Criptografía: conceptos básicos

Seguridad Informática

UNIVERSIDAD SIGLO 21 | MIEMBRO DE LA RED ILUMNO

Introducción

La lectura del presente material es meramente complementaria a la bibliografía básica. Definiciones teóricas de los conceptos aquí expuestos deben ser tomadas de dicha bibliografía.

A través de los siglos, se han creado cientos de protocolos y mecanismos para hacer frente a problemas de seguridad cuando la información es almacenada y transmitida a través de documentos físicos. Por ejemplo, la privacidad en correspondencias es provista por sobres sellados y enviados a través de servicios postales válidos u oficialmente habilitados.

Complementariamente a estos protocolos y mecanismos, se definieron marcos legales para resolver aquellos aspectos que pudiesen ser vulnerados. Un ejemplo es la seguridad física de una correspondencia que puede ser vulnerada. Si esto ocurre, se comete un acto ilícito (violación de privacidad) tipificado en la mayoría de los códigos penales de los países.

Mientras que la información ha sido históricamente almacenada y transmitida en papel, en la actualidad, gran parte de ella reside en soportes magnéticos y se transmite a través de sistemas de telecomunicaciones.

Un cambio radical que surge con esto es la posibilidad de copiar y alterar la información. Se puede hacer cientos de copias idénticas de una pieza de información almacenada electrónicamente y cada una es indistinguible de la original.

Se requiere entonces de nuevos esquemas para garantizar el cumplimiento de los servicios de seguridad de la información cuando esta es tratada de forma digital, servicios que se presentan en la siguiente tabla.

Tabla 1: Servicios de seguridad de la información

- **Confidencialidad**
  - De datos almacenados en un dispositivo.
  - De datos transmitidos.
  - De datos procesados.
- **Autenticación**
  - De Entidad (Usuario, dispositivo).
  - Del origen de los datos.
- **Integridad**
- **Protección a la réplica**
- **Reclamo de origen**
- **Reclamo de propiedad**
- **Referencia temporal**
- **No Repudio**
  - De origen.
  - De destino.
- **Confirmación de la prestación de un servicio**
- **Autorización**
  - Control de acceso a equipos y servicios.
- **Auditabilidad o Trazabilidad**
- **Disponibilidad del servicio**
- **Anonimato en el uso de servicios**
- **Certificación mediante Terceros de Confianza**

Fuente: adaptado de Gómez Vieites, 2014, p. 46.

Dotar de seguridad a la información de una sociedad electrónica requiere una amplia gama de habilidades técnicas y legales.

La técnica o medios técnicos **son provistos por la criptografía**.

Criptografía. Conceptos básicos

La criptografía ha sido empleada por el hombre desde la antiguedad. Desde los jeroglíficos egipcios, pasando por el cifrado César utilizado por el ejército romano para comunicarse, hasta los tiempos modernos, la necesidad de proteger información sensible ha estado presente y ha sido soportada por técnicas de cifrado.

Las técnicas primitivas o precientíficas, conocidas como criptografía simétrica, se basaron inicialmente en sustitución de los símbolos del alfabeto (desplazamientos), teniendo como clave la cantidad de símbolos del alfabeto desplazados.

Para recuperar el texto oculto, bastaba con aplicar el desplazamiento de forma inversa, aunque para ello se debía conocer la clave.

Esta necesidad de conocer la clave en ambos extremos de la comunicación es una característica conocida también como **secreto compartido**, secreto que debe ser comunicado entre las partes a través de canales seguros.

Con el tiempo, a las técnicas de sustitución se adicionaron otras técnicas, como la de transposición columnar (Vigenére), utilización de más de un alfabeto para el reemplazo de símbolos (polialfabéticos), las que, como se verá mas adelante en esta lectura, si bien dotaron de mayor complejidad y robustez a los métodos de cifrado, mantenían su punto débil en la necesidad de comunicar la clave de forma segura, pues si esta era revelada por terceros, derribaba toda la seguridad de la comunicación.

Ya en el siglo XX, en el año 1949, Claude Shannon[1] sienta las bases de la criptografía moderna, con la publicación de "Communication Theory of Secrecy Systems"[2], en la cual dota a la criptografía de un marco científico basado en principios matemáticos. Se habla entonces, a partir de este hito, de critpografía científica.
Un aporte de relevancia similar es el que realizan Diffie y Hellman[3], quienes en el año 1976, en su publicación "New directions in Cryptography"[4],

[1] Para más información sobre Claude Elwood Shanon, consulta en https://goo.gl/BAZxvh
[2] Shannon, C. E. (1949). Communication Theory of Secrecy Systems. *Bell System Thecnical Journal*, *28*(4), pp. 656-715.
[3] Para más información sobre Diffie & Hellman, puedes consultar: https://goo.gl/tU18oJ

definen el método de criptografía de clave pública, conocido también como criptografía asimétrica, haciendo posible la transmisión de las claves criptográficas a través de canales de comunicación inseguros, basándose para ello en los principios matemáticos expuestos anteriormente por Claude Shannon.

Figura 1: Reseña histórica de la criptografía

Fuente: Elaboración propia.

Referencias

- 4000 a. C. Jeroglíficos egipcios
- 500 a. C. Escítala espartana. Trasposición monoalfabética.
- 60 a. C. Cifrado César. Trasposición monoalfabética.
- 1883 August Kerckhoff. Teoría de algoritmos públicos y fortaleza basada en clave.
- 1940 La bomba de Turing utilizada para descifrar el algoritmo Lorenz implementado en Enigma.
- 1949 Claude Shannon: *Communication theory of secrecy systems*. Sienta las bases de la criptografía moderna o científica.
- 1976 Diffie & Hellman: *New directions in cryptography*. Criptografía asimétrica.
- 1976 DES (*Data Encription Standar*) adoptado como estándar EE. UU.
- 1984 Primeros desarrollos sobre criptografía cuántica.
- 1997 AES (*Advanced Encryption Standar*). Nuevo estándar EE. UU.

[4] Whitfield Diffie & Martin Hellman, 1976, New Directions in criptography. IEEE Transactions on Information Theory. Vol. IT-72. Nro 6. Pág. 644-654.

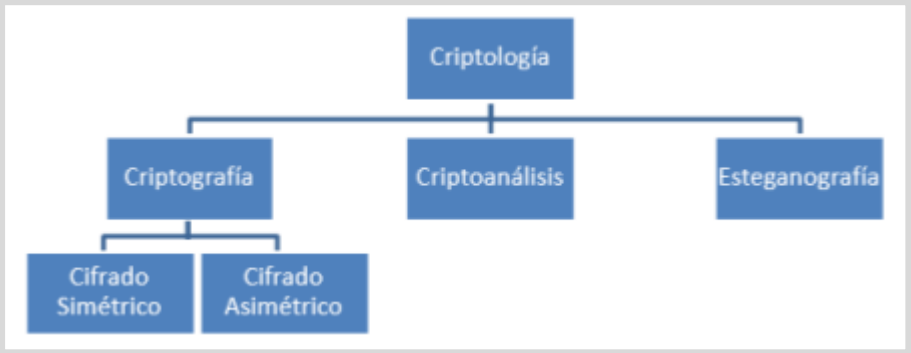
Criptología

La criptología es la ciencia que enmarca el estudio de las distintas técnicas que permiten ocultar información para transmitirla de forma segura. Entre estas técnicas se encuentran la **criptografía**, el **criptoanálisis** y la **esteganografía**.

Mientras que la rama de la criptografía se ocupa de estudiar los métodos criptográficos, el criptoanálisis, por su parte, estudia las formas posibles de vulnerar dichos métodos. Su rol es fundamental dentro de la criptología, dado que hace posible mejorar los métodos criptográficos con cada nuevo hallazgo.

Este enfoque debe sus inicios al criptógrafo holandés Auguste Kerckhoffs[5], quien en el año 1870 da a conocer una serie de principios deseables de un sistema criptográfico, conocidos como teoría de los algoritmos públicos. Entre estos principios, define que para que un algortimo sea seguro su fortaleza no debe estar basada en el desconocimiento de su diseño, mas bien este debe ser de dominio público, dando lugar a que sea expuesto a pruebas y mejorado a través de ellas. Su única fortaleza debe residir en la clave utilizada.

