UNIVERSIDAD CATÓLICA DE SANTIAGO DEL ESTERO

Departamento Académico Rafaela

Trabajo práctico N° 3

Carrera: Ing. en Informática

Materia: Información y Comunicación

Profesor: Jorge Duarte - Gonzalo Pérez

Fecha: 30/06/2015

Alumnos: Wendy Sclerandi

Camila Kopech

Giorgina Castagno

Miguel Delpuppo

INDICE:

Algoritmos de encriptación

Seguridad de la información

La seguridad de la información es una medida de protección que permite la protección de la misma, con el fin de evitar su pérdida o modificación no autorizada. La motivación para llevarla a cabo es la importancia material e inmaterial que tiene la información ya sea para una institución o persona.

Las técnicas que se utilicen deberán garantizar la confidencialidad, integridad y disponibilidad de los datos, como así también otros aspectos secundarios (autenticidad, etc.).

Protección de los datos

Otro interés para personas e instituciones es resguardar los datos personales. Estos datos son sensibles y deben ser protegidos por ética y obligación jurídica.

Diferencia entre seguridad física y lógica

La seguridad física consiste en la aplicación de barreras físicas y procedimientos de control frente a amenazas al hardware. Un buen sistema informático debe prever desastres naturales, incendios accidentales y robos o sabotajes.

Por otra parte, la seguridad lógica se refiere a la aplicación de barreras y procedimientos que protejan el acceso a los datos y a la información. Esta incluye la restricción a programas y archivos, que la información transmitida llegue solo al destinatario y que se utilicen los datos correctos en cada procedimiento.

Gestión privada de redes, sistemas de información y convergencia, redes internacionales

En la actualidad predomina la propiedad y gestión privada de las redes. Todas las empresas e instituciones que trabajan con redes propias intentan protegerlas con mecanismos de seguridad. A partir de la red se puede ingresar a toda la información de la organización. Es por esto que se intenta resguardar la red para que personas con fines malignos no puedan acceder a la información.

Hoy en día, se forman redes internacionales porque todas las organizaciones trabajan con internet. Hay flujo de información entre distintos países, y si no se toman las medidas de seguridad adecuadas, estarán más propensas a ataques no deseados.

Conceptos básicos

Seguridad

Es un conjunto de métodos, herramientas o procedimientos para proteger la información de posibles amenazas en los casos donde hay debilidades en el sistema informático.

Bien

Es todo hardware y aquella información o dato que represente una importancia para quienes los utilicen.

Vulnerabilidad

Es una debilidad, o algún punto en el que el sistema informático es inseguro y puede ser atacado. No representan problemas fundados, sino que son advertencias a situaciones que podrían llegar a suceder.

Amenaza

Se refiere a todos los factores físicos y lógicos que pueden llegar a afectar al sistema informático.

Ataque

Es toda acción interna o externa realizada por personas que afecta directamente a un sistema. Es usual hoy en día, que existan hackers que realizan estos ataques. También se pueden diferenciar dos tipos de ataques: aquellos en los que se afecta al hardware y su funcionamiento, y los que tienen como finalidad la obtención de información ajena.

Importancia de la seguridad en telecomunicaciones

En la industria de las telecomunicaciones hay que proteger las redes y los datos, porque si la red es vulnerable, será más fácil acceder a los datos contenidos en la misma. Los ataques también pueden darse internos a la empresa, y en estos casos se debe restringir el acceso a los datos de cada empleado.

Gestión de seguridad

Un sistema informático es seguro solo si se cumplen al menos la disponibilidad, integridad y confidencialidad. Una vez conocidas estas características deberán tomarse las medidas oportunas. Es muy importante que la aplicación de estos conceptos se dé de manera continua.

Disponibilidad

El acceso a los datos debe ser garantizado en el momento necesario. Hay que evitar fallas del sistema y proveer el acceso adecuado a los datos.

Autenticidad

La legitimidad y credibilidad de una persona, servicio o elemento debe ser comprobable.

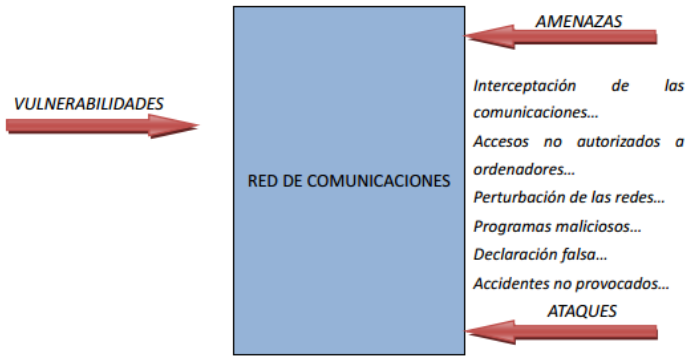
Integridad

Se debe garantizar que los datos estén completos, no modificados. Además se requiere saber quién realizó modificaciones y en qué momento.

