Desarrollo de Software

8° Semestre

Programa de la unidad didáctica:

Seguridad de la informática

Unidad 2.

Mecanismos criptográficos en los sistemas informáticos

Clave:

15144844

Ciudad de México, febrero de 2025

Universidad Abierta y a Distancia de México

DCEIT

Índice

Unidad 2. Mecanismos criptográficos en los sistemas informáticos

Presentación de la Unidad

Bienvenido a la segunda unidad de la unidad didáctica *Seguridad de la informática*. En la unidad anterior conociste conceptos y técnicas para identificar las características de un código malicioso para identificar posibles riesgos en los sistemas de información mediante la aplicación de la tríada de la seguridad informática.

La *Unidad 2. Mecanismos criptográficos en los sistemas informáticos* tiene como objetivo exponer los elementos necesarios para que analices y utilices los fundamentos de la criptografía, así como algoritmos, cifradores, generadores, firma electrónica, entre otros mecanismos para lograr certificados digitales y mayor seguridad en los sistemas de información.

La criptografía se emplea desde la época de los romanos, cuando manejaban códigos para ocultar sus tácticas de guerra de aquellos que no querían que las supieran; con ello solo podían acceder a dichas tácticas aquellos que conocían el código. Pero, ¿Para qué sirve? ¿Cómo funciona? ¿Dónde se aplica la criptografía? Y haciendo un análisis más profundo: ¿realmente con el uso de la criptografía moderna se pueden garantizar las propiedades de integridad y confidencialidad, y con ello resolver casi en su totalidad el problema de la seguridad informática?

La criptografía es la ciencia que se encarga de estudiar las distintas técnicas empleadas para transformar (“encriptar” o “cifrar”) la información y hacerla irreconocible, de modo que sólo los legítimos propietarios puedan recuperar (“desencriptar” o “descifrar”) la información original. Proviene del griego *kriptos* (oculto) y *grafos*, escritura; según su etimología significa el “arte de escribir de un modo secreto o enigmático”. Asimismo, permite garantizar la confidencialidad, integridad y autenticidad de los mensajes y documentos guardados en un sistema o red informático. (Gómez, 2011, p. 361)

Esta unidad pretende ofrecer el panorama para utilizar mecanismos criptográficos, herramientas de vanguardia que permitan el establecimiento de medidas preventivas a los ataques y la pérdida de información, con el fin de que puedas comprender los algoritmos

criptográficos que garanticen la continuidad de operación y estabilidad de la infraestructura humana y tecnológica en una organización, enfocándose en satisfacer las necesidades reales de las empresas donde participarán o participan como futuros ingenieros en Desarrollo de software, ya que tendrán que enfrentarse a la elección de métodos, tomando cuenta las necesidades de la empresa u organización.

La Unidad ofrece una noción para resolver problemas de seguridad en sistemas y redes, tomando en cuenta la criptografía y todas las derivaciones que de ella emanen, siendo en la actualidad la criptografía un icono importante en la seguridad informática. Además, es necesario conocer las técnicas de seguridad de sistemas, ya que con ella combatimos a los famosos hackers y podremos mantener segura la información.

El conocer la criptografía permite entender los delitos informáticos para poder tomar decisiones acertadas al momento de determinar una seguridad, tomando en cuenta que el control de software puede, a su vez, cometer un ilícito si no se conoce la normatividad y leyes que delimitan y determinan la seguridad informática.

Se iniciará con el estudio de la criptografía, exponiendo algunas definiciones básicas. Posteriormente se analizarán los sistemas criptográficos, mencionando sus características más importantes. A continuación, se describirán los distintos tipos de algoritmos criptográficos y se concluirá con la explicación de algunas de las aplicaciones más importantes de la criptografía, mismas que se relacionan con el área de desarrollo de software.

Logros:

Al finalizar la unidad podrás:

- Analizar los algoritmos criptográficos de clave privada y los algoritmos criptográficos de clave pública.
- Identificar los estándares y protocolos de la seguridad en los sistemas de información.
- Aplicar los certificados y firmas digitales.
- Modelar la infraestructura de clave pública PKI.