Figura 2: Ramas de la criptología



Fuente: elaboración propia.

Criptosistema

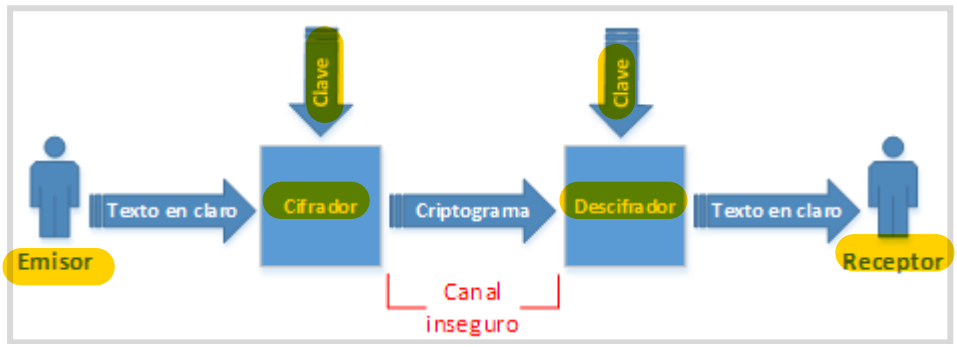
Criptosistema es un término general utilizado para referir al conjunto de técnicas utilizadas para proveer servicios de seguridad de la información.

[5] Sobre August Kerckhoffs puedes consultar en https://es.wikipedia.org/wiki/Auguste_Kerckhoffs

En el proceso que se representa en la siguiente figura, el emisor envía un mensaje en texto en claro que se somete a un proceso de cifrado, dicho proceso recibe como entrada una clave K, generando como salida un criptograma con el mensaje alterado (en forma de texto o bits) para atravesar el canal inseguro, como puede ser Internet.

En el otro extremo, el criptograma se somete a un proceso de descifrado, que recibe como entrada la misma clave K y genera como salida el texto en claro enviado por el emisor.

Figura 3: Criptosistema



Fuente: elaboración propia.

Algoritmos criptográficos

A continuación, se resumen las principales técnicas que implementan los algoritmos critpográficos.

- **Sustitución**: los símbolos se cambian conforme a reglas precisas que varían de un método a otro.
  - Monoalfabeto: sustitución biunívoca de las letras del alfabeto de mensajes en claro por las letras del alfabeto de mensajes cifrados.
  - Polialfabeto: consiste en el uso de varias sustituciones simples.
- **Permutación o transposición**: los símbolos no cambian su significado, sino que alteran sus posiciones según patrones que difieren de un método a otro.
  - Columnar: reordenan los símbolos del texto en claro sin alterar su significado.
  - Variaciones: columnar con clave, doble transposición columnar.
- **Transformaciones lógicas**: actualmente se parte de información almacenada en forma de cadena de bits. Los métodos criptográficos

hacen frecuentemente uso de las operaciones lógicas booleanas, con utilización mayoritaria de la función o-exclusivo (XOR).

- **Cifrado en bloque:** antes de emitirse el mensaje se divide en bloques y se cifra cada uno de estos por separado, utilizando la misma clave. Variantes posibles son cifrado de producto y exponencial.
- **Cifrado en flujo:** se emite el mensaje y se cifra a la vez, sin dividirlo en partes.

Fundamento de la clave criptográfica

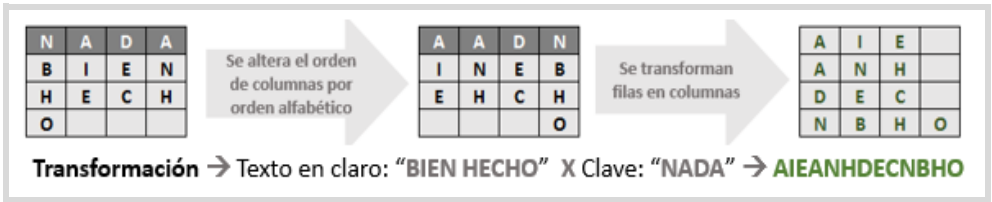
El desafío inmediato al cual se enfrenta un método criptográfico, sea éste de sustitución o de permutación, es recordar el orden establecido para obtener el criptograma, esto se vuelve todavía más crítico cuanto más compleja haya sido la secuencia aplicada (Huidobro Moya, 2012).

Una posible solución puede ser escribirla en un soporte cualquiera (ejemplo, papel), aunque se debería afrontar un nuevo problema, dado que si este soporte cae en manos no autorizadas, lanzaría por la borda el mecanismo de ocultación (Huidobro Moya, 2012).

Otra solución mas eficiente es implementar un mecanismo de sustitución o de transposición basado en una palabra o serie de caracteres fácil de memorizar. Por ejemplo, se puede definir un mecanismo criptográfico basado en una palabra corta (Huidobro Moya, 2012).

Supóngase que se pretente cifrar la frase *bien hecho* basándose en la palabra NADA. Para ello se escribe una tabla o matriz con tantas columnas como letras tenga la palabra elegida, y se coloca en la fila superior dicha palabra. El mensaje a cifrar se va situando en las filas siguientes consecutivamente y si sobran celdas, estas se mantienen vacías (Huidobro Moya, 2012).

Figura 4: Método de transposición columnar



Fuente: Elaboración propia.

Para obtener el texto en claro, esto es, descifrar el criptograma, se deberán realizar las operaciones aplicadas de forma inversa. La utilización de una palabra o serie de caracteres como base de un algoritmo de cifrado tiene

ciertas ventajas. Por un lado, si el método es complejo, solo quien conozca la palabrá podrá obtener el texto en claro de forma fácil; por otro lado, recordar una palabra resulta claramente mas fácil que recordar todo un método complejo (Huidobro Moya, 2012).

La palabra o serie de caracteres, utilizada como base de un mecanismo de cifrado se denomina **clave de cifrado**, y la cantidad de caracteres que la conforman se denomina **longitud de la clave** (Huidobro Moya, 2012).

"El secreto perfecto se alcanza mediante un cifrado en el que la clave que se utilice para cifrar debe ser de igual o mayor longitud que el mensaje y además, dicha clave, debe ser generada de forma aleatoria" (Shannon, 1949, p. 659).

En el fondo, los algortimos criptográficos han estado presente y en constante evolución a través del tiempo, como método para proveer servicios de seguridad de la información.

Esta evolución se debe gracias a la dialéctica permanente entre el criptoanálisis y la criptografía, entre ruptura de los algoritmos y su otpimización, principalmente a partir de los principios propuestos por August Kerckhoffs, entre los cuales establece que la seguridad de un sistema criptográfico no debe residir en la ocultación del algoritmo, sino que este debe ser de conocimiento público y sometido a análisis científico para detectar sus vulnerabilidades y mejorado en función de los hallazgos. Se trata de un enfoque contrapuesto a los criterios tradicionales, donde tanto el diseño de los algoritmos como sus claves eran parte del secreto.

La criptología como ciencia reúne y dota de un marco científico a las técnicas de protección de la información. El criptoanálisis, si bien se enfoca en lo contrario, sirve como método de validación tanto para la criptografía como para la esteganografía, con lo cual es acertado abordarlo como rama criptológica.

Por último, la seguridad de los algoritmos criptográficos, como se planteó, depende de la seguridad del canal por el que se transmite la clave, aunque es importante también la seguridad del almacenamiento de dicha clave.

Otro factor determinante es la capacidad computacional. Un algoritmo será computacionalmente seguro mientras no exista una capacidad de computo necesaria para criptoanalizarlo de forma existosa, en un lapso de tiempo durante el cual la información revista un carácter sensible.

Referencias

Gómez Vieites, A. (2011). *Enciclopedia de la Seguridad Informática.* (2° Ed.) Madrid: Ra-Ma.