Confidencialidad

Se refiere a que los datos solo pueden ser leídos y modificados por personas autorizadas, tanto en el acceso a datos almacenados como también durante la transferencia de ellos.

Análisis del gráfico: tipos de ataques y amenazas



Toda red de comunicaciones tiene vulnerabilidades, bajo estas circunstancias los niveles de amenazas aumentan proporcionalmente a los ataques. Si la organización sabe que tiene ciertos aspectos al descubierto deberá tomar medidas pertinentes para evitarlos.

En el gráfico se muestran los tipos de amenazas y ataques más comunes, éstos son:

Interceptación de las comunicaciones: es un ataque que se produce cuando un programa, proceso o persona accede a una parte del sistema para la cual no tiene autorización. Es el incidente de seguridad más difícil de detectar, ya que generalmente no produce una alteración en el sistema. Va directamente en contra del principio de confidencialidad.

Accesos no autorizados a ordenadores: es un ataque, producto de la explotación de una vulnerabilidad en el sistema del servidor o en alguna de sus aplicaciones o la utilización de algún otro método para subir privilegios como fuerza bruta, malware, sniffers o ingeniería social, entre otros.

Perturbación de las redes: representa una amenaza, ya que en grandes cantidades, las perturbaciones pueden generar problemas en la comunicación de una organización. Algunas de ellas son minimizables, como por ejemplo la atenuación, mientras que otras vienen dadas por el medio físico utilizado y deben conocerse para ser tenidas en cuenta.

Programas maliciosos: se refiere a todo software que contiene virus y spyware que se instalan en computadoras o dispositivos móviles sin consentimiento. Estos programas pueden colapsar el funcionamiento de la red y pueden utilizarse para monitorear y controlar las actividades que ésta realiza. Su propósito es robar información personal, enviar spam y cometer fraude. Se clasifica como ataque por su alto impacto negativo.

Accidentes no provocados: son una amenaza. En las organizaciones, no siempre se contempla que existen riesgos inevitables. Los riesgos más importantes son el fallo de algunos componentes de hardware y los desastres naturales. Es por esto, que siempre se deben tener planes de contingencia y respaldo de la información.

Dimensión de la seguridad

Control de acceso

El control de acceso consiste en la verificación de si una entidad que solicita acceso a un recurso tiene los derechos necesarios para hacerlo. Ofrece la posibilidad de acceder a recursos físicos (por ejemplo, a un edificio, a un local, a un país) o lógicos (por ejemplo, a un sistema operativo o a una aplicación informática específica).

Autenticación

Permite asegurar que un usuario de un sitio web u otro servicio similar es auténtico o quien dice ser. A menor tasa de fallo de la autenticación, mayor seguridad tendrá el sistema.

No repudio

Sirve a los emisores o a los receptores para negar un mensaje transmitido. Por lo que cuando un mensaje es enviado, el receptor puede probar que el mensaje fue enviado por el presunto emisor. De manera similar, cuando un mensaje es recibido, el remitente puede probar que el mensaje fue recibido por el presunto receptor.

Confidencialidad de los datos

Se refiere a que los datos solo pueden ser leídos y modificados por personas autorizadas, tanto en el acceso a datos almacenados como también durante la transferencia de ellos.

Seguridad de la comunicación

Es la disciplina que se encarga de prevenir que alguna entidad no autorizada que intercepte la comunicación pueda acceder de forma inteligible a la información. Incluye campos de estudios como la criptología, la emisión segura, la transmisión segura, la seguridad del flujo del tráfico y la seguridad física del equipo que se encarga de las comunicaciones.

Integridad de los datos

Se debe garantizar que los datos estén completos, no modificados. Además se requiere saber quién realizó modificaciones y en qué momento.

Disponibilidad

El acceso a los datos debe ser garantizado en el momento necesario. Hay que evitar fallas del sistema y proveer el acceso adecuado a los datos.

Privacidad

Es el derecho de mantener de forma reservada o confidencial los datos de la computadora y los que se intercambian en la red. Hoy en día se ve violada por spywares, cookies, piratas informáticos, virus, redes inseguras, etc.

