UNIVERSIDAD DEL VALLE DE GUATEMALA

Facultad de Ciencias y Humanidades

IMPLEMENTACION DE UN SISTEMA CRIPTOGRAFICO EN UN COMPUTADOR PERSONAL

ASTRID MARIA LLERENA GALVEZ

Guatemala

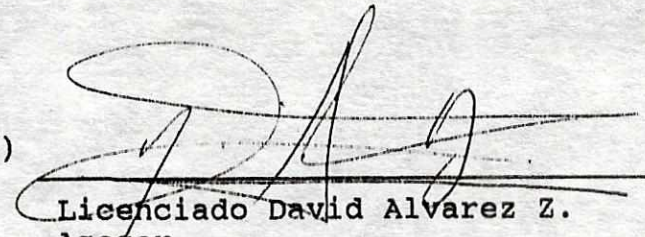
1989

IMPLEMENTACION DE UN SISTEMA CRIPTOGRAFICO EN UN COMPUTADOR PERSONAL

Trabajo presentado para optar el grado académico de

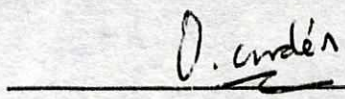
INGENIERA EN CIENCIAS DE LA COMPUTACION

Vo. Bo. :

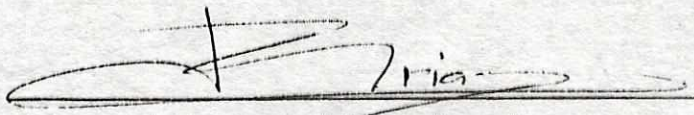
(f) 

Licenciado David Alvarez Z.
Asesor

Tribunal:

(f) 

Licenciado Luis Octavio Cordón

(f) 

Licenciado Rodrigo Arias P.

(f) 

Ingeniero Luis Furlán

Fecha de aprobación: 8 de noviembre de 1989

Al Creador,
Por darme la vida

A mi madre,
Ligia Gálvez de Llerena
Por su amor, dedicación y esfuerzo

A mis hermanos:
Mildred, Ingrid y Enio Llerena Gálvez
por su apoyo y cariño

A mis profesores
Por compartir sus conocimientos y
Dedicarse a una profesión tan noble

A mis amigos

INDICE DEL CONTENIDO

LISTA DE TABLAS Y GRAFICAS

RESUMEN

En el presente trabajo se combinan dos técnicas de seguridad para implementar el sistema para un computador personal. La primera de ellas es la criptografía, la cual se incorpora al sistema operativo para detectar cualquier acceso a disco. La segunda, verificación de la identidad, pertenece a un campo relativamente nuevo en computación y fue investigada para determinar las variaciones y semejanzas de un ser humano a otro, y poder determinar los parámetros con los cuales se reconocería a un usuario válido. A partir de estos puntos, se diseña e implementa el sistema criptográfico que se muestra a continuación.

I. INTRODUCCION

En la actualidad, existen varias redes que interconectan computadores personales. De una u otra forma, los sistemas operativos para dichas redes han brindado apoyo a la seguridad de los dispositivos que se comparten; algunos de los métodos más comunes para proporcionarla son los sistemas de passwords, listas de control de acceso, y audit trails, entre otros. Sin embargo, si el computador es utilizado sin hacer uso de la red o bien, se posee solamente un computador, la información en el disco duro (si lo posee) o la de los diskettes queda indefensa.

Por otra parte, el encriptamiento se ha utilizado ampliamente en seguridad; sin embargo, su mayor aplicación ha sido en la transmisión de datos (telecomunicaciones) y ningún programa se ha incorporado al sistema operativo de un computador personal para intervenir la lectura o escritura de los datos y encriptarlos a la vez, de forma tal, que dicho proceso sea "invisible para el usuario". Con el presente proyecto se persigue hacer un programa que haga posible lo anterior.

Objetivos:

Para el sistema criptográfico que se propone, intervendrá el sistema operativo para que cada acceso a disco sea reconocido (lectura y escritura en especial), en cuyos casos se usarán medidas de encriptación para la protección de los datos.

Este proceso permitirá que los datos fueran decodificados en una forma adecuada para aquella persona que conoce la "palabra clave" de los datos deseados. Las ventajas de ésto sobre otros métodos usados residen en:

- El usuario no se percata del proceso de encriptamiento/decriptamiento durante las escrituras/lecturas al disco.

- La palabra clave para utilizar cada archivo puede ser distinta o la misma, según lo decida el usuario, y puede ser modificada en cualquier momento sin interrumpir el proceso en el cual se encuentra (a excepción de una lectura o escritura a disco)

- A diferencia de los passwords o las listas de acceso, la "palabra clave" no se guarda dentro del disco donde se encuentran los datos.

El presente sistema incorporará una característica personalizada durante el ingreso de la clave. Cada individuo

posee un estilo y una cierta velocidad en mecanografía; debido a ello, se podría reconocer si es la persona adecuada quien desea accesar el archivo. Ello evitará que terceras personas con conocimiento de la clave, puedan utilizar o modificar los datos.

Para realizar lo anterior, una parte del programa a implementar será dedicada a familiarizarse con el estilo propio del individuo al teclear su clave. Se le requerirá al usuario ingresar la clave un número adecuado de veces (por ejemplo, doce) y a partir de los tiempos promedios entre tecla y tecla, se podrá estimar el tiempo esperado de tecleado. Esto será utilizado posteriormente para aceptar o rechazar el acceso a los archivos, con lo cual se incrementará la seguridad proporcionada por el sistema de criptografía.

II. DEFINICIONES BASICAS

A. Información:

La importancia de la información y la forma en la cual sea empleada, conduce al deseo de protegerla y proporcionarla a un número limitado de personas. Por otra parte, el computador ha brindado una gran capacidad de almacenamiento de datos; sin embargo, si no se les da la seguridad apropiada a éstos, podrían llegar a manos de personas inescrupulosas, quienes utilicen en forma no apropiada la información brindada por dichos datos.

La administración de la información se interesa por el almacenamiento y recuperación de los datos confiados al sistema. Sus funciones básicas se describen a continuación.

1. Registrar toda la información dentro del sistema. Ello lo realiza utilizando distintas tablas, siendo la principal el archivo de directorio. El contenido de estas tablas se basa en el nombre, localización y derechos de acceso a la información.

2. Elección de la política usada para determinar las posiciones y forma de almacenar la información. Algunos factores decisivos sobre dicha política son: uso

eficiente del almacenamiento secundario, acceso eficiente, flexibilidad a los usuarios, y protección a los privilegios de acceso de la información requerida.

3. Asignación de los recursos de información: Si se permite que un proceso accese la información, se deberá localizarla, hacerla disponible y establecer los derechos de acceso apropiados.

4. Liberación de un recurso: cuando la información deja de ser requerida, se deben liberar los recursos utilizados. Si el usuario modificó la información, la copia original de ésta deberá ser actualizada para su uso posterior. (Madnick: 337)

La información representa uno de los recursos más importantes del sistema operativo y tal vez, uno de los más pobremente tratados en sistemas contemporáneos (Madnick: 337); sin embargo, en los últimos años, el interés en su protección se ha visto incrementado.

B. Seguridad:

La seguridad de los datos es la ciencia y estudio de los métodos de protección de los mismos dentro de la computadora y sistemas de comunicación. Ella se encuentra íntimamente ligada a la administración de la información, esquemas

de control del derecho de acceso y protección, así como procedimientos de backup y recuperación. (Denn : 7)

La seguridad implica la proteción contra la destrucción de los sistemas y su contenido. Entre los elementos que contempla para tal objeto son: confiabilidad, la integridad y la protección de los datos. El primero de ellos, tiene como objetivo aumentar la probabilidad de que el sistema haga lo que se le indca. La integridad pretende conservar la consistencia de los datos en el computador. El tercer elemento es explicado con más detalle, ya que es el principal punto de interés para el presente trabajo.

C. Protección:

La protección a la información consiste en comprender, organizar y controlar el acceso a los datos de acuerdo con derechos específicos (Wiederhold: 642).

Un buen mecanismo de protección impedirá que un usuario interfiera con los otros usuarios, ya sea por ineficiencia, uso incorrecto o bien desautorizado del computador. Además, proveerá las herramientas para resguardar programas y datos propios contra sí mismo. (Tsichritzis : 148)

Además de la protección descrita con anterioridad, existen otros tipos de protección, por ejemplo, el

mecanismo de protección de un procesador inhibe las referencias efectuadas por un programa, a partes de la memoria fuera del rango asignado al mismo; ello previene daños al sistema operativo u otros programas de aplicación que comparten la memoria con dicho programa. (Lorin :13)

III. ESQUEMAS DE PROTECCION

A. A nivel de hardware

Usualmente, los esquemas a nivel de hardware se utilizan para asegurar el funcionamiento adecuado de los sistemas operativos y controlar el acceso a los programas y datos dentro del computador. Este tipo de protección posee un costo superior al implementado en software; sin embargo, a criterio de algunos expertos, brindan más seguridad.

Los sistemas más conocidos, a nivel hardware, hasta el momento, incluyen:

1. Control de acceso:

Un tablero con un "chip" EPROM interrumpe el sistema cuando éste se inicia ("boot") con el objeto de permitir el acceso sólo a usuarios válidos. La forma de identificación consiste en el nombre del individuo y una llave que lo identifica, los cuales son almacenados en dicho "chip".

2. Encriptamiento:

El encriptamiento por medio del hardware está formado por un microprocesador, el cual almacena las llaves, y un dispositivo de decodificación, el que

dirección de memoria, la llave del programa se compara a la llave del bloque deseado, lo cual permitirá o evitará el acceso a dicho bloque.

3. Combinación de los mecanismos de direccionamiento con los de protección:

Se utiliza un arreglo (array) asociativo, llamado MAP. Este representa la distribución de direcciones del programa en posiciones físicas de memoria. Cualquier programa puede referenciar sólo aquellas partes de la memoria presentes en la tabla MAP. A su vez, esta tabla contiene tres bits llamados RWE, los cuales definen el tipo de acceso permitido a un área de memoria: dependiendo del estado de estos bits, un programa adquiere los privilegios de lectura (Read), escritura (Write) y/o ejecución (Ejecución).