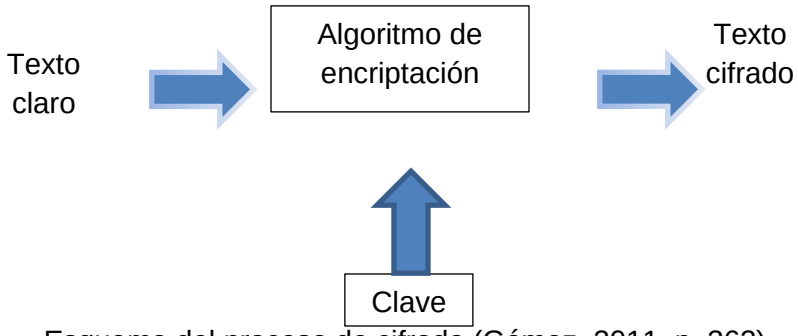
Competencia específica

- Desarrollar código criptográfico para implementar mecanismos de seguridad de acuerdo a las necesidades de la organización o del usuario en un sistema informático mediante estándares, protocolos de certificación y firmas digitales.

2.1. Criptografía

La criptografía, al igual que cualquier rama del conocimiento humano, tiene su propia nomenclatura. Se considera necesario conocer ésta para una mejor comprensión del tema en cuestión, sin embargo, una mera presentación de los términos puede ser no solo aburrida, sino contraproducente. Se optó por presentar en este apartado los diferentes métodos, su funcionamiento, y la nomenclatura utilizada en una forma gradual y lo más práctica posible en apego al campo de la criptografía clásica. Evidentemente no se incluyen todos los métodos conocidos, pero sí los más representativos. Una introducción más profunda y más matemática puede encontrarse en cualquier libro de los muchos que hay en el mercado dedicado al estudio de la criptografía y sus métodos, ya que como desarrollador de software es indispensable conocer métodos criptográficos para que cada software que se programe cumpla con los mínimos estándares de seguridad informática.

Para profundizar en el tema, es necesario que consultes, en la sección *Materiales para el desarrollo de la unidad 2*, el documento *U1*. *Introducción a la criptografía* de Gibrán Granados Paredes (2006), en el cual encontrarás los conceptos básicos de la seguridad, conceptos básicos de criptografía, su clasificación y la introducción a los certificados digitales.



Esquema del proceso de cifrado (Gómez, 2011, p. 362)

2.1.1. Clasificación de los algoritmos criptográficos

En el tema pasado se abordó la criptografía como concepto y función. Ahora es necesario analizar los principales algoritmos de la criptografía clásica, además de cómo se cifran y descifran mensajes y cómo ha evolucionado la criptografía a lo largo del tiempo.

Es importante dentro del desarrollo de software entender que la clasificación de los algoritmos criptográficos que actualmente se utilizan parten de la criptografía clásica, donde es de suma importancia analizar en primera instancia el cifrado simétrico (también conocido como cifrado de clave privada o cifrado de clave secreta), el cual consiste en utilizar la misma clave para el cifrado y el descifrado.

El cifrado consiste en aplicar una operación (un algoritmo) a los datos que se desea cifrar, utilizando la clave privada para hacerlos ininteligibles. El algoritmo más simple (como un OR exclusivo) puede lograr que un sistema sea prácticamente a prueba de falsificaciones (asumiendo que la seguridad absoluta no existe).

Sin embargo, en la década de 1940, Claude Shannon demostró que, para tener una seguridad completa, los sistemas de clave privada debían usar claves que tengan, como mínimo, la misma longitud del mensaje cifrado. Además, el cifrado simétrico requiere que se utilice un canal seguro para intercambiar la clave, y esto disminuye en gran medida la utilidad de este tipo de sistema de cifrado.

Para revisar los tipos de algoritmos criptográficos, revisa el documento de Granados (2006). *U2. Introducción a la criptografía* y de Vera y Palacios (2006) *U2. Introducción a la criptografía_Tipos de algoritmos* en la sección *Materiales para el desarrollo de la unidad 2*.

2.1.1.1. Algoritmos criptográficos de clave privada

Un cifrado de clave privada (o simétrico) se basa en un algoritmo, método y cifrado que usa una única clave para cifrar y descifrar los mensajes y criptogramas.

Dentro de los algoritmos criptográficos de clave privada se maneja un principio, el llamado principio de Kerkhoff, que textualmente dice: “todos los algoritmos de cifrados y

descifrados deben ser públicos y conocidos por todos, por tanto, lo único secreto es la clave del algoritmo", donde esta clave es la parte más importante del algoritmo.

