma práctica, Sin embargo con los avances tecnológicos muchos de estos protocolos en desarrollo acabarán resultándonos familiares en el futuro.

# CAPÍTULO 4

# CASO PRÁCTICO

# 4 CASO PRÁCTICO

## GIRO DE LA EMPRESA :

Emisión y Venta de Vales para : Despensa, Auto y Restaurante

## INTRODUCCIÓN :

El código de barras tiene gran utilidad en la administración de productos dentro de la empresa . Desde que la empresa se ha desarrollado en forma importante a demandando una mayor eficiencia del control del movimiento de sus productos, por lo cual se ha requerido enumerar, codificar e identificar los productos que se comercializan.

El crecimiento de la empresa conjuntamente con el comercio ha requerido que el uso de los códigos utilizados para el control de los productos se vuelvan cada vez más complicados, por lo que, para lograr un entendimiento entre las diversas sucursales, se requiere adoptar un código que sea estándar para todas.

Para entender el cómo y el porqué de la adopción de un código de producto estándar pasemos a ver lo que es propiamente el código de barras, qué tipo de información puede representar, los tipos de código que existen y la manera de interpretación de los mismos.

La presente propuesta es el resultado de diversos estudios de evaluación por el personal del área de sistemas, los cuales tienen como fundamento el ser objetivos ante los lineamientos marcados por la Dirección de Operaciones de la empresa, definidos dichos lineamientos en términos de considerar la situación actual y futura de la misma.

# 4.1 CÓDIGO DE BARRAS

## ¿QUE ES EL CÓDIGO DE BARRAS ?

Propiamente el código de barras es la forma de representar información que contiene números u otros caracteres haciendo uso de una secuencia de barras paralelas, claras y obscuras, anchas y estrechas, las cuales son leídas por medio de equipos de lectura óptica.

La información escrita mediante el código de barras puede ser la identificación de un producto (aplicación común para el sector industrial y comercial), código de acceso a algún área (usando como reloj checador o sistemas de seguridad), o cualquier otro dato para ser ingresado a una computadora.

La alta confiabilidad de los datos leídos y enviados a la computadora, gracias a que la lectura se hace por medio electrónico y no por medios manuales los cuales tienen un alto porcentaje de error.

La lectura de la información codificada, es rápida y automática ya que se hace por medio de lectores ópticos que envían directamente la información a la computadora o bien almacenan en algún dispositivo para después procesarla.

Cada carácter es compuesto de barras paralelas y la interpretación que hacen los lectores no dependen de la relación entre lo largo y ancho que esta sean sino de la relación entre las barras anchas y estrechas , claras y obscuras.

La información escrita mediante el código de barras puede ser utilizada en una gran variedad de aplicaciones, pero principalmente se utiliza en tres sectores :

- Automatización comercial.
- Control de inventarios.
-Sistemas de control de acceso, asistencias y productividad.

Existen varios patrones internacionales referentes al código de barras, por lo tanto, cuando se piensa en implantar un sistema donde los datos colectados se basen en este tipo de código, es necesario tomar en consideración algunos factores como :

- El tipo de dato que se va a manejar, ya sea numérico o alfanumérico, así como la cantidad de caracteres que éste contenga.

- El medio o material en el que serán impresos los datos codificados, el cual deberá tener una resistencia, durabilidad, propiedades mecánicas y ópticas consistentes con el equipo de lectura que se piense utilizar.

- Los métodos de impresión disponible para el dato codificado. La técnica de impresión utilizada debe ser capaz de generar códigos dentro de las tolerancias de anchura de las barras y de las propiedades ópticas del sistema. Un software capaz de generar los códigos e imprimirlos en una impresora láser sobre papel común , para posteriormente ser leídos por el dispositivo de control de acceso y registro de asistencia. Esto lógicamente permite al cliente una gran autonomía en la generación de documentos con código de barras.

- El espacio disponible donde fisicamente será puesto el código de barras. Se debe tener en cuenta que todo código de barras requiere de marcas de START y STOP, de una zona de silencio inicial (Zsi) y una zona de silencio final (ZSf) antes y después de los datos codificados. Las zonas de silencio generalmente son un múltiplo de la anchura de un elemento angosto, son áreas que obligatoriamente deben estar libres de impresión y que anteceden y siguen a las marcas de START y STOP.