B. A nivel de software

La implementación de un esquema de protección se puede realizar por medio de una colección de programas y estructuras de datos, los cuales aportan un mecanismo protector. (Tsich :154) El programa principal encargado de dicha seguridad en un computador es el sistema operativo.

1. Sistemas Operativos

Madnick y Donovan (1986: 1-3) definen un sistema

operativo como el conjunto de programas dentro del computador cuya función es controlar los recursos del equipo, tales como procesadores, almacenamiento principal y secundario, dispositivos de entrada y salida, y a los archivos. Estos programas actúan como una interfase entre los programas del usuario y el hardware del computador.

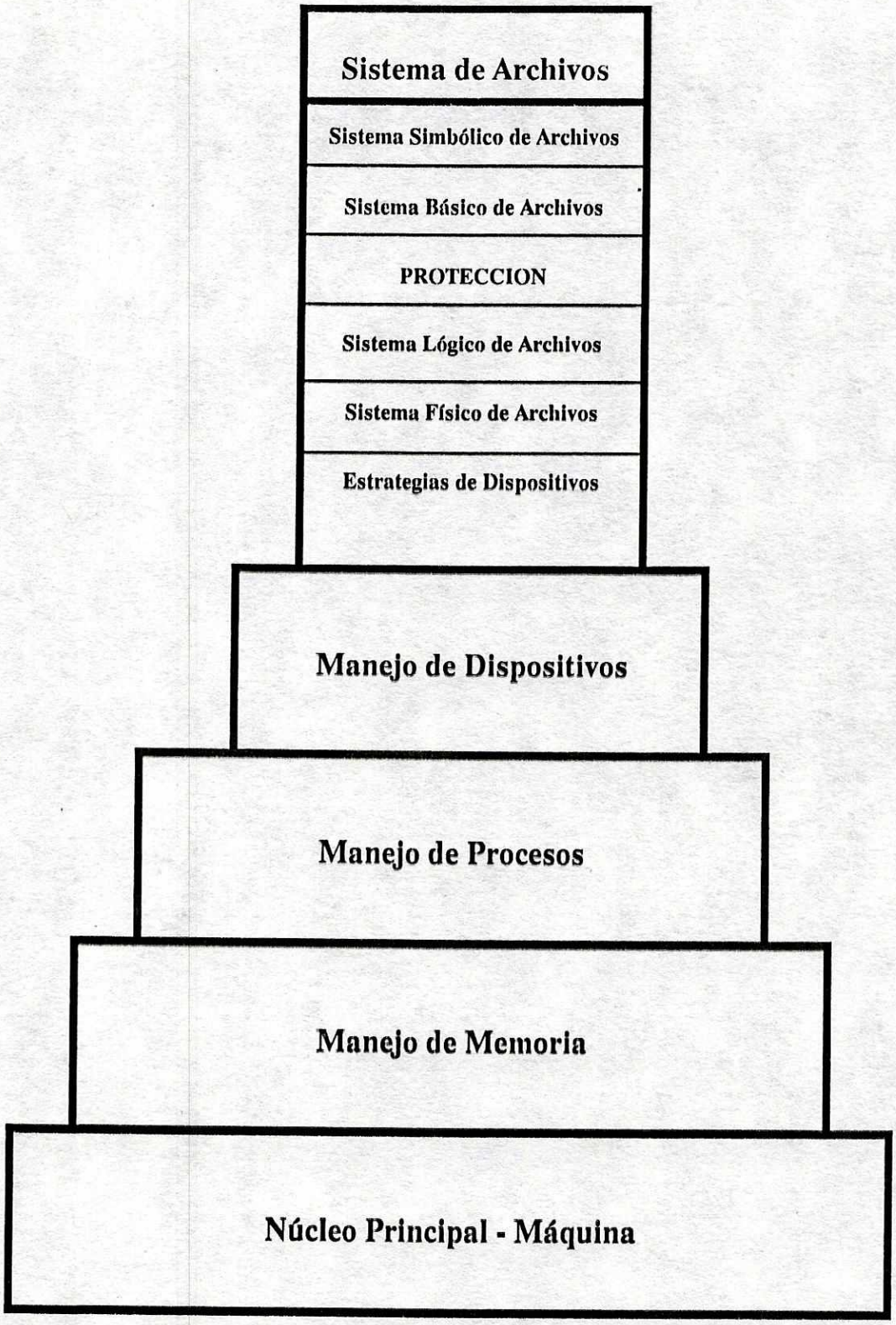
En pocas palabras, el sistema operativo es aquel programa que controla la operación de la computadora y como tal, interviene en el grado de seguridad que pueda brindar al usuario.

2. Influencia de los sistemas de protección en el diseño de un Sistema Operativo

Los conceptos de dirección de memoria, privilegios, protección, manejo de interrupciones y microprogramación afectan las decisiones del diseñador en lo referente a las funciones y estructuras más apropiadas para el sistema y su hardware. (Lorin :96)

Madnick y Donovan (86:337) muestran la base de un sistema operativo, la cual se ilustra en la Fig. 1.

Se debe hacer notar que en el presente diseño cada nivel depende sólo de los niveles bajo él, y, por tanto, puede realizar llamadas sólo a ellos (Madnick y Donovan



KERNEL DEL SISTEMA OPERATIVO

86:338). El punto de interés en la figura anterior es el sistema de archivos, el cual se propone permitir al programador preocuparse solamente por la estructura lógica y operaciones realizadas para procesar su información. A su vez, deberá facilitar el compartimiento de la información entre los usuarios y la protección de ésta de accesos no autorizados. (Madnick y Donovan 86: 338-339).

3. Seguridad en el sistema operativo del computador personal:

El sistema operativo DOS (Disk Operating System) se encuentra en la mayor parte de computadores personales, los cuales se basan en la familia de los microprocesadores 8086 de Intel. Este sistema ha ido evolucionando poco a poco; en su primer versión (1981) incluye el acceso aleatorio o secuencial a un archivo, así como la información sobre sus atributos (distingue entre archivos escondidos y del sistema) y otros datos relacionados a él (fecha y hora de la última modificación, tamaño medido en bytes). La segunda versión del DOS (1983) introduce una estructura jerárquica en el manejo de los archivos, así como su poder para utilizar discos duros.

El DOS fue un sistema operativo diseñado para atender a un sólo usuario; por tanto, no verifica la autenticidad del usuario ni distingue entre un usuario y otro. Así también,

se caracteriza porque es fácil de conocer y utilizar; pero carece de un sistema de protección. Todo ello permite el acceso, sin mayor dificultad, de un intruso dentro del computador. Si bien se incluyeron características como jerarquía de los archivos y la posibilidad de tener archivos escondidos, existen programas dedicados a descubrir la estructura del disco y los archivos dentro de él, se encuentren o no, escondidos; por tanto, ello no podría ser utilizado como una medida de seguridad apropiada.

En los últimos años, ha proliferado la tendencia hacia los programas amigables y ello no se ha excluido de los usados en los computadores personales. Sin embargo, este tipo de programas representan un gran peligro en lo que a seguridad se refiere: los sistemas amigables dan paso al uso inadecuado del software. La máquina, como se ha mencionado anteriormente, es incapaz de reconocer la validez del usuario: de la misma forma en que ayudan a conducir al usuario durante el uso del computador, así guiarán al intruso.

C. Ventajas comunes a las técnicas de seguridad:

1. Las medidas de seguridad incorporadas al sistema acelerarán su aplicación y estimularán su uso; pues de otra forma se requerirá mucho tiempo y el sistema de seguridad se podría convertir en una herramienta inútil.

2. Las técnicas de seguridad pueden reforzar el uso de otras medidas y no precisamente ser redundantes.

3. Su operación, usualmente, es automática. Con ello, quien las utilice no deberá realizar ninguna otra operación que requiera esfuerzo adicional para obtener seguridad.

D. Posibles dificultades en un sistema de seguridad:

1. Obtener un falso sentido de seguridad: puede ser que la técnica de seguridad aplicada no sea la más apropiada.

2. Interferencia de la medida de seguridad tomada en el uso eficiente de la computadora: ello se podrá notar en sistemas de password, cuyo ingreso permite la lectura de la clave en pantalla o bien en un método de encriptamiento lento.

3. Un dispositivo de seguridad es capaz de proteger sólo aquella parte del sistema en la cual fue instalado. Las otras partes carecerán de protección, como sucede en el caso de líneas de comunicación y terminales remotas, entre otras.

4. Vulnerabilidad de los dispositivos incorporados: un individuo que conoce el funcionamiento de un determinado dispositivo es capaz de modificarlo a su conveniencia. Percatarse de una usurpación de este tipo podría darse hasta que los daños ocasionados fueren considerables.

IV. CONTROL SOBRE LA VERIFICACION DE ACCESO

Los controles de acceso aseguran que todos los accesos directos a los objetos dentro del sistema estén autorizados; por tanto, proporcionarán protección contra amenazas a la secretividad, autenticidad y disponiblidad del sistema (Estos conceptos se presentan más adelante, en la sección de requerimientos criptográficos).

La efectividad de un control de acceso se basa en:

1. Adecuada identificación del usuario: ninguno podrá adquirir los derechos de acceso de otro.

2. La información relacionada a los derechos de acceso de un usuario o un programa, está protegida de posibles modificaciones causadas por personal no autorizado.

Al considerar los dos requerimientos anteriores, se podrá asumir que el control de acceso será útil para los propósitos de protección.

Existen varias técnicas para establecer el control de los derechos de acceso en un sistema, entre los cuales figuran: matriz de control de acceso, passwords y criptografía.

La matriz de control de acceso consiste en una matriz bidimensional, en la cual una de las dimensiones lista todos los usuarios de la computadora y la otra, todos los archivos dentro del sistema. Cada entrada de la matriz indica el tipo de acceso que posee un usuario sobre un archivo. El módulo de ACV compara la petición de acceso a la permitida al archivo: si las mismas no concuerdan, no se permitirá el acceso. (Madnick y Donovan 86: 356)

Conceptualmente, este método es sencillo; pero posee ciertas desventajas. La principal de ellas la presenta el exceso de espacio requerido para almacenar todos los usuarios y archivos dentro del sistema.

Una variación a esta técnica obviará el problema: el uso de una lista identificará los archivos, los usuarios y el tipo de acceso de ellos a un determinado archivo (Madnick y Donovan 86:356). Las listas poseen, sin embargo, una desventaja también: su mantenimiento es complejo, ya que la extensión de cada lista puede variar.