Este principio es la base de todos los cifrados de clave privada, donde el objetivo principal es el mantener secreta la clave bajo cualquier medio, siendo ésta una gran herramienta de utilidad para que todo aquel usuario que quiera ver nuestra clave no tenga acceso, y donde esta clave se comparte en varios sectores.

La criptografía clave privada es más insegura, ya que el hecho de pasar la clave es una gran vulnerabilidad, pero se puede cifrar y descifrar en menor tiempo del que tarda la criptografía asimétrica, que es el principal inconveniente.

Una forma sencilla de cifrado de bloques es el modo Electronic Codebook (ECB). El modo ECB no se considera un modo seguro porque no utiliza un vector de inicialización para iniciar el primer bloque de texto simple. En relación con una clave secreta k determinada, "un cifrado de bloques simple que no utiliza un vector de inicialización codificará el mismo bloque de entrada de texto simple en el mismo bloque de salida de texto cifrado. Por tanto, si hay bloques duplicados dentro la secuencia de texto simple de entrada, habrá bloques duplicados en la secuencia de texto cifrado de salida. Estos bloques de salida duplicados podrían alertar a los usuarios sin autorización sobre la posibilidad de que se haya utilizado un cifrado débil en los algoritmos y los posibles modos de ataque. El modo de cifrado ECB es, por tanto, bastante vulnerable al análisis, y en última instancia, a la detección de claves." (MSDN, 2015b)

2.1.1.2. Algoritmos criptográficos de clave pública

La criptografía de clave pública es un sistema criptográfico que requiere dos llaves, una secreta y una pública, estando matemáticamente relacionadas. La clave pública puede ser publicada sin comprometer la seguridad, mientras que la clave privada no debe ser revelada a personas no autorizadas para leer los mensajes.

Es importante que investigues en la web sobre la criptografía de clave pública. ¿Cómo funciona? ¿Cómo la definen, cómo ha sido su desarrollo a través del tiempo? Por

ejemplo, en el sitio de Antonio Villalón (n.d.) o en el sitio de Aguillón y López (2012) de la Facultad de Ingeniería *Fundamentos de criptografía*.

El RSA, llamado así por las siglas de sus creadores, Rivest, Shamir y Adelman, es el algoritmo de clave pública más popular (Drakos y Moore, 2002). El algoritmo se puede utilizar para encriptar comunicaciones, firmas digitales e intercambio de claves. El método RSA es uno de los más usados hoy en día para la transmisión segura de datos a través de canales inseguros.
La clave puede ser de tamaño variable, generalmente se usan claves entre 512 y 2048 bits. Las claves más grandes aumentan la seguridad del algoritmo, pero disminuyen su eficiencia y generan más texto cifrado. Los bloques de texto en claro pueden ser de cualquier tamaño, siempre que sea menor que la longitud de la clave. Los bloques de texto cifrado generados son del tamaño de la clave.

El algoritmo es lento en la respuesta, ya que emplea operaciones matemáticas que tienen un coste elevado, y trabaja con claves de gran tamaño. Parte del problema está en la elección del exponente e, ya que un exponente de 512 bits, escogido aleatoriamente, precisa 768 multiplicaciones en promedio. Para solucionarlo se suelen escoger los valores 3 ó 65537, que precisan 3 y 17 multiplicaciones respectivamente. La elección de un exponente fijo no disminuye la seguridad del algoritmo si se emplean esquemas de criptografía de clave pública adecuados, como, por ejemplo, el relleno de mensajes con bits aleatorios.

Adicionalmente, el uso de exponentes fijos hace que la encriptación sea más rápida que la desencriptación, y la verificación más rápida que la firma. Esta última característica es incluso deseable, ya que un usuario firma una vez un mensaje, pero es posible que la firma se valide muchas veces. A continuación, se expone el ejemplo planteado en la obra Tales (1999):

> “El algoritmo de Diffie Hellman es un algoritmo de clave pública que permite el intercambio seguro de un secreto compartido. Generalmente se emplea junto con algoritmos de cifrado simétrico como método para acordar una clave secreta. El algoritmo no se puede usar para encriptar conversaciones o firmas digitales.

El funcionamiento del algoritmo es como sigue:

- El emisor escoge un número primo grande p y un generador g (g<p) y se los envía al destinatario. A continuación, escoge un número grande dA como clave privada y calcula la clave pública correspondiente eA = gdA modulo p.
- De modo similar, el destinatario escoge una clave privada dB y una clave privada eB = gdB modulo p.
- Ambos participantes intercambian sus claves públicas y calculan un secreto compartido. El del emisor será sA = eBdA = (gdB)dA = gdBdA modulo p. Y el del destinatario sB = eAdB = (gdA)dB= gdAdB= gdBdA modulo p.

