Lic Sergio Daniel Conde - Ing. Osvaldo D. Marcovecchio

Facultad de Ingeniería - Universidad de la Marina Mercante.

Un sistema estocástico de cifrado

Resumen

En la actualidad los sistemas de encriptación utilizan métodos que se valen de algoritmos y funciones, junto a las altas velocidades de procesamiento de la CPU, que resuelven rápidamente funciones muy complejas.
Los algoritmos actuales se agrupan en dos grandes clases según se utilicen claves idénticas o distintas, para los procesos de encriptación y desencriptación.
Si usan la misma clave se los llama algoritmos de claves simétricas y si utilizan una clave para encriptar y otra para el proceso inverso se los llama algoritmos de claves asimétricas.

- DES: Adoptado como estándar ANSI en 1977.
- DESX: Variación de DES que introduce un proceso de cifrado en dos partes.
- TRIPLE DES: Algoritmo DES que utiliza 3 claves distintas
- RC2: Sistema de cifrado en bloques.
- RC4: Sistema de cifrado de flujo.

También hay investigaciones en el campo de la física que estudian la encriptación cuántica, basándose en la utilización de ecuaciones no lineales de solución caótica y transmitiendo fotones.
El trabajo propone una herramienta donde se fomenta la protección adecuada de la información aplicando diferentes métodos.

Palabras Clave

Criptografia. Seguridad Informática. Protección de datos. Control de acceso.

Abstract

The purpose of this work is the realization of an encryption system that works in a stochastic, using the application of combinatorial analysis and probability calculations.
The application of the system can be measured from an ethical / social / safety in a positive way, to safeguard the information that is specific to each individual.
Computer security is responsible for reviewing applicable policies and procedures relating to security within the Data Processing Center (DPC).
Ensure availability and service continuity.
Propose logical security controls in the server computers of the Data Processing Center. Educate users responsible for processing information about computer security.

Key Words

Cryptography. Computer Security. Data protection. Access Control.

1. Introducción

La propuesta de este trabajo es la realización de un sistema de encriptación que trabaje de manera estocástica, valiéndose de la aplicación del análisis combinatorio y el cálculo de probabilidad.
La aplicación del sistema puede medirse a nivel ético/social/seguridad de manera positiva, al salvaguardar la información que es propia de cada individuo.
La seguridad informática se encarga de estudiar políticas aplicables, y procedimientos relativos a la seguridad dentro del Centro de Procesamiento de Datos (CPD).
Asegurar la disponibilidad y continuidad del servicio. Proponer controles de seguridad lógica en los equipos servidores del Centro de Procesamiento de Datos.

Concientizar a los usuarios responsables del tratamiento de la información acerca de la seguridad informática.

2. Desarrollo

2.1. *¿Qué es la encriptación?*

Es la técnica que permite la transformación de información inteligible en una secuencia ininteligible. Para lograr esto, la criptografía actualmente se vale de algoritmos y funciones matemáticas.

En la antigüedad, ya se conocía la importancia de cierta información, por lo tanto la criptografía se desarrolló paralelamente a la tecnología militar y en las relaciones internacionales.

La criptografía se basa en dos procesos complementarios, la encriptación y la desencriptación, también pueden denominarse cifrado y descifrado o codificación y decodificación. El primero es la transformación de información inteligible en ininteligible, el segundo es el proceso inverso.

2.2. *De la antigüedad a hoy*

Los sistemas antiguos de cifrado se basaban en el corrimiento de letras del abecedario utilizado (se remplazaban las letras por otras que resultaban de la suma de un valor constante). Posteriormente se hicieron transposiciones de columnas y filas del texto o cambiar sílabas por valores de tablas.

En la actualidad los sistemas de encriptación utilizan métodos que se valen de algoritmos y funciones, unidas estas a las altas velocidades de procesamiento por CPU, resuelven rápidamente funciones muy complejas.