Ambos métodos poseen el inconveniente de existir dentro del sistema que les utiliza, dando así lugar a permitir su acceso si un programador es lo suficientemente astuto. (Madnick y Donovan 86:357)

Se debe hacer notar, que solamente el dueño de un

programa está autorizado para modificar, crear o destruir los privilegios que proporcionen el acceso a su programa o datos. En otras palabras, se debe satisfacer el principio de "Atenuación de Privilegio", el cual establece que un proceso no podrá incrementar nunca sus derechos o transferirlos si no los posee. (Denn :197)

En el sistema de passwords se asocia a cada archivo una clave: cuando un usuario requiera acceso a un archivo deberá proporcionar el password para éste.

La ventaja de esta técnica es el ahorro de espacio, ya que el necesario para la protección del archivo será fija y mínima. Sin embargo, posee varias desventajas como la dificultad para realizar cambios en el control de acceso; un programador deshonesto puede obtener los passwords, ya que al igual que los dos métodos anteriores, las claves se almacenan dentro el sistema. (Madnick y Donovan 86:357)

Se deberá considerar también el factor humano al usar este método, pues la seguridad de los sistemas de passsword se basan en la integridad y disciplina de quienes poseen el password.

V. CRIPTOGRAFIA

A. Definiciones

La criptografía se refiere a la ciencia y estudio de la escritura secreta. El encriptamiento y decriptamiento son controlados por una llave o varias de ellas. (Denn :1) El encriptamiento se refiere a la trasformación que se efectúa sobre un texto para codificarlo. El decriptamiento es el método por medio del cual se transforma el mensaje codificado al texto original. Debe notarse que el decriptamiento es el proceso utilizado por un usuario lícito; criptoanálisis describe la acción de un intruso para romper un mensaje codificado.

Un "cipher" es el método secreto de escritura. Los tipos más comunes son los de transposición y sustitución. Un "cipher" de transposición rearregla los bits o caracteres en los datos, concordando con un esquema dado. Una forma de realizar lo anterior se muestra a continuación:

```
                    S   U   D
SEGURIDAD  --->     E   R   A     --->  SUDERAGID
                    G   I   D

Palabra          Método de          Palabra
Original         Transposición      Codificada
```

La llave del "cipher" estará dada por la profundidad deseada para la codificación; en el ejemplo anterior era de 3.

Los "ciphers" de sustitución reemplazan los bits, caracteres o conjunto de ellos con substitutos. Un tipo simple de ello es aquel que mueve la letra dentro del alfabeto n posiciones, donde n es la llave. (Denn :2) Por ejemplo, si n=3, y se aplica a la palabra SEGURIDAD, la nueva expresión será:

VHJXULGDG

La mayoría de "ciphers" se basan en composiciones de los métodos de substitución y transposición; de forma tal que se incremente la dificultad de violar el sistema de seguridad. Un ejemplo de ello, lo presentan los "ciphers" de producto (Denn :90).

B. Componentes de un sistema criptográfico:

Un sistema de este tipo se compone de:

1. Un espacio para el texto del mensaje original, M
2. Un espacio para el mensaje codificado, C
3. Un espacio para la llave, K
4. Una familia de transformaciones de encriptamiento

$$E_k : M \rightarrow C, \text{ donde } k \in K$$

5. Una familia de transformaciones de decriptamiento

$$D_k : C \rightarrow M, \text{ donde } k \in K$$

TABLA 5.1

Ejemplos de algunos ciphers basados en

Transposición

Cipher de permutación	Cipher de transposición columnar
Consiste en permutar los caracteres del texto con un período fijo "d" de acuerdo a una función "f".	El mensaje original se escribirá en una matriz por filas; se toman las columnas de dicha matriz en un orden específico.
Sea el período de 4 caracteres y la función f(i), donde "i" representa la posición de un caracter, dada por: f(1) = 2; f(2) = 4; f(3) = 1; f(4) =3	Sea el orden de las columnas 3-2-4-1 y la matriz: S E G U R I D A D
EUSGIARDD	GDEIUASRD

C. Requerimientos de un sistema criptográfico:

Un sistema criptográfico debe cumplir con ciertos requisitos, entre los cuales están:

1. La transformaciones de codificación y decodificación deben ser eficientes para todas las llaves:

Los datos deben ser encriptados y decriptados cuando se transmiten, almacenan o recuperan de disco, y estas operaciones no deberán representar cuellos de botella.

2. Facilidad para usar el sistema:

Debe ser fácil encontrar una llave con transformación inversa.

3. La seguridad del sistema dependerá solamente de la secretividad (se define en el siguiente párrafo) de las llaves y no sobre la secretividad de los algoritmos usados para codificar (C) o decodificar (D): si se conoce la llave K, no deberá ser posible determinar C o D a partir de ella.

La secretividad requiere que un criptoanalista sea incapaz de determinar los datos del texto original de un mensaje codificado. Para ello debe cumplir:

a. Debe ser imposible para un criptoanalista,

determinar la transformación de decodificación Dk de un texto encriptado, incluso si se conoce el texto original M.

b. Debe ser computacionalmente imposible para un criptoanalista determinar sistemáticamente el texto original M de un mensaje C encriptado e interceptado.

La secretividad sólo necesita que la transformación Dk sea protegida. La transformación Ek puede revelarse, siempre y cuando no revele Dk. (Denn: 8-9)

La autenticidad de los datos requiere que un criptoanalista sea incapaz de substituir un mensaje encriptado falso C' para un mensaje C, sin que ello deje de ser detectado. Para ello deberá cumplir con:

a. Debe ser computacionalmente imposible para un criptoanalista determinar sistemáticamente la transformación de encriptamiento Ek dado C, incluso si conoce el texto original M.

b. Debe ser computacionalmente imposible para un criptoanalista encontrar en forma sistemática el texto encriptado C', de tal modo que $d_k(C')$ sea un texto válido en el conjunto M.

La autenticidad requiere solamente que la

transformación Ek (la llave de encriptamiento) sea protegida. La transformación Dk puede ser revelada si no proporciona a Ek. (Denn :9-10)

Las propiedades anteriores, secretividad y autenticidad, se deberán cumplir para proteger completamente un sistema computacional o la comunicación de datos.

D. Ventajas de sistemas criptográficos

Entre las principales ventajas de la criptografía se encuentran:

La llave no se encuentra almacenada en el sistema; ello evitará que un intruso con derecho de acceso al sistema, logre obtenerla y utilizarla para usar un archivo.

Protege un mensaje contra la modificación o inserción de palabras al imposibilitar que un individuo produzca código que se pueda decriptar, produciendo información lógica.

Si los datos se extraen del computador, incluso estarán codificados y continuarán protegidos de este modo.

E. Desventajas de sistemas criptográficos

La principal desventaja está relacionada al costo medido en tiempo para codificar y decodificar un archivo, pues

éste es mayor que el utilizado para las otras técnicas de protección. (Madnick y Donovan 86:358)

Si se utiliza la criptografía como un método aislado de seguridad, posee la incapacidad de impedir la destrucción de los datos.

Esta técnica no se ha incorporado al computador como un método invisible al usuario; por tanto, requiere tiempo extra para utilizarlo.

Si se olvida la clave de un archivo, los datos que éste contenía no se pueden recuperar. Sin embargo, esta desventaja es válida en los sistemas implementados en software.

VI. LOS ATRIBUTOS PERSONALES Y LA SEGURIDAD

A. Verificación de la identidad:

La verificación de los atributos personales en los sistemas de computación es un campo relativamente nuevo y que se encuentra en desarrollo.

Los avances en la tecnología y el bajo costo que han alcanzado los procesadores, así como los métodos de reconocimiento de patrones, han permitido el desarrollo de técnicas dedicadas a comprobar la identidad de un individuo basándose en sus atributos personales.

Obtener los datos exactos que caracterizan a una persona es una tarea difícil, ya que se deberán establecer los puntos de referencia y los patrones exactos que determinan la identidad del individuo y ésto podría variar dependiendo del estado de ánimo del humano (triste o alegre), de los cambios provocados por el medio ambiente que lo rodea (frío o caliente) o tal vez, se encuentre lo suficientemente nervioso porque los datos son requeridos con urgencia. Esta falta de precisión en las repeticiones debe ser un factor importante cuando se pruebe y evalúe un sistema sobre verificación de la identidad.

Durante el proceso de verificación de la identidad se pueden cometer dos tipos de errores: rechazar a un usuario válido o bien, aceptar a un impostor. Sin embargo, ninguno de estos errores será deseable y por tanto, la probabilidad de cometerlos deberá tratar de ser mínima. Con tal objeto, se define un margen de tolerancia en la exactitud de los datos obtenidos. El dispositivo encargado de la verificación realizará varias mediciones del atributo, procesará los datos y comparará los resultados con un archivo maestro (el cual posee la descripción del atributo); si los datos medidos concuerdan con los del archivo, tomando en cuenta el margen de tolerancia, entonces se podrá considerar como verificada la identidad del individuo y se aceptará su ingreso y uso del computador; de otro modo, el acceso será denegado.

Algunos de los atributos personales considerados hasta el momento, se describirán a continuación.

B. Atributos personales considerados en la actualidad

Cada persona se distingue de las otras por su tamaño, color de tez, cabello, forma de caminar o de vestir. En fin, existe un amplio número de características que describen a cada persona y nos dan capacidad de referirnos a ella por medio de su nombre. Sin embargo, para el computador no será tan fácil reconocer al individuo por muchos de estos detalles y por ello, se han buscado las formas más accesibles para

000471-468

UNIVERSIDAD DEL VALLE DE GUATEMALA
Biblioteca

No. 3

CLASIFICACION: Te U VE Comp L 64 1989

AUTOR: Llerena Gálvez, Astrid María

TITULO: Implementación de un sistema criptográfico en un ~~computador personal~~

COAUTOR:

PAIS: Guatemala : UVG

FECHA: 1989 p.: 72 il. X

cm.

Tesis(licenciatura en ciencias de la computación)-- Universidad del Valle de Guatemala, Facultad de Ciencias y Humanidades

Bibliografía:

MATERIAS:

1. Microcomputadores
2. Criptografía
3. Sistemas de almacenamiento y recuperación de información

I. t.

II. Facultad de Ciencias y Humanidades, Depto. de Ciencias de la computación.

identificar al humano. Algunas de las más usadas se presentan a continuación.

