
UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES CUAUTITLÁN

# LA CRIPTOGRAFÍA COMO ELEMENTO DE LA SEGURIDAD INFORMÁTICA

T E S I S

QUE PARA OBTENER EL TÍTULO DE:

LICENCIADO EN INFORMÁTICA

PRESENTA:

DAVID GLORIA HERNÁNDEZ

ASESOR: MAC. DOMINGO MÁRQUEZ ORTEGA

CUAUTITLÁN IZCALLI, ESTADO DE MÉXICO 2014

# ÍNDICE

# CAPÍTULO I. ANTECEDENTES Y EL ESTADO DEL ARTE

## 1.1 Introducción

Debido a que el uso de Internet se encuentra en aumento, cada vez más compañías permiten a sus socios y proveedores acceder a sus sistemas de información. Por lo tanto, es fundamental saber qué recursos de la compañía necesitan protección para así controlar el acceso al sistema y los derechos de los usuarios del sistema de información. Los mismos procedimientos se aplican cuando se permite el acceso a la compañía a través de Internet.

Además, debido a la tendencia creciente hacia un estilo de vida nómada de hoy en día, el cual permite a los empleados conectarse a los sistemas de información casi desde cualquier lugar, se pide a los empleados que lleven consigo parte del sistema de información fuera de la infraestructura segura de la compañía.

### 1.1.1 Orígenes

A partir de los años 80 el uso del ordenador personal comienza a hacerse común, apareciendo por la preocupación por la integridad de los datos almacenados. En la década de los años 90's comienzan a aparecer los virus y gusanos y se toma conciencia del peligro que nos acecha como usuarios de PC's y equipos conectados a internet. Además comienzan a proliferar ataques a sistemas informáticos, y la palabra hacker aparece incluso en la prensa. Al final de los 90's las amenazas empezaron a generalizarse, aparecen nuevos gusanos y malware generalizado. Y a partir del año 2000 los acontecimientos fuerzan a que se tome muy en serio la seguridad informática.[1]

Principalmente por el uso masivo de internet, el tema de la protección de la información se ha transformado en una necesidad y con ellos se populariza la terminología técnica asociada a la criptología:

- Cifrado, descifrado, criptoanálisis, firma digital.
- Autoridades de certificaciones, comercio electrónico.

Ya no solo se comentan estos temas en las universidades. Cualquier usuario desea saber, por ejemplo qué significa un email o qué significa que en una comunicación con su banco aparezca un candado en la barra de tareas de su navegador y le diga que el enlace es SSL con 128 bits, además de que el software actual viene con seguridad o embebida.

[1] Aguado, D. P. (2012). *Seguridad Informática para el Hogar*. Ed. Bubok

En los principios de la informática en los años 80 las organizaciones que utilizaban redes informáticas empezaron a comprender que múltiples equipos conectados en diversos lugares eran mucho más vulnerables que un mainframe único. Por ello surgió la necesidad de dotar a estos sistemas de medidas de seguridad de la información, y de formar profesionales cualificados para planificar e implementar los procedimientos y políticas de seguridad.

A partir de los inicios de la seguridad informática en 1983 se dio a conocer los primeros virus experimentales y la primera definición de "virus informático" que se menciona a continuación: Es una amenaza programada, es decir, es un pequeño programa escrito intencionadamente para instalarse en el ordenador de un usuario sin el conocimiento o el permiso de este. Decimos que es un programa parásito porque el programa ataca a los archivos o al sector de "arranque" y se replica a sí mismo para continuar su propagación.[2]

En 1985 comenzaron a aparecer los primeros virus informáticos, el primero de ellos se llamaba ELK CLONER (1985): el primer virus para computadores personales, concretamente para los sistemas Apple II. Creado por un estudiante, el virus infectaba al sistema operativo. Otro de los virus informáticos que se dio a conocer fue el "Virus Jerusalén" que es uno de los más destacados en la historia de los virus informáticos. Su descubrimiento y aislamiento en 1987 por la Universidad Hebrea de Jerusalén puso en vela a cientos de usuarios.

En 1994 se adoptó el Acta Federal de Abuso Computacional (18 U.S.C. Sec. 1030), modificando el Acta de 1986. Aquí se contempla la regulación de los virus (computer contaminant).

### 1.1.2 Herramientas para la Seguridad Informática

A continuación se mostrará las herramientas que usa la seguridad informática para prevenir amenazas que puedan ocasionar pérdidas de información, las herramientas que describe el autor Royer, J. M a continuación son herramientas de seguridad y hacking. Estas se utilizan para fines tanto legales como ilegales, y por lo tanto, la mayoría de las personas piensan que estas herramientas son solo utilizadas por hackers maliciosas (algo totalmente fuera de la realidad),

[2] Royer, J. M. (2004). *Seguridad en la Informática de Empresa: Riesgos, Amenazas, Prevención y Soluciones*. Ed. ENI.

cuando en realidad están diseñadas para ayudar a los administradores y profesionales de seguridad a asegurar las redes y los sistemas de información[3]. Las herramientas son las siguientes:

1) **Nmap** ("Network Mapper") es una herramienta gratuita de código abierto para la exploración de la red o la auditoría de seguridad. Fue diseñado para analizar rápidamente grandes redes, aunque funciona muy bien contra equipos individuales. Nmap utiliza paquetes IP para determinar qué hosts están disponibles en la red, qué servicios (nombre de la aplicación y la versión) estos equipos ofrecen, qué sistemas operativos (y versiones del sistema operativo) se están ejecutando, qué tipo de filtros de paquetes o cortafuegos están en uso, y docenas de otras características. Nmap se ejecuta en la mayoría de los ordenadores y la consola y versiones gráficas están disponibles. Nmap es libre y de código abierto.
2) **Nessus** es el escáner de vulnerabilidades más popular y es utilizado en más de 75.000 organizaciones en todo el mundo. Muchas organizaciones alrededor del mundo están dando cuenta de los importantes ahorros de costes que estas reciben mediante el uso de Nessus como herramienta de auditoría de sistemas de información para la búsqueda de fallas críticas de seguridad.
3) **John the Ripper** es esencialmente una herramienta de descifrado de contraseñas que se desarrolló para sistemas tipo UNIX. También sus desarrolladores han extendido su apoyo a los sistemas Windows y MAC.

   El software es utilizado por muchos usuarios para probar la fortaleza de la contraseña elegida. Obviamente, esta herramienta también puede ser usada para descifrar las contraseñas y entrar en un sistema. Es compatible tanto con ataque de diccionario (probando todas las palabras en el diccionario, de ahí que nunca se debe elegir una palabra que se ha encontrado en el diccionario) y ataque de fuerza bruta (en este caso todas las posibles combinaciones son juzgados – por lo tanto, si usted elige una contraseña que es alfanumérico y largo plazo, será difícil romperlo).
4) **Nikto** es un software de código abierto (GPL) para escanear vulnerabilidades en los servidores web. Esta herramienta tiene el potencial de detectar más de 3200 archivos potencialmente peligrosos / CGIs, versiones sobre más de 625 servidores, y los problemas específicos de la

[3] Royer, J. M. (2004). *Seguridad en la Informática de Empresa: Riesgos, Amenazas, Prevención y Soluciones*. Ed. ENI.

versión de más de 230 servidores. Los elementos de exploración y plugins pueden ser actualizado automáticamente (si se desea).

5) **Wireshark** es un programa analizador de protocolos de red o sniffer, que le permite capturar y navegar de forma interactiva por los contenidos de los paquetes capturados en la red. El objetivo del proyecto fue crear un analizador de calidad comercial para Unix. Funciona muy bien en Linux y Windows (con una interfaz gráfica de usuario), fácil de utilizar y puede reconstruir flujos TCP / IP y VoIP!
6) **PuTTY** es una implementación libre de Telnet y SSH para Win32 y Unix, junto con un emulador de terminal xterm.
7) **NetStumbler** es una herramienta de detección de redes inalámbricas para Windows. NetStumbler es una herramienta para Windows que permite detectar redes de área local (WLAN), usando 802.11b, 802.11a y 802.11g.

   Algunos de los usos de esta herramienta son:

   - Verificar que su red está configurada de la manera segura.
   - Buscar lugares con baja cobertura en su WLAN.
   - Detectar otras redes que puedan estar causando interferencias en la red.
   - Detectar AP no autorizados “rogue” en su lugar de trabajo.
   - Ayudar a apuntar antenas direccionales para enlaces de larga distancia WLAN.
8) **El Proyecto Metasploit** es un proyecto de seguridad informática que proporciona información sobre las vulnerabilidades, ayuda en las pruebas de penetración y en la ejecución de la explotación de vulnerabilidades de seguridad. Metasploit representa un conjunto de herramientas que ayuda a los profesionales de seguridad y hacker a llevar a cabo ataques informáticos de manera sistematizada y automatizada.

Su más conocido sub-proyecto es el marco de código abierto Metasploit, una herramienta para el desarrollo y ejecución de código de explotación en contra de un equipo o sistema de información destino remoto. Otros importantes sub-proyectos son la base de datos Opcode, archivo shellcode, e investigaciones de seguridad.

### 1.1.3 Importancia de la Seguridad y la Criptografía

A continuación se mencionará acerca de la importancia que tiene la seguridad informática y la criptografía en la actualidad para saber lo útil que puede ser para todos nosotros, sobre todo en las

empresas para proteger su información de ser robado por delincuentes cibernéticos.

**La seguridad informática** se puede definir de forma general como los recursos y procesos mediantes los cuales un sistema o sistemas informáticos tienen la capacidad de prevenir y hacer frente de manera efectiva a amenazas cibernéticas.

La seguridad informática ha adquirido una gran importancia en los tiempos más recientes, sobre todo para las organizaciones como las empresas y los miembros de estos. Esta situación se debe a que día con día las amenazas informáticas, como lo son los intrusos o programas maliciosos, representan un problema serio que merece tener una atención especial, ya que podrían tener efectos catastróficos si accedieran a información oficial y confidencial de la organización pudiendo usarla con fines poco éticos y ventajosos, o modificando dicha información causando problemas.

Además, la seguridad informática también es de gran importancia para hacer respaldos de la información y tenerla disponible sin correr el riesgo de perderla.

De igual forma, es vital para tener en buen funcionamiento a todos los equipos que formen parte de la red de la empresa u organización, teniendo la capacidad de evitar pérdidas o robos de la información u otros problemas que afecten a la infraestructura informática.

Otra parte importante son los usuarios que tendrán acceso a los equipos computacionales, por ello el departamento responsable de la seguridad informática deberá de hacer ciertas restricciones en los perfiles y limitar la accesibilidad a determinados sitios con el fin de asegurar un estado óptimo en las equipos; aparte de dar cierta capacitación a los usuarios antes mencionados.

Por todo esto, la importancia de la seguridad informática radica en el reto de tener la capacidad de lograr todos los objetivos antes mencionados, para que así, la organización pueda tener un desempeño óptimo basado en un buen estado de su infraestructura informática, que en estos tiempos es vital para todos los tipos de asociaciones.

La protección de la información se lleva a cabo variando su forma. Se llama cifrado (o transformación criptográfica) a una transformación del texto original (llamado también texto inicial

o texto claro) que lo convierte en el llamado **texto cifrado o criptograma**. Análogamente, se llama descifrado a la transformación que permite recuperar el texto original a partir del texto cifrado.

El objetivo de la criptografía es el de proporcionar comunicaciones seguras (y secretas) sobre canales inseguros. Ahora bien, la criptografía no es sinónimo de seguridad. No es más que una herramienta que es utilizada sobre la base de mecanismos de cierta complejidad para proporcionar no solamente protección, sino también garantizar que haya confidencialidad. Surgió históricamente por la necesidad de esconder información a los enemigos durante las batallas que se realizaban desde tiempos inmemoriales, hoy en día estas batallas se nos suelen presentar al transitar datos en Internet. En la actualidad, la Criptografía es la herramienta fundamental para el desarrollo y estabilidad del comercio electrónico.

Encriptar datos tiene dos principales objetivos: la confidencialidad, para mantener la información en secreto, y la integridad, para evitar que la información se destruya o sea corrompida.

El sistema de mercado capitalista ha transformado el valor de uso con el que inicialmente surge Internet en valor de cambio. Nuestra identidad se convierte en nuestro propio aval, la persona en gran medida se convierte en dinero. Desde que esto sucede, surge la necesidad urgente de la criptografía para proteger los datos confidenciales[4].

## 1.2 Seguridad Informática

La seguridad informática es un tema al que mucha gente no le da la importancia que realmente tiene; muchas veces por el hecho de considerar que es inútil o que jamás la utilizara. Pero en el mundo moderno, cada día más y más personas mal intencionadas intentan tener acceso a los datos de nuestros ordenadores.

El acceso no autorizado a una red informática o a los equipos que en ella se encuentran puede ocasionar en la gran mayoría de los casos graves problemas.

[4] Hoy, I. (s.f.). *Criptografía. Seguridad Informática*. http://www.informatica-hoy.com.ar/software-seguridad-virus-antivirus/Criptografia-Seguridad-informatica.php

Uno de las posibles consecuencias de una intrusión es la pérdida de datos. Es un hecho frecuente y ocasiona muchos trastornos, sobre todo si no estamos al día de las copias de seguridad. Y aunque estemos al día, no siempre es posible recuperar la totalidad de los datos.

Otro de los problemas más dañinos es el robo de información sensible y confidencial. La divulgación de la información que posee una empresa sobre sus clientes puede acarrear demandas millonarias contra esta, o un ejemplo más cercano a usted es el de nuestras contraseñas de las cuentas de correo por las que intercambiamos información con otros.

### 1.2.1 Definición de Seguridad Informática

Se entiende por seguridad informática al conjunto de normas, procedimientos y herramientas, que tienen como objetivo garantizar la disponibilidad, integridad, confidencialidad y buen uso de la información que reside en un sistema de información.

Cada día más y más personas mal intencionadas intentan tener acceso a los datos de nuestros ordenadores. El acceso no autorizado a una red informática o a los equipos que en ella se encuentran puede ocasionar en la gran mayoría de los casos graves problemas.

Uno de las posibles consecuencias de una intrusión es la pérdida de datos. Es un hecho frecuente y ocasiona muchos trastornos, sobre todo si no estamos al día de las copias de seguridad. Y aunque estemos al día, no siempre es posible recuperar la totalidad de los datos.

Otro de los problemas más dañinos es el robo de información sensible y confidencial. La divulgación de la información que posee una empresa sobre sus clientes puede acarrear demandas millonarias contra esta, o un ejemplo más cercano a nosotros es el de nuestras contraseñas de las cuentas de correo por las que intercambiamos información con otros.

Con la constante evolución de las computadoras es fundamental saber qué recursos necesitar para obtener seguridad en los sistemas de información.[5]

[5] Aguado, D. P. (2012). *Seguridad Informática para el Hogar*. Ed. Bubok.

### 1.2.2 Principios Fundamentales de la Seguridad Informática

Para lograr sus objetivos la seguridad informática se fundamenta en tres principios, que debe cumplir todo sistema informático[6]:

- **Confidencialidad:** Se refiere a la privacidad de los elementos de información almacenados y procesados en un sistema informático, Basándose en este principio, las herramientas de seguridad informática deben proteger el sistema de invasiones y accesos por parte de personas o programas no autorizados. Este principio es particularmente importante en sistemas distribuidos, es decir, aquellos en los que los usuarios, computadores y datos residen en localidades diferentes, pero están física y lógicamente interconectados.
- **Integridad:** Se refiere a la validez y consistencia de los elementos de información almacenados y procesador en un sistema informático. Basándose en este principio, las herramientas de seguridad informática deben asegurar que los procesos de actualización estén bien sincronizados y no se dupliquen, de forma que todos los elementos del sistema manipulen adecuadamente los mismos datos. Este principio es importante en sistemas descentralizados, es decir, aquellos en los que diferentes usuarios, computadores y procesos comparten la misma información.
- **Disponibilidad:** Se refiere a la continuidad de acceso a los elementos de información almacenados y procesados en un sistema informático. Basándose en este principio, las herramientas de seguridad informática deber reforzar la permanencia del sistema informático, en condiciones de actividad adecuadas para que los usuarios accedan a los datos con la frecuencia y dedicación que requieran, este principio es importante en sistemas informáticos cuyos compromiso con el usuario, es prestar servicio permanente.

### 1.2.3 Elementos Físicos y Lógicos en los Sistemas

En "Fundamentos de los sistemas informáticos", Ralph Stair y George Reynolds definen un sistema informático (CBIS en inglés) como un conjunto "único de equipo, programas, bases de datos, telecomunicaciones, gente y procedimientos configurados para recoger, manipular, almacenar y procesar datos en forma de información". Algunos expertos listan 5 elementos básicos de un CBIS:

[6] Portillo, S. (s.f.). *Historia de la Seguridad Informática de Susana Portillo en Prezi*. http://prezi.com/vnbaj88nuq0p/historia-de-la-seguridad-informatica/

equipo, programa, datos, procedimientos y personas. Otros agregan un sexto elemento a la lista, las comunicaciones.