Los algoritmos actuales se agrupan en dos grandes clases según se utilicen claves idénticas o distintas para los procesos de encriptación y desencriptación. Si usan la misma clave se los llama algoritmos de claves simétricas y si utilizan una clave para encriptar y otra para el proceso inverso se los llama algoritmos de claves asimétricas.

2.3. *Algoritmos simétricos más comunes*

- DES: Adoptado como estándar ANSI en 1977. (técnica de cifrado en 56 bits).
- DESX: Variación de DES que introduce un proceso de cifrado en dos partes.
- TRIPLE DES: Algoritmo DES que utiliza 3 claves distintas
- RC2: Sistema de cifrado en bloques (admite claves desde 1 a 2048 bits).
- RC4: Sistema de cifrado de flujo (admite claves desde 1 a 2048 bits).

2.4. *Algoritmos asimétricos más comunes*

Estos sistemas se basan en dos claves, una pública y otra privada, la primera se genera a partir de la privada, en estos casos el mensaje se cifra con la clave pública que es la que se da a conocer y se lo descifra con la privada

- Diffie-Hellman key exchange: sistema para generar e intercambiar llaves compartidas por un canal no seguro.
- RSA: Sistema de claves públicas desarrolladas en el MIT.
- DSS: Sistema de firma digital desarrollado por la Agencia de Seguridad Nacional de los EEUU. (trabaja entre 512 y 1024 bits).

2.5. *Seguridad Lógica*

Existe un viejo dicho en la seguridad informática que dicta que "todo lo que no está permitido debe estar prohibido" y esto es lo que debe asegurar la Seguridad Lógica, podemos pensar en la Seguridad Lógica como la manera de aplicar procedimientos que aseguren que sólo podrán tener acceso a los datos las personas o sistemas de información autorizados para hacerlo.

Los objetivos que se plantean serán:

Restringir el acceso a los programas y archivos.

Los operadores deben trabajar sin supervisión minuciosa y no podrán modificar ni programas archivos que no correspondan.

Asegurar que se estén utilizando los datos, archivos y programas correctos en y por el procedimiento correcto.

Asegurar que la información transmitida sea recibida sólo por el destinatario al cual ha sido dirigida y por ningún otro.

Asegurar que la información que el destinatario ha recibido sea la misma que ha sido transmitida.

2.6. *Controles de Acceso*

Los controles de acceso pueden implementarse a nivel de Sistema Operativo, de sistemas de información, en bases de datos, en un paquete específico de seguridad o en cualquier otro utilitario. Estos controles constituyen una ayuda importante para proteger al sistema operativo de la red, a los sistemas de información y software adicional; también para mantener la integridad de la información (restringiendo la cantidad de usuarios y procesos con autorización de acceso) y para resguardar la información confidencial de accesos no autorizados.

Las consideraciones relacionadas al procedimiento que se lleva a cabo para determinar si corresponde un permiso de acceso solicitado por un usuario, a un determinado recurso son planteadas por el National Institute for Standards and Technology (NIST) en el NIST Handbook [i]; donde se encuentran resumidos los siguientes esquemas para dotar de seguridad a cualquier sistema.

[i] http://www.csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf

2.7. *Identificación y Autentificación*

Se constituye en la primera línea de defensa para la mayoría de los sistemas computarizados, al prevenir el ingreso de personas no autorizadas y es la base para casi todos los controles de acceso, además permite efectuar un seguimiento de las actividades de los usuarios. Identificación es cuando el usuario se da a conocer en el sistema; y Autentificación es la verificación que realiza el sistema de la identificación.

2.8. *Roles*

El acceso a la información puede ser controlado también, considerando la función o rol del usuario que requiere dicho acceso. Algunos ejemplos de roles serían los siguientes:

- Líder de proyecto.
- Programador.
- Operador.
- Jefe de un área usuaria.