1. Huellas digitales

Esta técnica es una de las más utilizadas en la verificación de la identidad y por tanto, es una de las más conocidas. Las huellas digitales se basan en "minutiae"; este término se refiere a las líneas y bifurcaciones en el dedo que puedan ser identificadas. Estas pueden ser descritas por un sistema de coordenadas (X - Y) en el cual se distinguirán el número y posición de los minutiae, así como el ángulo de las bifurcaciones. Las huellas se almacenarán en un archivo con el cual, posteriormente, se comparará la impresión digital de quien requiera el ingreso al computador; este tipo de medida varía muy poco.

2. Firma (forma de escribir)

Firmar es un reflejo condicionado; es decir, no es una actividad consciente. A ello se debe, que aunque se pueda falsificar la firma de otra persona (lo cual requerirá de un control consciente), no se pueden imitar sus reflejos y su estilo de escritura. Los estudios realizados sobre las señales eléctricas derivadas del proceso de escritura han demostrado que cada persona posee características distintas tales como

la posición, la fuerza ejercida y la aceleración mostradas al momento de escribir. Con el objeto de medir tales atributos se han desarrollado nuevos dispositivos como la superficie en la cual se escribe o bien, el instrumento usado para ello. Dichos dispositivos deberán medir tanto las posiciones dentro de la firma, tanto como el tiempo en cada una de ellas. Se deberá, por tanto, tener cuidado en tales mediciones, pues la velocidad y la aceleración pueden variar.

VII. DISEÑO E IMPLEMENTACION DE UN SISTEMA CRIPTOGRAFICO

A. Definición del sistema

El presente programa sustituye algunas rutinas del sistema operativo MS-DOS/PC-DOS con el objeto de verificar la identidad del usuario y encriptar los datos almacenados en el computador personal. Para lograr lo primero, se reemplaza la rutina del teclado para advertir la presencia de las teclas que activarán el ingreso del password (Shift F10). Durante dicho ingreso se obtendrán los tiempos entre tecla y tecla (de acuerdo a los ticks del reloj, 18.2 por segundo), lo cual se usará durante el acceso a un archivo: si los tiempos son similares al promedio de tiempos obtenidos durante la creación del archivo, el acceso será perimitido; de otra forma, denegado.

Si se autoriza el uso del archivo, la rutina de lectura realizará el acceso a disco y se efectuará el decriptamiento de los datos. En caso contrario, simplemente se presentarán espacios en blanco al usuario, como si eso fuera la información.

Durante la escritura a un archivo se hará un procedimiento similar al de la lectura: si el acceso es

válido, se encriptarán los datos y se escribirán normalmente a disco; en caso contrario, se evitará la escritura para inhibir posibles daños al archivo.

Los nombres de los archivos encriptados y el tiempo promedio del ingreso de sus respectivas llaves, son almacenados en un archivo dentro del disco. Ello permitirá la verificación de la identidad y la distinción de aquellos archivos que sé encuentren encriptados para tomar las medidas correspondientes. Si un archivo no se encuentra encriptado se invocarán las antiguas rutinas del sistema operativo.

B. Objetivos

1. Generales

a. Dar un soporte técnico a todos aquellos individuos que hacen uso de computadores personales y desean proteger sus datos.

b. Incrementar la privacidad de la información en sistemas personales.

2. Particulares

a. Incorporar un sistema de criptografía al sistema

operativo de un computador personal.

b. Introducir una herramienta de seguridad usada en otras áreas de las ciencias de la computación, a computadores personales.

c. Implementar la verificación de identidad del usuario para brindarle una mayor protección.

C. Justificación

El sistema de seguridad desarrollado muestra varias características distintas a otros paquetes de criptografía. Algunas de ellas facilitarán su uso y motivarán su empleo. La principal característica es su incorporación al sistema operativo del computador personal: usualmente, para encriptar un archivo, se requiere un tiempo extra y llevar un control de los documentos encriptados y aquellos que no lo están. En el presente sistema, el encriptamiento / decriptamiento serán invisibles al usuario, pues será el archivo de identificaciones el que indique dicho factor. Por otra parte, el proceso será invisible al usuario, pues no requerirá otra cosa que introducir su llave para el sistema criptográfico lo pueda usar durante los accesos a disco. Además, el tiempo requerido por la codificación será mínimo, para evitar que la intervención del presente programa sea tediosa y resulte obsoleta.

La verificación de identidad reforzará la seguridad proporcionada por el sistema criptográfico: ayudará a disminuir la posibilidad de acceso de un intruso y que éste destruya el archivo al re-encriptarlo usando otra llave o bien, al introducir otros datos con los cuales se pondría en duda la integridad del archivo.

El desarrollo de un sistema de seguridad como éste, conduce a investigar nuevos campos en el ámbito computacional que ayuden al usuario a proteger su información.

D. Características y alcances

1. Cada archivo será encriptado sólo si el usuario lo desea. Su nombre y extensión serán conservados.

2. La llave de cada archivo NO será almacenada. El archivo de identificaciones sólo contendrá el nombre del archivo encriptado y el tiempo característico para el ingreso de la clave relacionada a él.

3. Utiliza un método criptográfico rápido: la velocidad de lectura o escritura no debe ser degradada.

4. El espacio a usar en disco será el mismo. Ello implica una ventaja, pues se empleará la misma cantidad de espacio en disco y se proveerá protección al archivo

sin sacrificar más tiempo o espacio.

5. Independencia del número de bloque o registro a accesar. Por ejemplo, ciertos métodos exigen que se accesen los n-1 bloques anteriores al deseado para poder descifrarlo en forma correcta, mientras que otros requieren que se re-encripten los n-1 bloques posteriores al utilizado; todo ello requiere más tiempo de acceso a disco, lo cual impediría cumplir con la característica (3).

6. El lenguaje con el cual se desarrolló el programa es Assembler, ya que permitirá una codificación - decodificación más rápida de los datos y da acceso simple a los interrupts del sistema operativo.

E. Requerimientos

El presente programa requiere de algunas especificaciones del computador, entre las cuales figuran:

1. El computador personal posea un procesador 8086/8088.
2. El sistema operativo MS-DOS/PC-DOS sea un versión 2.0 o más.
3. Carecer de EMS (Expanded Memory Specification), pues el programa substituye el interrupt relacionado al administrador de memoria expandida.
4. Poseer una memoria principal de 640 Kb.

F. Sugerencias

Con el objeto de mejorar el servicio proporcionado por el presente sistema de seguridad, se realizan a continuación algunas sugerencias:

1. Asegúrese de cumplir con los requerimientos especificados anteriormente; no satisfacer alguno de ellos porque podría provocar el mal uso del presente programa.

2. Al iniciar la operación del sistema, ejecute el programa de alteración del sistema operativo MS-DOS/PC-DOS.

3. Realice un "back-up" en forma periódica de todos sus datos, incluyendo los del archivo de identificaciones.

G. Advertencias

1. Eliminar el archivo de identificaciones provocará que los archivos encriptados no puedan ser reconocidos por el sistema operativo, con lo cual, resultarían ininteligibles, incluso para su dueño.

2. Evite cambiar la llave de acceso cuando tenga abierto otro archivo; las siguientes lecturas o escrituras podrían resultar inválidas.

H. Restricciones

El presente programa posee algunas limitaciones, entre las cuales se deben tomar en cuenta:

1. La clave para cada archivo permite un máximo de 15 caracteres.
2. Si se modifica la llave, después de abrir un archivo, podrían perderse los cambios posteriores, pues la verificación de identidad puede diferir y ello provocará la inhibición del acceso al archivo.
3. Si los programas o paquetes de software cuyo acceso a los archivos al sistema son por medio de un interrupt distinto al 21h, se alejan de la capacidad de encriptamiento del presente programa.

I. Aspectos considerados en el diseño

1. Validación del usuario:

Cada persona cuenta con características que le distinguen de otras, tal y como se describió en el capítulo anterior. Una de dichas características se relaciona con la habilidad de digitación del individuo, pues unos podrán teclear con más velocidad que otros; o bien, habrán desarrollado facilidad para teclear una cierta secuencia de letras. Con el objeto de verificar la identidad del usuario, se ha utilizado esta técnica en el presente proyecto. Ella dificultará el uso de los archivos encriptados por intrusos al verificar que la clave haya sido tecleada en la forma usual del dueño.

Durante la creación de un archivo se le requerirá al usuario que ingrese diez veces una clave, la cual será utilizada posteriormente para el encriptamiento o decriptamiento del archivo. Esto permitirá que se realice un promedio del tiempo usado entre una tecla y la otra, el cual se adjunta a la identificación del archivo para validar futuros accesos al mismo.

El usuario podrá ingresar su clave en cualquier momento con sólo presionar "SHIFT F10". El cambio del cursor a la esquina superior izquierda de la pantalla,

indicará cuando se pueda iniciar el ingreso de la clave. Se presiona la tecla de "ENTER" para finalizar dicho ingreso; no se aceptan más de 15 caracteres.

En la presente validación del usuario, aun se debe analizar otro factor: la reacción del individuo a un estímulo puede variar y ello depende de distintas situaciones. El estímulo será el movimiento del cursor y la respuesta a éste, será el inicio del ingreso de la clave. Sin embargo, y el usuario lo podrá comprobar por sí mismo al usar el programa descrito en el apéndice A, el tiempo de respuesta puede ser totalmente variable, a menos que se ponga toda la atención. Como consecuencia de esta situación se debe que los tiempos utilizados para la representación del individuo sean aquellos a partir de la primer tecla. Es decir, si $x_1 x_2 \ldots x_n$ representa la secuencia de n caracteres de la clave y los tiempos se describen como:

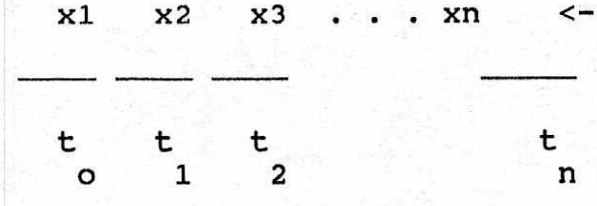
$$x_1 \quad x_2 \quad x_3 \quad \ldots \quad x_n \quad <-$$

$$t_o \quad t_1 \quad t_2 \qquad\qquad t_n$$

Donde t_o denota el tiempo entre la indicación de que el computador está listo para recibir el primer carácter y la presión de la tecla que lo representa;

indicará cuando se pueda iniciar el ingreso de la clave. Se presiona la tecla de "ENTER" para finalizar dicho ingreso; no se aceptan más de 15 caracteres.