Para seguir hablando de estos códigos será conveniente aclarar los siguientes términos, comúnmente usados cuando se trata el tema de código de barras :

**Barra :** se refiere a una barra de color obscuro , ya sea ancha o angosta.

**Espacio :** se refiere propiamente a una barra clara ya sea ancha o estrecha.

**Elemento :** hace referencia a cualquier elemento integrante del código sin importar si es una barra o un espacio.

## 4.2 RENDIMIENTO DE UN SISTEMA DE CÓDIGO DE BARRAS

El rendimiento de un sistema de código de barras se describe en términos de dos parámetros :

- El de tasa de lectura
- El de tasa de error

El parámetro de tasa de lectura es definida como el número de lecturas con error y el número de lecturas sin error. Un buen sistema debe ofrecer una tasa de lectura aproximada del 80% ; una tasa de lectura baja es causada generalmente por problemas de impresión o bien por problemas de operación en el que la persona que maneja el lector no lo posiciona correctamente para que se puedan leer los datos codificados.

También existe la posibilidad de que la baja de tasa de lectura se deba a que el lector esté sucio, y sólo bastará con limpiarlo, en el peor de los casos la tasa de lectura baja se puede deber a imperfecciones del dispositivo lector, como mala calibración del mismo, por lo que será necesario llevarlo con su proveedor para que se encargue de repararlo o sustituirlo.

El segundo parámetro para evaluar el rendimiento de un sistema de código de barras es el de tasa de error de sustitución ocurre cuando todos los caracteres codificados son leídos o interpretados como si fuesen otros completamente distintos. La tasa de error de sustitución depende directamente de la estructura del patrón de códigos de barras adoptado, de la calidad de impresión y del algoritmo de decodificación que se programe.

Si el sistema de colección de datos no cuenta con alguna forma de tratamiento de estos datos corrompidos (rechazados) entonces aceptará un dato inválido. Un buen sistema de código de barras debe ofrecer una tasa de error de sustitución de alrededor de un carácter mal interpretado por cada millón de caracteres leídos.

## 4.3 LECTURA DEL CÓDIGO DE BARRAS

Aunque existen diversos modelos de lectores ópticos para códigos de barras, todos trabajan en base al mismo principio de funcionamiento, el cual consiste en emitir y sensar la luz.

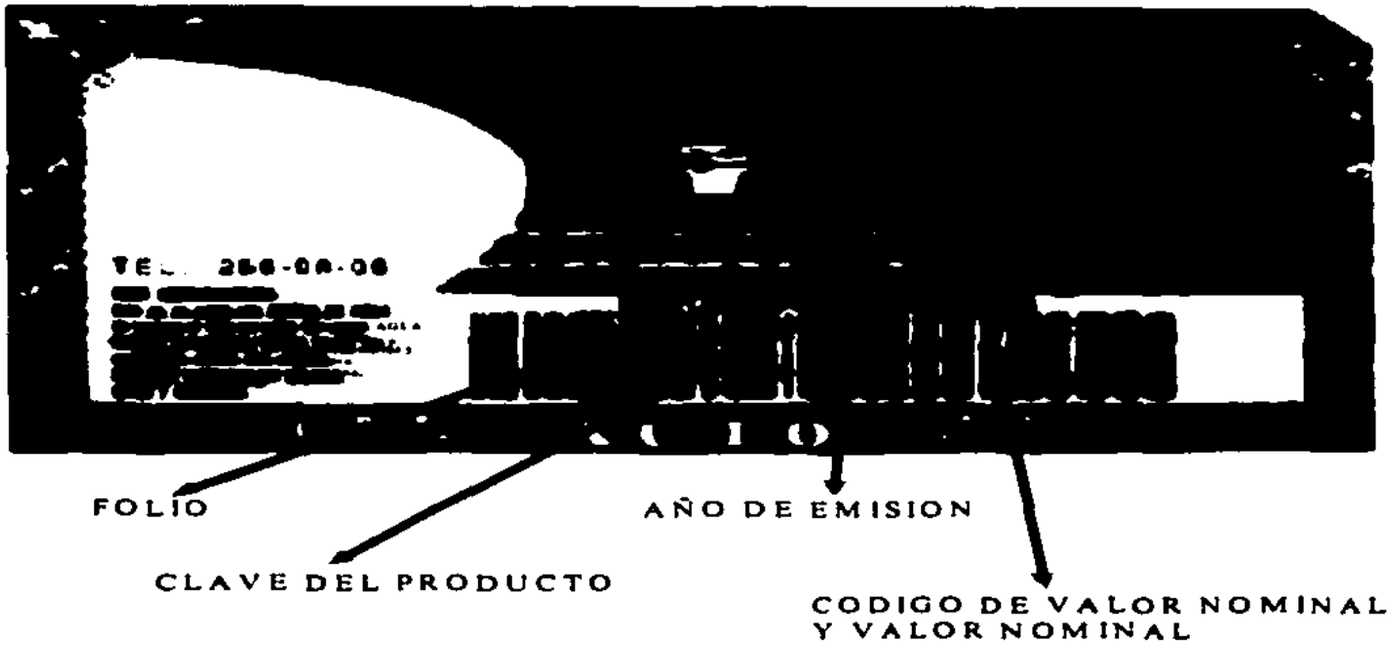
Es importante que haya una gran diferencia entre los índices de reflexión de la barras y los espacios ya que para sensar la luz emitida por un medio, ésta debe ser reflejada por las barras y espacios , y si éstos no tienen diferentes índices de reflexión la lectura será incorrecta. Los códigos de barra pueden ser divididos en dos grupos ; los de contacto y los de no - contacto. Entre los lectores de contacto encontramos lectores de baja capacidad y de alta capacidad.