Contingencia y respaldo de la información

Es un instrumento de gestión para el buen manejo de las Tecnologías de la Información y las Comunicaciones. Dicho plan contiene las medidas técnicas, humanas y organizativas necesarias para garantizar la continuidad de las operaciones de la institución. Surge de un análisis de riesgos, donde entre otras amenazas, se identifican aquellas que afectan a la continuidad de la operación de la institución. Su objetivo es doble: por un lado, tomar las medidas necesarias para minimizar la probabilidad de que dichos riesgos se conviertan en una realidad y, por otra parte, si esto ocurriera, posibilitará que el sistema pueda responder sin que ello suponga un grave impacto para su integridad.

Otra de las necesidades es respaldar la información en medios factibles y periódicamente para poder recuperarla en determinados casos.

Ejemplo concreto de un plan de respaldo

Analizamos el caso de una empresa petrolera llamada Petrodow.

Los back up se realizan en cintas magnéticas y cada una de ellas se rotula para saber qué datos contiene. La periodicidad de respaldo es de dos semanas, aunque algunas veces se realiza una vez por mes por restricciones de tiempo. Se hacen a media noche porque en esa hora hay uso mínimo de CPU y los archivos a respaldar no se están siendo utilizados.

Uno de los principales sistema de respaldo es NAS (Network Area Storage) en donde hay un servidor principal y las máquinas están conectadas a él por medio de la red (Internet), cada computador traspasa la información a respaldar al servidor y éste la envía a una máquina a la que se adjunta algún sistema de respaldo. El inconveniente es la saturación de la red si se transmitiera información de alta densidad.

El otro sistema de almacenamiento es SAN (Storage Area Network). En este sistema, al momento de almacenar la información, se realiza en una sola unidad, creando una red de máquinas (computadores) que se conecta con algún dispositivo de almacenamiento, compuesto por múltiples discos, al que se le adjunta un dispositivo de respaldo, ej: cintas magnéticas. Este sistema facilita la labor de respaldo puesto que los discos a respaldar se encuentran todos en un mismo lugar, haciendo más rápido y simple el proceso de back-up, sin congestionar la red.

Métodos de Encriptación

La encriptación es la única forma eficiente de transmitir información confidencial por Internet. El objetivo es garantizar la confidencialidad, integridad e irrefutabilidad de la información. Se deben desarrollar y aplicar mecanismos de encriptación que no puedan detectarse ni piratearse teóricamente.

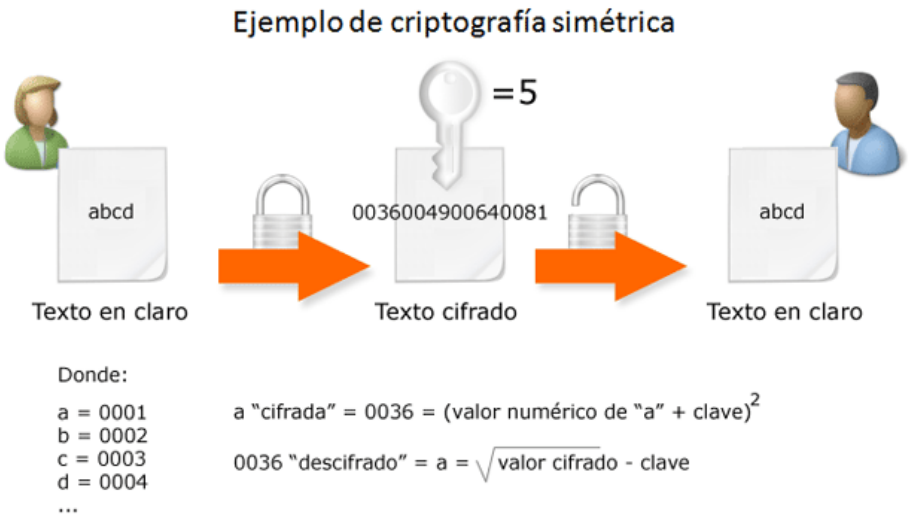
La operación de cifrado consiste en algoritmos matemáticos complejos en los que la clave es una cifra larga. La fuerza de la encriptación depende de la longitud de la clave, es decir, la cantidad de bits del número.