Diffie, W., Hellman, M. (1976). *New directions in Cryptography. IEEE: Transactions on Information Theory* (Traducción propia) Vol. 22., p. 644-654. Recuperado de: https://www-ee.stanford.edu/~hellman/publications/24.pdf

Shannon, C. (1949). *Communication Theory of Secrecy Systems*. Bell System: Thechnical Journal vol. 28, p. 656-715. Recuperado de: http://netlab.cs.ucla.edu/wiki/files/shannon1949.pdf

Huidobro Moya, J, (2012). Protección de la información y gestión de claves. En *Manual formativo de ACTA*, Nº. 63, págs. 59-66. Recuperado de: https://www.acta.es/medios/articulos/comunicacion_e_informacion/063059.pdf

Cifrado.
Clave privada,
Clave pública.

Seguridad Informática

UNIVERSIDAD SIGLO 21 | MIEMBRO DE LA RED ILUMNO

Cifrado

La lectura del presente material es meramente complementaria a la Bibliografía Básica. Definiciones teóricas de los conceptos aquí expuestos deben ser tomadas de dicha Bibliografía.

Cifrado de clave privada

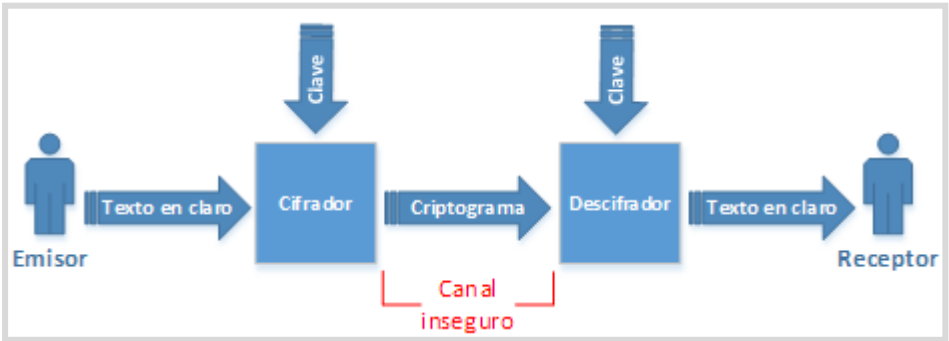
Los algoritmos criptográficos de clave privada, también denominados criptosistemas simétricos o cifrado simétrico, son los más empleados en la Criptografía.

Estos algoritmos, en los que la clave de cifrado y descifrado son la misma, o de una es posible obtener la otra, tienen la desventaja de necesitar un canal seguro para que los extremos de la comunicación puedan intercambiar la clave de cifrado, pero a la vez, se trata de algoritmos generalmente más veloces que los asimétricos y permiten alcanzar niveles de seguridad elevados, utilizando claves de cifrado de longitudes menores que éstos.

Un criptosistema que utiliza cifrado de clave privada se representa como se ilustra a continuación, adonde existen dos procesos bien definidos. Por un lado, el Cifrador recibe que como entrada un texto en claro y una clave, y produce como salida un criptosistema.

El segundo proceso, el Descifrador, recibe como entrada un criptosistema y una clave, la misma utilizada en el proceso anterior, y produce como salida el texto en claro.

Figura 1. Criptosistema con Cifrado de Clave Privada



Fuente: Elaboración propia.

Características del crifrado de clave privada

- Requieren del establecimiento previo de un secreto compartido entre las partes involucradas, la Clave.

- Si la Clave es revelada, el criptosistema es inseguro.
- La distribución de claves es compleja en sistemas de tamaño medio o alto.
- El cifrado es muy rápido en comparación a otros sistemas de cifrado.
- Pueden proporcionar Integridad, Autenticación de Origen y No Repudio en relación a los servicios de seguridad de la información.

Tabla 1: Principales algoritmos de cifrado de clave privada

Algoritmo	Clave	Reseña
DES	64 bits	Data Encription Standard. Tipo de Cifrado en Bloques de 64 bits.
3xDES	168 bits	Triple DES. Consiste en aplicar tres veces DES.
RC2	40 bits	Rivest Cipher 2. Tipo de Cifrado en Bloques de 64 bits.
RC4	128 bits	Rivest Cipher 4. Tipo de Cifrado en Flujo.
RC5	0-2040 bits	Rivest Cipher 5. Tipo de Cifrado en Bloques variables de 32, 64 o 128 bits.
IDEA	128 bits	International Data Encription Algorithm. Cifrado en Bloques de 64 bits.
CAST	40-128 bits.	De sus creadores **C**arlisle **A**dams y **S**tafford **T**avares. Cifrado en Bloques de 64 bits.
AES/ RIJNDAEL	128, 192, 256 bits	Advanced Encription Standard. Cifrado en Bloques de 128 bits.

Fuente: Adaptado de Lucena López, 2010.

Funciones Resumen

Las funciones resumen, conocidas ampliamente como funciones Hash, son funciones unidireccionales empleadas para transformar un mensaje en otro de tamaño fijo (huella digital). Es unidireccional porque desde un mensaje cifrado no es posible obtener el mensaje en claro. Si esto ocurre, se trata de una vulneranilidad del algoritmo empleado.

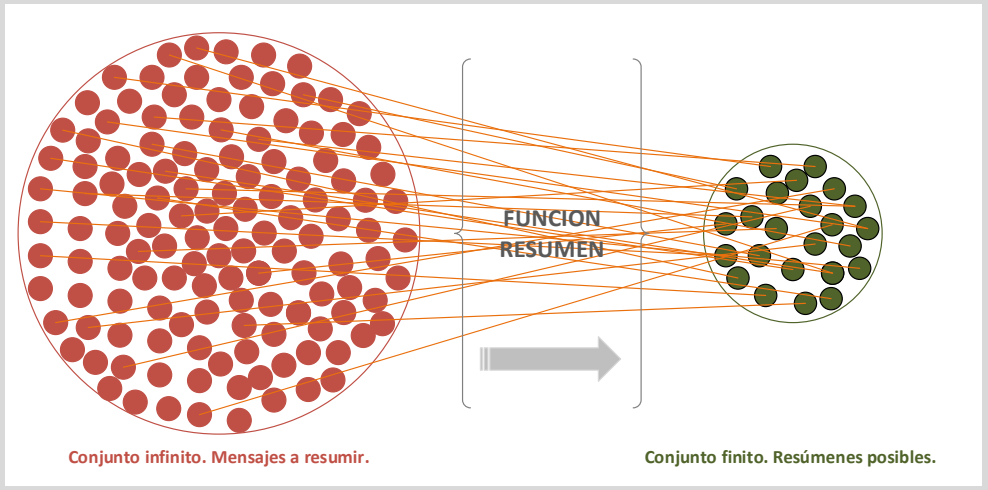
Su utilización es muy amplia, por ejemplo en el almacenamiento de claves de usuarios, en el control de integridad de archivos, en Firma Electrónica, Certificados Digitales, entre otros.

Existen dos tipos de funciones resumen:

- MDC: del inglés modification detection codes. Permiten verificar la integridad de un mensaje.
- MAC: del inglés message authentication codes. A diferencia de la anterior, ésta función utiliza una clave de cifrado, haciendo posible verificar tanto la integridad del mensaje como la autenticidad de su origen, puesto que la clave es conocida por los dos extremos de la comunicación.

El conjunto de valores posibles que puede generar una función resumen se encuentra limitado por la longitud de la salida implementada en el algoritmo (128 bits, 256 bits, etc.). Esto implica que, dado que el conjunto de entrada (conjunto de mensajes a resumir) es infinito, existen infinitos mensajes que pueden generar el mismo resumen. La siguiente imagen grafica la problemática planteada.

Figura 2. Conjunto infinito de mensajes vs conjunto finito de resumenes



Fuente: elaboración propia.

De acuerdo a esto, la seguridad de una función resumen depende de dos aspectos fundamentales:

- Evitar colisiones. Esto es, reducir la probabilidad de que dos mensajes distintos obtengan un mismo resumen.
- Evitar ataques de preimagen. Se basan en calcular un mensaje que obtenga el mismo resumen que otro texto elegido.