Los lectores de contacto de baja capacidad presentan como fuente un emisor de luz, un LED y como sensor un foto - receptor. Estos equipos requieren que el código sea pesado directamente sobre ellos ya que la luz emitida por el LED tiene una baja intensidad.

Los lectores de contacto de alta capacidad, también conocidos como CCD (Charge Coupled Device) presentan varios LEDs y fotosensores dispuestos matricialmente que requieren cubrir toda el área que ocupa el dato codificado iluminándolo completamente para que la luminosidad reflejada por las barras y espacios sensibilice a todos los fotosensores.

Por otro lado, los lectores de "no - contacto" poseen tecnología bastante sofisticada basada en un rayo láser y una serie de lentes y espejos ; son ideales para supermercados y para quienes requieren un aparato capaz de leer los código en movimiento. Con esto el operador no necesita mayores cuidados en el manejo de la mercancía para que su código sea leído, basta con que pase la mercancía sobre el lector.

## 4.4 ESTRUCTURA DEL VALE




A cada vale se le asigna un número de 20 dígitos llamados prefijos. De los cuales se desglosan de la siguiente manera :

**FOLIO :** Se compone de los 8 primeros digitos (Empezando el conteo de izquierda a derecha) .

**DÍGITO VERIFICADOR :** El que va junto al folio numérico abajo del valor nominal y tiene como función asegurar la correcta lectura de los primeros 8 dígitos.

**PRODUCTO :** La clave que identifica el producto, el cuál ocupa las posiciones 9 y 10.

**EMISIÓN :** El año en que se emite el vale, el cuál ocupa las posiciones 11 y 12.

**CÓDIGO DEL VALOR :** Código del valor normal, el cual ocupa las posiciones 13 y 14.

**VALOR :** El valor normal del vale, el cual ocupa las posiciones 15, 16, 17, 18, 19, 20

## 4.5 APLICACIÓN :

### ENCRIPTACIÓN DE VALORES EN EL CÓDIGO DE BARRAS PARA LA PROTECCIÓN DEL VALE.

### 4.5.1 PROCEDIMIENTO PARA GENERAR EL ENCRIPTADO DEL VALOR Y CÓDIGO DEL VALOR PARA LA EMISIÓN 1997.

***PASO 1 :*** Se aplica un método numérico

***PASO 2:*** Se adoptan cuatro claves dentro de las formulas a utilizar, las cuales son proporcionadas por la empresa.
CLAVES FIJAS: 182,15,11,23

***PASO 3:*** Desglosar el prefijo:

FOLIO, PRODUCTO, EMISIÓN, CÓDIGO DEL VALOR, VALOR

*Ejemplo:*

PREFIJO: 021783091697120020000 (Valores asignados al código de barras del vale).