- **Equipo:**

El equipo es la parte más evidente de un sistema de informática. El equipo se refiere a la propia computadora, junto con los accesorios periféricos, incluidos los servidores, enrutadores, monitores, impresoras y dispositivos de almacenamiento. Un CBIS se puede utilizar en una sola computadora o en miles.

- **Programa:**

Sin el sistema, el equipo no sería muy útil. El sistema es el segundo elemento de un CBIS, es lo que le dice al equipo cómo debe funcionar. Reúne, organiza y manipula los datos para dar instrucciones. Todo lo que haces cuando usas la computadora lo haces a través del sistema.

- **Datos:**

Los datos, o información, es el tercer elemento de un CBIS. Al igual que el equipo no puede funcionar sin el sistema, el sistema no funciona sin los datos. Esta es la parte de información de un sistema, y puede tener datos estadísticos, conjuntos de instrucciones, listas de nombres o incluso gráficos y animaciones, todo es importante para un CBIS.

- **Procedimientos:**

Comúnmente se dice que "los procedimientos son a la gente lo que es el sistema al equipo". El cuarto elemento del CBIS, los procedimientos son las reglas, las descripciones y las instrucciones para saber cómo se hacen las cosas. En los sistemas informáticos, los procedimientos son frecuentemente cubiertos por los manuales de instrucciones o el usuario describe cómo utilizar el equipo, programa y datos.

- **Gente:**

Las personas son la parte más a menudo pasada por alto y son la parte más importante de un sistema informático. Las personas son quienes diseñan y operan el sistema, introducen los datos, construyen el equipo y hacen que siga funcionando, escriben los procedimientos y, en definitiva, son quienes determinan el éxito o fracaso de un CBIS.

- **Comunicación:**

La comunicación se deja de lado en algunas listas de elementos de CBIS, pero para un sistema que involucra más de una pieza del equipo para funcionar, la comunicación o la conectividad es una necesidad. Esto sucede en cierta forma porque partes de ella están cubiertas por el equipo. Los

componentes de un equipo son lo que permite que una computadora se comunique con otra y están controladas por un sistema. Sin embargo, si la comunicación entre personas está incluida entonces es un elemento importante.

## 1.3 Seguridad en Redes de Computadores

La rápida expansión y popularización de Internet ha convertido a la seguridad en redes en uno de los tópicos más importantes dentro de la Informática moderna. Con tal nivel de interconexión, los virus y los *hackers* campan a sus ancas, aprovechando las deficientes medidas de seguridad tomadas por administradores y usuarios a los que esta nueva revolución ha cogido por sorpresa.

Las ventajas de las redes en Informática son evidentes, pero muchas veces se minusvaloran ciertos riesgos, circunstancia que a menudo pone en peligro la seguridad de los sistemas. En unos pocos años la inmensa mayoría de las empresas operarán a través de la Red, y esto sólo será posible si los profesionales de la Informática saben aportar soluciones que garanticen la seguridad de la información.

### 1.3.1 Importancia de las Redes

La Informática es la ciencia del tratamiento automático de la información, pero tanto o más importante que su procesamiento y almacenamiento es la capacidad para poder transmitirla de forma eficiente. La información tiene un tiempo de vida cada vez menor y la rapidez con la que pueda viajar es algo crucial. Los últimos avances en compresión y transmisión de datos digitales permiten hoy por hoy transferir cantidades enormes de información a velocidades que hace tan solo unos años eran impensables. En este sentido las redes de computadoras desempeñan un papel fundamental en la Informática moderna.[7]

Pero hemos de tener en cuenta que la complejidad de las grandes redes y su carácter público convierten la protección física de los canales de comunicación en algo tremendamente difícil. Hemos de depositar nuestra confianza en la Criptografía para garantizar la confidencialidad en las comunicaciones.

[7] Bertolín, J. A. (2008). *Seguridad de la Información: Redes, Informática y Sistema de Información*. Ed. Paraninfo.

Uno de los mayores obstáculos que han tenido que superarse para que las redes pudieran desarrollarse, ha sido encontrar *lenguajes* comunes para que computadoras de diferentes tipos pudieran entenderse. En este sentido el protocolo TCP/IP se ha erigido como estándar *de facto* en la industria de la Informática. En general todas las redes de computadoras se construyen conceptualmente sobre diferentes capas de abstracción, que desarrollan tareas distintas y proporcionan un protocolo unificado a las capas superiores. La Criptografía podrá entonces ser empleada en diferentes niveles de abstracción. Por ejemplo, podemos codificar un fichero antes de transmitirlo por la red, lo cual correspondería al nivel de abstracción mayor, o podemos enviarlo sin codificar, pero a través de un protocolo de bajo nivel que cifre cada uno de los *paquetes* de información en los que se va a subdividir el fichero en el momento de transmitirlo.

En función del tipo de red con el que trabajemos nos enfrentaremos a diferentes tipos de riesgos, lo cual nos conducirá inevitablemente a medidas de diferente naturaleza para garantizar la seguridad en las comunicaciones. En este capítulo haremos una breve reflexión sobre algunos de los casos que pueden darse, sin tratar de ser exhaustivos (sería imposible, dada la inmensa cantidad de posibilidades). Nuestro objetivo se centrará en aportar una serie de directrices que nos permitan analizar cada situación y establecer una correcta política de protección de la información.

Ya que no existe una solución universal para proteger una red, en la mayoría de los casos la mejor estrategia suele consistir en tratar de *colarnos* nosotros mismos para poner de manifiesto y corregir posteriormente los *agujeros de seguridad* que siempre encontraremos. Esta estrategia se emplea cada vez con mayor frecuencia, y en algunos casos hasta se contrata a *hackers* para que impartan cursillos de seguridad a los responsables de las redes de las empresas.

### 1.3.2 Redes Internas

El caso más sencillo de red que nos podemos encontrar es local (LAN), con todos los computadores interconectados a través de unos cables de los que también se es propietario. Esta última circunstancia nos va a permitir ejercer un control total sobre el canal de comunicaciones, pudiendo protegerlo físicamente, lo cual evita prácticamente cualquier riesgo de falta de privacidad en la información.

Uno de los riesgos dignos de mención de estos casos son las posibles pérdidas de información debidas a fallos físicos, que pueden ser minimizados llevando a cabo una adecuada política de *copias de respaldo*, que deberán ser confeccionadas periódicamente, almacenadas en un lugar diferente de aquel donde se encuentra la red, y protegidas adecuadamente contra incendios y accesos no deseados.

Otro riesgo que se da en las redes locales, a menudo infravalorado, es el que viene del uso inadecuado del sistema por parte de los propios usuarios. Ya sea por mala fe o descuido, un usuario con demasiados privilegios puede destruir información, por lo que estos permisos deben ser asignados con mucho cuidado por parte de los administradores. Esta circunstancia es muy importante, ya que, sobre todo en pequeñas empresas, el dueño muchas veces cree que debe conocer la clave del administrador, y luego es incapaz de resistir la tentación de *jugar con ella*, poniendo en serio peligro la integridad del sistema y entorpeciendo el trabajo del superusuario.

Existen redes internas en las que un control exhaustivo sobre el medio físico de transmisión de datos es en la práctica imposible. Piénsese en un edificio corporativo con un acceso no muy restringido, por ejemplo un aulario de una universidad, que posee conexiones *Ethernet* en todas sus dependencias. En principio, nada impediría a una persona conectar un ordenador portátil a una de esas conexiones para llevar a cabo un análisis del tráfico de la red sin ser descubierta, o *suplantar* a cualquier otro computador. En esos casos será conveniente llevar a cabo algún tipo de control, como la deshabilitación dinámica de las conexiones de red concreta que debe estar conectada en cada punto, o la adopción de protocolos de autentificación de las computadoras dentro de la red, como por ejemplo *kerberos* (que forma parte del proyecto *Athena*, en el MIT)[8].

### 1.3.3 Redes Externas

Consideraremos red externa a aquella que en todo o en parte se apoye en un canal físico de comunicación ajeno. Existirán redes externas de muy diferentes tipos, pero todas ellas tienen en común la característica de que en algún momento la información viaja por canales sobre los que no se tiene ningún tipo de control. Todas las técnicas que nos va a permitir llevar a cabo protecciones efectivas de los datos deberán hacer uso necesariamente de la Criptografía[9].

[8]Bertolín, J. A. (2008). *Seguridad de la Información: Redes, Informática y Sistema de Información*. Ed. Paraninfo

[9] Bertolín, J. A. (2008). *Seguridad de la Información: Redes, Informática y Sistema de Información*. Ed. Paraninfo

Para identificar los posibles riesgos que presentará una red externa, hemos de fijarnos en cuestiones tan dispares como el sistema operativo que corre sobre los ordenadores o el tipo de acceso que los usuarios *legales* del sistema pueden llevar a cabo.

Una de las configuraciones más comunes consiste en el uso de una red local conectada al exterior mediante un *firewall* (computadora que filtra el tráfico entre la red interna y el exterior). Los firewalls son herramientas muy poderosas si se emplean adecuadamente, pero pueden entrañar ciertos riesgos si se usan mal. Por ejemplo, existen muchos lugares donde el firewall está conectado a la red local y ésta a su vez a la red externa (ver Fig. 1.3, caso A). Esta configuración es la más sencilla y barata, puesto que sólo necesitamos una tarjeta de red en el firewall, pero no impediría a un computador situado en el exterior acceder directamente a los de la red local. La configuración correcta se puede apreciar en el caso B de la Fig. 1.3 donde se ilustra el caso A, que muestra la red externa (y todos sus peligros) está separada físicamente de la red local.

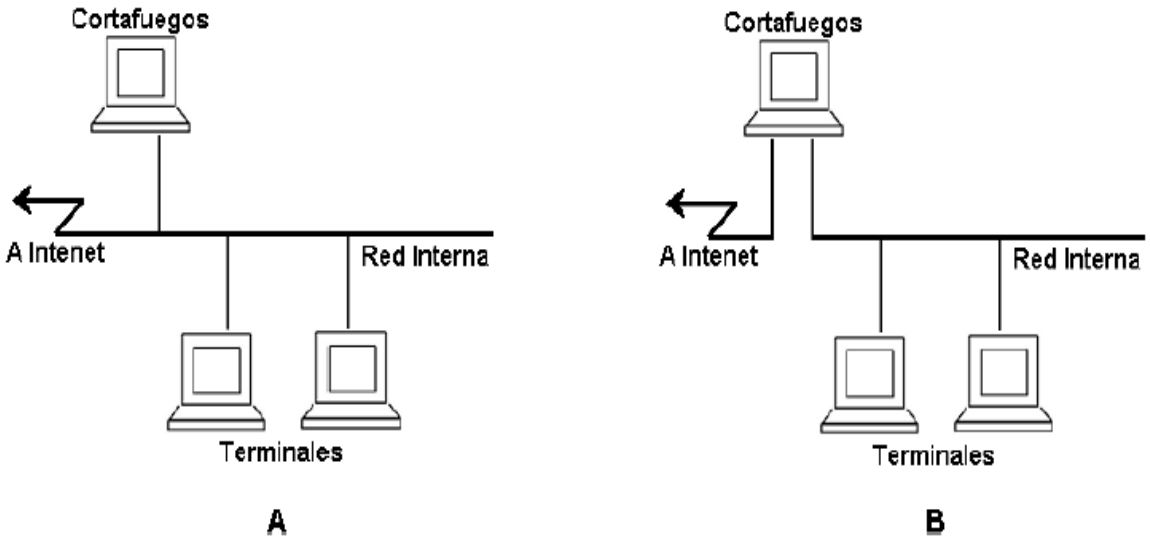


**Figura 1.3.** **Caso A:** Configuración Incorrecta, el firewall tiene una única tarjeta de red, y los terminales están conectados físicamente a la red externa. **Caso B:** Configuración correcta, el firewall dispone de dos tarjetas de red y el resto de las computadoras está aislado físicamente de la red externa.

Podemos distinguir dos grandes tipos de peligros potenciales que pueden comprometer nuestra información desde una red externa:

- **Ataques Indiscriminados**: Suelen ser los más frecuentes, y también los menos dañinos. Dentro de esta categoría podemos incluir los troyanos y los virus, programas diseñados normalmente para *colarse* en cualquier sistema y producir efectos de lo más variopinto. Precisamente por su carácter general, existen programas específicos que nos protegen de ellos, como los antivirus. Conviene disponer de un buen antivirus y actualizarlo periódicamente.
- **Ataques a *Medida***: Mucho menos comunes que los anteriores, y también más peligrosos, son los ataques que generalmente llevan a cabo los *hackers*. En estos casos las víctimas son casi siempre grandes corporaciones, y muchas veces la información ni siquiera es destruida o comprometida, puesto que los *hackers* sólo persiguen enfrentarse al reto que supone para ellos entrar en un sistema *grande*. El problema es que para borrar sus huellas y dificultar el rastreo de sus acciones, suelen atacar en primer lugar sistemas pequeños para desde ellos cometer sus *travesuras*, lo cual convierte a cualquier sistema en potencial víctima de estos personajes. Lo que ocurre en la mayoría de los casos es que su necesidad de emplear sistemas pequeños como plataforma les obliga a no dañarlos, para no dejar ningún tipo de rastro que permita localizarlos posteriormente. Por desgracia, no existe otro sistema para protegerse de los *hackers*, más que la vigilancia constante.

En cuanto a la protección de las comunicaciones en sí, baste decir que existen protocolos de comunicación segura de *bajo nivel*, como el SSL (Secure Sockets Layer), que permite establecer comunicaciones seguras a través de Internet, haciendo uso de algoritmos simétricos y asimétricos simultáneamente. Este protocolo es transparente y puede correr bajo otros protocolos ampliamente conocidos, como POP3, TELNET, FTP, HTTP, etc. De hecho, gran cantidad de aplicaciones emplean protocolos de este tipo en sus comunicaciones. Desgraciadamente, las restrictivas leyes norteamericanas en cuanto a la exportación de material criptográfico hacen que la gran mayoría de las aplicaciones *seguras* que se venden fuera de los EE.UU. y Canadá estén en realidad debilitadas, por lo que hemos de informarnos muy bien antes de depositar nuestra confianza en ellas.

### 1.3.4 Intranets

El término *intranet* se ha popularizado recientemente y hace alusión a redes externas que se comportan de cara a los usuarios como redes privadas internas. Obviamente, este tipo de redes ha de ser implementado haciendo uso de protocolos criptográficos de autentificación y codificación de las transmisiones, puesto que el tráfico que nosotros vemos como *interno* a nuestra red, en realidad viaja por Internet.[10]

[10] Bertolín, J. A. (2008). *Seguridad de la Información: Redes, Informática y Sistema de Información*. Ed. Paraninfo.

# CAPÍTULO II. LA CRIPTOGRAFÍA

## 2.1 Algoritmos Simétricos de Cifrado

### 2.1.1 Algoritmo DES

Es el algoritmo simétrico más extendido mundialmente. Data de mediados de los setenta, cuando fue adoptado como estándar para las comunicaciones seguras por el Gobierno de los EE.UU. en realidad la NSA (National Security Agency) lo diseñó para ser implementado por hardware, pero al parecer por un malentendido entre ellos y la Oficina Nacional de Estandarización, su especificación se hizo pública con suficiente detalle como para que cualquiera pudiera implementarlo por software. No fue casualidad que el siguiente algoritmo adoptado (*Skipjack*) se considerara secreto.

El algoritmo DES codifica bloques de 64 bits empleando claves de 56 bits. Es una Red de Feistel de 16 rondas con dos permutaciones, una inicial ($P_i$) y otra final ($P_f$), tales que $P_i = P_f^{-1}$.

La función *f* se compone de una permutación de expansión (*E*), que convierte el bloque de 32 bits correspondiente en uno de 48. Después realiza un *or-exclusivo* con el valor $K_i$ , también de 48 bits, aplica ocho S-Cajas de $6^4$ bits, y efectúa una nueva permutación *P*.

Se calcula un total de 16 valores de $K_i$ , uno para cada ronda, efectuando primero una permutación inicial sobre la clave, y luego llevando a cabo desplazamientos a la izquierda de cada una de las dos mitades (de 28 bits) resultantes, y realizando una elección permutada de 48 bits en cada ronda, que será la $K_i$ .