Firma digital

La firma digital es una herramienta tecnológica que permite garantizar la autoría e integridad de los documentos digitales, posibilitando que éstos gocen de una característica que únicamente era propia de los documentos en papel. La firma digital es un instrumento con características técnicas y normativas. Esto significa que existen procedimientos técnicos que permiten la creación y verificación de firmas digitales, y existen documentos normativos que respaldan el valor legal que dichas firmas poseen. Son únicas, infalsificables, verificables, innegables y viables.

Clave secreta (encriptación simétrica)

Es un método criptográfico en el cual se usa una misma clave para cifrar y descifrar mensajes. Las dos partes que se comunican han de ponerse de acuerdo de antemano sobre la clave a usar. Una vez que ambas partes tienen acceso a esta clave, el remitente cifra un mensaje usando la clave, lo envía al destinatario, y éste lo descifra con la misma clave.



Clave pública (encriptación asimétrica)

Es un método criptográfico que usa un par de claves para el envío de mensajes. Las dos claves pertenecen a la misma persona que ha enviado el mensaje. Una clave es pública y se puede entregar a cualquier persona, la otra clave es privada y el propietario debe guardarla de modo que nadie tenga acceso a ella. Además, los métodos criptográficos garantizan que esa pareja de claves sólo se puede generar una vez, es decir que no es posible que dos personas hayan obtenido casualmente la misma pareja de claves.

Ejemplo de cifrado de mensaje: ***Ana envía un mensaje a David***

1. Ana redacta un mensaje
2. Ana cifra el mensaje con la **clave pública** de David
3. Ana envía el mensaje cifrado a David a través de internet, ya sea por correo electrónico, mensajería instantánea o cualquier otro medio
4. David recibe el mensaje cifrado y lo descifra con su **clave privada**
5. David ya puede leer el mensaje original que le mandó Ana

SSL

Secure Sockets Layer es un protocolo diseñado para permitir que las aplicaciones transmitan información de manera segura. Las aplicaciones que utilizan el protocolo Secure Sockets Layer sí saben cómo dar y recibir claves de cifrado con otras aplicaciones, así como la manera de cifrar y descifrar los datos enviados entre los dos.

De forma básica, una conexión usando el protocolo SSL funciona de la siguiente forma: el cliente y el servidor entran en un proceso de negociación, conocido como ***handshake*** (apretón de manos). Este proceso sirve para que se establezcan varios parámetros para realizar la conexión de forma segura. Una vez terminada la negociación, la conexión segura es establecida. Usando llaves preestablecidas, se codifica y descodifica todo lo que sea enviado hasta que la conexión se cierre.

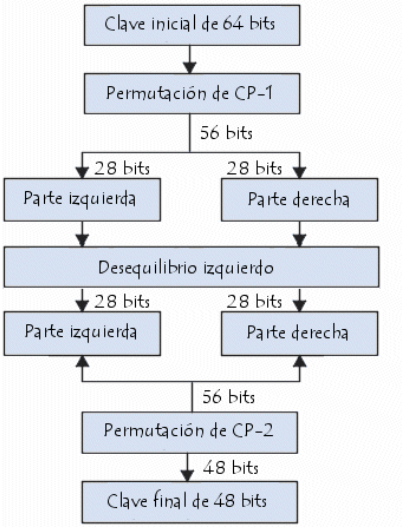
Usos

Algunas aplicaciones que están configuradas para ejecutarse SSL incluyen navegadores web como Internet Explorer y Firefox, los programas de correo como Outlook, Mozilla Thunderbird, Mail.app de Apple, y SFTP (Secure File Transfer Protocol) programas, etc Estos programas son capaces de recibir de forma automática SSL conexiones.

Cifrado DES

Se trata de un sistema de cifrado simétrico por bloques de 64 bits, de los que 8 bits (un byte) se utilizan como control de paridad (para la verificación de la integridad de la clave). Cada uno de los bits de la clave de paridad (1 cada 8 bits) se utiliza para controlar uno de los bytes de la clave por paridad impar, es decir, que cada uno de los bits de paridad se ajusta para que tenga un número impar de "1" dentro del byte al que pertenece. Por lo tanto, la clave tiene una longitud "útil" de 56 bits, es decir, realmente sólo se utilizan 56 bits en el algoritmo. Existen un total de 2^{56} combinaciones posibles de claves.

El algoritmo se encarga de realizar combinaciones, sustituciones y permutaciones entre el texto a cifrar y la clave, asegurándose al mismo tiempo de que las operaciones puedan realizarse en ambas direcciones (para el descifrado). La combinación entre sustituciones y permutaciones se llama cifrado del producto.