FOLIO= 02178309

PRODUCTO = 16

EMISIÓN = 97

CÓDIGO DEL VALOR = 12

VALOR = $20.00

**NOTA :** No tomar en cuenta los último dos valores "00" (0020"00"), en donde las cuatros cifras significativas siguientes van a enmarcar el valor del vale que representa, en este caso vamos a utilizar el valor de $20.00(0020).

***PASO 4:*** **Asignar una variable, por cada número que conforma el folio (empezando de izquierda a derecha).**

*Ejemplo:*

| A8 | A7 | A6 | A5 | A4 | A3 | A2 | A1 |
|---|---|---|---|---|---|---|---|
| 0 | 2 | 1 | 7 | 8 | 3 | 0 | 9 |

***PASO 5:*** **Comprobación del "dígito verificador":**

Formula 1:

SUMA_FOLIO=(A1*2)+(A2*3)+(A3*4)+(A4*5)+(A5*6)+(A6*7)+(A7*2)+(A8*3)

SUMA_FOLIO= (9 * 2)+(0* 3)+(3 *4)+(8* 5)+(7 *6)+(1 *7)+(2* 2)+(0* 3)
SUMA_FOLIO= 18 + 0 + 12 + 40 + 42 + 7 + 4 + 0
SUMA_FOLIO= **123**

Formula 2:

VERIFICA = SUMA_FOLIO = INT (SUMA_FOLIO/11) * 11

VERIFICA = 123 - INT (123/11) * 11
VERIFICA = 123 - (11 * 11)
VERIFICA =123 -121
VERIFICA =**2**

Formula 3:

DÍGITO_VERIFICADOR = 11 – VERIFICA

DÍGITO_VERIFICADOR = 11 - 2

DÍGITO_VERIFICADOR = **9**

Observamos que el dígito verificador corresponde a la última cifra del folio, descrita en el paso 4 y que corresponde a la variable A1.

***PASO 6*: Generar el valor encriptado (valor nominal del vale)**

Formula:

VALOR_ENCRIPTADO=VALOR*10 +A1*182+15+A2+A3+A4+A5+A6+A7+A8

VALOR_ENCRIPTADO =20 * 10 + 9 * 182 + 15 + 0 + 3 + 8 + 7 + 1 + 2 + 0

VALOR_ENCRIPTADO =**1874**



***PASO 7*:Generar el código de valor encriptado (código del valor nominal)**

Formula:

CÓDIGO_VALOR_ENCRIPTADO =CÓDIGO_VALOR + 23 + A1 + A2 -
DÍGITO_VERIFICADOR

CÓDIGO_VALOR_ENCRIPTADO = 12+23+9+0-9

CÓDIGO_VALOR_ENCRIPTADO = 35

### 4.5.2 PROCEDIMIENTO PARA EL DESCIFRADO DE LOS VALORES ENCRIPTADOS

***PASO 1:*** Realiza la lectura del código de barras ,por medio de un dispositivo óptico (Lectoras de vales).

***PASO 2:*** Desglosar el prefijo:

FOLIO, PRODUCTO, EMISIÓN, CÓDIGO DEL VALOR ENCRIPTADO, VALOR ENCRIPTADO

*Ejemplo:*
PREFIJO: 021783091697350018 74

FOLIO= 02178309
PRODUCTO = 16
EMISIÓN = 97
CÓDIGO DEL VALOR ENCRIPTADO = 35
VALOR ENCRIPTADO = 1874 (001874)

***PASO 3:*** Asignar una variable, por cada número que conforma el folio (empezando de izquierda a derecha).

*Ejemplo:*

| A8 | A7 | A6 | A5 | A4 | A3 | A2 | A1 |
|---|---|---|---|---|---|---|---|
| 0 | 2 | 1 | 7 | 8 | 3 | 0 | 9 |

***PASO 4:*** Comprobar el "digito verificador":

Formula 1:

SUMA_FOLIO = (A1*2) +(A2 *3) (A3*4) +(A4 *5)+ (A5*6) +(A6 *7)+ (A7*2) +(A8 *3)

Formula 2:

VERIFICA = SUMA_FOLIO = INT (SUMA_FOLIO/11) * 11

Formula 3:

DÍGITO_VERIFICADOR= 11 - VERIFICA

**NOTA:** Se realiza el mismo procedimiento que en el paso 5 del método de encriptación

***PASO 5:*** Descifra el valor encriptado (valor nominal del vale)

Formula:

