ACIMED
ISSN 1024-9435 *versión impresa*

ACIMED v.11 n.6 Ciudad de La Habana nov.-dic. 2003

Como citar este artículo

La Criptografía como elemento de la seguridad informática

Ing. Yran Marrero Travieso1

Resumen

El surgimiento de redes de comunicación, en particular de Internet, ha abierto nuevas posibilidades para el intercambio de información. Al mismo tiempo, son cada vez mayores las amenazas a la seguridad de la información que se transmite. Es necesario entonces, crear diferentes mecanismos, dirigidos a garantizar la confidencialidad y autenticidad de los documentos electrónicos, todo ello es parte de una nueva tecnología denominada Criptografía. Se aborda el tema de la seguridad informática, en específico las diversas variantes criptográficas: simétrica y asimétrica. Se explican algunos esquemas de manejo de llaves privadas y públicas: RSA y PGP. Finalmente, se tratan algunas de las limitaciones de las soluciones que ofrece esta nueva disciplina.

Descriptores (DeCS): SEGURIDAD COMPUTACIONAL; CONFIDENCIALIDAD
Descriptores (DeCI): SEGURIDAD COMPUTACIONAL; PROTECCION DE DATOS; CRIPTOGRAFIA; CONFIDENCIALIDAD

Abstract

The arise of communication networks, particularly Internet, has paved the way for new chances in information interchange. There are also greater menaces to information security. In this case the creation of several mechanisms to guard the confidentiality and authenticity of electronic documents is necessary. All of this is part of a new technology called cryptography. Information security topics are discussed with emphasis in the cryptographic variants: symetrical and asymetrical. Some schemes for the management of public and private keys: RSA and PSP are exposed. Finally the limitations of some solutions offered by this new discipline are provided.

Subject headings (DeCS): COMPUTER SECURITY; CONFIDENTIALITY
Subject headings (DeCI): COMPUTER SECURITY; DATA PROTECTION; CRYPTOGRAPHY; CONFIDENTIALITY

Si se parte del criterio de que la seguridad se ocupa de la protección de los bienes, parece natural establecer cuáles son los bienes informáticos a proteger. A primera vista, puede decirse que estos son: el hardware; el software y los datos. Entre ellos, los más expuestos a riesgos, son los datos. Se devalúan rápidamente, su tiempo de vida útil suele ser corto y pierden su valor antes que el hardware, cuyo tiempo de vida se estima en 2 ó 3 años, y el software, que en ocasiones, con los mantenimientos oportunos, pueden operar durante más de 5 años.

Las amenazas sobre los sistemas informáticos presentan orígenes diversos. Así, el hardware puede ser

físicamente dañado por la acción del agua, el fuego, los sabotajes, etcétera. Ellos también pueden dañar los medios magnéticos de almacenamiento externo. Pero, además, la información almacenada en estos últimos, también puede afectarse como resultado de la influencia de campos magnéticos intensos y, frecuentemente, por errores de operación. Las líneas de comunicación pueden interferirse o "pincharse". Otra clase de amenaza es la que representan usuarios o empleados infieles, que pueden usurpar la personalidad de usuarios autorizados para acceder y manipular indebidamente los datos de una o más organizaciones.

Amenazas más sutiles provienen de los controles inadecuados de la programación, como es el problema de los residuos, es decir, de la permanencia de información en memoria principal cuando un usuario la libera o, en el caso de dispositivos externos, cuando se borra incorrectamente. Una técnica fraudulenta muy utilizada consiste en transferir información de un programa a otro mediante canales ilícitos, no convencionales (canales ocultos). El análisis del comportamiento de las amenazas a la seguridad de la información revela que la mayoría de los hechos se cometen por intrusos individuales. Un por ciento menor corresponde a incidentes protagonizados por grupos organizados, y en la punta de la pirámide, se ubican los casos de espionaje (industrial, económico, militar...).

Según la Oficina de Ciencia y Tecnología de la Casa Blanca, las pérdidas anuales estimadas en Estados Unidos, debido al espionaje económico ascienden a 100 mil millones de dólares.1

En Internet, las principales amenazas para la protección de la información provienen de:

- Anexos a mensajes enviados por correo electrónico infectados con virus.
- El intercambio de códigos de virus.
- Firewalls o cortafuegos mal configurados.
- Ataques a la disponibilidad de los recursos de información existentes en la red (bancos de datos o software disponibles para descargar por los usuarios).
- La alteración de las páginas web.
- El "repudio" y las estafas asociadas al comercio electrónico.
- Las vulnerabilidades de los sistemas operativos y la desactualización de los "parches" concernientes a su seguridad.
- La rotura de contraseñas.
- La suplantación de identidades.
- El acceso a páginas pornográficas, terroristas, etc.
- El robo y la destrucción de información.
- Pérdida de tiempo durante el acceso a sitios ajenos a la razón social de la entidad.
- El hecho de que herramientas de hacking y cracking se ofrezcan como freeware.