Para descifrar basta con usar el mismo algoritmo (ya que $P_i = P_f^{-1}$ ) empleando las $K_i$ en orden inverso.[11]

#### 2.1.1.1 Variantes

A mediados de julio de 1998, una empresa sin ánimo de lucro, llamada EFF (Electronic Frontier Foundation), logró fabricar una máquina capaz de descifrar un mensaje DES en menos de 3 días. Curiosamente, pocas semanas antes, un alto cargo de la NSA había declarado que dicho algoritmo

[11] Fúster Sabater A., L. H. (2012). *Criptografía, Protección de Datos y Aplicaciones*. Ed. Alfaomega Grupo Editor.

seguía siendo seguro, y que descifrar un mensaje resultaba aun excesivamente costoso, incluso para organizaciones gubernamentales. *DES-Cracker* costó menos de 40 millones de pesetas.

A pesar de su *caída*, DES sigue siendo ampliamente utilizado en multitud de aplicaciones, como por ejemplo las transacciones de los cajeros automáticos. De todas formas, el problema real de DES no radica en su diseño, sino en que emplea una clave demasiado corta (56 bits), lo cual hace que con el avance actual de las computadoras los ataques por la fuerza bruta comiencen a ser opciones realistas. Mucha gente se resiste a abandonar este algoritmo, precisamente porque ha sido capaz de *sobrevivir* durante 20 años sin mostrar ninguna debilidad en su diseño, y prefieren proponer variantes que, de un lado evitarían el riesgo de tener que confiar en algoritmos nuevos, y de otro permitirían aprovechar gran parte de las implementaciones por hardware existentes de DES.

A continuación se explicará sobre las variantes con las que cuenta el algoritmo DES:

- **DES Múltiple:**

Consiste en aplicar varias veces el algoritmo DES con diferentes claves al mensaje original. Se puede hacer ya que DES no presenta estructura de *grupo*. El más común de todos ellos es el Tripe-DES, que responde a la siguiente ecuación:

$$\mathrm{C} = E_{k1}\left(E_{k2}^{-1}\left(E_{k1}\left(M\right)\right)\right)$$ Ecuación DES Múltiple

Es decir, codificamos con la subclave $K_1$ , decodificamos con $K_2$ y volvemos a codificar con $K_1$ .
La clave resultante es la concatenación de $K_1$ y $K_2$ , con una longitud de 112 bits.

- **DES con Subclaves Independientes:**

Consiste en emplear subclaves diferentes para cada una de las 16 rondas de DES. Puesto que estas subclaves son de 48 bits, la clave resultante tendría 768 bits en total. No es nuestro objetivo entrar en detalles, pero empleando criptoanálisis diferencial, esta variante podría ser rota con $2^{61}$ textos planos escogidos, por lo que en la práctica no presenta un avance sustancial sobre DES estándar.

- **DES Generalizado:**

Esta variante emplea *n* trozos de 32 bits en cada ronda en lugar de dos, por lo que aumentamos tanto la longitud de la clave como el tamaño de mensaje que se puede codificar, manteniendo sin

embargo el orden de complejidad del algoritmo. Se ha demostrado sin embargo que no sólo se gana poco en seguridad, sino que en muchos casos incluso se pierde.

- **DES con S-Cajas Alternativas:**

Consiste en utilizar S-Cajas diferentes a las de la versión original de DES. En la práctica no se han encontrado S-Cajas mejores que propias de DES. De hecho, algunos estudios han revelado que las S-Cajas originales presentan propiedades que las hacen resistentes a técnicas de criptoanálisis que no fueron conocidas fuera de la NSA hasta muchos años después de la aparición del algoritmo.[12]

### 2.1.2 Algoritmo IDEA

El algoritmo IDEA (International Data Encryption Algorithm) es bastante más joven que DES, pues data de 1992. Para muchos constituye el mejor y más seguro algoritmo simétrico disponible en la actualidad. Trabaja con bloques de 64 bits de longitud y emplea una clave de 128 bits. Como en el caso de DES, se usa el mismo algoritmo tanto para cifrar como para descifrar.

Como ocurre con todos los algoritmos simétricos de bloques, IDEA se basa en los conceptos de confusión y difusión, haciendo uso de las siguientes operaciones elementales (todas ellas fáciles de implementar):

- XOR.
- Suma Módulo $2^{16}$.
- Producto Módulo $2^{16} + 1$.

El algoritmo IDEA consta de ocho rondas. Dividiremos el bloque *X* a codificar, de 64 bits, en cuatro partes $X_1$ , $X_2$ , $X_3$ y $X_4$ de 16 bits. Denominaremos $Z_i$ a cada una de las 52 subclaves de 16 bits que vamos a necesitar. Las operaciones que llevaremos a cabo en cada ronda son las siguientes:

1. Multiplicar $X_1$ por $Z_1$.
2. Sumar $X_2$ con $Z_2$.
3. Sumar $X_3$ con $Z_3$.
4. Multiplicar $X_4$ por $Z_4$.

[12] Fúster Sabater A., L. H. (2012). *Criptografía, Protección de Datos y Aplicaciones*. Ed. Alfaomega Grupo Editor.

5. Hacer un XOR entre los resultados del paso 1 y el paso 3.
6. Hacer un XOR entre los resultados del paso 2 y el paso 4.
7. Multiplicar el resultado del paso 5 por $Z_5$.
8. Sumar los resultados de los pasos 6 y 7.
9. Multiplicar el resultado del paso 8 por $Z_6$.
10. Sumar los resultados de los pasos 7 y 9.
11. Hacer un XOR entre los resultados de los pasos 1 y 9.
12. Hacer un XOR entre los resultados de los pasos 3 y 9.
13. Hacer un XOR entre los resultados de los pasos 2 y 10.
14. Hacer un XOR entre los resultados de los pasos 4 y 10.

La salida de cada iteración serán los cuatro sub-bloques obtenidos en los pasos 11, 12, 13 y 14, que serán la entrada del siguiente ciclo, en el que emplearemos las siguientes seis subclaves, hasta un total de 48. Al final de todo intercambiaremos los dos bloques centrales (en realidad con eso *deshacemos* el intercambio que llevamos a cabo en los pasos 12 y 13).

Después de la octava iteración, se realiza la siguiente transformación:

1. Multiplicar $X_1$ por $Z_{49}$.
2. Sumar $X_2$ con $Z_{50}$.
3. Sumar $X_3$ con $Z_{51}$.
4. Multiplicar $X_4$ con $Z_{52}$.

Las primeras ocho subclaves se calculan dividiendo la clave de entrada en bloques de 16 bits. Las siguientes ocho se calculan rotando la clave de entrada 25 bits a la izquierda y volviendo a dividirla, y así sucesivamente.

Las subclaves necesarias para descifrar se obtienen cambiando de orden las $Z_i$ y calculando sus inversas para la suma o la multiplicación, según la tabla 2.2. A efectos de cálculo, consideraremos que la inversa para el producto de 0 módulo $2^{16}+1$ es 0.[13]

[13] Fúster Sabater A., L. H. (2012). *Criptografía, Protección de Datos y Aplicaciones*. Ed. Alfaomega Grupo Editor.

Tabla 2.2: Subclaves empleadas en el algoritmo IDEA

| Ronda | Subclaves de Cifrado | Subclaves de Descifrado |
|---|---|---|
| 1 | $Z_1 \quad Z_2 \quad Z_3 \quad Z_4 \quad Z_5 \quad Z_6$ | $Z_{49}^{-1} \quad -Z_{50} \quad -Z_{51} \quad Z_{52}^{-1} \quad Z_{47} \quad Z_{48}$ |
| 2 | $Z_7 \quad Z_8 \quad Z_9 \quad Z_{10} \quad Z_{11} \quad Z_{12}$ | $Z_{43}^{-1} \quad -Z_{45} \quad -Z_{44} \quad Z_{46}^{-1} \quad Z_{41} \quad Z_{42}$ |
| 3 | $Z_{13} \quad Z_{14} \quad Z_{15} \quad Z_{16} \quad Z_{17} \quad Z_{18}$ | $Z_{37}^{-1} \quad -Z_{39} \quad -Z_{38} \quad Z_{40}^{-1} \quad Z_{35} \quad Z_{36}$ |
| 4 | $Z_{19} \quad Z_{20} \quad Z_{21} \quad Z_{22} \quad Z_{23} \quad Z_{24}$ | $Z_{31}^{-1} \quad -Z_{33} \quad -Z_{32} \quad Z_{34}^{-1} \quad Z_{29} \quad Z_{30}$ |
| 5 | $Z_{25} \quad Z_{26} \quad Z_{27} \quad Z_{28} \quad Z_{29} \quad Z_{30}$ | $Z_{25}^{-1} \quad -Z_{27} \quad -Z_{26} \quad Z_{28}^{-1} \quad Z_{23} \quad Z_{24}$ |
| 6 | $Z_{31} \quad Z_{32} \quad Z_{33} \quad Z_{34} \quad Z_{35} \quad Z_{36}$ | $Z_{19}^{-1} \quad -Z_{21} \quad -Z_{20} \quad Z_{22}^{-1} \quad Z_{17} \quad Z_{18}$ |
| 7 | $Z_{37} \quad Z_{38} \quad Z_{39} \quad Z_{40} \quad Z_{41} \quad Z_{42}$ | $Z_{13}^{-1} \quad -Z_{15} \quad -Z_{14} \quad Z_{16}^{-1} \quad Z_{11} \quad Z_{12}$ |
| 8 | $Z_{43} \quad Z_{44} \quad Z_{45} \quad Z_{46} \quad Z_{47} \quad Z_{48}$ | $Z_7^{-1} \quad -Z_9 \quad -Z_8 \quad Z_{10}^{-1} \quad Z_5 \quad Z_6$ |
| Final | $Z_{49} \quad Z_{50} \quad Z_{51} \quad Z_{52}$ | $Z_1^{-1} \quad -Z_2 \quad -Z_3 \quad Z_4^{-1}$ |

### 2.1.3 Algoritmos de Cifrado por Bloques

En esta sección comentaremos algunos métodos para aplicar cifrados por bloques a mensajes de gran longitud. En primer lugar independientemente del método empleado para codificar, hemos de tener en cuenta lo que ocurre cuando la longitud de la cadena que queremos cifrar no es un múltiplo exacto del tamaño de bloque. Entonces tenemos que añadir información al final para que sí lo sea. El mecanismo más sencillo consiste en rellenar con cero (o algún otro patrón) el último bloque que se codifica. El problema ahora consiste en saber cuándo se descifra por dónde hay que cortar. Lo que se suele hacer es añadir como último byte del último bloque el número de bytes que se han añadido (ver fig. 2.3). Esto tiene el inconveniente de que si el tamaño original es múltiplo del bloque, hay que alargarlo con otro bloque entero. Por ejemplo, si el tamaño de bloque fuera 64 bits, y sobraran cinco bytes al final, añadiríamos dos ceros y un tres. Si por el contrario no sobrara nada, tendríamos que añadir siete ceros y un ocho.

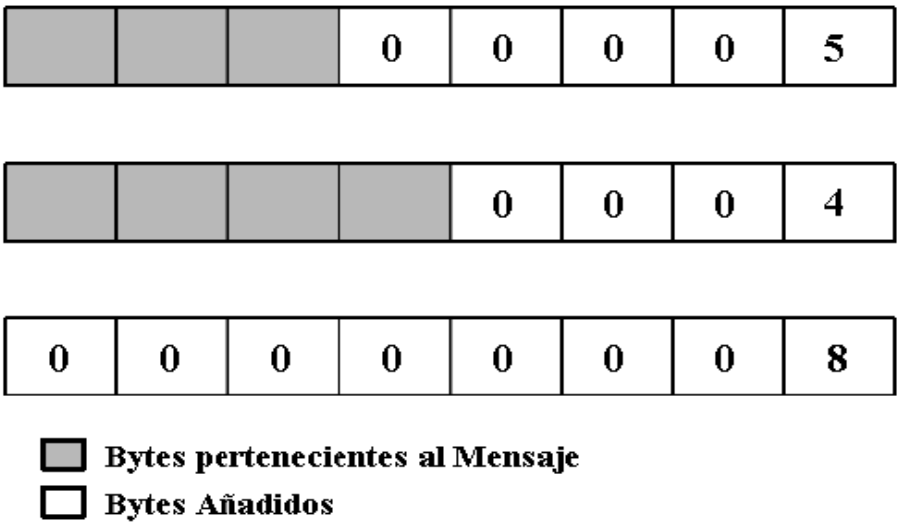


**Figura 2.3**: Relleno (*padding*) de los bytes del último bloque al emplear un algoritmo de cifrado por bloques[14]

### 2.1.3.1 Modos de Operación

A continuación se dará a conocer sobre los modos con los que opera el algoritmo de cifrado por bloques:

- **Modo ECB:**

El modo ECB (*Electronic Codebook*) es el método más sencillo y obvio de aplicar un algoritmo de cifrado por bloques. Simplemente se subdivide la cadena que se quiere codificar en bloques del tamaño adecuado y se cifran todos ellos empleando la misma clave.

A favor de éste método podemos decir que permite codificar los bloques independientemente de su orden, lo cual es adecuado para codificar bases de datos o ficheros en los que se requiera un acceso aleatorio. También es resistente a errores, pues si uno de los bloques sufriera una alteración, el resto quedaría intacto.

Por el contrario, si el mensaje presenta patrones repetitivos, el texto cifrado también los presentará, y eso es peligroso, sobre todo cuando se codifica información muy redundante (como ficheros de texto), o con patrones comunes al inicio y final (como el correo electrónico). Un contrincante puede en estos casos efectuar un ataque estadístico y extraer bastante información.

[14] Fúster Sabater A., L. H. (2012). *Criptografía, Protección de Datos y Aplicaciones*. Ed. Alfaomega Grupo Editor.

Otro riesgo bastante importante que presenta el modo ECB es el de la *sustitución de bloques*. El atacante puede cambiar un bloque sin mayores problemas, y alterar los mensajes incluso desconociendo la clave y el algoritmo empleados. Simplemente se *escucha* una comunicación de la que se conozca el contenido, como por ejemplo una transacción bancaria a nuestra corriente. Luego se escuchan otras comunicaciones y se sustituyen los bloques correspondientes al número de cuenta del beneficiario de la transacción por la versión codificada de nuestro número (que ni siquiera nos habremos molestado en descifrar). En cuestión de horas nos habremos hecho ricos.

- **Modo CBC:**

El modo CBC (*Cipher Book Chaining Mode*) incorpora un mecanismo de retroalimentación en cifrado por bloques. Esto significa que la codificación de bloques anteriores condiciona la codificación del bloque actual, por lo que será imposible sustituir un bloque individual en el mensaje cifrado. Esto se consigue efectuando una operación XOR entre el bloque del mensaje que queremos codificar y el último criptograma obtenido (ver Fig. 2.4).

En cualquier caso, dos mensajes idénticos se codificarán de la misma forma usando el modo CBC. Más aun, dos mensajes que empiecen igual se codificarán igual hasta llegar a la primera diferencia entre ellos. Para evitar esto se emplea un *vector de inicialización*, que puede ser un bloque aleatorio, como bloque inicial de la transmisión. Este vector será descartado en destino, pero garantiza que siempre los mensajes se codifiquen de manera diferente, aunque tengan partes comunes.