En la presente validación del usuario, aun se debe analizar otro factor: la reacción del individuo a un estímulo puede variar y ello depende de distintas situaciones. El estímulo será el movimiento del cursor y la respuesta a éste, será el inicio del ingreso de la clave. Sin embargo, y el usuario lo podrá comprobar por sí mismo al usar el programa descrito en el apéndice A, el tiempo de respuesta puede ser totalmente variable, a menos que se ponga toda la atención. Como consecuencia de esta situación se debe que los tiempos utilizados para la representación del individuo sean aquellos a partir de la primer tecla. Es decir, si $x_1 x_2 \ldots x_n$ representa la secuencia de n caracteres de la clave y los tiempos se describen como:



Donde t_o denota el tiempo entre la indicación de que el computador está listo para recibir el primer carácter y la presión de la tecla que lo representa;

t_1, el tiempo entre el primer y segundo carácter y así sucesivamente hasta t_n, que representa el tiempo entre el último carácter y el ENTER, o bien, entre el caracter número 14 y el 15.

Los tiempos t_1, t_2 hasta t_n, se asumen casi constantes en un individuo; ésto se debe a que el proceso de teclear una secuencia de caracteres es mecánico y poco reflexivo. En estos tiempos se ha basado la identificación del individuo dentro del presente sistema.

2. Método de encriptamiento/decriptamiento:

La forma de codificación para el presente sistema criptográfico se basa en la substitución y las propiedades de la operación XOR.

Sea K la llave y S la secuencia de caracteres a codificar. S podría ser descrito por:

$$S = S_1 S_2 S_3 \ldots S_m$$

Donde cada S_i representa un grupo de n caracteres en la posición i de S. El número n está determinado por la longitud de la llave de acceso relacionada al archivo a encriptar. Ahora bien, sea C la representación de S cuando ya se ha codificado por el

método E. Se tiene:

$$C = C_1 C_2 C_3 \ldots C_m$$

Donde cada C_i ha sido codificado como:

$$C_i = E(S_i) = S_i + C_{i-1}$$

y $C_o = S_o + K.$

Para la decodificación, representada por el símbolo D, se usará el método inverso usado para el encriptamiento. Es decir,

$$S_i = D(C_i) = C_i + C_{i-1}$$

Donde S_o se calcula como: $S_o = C_o + K.$

Para demostrar que el método de decriptamiento funciona adecuadamente, nótese:

$$Ci + Ci\text{-}1 = (Si + Ci\text{-}1) + Ci\text{-}1 \quad (1)$$

$$= S_i + (C_{i-1} + C_{i-1}) \quad (2)$$

$$= S_i + 0 \quad (3)$$

$$= Si \quad (4)$$

La justificación de los pasos anteriores se presenta a continuación:

(1) Substitución de C_i (Véase método encriptamiento).

Cada programa dentro del computador identifica un archivo con un estilo distinto, aunque se refiera al mismo archivo. Por ejemplo, si se encuentra en el directorio principal del disco B y se crea el archivo PRUEBA, con la instrucción:

COPY CON PRUEBA

La identificación del archivo sólo será "PRUEBA"; mientras que Turbo Pascal versión 4.0 lo hubiera descrito como "B:PRUEBA". En el momento de comparar las dos secuencias de caracteres, éstas no coincidirán. Por tanto, se deberá crear un estándar en el cual, cada archivo, sin importar el programa que lo accese, quede plenamente identificado. En el presente sistema criptográfico se incluye un procedimiento cuyo propósito es identificar completamente un archivo como:

<DIRECTORIOS\> <NOMBRE DEL ARCHIVO> <.> <EXTENSION>

lo cual dará acceso a un archivo dentro del sistema en una forma totalmente invisible para el usuario.

Se deberá notar que en la presente identificación del archivo no se incluye el "DRIVE", en el cual se encontraba originalmente el archivo (es decir, donde fue creado); ello proporcionará una mayor flexibilidad en el uso de los archivos, pues se podrán copiar de una

unidad de disco a otra y aun podrán ser identificados en una forma adecuada. Sin embargo, la descripción del directorio al cual pertenece, aún se conserva; ello permitirá distinguir entre dos archivos con el mismo nombre, pero en distintos directorios.

J. Instalación del sistema criptográfico

Durante la instalación del sistema criptográfico se substituirán varios interrupts del sistema operativo PC-DOS/MS-DOS, entre los cuales se encuentran los relacionados al teclado, al reloj y al acceso a archivos.

La rutina de teclado ha sido diseñada para reconocer una llamada de requerimiento para el ingreso de la clave en el momento que el usuario lo desee. Por su parte, la nueva rutina de reloj, verificará si se ha activado el proceso relacionado a dicho ingreso; si éste no se encuentra en uso, entonces verificará si el usuario la necesita. Si es así, permitirá el ingreso de dicha clave.

El acceso a los archivos se describe en la siguiente sección con mayor detalle.

K. Funcionamiento del sistema criptográfico ante las distintas operaciones efectuadas en archivos

1. Creación de un archivo:

Un archivo se crea, en forma usual, cuando el usuario envía un comando para guardar un archivo con un nombre dado, invocando la creación del mismo (es distinto, a modificar un archivo antiguo y guardarlo). Puede ser que el archivo a crear hubiera tenido una existencia previa en el directorio, en cuyo caso se borrará el archivo anterior y se permitirá el ingreso de los datos al mismo. El otro caso es en el que el archivo no aparecía en el directorio y, por tanto, se agrega su nombre al mismo, así como se graban los datos.

Durante la creación de un archivo, el sistema criptográfico presentado buscará en la tabla de identificaciones el nombre del archivo a crear, y si la búsqueda es exitosa se asumirá que la clave es la misma. Por otra parte, si el archivo no se encontraba en la tabla, se le requerirá al usuario ingresar una clave diez veces, con lo cual se realizará el promedio de tiempos y se agregará la identificación a la tabla; además, se guardará la tabla al archivo de identificaciones en el disco, con el objeto de

conservar consistencia entre los datos de uno y otro. Ello se ha realizado así para evitar depender del usuario y para salvar la tabla, pues puede ser que esta operación sea olvidada y se pierdan los datos relacionados a los archivos recién ingresados al sistema criptográfico.

2. Abrir un archivo:

Cuando se abre un archivo, la nueva rutina buscará su nombre en la tabla de identificaciones, y si lo encuentra indicará que el archivo estaba encriptado, en cuyo caso, también verificará si el tiempo promedio característico de la clave coincide con el ingresado recientemente por el usuario. Si éstos se parecen lo suficiente, permitirá que se abra el archivo; en caso contrario, encenderá la bandera del "CARRY", con la cual se indica error en la operación de apertura del archivo. Si todo lo anterior muestra que el individuo posee el derecho de acceso al archivo, o bien, el archivo no había sido encriptado, entonces se realizará la llamada al sistema operativo para efectuar la apertura del archivo.

3. Lectura de un archivo:

La lectura se realiza utilizando la rutina del

sistema operativo. Si ésta fue exitosa, se verifica si dicho archivo estaba encriptado. En caso afirmativo, se llama a la rutina de decriptamiento, con la cual, se descifran los datos de forma que el usuario los pueda entender y trabaje con ellos.

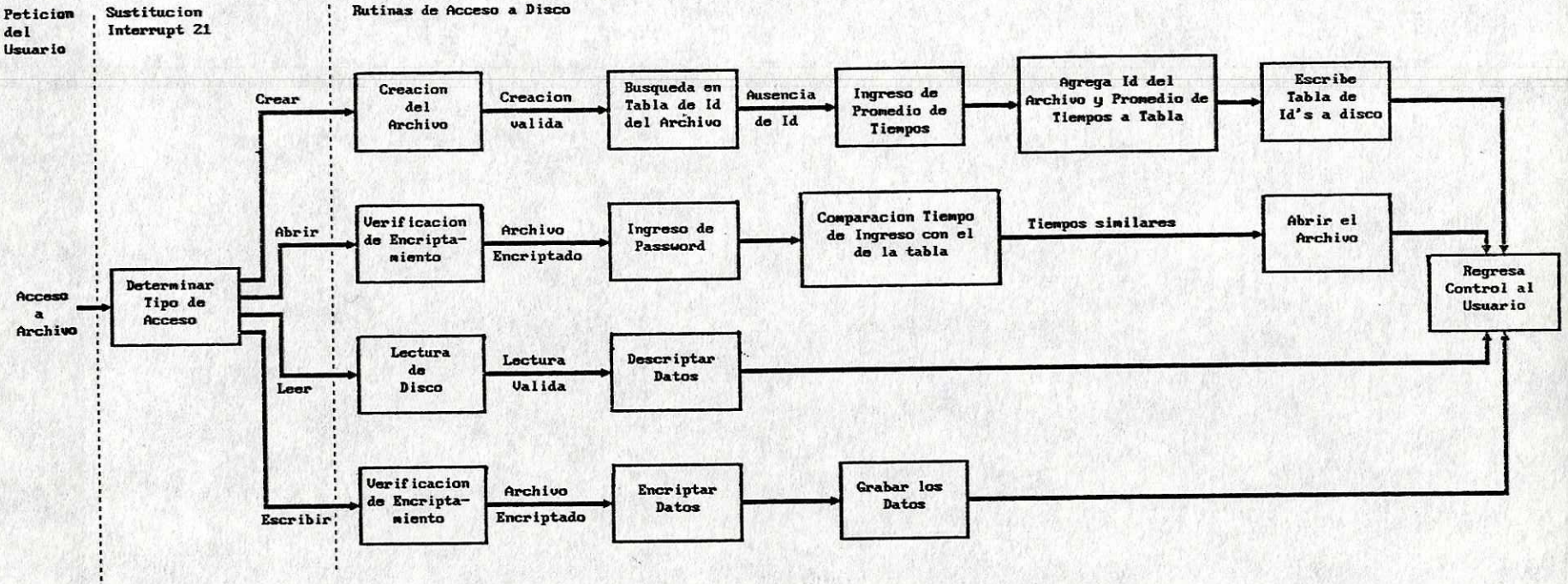
Si el usuario modifica la clave después de la apertura del archivo, los datos serán decodificados inadecuadamente y resultarán ininteligibles. Por tanto, se deberá tener cuidado para no modificar la clave cuando se tengan uno o más archivos abiertos con dicha clave.