Los derechos de acceso se agrupan de acuerdo con un rol determinado y el uso de los recursos se restringe a las personas autorizadas a asumir dicho rol, cambiar de rol implicaría salir del sistema y reingresar. El uso de roles es una manera bastante efectiva de implementar el control de accesos, siempre que el proceso de definición de roles esté basado en un profundo análisis de cómo la organización opera. Es importante aclarar que el uso de roles no es lo mismo que el uso compartido de cuentas.

2.9. *Limitaciones a los Servicios*

Las limitaciones a los servicios son controles que se refieren a las restricciones que dependen de parámetros propios de la utilización de la aplicación o que han sido preestablecidos por el administrador del sistema. Un ejemplo de este tipo de control es cuando en un cajero automático establece un límite para la cantidad de dinero que se puede transferir de una cuenta a otra, y también para los retiros. Otro ejemplo podría ser cuando los usuarios de una red, tienen permitido intercambiar emails entre sí, pero no tienen permitido conectarse para intercambiar emails con usuarios de redes externas.

2.10. *Modalidad de Acceso*

Adicionalmente se considera cuando un acceso se permite, se debe tener en cuenta también que tipo de acceso o modo de acceso se permitirá. El concepto de modo de acceso es fundamental para el control respectivo, los modos de acceso que pueden ser usados son:

- Lectura.
- Escritura.
- Ejecución.
- Borrado.

Además existen otras modalidades de acceso especiales, que generalmente se incluyen en los sistemas de aplicación:

- Creación.
- Búsqueda.

Estos criterios pueden ser usados de manera conjunta con otros, por ejemplo, una organización puede proporcionar a un grupo de usuarios acceso de Escritura en una aplicación en cualquier momento dentro del horario de oficina, y acceso sólo de lectura fuera de él.

2.11. *Ubicación y Horario*

El acceso a determinados recursos del sistema puede estar basado en la ubicación física o lógica de los datos o personas. En cuanto al horario, el uso de parámetros como horario de oficina o día de semana son comunes cuando se implementan este tipo de controles, que permiten limitar el acceso de los usuarios a determinadas horas.

2.12. *Control de Acceso Interno*

Los controles de acceso interno determinan lo que un usuario (o grupo de usuarios) puede o no hacer con los recursos del sistema. Se detallarán cinco métodos de control de acceso interno:

2.13. *Palabras Clave (Passwords)*

Las palabras clave o passwords, están comúnmente asociadas con la autenticación del usuario, pero también son usadas para proteger datos, aplicaciones e incluso PC's. Por ejemplo, una aplicación de contabilidad puede solicitar al usuario un password, en caso de que aquel desee acceder a cierta información financiera. Los controles implementados a través de la utilización de palabras clave resultan de muy bajo costo e incluyen una gran variedad de aplicaciones.

2.14. *Listas de Control de Accesos*

Estas listas se refieren a un registro de:

Usuarios (incluye grupos de usuarios, computadoras, procesos), a quienes se les ha proporcionado autorización para usar un recurso del sistema.

Los tipos de acceso que han sido proporcionados.

Hay una gran flexibilidad para el manejo de estas listas, pueden definir también a que usuario o grupos de usuarios se les niega específicamente el acceso a un recurso. Se pueden implementar Listas de Control de Accesos Elementales y Avanzadas.

2.15. *Límites sobre la interface de usuario*

Comúnmente utilizados en conjunto con listas de control de accesos, estos límites restringen a los usuarios a funciones específicas. Pueden ser de tres tipos:

- Menús.
- Vistas sobre la Base de Datos (BD).
- Límites físicos sobre la interface de usuario.