Con este sistema, aunque un tercero interceptara los números p y g y las claves públicas eA y eB, no podría calcular el secreto compartido sin tener una de las claves privadas, lo que equivale a calcular el logaritmo discreto de una de las claves públicas, que es un problema intratable computacionalmente.

“El problema fundamental de este algoritmo es que es sensible a ataques activos del tipo hombre en el medio. Si la comunicación es interceptada por un tercero, éste se puede hacer pasar por el emisor cara al destinatario y viceversa, ya que no disponemos de ningún mecanismo para validar la identidad de los participantes en la comunicación. Así, el hombre en el medio podría acordar una clave con cada participante y retransmitir los datos entre ellos, escuchando la conversación en ambos sentidos.”

Comparado con los sistemas de cifrado simétrico como el DES, el algoritmo de RSA es 100 veces más lento en software y de 1,000 a 10,000 veces más lento en hardware.
“Para revisar un ejemplo de sistema DES se recomienda el artículo de Ángel (2001), donde presenta un estudio detallado del algoritmo de cifra con clave secreta DES, *Data Encryption Standard*, a través del seguimiento de un ejemplo práctico de cifrado y descifrado”. (Tales, 1999)
Revisa los conceptos de la criptografía, tipos y operación.

Domínguez, J. (2015). Seguridad Informática Personal y Corporativa (Primera parte). https://www.researchgate.net/publication/284733916_Seguridad_Informatica_Personal_y_Corporativa_Primera_parte

2.1.1.3. Aplicaciones de la criptografía

La criptografía es una disciplina con multitud de aplicaciones, muchas de las cuales están en uso hoy en día. Según Tales (1999), las más importantes son las siguientes:

- **Seguridad de las comunicaciones.** Es la principal aplicación de la criptografía a las redes de computadoras, así como los archivos dentro de una computadora o sistema, ya que permiten establecer canales seguros sobre redes que no lo son. Además, con la potencia de cálculo actual y empleando algoritmos de cifrado simétrico (que se intercambian usando algoritmos de clave pública) se consigue la privacidad sin perder velocidad en la transferencia.
- **Identificación y autentificación.** Gracias al uso de firmas digitales y otras técnicas criptográficas es posible identificar a un individuo o validar el acceso a un recurso en un entorno de red con más garantías que con los sistemas de usuario y clave tradicionales.
- **Certificación.** La certificación es un esquema mediante el cual agentes fiables (como una entidad certificadora) validan la identidad de agentes desconocidos (como usuarios reales). El sistema de certificación es la extensión lógica del uso de la criptografía para identificar y autentificar cuando se emplea a gran escala.
- **Comercio electrónico.** Gracias al empleo de canales seguros y a los mecanismos de identificación se posibilita el comercio electrónico, ya que tanto las empresas como los usuarios tienen garantías de que las operaciones no pueden ser espiadas, reduciéndose el riesgo de fraudes y robos.

Para profundizar en el tema, consulta el artículo *Introducción a la Criptografía: tipos de algoritmos* (Palacios y Vera, 2006), en el cual encontrarás la clasificación de algoritmos criptográficos.

Para que observes la aplicación práctica de la criptografía y de los algoritmos, revisa el artículo *Aplicaciones prácticas de la criptografía* (Palacios y Vera, 2006).

En el sitio de Microsoft MSDN (2015a) *Compatibilidad con certificados en las aplicaciones con .NET Framework 2.0*, podrás consultar sobre la forma de obtener un certificado

2.2. Certificados y firmas digitales

Los certificados es la electrónica que vincula unos datos de verificación de firma a un signatario y confirma su identidad. Los prestadores de servicios de certificación generalmente buscan vender el servicio; además, requieren que se firme un documento electrónico y utilizar realmente las claves de quién dicen ser, para lo cual, quien desarrolla el software genera previamente la clave pública y privada del firmante, y lo ha identificado. Por su parte, la firma electrónica es un conjunto de datos adjuntos o lógicamente asociado a un mensaje, documento electrónico o archivo digital, cuya finalidad es comprobar su integridad y permitir la identificación unívoca del autor.