4. Escritura a un archivo:

Si el archivo al cual se escribirá pertenece al sistema criptográfico, se encriptarán los datos antes de grabarlos. Por supuesto, se deberá poseer el mismo cuidado que se tiene con la lectura con respecto a la modificación de la clave, pues en el presente caso, se encriptarán los datos en forma distinta y ello provocaría serios daños al archivo.

5. Cerrar un archivo:

Esta rutina ha sido dejada intacta, pues cerrar un archivo no necesita protección.


Peticion del Usuario
Sustitucion Interrupt 21
Rutinas de Acceso a Disco
Acceso a Archivo
Determinar Tipo de Acceso
Crear
Abrir
Leer
Escribir
Creacion del Archivo
Creacion valida
Busqueda en Tabla de Id del Archivo
Ausencia de Id
Ingreso de Promedio de Tiempos
Agrega Id del Archivo y Promedio de Tiempos a Tabla
Escribe Tabla de Id's a disco
Verificacion de Encripta-miento
Archivo Encriptado
Ingreso de Password
Comparacion Tiempo de Ingreso con el de la tabla
Tiempos similares
Abrir el Archivo
Lectura de Disco
Lectura Valida
Descriptar Datos
Verificacion de Encripta-miento
Archivo Encriptado
Encriptar Datos
Grabar los Datos
Regresa Control al Usuario

CONCLUSIONES

1. El sistema criptográfico presentado fue incorporado al sistema operativo; con ello, el encriptamiento y decriptamiento se convierten en procesos invisibles para el usuario.

2. El método de encriptamiento/decriptamiento utilizado incrementa en una mínima parte el tiempo requerido para una escritura o lectura a disco, utiliza el mismo espacio en disco que el usado por el original y es independiente del número de bloque o registro deseado.

3. El archivo con la identificación de los archivos encriptados permite discernir entre aquellos que lo están y los que no, lo cual es vital para obtener y grabar los datos en forma adecuada.

4. La verificación de la identidad del usuario limitará el uso de un archivo al dueño del mismo; pues utilizar un archivo no dependerá, solamente, de la secretividad de la llave o el método de encriptamiento, sino también de una característica personal como lo es la velocidad mecanográfica de cada persona.

Bibliografía

Abel, Peter. Assembler for the IBM PC and PC-XT. Virginia (U.S.A.); Prentice-Hall Company, 1983. 416 pp.

Baker, Richard H. The computer security handbook. First Edition. Philadelphia; Tab Books Inc., 1985. 281 pp.

Cronin, Daniel. Microcomputer Data Security. New York; Prentice Hall Press, 1986. 281 pp.

Denning, Dorothy E. Cryptography and data security. Massachusetts; Addison-Wesley Publishing Company, 1982. 400 pp.

Duncan, Ray. Advanced MS-DOS programming. Second Edition. Washington; Microsoft Press, 1988. 669 pp.

Hansen, Brinch. Operating System Principles. New Jersey; Prentice hall, Inc., 1973. 366 pp.

Jourdain, Robert. Programmer's Problem solver for the IBM PC, XT & AT. New York; Prentice Hall Press, 1986. 473 pp.

Lorin, Harold and Harvey Deitel. Operating Systems. Massachusetts; Addison-Wesley Pulishing Co., 1981. 378 pp.

Madnick, Stuart and John Donovan. Operating Systems. 12th Printing. Singapore; McGraw-Hill Book Co., 1986. 638 pp.

Myers, Glenford. Advances in Computer Architecture. Second Edition. New York; John Wiley & Sons, 1982. 545 pp.

Norton, Peter. Programmer's guide to the IBM PC. Washington; Microsoft Press, 1985. 426 pp.

Tsichritzis, Dionysios and Philip A. Bernstein. Operating Systems. New York; Academic Press, Inc., 1974. 298 pp.

Wiederhold, Gio. Diseño de bases de datos. Segunda Edición. México; McGraw-Hill, 1985. 921 pp.

APENDICE A

En esta sección se muestran los tiempos de tecleado de varias personas. La palabra utilizada para esta prueba fue "MURCIELAGO" y fue elegida, por la diversidad de caracteres que posee. Se obtuvieron dos ejemplos con cada individuo, los cuales fueron realizados en distintos días con el objeto de verificar si la velocidad al teclear una palabra se conserva o varía.

Las tablas que se presentan a continuación fueron realizadas con un programa estrechamente relacionado al sistema criptográfico desarrollado en este estudio y que permitirá a un usuario conocer su forma y velocidad al teclear. Ello le familiarizará con el sistema criptográfico y le facilitará obtener el mayor provecho del mismo al utilizar, en una forma adecuada, la verificación de la identidad.

Resultados de Persona 1

Prueba	Tiempos										
1	55	5	3	5	4	4	3	3	4	3	15
2	90	4	3	5	3	4	3	2	6	5	7
3	14	4	3	5	2	2	3	4	5	5	5
4	10	3	3	4	2	4	2	3	4	4	6
5	12	4	3	6	6	8	2	2	5	3	6
6	7	4	8	6	2	4	2	2	5	4	6
7	21	4	3	42	2	3	6	4	3	4	4
8	23	5	3	4	3	3	5	3	5	3	5
9	7	4	3	4	2	2	3	1	4	5	5
10	7	3	3	5	1	5	3	2	12	12	5
11	57	4	3	5	3	2	2	3	4	3	6
12	8	3	3	4	2	3	1	3	4	4	6
13	9	3	4	5	3	3	2	3	5	4	4
14	7	3	3	5	3	1	3	2	3	4	4
15	7	4	4	5	2	2	2	3	4	4	5
16	14	4	3	9	2	6	2	2	5	4	4
17	6	3	3	4	3	1	2	2	5	5	6
18	8	4	3	5	2	2	2	2	5	4	5
19	14	5	2	8	2	2	2	2	4	4	5
20	11	5	2	5	3	2	2	4	5	8	8
N	20	20	20	19	20	20	20	20	19	19	19
X	19	4	3	5	3	3	3	3	4	4	5
σ	22	1	1	1	1	2	1	1	1	1	1

Resultados de Persona 2

Prueba	Tiempos										
1	29	5	4	8	1	4	2	2	9	2	43
2	131	4	3	6	3	2	2	3	11	4	16
3	18	5	4	7	3	3	2	3	6	3	7
4	22	6	3	6	3	3	2	2	11	3	10
5	8	4	3	6	3	3	2	3	4	3	8
6	13	5	3	9	3	3	3	2	5	3	8
7	21	4	3	5	2	2	3	1	4	3	19
8	101	4	3	4	3	2	2	2	4	2	11
9	42	4	3	5	2	2	2	2	4	3	10
10	17	5	3	4	2	2	2	2	4	3	6
11	23	4	4	5	2	2	2	2	4	3	16
12	42	3	3	4	3	1	3	2	4	2	6
13	17	4	3	4	1	3	2	2	4	2	6
14	5	5	3	4	2	2	3	2	3	3	5
15	16	4	2	5	3	1	3	2	3	4	7
16	5	3	3	4	2	2	2	3	3	3	5
17	4	4	2	5	2	2	2	2	4	2	5
18	5	4	2	4	2	2	2	3	3	3	6
19	6	3	3	4	3	1	3	2	5	2	5
20	9	4	3	6	2	2	2	2	4	2	6
N	20	20	20	20	20	20	20	20	18	20	18
X	27	4	3	5	2	2	2	2	4	3	8
σ	32	1	1	1	1	1	0	1	1	1	3

Resultados de Persona 3

Prueba	Tiempos										
1	7	4	4	4	38	2	3	2	2	3	1
2	8	4	4	5	9	2	3	3	3	2	2
3	9	5	3	4	8	2	4	3	2	3	1
4	5	5	4	5	4	8	3	5	3	3	2
5	6	5	4	4	8	5	3	5	3	4	2
6	9	5	4	6	6	1	3	3	2	3	2
7	8	4	4	6	5	1	4	2	3	2	2
8	5	5	4	16	6	2	2	3	2	3	1
9	4	5	4	5	6	1	3	3	2	3	2
10	9	4	4	4	7	2	2	3	2	3	2
11	7	6	4	6	6	2	4	5	2	4	2
12	13	6	5	8	6	2	5	3	2	4	1
13	8	4	5	4	47	2	3	3	3	4	1
14	7	5	4	5	7	2	4	3	2	3	2
15	8	4	4	5	6	2	3	3	2	4	2
16	6	5	4	5	7	3	9	4	2	3	1
17	5	4	5	5	5	2	3	4	2	3	2
18	5	4	12	12	5	2	3	3	1	3	2
19	4	5	4	4	5	1	3	3	2	15	1
20	6	5	3	5	7	1	5	3	3	3	1
N	19	20	19	19	18	20	20	20	20	19	20
X	7	5	4	5	6	2	4	3	2	3	2
σ	2	1	1	2	1	2	1	1	1	1	0

Resultados de Persona 4

Prueba	Tiempos										
1	11	7	2	6	4	4	11	2	4	2	6
2	11	6	3	15	3	2	7	3	5	3	6
3	15	12	2	10	4	2	12	2	4	3	5
4	13	6	1	7	3	2	14	2	4	3	5
5	13	6	2	9	6	3	16	3	4	2	5
6	12	5	2	5	3	3	12	3	4	2	5
7	10	7	1	7	5	3	24	2	5	2	5
8	10	5	1	6	2	2	10	2	4	3	5
9	14	5	2	9	3	2	9	3	3	3	5
10	11	5	2	6	2	3	9	1	6	2	6
11	11	7	3	18	4	2	13	7	4	2	6
12	14	5	2	5	3	4	15	7	4	3	6
13	12	6	2	6	3	7	10	2	5	6	5
14	15	6	2	6	4	2	12	2	6	2	7
15	13	7	2	13	8	2	23	2	4	3	5
16	11	6	1	6	3	3	8	3	7	4	6
17	14	7	2	8	6	2	11	2	8	2	6
18	14	6	1	10	4	2	11	2	4	3	6
19	12	6	1	7	4	2	10	2	5	3	18
20	14	6	2	6	6	2	9	3	8	4	7
N	20	19	20	18	19	19	18	20	20	20	19
X	13	6	2	7	4	2	11	3	5	3	6
σ	2	1	1	2	1	1	2	2	1	1	1