Los algoritmos de Función Resumen mas reconocidos son MD5, con salida de 128 bits, SHA-1 con salida de 128 bits, SHA-2 con salidas de 256 bits, H-MAC utilizados en Firma Electrónica.

Cifrado de clave pública

Los algoritmos criptográficos de cifrado de clave pública, también conocidos como criptosistemas asimétricos o de cifrado asimétrico, son criptosistemas que emplean dos claves de cifrado, una pública y otra privada, y no requieren de un canal seguro para que los extremos de la comunicación intercambien la clave de cifrado (UNIR, s.f, https://goo.gl/Ef8Z0R).

Esta característica hace posible que, si el destinatario dispone de la clave pública del emisor, éste ultimo pueda enviarle mensajes de forma segura, sin que deba acordarse de forma previa un secreto compartido entre las partes (UNIR, s.f, https://goo.gl/Ef8Z0R).

Por otra parte, y en contraposición con los algoritmos simétricos, los algoritmos asimétricos son más lentos, requieren de una mayor capacidad computacional como producto del uso de claves de crifrado de mayor longitud (UNIR, s.f, https://goo.gl/Ef8Z0R).

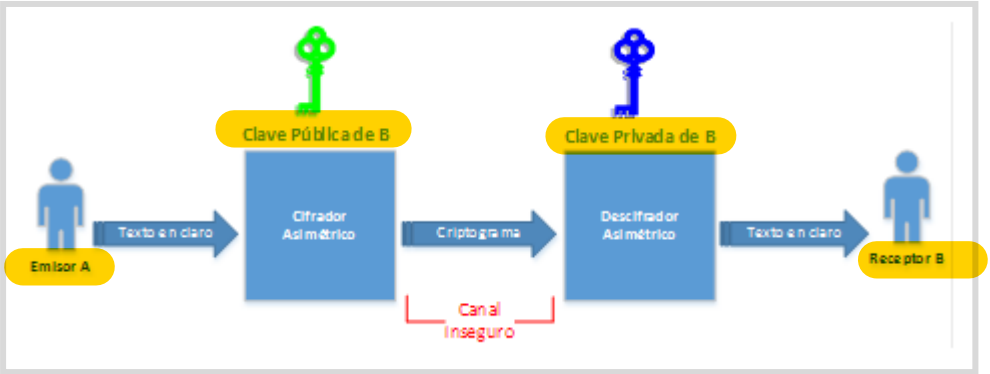
La seguridad de los algoritmos de clave pública reside en la complejidad computacional existente para calcular la clave privada a partir de la clave pública.

El cifrado asimétrico no se utiliza para cifrar mensajes de longitud considerable, debido al costo computacional que esto implicaría, sino que se utilizan para cifrar las claves de sesión que serán empleadas por cifradores simétricos. Son éstos los que se ocuparán de cifrar los mensajes dentro de la sesión establecida. Es decir, ambos algoritmos de cifrado se implementan de forma complementaria (UNIR, s.f, https://goo.gl/Ef8Z0R).

Un criptosistema que utiliza cifrado de clave pública se representa como se ilustra a continuación, adonde existen dos procesos bien definidos. Por un lado, el Cifrador recibe que como entrada un texto en claro y una **clave Pública de B**, y produce como salida un criptosistema (UNIR, s.f, https://goo.gl/Ef8Z0R).

El segundo proceso, el Descifrador, recibe como entrada un criptosistema y una **clave Privada de B**, y produce como salida el texto en claro.

Figura 3. Criptosistema con Cifrado de Clave Pública



Fuente: Elaboración propia.

Cuando el Receptor decide autenticar el origen del mensaje que recibe, genera un resumen de dicho mensaje y lo compara con el resumen enviado, habiendo para ello descifrado previamente el resúmen recibido con la clave pública del origen. Si ambos coinciden, el origen es auténtico y el mensaje es íntegro, no ha sido alterado.

Características del cifrado de clave pública

Tomando como base el ejemplo desarrollado por la Universidad Pontificia Comillas (S.f., https://goo.gl/XIbQpX):

- R y D obtienen un par de claves privada y pública, (Kpv_R, Kpb_R) y (Kpv_D, Kpb_D).
- Si R conoce Kpb D puede cifrar un mensaje **M** con ésta: **C** = E(M, Kpb_D).
- D puede descifrar **C** empleando su clave privada, **M** = D(C, Kpv_D).
- Utilizando cualquiera de las claves públicas es computacionalmente imposible encontrar la clave privada.
- Es computacionalmente imposible recuperar el mensaje **M** partiendo del criptograma **C** y de la clave pública utilizada para cifrarlo.
- Esto posibilita que las claves públicas puedan ser enviadas por canales inseguros sin que esto represente una amenaza para el criptosistema.
- Pueden proporcionar Integridad, Confidencialidad, Autenticación y No Repudio, en relación a los servicios de seguridad de la información.

Tabla 2: Principales algoritmos de cifrado de Clave Pública

Algoritmo	Reseña	Fortaleza
RSA	Rivest, Shamir y Adleman.	Complejidad de factorización del producto de números primos de gran tamaño.
DF	Diffie-Hellman	Dificultad de cálculo de logaritmos discretos en conjuntos finitos.
ElGammal	Taher ElGammal	Dificultad de cálculo de logaritmos discretos en conjuntos finitos.
DSA	Digital Signature Algorithm	Dificultad de cálculo de logaritmos discretos en conjuntos finitos.

Fuente: Adaptado de Lucena López, M. 2010. Criptografía y Seguridad en computadores

Ataques a los algoritmos Criptográficos

Los ataques a los algoritmos criptográficos, en el contexto criptoanálisis, son una de las principales causas que impulsan la evolución permanente de la Criptografía. El incremento computacional es un factor que ha contribuido al descubrimiento de muchas vulnerabilidades presentes en los algoritmos criptográficos.

A continuación, se presentan algunos tipos de ataques conocidos y sus características.

- Ataques en función del impacto que tienen en el sistema.
  - Ataques activos: el atacante tiene acceso a la información y puede para manipularla. Ej. suplantación, denegación de servicio.
  - Ataques pasivos: el atacante tiene acceso a la información pero no tiene capacidad para manipularla. Ej. análisis de tráfico.
- Ataques en función de la información que posee el atacante.
  - A partir de un mensaje cifrado. Análisis por fuerza bruta, se prueban todas las claves posibles.
  - A partir de un mensaje en claro. Se introduce el mensaje y se analiza el cifrado.
- Ataques a los Protocolos.
  - Buscan vulnerabilidades en el diseño de los protocolos.
  - También habituales en la implementación de protocolos con diseños seguros.
  - Reutilización de claves o fragmentos de protocolos pasados.
  - Suplantación de entidades.
  - Secuestro de sesiones.
  - Habitualmente en conjunción con ataques de denegación de servicios (DDOS).

En resumen, los algoritmos de clave privada, tienen la particularidad de que la clave de cifrado es la misma en ambos extremos de la comunicación, o bien de una es posible obtener la otra, y por lo tanto, su seguridad se basa directamente en la capacidad de trasmitir dicha clave de un extremo al otro a través de un canal seguro, si no es posible asegurar el canal, no se logrará un criptosistema seguro. A partir de allí, se podrá utilziar el cifrado de flujo o de bloque, según el contexto que se pretenda asegurar, pues ambos responden a distintas necesidades. Se utilizará el primero cuando sea necesario cifrar en tiempo real, y el segundo cuando sea necesario cifrar grandes volumenes de informacion; en el fondo, todos ellos serán útiles a un objetivo específico, haciendo posible Confidencialidad, Autenticación, Integridad, entre otros Servicios de Seguridad.

Por otra parte, el cifrado de clave publica supone muchas ventajas frente al cifrado de clave privada. Desde el punto de vista de la flexibilidad, pueden ser utilziados en un mayor número de situaciones; no es necesario un canal seguro para el intercambio de claves, pero esto no significa que se deje de utilizar la criptografía simétrica, dado que el cifrado asimétrico es computacionalmente mas costoso, con lo cual el complemento de ambos métodos será lo que va a permitir implementar servicios mas adecuados, ambos complementarán sus deficiencias.