VALOR =VALOR_ENCRIPTADO- A1*182 -1 5- A2 -A3- A4 - A5 - A6 - A7 - A8

VALOR =1874 - 9 * 182 - 15 - 0 - 3 - 8 - 7 - 1 - 2 - 0

VALOR =200*10 (002000)

VALOR=**2000**

***PASO 6:***Descifrar el código del valor encriptado (código del valor nominal)

Formula:

CÓDIGO_VALOR = CÓDIGO_VALOR_ENCRIPTADO -23 -A1-A2+
DÍGITO_VERIFICADOR[3]

CÓDIGO_VALOR =35 - 23 - 9 - 0 + 9

CÓDIGO_VALOR =**12**

## 4.5.3 CÓDIGO PARA GENERAR ENCRIPTADO EN VALOR Y CÓDIGO DEL VALOR PARA LA EMISIÓN 97 (LENGUAJE : QBASIC)

**Prefijo : 0217830916971200200 2**

| SIGNIFICADO | TAMAÑO | ASIGNACION DE VALORES | DESCRIPCIÓN |
|---|---|---|---|
| FOLIO | 8(incluye dígito verificador) | 02178309 | No. de folio |
| DÍGITO VERIFICADOR | 1 | 9 | Dígito verificador |
| PRODUCTO | 2 | 16 | clave del producto |
| EMISIÓN | 2 | 97 | año en que se emite el vale |
| CÓDIGO DEL VALOR | 2 | 12 | código de valor normal |
| VALOR | 6 | 002000 | valor normal del vale |
| CÓDIGO DEL VALOR ENCRIPTADO | 2 | 35 | código del valor encriptado |
| VALOR ENCRIPTADO | 6 | 001874 | valor encriptado |

## CIFRADO

```
**********
INICIA BLOQUE
**********
REM <<<--- rutina para generar encriptado en valor y código del valor para la emisión 1997 --->>>
<<<ENCRIPTADO>>>
```

**d$ = 0217830916971200200 && se toma este prefijo para prueba**

CONSTANTES : 182,15,23,11

- xValor$ = 20
- xcodval$ = 12
- n%=2178309 && un valor cualquiera de inicio
- o%=1 && contador del rango deseado a producir
- proemix$ = 1697 && clave del producto + año de emisión del vale

```
t = TRUE
WHILE t
foliox$ = tran ( n."99999999")
valorx% = xValor% *10
codvalx% = xcodval%
```

```
a$ = foliox$
veri% = 0
xx% = 0
bx% = 0

a1x% = VAL(MID$(a$, 8, 1)) * 2
a2x% = VAL(MID$(a$, 7, 1)) * 3
a3x% = VAL(MID$(a$, 6, 1)) * 4
a4x% = VAL(MID$(a$, 5, 1)) * 5
a5x% = VAL(MID$(a$, 4, 1)) * 6
a6x% = VAL(MID$(a$, 3, 1)) * 7
a7x% = VAL(MID$(a$, 2, 1)) * 2
a8x% = VAL(MID$(a$, 1, 1)) * 3
bx% = a1x% + a2x% + a3x% + a4x% + a5x% + a6x% + a7x% + a8x%
t = TRUE
WHILE t
  IF bx% < 11 THEN
     veri% = 11 - bx%
     t = false
  ELSE
     xx% = bx% - INT(bx% / 11) * 11
     IF xx% = 1 THEN
            veri% = 0
            t = false
     ELSEIF xx% = 0 THEN
            veri% = 1
            t = false
     END IF
     bx% = xx%
  END IF
WEND

dverifica% = tran (veri%,"9")
a1x% = VAL(MID$(a$, 8, 1))
a2x% = VAL(MID$(a$, 7, 1))
```

```
a3x% = VAL(MID$(a$, 6, 1))
a4x% = VAL(MID$(a$, 5, 1))
a5x% = VAL(MID$(a$, 4, 1))
a6x% = VAL(MID$(a$, 3, 1))
a7x% = VAL(MID$(a$, 2, 1))
a8x% = VAL(MID$(a$, 1, 1))

vencripta% = valorx% + a1x% * 182 + 15 + a2x% + a3x% + a4x% + a5x% + a6x% + a7x% + a8x%
codvalencr% = codvalx% + 23 + a1x% + a2x% - veri%

Vencritax$ = LTRIM$(STR$(vencrpta%))
codvalencrx$ = LTRIM$(STR$(codvalencr%))

SELECT CASE LEN(codvalencrx$)
 CASE 1: codvalencrx$ = "0" + codvalecrx$
END SELECT

SELECT CASE LEN(Vencrptax$)
 CASE 1: Vencriptax$ = "0000" + Vencriptax$
 CASE 2: Vencriptax$ = "000" + Vencriptax$
 CASE 3: Vencriptax$ = "00" + Vencriptax$
 CASE 4: Vencriptax$ = "0" + Vencriptax$
END SELECT
REM  RESULTADO FINAL
 d$ = foLiox$ + proemix$ + codvalencrx$ + Vencriptax$
n% = n% +1
o% = o% +1
IF o% > 100 THEN     && en este caso se hace la prueba con 100 folios
   EXIT
END IF
WEND
**********
NOTA :   los valores 182, 23,15,11 son claves que se emplearon para realizar el encriptado.
FIN DEL BLOQUE
**********
```