Resultados de Persona 5

Prueba	Tiempos										
1	23	5	5	6	3	4	3	3	3	2	5
2	9	3	4	5	12	4	3	4	6	2	5
3	12	5	3	5	3	3	3	2	5	1	5
4	6	4	3	4	4	4	12	2	6	2	5
5	11	4	3	5	3	5	7	1	4	2	5
6	5	4	3	5	8	3	5	2	5	2	5
7	9	5	3	6	6	10	5	4	24	1	4
8	10	4	3	7	7	4	5	2	3	1	5
9	5	4	3	5	3	3	2	3	2	2	5
10	9	4	3	6	4	5	2	2	3	2	5
11	33	5	4	6	3	4	2	3	5	1	4
12	13	4	3	4	3	6	3	2	5	1	4
13	10	5	2	4	3	2	3	3	3	2	4
14	9	13	5	5	3	4	2	2	4	3	5
15	7	5	2	5	2	3	2	2	5	1	4
16	8	5	2	5	3	2	3	2	5	2	5
17	8	5	2	5	2	3	2	2	3	2	4
18	9	4	2	4	3	2	2	2	3	2	5
19	9	4	2	4	3	2	2	2	3	2	4
20	8	5	1	5	2	3	2	2	4	2	4
N	20	19	20	20	19	19	19	20	19	20	20
X	11	4	3	5	4	3	3	2	4	2	5
σ	6	1	1	1	2	1	1	1	1	1	0

Resultados de Persona 6

Prueba	Tiempos										
1	44	7	3	7	4	4	5	8	7	4	19
2	14	5	4	6	4	5	6	11	8	4	8
3	12	13	5	7	6	6	7	7	10	8	7
4	10	7	6	11	5	5	6	5	6	5	6
5	15	5	4	6	8	4	16	6	7	5	11
6	17	6	4	9	5	4	6	7	5	4	6
7	19	5	6	8	5	5	17	5	6	4	4
8	10	5	4	6	5	4	4	7	9	4	12
9	18	5	5	9	5	4	5	7	8	5	5
10	17	5	5	7	4	5	5	6	8	3	6
11	18	5	4	7	10	3	6	3	5	4	15
12	23	5	7	7	4	3	4	4	5	3	5
13	11	4	5	6	5	3	4	4	5	3	5
14	12	4	5	6	4	4	4	4	8	3	4
15	32	5	5	6	5	4	6	4	5	4	5
16	14	11	19	6	6	4	3	3	6	4	5
17	19	4	5	6	5	4	5	3	4	4	4
18	13	4	4	5	5	3	5	3	5	4	4
19	7	5	4	10	4	4	4	3	5	3	5
20	22	4	4	5	4	3	5	3	5	2	4
N	20	18	19	20	19	20	18	19	20	19	19
X	17	5	5	7	5	4	5	5	6	4	6
σ	8	1	1	2	1	1	1	2	2	1	3

Resultados de Persona 7

Prueba	Tiempos										
1	92	5	4	8	2	2	3	4	7	3	64
2	32	12	3	5	2	2	3	3	6	2	8
3	12	5	3	4	3	2	2	4	4	3	12
4	11	6	7	5	2	3	2	4	6	4	6
5	11	3	3	5	2	2	3	4	4	6	7
6	12	5	2	4	2	3	2	3	5	6	18
7	18	4	2	5	1	3	2	3	4	3	5
8	11	4	2	5	2	2	3	3	5	3	5
9	11	4	3	4	4	2	3	3	6	4	6
10	13	4	3	4	2	3	2	3	4	3	7
11	106	4	3	4	1	3	2	4	6	2	18
12	19	4	2	4	2	3	2	3	7	7	5
13	12	4	3	4	2	2	3	2	5	2	6
14	11	3	2	4	2	3	2	3	4	2	6
15	58	4	2	5	2	2	2	3	7	4	5
16	32	5	3	4	1	3	2	3	4	13	5
17	10	4	2	3	2	3	3	6	16	8	5
18	15	5	2	4	1	4	2	2	5	3	5
19	12	4	1	4	3	2	3	2	4	3	5
20	41	4	2	4	14	2	17	2	3	2	7
N	20	19	19	19	19	20	19	19	19	19	19
X	27	4	2	4	2	3	2	3	5	4	7
σ	27	1	1	1	1	1	0	1	1	2	4

Resultados de Persona 8

Prueba	Tiempos										
1	212	3	5	7	2	6	4	8	14	2	8
2	15	3	7	13	2	6	3	8	7	3	9
3	16	4	5	8	2	8	3	5	9	3	7
4	13	3	8	10	2	9	3	4	7	2	8
5	15	3	6	8	2	7	3	4	9	3	8
6	11	4	5	6	3	5	3	5	7	2	7
7	17	4	7	8	2	35	3	5	14	3	7
8	37	3	7	5	4	4	6	3	6	4	7
9	14	4	8	5	3	5	3	3	9	3	7
10	29	4	4	6	3	3	4	4	7	3	6
11	18	4	4	8	2	2	4	4	11	3	5
12	21	3	8	7	2	4	3	4	7	3	7
13	101	3	4	10	2	7	3	26	6	3	7
14	15	4	8	5	4	3	4	7	6	3	6
15	13	3	6	8	3	3	3	7	7	3	5
16	12	4	8	5	3	4	3	4	10	3	5
17	15	2	5	6	4	4	7	4	6	6	4
18	11	3	5	8	3	7	3	2	7	5	5
19	42	3	5	7	4	16	6	3	6	3	6
20	12	3	4	7	4	6	2	4	5	4	6
N	20	20	20	19	20	19	19	19	18	19	20
X	32	3	6	7	3	6	3	5	7	3	7
σ	46	1	1	2	1	3	1	2	2	1	1

Resultados de Persona 9

Prueba	Tiempos										
1	26	4	1	6	3	3	2	3	2	3	4
2	19	4	1	6	2	4	3	15	3	3	5
3	6	4	1	19	2	2	2	2	2	4	5
4	6	4	1	9	3	3	4	11	3	4	4
5	7	4	2	6	2	3	4	8	3	3	5
6	6	4	1	16	2	3	2	9	3	3	5
7	5	4	1	12	2	2	6	3	4	2	5
8	9	3	3	6	2	3	2	3	3	4	6
9	17	4	2	20	1	3	2	3	3	3	4
10	11	4	2	6	2	3	4	2	5	2	5
11	131	4	1	6	2	3	3	2	7	2	5
12	8	4	1	8	2	3	3	5	3	3	5
13	4	4	1	6	1	3	3	3	9	3	6
14	9	4	2	7	2	3	3	3	4	4	6
15	5	4	1	17	7	5	4	3	3	3	4
16	14	3	1	4	3	2	13	2	3	2	6
17	13	3	1	5	8	2	4	2	3	3	5
18	12	3	1	6	2	2	3	2	3	3	4
19	7	3	1	7	3	3	3	2	3	4	6
20	5	4	1	13	2	2	3	3	2	2	4
N	20	20	19	19	18	19	19	19	19	20	20
X	16	4	1	9	2	3	3	4	3	3	5
σ	27	0	0	4	1	1	1	3	1	1	1

Resultados de Persona 10

Prueba	Tiempos										
1	40	5	3	6	3	2	4	2	8	4	5
2	23	4	3	5	5	2	5	3	8	4	5
3	39	4	4	13	2	3	4	3	10	3	4
4	19	4	2	5	5	3	4	2	6	4	4
5	15	4	3	4	4	3	3	3	7	4	4
6	15	4	3	4	4	2	3	3	6	3	5
7	12	4	3	5	3	3	2	3	6	3	5
8	12	4	3	4	4	2	3	3	6	8	5
9	15	4	3	5	3	2	3	2	9	3	6
10	13	4	3	5	3	3	2	3	6	3	4
11	18	4	3	7	2	3	3	2	11	2	5
12	15	5	3	6	3	3	2	2	7	3	4
13	23	4	3	5	3	3	3	4	7	3	5
14	10	4	3	7	3	3	3	2	6	4	4
15	12	4	3	4	4	2	4	3	5	3	5
16	8	5	2	5	3	3	2	3	6	3	4
17	7	5	2	4	4	3	3	1	7	3	5
18	10	4	2	5	4	2	2	2	6	4	4
19	10	4	2	4	3	3	3	2	6	3	4
20	10	4	3	4	3	2	3	2	5	3	4
N	20	20	20	19	20	20	20	20	20	20	20
X	16	4	3	5	3	3	3	3	7	4	5
σ	9	0	1	1	1	0	1	1	2	1	1

APENDICE B

Análisis de los datos relacionados a la validación del usuario

En las tablas de resultados presentadas en el apéndice A, se muestran los tiempos entre tecla y tecla del ingreso de distintas claves por varias personas. Cada ingreso fue numerado, y las últimas líneas de la tabla, muestran el número de datos con los cuales se realizaron las estadísticas (esto se comprenderá mejor posteriormente), así como el promedio y desviación standard de dichos datos.

El primer tiempo, llamado t_o en el capítulo VII, ha sido variable en su mayoría; aún entre un ingreso y otro. La diferencia es tan notable, que dicho tiempo no debe ser tomado como característico de la persona. La variación de t_o se debió en algunos casos a la falta de concentración y por ende, la respuesta tardía hacia el inicio de teclear. En otros casos, especialmente cuando el individuo no se encontraba familiarizado con la palabra a teclear, antes de iniciar el ingreso se tomaba un tiempo para pensar en dicha palabra.

DIFERENCIAS ENTRE INDIVIDUOS:

Para averiguar si existe diferencia entre la velocidad al teclear de un individuo a otro, se siguieron los pasos que se describen a continuación:

1. Se eliminaron los tiempos que se encontraban más allá de $X \pm 2s$ (fueron subrayados), y se calcularon de nuevo el promedio y la desviación estándar.

2. Con dichos datos, se obtuvo la t de student del primer individuo con el segundo, con el tercero hasta el décimo, luego, se compararon el segundo con el tercero y así sucesivamente hasta comparar el noveno con el décimo.