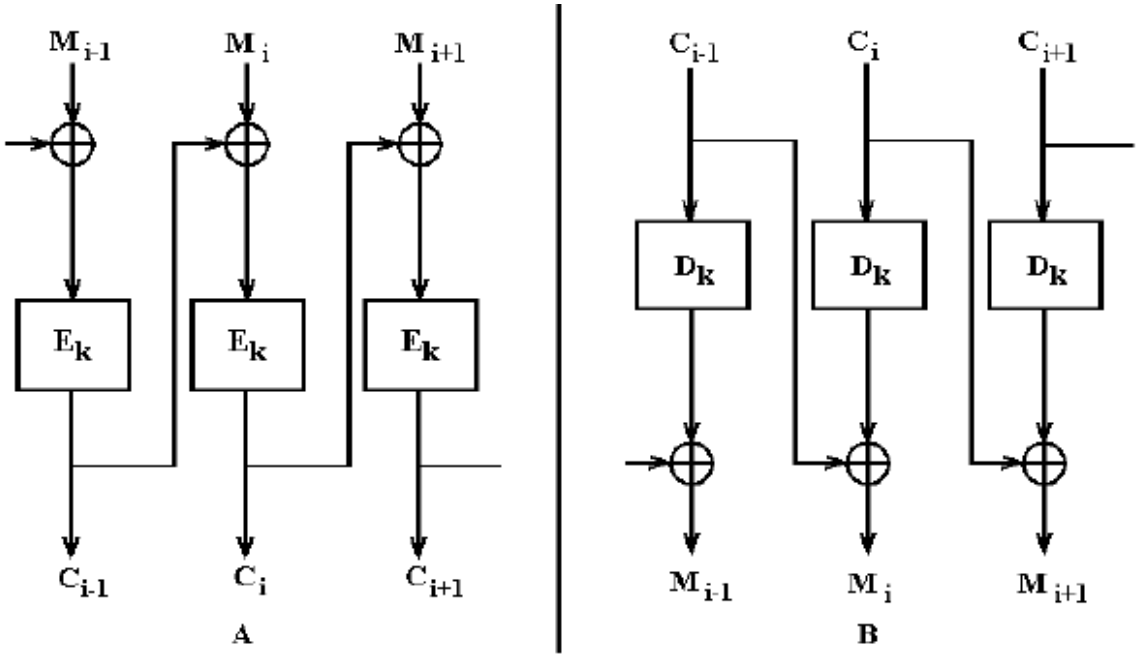


**Figura 2.4**: Modo de Operación CBC. A) Codificación, B) Decodificación.

- **Modo CFB:**

El modo CBC no empieza a codificar (decodificar) hasta que no se tiene que transmitir un bloque completo. Esto puede ser un inconveniente, por ejemplo en el caso de terminales, que deberían poder transmitir cada carácter que pulsa el usuario individualmente. Tendremos pues que emplear un bloque completo para transmitir cada byte, rellenando el resto con ceros, pero esto hará que tengamos únicamente 256 mensajes diferentes en nuestra transmisión y que un atacante pueda efectuar un análisis estadístico. El modo de operación CFB (*Cipher-Feedback Mode*) permitirá codificar la información en unidades inferiores al tamaño del bloque, manteniendo un nivel de seguridad adecuado.

Sea *p* el tamaño de bloque del algoritmo simétrico, y sea *n* el tamaño de los bloques que queremos transmitir (*n* ha de divisor de *p*). Sea $m_i$ el *i*-ésimo bloque del texto plano, de tamaño *n*. empleamos entonces un registro de desplazamiento *R* de longitud *m* y lo cargamos con un vector de inicialización. Codificamos el registro *R* con el algoritmo simétrico y obtenemos en *r* su *n* bits más a la izquierda. El bloque que deberemos enviar es $c_i = r \oplus m_i$ . Desplazamos *R n* bits a la izquierda e introducimos $c_i$ por la derecha.

Para descifrar basta con cargar el vector de inicialización en *R* y codificarlo, calculando *r*. Entonces $m_i = r \oplus c_i$ . Desplazamos entonces *R* e introducimos $c_i$ por la derecha como en el algoritmo de cifrado.

Hay que notar que si *n = p*, el modo CFB queda reducido al modo CBC[15].

- **Otros Modos:**

Existen protocolos criptográficos que no se basan en la transmisión de bloques, sino en un mecanismo secuencial de codificación de *streams* de tamaño variable. Estos algoritmos permiten cifrar un mensaje bit a bit de forma continua y enviar cada bit antes que el siguiente sea codificado. Funcionan a partir de lo que se llama un *generador de secuencia de clave (keystream generator)*, un algoritmo que genera una clave continua de longitud infinita (o muy grande) bit a bit. Lo que se hace es aplicar una operación XOR entre cada bit del texto plano y cada bit de la clave. En el destino existe otro generador idéntico sincronizado para llevar a cabo el descifrado. El problema fundamental es mantener ambos generadores sincronizados, para evitar errores si se pierde algún bit de la transmisión.

Los algoritmos de codificación por bloques pueden ser empleados como generadores de secuencia de clave. Existen para ello otros modos de operación de estos algoritmos, como el OFB (*Output-Feedback*), que incorporan mecanismos para mantener la sincronía entre generadores de secuencia origen y destino.

## 2.1.4 Criptoanálisis de Algoritmos Simétricos

Se podría decir que el criptoanálisis se comenzó a estudiar seriamente con la aparición de DES. Mucha gente desconfiaba (y aun desconfía) del algoritmo propuesto por la NSA. Se dice que existen estructuras *extrañas*, que muchos consideran sencillamente *puertas traseras* colocadas por la Agencia para facilitarles la decodificación de los mensajes. Nadie ha podido aún demostrar ni desmentir este punto. Lo único cierto es que el interés por buscar posibles debilidades en él ha llevado a desarrollar técnicas que posteriormente han tenido éxito con otros algoritmos.

[15] Fúster Sabater A., L. H. (2012). *Criptografía, Protección de Datos y Aplicaciones*. Ed. Alfaomega Grupo Editor.

Ni que decir tiene que estos métodos no han conseguido doblegar a DES, pero sí representan mecanismos significativamente más eficientes que la fuerza bruta para criptoanalizar un mensaje. Los 2 métodos que vamos a comentar parten de que nosotros podemos codificar cuantos mensajes queramos usando la clave que podemos descubrir.

- **Criptoanálisis Diferencial:**

Descubierto por Biham y Shamir en 1990, permite efectuar un ataque de texto plano escogido a DES que resulta más eficiente que la fuerza bruta. Se basa en el estudio de los pares de criptogramas que surgen cuando se codifican dos textos planos con diferencias particulares, analizando la evolución de dichas diferencias a lo largo de las rondas de DES.

Para llevar a cabo un criptoanálisis diferencial se toman dos mensajes cualesquiera (incluso aleatorios) idénticos salvo en un número concreto de bits. Usando las diferencias entre los textos cifrados, se asignan probabilidades a las diferentes claves de cifrado. Conforme tenemos más y más pares, una de las claves aparece como la más probable. Esa será la clave buscada.

- **Criptoanálisis Lineal:**

El criptoanálisis lineal, descubierto por Mitsuru Matsui, basa su funcionamiento en tomar algunos bits del texto plano y efectuar una operación XOR entre ellos, tomar algunos del texto cifrado y hacerles lo mismo, y finalmente hacer un XOR de los dos resultados, obteniendo como resultado un único bit. Efectuando esa operación a muchos pares de texto plano y criptograma diferentes podemos ver si salen más ceros o más unos.

Existen combinaciones de bits que, bien escogidas, dan lugar a un sesgo significativo en la medida anteriormente definida, es decir, que el número de ceros (o unos) es significativamente superior. Esta propiedad nos va a permitir poder asignar mayor probabilidad a unas claves sobre otras y de esta forma descubrir la clave que buscamos.

## 2.2 Algoritmos Asimétricos de Cifrado

Los algoritmos de llave pública, o algoritmos asimétricos, han demostrado su interés para ser empleados en redes de comunicación inseguras (Internet). Introducidos por Whitfield Diffie y Martin Hellman a mediados de los años 70, su novedad fundamental con respecto a la criptografía

simétrica es que las claves no son únicas, sino que forman pares. Hasta la fecha han aparecido multitud de algoritmos asimétricos, la mayoría de los cuales son inseguros, otros son poco prácticos, bien sea porque el criptograma es considerablemente mayor que el mensaje original, bien sea porque la longitud de la clave es enorme. En la práctica muy pocos algoritmos son útiles, y se basan en general en plantear al atacante problemas matemáticos difíciles de resolver. El algoritmo más popular es RSA, que aún se mantiene a salvo de ataques, si bien necesita una longitud de clave considerable. Otros algoritmos son los de ElGamal y Rabin.

En general, los algoritmos asimétricos emplean longitudes de clave mucho mayores que los algoritmos simétricos. Por ejemplo, mientras que para algoritmos simétricos se consideran seguros 128 bits, para algoritmos asimétricos se recomienda al menos 1024 bits en las claves. Además, la complejidad de cálculo de estos algoritmos los hace considerablemente más lentos que los algoritmos por bloques. En la práctica los algoritmos asimétricos se emplean únicamente para codificar la *clave de sesión* (simétrica) de cada mensaje.[16]

## 2.2.1 Aplicaciones de los Algoritmos Asimétricos

Los algoritmos asimétricos poseen dos claves diferentes en lugar de una, $K_p$ y $K_P$ , denominadas *clave privada* y *clave pública*. Una de ellas se emplea para codificar, mientras que la otra se usa para decodificar. Dependiendo de la aplicación que le demos al algoritmo, la clave pública será la de cifrado o viceversa. Para que estos criptosistemas sean seguros también ha de cumplirse que a partir de una de las claves resulte extremadamente difícil calcular la otra. A continuación se dará a conocer las aplicaciones que usa este algoritmo:

- **Protección de la Información:**

Una de las aplicaciones inmediatas de los algoritmos asimétricos es el cifrado de la información sin tener que transmitir la clave de decodificación, lo cual permite su uso en canales inseguros. Supongamos que *A* quiere enviar un mensaje a *B* (ver Fig. 2.5). Para ello solicita a *B* su clave pública $K_P$ . *A* genera entonces el mensaje cifrado $E_{K_P}$ (*m*). Una vez hecho esto únicamente quien posea la clave $K_p$ podrá recuperar el mensaje original *m*.

[16] Fúster Sabater A., L. H. (2012). *Criptografía, Protección de Datos y Aplicaciones*. Ed. Alfaomega Grupo Editor.

Se nota que para este tipo de aplicación, la llave que se hace pública es aquella que permite codificar los mensajes, mientras que la llave privada es aquella que permite descifrarlos.

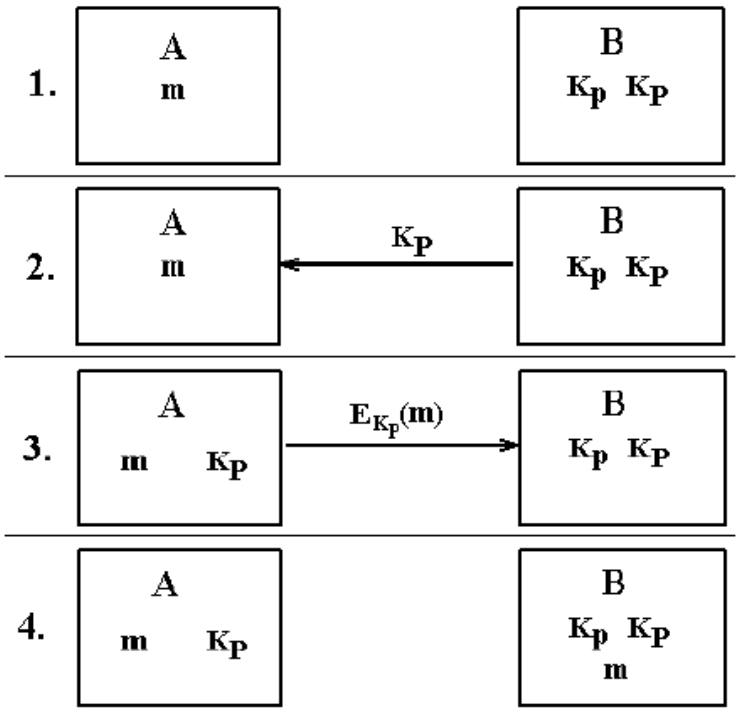


**Figura 2.5**: Transmisión de información empleando algoritmos asimétricos. 1.- **A** tiene el mensaje *m* y quiere enviárselo a **B**; 2.- **B** envía a **A** su clave pública, $K_P$ ; 3.- **A** codifica el mensaje *m* y envía a **B** el criptograma $E_{K_P}$ (*m*); 4.- **B** decodifica el criptograma empleando la clave privada $K_p$ .

- **<u>Autenticación:</u>**

La segunda aplicación de los algoritmos asimétricos es la autentificación de mensajes, con ayuda de funciones *resumen*, que nos permiten obtener una firma a partir de un mensaje. Dicha firma es mucho más pequeña que el mensaje original, y es muy difícil encontrar otro mensaje que tenga la misma firma. Supongamos que *A* recibe un mensaje *m* de *B* y quiere comprobar su autenticidad. Para ello *B* genera un resumen del mensaje *r* (*m*) (ver Fig. 2.6) y lo codifica empleando la clave de cifrado, que en este caso será privada. La clave de descifrado se habrá hecho pública previamente, y debe estar en poder de *A*. *B* envía entonces a *A* el criptograma correspondiente a *r* (*m*). *A* puede ahora generar su propia copia de *r* (*m*) y compararla con el criptograma enviado por *B*. Si coinciden, el mensaje será auténtico, puesto que el único que posee la clave para codificar es precisamente *B*.

Hay que notar que en este caso la clave que se emplea para cifrar es la clave privada, justo al revés que para la simple codificación de mensajes.

Muchos de los algoritmos asimétricos presentan claves *duales*, esto quiere decir que si empleamos una para codificar, la otra permitirá decodificar y viceversa. Esto ocurre con el algoritmo RSA, por lo que un único par de claves es suficiente para codificar y autentificar.

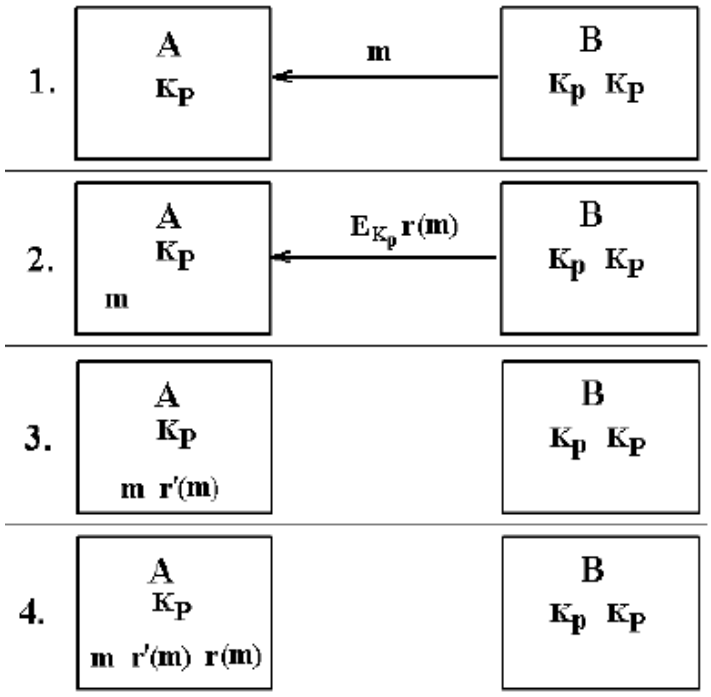


**Figura 2.6**: Autentificación de información empleando algoritmos asimétricos. 1.- **A**, que posee la clave pública $K_P$ de **B**, recibe el mensaje *m* y quiere autentificarlo; 2.- **B** genera el resumen de *m* envía a **A** el criptograma asociado $E_{K_P}(r(m))$ ; 3.- **A** genera por su cuenta $r'(m)$ y decodifica el criptograma recibido usando la clave $K_P$ ; 4.- **A** compara ***r* (*m*)** y $r'(m)$ para comprobar la autenticidad del mensaje *m*.

## 2.2.2 Algoritmo RSA

De entre todos los algoritmos asimétricos, quizá RSA sea el más sencillo de comprender e implementar. Sus pares de claves son duales, por lo que sirve tanto para codificar como para autentificar. Su nombre proviene de sus tres inventores: Ron Rivest, Adi Shamir y Leonard

Adleman. Desde su nacimiento nadie ha conseguido probar o rebatir su seguridad, pero se le tiene como uno de los algoritmos asimétricos más seguros.

RSA se basa en la dificultad para factorizar números grandes. Las claves pública y privada se calculan a partir de un número que se obtiene como producto de dos *primos grandes*. El atacante se enfrentará, si quiere recuperar un texto plano a partir del criptograma y la llave pública, a un problema de factorización.

Para generar un par de llaves ( $K_P$ , $K_p$ ), en primer lugar se escogen aleatoriamente dos números primos grandes, *p* y *q*. después se calcula el producto $n = pq$ .

Escogeremos ahora un número *e* primo relativo con $(p-1)(q-1)$. $(e\,, n)$ Será la clave pública. Nótese que "*e*" debe tener inversa módulo $(p-1)(q-1)$, por lo que existirá un número *d* tal que:

$$de \equiv 1(mod\ (p-1)(q-1))$$

Es decir, que *d* es la inversa de *e* módulo $(p-1)(q-1)$. $(d\,, n\,)$ Será la clave privada. Esta inversa puede calcularse fácilmente empleando el Algoritmo Extendido de Euclides. Nótese que si desconocemos los factores de *n*, este cálculo resulta prácticamente imposible.
La *codificación* se lleva a cabo según la expresión:

$$c = m^e \pmod{n}$$

Mientras que la *decodificación* se hará de la siguiente forma:

$$m = c^d \pmod{n}$$

Ya que:

$$c^d = (m^e)^d = m^{ed} = m^{k\,(p-1)(q-1)+1} = (m^k)^{(p-1)(q-1)}m$$

En la práctica, cogeremos *p* y *q* con un número grande de bits, por ejemplo 200, con lo que *n* tendrá 400 bits. Subdividiremos el mensaje que queramos enviar en bloques de 399 bits (de esta forma garantizamos que el valor de cada bloque sea menor de *n*) y efectuamos la codificación de

cada uno. Obtendremos un mensaje cifrado ligeramente más grande, puesto que estará compuesto por bloques de 400 bits. Para decodificar partiremos el mensaje cifrado en bloques de 400 bits (ya que en este caso sabemos que el valor de cada bloque ha de ser menor que *n*), y obtendremos bloques de 399 bits.