Por ultimo, se recomienda una revisión de la **Recomendación X.800**, citada en las Referencias, para una comprensión profunda de los Servicios de Seguridad de la Información y los mecanismos adecuados para alcanzarlos.

Referencias

Gómez Vieites, A. (2011). *Enciclopedia de la Seguridad Informática*. (2° Ed.) Madrid, España: Ra-Ma.

Lucena López, M. (2010). *Criptografía y seguridad en computadores*. 4° Edición. Versión 0.7.0. Jaén, España: Universidad de Jaen.

Recomendación X.800. (1991). *Arquitectura de Seguridad para la Interconexión de Sistemas Abiertos para Aplicaciones del CCIT. Recomendación X.800*. Unión Internacional de Telecomunicaciones, UIT. Recuperado de: https://www.itu.int/rec/T-REC-X.800-199103-I/es

UNIR (s.f). *Algoritmos de criptografía asimétrica – Tema 3*. Esquema. España: Universidad Internacional de La Rioja. Recuperado de: https://studylib.es/doc/7210232/algoritmos-de-criptografia-asimetrica.

Escuela Técnica Superior de Ingeniería (s.f.) *Tema2: La criptografía para la protección de comunicaciones*. España: Universidad Pontificia Comillas. Recuperado de: https://www.iit.comillas.edu/palacios/seguridad_dr/tema2_cripto.pdf

Infraestructura de clave pública

Seguridad Informática

UNIVERSIDAD SIGLO 21 | MIEMBRO DE LA RED ILUMNO

Infraestructura de clave pública

La lectura del presente material es meramente complementaria a la Bibliografía Básica. Definiciones teóricas de los conceptos aquí expuestos deben ser tomadas de dicha Bibliografía.

Una Infraestructura de clave pública, **PKI** por sus siglas en inglés, es un protocolo que especifíca los procesos organizativos necesarios para la gestión de mecanismos criptográficos y Certificados Digitales de Clave Pública, para el intercambio seguro de información, y abarca tanto componentes de software como de harware.

Sus principales objetivos se pueden agrupar en los siguientes:

- Autenticidad de la información.
  - Autenticación del origen de la información.
  - Autenticación de entidades (físicas o jurídicas).
  - Integridad de la información.
- Confidencialidad de la información.
- No Repudio.
  - En origen.
  - En destino.
- Establecimiento claves simétricas.

En materia de estándares de referencia, Public Key Criptography Standards[1] (#PKCS) son un conjunto de recomendaciones y guias de implementación publicadas por RSA[2] en colaboración con otras empresas tecnológicas líderes como Microsoft, Apple, Intel, EMC, solo por citar algunas.

Otro recurso de referencia es el SP-800-32 Introduction to Public Key Technology[3] publicado por NIST, que brinda definiciones conceptuales del contexto y recomendaciones de implementación.

Una PKI esta compuesta por una serie de elementos, que se detallan, pero que no se limitan, a continuación:

- Firma digital.
- Certificados digitales. Versión X.509 v3.
- Organización jerárquica. Autoridad de certificación (CA), Autoridad de registro (RA), *Pretty Good Privacy* (PGP).
- Directorios de certificados. (LDAP).
- *Software* de Administración de Certificados.
  - Comprobación

[1] Para más información sobre PKCS RSA, consulte: https://goo.gl/pSSSPm
[2] Para más información sobre RSA Laboratories, consulte: https://goo.gl/RjX16N
[3] Para más información acerca de NIST SP-800-32, consulte: https://goo.gl/wxeRHb

  - Generación
  - Gestión de Certificados
- Dispositivos seguros de generación de firmas.

Firma digital

Una firma digital es un digesto o resumen cifrado con clave privada de quien lo genera, que se adjunta a un objeto de información, desde el cual ha sido generada (Alfonso R, 2008).

Esta característica de estar adjunta al objeto, hace posible verificar su autenticidad a través de las funciones de resumen.

Presenta una analogía con la firma manuscrita, aunque para ello debe reunir ciertas propiedades:

- Debe estar ligada de forma unívoca al mensaje. Una firma digital válida para un documento no puede ser válida para otro distinto (Alfonso R, 2008).
- Sólo puede ser generada por su titular legítimo. Así como una persona tiene una forma propia de escribir, y que el manuscrito de dos personas distintas puede ser reconocida mediante un análisis grafológico, una firma digital solo puede ser generada por la persona (física o jurídica) a la que pertenece legalmente (Alfonso R, 2008).
- Se debe poder verificar de forma pública. La comprobación de su autenticidad debe estar al alcance de quien lo requiera, en cualquier momento (Alfonso R, 2008).

La forma de generar firmas digitales consiste en emplear una combinación de cifrado asimétrico y funciones de resumen del tipo MAC, cifrando dicho resume con la clave privada de quien genera dicha firma.

Certificados digitales

Un Certificado Digital es, en términos generales, un certificado de clave pública. Está compuesto por una clave pública y un identificador, firmados digitalmente por una tercera parte de confianza o Autoridad de Certificación reconocida. Su finalidad consiste en demostrar que una clave pública pertenece a una entidad (física o jurídica) en concreto (Alfonso R, 2008).

Para ello, la citada Autoridad de Certificación debe implementar los controles necesarios para asegurar y verificar previamente que la clave pública es auténtica, es decir, pertenece a quien dice ser su titular.

En Argentina, la ONTI[4] actúa como Autoridad de Certificación de los Organismos Públicos nacionales, firmando las claves públicas de los Organismos y generando los Certificados Digitales correspondientes.

Cualquier Entidad que disponga de la clave pública de la ONTI estará en condiciones de verificar sus Certificados Digitales, otorgando la confianza correspondiente a las claves públicas asociadas a los mismos.

Es importante destacar que la ONTI no es un organismo descentralizado de gobierno, sino que se trata de un organismo dependiente de la Jefatura de Gabinete de Ministros de la Nación

Certificados digitales X.509

X.509 es el formato de certificados digitales de mayor implementación. Es producto de la recomendación ITU-T Recomendation X.509[5], que data del año 1988. Esta recomendación se ha convertido en un estándar del Organismo Internacional de Estándares (ISO), en la norma ISO/IEC 9494-8[6] (Betoret Cortés, 2003, https://goo.gl/jGDCZs).

X.509 define la sintáxis de los certificados digitales y especifica los campos que éstos deben contener. Su formato se presenta a continuación (Betoret Cortés, 2003, https://goo.gl/jGDCZs).

[4] Para más información acerca de la Oficina Nacional de Tecnologías de Información (ONTI), consulte: https://goo.gl/P6XwOY
[5] Para más información sobre X.509 Recomendation, consulte: https://goo.gl/gQ6ahP
[6] Para más información sobre ISO/IEC 9594-8, 2014, consulte: https://goo.gl/kAS26U

Figura 1: Formato de certificado digital X.509

Versión		Número de versión del formato X.509
Número de Serie (Serial Number)		Unico número identificador del certificado generado por el emisor del mismo.
Firma (Signature)	ID del Algoritmo	Algoritmo usado para firmar el certificado
Emisor (Issuer)		Nombre del emisor del certificado (en formato X.500)
Validez (Validity)	No antes de (Not Before)	Fecha de inicio de validez
	No después de (Not After)	Fecha de finalización
Titular (Subject)		Nombre del titular del certificado (en formato X.500)
Información de la clave pública del Titular	ID del Algoritmo	Algoritmo de firma del titular
	Parámetros	Parámetros aplicables a la clave pública
	Clave Pública	Clave Pública del titular
Extensiones	(Opcional)	Extensiones agregadas a los certificados tal como lo indica el estándar.
Firma del Emisor	ID del Algoritmo	Algoritmo usado para esta firma
	Encriptado de resultado de la función de Hash sobre el certificado	

Fuente: Secretaría de la Función Pública, 1998, Recuperado de: https://goo.gl/dM2Qk6

Tipos de certificados digitales

Existen tipos de Ceritificados Digitales que se utilizan en función del ambito y de la entidad que se pretende identificar.