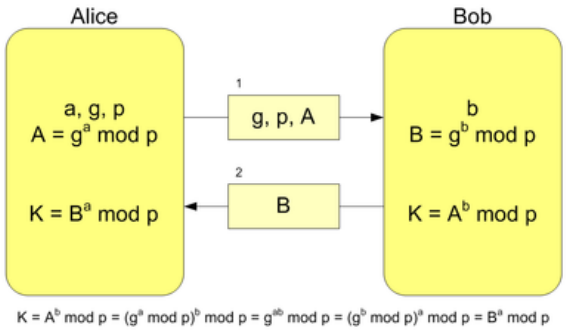
Cifrado Diffie-Hellman

Es un protocolo de establecimiento de claves entre partes que no han tenido contacto previo, utilizando un canal inseguro, y de manera anónima (no autentificada). Se emplea generalmente como medio para acordar claves simétricas de sesión.

El sistema se basa en la idea de que dos interlocutores pueden generar conjuntamente una clave compartida sin que un intruso que esté escuchando las comunicaciones pueda llegar a obtenerla.

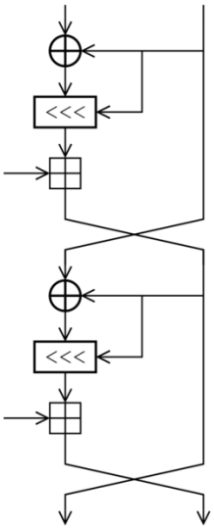
Para ello cada interlocutor elige un número público y un número secreto. Usando una fórmula matemática, que incluye la exponenciación, cada interlocutor hace una serie de operaciones con los dos números públicos y el secreto. A continuación, los interlocutores se intercambian los resultados de forma pública. Luego, ambos interlocutores utilizan por separado una fórmula

matemática que combina los dos números transformados con su número secreto y al final los dos llegan al mismo número resultado que será la clave compartida.



Cifrado RC5

Es un tipo de cifrado simétrico por bloques muy simple. RC5 tiene tamaño variable de bloques, de clave y de número de vueltas. Una característica importante de RC5 es el uso de rotaciones dependientes de los datos. También contiene algunas unidades de sumas modulares y de Puertas O-exclusivo (XOR). Las rutinas de cifrado y descifrado pueden ser especificadas en pocas líneas de código, pero la programación de claves es más complicada.



Cifrado RSA

Es un sistema criptográfico de clave asimétrica desarrollado en 1977. Es el primer y más utilizado algoritmo de este tipo y es válido tanto para cifrar como para firmar digitalmente.

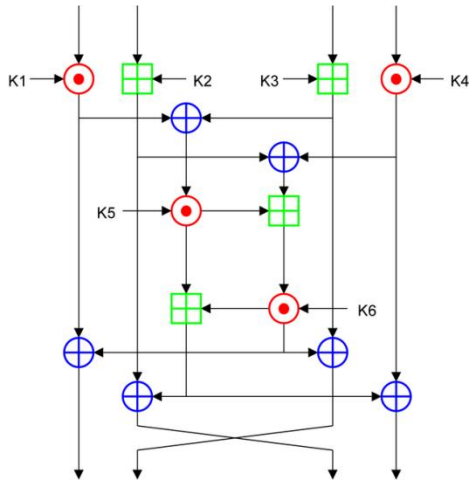
La seguridad de este algoritmo radica en el problema de la factorización de números enteros. Los mensajes enviados se representan mediante números, y el funcionamiento se basa en el producto, conocido, de dos números primos grandes elegidos al azar y mantenidos en secreto. Actualmente estos primos son del orden de 10^{200}.

Cifrado IDEA

Es un cifrador simétrico por bloques inventado en 1991. Fue un algoritmo propuesto como reemplazo del DES (Data Encryption Standard).

IDEA opera con bloques de 64 bits usando una clave de 128 bits y consiste de ocho transformaciones idénticas (cada una llamada un ronda) y una transformación de salida (llamada media ronda). El proceso para cifrar y descifrar es similar. Gran parte de la seguridad de IDEA deriva del intercalado de operaciones de distintos grupos:

- Adición ⊞ verde en la imagen.
- Multiplicación modular ⊙ rojo en la imagen
- O-exclusivo (XOR) ⊕ azul en la imagen.