Los límites sobre la interface de usuario pueden proporcionar una forma de control de acceso muy parecida a la forma en que la organización opera, es decir, el Administrador del Sistema restringe al usuario a ciertos comandos, generalmente a través de un menú. Las vistas sobre la Base de datos, limitan el acceso de los usuarios a los datos contenidos en la BD, de tal forma que los

usuarios dispongan sólo de aquellos que puedan requerir para cumplir con sus funciones en la organización.
Un ejemplo de los límites físicos sobre la interface de usuario se da en un cajero automático, que proporciona un número determinado de botones para seleccionar opciones.

2.16. *Control de Acceso Externo*

Los controles de acceso externo son una protección contra la interacción de nuestro sistema con los sistemas, servicios y gente externa a la organización. Dispositivos de control de puertos. Estos dispositivos autorizan el acceso a un puerto determinado del equipo host y pueden estar físicamente separados o incluidos en otro dispositivo de comunicaciones, como por ejemplo un módem. Los dispositivos de control de puertos actúan de manera previa e independiente de las funciones de control de acceso propias del computador y comúnmente son usados en comunicaciones seriales.

2.17. *Firewalls o Puertas de Seguridad*

Los firewalls permiten bloquear o filtrar el acceso entre dos redes, generalmente una privada y otra externa (por ejemplo Internet), entendiendo como red privada una "separada" de otras. Las puertas de seguridad permiten que los usuarios internos se conecten a la red exterior al mismo tiempo que previenen la intromisión de atacantes o virus a los sistemas de la organización, adicionalmente a estos beneficios los firewalls reducen la carga del sistema en procesos de seguridad y facilitan la centralización de servicios.

2.18. *Autenticación Basada en el Host*

La autenticación basada en Host, proporciona el acceso según la identificación del Host en el que se origina el requerimiento de acceso, en lugar de hacerlo según la identificación del usuario solicitante. Un ejemplo de autenticación basada en Host es el Network File System (NFS) que permite a un servidor poner a disposición de un grupo específico de computadoras determinados sistemas y/o directorios.

2.19. *Seguridad Física*

Se argumenta que la seguridad perfecta sólo existe en una habitación sin puertas, pero eso naturalmente no es posible, en la actualidad el objetivo es prevenir, detectar y detener las rupturas de seguridad informática y de las organizaciones. ISO 27001 ofrece un marco para la definición de la seguridad informática en la organización y ofrece mecanismos para administrar el proceso de seguridad.

2.20. *Propuesta*

Se desarrolla un sistema de encriptación para el transporte de datos, entre dos puntos, a través de cualquier medio existente o futuro, para la comunicación de información sensible.
Que sea simple de operar, transparente al medio de enlace, para lograr una total independencia en la contratación del carrier por parte de los usuarios.
El sistema de encriptación propuesto, es un sistema estocástico. Resuelve por medio de probabilidades el resultado de cada proceso y hace una composición de datos y ruido. No maneja claves en forma directa ni preestablecida, ya que esas decisiones las toma el software.
Las cabeceras que posee son exclusivas para su uso interno y pueden publicarse sin alterar la seguridad e integridad de la información cifrada.
El nivel de seguridad no decae por conocer parte de la información cifrada, más aún, no se podría conocer el proceso de cifrado aunque se tuviera junto al texto encriptado el original.
Todo esto hace al COD un sistema de seguridad que ofrece la más alta seguridad para encriptar información.
Utilizando técnicas criptográficas podemos enviar información sensible a través de un medio no seguro. Si la técnica utilizada presupone transferir alguna parte de la clave por un canal seguro entonces no sería preciso cifrar el mensaje, pues utilizaríamos el canal seguro para la transferencia de la información. Algunos métodos de cifrado aseguran un gran nivel de seguridad, pero esta decae exponencialmente si se tiene alguna parte del mensaje.
El proyecto garantiza que esa información sea accesible solo por aquellas personas que estén autorizadas.

2.21. *El sistema*

Básicamente se puede definir al sistema por sus partes esenciales y son:

- Un generador de ruido blanco.
- Aplicación de una distribución binomial con los valores obtenidos.
- Ubicación del próximo valor más probable.
- Introducción del valor anteriormente obtenido en el cálculo combinatorio.