El atacante, si quiere recuperar la clave privada a partir de la pública, debe conocer los factores *p* y *q* de *n*, y esto representa un problema computacionalmente intratable, siempre que *n*, *p* y *q* sean lo suficientemente grandes.[17]

### 2.2.3 Algoritmo ElGamal

Fue diseñado en un principio para producir firmas digitales, pero posteriormente se extendió también para codificar mensajes. Se basa en el problema de los logaritmos discretos.[18]

Para generar un par de llaves, se escoge un número primo *p* y dos números aleatorios *g* y *x* menores que *p*. Se calcula entonces:

$$y = g^x \pmod{p}$$

La llave pública es (*g, y, p*), mientras que la llave privada es *x*.

- **Firmas Digitales de ElGamal:**

Para *firmar* un mensaje *m* basta con escoger un número *k* aleatorio, tal que $\text{mcd}\,(k,\ p-1) = 1$ , y calcular:

$$a = g^k \pmod{p}$$

Luego se emplea el Algoritmo Extendido de Euclides para resolver la ecuación:

$$m = (xa + kb) \pmod{(p-1)}$$

La firma la constituye el par (*a, b*). En cuanto al valor *k*, debe mantenerse en secreto y ser diferente cada vez. La firma se verifica comprobando que:

$$y^a a^b = g^m \pmod{p}$$

[17] Fúster Sabater A., L. H. (2012). *Criptografía, Protección de Datos y Aplicaciones*. Ed. Alfaomega Grupo Editor.

[18] Fúster Sabater A., L. H. (2012). *Criptografía, Protección de Datos y Aplicaciones*. Ed. Alfaomega Grupo Editor.

➢ **Codificación de ElGamal:**

Para codificar el mensaje *m* se escoge primero un número aleatorio *k* primo relativo con $(p-1)$, que también será mantenido en secreto. Calculamos entonces las siguientes expresiones:

$$a = g^k \pmod{p}$$

$$b = y^k m \pmod{p}$$

El par (*a, b*) es el texto cifrado, de doble longitud que el texto original. Para decodificar se calcula:

$$m = \frac{b}{a^x} \pmod{p}$$

## 2.2.4 Algoritmo Rabin

El sistema de llave asimétrica de Rabin se basa en el problema de calcular raíces cuadradas módulo un número compuesto. Esto es equivalente a factorizar dicho número.

En primer lugar escogemos dos números primos, *p* y *q*, ambos congruentes con 3 módulo 4 (los dos últimos bits a 1). Estos primos son la clave privada. La clave pública es su producto, $n = pq$ .

Para codificar un mensaje *m*, simplemente se calcula:

$$c = m^2 \pmod{n}$$

La decodificación del mensaje se hace calculando lo siguiente:

$$m_1 = c^{(p+1)/4} \pmod{p}$$

$$m_2 = \left(p - c^{\frac{p+1}{4}}\right) \pmod{p}$$

$$m_3 = c^{\frac{q+1}{4}} \pmod{q}$$

$$m_4 = \left(q - c^{\frac{q+1}{4}}\right) \pmod{q}$$

Luego se escogen $a$ y $b$ tales que $a = q(q^{-1} (\text{mod } p))$ y $b = p(p^{-1} (\text{mod } q))$. Los cuatro posibles mensajes originales son:

$$m_a = (am_1 + bm_3) \ (\text{mod } n)$$
$$m_b = (am_1 + bm_4) \ (\text{mod } n)$$
$$m_c = (am_2 + bm_3) \ (\text{mod } n)$$
$$m_d = (am_2 + bm_4) \ (\text{mod } n)$$

Desgraciadamente, no existe ningún mecanismo para decidir cuál de los cuatro es el auténtico, por lo que el mensaje deberá incluir algún tipo de información para que el receptor pueda distinguirlo de los otros.[19]

## 2.3 Criptografía Clásica

En este subtema el autor Jesús Ortega considera a los mecanismos criptográficos como *clásicos*. Se puede llamar así a todos los sistemas de cifrado anteriores a la 2ª. Guerra Mundial, o lo que es lo mismo, al nacimiento de las computadoras.

La transición desde la Criptografía clásica a la moderna se da precisamente durante la 2ª. Guerra Mundial, cuando el Servicio de Inteligencia aliado *rompe* la máquina de cifrado del ejército alemán, llamada ENIGMA.

Todos los algoritmos criptográficos clásicos son simétricos, ya que hasta mediados de los años setenta no nació la Criptografía asimétrica, y por esa razón este subtema se engloba dentro del bloque de la asignatura dedicado a los algoritmos de llave privada[20].

### 2.3.1 Algoritmos Clásicos de Cifrado

Estudiaremos en esta sección algunos criptosistemas que en la actualidad han perdido su eficacia, debido a que son fácilmente criptoanalizables empleando cualquier computadora doméstica, pero

[19] Fúster Sabater A., L. H. (2012). *Criptografía, Protección de Datos y Aplicaciones*. Ed. Alfaomega Grupo Editor.
[20] Jesús Javier Ortega Triguero, M. Á. (2006). *Introducción a la Criptografía: Historia y Actualidad*. Ed. Univ. de Castilla La Mancha.

que fueron empleados con éxito hasta principios del siglo XX. Algunos se remontan incluso, como el algoritmo de César, a la Roma Imperial. Sin embargo mantienen un interés teórico, ya que nos van a permitir explotar algunas de sus propiedades para entender mejor los algoritmos modernos. A continuación se mencionarán los cifrados que se dan con estos algoritmos:

- **Cifrados Monoalfabéticos:**

Se engloban dentro de este apartado todos los algoritmos criptográficos que, sin desordenar los símbolos del lenguaje, establecen una correspondencia única para todos ellos en todo el mensaje. Es decir, si al símbolo *A* le corresponde el símbolo *D*, esta correspondencia se mantiene a lo largo de todo el mensaje.

- **Algoritmo de César[21]:** El algoritmo de *César*, llamado así porque es el que empleaba Julio César para enviar mensajes secretos, es uno de los algoritmos criptográficos más simples. Consiste en sumar 3 al número de orden de cada letra. De esta forma a la *A* le corresponde la *D*, a la *B* la *E*, y así sucesivamente. Si asignamos a cada letra un número $(A = 0\,,\ B = 1\ldots)$, y consideramos un alfabeto de 26 letras, la transformación criptográfica sería:

$$C = (M + 3) \bmod 26$$

Obsérvese que este algoritmo ni siquiera posee clave, la transformación siempre es la misma.

**Sustituto Afín**:

Es el caso general del algoritmo de César. Su transformación sería:

$$E_k(M) = (aM + b) \bmod 26$$

Siendo *a* y *b* dos números enteros menores que el cardinal *N* del alfabeto, y cumpliendo que $mcd\ (a, N) = 1$ . La clave *k* es el par (*a, b*).

- **Cifrado Monoalfabético General:** Es el caso más general de cifrado Monoalfabético. La sustitución ahora es arbitraria, siendo la clave *k* precisamente la tabla de sustitución de un símbolo por otro.

[21] Jesús Javier Ortega Triguero, M. Á. (2006). *Introducción a la Criptografía: Historia y Actualidad*. Ed. Univ. de Castilla La Mancha.

- **Criptoanálisis de los Métodos de Cifrado Monoalfabéticos:** El cifrado Monoalfabético constituye la familia de métodos más simple de criptoanalizar, puesto que las propiedades estadísticas del texto plano se conviertan en el criptograma. Supongamos que, por ejemplo, la letra que más aparece en Castellano es la *A*. parece lógico que la letra más frecuente en el texto codificado sea aquella que corresponde con la *A*. Emparejando las frecuencias del idioma en el que se supone está el texto plano, podremos averiguar fácilmente la clave.

  En el peor de los casos, es decir, cuando tenemos un emparejamiento arbitrario, la distancia de unicidad de Shannon que obtenemos es:

$$N = \frac{H(K)}{D} = \frac{log_2\,(n!)}{D}$$

  Donde *D* es la redundancia del lenguaje empleado en el mensaje original, y *n* es el número de símbolos de dicho lenguaje. Suponemos que las *n!* claves diferentes son equiprobables en principio.
  En casos más restringidos, como el afín, el criptoanálisis es aún más simple, puesto que el emparejamiento de todos los símbolos debe responder a alguna combinación de coeficientes (*a, b*).

➢ **Cifrados Polialfabéticos[22]:**

En los cifrados Polialfabéticos la sustitución aplicada a cada carácter varía en función de la posición de éste dentro del texto plano. En realidad corresponde a la aplicación cíclica de *n* cifrados Monoalfabéticos.

- **Cifrado de Vigenere**: Es un ejemplo típico de cifrado polialfabético, cuya clave es una secuencia de letras $K = \{k_0,\ k_1, \ldots\ k_{d-1}\}$ y que emplea la siguiente función de cifrado:

$$E_k(m_i) = m_i + k_{(i \bmod d)} (\bmod\ n)$$

  Siendo $m_i$ el *i*-ésimo símbolo del texto plano y *n* el cardinal del alfabeto de entrada.

[22] Jesús Javier Ortega Triguero, M. Á. (2006). *Introducción a la Criptografía: Historia y Actualidad*. Ed. Univ. de Castilla La Mancha.

- **Criptoanálisis:** Para criptoanalizar este tipo de claves basta con efectuar *d* análisis estadísticos independientes agrupando los símbolos según la $k_i$ empleada para codificarlos. Para estimar *d*, buscaremos la periodicidad de los patrones comunes que puedan aparecer en el texto cifrado. Obviamente, para el criptoanálisis, necesitaremos al menos *d* veces más cantidad de texto que con los métodos Monoalfabéticos.

➢ **Cifrados por Sustitución Homofónica[23]:**

Para paliar la sensibilidad frente a ataques basados en el estudio de las frecuencias de aparición de los símbolos, existe una familia de algoritmos que trata de ocultar las propiedades estadísticas del texto plano empleando un alfabeto de salida con más símbolos que el alfabeto de entrada.

Supongamos que nuestro alfabeto de entrada posee cinco letras, {*a, b, c, d*}. Supongamos además que en nuestros textos la letra *a* aparece con una probabilidad 0.4 y el resto con probabilidad 0.2. Podríamos emplear el siguiente alfabeto de salida {α, β, γ, δ, ε}. Efectuaremos entonces la siguiente asociación:

$$E(a) = \begin{cases} \alpha & \text{con probabilidad } 1/2 \\ \beta & \text{con probabilidad } 1/2 \end{cases}$$

$$E(b) = \gamma$$

$$E(c) = \delta$$

$$E(d) = \varepsilon$$

En el texto cifrado ahora todos los símbolos aparecen con igual probabilidad, lo que imposibilita un ataque basado en frecuencias. El inconveniente es que necesitamos conocer la distribución estadística de los símbolos en el texto plano y que el alfabeto de salida es mayor que el de la entrada.

➢ **Cifrados de Transposición[24]:**

Este tipo de mecanismos de cifrado no sustituye los símbolos por otros, sino que cambia su orden dentro del texto. Un mecanismo de transposición podría consistir en colocar el texto en una tabla

[23]Jesús Javier Ortega Triguero, M. Á. (2006). *Introducción a la Criptografía: Historia y Actualidad*. Ed. Univ. de Castilla La Mancha.

[24] Jesús Javier Ortega Triguero, M. Á. (2006). *Introducción a la Criptografía: Historia y Actualidad*. Ed. Univ. de Castilla La Mancha.

de *n* columnas, y dar como texto cifrado los símbolos de una columna (ordenados de arriba abajo) concatenados con los de otra, etc. La clave sería el número *n* y el orden en el que se leen las columnas.

Por ejemplo, supongamos que queremos cifrar el texto "*El perro de San Roque no tiene rabo*", con $n = 5$ y la permutación {3, 2, 5, 1, 4} como clave.

De acuerdo a los datos mencionados en el párrafo anterior se obtiene la siguiente tabla:

| 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|
| E | L | | P | E |
| R | R | O | | D |
| E | | S | A | N |
| | R | O | Q | U |
| E | | N | O | |
| T | I | E | N | E |
| | R | A | B | O |

Tendríamos como texto cifrado *"Osonealr r irednu eoere et p aqonb"*.

- **Criptoanálisis:** Este tipo de mecanismos de cifrado se puede criptoanalizar efectuando un estudio estadístico sobre la frecuencia de aparición de pares y tripletas de símbolos en el texto plano.

# CAPÍTULO III. CRIPTOANÁLISIS Y LOS SISTEMAS INFORMÁTICOS

## 3.1 Fundamentos[25]

**Fundamentos Generales sobre los Elementos Software de un Sistema Informático**

Se ha contado que el software es el conjunto de herramientas y programas que permiten al usuario comunicarse con el ordenador y aprovechar sus prestaciones.

Básicamente y según su funcionalidad podemos definir dos tipos de software:

- Software de Sistema Operativo:

El Sistema Operativo es el programa o conjunto de programas que permite la comunicación del usuario con el ordenador así como el control de todos los componentes del sistema para obtener un rendimiento adecuado del ordenador.

Según su aspecto y modo de trabajo tenemos dos tipos: "de línea de comando" que son aquellos sistemas en los que las órdenes se dan con ayuda de una consola y han de teclearse con todos sus parámetros. (Ej. MS-DOS, LINUX sin entorno gráfico). Otro tipo es "de entorno gráfico" que permiten la comunicación con el ordenador de una forma más rápida e intuitiva con ayuda de íconos gráficos y pulsaciones de ratón. (Ej. Windows XP / VISTA o LINUX con entornos G-NOME o KDE).

- Software de Aplicación:

El software de aplicación es el que permite al usuario realizar tareas concretas con ayuda de un ordenador. Aplicaciones hay de muchos tipos teniendo en cuenta incluso los programas por un usuario con conocimientos de programación se pueden considerar aplicaciones.

En función de su utilidad las más conocidas por los usuarios son las que tienen que ver con la ofimática:

[25]Montero, M. S. (1995). *Administración de Sistemas Informáticos*. Ed. Ministerio de Educación.

- **Procesadores de Texto**: Para la elaboración de documentos. (Word, Word Perfect, etc.)
- **Hojas de Cálculo**: Para la automatización de cálculos. (Lotus 123, Excel, etc.)
- **Sistemas Gestores de Bases de Datos**: Son herramientas que nos permiten la creación y mantenimiento de grandes cantidades de información de forma que sea fácil su consulta o manipulación. (Access, Oracle, Paradox, etc.)
- **Programas de Retoque Fotográfico o Edición de Video**: Permiten la obtención y retoque de fotografías así como la edición de video en el ordenador. Son herramientas más profesionales.
- **Aplicaciones de Internet**: Permiten al usuario utilizar todas las posibilidades que ofrece el Internet:

    - Consulta de información con navegadores como Explorer, Opera, Mozilla, Netscape, etc.
    - Consulta de correo con programas como Outlook, Eudora, etc.
    - Transferencia de archivos con programas como WS-FTP, COMMANDER, etc.
    - Programas de comunicación en tiempo real con audio y video como Messenger, NetMeeting, etc.

En esta relación no se describen todos los tipos de aplicaciones ya que sería imposible. Prácticamente cada campo profesional donde el ordenador se utiliza como herramienta de trabajo tiene sus propias aplicaciones.

## 3.2 Criptoanálisis y la Seguridad[26]

A continuación se darán los conceptos de criptoanálisis y seguridad para saber la diferencia que hay entre ambos:

➢ **Criptoanálisis:**

El *criptoanálisis* consiste en comprometer la seguridad de un criptosistema. Esto se puede hacer descifrando un mensaje sin conocer la llave, o bien obteniendo la llave empleada para cifrar algún

[26] Pastor Franco J., M. Á. (2001). *Criptografía Digital: Fundamentos y Aplicaciones*. Ed. 2, Illustrated

mensaje. No se considera criptoanálisis el descubrimiento de un algoritmo secreto de cifrado; hemos de considerar por el contrario que el algoritmo de cifrado siempre es conocido.