Por estas y otras razones, el tratamiento de los temas relacionados con la seguridad informática ha tomado un gran auge.
Muchas organizaciones gubernamentales y no gubernamentales han preparado documentos, dirigidos a orientar el uso adecuado de las tecnologías existentes y a evitar su uso indebido, que puede ocasionar serios problemas en los bienes y servicios de las empresas en el mundo.2,3

Las medidas tomadas para enfrentar las amenazas informáticas pueden clasificarse en dos grupos:

- Seguridad física y lógica
- Seguridad técnica o lógica

El término seguridad física se emplea frecuentemente para referirse a las medidas de protección externas. Normalmente, se implementan mediante dispositivos eléctricos, electrónicos, etcétera.

Ellas son, probablemente, las primeras que se introducen en todas las instalaciones informáticas. Esto se debe a dos factores; por un lado, ante la ocurrencia de una catástrofe las pérdidas serían completas, por otro, estas medidas de protección son generalmente las más fáciles de tomar. Su costo no es excesivo (con la excepción de los sistemas de continuidad eléctrica) y su mantenimiento no presenta dificultades especiales.

La primera medida de protección para las salas de los centros de procesamiento de datos (CPD), común a todas las amenazas expuestas, es la correcta selección de su ubicación geográfica. Una segunda

consideración, también de carácter general, es su adecuada construcción y su situación idónea dentro del edificio.

Por su parte, las medidas de seguridad técnicas y lógicas, pretenden proteger, tanto el software (sea de base o de aplicación) como los datos. Pueden implementarse en dispositivos hardware o en productos software.

Para el desarrollo de estas medidas, se ha hecho necesaria una investigación académica muy intensa, principalmente durante los últimos 15 años, que ha generado varios modelos teóricos de interés como: el control de accesos, el control del flujo de la información; así como el desarrollo de criptosistemas de clave privada y pública y de sistemas de firma digital y no repudio en la transmisión de datos.1 Cuando se recibe un mensaje no sólo es necesario poder identificar de forma unívoca al remitente, sino que este asuma todas las responsabilidades derivadas de la información que envía. En este sentido, es fundamental impedir que el emisor pueda rechazar o repudiar un mensaje, es decir, negar su autoría sobre la información que envía y sus posibles consecuencias. A esto se denomina no repudio en el contexto de la transmisión de datos.

La posibilidad de interconectarse mediante las redes ha abierto nuevos horizontes para explorar más allá de las fronteras nacionales. Pero con ello, surgieron también nuevas amenazas para los sistemas computarizados y la información que atesoran.

Entre las propiedades más importantes de los documentos electrónicos se encuentran la confidencialidad y la autenticidad.

La primera se refiere a la posibilidad de mantener un documento electrónico inaccesible a todos, excepto a una lista de individuos autorizados. La autenticidad, por su parte, es la capacidad de determinar si uno o varios individuos han reconocido como suyo y se han comprometido con el contenido del documento electrónico.4 El problema de la autenticidad en un documento tradicional se soluciona mediante la firma autógrafa. Mediante su firma autógrafa, un individuo, o varios, manifiestan su voluntad de reconocer el contenido de un documento, y en su caso, a cumplir con los compromisos que el documento establezca para con el individuo.

Los problemas relacionados con la confidencialidad, integridad y autenticidad en un documento electrónico se resuelven mediante la tecnología llamada Criptografía.4

Debido a su importancia entre los aspectos tratados actualmente en materia de seguridad informática, los autores de este trabajo se propusieron realizar una aproximación teórico - práctica al tema con el objetivo de comprender sus principales aristas y determinar algunas de las tendencias fundamentales que caracterizan el desarrollo de esta disciplina.

Métodos

Se realizó una revisión bibliográfica selectiva sobre el tema objeto de estudio. La consulta se realizó en dos niveles: primero, desde la perspectiva de la seguridad informática en general y segundo, dirigida particularmente al tema de la Criptografía. Así, se obtuvo una gran cantidad de documentos generales y específicos que permitieron ubicar y comprender mejor al objeto de estudio particular: la Criptografía, en el contexto de la seguridad informática.