Señalamos la importancia del generador de ruido blanco ya que los valores producidos no pueden ser pseudoaleatorios, años atrás habría que haber utilizado algún medio físico (riesgoso como elementos radiactivos o más seguros como por ejemplo la polarización de un diodo en inversa y aprovechar la inestabilidad que produce), hoy es más sencillo, se puede obtener un muy buen generador de valores aleatorios desde una planilla Excel, o bien utilizando como base de alguna función no líneal una semilla random en alguno de los entornos de programación que se ofrecen al mercado.
Los elementos enumerados anteriormente como base del sistema de encriptación estocástico son a grandes rasgos las etapas que se debieron realizar en el trabajo.
Primeramente se realizó el módulo de generación de ruido blanco, se controló la generación de valores que no hubiera correlación.
Por ejemplo: Suponga que la información que va a pasar por el canal de transmisión sin codificar es:

"Hola amigo, te aviso que llego mañana en el vuelo de las 11 horas, su número es el 1166"

Canal de Transmisión

La que pasaría por el canal de transmisión una vez codificada podría ser:

"¡2~☺(m¢x˅°☹ıt ¶½À ☹¼ "$#® ,>nb<'; ;7[sd w fp}"

Canal de Transmisión

En este paquete estaría la información del primer texto ya codificado. Hay que tener en cuenta que los archivos encriptados aumentan en tamaño respecto del original en unas 10 veces, o sea, si el archivo original es de 1 Kbyte el encriptado rondará los 10 Kbyte.
De este modo en el medio de transmisión (par telefónico, telefonía celular, radio Módem, acceso a satélite) la información que viaja será la codificada.

2.22. *Ventajas*

- Simple de Implementar.
- Fácil aprendizaje para su Utiliza-ción.
- Altísimo nivel de Seguridad y Confidencialidad de las Comunicaciones.
- Transparencia con el Medio de Comunicaciones Empleado.
- Solo el Destinatario es capaz de devolver los originales.
- Posibilidad de envíos:
- A un único destinatario.
- A un grupo primario de destinatarios.
- A todos los grupos.

2.23. *El Proceso*

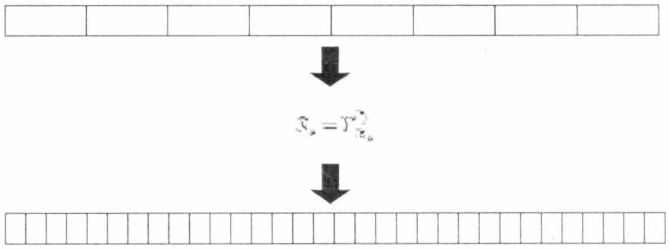
Se obtienen una cantidad de valores random (Pj), este proceso puede ser paralelizable y es realizado durante toda la operación [Ecuación 1]

$$P_j = \frac{1}{2^{48}}$$

Ecuación 1
Se fijan condiciones iniciales las cuales indican el entorno aceptable de la diferencia entre dos números random tomados al azar y el cociente de la diferencia anterior, en los experimentos se utilizó un entorno el cual aceptaba diferencias que iban entre el 20% al 80%.

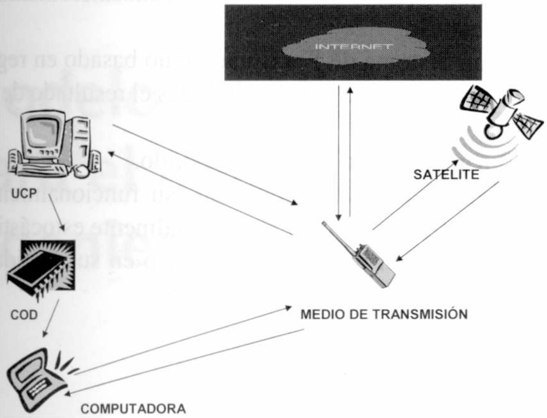
$$0.2 < \frac{P_{(j-1)} - P_j}{P_{(j-k-1)} - P_{(j-k)}} < 0.8$$