## 4.5.4 CÓDIGO PARA DESCIFRAR EL VALOR Y CÓDIGO DEL VALOR PARA LA EMISIÓN 97 (LENGUAJE : QBASIC)

### DESCIFRADO

```
***************
INICIA BLOQUE
***************
REM <<<--- inicia verificación de folios emitidos, realiza el descifrado--->>> <<<ENCRIPTADO>>>
d$ = MID$(lectura_vale$,1,20)  &&  Simula la lectura del vale
proemix$ = MID$(d$, 9, 4)      &&  clave del producto + emisión
foLiox$ = MID$(d$, 1, 8)       &&  folio
Valorx$ = MID$(d$, 15, 5)      &&  valor nominal
IF (proemix$ = "1697" AND foLiox$ >= "02149000") OR proemix$ = "1897" OR (proemix$ = "1597" AND
foLiox$ >= "01545449") THEN
veri% = 0
xx% = 0
bx% = 0
a1x% = VAL(MID$(foLiox$, 8, 1)) * 2
a2x% = VAL(MID$(foLiox$, 7, 1)) * 3
a3x% = VAL(MID$(foLiox$, 6, 1)) * 4
a4x% = VAL(MID$(foLiox$, 5, 1)) * 5
a5x% = VAL(MID$(foLiox$, 4, 1)) * 6
a6x% = VAL(MID$(foLiox$, 3, 1)) * 7
a7x% = VAL(MID$(foLiox$, 2, 1)) * 2
a8x% = VAL(MID$(foLiox$, 1, 1)) * 3
bx% = a1x% + a2x% + a3x% + a4x% + a5x% + a6x% + a7x% + a8x%
t = TRUE
WHILE t
  IF bx% < 11 THEN
     veri% = 11 - bx%
     t = false
  ELSE
     xx% = bx% - INT(bx% / 11) * 11
     IF xx% = 1 THEN
            veri% = 0
```

```
            t = false
        ELSEIF xx% = 0 THEN
            veri% = 1
            t = false
        END IF
        bx% = xx%
    END IF
WEND
a1x% = VAL(MID$(foLiox$, 8, 1))
a2x% = VAL(MID$(foLiox$, 7, 1))
a3x% = VAL(MID$(foLiox$, 6, 1))
a4x% = VAL(MID$(foLiox$, 5, 1))
a5x% = VAL(MID$(foLiox$, 4, 1))
a6x% = VAL(MID$(foLiox$, 3, 1))
a7x% = VAL(MID$(foLiox$, 2, 1))
a8x% = VAL(MID$(foLiox$, 1, 1))
valencrix% = VAL(MID$(d$, 15, 6))
digencrix% = VAL(MID$(d$, 13, 2))
cvalorx% = digencrix% - 23 - a1x% - a2x% + veri%
valor% = valencrix% - a1x% * 182 - 15 - a2x% - a3x% - a4x% - a5x% - a6x% - a7x% - a8x%
Valorx$ = LTRIM$(STR$(valor%))
covalorx$ = LTRIM$(STR$(cvalorx%))
SELECT CASE LEN(covalorx$)
 CASE 1: covalorx$ = "0" + covalorx$
END SELECT
SELECT CASE LEN(Valorx$)
 CASE 1: Valorx$ = "0000" + Valorx$
 CASE 2: Valorx$ = "000" + Valorx$
 CASE 3: Valorx$ = "00" + Valorx$
 CASE 4: Valorx$ = "0" + Valorx$
END SELECT
 d$ = foLiox$ + proemix$ + covalorx$ + Valorx$ + "0"
END IF
*****************
NOTA :  los valores 182, 23,15,11 son claves que se emplearon para realizar el encriptado.
FIN DEL BLOQUE
```