- Certificados de usuario final. Emitidos para una persona física o jurídica.
- Certificados de firma de *software* o componente informático. Se emiten para un fabricante de soluciones software. Se utilizan para verificar los productos que éste produce.
- Certificados de servidor. Se utilizan para autenticar a un Servidor determinado. Un ejemplo es el caso de servidores Web bajo protocolo SSL, o certificados de Servidores de Escritorio Remito.
- Certificados de usuario final. Se clasifican en distintos subtipos en función del proceso de identificación implementado y de la información incluida.
  - Clase 1.
  - Clase 2.
  - Clase 3.
  - Clase 4.
- Certificados de atributos para control de acceso. Utilizados para control de acceso en función de roles bajo un esquema de servicio de autorización.

Organización jerárquica

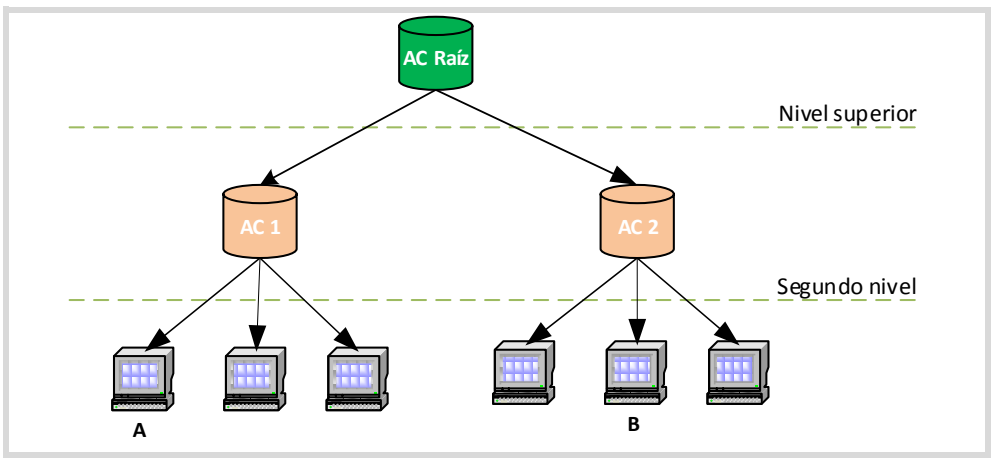
Las autoridades de certificación (AC) se organizan en forma de "árbol", por niveles, de tal manera que las autoridades de certificación de un nivel poseen certificados digitales emitidos por autoridades de niveles superiores.
Es posible verificar un certificado digital siempre que se posea la clave pública de una autoridad de primer nivel, que se limitan a un conjunto muy reducido, internacionalmente reconocidas.

Las autoridades de certificación que generan certificados finales correspondientes a las hojas del árbol tienen la responsabilidad de comprobar de manera fidedigna que cada clave pública pertenece a su propietario.

Sin embargo, aquellas autoridades que certifiquen a otras autoridades, deben garantizar, además, que estas últimas empleen mecanismos adecuados para comprobar las identidades de sus clientes. De lo contrario, alguien podría crear una autoridad de certificación cualquiera, obtener el correspondiente certificado digital de niveles superiores, y luego emitir certificados falsos.

El esquema jerárquico es simple y efectivo, aunque presenta un problema importante: si una de las autoridades de certificación resulta comprometida, todos sus descendientes en el árbol serán invalidados. Esto obliga, por un lado, a que las autoridades de certificación sean lo más transparentes posible, y por otro a que se mantengan las denominadas **Listas de Revocación** (Certificate Revocation Lists CRL), que anulan todas aquellas claves públicas que, por alguna causa, han dejado de ser válidas.

Figura 2. Organización jerárquica de Autoridades de Certificación



Fuente: adaptado de Lucena López, 2010.

En el esquema jerárquico de certificación que se presenta en la figura Si A quiere comprobar la identidad de B, emplearía la clave pública de AC 1 para verificar el certificado digital de AC 2. Una vez hecha esta comprobación, podría confiar en AC 2 como certificador de la clave pública de B.

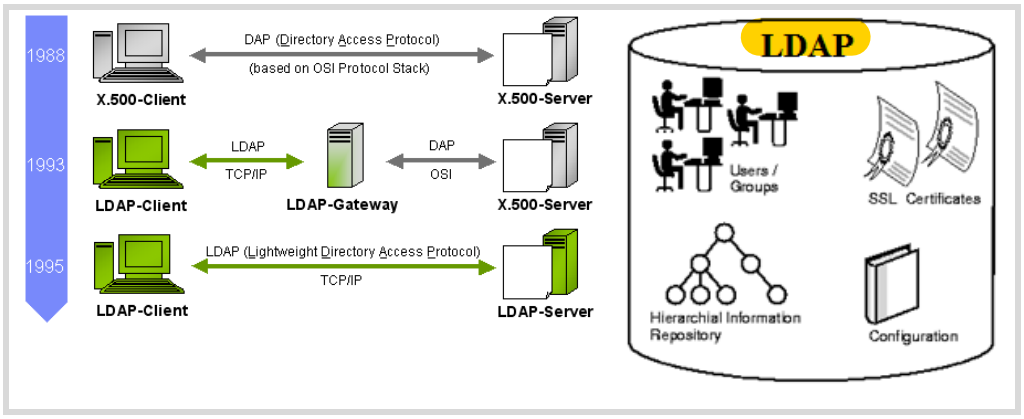
Directorios de certificados

Un Directorio de Certificados proporciona un mecanismo para el almacenamiento de información, en modo jerárquico, de firmas, claves, certificados y listas de revocación de certificados.

Está basado en un servicio de directorio **LDAP** (Protocolo Ligero/Simplificado de Acceso a Directorios) y puede incorporar funcionalidades mas avanzadas, como servicios de recuperación automática de claves, gestión de usuarios, entre muchos otros.

LDAP opera bajo el modelo Cliente/Servidor, atendiendo peticiones de los distintos componentes del entorno (**dominio**). De acuerdo al modelo implementado, la respuesta puede requerir la derivación de la consulta a un directorio remoto.

Figura 3. Evolución de la arquitectura de servicios de directorio



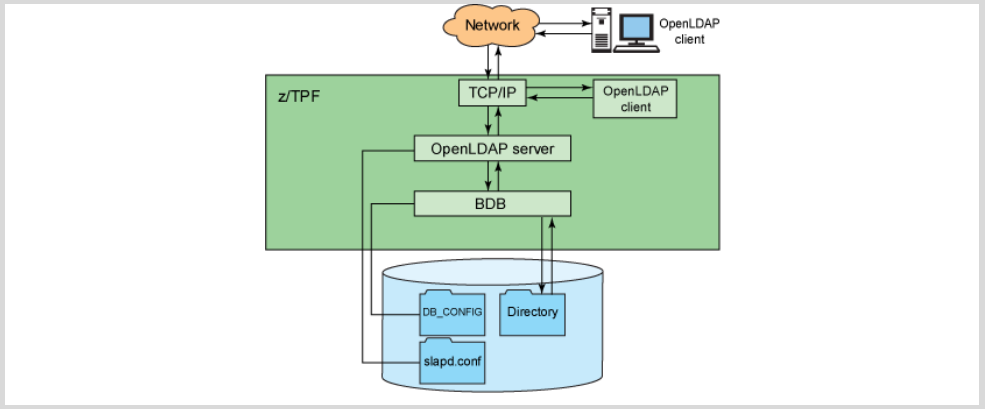
Fuente: adaptado de Networx Security, 2015, https://goo.gl/RKHlvM

Software de administración de certificados

La administración o gestión de una Infraestructura de Clave Pública se basa en una solución de servicios de directorios (LDAP). Para el caso de sistemas