Ecuación 2
Si el valor está dentro de las condiciones prefijadas, entonces se toma un tramo del archivo a encriptar (en el experimento se tomó de a un byte y se lo combinó con el valor de ruido Pj en un espacio nuevo de 4 bytes) y se lo permuta de acuerdo al valor de ruido obtenido.
Byte original: Bn

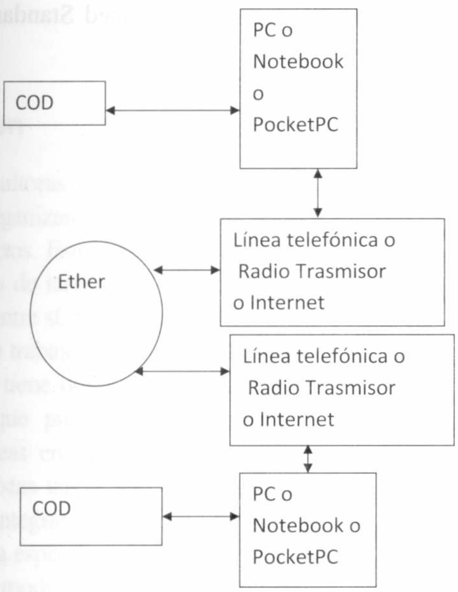


Donde Sn es la variación sin repetición del byte de información tratado para ese instante de tiempo, cada uno de sus componentes (bit) es ubicado en la posición que de la permutación indicada por el valor generado y aceptado para esa ocasión y los espacios vacíos hasta la cantidad de 32 bits es completada por el valor del ruido discretizado, el resultado a la salida será un conjunto de valores combinados al azar de valores del dato del Byte y de los valores generados totalmente desordenados.
En el caso que los valores de probabilidad arrojados en el cálculo no caen dentro del entorno prefijado, se completa una línea (en el experimento la línea se la definió de 32 bits) con el ruido generado que no cumple las condiciones.
Se observó que el tamaño del archivo de salida (encriptado) con las condiciones iniciales mencionadas más arriba tuvo un crecimiento promedio de diez veces. No se verificaron repeticiones al encriptar un mismo archivo varias veces ni en tamaño ni en contenido, la entropía del sistema fue muy alta.

2.24. *Fácil Implementación*

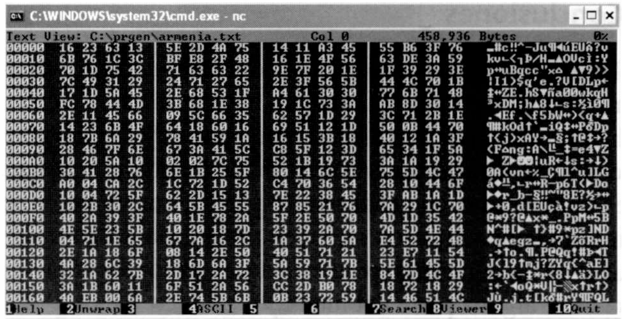


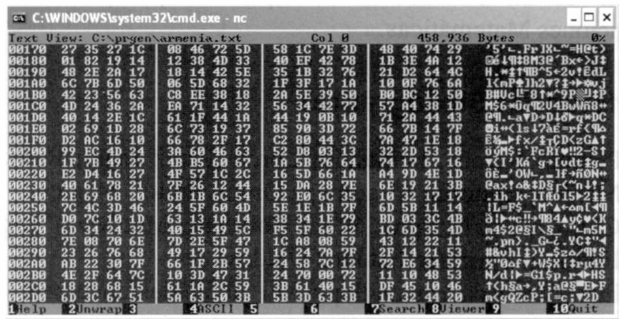
2.25. *Esquema Básico de Funcionamiento*