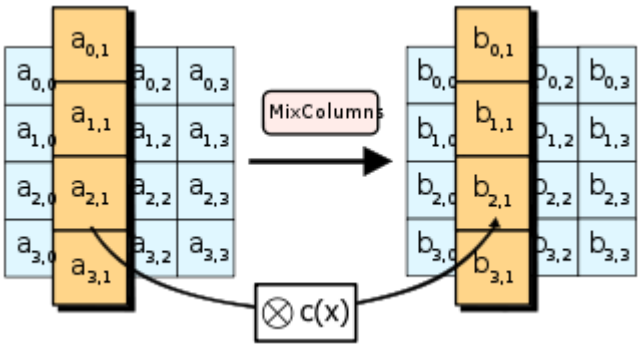
Cifrado 3DES

Cuando se descubrió que una clave de 56 bits no era suficiente para evitar un ataque de fuerza bruta, Triple DES fue elegido como forma de agrandar el largo de la clave sin necesidad de cambiar de algoritmo de cifrado. Este método de cifrado es inmune al ataque por encuentro a medio camino, doblando la longitud efectiva de la clave, pero en cambio es preciso triplicar el número de operaciones de cifrado, haciendo este método de cifrado muchísimo más seguro que el DES. Por tanto, la longitud de la clave usada será de 192 bits, pero su eficacia es de 112 bits.

Cifrado AES

AES es una criptografía de clave simétrica. Este algoritmo es el más conocido entre los usuarios de routers, ya que WPA opera con AES como método de cifrado. Este cifrado puede implementar tanto en sistemas hardware como en software. El sistema criptográfico AES opera con bloques y claves de longitudes variable, hay AES de 128bits, de 192 bits y de 256 bits.

El resultado intermedio del cifrado constituye una matriz de bytes de cuatro filas por cuatro columnas. A esta matriz se le vuelve a aplicar una serie de bucles de cifrado basado en operaciones matemáticas. A diferencia de la mayoría de los cifradores de bloques, AES tiene una descripción matemática muy ordenada.



AES-CBC (Cipher-block chaining)

A cada bloque de texto plano se le aplica la operación XOR con el bloque cifrado anterior antes de ser cifrado. De esta forma, cada bloque de texto cifrado depende de todo el texto en claro procesado hasta este punto. Como no se dispone de un texto cifrado con el que combinar el primer bloque, se usa un vector de inicialización IV (número aleatorio que puede ser públicamente conocido). La desventaja es que el cifrado es de forma secuencial y por tanto no puede ser paralelizado.

AES-OFB (Output feedback)

Se generan bloques de flujo de claves, que son operados con XOR y el texto en claro para obtener el texto cifrado. Al igual que con otras unidades de flujo de cifrado, al intercambiar un bit en el texto cifrado produce texto cifrado con un bit intercambiado en el texto plano en la misma ubicación. También se usa un vector de inicialización para el primer bloque.

AES-CFB (Cipher feedback)

Se hace igual que en OFB, pero para producir el keystream cifra el último bloque de cifrado, en lugar del último bloque del keystream como hace OFB. Un bit erróneo en el texto cifrado genera 1+64/m bloques de texto claro incorrectos (siendo m la longitud del flujo en el que se divide el bloque). El cifrado no puede ser paralelizado, sin embargo el descifrado sí.

Bibliografía:

Libro Comunicaciones y Redes de Comunicación de Stallings.

http://seguridaddatos.blogspot.com.ar/

http://e-ducativa.catedu.es/44700165/aula/archivos/repositorio//1000/1063/html/11_seguridad_fsica_y_seguridad_lgica.html

https://protejete.wordpress.com/glosario/

https://es.wikipedia.org/wiki/Control_de_acceso

https://es.wikipedia.org/wiki/Autenticaci%C3%B3n

http://redyseguridad.fi-p.unam.mx/proyectos/seguridad/ServNoRepudio.php

https://es.wikipedia.org/wiki/Criptograf%C3%ADa_sim%C3%A9trica

https://es.wikipedia.org/wiki/Criptograf%C3%ADa_asim%C3%A9trica

http://es.ccm.net/contents/130-introduccion-al-cifrado-mediante-des

https://es.wikipedia.org/wiki/Diffie-Hellman

http://es.slideshare.net/nenitapunker/metodo-de-encriptacion

http://www.firmadigital.gba.gov.ar/

http://aprenderinternet.about.com/od/ConceptosBasico/a/Que-Es-Ssl.htm

http://www.redeszone.net/2010/11/04/criptografia-algoritmos-de-cifrado-de-clave-simetrica/

http://redyseguridad.fi-p.unam.mx/proyectos/seguridad/AtaqItercepcion.php

http://www.alertaenlinea.gov/articulos/s0011-software-malicioso