La búsqueda se ejecutó con los términos: "seguridad informática" y "criptografía" en idioma español e inglés en buscadores como Google, Yahoo, Altavista, entre otros. La literatura recuperada es de una tipología variada, sin embargo, es notoria la escasez de bibliografía en idioma español sobre estos temas y además que los autores cubanos no abordan habitualmente dicho tema en la literatura nacional disponible en Internet.

La Criptografía es una rama de las matemáticas que, al orientarse al mundo de los mensajes digitales, proporciona las herramientas idóneas para solucionar los problemas relacionados con la autenticidad y la confiabilidad. El problema de la confidencialidad se vincula comúnmente con técnicas denominadas de "encripción" y la autenticidad con técnicas denominadas de "firma digital", aunque la solución de ambos, en realidad, se reduce a la aplicación de procedimientos criptográficos de encripción y desencripción.4

El uso de técnicas criptográficas tiene como propósito prevenir algunas faltas de seguridad en un sistema computarizado.
La seguridad, en general, se considera como un aspecto de gran importancia en cualquier corporación que trabaje con sistemas computarizados. El hecho de que gran parte de actividades humanas sean cada vez más dependientes de los sistemas computarizados, hace que la seguridad desempeñe una función protagónica.5

Otros autores plantean que la Criptografía se ocupa del problema de enviar información confidencial por un medio inseguro. Para garantizar la confidencialidad, podría asegurarse el medio de transmisión o bien la información; la Criptografía utiliza este último enfoque, encripta la información de manera que, aun cuando se encuentre disponible para cualquiera, no pueda utilizarla, a menos que alguien autorizado la descifre.6

La diferencia entre Criptografía y seguridad informática puede ilustrarse así:

En un modelo criptográfico típico, existen dos puntos: "a" y "b", que se consideran fiables y, entre ellos, se transmite información mediante un canal no fiable. La Criptografía se ocupa de los problemas relacionados con la transmisión confidencial y segura por el medio no fiable, en tanto la seguridad informática se ocupa de asegurar la fiabilidad de los nodos "a" y "b".

La Criptografía se divide en dos grandes ramas, la Criptografía de clave privada o simétrica y la Criptografía de clave pública o asimétrica.5 La primera se refiere al conjunto de métodos que permiten una comunicación segura entre las partes siempre que, con anterioridad, se intercambie la clave correspondiente, que se denomina clave simétrica. La simetría se refiere a que las partes tienen la misma llave, tanto para cifrar como para descifrar.

La Criptografía simétrica, se ha implementado en diferentes tipos de dispositivos: manuales, mecánicos, eléctricos, hasta llegar a las computadoras, donde se programan los algoritmos actuales. La idea general es aplicar diferentes funciones al mensaje que se desea cifrar de modo tal, que sólo conociendo la clave, pueda descifrarse. Aunque no existe un tipo de diseño estándar, tal vez, el más popular es el de *Fiestel*,5 que realiza un número finito de interacciones de una manera particular, hasta que finalmente el mensaje es cifrado. Este es el caso del sistema criptográfico simétrico más conocido: DES (Data Encryption Standard).

Este último, el DES, es un sistema criptográfico que toma como entrada un bloque de 64 bits del mensaje y lo somete a 16 interacciones. Su clave de 56 bits, en la práctica tiene 64 bits, porque a cada conjunto de 7 bits se le agrega un bit que puede utilizarse para establecer la paridad. DES tiene 4 modos de operación: ECB (Electronic Codebook Mode) para mensajes cortos, de menos de 64 bits, CBC (Cipher Block Chaining Mode) para mensajes largos, CFB (Cipher Block Feedback) para cifrar bit por bit o byte por byte y el OFB (Output Feedback Mode) con el mismo uso, pero que evita la propagación de errores.7-11

Hasta el momento, no se ha podido romper el sistema DES mediante la deducción de la clave simétrica a partir de la información interceptada; sin embargo, con un método de fuerza bruta, la prueba de alrededor de 256 posibles claves, pudo descifrarse DES en enero de 1999.5 Ello implica que, es posible obtener la clave del sistema DES en un tiempo relativamente corto; así, se ha vuelto inseguro para propósitos de alta seguridad. La opción que se ha tomado para sustituir a DES es el cifrado múltiple, que aplica varias veces el mismo algoritmo para fortalecer la longitud de la clave y que ha tomado forma como nuevo sistema para el cifrado y se conoce actualmente como triple-DES o TDES.