Uno de los tipos de análisis más comunes que se realizan es el de *texto plano escogido*, que parte de que conocemos una serie de pares de textos planos y textos cifrados, codificados con la misma clave. Esta situación se suele dar cuando tenemos acceso al dispositivo de cifrado y éste nos permite efectuar operaciones, pero no nos permite leer su clave (por ejemplo: las tarjetas de los teléfonos móviles GSM). Cuando el sistema es débil, basta con escoger unos cientos de mensajes y codificarlos, y de esta forma tendremos información suficiente para deducir la clave empleada.

También podemos tratar de criptoanalizar un sistema aplicando el algoritmo de descifrado a un mensaje codificado que poseemos y comprobar si lo que nos sale *tiene sentido* como posible texto plano. Este método y todos los que buscan exhaustivamente por el espacio de claves *K*, se denominan *ataques por la fuerza bruta*, y en muchos casos no suelen considerarse técnicas de criptoanálisis, reservándose este término para aquellos mecanismos que explotan posibles debilidades intrínsecas en el algoritmo de cifrado. Se da por supuesto que el espacio de claves para cualquier criptosistema digno de interés ha de ser suficientemente grande como para que un ataque por la fuerza bruta no sea viable. Hemos de tener en cuenta no obstante que la capacidad de cálculo de las computadoras crece a gran velocidad, por lo que algoritmos que hace unos años eran resistentes frente a ataques por la fuerza bruta hoy por hoy pueden ser inseguros (como es el caso de DES).

Un par de métodos de criptoanálisis que han dado interesantes resultados son el *análisis diferencial* y el *análisis lineal*. El primero de ellos, partiendo de pares de mensajes con diferencias mínimas (usualmente de un bit), estudia las variaciones que existen entre los mensajes cifrados correspondientes, tratando de identificar patrones comunes. El segundo emplea operaciones XOR entre algunos bits del texto plano y algunos bits del texto cifrado, obteniendo finalmente un único bit. Si realizamos esto con muchos pares de texto plano-texto cifrado podemos obtener una probabilidad *p* en ese bit que calculamos. Si *p* está suficientemente sesgada (no se aproxima a ½), tendremos la posibilidad de recuperar la clave.

Otro tipo de análisis, esta vez para los algoritmos asimétricos, consistiría en tratar de deducir la llave privada a partir de la pública. Suelen ser técnicas analíticas que básicamente intentan resolver los problemas de elevado coste computacional en los que se apoyan estos criptosistemas: factorización, logaritmos discretos, etc. Mientras estos problemas genéricos permanezcan sin solución, podremos seguir confiando en estos algoritmos.

La criptografía no sólo se emplea para proteger información, también se utiliza para permitir su autentificación, es decir, para identificar al autor de un mensaje e impedir que nadie suplante su personalidad. En estos casos surge un nuevo tipo de criptoanálisis que está encaminando únicamente a permitir que elementos falsos pasen por buenos. Puede que ni siquiera nos interese descifrar el mensaje original, sino simplemente poder sustituirlo por otro falso y que supere las pruebas de autentificación.

- **Seguridad:**

El concepto de seguridad en la información es mucho más amplio que la simple protección de los datos a nivel *lógico*. Para proporcionar una seguridad real hemos de tener en cuenta múltiples factores, tanto internos como externos. En primer lugar habría que caracterizar el sistema que va a albergar la información para poder identificar las amenazas, y en este sentido podríamos hacer la siguiente subdivisión:

1. ***Sistemas Aislados***: Son los que no están conectados a ningún tipo de red. De unos años a esta parte se han convertido en minoría, debido al auge que ha experimentado Internet.
2. ***Sistemas Interconectados***: Hoy por hoy casi cualquier ordenador pertenece a alguna red, enviando y recogiendo información del exterior casi constantemente. Esto hace que las redes de ordenadores sean cada día más complejas y supongan un peligro potencial que no puede en ningún caso ser ignorado.

En cuanto a las cuestiones de seguridad que hemos de fijar podríamos clasificarlas de la siguiente forma:

1. ***Seguridad Física***: Englobaremos dentro de esta categoría a todos los asuntos relacionados con la salvaguarda de los soportes físicos de la información, más que de la información

propiamente dicha. En este nivel estarían, entre otras, las medidas contra incendios y sobrecargas eléctricas, la prevención de ataques terroristas, las políticas de *backup*, etc. También se suelen tener en cuenta dentro de este punto aspectos relacionados con la restricción de acceso físico a las computadoras únicamente a personas autorizadas.

2. ***Seguridad de la Información***: En este apartado presentaremos atención a la preservación de la información de la información frente a observadores no autorizados. Para ello podemos emplear tanto la criptografía simétrica como asimétrica, estando la primera únicamente indicada en sistemas aislados, ya que si la empleáramos en redes, al tener que transmitir la clave por el canal de comunicación, estaríamos asumiendo un riesgo excesivo.
3. ***Seguridad del Canal de Comunicación***: Los canales de comunicación rara vez se consideran seguros. Debido a que en la mayoría de los casos escapan a nuestro control, ya que pertenecen a terceros, resulta imposible asegurarse de que no están siendo escuchados o intervenidos.
4. ***Problemas de Autentificación***: Debido a los problemas del canal de comunicación, es necesario asegurarse de que la información que recibimos en la computadora viene de quien realmente creemos que viene. Para esto se suele emplear criptografía asimétrica en conjunción con funciones *resumen*.
5. ***Problemas de Suplantación***: En las redes tenemos el problema añadido de que cualquier usuario autorizado puede acceder al sistema desde fuera, por lo que hemos de confiar en sistemas fiables para garantizar que los usuarios no están siendo suplantados por intrusos. Normalmente se emplean mecanismos basados en *password* para conseguir esto.

## 3.3 Concepto de Sistemas Informáticos[27]

En términos genéricos se puede afirmar que el sistema informático es un conjunto de elementos interrelacionados entre sí y relacionados a su vez con el sistema global en que se encuentra que pretende conseguir unos fines determinados. Los elementos constitutivos de un sistema informático serán físicos, lógicos y humanos.

Estructuralmente un sistema se puede dividir en partes pero, funcionalmente es indivisible, ya que si se dividiera perdería alguna de sus propiedades esenciales. Así, un sistema informático sin

[27] Bertolín, J. A. (2008). *Seguridad de la Información: Redes, Informática y Sistema de Información*. Ed. Paraninfo.

alguno de sus componentes, no funcionaría. Como características globales de un sistema informático podríamos señalar las siguientes:

- Las propiedades o comportamiento de cada uno de los elementos del sistema influyen en las propiedades y funcionamiento del sistema completo.
- El tipo de influencia que ejerce cada elemento del sistema depende, al menos, del comportamiento de otro elemento.
- Cada sistema informático se compone, a su vez, de subsistemas que son sistemas informáticos por sí mismo. Al final de la descomposición se llegará al sistema informático elemental (un ordenador y su equipo lógico). Habrá que determinar en qué sentido y nivel de descomposición estamos hablando cuando nos referimos a un sistema informático.
- Normalmente, el rendimiento de un sistema informático depende más de la relación y coordinación entre sus componentes que del funcionamiento de cada uno de ellos individualmente. Por eso, a veces, el funcionamiento de un sistema informático no se mejora usando los mejores componentes físicos, lógicos y humanos sino armonizando y coordinando efectivamente sus relaciones.

### 3.3.1 Desarrollo[28]

El analista debería aplicar un enfoque sistemático en el análisis y el diseño de los sistemas de información. El ciclo de desarrollo de los sistemas o ciclo de vida de los sistemas (SDLC: Systems Development Life Cycle) es un enfoque por etapas de análisis y de diseño, que postula que el desarrollo de los sistemas mejora cuando existe un ciclo específico de actividades del analista y de los usuarios.

En general, los analistas no están de acuerdo respecto al número exacto de etapas que conforman el ciclo de desarrollo de los sistemas; sin embargo, se reconoce la importancia de su enfoque sistemático. Se dividirá el ciclo de vida en siete etapas, que aunque se presentan de manera discreta, nunca se llevan a cabo como un elemento Independiente. En lugar de ello. Se realizan al mismo tiempo diversas actividades, y éstas llegan a repetirse. Por ello es de mayor

[28] Bertolín, J. A. (2008). *Seguridad de la Información: Redes, Informática y Sistema de Información*. Ed. Paraninfo.

utilidad suponer que el ciclo de desarrollo de los sistemas transcurre en etapas (con actividades en acción que luego cesan poco a poco) y no como elementos separados.

**1. Identificación de problemas, oportunidades y objetivos.**

En esta primera etapa del ciclo de desarrollo de los sistemas, el analista se involucra en la identificación de los problemas, de las oportunidades y de los objetivos. Esta fase es crucial para el éxito del resto del proyecto, pues nadie estará dispuesto a desperdiciar su tiempo dedicándolo al problema equivocado.

La primera etapa requiere que el analista observe de forma objetiva lo que ocurre en una empresa. Luego, en conjunto con los otros miembros de la organización hará notar los problemas. Muchas veces esto ya fue realizado previamente: y por ello. Es que se llega a invitar al analista.

Las oportunidades son aquellas situaciones que el analista considera que pueden perfeccionarse mediante el uso de los sistemas de información computarizados. Al aprovechar las oportunidades, la empresa puede lograr una ventaja competitiva o llegar a establecer un estándar industrial.

La identificación de objetivos también es un componente importante de la primera fase. En un comienzo, el analista deberá descubrir lo que la empresa intenta realizar, y luego. Estará en posibilidad de determinar si el uso de los sistemas de información apoyaría a la empresa para alcanzar sus metas, el encaminarla a problemas u oportunidades específicas.

**2. Determinación de los requerimientos de información.**

La siguiente etapa que aborda el analista, es la determinación de los requerimientos de información a partir de los usuarios particularmente involucrados. Para identificar los requerimientos de información dentro de la empresa, pueden utilizarse diversos instrumentos, los cuales incluyen: el muestreo, el estudio de los datos y formas usadas por la organización, la entrevista, los cuestionarios: la observación de la conducta de quien toma las decisiones, así como de su ambiente: y también el desarrollo de prototipos.

En esta etapa el analista hace todo lo posible por identificar qué información requiere el usuario para desempeñar sus tareas. Puede ver, cómo varios de los métodos para establecer las

necesidades de información, lo obligan a relacionarse directamente con los usuarios. Esta etapa sirve para elaborar la imagen que el analista tiene de la organización y de sus objetivos. En ocasiones, se llegan a concluir sólo las primeras dos etapas del ciclo de desarrollo de los sistemas. El analista es el especialista que emprende esta clase de estudios.

**3. Análisis de las necesidades del sistema.**

La siguiente etapa que ejecuta el analista de sistemas consiste en analizar las necesidades propias del sistema. Una vez más, existen herramientas y técnicas especiales que facilitan al analista la realización de las determinaciones requeridas. Estas incluyen el uso de los diagramas de flujo de datos (DFD) que cuentan con una técnica estructurada para representar en forma gráfica la entrada de datos de la empresa, los procesos y la salida de la información. A partir del diagrama de flujo de datos se desarrolla un diccionario de datos que contiene todos los elementos que utiliza el sistema, así como sus especificaciones, si son alfanuméricos, descripción, clave primaria, entre otros.

Durante esta fase. El analista de sistemas también analiza las decisiones estructuradas por realizar, que son decisiones donde las condiciones, condiciones alternativas, acciones y reglas de acción podrán determinarse. Existen tres métodos para el análisis de las decisiones estructuradas: el lenguaje estructurado (en nuestro caso el español), las tablas de decisión y los árboles de decisión.

No todas las decisiones en las empresas se encuentran estructuradas; no obstante, es importante que las comprenda el analista de sistemas. Las decisiones semiestructuradas (decisiones que se toman bajo nesgo) con frecuencia se apoyan en los Sistemas de Toma de Decisiones. Cuando analiza las decisiones semiestructuradas. El analista las examina de acuerdo con el grado de complejidad del problema y con el número de criterios considerados al llevar a cabo las decisiones.

El análisis de decisiones de criterio múltiple (aquellas decisiones donde numerosos factores tienen que equilibrarse) también es parte de esta etapa. Se disponen de muchas técnicas para el análisis de decisiones de criterio múltiple; incluyendo entre otras, el proceso de intercambio y la aplicación de métodos de ponderado.

A esta altura del ciclo de desarrollo del sistema, el analista prepara una propuesta del sistema que resume todo lo que ha encontrado, presenta un análisis costo / beneficio de las alternativas y plantea las recomendaciones (si es que existen) de lo que deberá realizarse. Si la dirección acepta alguna de las recomendaciones, el analista procederá de acuerdo con ella.

**4. Diseño del sistema recomendado.**

En esta etapa del ciclo de desarrollo de los sistemas, el analista de sistemas usa la información que recolectó con anterioridad y elabora el diseño lógico del sistema de información. El analista diseña procedimientos precisos de captura de datos, con el fin de que los datos que se introducen al sistema sean los correctos. El analista también diseña accesos efectivos al sistema de información, mediante el uso de las técnicas de diseño de formularios y de pantallas.

Una parte del diseño lógico del sistema de información es el diseño de la interfaz con el usuario. La interfaz conecta al usuario con el sistema, y evidentemente, es de suma importancia. Serían ejemplos de interfaces para el usuario: el uso del teclado para introducir preguntas o respuestas, el uso de menús en la pantalla, con las opciones que tiene el usuario, el uso de dispositivos como el ratón (mouse) y muchos otros.

La etapa del diseño también incluye el diseño de los archivos o la base de datos que almacenará aquellos datos requeridos por quien toma las decisiones en la organización. Una base de datos bien organizada es fundamental para cualquier sistema de información. En esta etapa, el analista diseña la salida (en pantalla o impresa) hacia el usuario, de acuerdo con sus necesidades de información.

**5. Desarrollo y documentación del software**

En esta etapa del ciclo de desarrollo de los sistemas, el analista trabaja con los programadores para desarrollar todo el software original que sea necesario. Dentro de las técnicas estructuradas para el diseño y documentación del software se tienen: el método HIPO, los diagramas de flujo. Los diagramas Nassi-Schneiderman, los diagramas Warnier-Orr y el pseudocódigo. Aquí es donde, el analista de sistemas transmite al programador los requerimientos de programación.

Durante esta fase, el analista también colabora con los usuarios para desarrollar la documentación indispensable del software, incluyendo los manuales de procedimientos. La documentación le dirá al usuario como operar el software, y así también, qué hacer en caso de presentarse algún problema.

**6. Pruebas y mantenimiento del sistema.**

El sistema de información debe probarse antes de utilizarlo. El costo es menor si se detectan los problemas antes de la entrega del sistema. El programador realiza algunas pruebas por su cuenta, otras se llevan a cabo en colaboración con el analista de sistemas. En un principio, se hace una serie de pruebas, con datos tipo, para identificar las posibles fallas del sistema: más adelante, se utilizarán los datos reales.

El mantenimiento del sistema y de su documentación empiezan justamente en esta etapa: y después, esta función se realizará de forma rutinaria a lo largo de toda la vida del sistema. Las actividades de mantenimiento integran una buena parte de la rutina del programador, que para las empresas llegan a implicar importantes sumas de dinero. Sin embargo, el costo del mantenimiento disminuye de manera importante cuando el analista aplica procedimientos sistemáticos en el desarrollo de los sistemas.

**7. Implantación y evaluación de sistema.**

En esta última etapa del desarrollo del sistema, el analista ayuda a implantar el sistema de información. Esto incluye el adiestramiento que el usuario requerirá. Si bien, parte de esta capacitación la dan las casas comerciales, la supervisión del adiestramiento es una responsabilidad del analista de sistemas. Más aún, el analista necesita planear la suave transición que trae consigo un cambio de sistemas.

Aunque la evaluación del sistema se plantea como parte integrante de la última etapa del ciclo de desarrollo de los sistemas; realmente, la evaluación toma parte en cada una de las etapas. Uno de los criterios fundamentales que debe satisfacerse, es que el futuro usuario utilice el sistema desarrollado.

### 3.3.2 Estructura[29]

Un sistema informático está compuesto por:

a) **Componente Físico**: Que constituye el hardware del sistema informático que lo conforman, básicamente, los ordenadores, los periféricos y el sistema de comunicaciones. Los componentes físicos proporcionan la capacidad y la potencia de cálculo del sistema informático.
b) **Componente Lógico**: Que constituye el software del sistema informático y lo conforman, básicamente, los programas, las estructuras de datos y la documentación asociada. El software se encuentra distribuido en el hardware y lleva a cabo el proceso lógico que requieren los datos.
c) **Componente Humano**: Constituido por todas las personas participantes en todas las fases de la vida de un sistema informático (diseño, desarrollo, implantación, explotación). Este componente humano es sumamente importante ya que los sistemas informáticos están desarrollados por humanos y para uso de humanos.