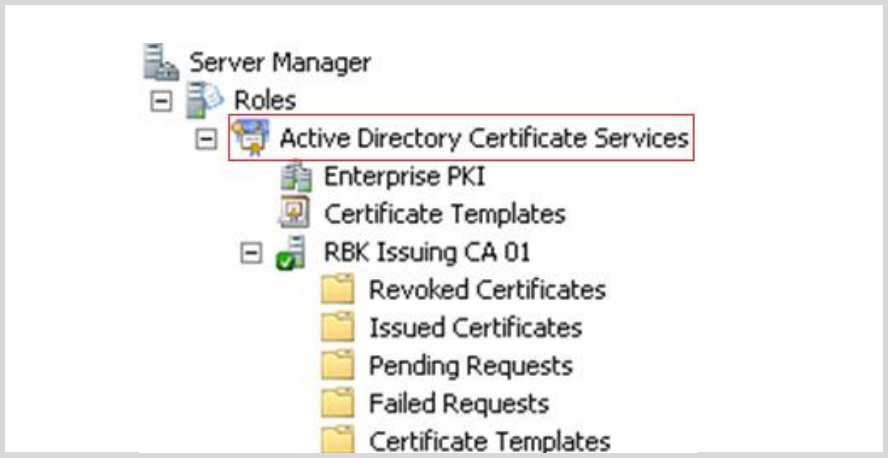
operativos basados en Unix/Linux se podrá considerar la solución **OpenLDAP**, mientras que en entornos Microsoft será **Active Directory**.

Figura 4. Solución LDAP basado en sistema operativo Unix/Linux.



Fuente: Elaboración propia.

Figura 5. Solución LDAP según sistema operativo MS Windows.



Fuente: Elaboración propia.

En resumen, la Infraestructura de Clave Pública es un marco que sienta las bases para la implementación de los métodos criptográficos de clave pública. Se trata de una implementación que abarca una serie de componentes (hardware/software) como lo son la Firma Digital, Certificados Digitales, Servicios de Directorio, dispositivos seguros de generación de firmas, entre otros.

Si bien a través de una PKI se pueden proveer Servicios de Seguridad tales como Autenticación, Integridad, Confidencialidad y No Repudio, existe un componente sensible sobre el cual reside este esquema de confianza, y es la Autoridad de Certificación, entidad ésta que valida la relación clave pública-propietario ante un tercero. Si esta Autoridad de Certificación se suplanta, todo el esquema de seguridad quedará expuesto, y cierto es que han existido vulnerabilidades en la PKI que han permitido estos eventos, y que a la vez han sido corregidas durante el tiempo.

El uso de certificados firmados por autoridades de certificación externas acarrea un costo ecnómico, por lo que es común la utilización de certificados autofirmados para servicios que son internos a la organización, recurriéndose a Autoridades de Certificación externas exclusivamente en casos en los que se brinden servicios a terceros que requieren confianza.

Si bien han surgido Autoridades de Certificación que ofrecen servicios de confianza gratuitos que valen la pena ser evaluadas, su nivel de aceptación se encuentra limitado por por parte de los navegadores que implementan para ello una política de requisitos que deben ser cumplidos. Caso contrario, los navegadores emitiren un alerta de seguridad cuando se encuentran con Certificado Digital cuyo certificante no se encuentre en su lista de confianza.

Existen a la vez, Autoridades de Certificación abiertas o distribuidas, cuyo fin es promover un anillo de confianza en el que todos los usuarios actuan como autoridades de certificación, como una alternativa frente a las estructuras jerarquicas tradicionales.

Según el grado de confianza que presente un tercero, se puede optar por confiar en todos sus certificados, no confiar en ninguno, considérese un usuario que certifica todo lo que atraviesa por sus manos sin hacer ninguna comprobación, o confiar en aquellos que, además, posean firmas de otros usuarios.

Nótese que en este ultimo esquema la confianza en una Autoridad certificadora puede tomar muchos valores (desconfianza absoluta a confianza total), frente a los dos (confiable y no confiable) que puede tomar en un esquema jerárquico.

Referencias

Gómez Vieites, A. (2011). *Enciclopedia de la Seguridad Informática.* (2° Ed.) Madrid, España: Ra-Ma.

López López, M. (2010). *Criptografía y seguridad en computadores*. 4° Edición. Versión 0.7.0. Jaén, España: Universidad de Jaen.

Secretaría de la Función Pública. (1998). *Resolución N° 194/98. Anexo Estandares sobre Tecnología de Firma Digital para la Administración Pública Nacional.* Buenos Aires: Jefatura de Gabinete de Ministros. Recuperado de: http://www.mecon.gov.ar/digesto/resoluciones/sfp/1998/resolsfp194.htm

Networx Security. (2015). *Evolución de la arquitectura de servicios de directorio* [Imagen]. Recuperado de: http://www.networxsecurity.org/members-area/glossary/l/ldap.html

Alfonso, R. (2008). *Sistemas de Computación*. [Trabajo monográfico]. Córdoba: Universidad Nacional de Córdoba. Recuperado de: http://sistemasdecomputacion2008.blogspot.com.ar/2008/11/criptografa-alfonso-quinzio.html

Betoret Cortés, J. (2003). *Firma digital* . Recuperado de: http://spi1.nisu.org/recop/al02/betoret/index.html

Firma electrónica

Seguridad Informática

UNIVERSIDAD SIGLO 21 | MIEMBRO DE LA RED ILUMNO

Firma electrónica

La lectura del presente material es meramente complementaria a la Bibliografía Básica. Definiciones teóricas de los conceptos aquí expuestos deben ser tomadas de dicha Bibliografía.

La firma electrónica se define como una secuencia de bits, adherida a un objeto de información, que permite garantizar su autenticidad e integridad y consecuentemente, el no repudio. Une dos conceptos, por un lado el contenido o los datos y por otro lado la identidad de quien lo genera.
Está vinculada a un único objeto de información, es decir, la firma de dos documentos distintos no puede producir la misma firma. Además, únicamente puede ser generada por su legítimo titular y es públicamente verificable.

La Firma Electrónica se genera al cifrar, con la clave privada del remitente, el resumen que se obtiene de un objeto de información dado.

El algoritmo de cifrado que se utiliza para ello es un algoritmo asimétrico, y el resumen se obtiene por medio de la aplicación de una función Hash.

El destinatario recibe, tanto el objeto de infomación en claro, como la Firma Electrónica generada por el remitente.
Éste descifra la Firma Electrónica utilizando la clave pública del remitente, proceso que le permite obtener el resumen generado en el origen.
A la vez, genera él tambien un resumen del objeto de información en claro recibido y procede a la comparación de ambos resumenes.

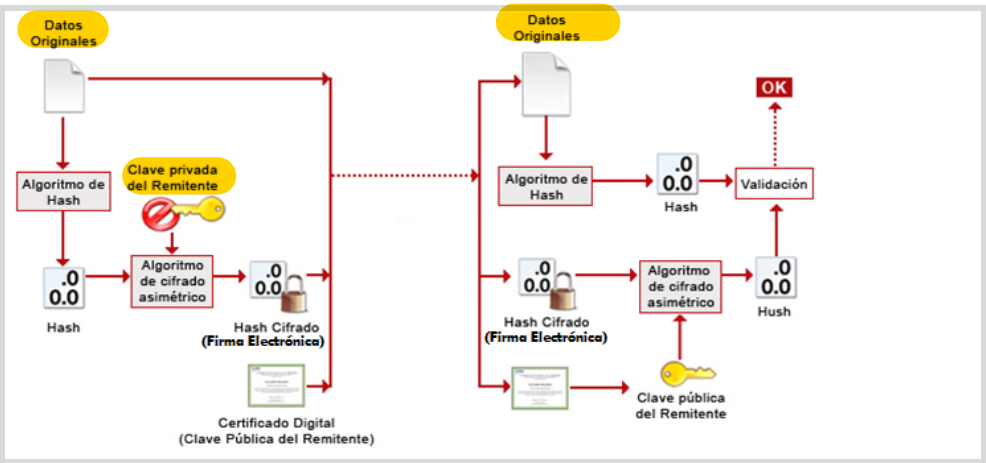
Si estos son iguales, se concluye que:

- La información es íntegra, pues el mismo resumen que obtuvo el remitente en origen lo pudo obtener el destinatario, hecho éste que no sería posible si la información fuera manipulada durante la comunicación.