La firma digital es una modalidad de la firma electrónica, desarrollada a partir de una infraestructura de clave pública (PKI) y privada; es decir, de la tecnología de criptografía asimétrica. En el mismo sentido, se habla de firma electrónica avanzada cuando la identificación es altamente fiable y permite detectar cualquier alteración del documento no autorizada, merced a que los dispositivos empleados en la creación de la firma son seguros, por cumplir determinadas exigencias técnicas, y porque el **prestador de servicios de certificación** que ha intervenido está acreditado como tal.

Un certificado es un documento electrónico que contiene un conjunto de información que permite identificar al usuario titular de una clave pública, es decir, la única persona que administra la clave privada que le corresponde a esta clave pública. En cambio, la firma digital como tal es un conjunto de 150 caracteres o más que permite identificar al autor del documento en el que consta.

Mediante la firma digital se garantizan aspectos en general, como los siguientes:

Autenticidad: que es la posibilidad técnica de establecer un nexo unívoco entre un documento, mensaje, archivo o firma electrónica y su autor.

No Repudio: ofrece protección a un usuario frente a que otro usuario niegue posteriormente que en realidad se realizó cierta comunicación. Esta protección se efectúa por medio de una colección de evidencias irrefutables que permitirán la resolución de

cualquier disputa. El no repudio de origen protege al receptor de que el emisor niegue haber enviado el mensaje, mientras que el no repudio de recepción protege al emisor de que el receptor niegue haber recibido el mensaje. Las firmas digitales constituyen el mecanismo más empleado para este fin.

Confidencialidad: se trata de la seguridad de que los datos que contiene el documento permanecen ocultos a los ojos de terceras personas durante su viaje por el medio desde A a B.

2.2.1. Infraestructuras de clave pública PKI

Para la mayoría de autores, la clave pública PKI es una combinación de programas, tecnologías de encripción, procesos, y servicios, que permite a las organizaciones asegurar las comunicaciones y las transacciones del negocio.

Es importante que investigues algunos ejemplos de gestión de la infraestructura de clave pública, por ejemplo DIGICERT.

Para abordar los temas sobre certificados de clave pública e infraestructura de clave privada, revisa el material de España Boquera (2003), en los Materiales de desarrollo de la unidad. Encontrarás en este documento también la explicación acerca de los tipos de autoridad de certificación y los elementos del formato de certificado.
Consulta esta fuente para que amplies los conocimientos de tipos de certificados, funcionamiento y aplicación.

Álvarez, G., Pérez, P. (2004). Seguridad Informática para Empresas y Particulares. Mc – Graw Hill. P.P. 150 - 161

2.2.2. Estándares y protocolos de certificación digital

Es importante recalcar que un certificado de clave pública dentro de una entidad es un punto de unión, con uno a más atributos de la identidad. Dicho certificado permite que corresponda la clave privada a una entidad que se identifica dentro de un programa. Los certificados de clave pública se denominan comúnmente Certificado Digital, ID Digital o simplemente certificado.

Los certificados digitales sólo son útiles si existe alguna Autoridad Certificadora (*Certification Authority* o CA) que los valide, tomando en cuenta que no hay garantías por certificarse uno mismo; siempre debe haber una certificación para validad nuestra información y darle credibilidad y viabilidad.

Una entidad certificadora dará validez y autentificará la identidad de una empresa o sujeto por medio de una firma de certificado digital y, a su vez, se permite que otro la valide por si no está certificada. Los certificados digitales proporcionan un mecanismo criptográfico para implementar la autentificación; también proporcionan un mecanismo seguro y escalable para distribuir claves públicas en comunidades grandes. Revisa la información sobre los certificados digitales y su funcionalidad en el documento de Tales (1999).

Algunos estándares de certificados y firmas digitales los puedes consultar en el sitio del *Gobierno de Argentina.*

Los protocolos de criptográficos se deberán consultar en el documento *U2. Protocolos criptográficos.* Que se localiza en los materiales de desarrollo de la unidad 2.

Para revisar cómo se realiza la configuración de aplicaciones para el reconocimiento de certificados digitales, puedes investigar documentos en internet por ejemplo el sitio de Tivoli Software.

Este tema se complementa muy bien con el siguiente sitio, donde se puede observar un ejemplo de cómo emplear un certificado digital y cuándo se requiere:

Configuración de aplicaciones para el reconocimiento de firmas digitales

Actualmente, además de desarrollar software para una empresa, se incrementa el uso de redes abiertas, en su caso, el internet, tomando en cuenta que permite estar relacionados y comunicados a nivel mundial, y lo mejor del caso, a un bajo costo.