Veamos, gráficamente en la Fig. 3.1 la estructura de un sistema informático genérico:

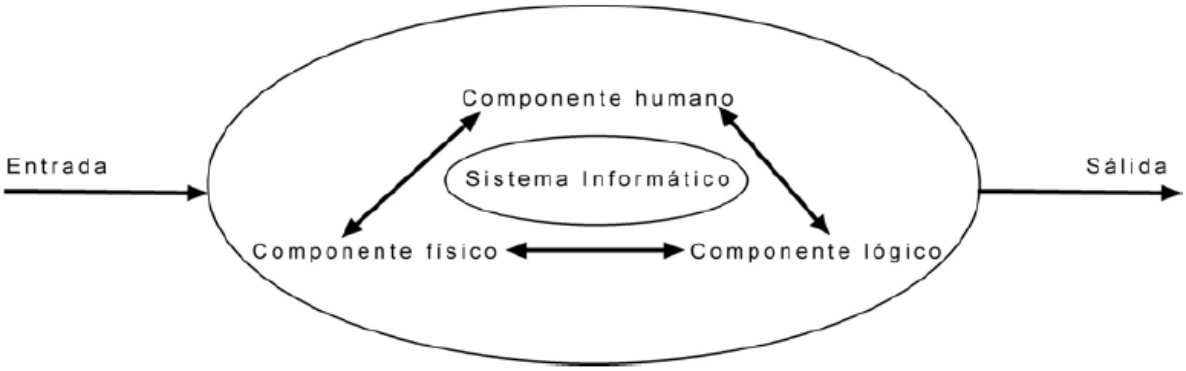


**Figura 3.1**: Estructura de un S.I Genérico

El sistema informático ha evolucionado desde una primera situación en que todos los componentes del sistema (físicos, lógicos y humanos) se encontraban centralizados en una sala de ordenadores a la situación actual en que los componentes del sistema se encuentran, normalmente, ampliamente distribuidos en diferentes lugares físicos.

[29] Bertolín, J. A. (2008). *Seguridad de la Información: Redes, Informática y Sistema de Información*. Ed. Paraninfo.

Este camino hacia la implantación progresiva de sistemas distribuidos ha pasado por diferentes fases y se puede considerar que aún no ha finalizado. Veamos estas fases más detenidamente:

- ***1ª. Fase***: Al inicio de la informatización de las organizaciones, los recursos están totalmente centralizados.
- ***2ª. Fase***: Se distribuyen los componentes físicos (y, en ocasiones, los humanos) del sistema. La capacidad de proceso y almacenamiento sigue estando centralizada pero las entradas y salidas de datos se han distribuido físicamente (terminales "tontos" conectados a un equipo central).
- ***3ª. Fase***: Se distribuyen, además, los componentes lógicos del sistema. Las capacidades de proceso también se empiezan a distribuir pero no totalmente (terminales con cierta capacidad de proceso conectados a un equipo central).
- ***4ª. Fase*:** Se llega al modelo más avanzado de informática distribuida en que tanto la capacidad de proceso como la capacidad de almacenamiento se encuentran distribuidas en diferentes lugares.

"Los sistemas distribuidos pueden organizarse de forma vertical o jerárquica y de forma horizontal."

En una organización horizontal todos los equipos tienen la misma "categoría", es decir, no existe un equipo central sino un conjunto de equipos interconectados que cooperan entre sí.

Por el contrario, en una organización vertical nos encontramos con varios niveles jerárquicos, entre los que podemos destacar:

- El nivel más alto de la jerarquía lo formas los equipos más potentes, del tipo de los mainframes y realiza los trabajos de la organización que necesiten mayores recursos. Este es el nivel de la Informática Corporativa, que soporta el Sistema General de Información de la organización.
- El segundo nivel en importancia es el de la Informática Departamental, en el que nos encontramos con ordenadores menos potentes, del tipo de los miniordenadores, que interaccionan con los mainframes del nivel superior y con los ordenadores del nivel inferior.

Actualmente, los miniordenadores de este nivel son sustituidos, cada vez con más frecuencia, por redes locales de ordenadores.

- El último nivel de la jerarquía es el de la Informática Personal, constituido por los microordenadores o estaciones de trabajo que interactúan con los ordenadores de los niveles superiores a través de redes de comunicaciones. Los ordenadores de este nivel suelen disponer de herramientas especializadas para el trabajo personal.

### 3.3.3 Clasificación[30]

Los S.I. pueden clasificarse en base a numerosos criterios. Por supuesto las clasificaciones no son estancas y es común encontrar sistemas híbridos que no encajen en una única categoría.

❖ **Por su uso pueden ser:**

- De uso general.
- De uso específico.

❖ **Por el paralelismo de los procesadores, que puede ser:**

- SISD: Single Instruction Single Data
- SIMD: Single Instruction Multiple Data
- MIMD: Multiple Instruction Multiple Data

❖ **Por el tipo de ordenador utilizado en el sistema:**

- Estaciones de trabajo (Workstations)
- Terminales ligeros (Thin clients)
- Microordenadores (por ejemplo ordenadores personales)
- Miniordenadores (servidores pequeños)
- Macroordenadores (servidores de gran capacidad)
- Superordenadores

[30] Bertolín, J. A. (2008). *Seguridad de la Información: Redes, Informática y Sistema de Información*. Ed. Paraninfo.

- **Por la arquitectura:**
  - Sistema aislado
  - Arquitectura cliente-servidor
  - Arquitectura de 3 capas
  - Arquitectura de n capas
  - Servidor de aplicaciones
  - Monitor de teleproceso o servidor de transacciones.

# CONCLUSIONES, RECOMENDACIONES Y CONSEJOS BÁSICOS

## Conclusiones

Se entiende por seguridad informática al conjunto de normas, procedimientos y herramientas, que tienen como objetivo garantizar la disponibilidad, integridad, confidencialidad y buen uso de la información que reside en un sistema de información.

Cada día más y más personas mal intencionadas intentan tener acceso a los datos de los ordenadores del plantel.

El acceso no autorizado a una red informática o a los equipos del plantel que en ella se encuentran puede ocasionar en la gran mayoría de los casos graves problemas.

Con la constante evolución de las computadoras es fundamental saber que recursos necesitar para obtener seguridad en los sistemas de información.

Como hemos estado hablando durante todo el documento hoy en día la información puede que sea uno de los bienes más preciados, o la desinformación una de las peores armas con las que atacar a alguien. Por lo que en esta en la sociedad en la que vivimos se hace muy necesario la seguridad en las comunicaciones, y como principal exponente en Internet , ya que este método de comunicación es cada vez más utilizado, no solo por estudiantes y comunidad universitaria, sino por empresas, particulares, y cada vez para realizar más cosas. Con lo cual cabe pensar que el tema que hemos tratado será uno de los claros exponentes a tener muy en cuenta en el futuro de la informática, sobre todo a la velocidad que se implementan nuevas tecnologías, las cuales permiten el envío de información más valiosa y que puede comprometer mucho a los interlocutores en caso de que sea interceptada por otras personas. La verdad que se trata de un mundo muy fascinante y que tiene muchas posibilidades de investigación.

El uso de la criptografía es indispensable en la sociedad moderna. Como usuarios de Internet, lo único que veremos son las pantallas que presentamos y el candadito en la esquina inferior derecha, sin embargo detrás de todo esto, hay toda una infraestructura que debemos tener

alguna idea de cómo funciona para poder estar seguros de que nuestra información está en buenas manos.

Actualmente, existen muchos intentos de “robar” información personal, así como números de tarjetas, cuentas de banco y contraseñas para cuentas en servicios financieros o de compra en línea.

Es importante mencionar que en muchos portales que ofrecen venta en línea deben poseer un certificado válido (en especial las instituciones bancarias) por lo que siempre debemos verificar que el navegador no nos mande advertencias con respecto al certificado.

## Recomendaciones

### Recomendaciones [Criptografía]

Durante las primeras décadas de su existencia y a lo largo del tiempo la seguridad en las redes de computadoras se ha centrado en desarrollar sistemas criptográficos, que garanticen la confiabilidad, integridad y validación de identificación en las transmisiones. Sin embargo, estos sistemas nunca son suficientes, pues con el tiempo y con el avance de la tecnología es posible quebrantarlos. El ingenio humano no es capaz de diseñar un sistema que el ingenio humano no pueda romper. Al diseñar un sistema criptográfico se estima el tiempo que se necesitaría para descifrarlo, este tiempo siempre es mayor que lo que en la práctica se necesita. Es por ello que es necesario que constantemente se estén realizando investigaciones para proveer nuevos métodos criptográficos que puedan satisfacer los requisitos más exigentes.

Debido a que en la actualidad es necesario el uso de criptografía "fuerte" en dispositivos móviles que anteriormente no fueron considerados para tal fin también es imprescindible que los nuevos criptosistemas puedan usarse con facilidad en dichos dispositivos. Estos requerimientos pueden que sean difíciles de satisfacer, pues en general los algoritmos fuertes en la criptografía moderna necesitan un considerable poder de cálculo para su funcionamiento eficaz, pero esto no debe ser un impedimento para la incorporación de mecanismos de seguridad en los dispositivos móviles que usamos diariamente.

Gran cantidad de investigaciones se encuentran actualmente en desarrollo para tratar de establecer nuevos algoritmos criptográficos como estándares mundiales. Sin embargo es importante mencionar que los criptosistemas que se desarrollen en la actualidad tendrán que pasar por un proceso largo para poder ser considerados "seguros". Esto se debe principalmente a que es necesario que la atención pública concentre su interés en ellos y traten de explotar sus "fallas" (si las tiene). Esto representa un gran problema pues por más esfuerzo que se use para crear nuevas técnicas que satisfagan los retos actuales estas no deberían ser usadas hasta después de un tiempo prudencial (la magnitud de este tiempo es de años). Debido a este gran problema es recomendable usar modificaciones de métodos conocidos y suficientemente probados para lograr seguridad en la actualidad e ir incorporando paulatinamente el uso de mecanismos de seguridad más nuevos.

Para alcanzar un nivel satisfactorio de seguridad en nuestras comunicaciones a través de celulares y PDA's los expertos no deben enfocarse únicamente en la creación de algoritmos más seguros y eficientes. Hay que tomar en cuenta que la mayoría de los usuarios no quieren complicaciones en sus tareas cotidianas. Esto implica que si el uso de los algoritmos criptográficos necesita un poco de sofisticación por parte del usuario este no lo usará (independientemente de lo bueno que sea). Por tal motivo es recomendable que entre los retos que se propongan los criptoanalistas al diseñar un algoritmo este el fácil acceso al mecanismo de seguridad para un usuario inexperto y no interesado (quienes son mayoría).

Las medidas criptográficas pueden proporcionar una importante capa de protección en la protección de datos, lo cual reduce el impacto de las violaciones. Las principales partes implicadas (las autoridades de protección de datos y los proveedores de servicios) deberían recomendar a usuarios y otros la implementación de medidas de seguridad para la protección de datos personales, al mismo tiempo que deberían confiar en las configuraciones y soluciones de vanguardia diseñadas con este propósito.

### Recomendaciones [Seguridad Informática]

Este documento tiene el propósito de proveer información básica sobre la seguridad informática para usuarios de computadoras e internet. Ningún sistema es invulnerable pero creemos que

siguiendo los consejos y tutoriales que ofrecemos aquí puedes dar un gran paso para proteger la seguridad de tus datos públicos, tus datos privados y tu identidad en internet.

A continuación se darán unos consejos básicos para saber cómo protegerse de ataques y robos de información de suma importancia:

## 1. Consejos Básicos

- **Hacer respaldos de tus datos:** El consejo más importante que podemos ofrecer a cualquier organización, colectivo o individuo es que siempre mantienen respaldos de su información digital más importante. De nada te servirán técnicas más avanzadas de seguridad si pierdes tu información por una falla mecánica o eléctrica.

  Todo tipo de almacenamiento digital es propenso a fallas. Los discos duros, cd's, dvd's, y memorias de USB pueden fallar en cualquier momento. Es difícil predecir las condiciones bajo las cuales eso puede pasar. La única solución viable para prevenir la pérdida de datos es mantener múltiples respaldos de tu información.
- **Documentación privada: archivos, carpetas y discos cifrados:** Las computadoras y los discos pueden ser robados, extraviados o caer en las manos equivocadas. Si tienes datos sensibles que no deben ser revisados por otras personas debes tomar precauciones para protegerlos.
- **Contraseñas seguras:** Hoy en día las contraseñas digitales son las llaves de control sobre nuestras vidas. Son muchas las ocasiones en las que estamos encargados de proteger el acceso y control de un sin fin de información sobre nuestro trabajo, dinero, identidad, vida personal y la de otros con una serie de números y/o letras que no debemos olvidar. Esta situación se complica por el hecho de que tenemos que recordar varias contraseñas a la vez. Si pensabas que memorizar tus tablas de multiplicación en la primaria fue difícil esta nueva situación puede ser una verdadera pesadilla. Las contraseñas pueden ser un punto muy débil en nuestra seguridad si no tomamos las precauciones necesarias.
- **No utilices contraseñas débiles:**
  - No utilices una cuenta sin contraseña ni dejes una contraseña vacía, esto sin duda es la práctica más insegura que existe.
  - Nunca utilices la contraseña que el sistema te da por omisión, siempre debes cambiarla por una contraseña nueva.

- Nunca utilices una contraseña derivada de tus datos personales como:
  - ❖ Tu nombre
  - ❖ Fechas de Nacimiento
  - ❖ Números de Identificación
  - ❖ Números de Teléfono
  - ❖ Dirección
  - ❖ Nombre de tu Novi@, Hijos o Mascota

(Contraseñas basadas en estos datos son muy fáciles de adivinar.)

- Nunca elijas como contraseña una palabra o una frase basada en palabras que aparecen en el diccionario o del lenguaje común. Estas contraseñas serán adivinadas fácilmente por ataques de fuerza bruta.

**¿Qué es un ataque de fuerza bruta?**

- No es suficiente intercambiar números por letras de una palabra en el diccionario. Ejemplo: contraseña a c0n+ra53ñ4.
- No utilices contraseñas de menos de 8 caracteres.

➢ **Utiliza contraseñas fuertes**

- Tu contraseña debe utilizar 8 caracteres o más.
- Tu contraseña debe ser una mezcla de letras, números y símbolos.
- Evita que algún carácter se repita
- La mezcla de caracteres que componen tu contraseña debe parecer completamente azarosa. Ejemplo: %UoAg&e0a6

➢ **No olvides tu contraseña:** El problema de las contraseñas fuertes es que son difíciles de recordar. En algunas situaciones olvidar tu contraseña puede ser catastrófico y no tiene remedio. Muchas veces existe la posibilidad de que un sistema te ofrezca pistas para recordar tu contraseña o te permita regenerarla pero debemos evitar recurrir a estas opciones ya que nos pueden hacer vulnerables a otros tipos de ataques. Lo más seguro es no olvidar nuestra contraseña. Para eso podemos emplear alguna técnica que nos permite componer una contraseña fuerte basada en otra información que nos sea más fácil de recordar.

Una estrategia fácil es tomar una cita de un autor, las letras de una canción, o cualquier frase que te sea fácil recordar y utilizar un método para derivar tu contraseña fuerte de ella.

- **No repitas contraseñas:** Nunca utilizar la misma contraseña para más que una cuenta. Si la seguridad de tu contraseña es comprometida el atacante tendrá acceso a más que una cuenta.
- **No compartas tu contraseña:** Aunque haya momentos en los cuales nos puede parecer inocente compartir nuestra contraseña con un conocido esto no es una práctica segura. Evita compartir usuarios de computadora, bandejas de correo u otros servicios. Si necesitas compartir la misma información con otras personas existen herramientas diseñados para hacer esto que permite a cada persona tener acceso a la misma información con su propia contraseña.

  Bajo ninguna circunstancia debes compartir tu contraseña con un desconocido. Existen muchas trampas con las cuales una persona puede intentar obtener tu contraseña simplemente comunicándose contigo por correo o por teléfono fingiendo ser alguna autoridad. Esta táctica se llama ingeniería social y consiste en la utilización de técnicas de índole psicológica, para lograr obtener información confidencial. No seas timado. Ninguna autoridad o administrador legítimo te pediría tu contraseña.
- **No escribas tu contraseña:** No escribas físicamente tu contraseña en ningún lado donde podría ser descubierto fácilmente por otras personas. Por lo general evita escribir contraseñas al menos que estés 100% seguro de que nadie más tendrá acceso a la copia escrita. Nunca mandes una contraseña a otra persona por correo electrónico al menos que esta comunicación sea cifrada.