La Criptografía de clave pública o asimétrica, también denominada RSA por las siglas de los apellidos de sus inventores Rivest Shamir y Adelman, es por definición aquella que utiliza dos claves diferentes para cada usuario, una para cifrar que se llama clave pública y otra para descifrar que es la clave privada. El nacimiento de la Criptografía asimétrica ocurrió como resultado de la búsqueda de un modo más práctico de intercambiar las llaves simétricas.5

El esquema propuesto en RSA se explica así:

Mediante un programa de cómputo cualquier persona puede obtener un par de números, matemáticamente relacionados, a los que se denominan llaves. Una llave es un número de gran tamaño, que usted puede conceptualizar como un mensaje digital, como un archivo binario, o como una cadena de bits o bytes. Las llaves, públicas y privadas, tienen características matemáticas, su generación se produce siempre en parejas,

y se relacionan de tal forma que si dos llaves públicas son diferentes, entonces, las correspondientes llaves privadas son diferentes y viceversa. En otras palabras, si dos sujetos tienen llaves públicas diferentes, entonces sus llaves privadas son diferentes. La idea es que cada individuo genere un par de llaves: pública y privada. El individuo debe de mantener en secreto su llave privada, mientras que la llave pública la puede dar a conocer.

El procedimiento de firma de un documento digital, por ejemplo, implica que, mediante un programa de cómputo, un sujeto prepare un documento a firmar y su llave privada (que sólo él conoce). El programa produce como resultado un mensaje digital denominado firma digital. Juntos, el documento y la firma, constituyen el documento firmado.

Es conveniente señalar que, a diferencia de la firma autógrafa, si dos documentos son diferentes entonces la firma digital también es diferente. En otras palabras, la firma digital cambia de documento a documento, si un sujeto firma dos documentos diferentes producirá dos documentos firmados diferentes. Si dos sujetos firman un mismo documento, también se producen dos documentos firmados diferentes.

El proceso de autentificación se efectúa de la siguiente forma:

Dos puntos I y II mantienen comunicación, conociendo I la llave pública de II. Desde el punto II, se envía un documento firmado digitalmente y un criptograma asociado que sólo es posible hacerse utilizando su clave privada. Entonces I, utilizando la llave pública de II genera un criptograma reflejo, compara ambos criptogramas y, si son iguales, el documento es auténtico.
Si alguna parte del documento o parte de la firma se modifica, aunque sea ligeramente, entonces, el procedimiento de autentificación indicará que el documento no es auténtico. Si una llave pública autentifica un documento firmado, entonces el documento fue firmado con la correspondiente llave privada, es decir, si un individuo tiene asociada la llave pública que autentifica el documento, entonces, el documento fue efectivamente firmado por ese individuo.

A diferencia de la firma autógrafa, que es biométrica, y efectivamente prueba el acto personal de firma, la firma digital sólo prueba que se utilizó la llave privada del sujeto y no necesariamente el acto personal de firma. En consecuencia, no es posible establecer con total seguridad que el individuo firmó un documento, sino que sólo es posible demostrar que es el individuo es el responsable de que el documento se firmara con su llave privada. En otras palabras, si un documento firmado corresponde con la llave pública de un sujeto, entonces el sujeto, aunque no lo haya hecho, debe de reconocer el documento como auténtico.

Por lo tanto, el sujeto debe cuidar de mantener su llave privada en total secreto y no revelársela a nadie, porque de hacerlo es responsable de su mal uso.

Un sujeto, en el proceso de autentificar un documento firmado debe conocer la llave pública del supuesto firmante. El sujeto que autentifique documentos firmados por 10 individuos deberá contar con 10 archivos o con una base de datos, que contenga las 10 llaves públicas de los posibles firmantes. Si este número lo aumentamos a cien, mil o a un millón, el problema crece considerablemente.

Una solución para el problema del manejo de las llaves es el conocido certificado digital.4
Un certificado digital es un documento firmado digitalmente por una persona o entidad denominada autoridad certificadora (AC). Dicho documento establece un vínculo entre un sujeto y su llave pública, es decir, el certificado digital es un documento firmado por una autoridad certificadora, que contiene el nombre del sujeto y su llave pública. La idea es que quienquiera que conozca la llave pública de la AC puede autentificar un certificado digital de la misma forma que se autentifica cualquier otro documento firmado.