## 4.6 ESQUEMA REPRESENTATIVO DEL CIFRADO Y DESCIFRADO

**PREFIJO = 021783091697120020000**

### *CIFRADO*

| FOLIO | PRODUCTO | EMISIÓN | CÓDIGO DEL VALOR ENCRIPTADO | VALOR ENCRIPTADO |
|---|---|---|---|---|
| 02178309 | 16 | 97 | 35 | 001874 |
| 02178309 | 16 | 97 | 12 | 002000 |

| FOLIO | PRODUCTO | EMISIÓN | CÓDIGO DEL VALOR | VALOR |
|---|---|---|---|---|

### *DESCIFRADO*

# CONCLUSIÓN

Las redes de computadoras presentan múltiples problemas de seguridad debido a su naturaleza multiusuaria.

La parte más débil en cuanto a seguridad de una red son las conexiones de comunicaciones. Esto implica a todos los tipos de redes, por lo que la mayoría de las precauciones que deben aplicarse en una red LAN, se aplican para las demás.

Un sistema completo de seguridad de LAN incluye :

- Un sistema de disponibilidad para asegurar que los equipos informáticos de una red están listos para ser usados por los usuarios autorizados.

- Un sistema de control de acceso que permita que los datos restringidos sean usados únicamente por personas autorizadas.

- Un sistema de integridad que protege contra la modificación de datos ya sea accidentalmente ó intencionalmente.

Por otro lado :

- La protección se debe basar en métodos de seguridad lógica implementadas en hardware o software, ya que estos tipos de procesamiento da poder de computo a muchos sitios remotos.

- Los sistemas se deben plasmar en métodos de identificación y autentificación.

- La seguridad depende mucho de los usuarios de los sistemas computacionales. Estos adquieren conciencia de la importancia de la seguridad ; tienen más facilidad para aceptar y aplicar las medidas de seguridad sugeridas, obteniendo un mayor conocimiento sobre las técnicas criptográficas que pueden aplicar ellos mismos, para incrementar la seguridad del sistema y un optimo rendimiento en el mismo.

La criptografía es una herramienta básica que se usa en muchas aplicaciones de seguridad.

Históricamente, el estudio y la aplicación de la criptografía ha estado casi exclusivamente en manos militares y diplomáticos. Sin embargo, en la sociedad actual ha surgido la necesidad de la criptografía *civil*, debido a la utilización de gran cantidad de información (personal, financiera, comercial y tecnológica) que se almacena en bancos de datos y se transmite a través de redes de computadoras.

Las aplicaciones de la criptografía han aumentado progresivamente, hasta alcanzar muchas otras áreas donde los sistemas de comunicación tienen un papel vital. Cada vez con mayor frecuencia se pueden encontrar grandes redes de usuarios en las que es necesario que dos cualesquiera sean capaces de mantener secretas sus comunicaciones entre sí. Sin embargo, el intercambio continuo de claves no es una solución eficiente.

Hoy en día la criptografía moderna tiene otras aplicaciones, no sólo, el establecimiento de la comunicaciones seguras sobre canales inseguros, sino también: la autentificación, que más que una simple aplicación representa la segunda utilidad principal de la criptografía ; las firmas digitales y la aplicación criptográfica en la identificación de usuarios (passwords-contraseñas).

Los principales problemas que surgen al utilizar la criptografía para la protección de una red son :

- La gestión de las claves y

- Los protocolos a usar.

El problema de la gestión de la clave en un sistema criptográfico incluye la generación, almacenamiento , distribución y mantenimiento de las claves necesarias para que el sistema tenga garantizada la seguridad. El problema radica principalmente en sistemas de clave secreta (simétricos), porque los cuatro procesos se tienen que realizar constantemente . Para esto se recomienda utilizar generadores de secuencias aleatorias.

Por otro lado , los protocolos se diseñan para una utilidad específica.