Puesto que dicho desarrollo también permite la vulnerabilidad de los sistemas e información que se maneja, las firmas digitales intervienen a gran medida para hacer factibles dichos intercambios de información y garantizar la seguridad informática.

Para abordar este tema es recomendable que revises el documento del *Ministerio de Presidencia de España* que describe cómo validar, con la aplicación Adobe Reader o Adobe Acrobat, la firma de los documentos en formato PDF y BOE.

Para profundizar en el tema deberás leer las páginas 1 a 10 del ***Artículo Criptografía, certificado digital y firma digital Guía básica de supervivencia***, donde encontrarás un ejemplo de uso de certificados y firmas digitales.
También se debe abordar el Artículo *Infraestructura de clave pública (PKI) (INDRA)*, donde se explica detalladamente, por medio de un seminario, el manejo e infraestructura de la clave pública PKI.

Algunos estándares y protocolos criptográficos los puedes consultar en el sitio Protocolos Criptográficos y Estándares.

Es importante revisar el texto de Huguet, Rifà y Tena (2013) *Protocolos criptográficos* en los *Materiales de desarrollo de la unidad.*

Cierre de la Unidad

En la actualidad el manejo de redes de comunicación, en particular de internet, además de los medios de almacenamiento, ha abierto nuevas posibilidades para el intercambio de información. Al mismo tiempo, son cada vez mayores las amenazas a la seguridad de la información que se transmite. Es necesario, entonces, crear diferentes mecanismos, dirigidos a garantizar la confidencialidad y autenticidad de los documentos electrónicos; todo ello es parte de una nueva tecnología denominada Criptografía.

Los algoritmos criptográficos tienden a degradarse con el tiempo. A medida que transcurre el tiempo, los algoritmos criptográficos se hacen más fáciles de quebrar (que sería la ruptura de algún código, o violación de una firma o certificado digital) debido al avance de la velocidad y potencia de los equipos de computación.

Todos los algoritmos criptográficos son vulnerables a los ataques de fuerza bruta –tratar sistemáticamente con cada posible clave de encripción, buscando colisiones para funciones hash, factorizando grandes números, etc. –; la fuerza bruta es más fácil de aplicar en la medida que pasa el tiempo.

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

Debido a las cambiantes condiciones y nuevas plataformas de computación disponibles, es vital el desarrollo de documentos y directrices que orienten a los usuarios en el uso adecuado de las tecnologías para aprovechar mejor sus ventajas.

El auge de la interconexión entre redes abre nuevos horizontes para la navegación por internet, y con ello, surgen nuevas amenazas para los sistemas computarizados, como son la pérdida de confidencialidad y autenticidad de los documentos electrónicos.

La criptografía es una disciplina/tecnología orientada a la solución de los problemas relacionados con la autenticidad y la confidencialidad, que provee las herramientas idóneas para ello. Los usuarios son quienes deben elegir la conveniencia de una u otra herramienta para la protección de sus documentos electrónicos.

Para saber más

Para tener mayores conocimientos sobre la unidad se recomienda consultar:

- José Ramón Soler Fuensanta, *Una introducción a la Criptografía Clásica.*

http://www.criptohistoria.es/files/cifras.pdf , que permite entender el cifrado de información, métodos de sustitución monoalfabética, así como los métodos de sustitución poligráfica y ejemplos de ambos, además de ejemplos de los métodos de transposición.

En los siguientes materiales encontrarás artículos e información diversa sobre criptología:

- Ángel Ángel, J.J. (enero de 2001). DES Data Encryption Standard. SeguriDATA (México). Criptored. https://usuaris.tinet.cat/acl/html_web/seguridad/cripto_p/cripto_princ_2.html
- Gabinete de Tele-Educación de la Universidad Politécnica de Madrid. *UPM (24 de noviembre de 2010). Seminario de introducción a la Computación y Criptografía Cuántica 1 [Archivo de Vídeo]. YouTube.* https://youtu.be/3zsg3DGfWFg
- Gabinete de Tele-Educación de la Universidad Politécnica de Madrid. *UPM (24 de noviembre de 2010). Seminario de introducción a la Computación y Criptografía Cuántica 2 [Archivo de Vídeo]. YouTube.* https://www.youtube.com/watch?v=sW11m1JzXDs
- William Quimis *(15 de junio de 2014).* Uso de certificados y firmas digitales *[Archivo de Vídeo]. YouTube. https://www.youtube.com/watch?v=SRVQCrMH7E0*
- https://s2grupo.es/es/inicio/