3. La t de student obtenida, fue comparada con $t_{0.05}$ (es decir con una aceptación del 95%) y un rango de libertad de 40 (fueron entre 30 y 40 los casos obtenidos entre los dos grupos a comparar y ello, determina el rango de libertad).

Las hipótesis planteadas fueron:

Hipótesis nula:

No hay diferencia esencial entre el tiempo de tecleo de un individuo y otro.

Hipótesis alterna:

Hay diferencia entre el tiempo de tecleo de un individuo y otro.

Bajo la hipótesis nula,

$$t = \frac{X_1 - X_2}{\sigma\sqrt{1/N_1 + 1/N_2}}$$

$$\text{donde } \sigma = \sqrt{\frac{N_1 S_1^2 + N_2 S_2^2}{N_1 + N_2 - 2}}$$

La hipótesis alterna se acepta sólo cuando

$$t < -t_{\alpha/2} \quad \text{ó} \quad t > t_{\alpha/2}$$

Por tanto, al comparar la t de student obtenida con la $t_{\alpha/2}$, se anotaron el número de casos que aceptaron la hipótesis alterna y con dicho número y el total de casos, se contruyó la tabla de porcentajes de diferencias en la forma de teclear.

Como se podrá ver, en la mayoría de casos, más del 40% de las teclas fueron distintas entre un individuo y otro.

Se puede concluir, que la forma de teclear puede ser utilizada para distinguir entre los individuos.

Porcentajes de diferencias en la forma y velocidad de tecleo para una muestra de 10 personas

	1	2	3	4	5	6	7	8	9	10
1	*	40	90	60	40	80	60	90	60	40
2	40	*	80	60	50	90	50	90	80	60
3	90	80	*	70	70	90	70	80	60	60
4	60	60	70	*	80	80	70	80	60	70
5	40	50	70	80	*	100	80	90	90	30
6	80	90	90	80	100	*	80	70	80	80
7	60	50	70	70	80	80	*	70	60	80
8	90	90	80	80	90	70	70	*	60	70
9	60	80	60	60	90	80	60	60	*	70
10	40	60	60	70	30	80	80	70	70	*

FUNCIONALIDAD DEL METODO PARA VERIFICACION DE LA IDENTIDAD:

Si el presente método, la velocidad al teclear una clave, es útil para verificar la identidad de un individuo, sólo se puede mostrar utilizando dos parámetros:

1. ¿El individuo teclea en forma similar en varias ocasiones?

2. ¿Varios individuos pueden ser confundidos e identificados de igual manera?

Para comprobar si un individuo teclea de la misma forma en varias ocasiones se efectuó el primer paso del análisis anterior.

Posteriormente, se revisó el número de tiempos que se encontraban en el rango:

$$| t_i \pm X_i | \leq s_i$$

Donde t_i denota el tiempo entre la tecla "i - 1" y la tecla "i"; X_i, el promedio relacionado y s_i, representa la desviación standard. Este rango representa el criterio de coincidencia que se utiliza para aceptar a un individuo.

La tabulación de los resultados obtenidos se encuentra en la tabla denominada "Nivel de aceptación: casos autorizados". Se tomaron todos aquellos ingresos de la clave

que coincidieron con el nivel de aceptación propuesto: 60, 70 u 80%. Cada fila de la tabla representa a un individuo. El nivel de aceptación indica el porcentaje de los caracteres que cumplieron con el criterio anterior de coincidencia en los tiempos. Al final de la tabla, se muestra el promedio obtenido de los diez individuos; ésta es la representación del porcentaje de individuos reconocidos en los distintos niveles de aceptación. Como se puede notar, al 60% de aceptación se reconoció la mayor parte de veces a un individuo; mientras que al 80% fue muy bajo el porcentaje de accesos autorizados que se aceptaron como válidos.

Contestar a la segunda pregunta propuesta para medir la funcionalidad del método, requirió comparar el porcentaje de los accesos permitidos a "intrusos" (personas distintas al individuo que se intenta identificar). Con tal objeto, se realizaron las tablas denominadas "Porcentaje de aceptación de un intruso respecto al XXX individuo" ; donde XXX representa el número del individuo que se ha tomado como válido. Nótese que la línea que representa al individuo contiene asteriscos (*), pues siendo él el "válido" no se puede comparar con los "intrusos". Para cada tabla, se obtuvo el promedio de los "intrusos" cuyo acceso hubiera sido permitido a los distintos niveles de aceptación; estos resultados se tabularon en la tabla titulada "Nivel de

aceptación: intrusos". El ideal, como se podrá notar en dicha tabla, es el nivel de aceptación del 80%, pues se ha permitido el acceso a menos intrusos que en los otros niveles.

Por tanto, el mejor nivel de aceptación se puede obtener comparando el porcentaje de individuos válidos reconocidos y el porcentaje de intrusos aceptados como usuarios válidos. Como se vio anteriormente, el ideal para reconocer a los válidos sería el nivel del 60%; sin embargo, a este nivel el porcentaje de intrusos aceptados es muy alto (25% de los válidos), lo cual no es deseable. Al nivel del 80%, se obtuvo un nivel de aceptación de usuarios válidos muy pobre (sólo imagine ser usted el usuario válido y aún así ser aceptado en un sistema tan sólo el 37% de los intentos de ingreso; muy probablemente ello le lleve a la desesperación y a catalogar al sistema como "obsoleto e inútil"); sin embargo, fue el mejor nivel para rechazar a los "intrusos" (sólo fueron aceptados un 3% de los intentos de ingreso de los intrusos; lo cual representa un 9% de los accesos permitidos a usuarios válidos).

Por tanto, lo mejor es hacer un "compromiso" entre el número de accesos permitidos tanto a usuarios como a intrusos. A pesar de no ser el ideal en ninguno de estos dos aspectos, el nivel del 70% de aceptación representa lo mejor en cuanto a ambos criterios. Debido a ello, fue el utilizado

en la verificación de la identidad de este proyecto.

Debido a los resultados obtenidos del análisis anterior, se consideró que (1):

1. El tiempo entre la indicación de ingreso de la clave y el inicio del acto de teclear la misma es muy variable, aun en el mismo individuo; por tanto, dicho tiempo es eliminado durante la verificación de la identidad.

2. El tiempo promedio entre tecla y tecla puede variar según el individuo y la secuencia de caracteres, pero se conserva para el mismo individuo. Por tanto, se considera como una caracterítica personal con la cual es posible verificar la identidad.

(1) Nota: El cambio en la forma de teclear relacionado con la edad, la muerte del usuario u otros factores vinculados a la salud del usuario no han sido considerados, aunque en un período prolongado de tiempo afectarían, pues van más allá de los alcances del presente trabajo.

Porcentaje de aceptación de un intruso respecto al primer individuo

	60%	70%	80%
1	*	*	*
2	90	75	45
3	25	5	0
4	20	0	0
5	75	40	10
6	20	5	0
7	80	50	30
8	10	0	0
9	50	25	5
10	80	65	15

Porcentaje de aceptación de un intruso respecto al segundo individuo

	60%	70%	80%
1	70	40	15
2	*	*	*
3	0	0	0
4	15	5	0
5	50	20	5
6	0	0	0
7	50	25	15
8	0	0	0
9	40	0	0
10	45	20	10

Porcentaje de aceptación de un intruso respecto al tercer individuo

	60%	70%	80%
1	5	0	0
2	5	0	0
3	*	*	*
4	0	0	0
5	0	0	0
6	5	0	0
7	5	0	0
8	5	0	0
9	0	0	0
10	0	0	0

Porcentaje de aceptación de un intruso respecto al cuarto individuo

	60%	70%	80%
1	15	0	0
2	30	0	0
3	0	0	0
4	*	*	*
5	10	5	0
6	10	5	0
7	20	0	0
8	10	0	0
9	10	5	0
10	25	0	0

Porcentaje de aceptación de un intruso respecto al quinto individuo

	60%	70%	80%
1	75	40	10
2	80	50	5
3	10	0	0
4	30	5	5
5	*	*	*
6	25	10	0
7	65	50	10
8	5	0	0
9	45	20	5
10	95	35	10

Porcentaje de aceptación de un intruso respecto al sexto individuo

	60%	70%	80%
1	0	0	0
2	0	0	0
3	0	0	0
4	0	0	0
5	5	0	0
6	*	*	*
7	0	0	0
8	10	10	0
9	0	0	0
10	0	0	0

Porcentaje de aceptación de un intruso respecto al séptimo individuo

	60%	70%	80%
1	75	50	30
2	70	45	45
3	5	0	0
4	20	0	0
5	45	15	0
6	10	0	0
7	*	*	*
8	0	0	0
9	50	20	5
10	75	50	20

Porcentaje de aceptación de un intruso respecto al octavo individuo

	60%	70%	80%
1	0	0	0
2	5	5	0
3	0	0	0
4	5	0	0
5	5	0	0
6	20	10	0
7	0	0	0
8	*	*	*
9	25	0	0
10	5	0	0

Porcentaje de aceptación de un intruso respecto al noveno individuo

	60%	70%	80%
1	10	0	0
2	30	0	0
3	0	0	0
4	10	5	0
5	5	0	0
6	10	5	0
7	20	15	0
8	25	5	0
9	*	*	*
10	20	10	0

Porcentaje de aceptación de un intruso respecto al décimo individuo

	60%	70%	80%
1	35	10	0
2	15	0	0
3	0	0	0
4	0	0	0
5	25	10	0
6	10	0	0
7	25	5	0
8	20	0	0
9	10	0	0
10	*	*	*

Nivel de aceptación
Casos autorizados

Pers.	60%	70%	80%
1	85	75	55
2	90	65	50
3	75	60	30
4	95	70	50
5	90	75	50
6	75	20	5
7	85	60	40
8	70	55	30
9	80	55	20
10	95	75	35
$\bar{X}$	84	61	37

Nivel de aceptación
Intrusos

Pers.	60%	70%	80%
1	50	29	12
2	27	11	5
3	3	0	0
4	13	2	0
5	43	21	5
6	2	1	0
7	35	18	10
8	7	2	0
9	13	4	0
10	14	3	0
$\bar{X}$	21	9	3

Niveles de aceptacion para usuarios autorizados e intrusos