La criptografía (Encriptamiento) ofrece una resistencia técnica muy efectiva. Sin embargo , la utilización de sistemas de encriptamiento avanzado puede llegar a considerarse ilegal.

Las medidas efectivas de seguridad consisten en un adecuado equilibrio entre la tecnología y la administración de los sistemas.

# BIBLIOGRAFÍA

[ 1 ] A. Curry David, UNIX System Security
Ed. México: Addison Wesley, 1994 -- 720p -- (Informática)

[ 2 ] A. Menascé Daniel, Redes de computadoras :Aspectos Técnicos y Operacionales
Ed. México :Paraninfo, 1994.--168p -- (Informática)

[ 3 ] black Uyless, Redes de Computadoras: Protocolos, Normas e Interfaces
Ed. México: Macrobit Editores, 1995 -- 421p-- (Informática)

[ 4 ] Ettinger J.E, Informtion Security
Ed. Chapman Hall,1993 -- 195p -- (Informática)

[ 5 ] H. Fine Leonard, Seguridad en centros de computo :Políticas y Procedimientos
Ed. México :Trillas, 1997 -- 130p -- (Informática)

[ 6 ] Neil Willis, Fundamentos de arquitectura de ordenadores y comunicaciones de datos
Ed. México: Anaya Multimedia, 1990 -- 303p, -- (Informática)

[ 7 ] C.P. PEELEGER, Security in Computing
Ed. México :Prentice-Hall,1994 -- 320p -- (Informática)

[ 8 ] Pino Caballero, Seguridad Informática: Técnicas Criptográficas
Ed. México : Alfaomega, 1997--133p-- (Informática)

[ 9 ] Rodríguez Prieto, Protección de la información : Diseño de Criptosistemas Informáticos,
Ed. México :Paraninfo, 1995.--255p -- (Informática)

[ 10 ] Rodríguez L. Angel, Seguridad en redes
Ed. México: Ventura, 1995 -- 353p -- (Informática)

[ 11 ] Salas P. Jesus, Organización de los servicios Informáticos
Ed. México :McGraw-Hill, 1994 -- 280p -- (Informática)

[ 12 ] Santifaller Michael, TCP/IP and ONC/NFS
Ed. Addison- Wesley, 1994 -- 288p -- (Informática)

[ 13 ] S. Tanenbaum Andrew, Sistemas Operativos Modernos
Ed. México: Prentice-Hall, 1996 -- 859p -- (Informática)

[ 14 ] S. Tanenbaum Andrew, Redes de Ordenadores
Ed. México: Prentice-Hall, 1991 -- 759p -- (Informática)

[ 15 ] Silberschatz Abraham, Sistemas Operativos
Ed. México : Addison Wesley, 1994 -- 780p-- (Informática)

[ 16 ] Siyan Karanjil, Internet y Seguridad en Redes
Ed. México: Prentice-Hall, 1995 -- 407p -- (Informática)

[ 17 ] Stallings William, Sistemas Operativos
Ed. México : Megabyte, 1995 -- 845p-- (Informática)

[ 18 ] Van TILBORG, H.C.A, An Introduciión to Criptology
Ed. Kluwer Academic Plubishers, 1993 -- 355p -- (Criptografía)

**Direcciones de documentos en Internet :**

[ 19 ] http ://www.victoria.upf.tche.br/computacao/leandro/histo.html*
[ 20 ] http ://www.victoria.upf.tche.br/computacao/leandro/simetri.html*
[ 21 ] http ://www.reidgroup.com/~dmg/tejiendo/neta7.html*
[ 22 ] http ://www.visao.com.br/people/aver/ucsintro.htm*
[ 23 ] http ://www.visao.com.br/people/aver/ucstradi.htm*
[ 24 ] http ://www.di.uminho.pt/~jmv/htmls/Criptografia/Criptografy*
[ 25 ] http ://www.victoria.upf.tche.br/computacao/leandro/sigilo.html*
[ 26 ] http ://www.di.uminho.pt/~jmv/htmls/Criptografia/programa.html*
[ 27 ] http ://www.cs.hut.fi/ssh/crypto/algoritms.html*
[ 28 ] http ://www.itr.ch.ch :800/~pheinzma/quantli.html*

* Dentro de cada documento se encuentran otras direcciones el cuál puedes accesar.