Fuentes de consulta

Básica

- Aguillón Martínez, E., y López Barrientos, J. (2012). Fundamentos de criptografía. México: Facultad de ingeniería UNAM. https://repositorio.unam.mx/contenidos/sistema-tutorial-de-fundamentos-de-criptografia-124513?c=plMWJ9&d=false&q=*:*&i=1&v=1&t=search_0&as=0
- Ángel Ángel, J.J. (2010). *Criptografía para principiantes*. http://spi1.nisu.org/recop/www.seguridata.com/pdf/cbasica.pdf
- Ángel Ángel, J.J. (enero de 2001). *DES Data Encryption Standard. SeguriDATA (México).* Criptored. https://usuaris.tinet.cat/acl/html_web/seguridad/cripto_p/cripto_princ_2.html
- Drakos N., y Moore, R. (2002). *Criptosistema de clave secreta*. Sidney-Leeds: University of Leeds–Mcquarie University.
- España Boquera, M.C. (2003). *Servicios avanzados de telecomunicación*. Madrid: Díaz de Santos. pp. 67-69, 72-76, 79-82.
- Gómez, V. A. (2011). *Enciclopedia de la seguridad informática*. 2ª Edición. México: Alfaomega-Ra-Ma.
- Granados Paredes, G. (2006). Introducción a la criptografía. En *Revista Digital Universitaria*. *México:* DGSCA, UNAM.10 de julio 2006, Vol.7 No. 7. http://www.revista.unam.mx/vol.7/num7/art55/art55-3.htm
- Huguet Rotger, L., Rifà Coma, J., y Tena Ayuso, J.G. (2013). Protocolos criptográficos. https://www.exabyteinformatica.com/uoc/Informatica/Criptografia_avanzada/Criptografia_avanzada_(Modulo_3).pdf
- Mendivil I. *El ABC de los documentos electrónicos seguros*. https://fdocuments.mx/document/el-abc-de-los-documentos-electronicos-seguros-conceda-a-los-documentos-firmados.html?page=3
- MSDN Microsoft Developer Network (2015a). *Compatibilidad con certificados en las aplicaciones con .NET Framework 2.0*. https://msdn.microsoft.com/es-es/magazine/cc163454.aspx#S3
- MSDN Microsoft Developer Network (2015b). *Servicios criptográficos*. https://msdn.microsoft.com/es-es/library/92f9ye3s%28v=vs.110%29.aspx

- Palacios, R. y Delgado, V. (Marzo/Abril 2006). Aplicaciones prácticas de la criptografía. *Revistas anales mecánica y electricidad*. Sevilla: Escuela Técnica Superior de Ingeniería (ICAI). pp. 10-16. https://www.researchgate.net/publication/28109789_Aplicaciones_practicas_de_la_criptografia
- Palacios, R. y Delgado, V. (enero-febrero, 2006). *Introducción a la criptografía. Tipos de algoritmos.* En *Revista anales mecánica y electricidad*. Sevilla: Escuela Técnica Superior de Ingeniería (ICAI) (2006, pp. 42-46) https://www.researchgate.net/publication/28106424_Introduccion_a_la_Criptografia_tipos_de_algoritmos
- Rodríguez, A. L. O. (2000). *Elementos de arquitectura y seguridad informática*. La Habana: Instituto Superior Politécnico Eduardo García Delgado.
- Segu Info (2013). Protocolos Criptográficos y Estándares. *En Criptografía de la A-Z*.
- Tales Oliag, S. (1999). *Algoritmos de clave pública RSA*. Valencia: Instituto Tecnológico de Valencia.
- Varela Velasco, R. Criptografía, una necesidad moderna. En *Revista Digital Universitaria*. 10 de julio 2006, Vol. 7 No. 7. http://www.revista.unam.mx/vol.7/num7/art56/jul_art56.pdf
- Villalón Huerta, A. (n.d.). Página personal. http://www.shutdown.es/
- Villalón Huerta, A. (julio, 2002). *Seguridad en Unix y Redes Versión 2.1.* Valencia: n.d. https://www.rediris.es/cert/doc/unixsec/unixsec.pdf