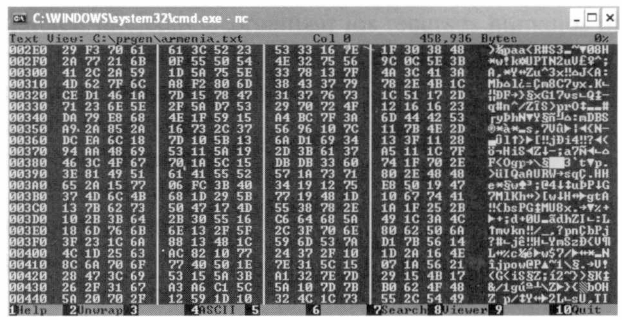


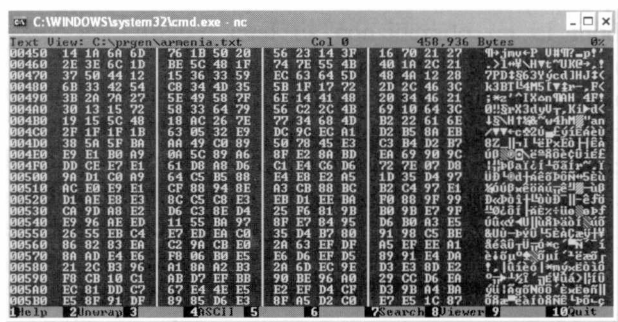
2.26. *Demostración de Encriptación*

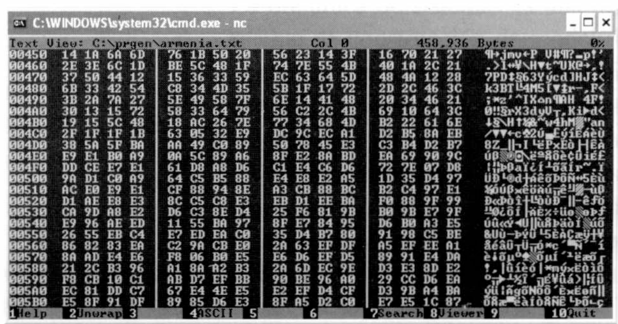
Archivo Hoy.











3. Conclusiones

Utilizando técnicas criptográficas podemos enviar información sensible a través de un medio no seguro. Si la técnica utilizada presupone transferir alguna parte de la clave por un canal seguro entonces no sería preciso cifrar el mensaje, pues utilizaríamos el canal seguro para la transferencia de la información. Algunos métodos de cifrado aseguran un gran nivel de seguridad, pero esta decae exponencialmente si se tiene alguna parte del mensaje.

COD es un Sistema de Encriptación que no utiliza Funciones Matemáticas.

COD es un Sistema de Encriptación que no funciona Sincrónicamente, no utiliza Pseudosincronismo ni Pseudoaleatorio.

COD es un Sistema de Encriptación no basado en reglas.

Resuelve por medio de probabilidades el resultado de cada proceso.

Hace una composición de datos y ruido.

No maneja claves preestablecidas, su funcionamiento lo resuelve en tiempo real en forma totalmente estocástica.

Conocer parte del mensaje sin cifrar o en su totalidad no permite conocer el proceso de cifrado.

Referencias Bibliográficas

1. Picouto Ramos, Fernando; Lorete Pérez Iñaki; Ramos Varón, Antonio; "Hacking y Seguridad en Internet(2008). México; Editorial Alfaomega Grupo Editor. México
2. Cid, Carlos; Murphy, Sean; Robshaw, Matthew; "Algebraic Aspects of the Encryption Advanced Standard(2008). Editorial Springer. Estados Unidos.
3. http://www.catarina.udlap.mx/u_dl_a/tales/documentos/lap/carmona_c_dc/capitulo1.pdf