Si el certificado es auténtico y confiamos en la AC, entonces, puede confiarse en que el sujeto identificado en el certificado digital posee la llave pública que se señala en dicho certificado. Así pues, si un sujeto firma un documento y anexa su certificado digital, cualquiera que conozca la llave pública de la AC podrá autentificar el documento.

Pretty Good Privacy (PGP)

Los conceptos expuestos anteriormente tienen su expresión práctica en el programa Pretty Good Privacy (Privacidad Bastante Buena) creado por Phill Zimmermann, que es el estándar de facto utilizado para la encriptación de correos electrónicos, discos duros, comunicaciones de voz y muchas otras aplicaciones.6

PGP Enterprise Security ofrece una infraestructura de cifrado y autentificación capaz de mantener la seguridad de los datos del correo electrónico, de los archivos, las carpetas y los volúmenes en el disco. Las aplicaciones "cliente" de PGP incluyen interfaz fáciles de utilizar para mantener la seguridad de los datos, mientras que las aplicaciones "servidor" PGP proporcionan la adaptabilidad necesaria para ampliaciones y el cumplimiento de las políticas de los sistemas.13

Cuando se implementa en entornos empresariales, PGP Enterprise Security se convierte en una infraestructura completa de cifrado y autentificación, adaptable a las ampliaciones y con facilidad de administrar.

PGP Enterprise Security es una solución adaptable y compatible entre plataformas, que permite a los usuarios proteger la correspondencia electrónica, las transacciones en línea y los archivos de datos mediante su cifrado de forma que únicamente los destinatarios previstos puedan descifrar su contenido. Debido a que los productos PGP, trabajan sobre complejos algoritmos criptográficos y longitudes de clave específicas, se asegura una protección definitiva de los datos almacenados en las computadoras y que se transmiten por intranets e Internet. Para una mayor seguridad, PGP incorpora además, un sistema de firma digital que verifica la propiedad e integridad de los documentos.

PGP se conoce internacionalmente como el sistema estándar para mantener la seguridad del correo electrónico y de los archivos. PGP no sólo se adapta a un nivel superior para los entornos empresariales, sino que también se adapta a un nivel inferior para los individuos. Este hecho es cada vez más importante, porque las compañías intercambian sus datos críticos no sólo internamente, sino también con consultores o socios en el exterior.13

Su funcionamiento es muy sencillo, cada usuario tiene dos llaves: una pública y otra privada. La pública es la que distribuye a los demás y sirve para que ellos puedan enviarle un mensaje codificado que solo él mediante su llave privada podrá descifrar. También ofrece la posibilidad de firmar un mensaje al colocar una parte de su llave privada (irreconocible claro) en una firma, que actúa como un certificado de autenticidad. Cuando el destinatario recibe el mensaje, el PGP comprueba la firma y texto y lo compara con la llave pública que tiene del remitente, y si algo en el texto o la firma ha cambiado envía un mensaje de error donde informa que el mensaje no corresponde a la persona que dice que nos envía el mensaje.

Sirve también para enviar ficheros codificados en formato ASCII por correo electrónico. Es mucho mejor que otros sistemas como el UUENCODE porque antes de codificar el fichero, el PGP realiza una compresión ZIP del documento o programa que codificará.

PGP puede descargarse gratuitamente en http://www.pgpi.com y sus versiones más populares son la 2.6 (para MS-DOS) y la actual 6.0.2 (para Windows 9x). También existen versiones de PGP para Macintosh, Unix, Linux y para casi cualquier sistema operativo actual que sea medianamente popular.

Desde el punto de vista del usuario, el PGP es muy cómodo para gestionar las claves (que es precisamente lo más difícil en los sistemas de clave pública). Las claves se almacenan en dos archivos: secring.skr (que guarda las claves privadas) y pubring.pkr (que registra las claves públicas). Estos archivos son una especie de "llaveros", donde se colocan nuestras llaves privadas, públicas y las llaves públicas de los demás. Obviamente, si se pierde algunos de ellos, no se podrá desencriptar ni encriptar ningún mensaje, por lo que es buena idea guardar una copia en un lugar seguro.

También PGP guarda la "semilla" para generar nuestras claves aleatorias en el archivo randseed.bin, el cual es otro archivo importante que no puede quedar expuesto al robo. Si randseed.bin se borra, PGP creará otro automáticamente a partir del reloj interno de la computadora, e igualmente es recomendable guardar una copia suya en algún lugar seguro.