## 2. Acceso físico

- **Evita compartir tu computadora o con desconocidos:** Si alguien más tiene acceso físico a la computadora donde trabajas o donde estarás trabajando hay muchas formas en los cuales pueden capturar tus contraseñas o copiar, borrar, o modificar los datos que tienes guardado en esta máquina o contagiar la maquina con un virus. Si tienes que compartir una computadora con otros usuarios conocidos asegura que cada persona tiene su propia cuenta en esa máquina y que también se preocupan por proteger su seguridad informática.
- **Evita utilizar los llamados "Cybercafe" o "Café Internet":** Nunca sabemos quienes más han estado trabajando en la máquina de un "Cibercafé" antes de nosotros o que tan confiables

sean los operadores del establecimiento. Si es absolutamente necesario que uses una computadora en un "Café Internet" procura encontrar un establecimiento donde los operadores te permitan arrancar la computadora con una versión portátil del sistema operativo GNU-Linux desde un CD (live cd) o memoria USB.

## 3. Comunicación por Internet

- **Las Redes Sociales:** Hoy en día servicios comerciales de redes sociales como **Facebook, Twitter, MySpace, Hi5, Google Buzz**, y otros están disfrutando de una enorme popularidad entre los usuarios de internet. Estos servicios están rápidamente desplazando la importancia que tuvieron otros medios de comunicación por internet como el correo electrónico y los mensajes instantáneos. Sin embargo estos servicios representan una amenaza para la seguridad y la libertad de sus usuarios por las siguientes razones:

  - Sus productos principales no son software libre
  - Obligan al usuario trabajar dentro un sistema propietario que no es compatible con otros sistemas
  - Revelan información personal que puede ser usada con fines maliciosos
  - Obligan al usuario ceder los derechos del uso de sus datos personales indefinidamente.
  - Capturan los datos personales de sus usuarios para ser procesados vía análisis estadístico y vendidos a terceros
  - Son los blancos de un nuevo brote de virus que infectan las cuentas de sus usuarios

## 4. Correo electrónico

- **Servidores de Correo Electrónico como Hotmail, Yahoo, Gmail, etc.:** La gratuidad, la multiplicidad de servicios agregados a una sola cuenta, contar con cada vez mayores capacidades de almacenamiento, la posibilidad de interactuar y colaborar con otr@s, son explicación de la popularidad de estos servicios, pero ¿cuáles son los costos?, ¿cuáles son sus contras?

Como contras del servicio de correos populares listamos algunos:

- Almacenan datos privados de sus usuarios: nombre y apellidos, CP, teléfono, otras cuentas de correo, fecha de nacimiento, entre otros.
- Todos los archivos que adjuntes podrá ser usados por la empresa que provee el servicio sin avisar al usuario y para cualquier fin incluso comercial.
- Analizan de forma permanente el contenido de los mensajes para fines comerciales pero también para entregar a entes gubernamentales cuando estos así lo soliciten.
- Almacena las IP's desde donde te conectas.

- **La privacidad en el uso del correo electrónico:** Normalmente se ha hecho énfasis en las medidas que l@s usuari@s pueden tomar para evitar que su contraseña sea robada (como cerrar la sesión al terminar, cambiar periódicamente la contraseña, elegir una respuesta a la pregunta secreta que no sea evidente, contar con un antivirus poderoso y actualizado que detecte programas maliciosos que registran contraseñas, etc.), todas estas medidas ubican los riesgos a la privacidad en nuestro entorno inmediato; sin embargo, es necesario considerar el riesgo de que nuestras comunicaciones sean filtradas, analizadas y leídas remotamente, más allá de dicho entorno, en el tránsito o almacenamiento de los mensajes entre nuestra máquina y la del (la) destinatari@.

# BIBLIOGRAFÍA Y REFERENCIAS ELECTRÓNICAS

## Bibliografía


[1] Harton, M. (2004). *Claves Hackers*. Ed. McGraw-Hill.

[2] Acissi. (2011). *Epsilon Seguridad Informática- Ethical Hacking - Conocer el Ataque para una Mejor Defensa*. Ed. ENI.

[3] Paraninfo. (2011). *Seguridad Informática* ED. 11. Ed. Paraninfo.

[4] Royer, J. M. (2004). *Seguridad en la Informática de Empresa: Riesgos, Amenazas, Prevención y Soluciones*. Ed. ENI.

[5] Aguado, D. P. (2012). *Seguridad Informática para el Hogar*. Ed. Bubok.

[6] Fisher, R. P. (1988). *Seguridad en los Sistemas Informáticos*. Ed. Díaz de Santos.

[7] Jesús Javier Ortega Triguero, M. Á. (2006). *Introducción a la Criptografía: Historia y Actualidad*. Ed. Univ. de Castilla La Mancha.

[8] Bertolín, J. A. (2008). *Seguridad de la Información: Redes, Informática y Sistema de Información*. Ed. Paraninfo.

[9] López, P. A. (2010). *Seguridad Informática: Ciclos Formativos*. Ed. Editex.

[10] Montero, M. S. (1995). *Administración de Sistemas Informáticos*. Ed. Ministerio de Educación.

[11] Aguilera López, P. (2010). *Seguridad Informática – Ciclos Formativos*. Ed. Editex.

[12] Pastor Franco J., M. Á. (2001). *Criptografía Digital: Fundamentos y Aplicaciones*. Ed. 2, Illustrated

[13] Fúster Sabater A., L. H. (2012). *Criptografía, Protección de Datos y Aplicaciones*. Ed. Alfaomega Grupo Editor.

## Referencias Electrónicas

(s.f.).

[1] Genbetadev. (s.f.). *¿Qué es y como surge la criptografía un repaso por su historia?* Recuperado el 19 de Noviembre de 2013, de http://www.genbetadev.com/seguridad-informatica/que-es-y-como-surge-la-criptografia-un-repaso-por-su-historia

[2] Hoy, I. (s.f.). *Criptografía. Seguridad Informática*. Recuperado el 16 de Noviembre de 2013, de http://www.informatica-hoy.com.ar/software-seguridad-virus-antivirus/Criptografia-Seguridad-informatica.php

[3] Informática, S. (s.f.). *Seguridad Informática - Criptología*. Recuperado el 16 de Noviembre de 2013, de http://www.segu-info.com.ar/criptologia/criptologia.htm

[4] *Introducción a la Seguridad Informática*. (Febrero de 2014). Recuperado el 10 de Febrero de 2014, de http://es.kioskea.net/contents/622-introduccion-a-la-seguridad-informatica

[5] Kioskea. (s.f.). *Introducción a la Seguridad Informática*. Recuperado el 14 de Enero de 2014, de http://es.kioskea.net/contents/622-introduccion-a-la-seguridad-informatica

[6] math.com. (s.f.). *Criptografía, Criptografia, Cryptography, Crypto, Cifrado*. Recuperado el 25 de Noviembre de 2013, de http://www.math.com.mx/criptografia.html

[7] Portillo, S. (s.f.). *Historia de la Seguridad Informática de Susana Portillo en Prezi*. Recuperado el 13 de Enero de 2014, de http://prezi.com/vnbaj88nuq0p/historia-de-la-seguridad-informatica/

[8] Red, S. e. (s.f.). *Seguridad en la Red - Criptografía*. Recuperado el 16 de Noviembre de 2013, de http://www.seguridadenlared.org/es/index25esp.html

[9] Spaces, W. (s.f.). *Seguridad Informática - Informe - Importancia de la Seguridad Informática*. Recuperado el 13 de Enero de 2014, de http://queen4.wikispaces.com/Informe+-+Importancia+de+la+seguridad+inform%C3%A1tica

[10] Spaces, W. (s.f.). *Seguridad Informática SMR - TEMA 7 - CRIPTOGRAFIA*. Recuperado el 16 de Noviembre de 2013, de http://seguridadinformaticasmr.wikispaces.com/TEMA+7+-+CRIPTOGRAFIA

[11] UNAM. (Miércoles 9 de Octubre de 2013). *Seguridad*. Recuperado el 9 de Octubre de 2013, de www.seguridad.unam.mx

[12] Virus, Z. (s.f.). *Acerca de la Criptografía*. Recuperado el 13 de Enero de 2014, de http://www.zonavirus.com/articulos/acerca-de-la-criptografia.asp

## GLOSARIO DE TÉRMINOS

| Término | Significado |
|---|---|
| AES | Norma avanzada de cifrado<br>(Advanced Encryption Standard) |
| ASCII | Código normalizado americano para el intercambio de información<br>(American Standard Code for Information Interchange) |
| CBC | Encadenamiento de bloques cifrados<br>(Cipher Block Chaining) |
| CFB | Realimentación del texto cifrado<br>(Cipher Feedback) |
| CGI | Interfaz de Entrada Común<br>(Common Gateway Interface) |
| CPU | Unidad de control de procesos<br>(Central Processing Unit) |
| DEA | Algoritmo de cifrado de datos<br>(Data Encryption Algorithm) |
| DES | Norma de cifrado de datos<br>(Data Encryption Standard) |
| DSA | Algoritmo de firma digital<br>(Digital Signature Algorithm) |
| DSS | Estándar de firma digital<br>(Digital Signature Standard) |
| ECB | Libro de Códigos Electrónicos<br>(Electronic Codebook) |
| EFF | Fundación de Fronteras Electrónicas<br>(Electronic Frontier Foundation) |
| FTP | Protocolo de Transferencia de Archivos<br>(File Transfer Protocol) |
| GNU | Sistema Operativo de UNIX |
| GNU GPL | Licencia Pública General de GNU<br>(GNU General Public License) |
| GSM | Sistema global para comunicaciones móviles<br>(Global System for Mobile Communications) |
| HIPO | Diagrama de Salida del Proceso de Entrada Jerárquica<br>(Hierarchy Input Process Output) |
| HTTP | Protocolo de Transferencia de Hipertexto<br>(Hypertext Transfer Protocol) |
| IDEA | Algoritmo de Cifrado de Datos Internacionales<br>(International Data Encryption Algorithm) |
| IP | Protocolo de Internet<br>(Internet Protocol) |
| ISO | Organización Internacional de Normativa<br>(International Organization for Standardization) |
| LAN | Red de Área Local |

| | |
|---|---|
| | (Local Area Network) |
| MAC | Código de autenticación de mensaje<br>(Authentication Message Code) |
| MIMD | Múltiples Instrucciones de Datos Múltiples<br>(Multiple Instruction Multiple Data) |
| MIT | Instituto Tecnológico de Massachusetts<br>(Massachusetts Institute of Technology) |
| NSA | Agencia de Seguridad Nacional<br>(National Security Agency) |
| OFB | Realimentación de la salida<br>(Output Feedback) |
| PC | Ordenador Personal<br>(Personal Computer) |
| PIN | Número de identificación personal<br>(Personal Identification Number) |
| POP3 | Protocolo de Oficina Postal<br>(Post Office Protocol) |
| RAM | Memoria de acceso aleatorio<br>(Random Access Memory) |
| ROM | Memoria de sólo lectura<br>(Read – Only Memory) |
| RSA | Sistema Criptográfico de Clave Pública de Rivest, Shamir y Adleman<br>(Rivest, Shamir & Adleman) |
| SDCL | Ciclo de Vida del Desarrollo de Sistemas<br>(Systems Development Life Cycle) |
| SI | Sistemas Informáticos<br>(Computer Systems) |
| SIMD | Única Instrucción de Datos Múltiples<br>(Single Instruction Multiple Data) |
| SISD | Única Instrucción de Datos Únicos<br>(Single Instruction Single Data) |
| SSH | Intérprete de Órdenes Seguras<br>(Secure SHell) |
| SSL | Capa de conexión segura<br>(Secure Sockets Layer) |
| TCP | Protocolo de Control de Transmisión<br>(Transmission Control Protocol) |
| TDEA | Triple DEA<br>(Triple Data Encryption Algorithm) |
| TELNET | Red de Telecomunicaciones<br>(TELecommunication NETwork) |
| UNIX | Acrónimo de UNICS<br>(Uniplexed Information and Computing Service) |
| XEX | O cifrar O<br>(XOR Encrypt XOR) |
| VoIP | Voz sobre Protocolo de Internet<br>(Voice over IP) |

| | |
|---|---|
| WLAN | Red de Área Local Inalámbrica<br>(Wireless Local Area Network) |
| XOR | «O» exclusiva, disyunción exlusiva<br>(eXclusive OR) |

# GLOSARIO

## >> Capítulo I: Antecedentes y Estado del Arte

- Infraestructura: f. Conjunto de elementos o servicios que se consideran necesarios para el funcionamiento de una organización o para el desarrollo de una actividad.

- Proliferar: intr. Multiplicarse abundantemente el número o la cantidad de alguna cosa.

- Hacker: (voz i.) com. INFORM. Persona muy aficionada y hábil en informática que entra ilegalmente en sistemas y redes ajenas.

- Malware: (Abreviatura de "Malicious Software") Término que engloba a todo tipo de programa o código informático malicioso cuya función es dañar un sistema o causar un mal funcionamiento.

- Criptología: Disciplina científica que se dedica al estudio de la escritura secreta, es decir, estudia los mensajes que, procesados de cierta manera, se convierten en difíciles o imposibles de leer por entidades no autorizadas.

- Embebida: intr. Encogerse, apretarse, como el tejido de lana cuando se moja.

- Mainframe: (Computadora Central) Computadora grande, potente y costosa usada principalmente por una gran compañía para el procesamiento de una gran cantidad de datos.

- Host: ("anfitrión", en español) Usado en informática para referirse a las computadoras conectadas a una red, que proveen y utilizan servicios de ella. Los usuarios deben utilizar anfitriones para tener acceso a la red.

- Plugin: (Complemento) Aplicación que se relaciona con otra para aportarle una función nueva y generalmente muy específica.

- Intrusión: f. Acción de introducirse sin derecho en una jurisdicción, cargo, propiedad, etc.

- Enrutadores: (Router) Dispositivo que proporciona conectividad a nivel de red o nivel tres en el modelo OSI.

- Superusuario: (root) En S.O del tipo Unix. Nombre convencional de la cuenta de usuario que posee todos los derechos en todos los modos (mono o multi usuario). Normalmente esta es la cuenta de administrador.

- Variopinto: adj. Que ofrece diversidad de colores o de aspecto. Multiforme, mezclado o diverso.

- Autentificación: tr. Autorización o legalización de una cosa.

**>> Capítulo II: La Criptografía**

- Red de Feistel: (Criptografía) Método de cifrado en bloque con una estructura particular. Debe su nombre al criptógrafo de IBM Horst Feistel. Las redes de Feistel presentan la ventaja de ser reversibles por lo que las operaciones de cifrado y descifrado son idénticas, requiriendo únicamente invertir el orden de las subclaves utilizadas.

- Permutación: (Matemáticas) Variación del orden o de la disposición de los elementos de un conjunto.

- Codificar: INFORM. Traducir la información al lenguaje del ordenador.

- Decodificar: tr. Descodificar: Aplicar inversamente a un mensaje o señal codificado las reglas de su código para obtener la forma primitiva del mensaje.

- Concatenación: f. Unión, enlace entre ideas o actos.

- Iteración: Acto de repetir un proceso con el objetivo de alcanzar una meta deseada, objetivo o resultado.

- Stream: Distribución de multimedia a través de una red de computadoras de manera que el usuario consume el producto, generalmente archivo de video o audio, en paralelo mientras se descarga.

- Sesgo: adj. Cortado o situado oblicuamente.

- Congruente: adj. Coherente, razonable, oportuno.

- Arbitrario: adj. [Persona] que actúa injusta o caprichosamente, y [cosa] que es resultado de esta actitud.

- Unicidad: f. Cualidad de único.

**>> Capítulo III: Criptoanálisis y los Sistemas Informáticos**

- Ofimática: Conjunto de técnicas, aplicaciones y herramientas informáticas que se utilizan en funciones de oficina para optimizar, automatizar y mejorar los procedimientos o tareas relacionadas.

- Intrínsecas: adj. Característico, esencial.

- Albergar: Encerrar, contener. Tener una determinada idea o sentimiento sobre algo.

- Método HIPO: (Diagrama HIPO) Indica cuales son las entradas a un proceso, después la elaboración de un proceso y también las salidas de un proceso.

- Informatización: f. Aplicación de sistemas y equipos informáticos al tratamiento de información.

- Híbrido: En general, que está formado por elementos de distinta naturaleza.

- Paralelismo: Correspondencia, semejanza.

**>> Conclusiones, Recomendaciones y Consejos Básicos**

- Quebrantar: tr. Romper, deteriorar algo. Violar una ley, no cumplir una obligación.

- Prudencial: adj. De la prudencia o relativo a ella. Que no es exagerado o excesivo.

- Paulatinamente: adj. Que procede o actúa despacio y de forma gradual.

- Azarosa: adj. Desgraciado, desafortunado, ajetreado.

- Índole: f. Carácter propio de cada uno. Naturaleza, calidad y condición de las cosas.