PGP tiene además, una función muy útil llamada "armadura ASCII" que permite convertir los archivos encriptados de cualquier tipo en ficheros de texto ASCII. Así, por ejemplo, un archivo binario, como sucede

con un programa, puede encriptarse, convertirse en texto ASCII y enviarse como texto simple por correo.

Limitaciones de la Criptografía

Los algoritmos criptográficos tienden a degradarse con el tiempo. A medida que transcurre el tiempo, los algoritmos de encripción se hacen más fáciles de quebrar debido al avance de la velocidad y potencia de los equipos de computación.
Todos los algoritmos criptográficos son vulnerables a los ataques de fuerza bruta -tratar sistemáticamente con cada posible clave de encripción, buscando colisiones para funciones hash, factorizando grandes números, etc.- la fuerza bruta es más fácil de aplicar en la medida que pasa el tiempo.

En 1977 Martin Gardner escribió que los números de 129 dígitos nunca serían factorizados, en 1994 se factorizó uno de esos números. Además de la fuerza bruta, avanzan las matemáticas fundamentales que proveen nuevos métodos y técnicas de criptoanálisis.6

Conclusiones

1. Debido a las cambiantes condiciones y nuevas plataformas de computación disponibles, es vital el desarrollo de documentos y directrices que orienten a los usuarios en el uso adecuado de las tecnologías para aprovechar mejor sus ventajas.
2. El auge de la interconexión entre redes abre nuevos horizontes para la navegación por Internet y con ello, surgen nuevas amenazas para los sistemas computarizados, como son la pérdida de confidencialidad y autenticidad de los documentos electrónicos.
3. La Criptografía es una disciplina/tecnología orientada a la solución de los problemas relacionados con la autenticidad y la confidencialidad, y provee las herramientas idóneas para ello.
4. Los usuarios son quienes deben elegir la conveniencia de una u otra herramienta para la protección de sus documentos electrónicos.

Referencias bibliográficas

1. Aneiro Rodríguez LO. Elementos de arquitectura y seguridad informática. La Habana: Instituto Superior Politécnico "Eduardo García Delgado", 2000.
2. Organization for Economic Cooperation and Development. Guidelines for security of information systems. New York: Lippincott; 1992.
3. National Institute of Standard and Technology. General Principles for Information Systems Security Policies. New York: Mc Graw Hill, 1996.
4. Mendvil I. El ABC de los documentos electrónicos seguros. Disponible en: http://www.criptored.upm.es/guiateoria/gt_m163a.htm Acceso: 20 de enero del 2003.
5. Angel Angel JJ. Criptografía para principiantes. Disponible en: http://www.htmlweb.net/seguridad/cripto_p/cripto_princ_1.html Acceso: 15 de enero del 2003.
6. Bradanovic T. Algo sobre Criptografía. Disponible en: http://www.vcd.cl/tombrad/pcasual/ayuda5.html Acceso: 20 de enero del 2003.
7. Menezes AJ, Oorschot PC, Vanstone SA. Handbook of applied Cryptography. Disponible en: http://www.cacr.math.uwaterloo.ca/hac/ Acceso: 10 de febrero del 2003 [STANDARDIZEDENDPARAG]
8. American National Standards Institute. ANSI X3.92 American National Standard- Data Encryption Algorithm. Washington DC: American National Standards Institute,1981.
9. Federal Information Processing Standards. Data Encryption Standard (FIPS 46-2). Disponible en: http://www.itl.nist.gov/fipspubs/fip46-2.htm Acceso: 20 de febrero del 2003.
10. American National Standards Institute. ANSI X3.106 American National Standard - Data Encryption Algorithm Modes of Operation. Washington DC:American National Standards Institute,1983.
11. Federal Information Processing Standards. FIPS 81. DES modes of operation. Disponible en: http://www.itl.nist.gov/fipspubs/fip81.htm Acceso: 24 de febrero del 2003.
12. ISO. ISO 8372 Information processing - Modes of operation for a 64-bit block cipher algorithm. Geneva: ISO, 1997.
13. Hispasec Sistemas. PGP Enterprise: Componentes de PGP Enterprise Security. Seguridad de comunicación mundial con PGP. Disponible en: http://www.hispasec.com/directorio/laboratorio/articulos/PGPEnterprise/03.html Acceso: 6 de febrero

del 2003.

Recibido: 18 de septiembre del 2003. Aprobado: 5 de octubre del 2003
Ing. *Yran Marrero Travieso*. Centro Provincial de Información de Ciencias Médicas. La Habana. Carretera a Catalina Km ½ Güines CP 33 900 Correo electrónico: ymar@infomed.sld.cu

---