- El origen es auténtico, dado que ha sido posible descifrar la Firma recibida utilizando para ello la clave pública del titular, que a su vez se encuentra relacionada matemáticamente y de forma unívoca con su clave privada.
  Se debe tener en cuenta que, dado un criptograma cifrado con una clave privada, solo es posible descifrarlo con su clave pública pues, como ya se planteó, ambas claves se encuentran matemáticamente relacionadas.
  Si la clave privada utilizada para generar la Firma no estuviese relacionada con la clave pública, al descifrarla en destino, no se obtendría el mismo resultado y resultaría en un origen no auténtico.

Todo este proceso de firma en origen y comprobación de la firma en destino, queda ilustrado tal como se presenta a continuación en la figura 1.

Figura 1: Generación y comprobación de firma electrónica



Fuente: Adaptado de INCIBE, 2014, recuperado de: https://goo.gl/Cu22FP

Fundamentos técnicos de la firma electrónica

La Firma Electrónica está basada en algoritmos criptográficos asimétricos en los que son necesarias un par de claves para el intercambio de información.

- La clave pública y la privada están relaciondas matemáticamente, de modo que lo que se cifra con una solo se puede descifrar con la otra.
- La clave privada debe ser secreta, no así la pública.
- La clave privada es almacenada y conocida exclusivamente por su titular.
- La clave pública es distribuida entre todos los posibles destinatarios de información con los que interactúe el titular de la clave.

Los algoritmos comunmente utilizados en un proceso de Firma Electrónica, se presentan en la siguiente Tabla 1.

Tabla 1: Algoritmos de Firma Electrónica.

Algoritmo	Fortaleza
RSA	Su seguridad se basa la dificultad computacional para factorizar el producto de dos números primos de gran longitud.
ElGamal	Su seguridad se basa en la dificultad computacional para calcular logaritmos discretos en un tiempo razonable.
DSA	Se deriva del algoritmo ElGamal. Su seguridad se basa en la misma dificultad que el algoritmo que le da origen.

Fuente: Adaptado de Lucena López, 2010.

Cerificados Digitales y su relación con la Firma Electrónica

Un certificado digital es, en términos generales, un certificado de clave pública. Está compuesto por una clave pública y un identificador, firmados digitalmente por una tercera parte de confianza o Autoridad de Certificación reconocida. Su finalidad consiste en demostrar que una clave pública pertenece a una entidad (física o jurídica) en concreto. Contiene la información necesaria para firmar digitalmente e identificar a su propietario (PAe, https://goo.gl/wLwsPZ).

Entre los datos que se incluyen en un Certificado se encuentran su nombre, DNI/CUIL/CUIT, algoritmo y claves utilizados en la firma, fecha de validez y organismo que lo expide (PAe, https://goo.gl/wLwsPZ).

Es importante destacar que el Certificado Digital contiene unicamente la clave pública del firmante, no así la clave privada. La identificación del titular es posible a través de la confianza que genera la Autoridad de Certificación y también a la relación univoca que existe entre la clave pública y la privada.

Fundamento Jurídico de la Firma Electrónica

Dada su relevancia y especial característica de identificación unívoca, la Firma Electrónica debe ser abordada tanto desde el ámbito técnico y tecnológico, como desde el ámbito legal.

En los términos de la **Ley N° 25.506 de Firma Digital Argentina**, promulgada en el año 2001, la Firma Electrónica se define como se presenta a continuación:

> **ARTÍCULO 5º — Firma electrónica**. Se entiende por firma electrónica al conjunto de datos electrónicos integrados, ligados o asociados de manera lógica a otros datos electrónicos, utilizado por el signatario como su medio de identificación, que carezca de alguno de los requisitos legales para ser considerada firma digital. En caso de ser desconocida la firma electrónica corresponde a quien la invoca acreditar su validez[1].

[1] Ley N° 25.506 (2001). Firma digital Argentina. Senado y Cámara de Diputados de la Nación Argentina. Recuperado de: https://goo.gl/xrPxm2

Luego,

> **ARTÍCULO 2º — Firma Digital.** Se entiende por firma digital al resultado de aplicar a un documento digital un procedimiento matemático que requiere información de exclusivo conocimiento del firmante, encontrándose ésta bajo su absoluto control. La firma digital debe ser susceptible de verificación por terceras partes, tal que dicha verificación simultáneamente permita identificar al firmante y detectar cualquier alteración del documento digital posterior a su firma. [2]
>
> **ARTÍCULO 9º — Validez.** Una firma digital es válida si cumple con los siguientes requisitos:
>
> a) Haber sido creada durante el período de vigencia del certificado digital válido del firmante;
>
> b) Ser debidamente verificada por la referencia a los datos de verificación de firma digital indicados en dicho certificado según el procedimiento de verificación correspondiente;
>
> c) Que dicho certificado haya sido emitido o reconocido, según el artículo 16 de la presente, por un certificador licenciado. [3]

De acuerdo a la legislación, la Firma Digital adquiere la misma relevancia que la firma hológrafa; si un tercero desconoce la validez de la firma, es éste, el que recusa, quien debe responsabilizarse por demostrar técnica y jurídicamente esa invalidez.

Por otro lado, la Firma Electrónica puede ser desde una firma hológrafa escaneada hasta una Firma basada en clave pública y privada, que carezca de las características definidas en el Artículo 9°. En este caso, si un tercero desconoce la validez de la firma, la responsabilidad probatoria recae del lado del titular, contrario a lo que sucede con la Firma Digital.

Se puede concluir que, en los términos de la legislación Argentina, la diferencia entre Firma Digital y Firma Electrónica subyace en que la primera cuenta con un Certificado Digital emitido por una Autoridad de confianza y reconocida que valida la autenticidad de la firma, a diferencia de la Firma Electrónica.

---

[2] Ley N° 25.506 (2001). Firma digital Argentina. Senado y Cámara de Diputados de la Nación Argentina. Recuperado de: https://goo.gl/xrPxm2

[3] Ley N° 25.506 (2001). Firma digital Argentina. Senado y Cámara de Diputados de la Nación Argentina. Recuperado de: https://goo.gl/xrPxm2

En otros países, como España, por citar un ejemplo, la Firma Electrónica se encuentra tipificada como Simple y Avanzada (o Reconocida)[4], siendo ésta última concordante con lo que la legislación Argentina define como Firma Digital.

El concepto de Firma Electrónica presentado en este material, en el marco de la legislación vigente, **se corresponde con Firma Digital**.

Autoridadades de Certificación

La misión de una Autoridad de Certificación es dar fe de que la Firma Electrónica se corresponde con una entidad en concreto.
Con el fin de cumplir esto las Autoridadades de Certificación deben mantener y proteger todos los datos y procesos involucrados en la generación de los Ceritificados Digitales que expiden.

Las Autoridades de Certificación, referidas en la Ley de Firma Digital Argentina como **Certificador Licenciado**, tanto en el sector público como en el privado, se encuentran alcanzados por dicha Ley y deben cumplir con los requisitos definidos en su **Capítulo III de Certificador Licenciado**.
Es importante destacar que también se encuentran alcanzados por esta Ley las Autoridades de Certificación de origen extranjero.

Para operar como Autoridad de Certificación, según fija la Ley, se debe tramitar la inscripción ante el Ente Licenciante, figura representada por la Secretaría de Gabinete y Coordinación Administrativa, dependiente de la Jefatura de Gabinete de Ministros de la Nación.

En el ambito Público, los siguientes organismos operan como Autoridades de Certificación:

- ONTI[5]. Oficina Nacional de Tecnologías de Información.
- AFIP[6]. Administración Federal de Ingresos Públicos.
- ANSES[7]. Administración Nacional de Seguridad Social.

[4] Para más información sobre Ley 59/2003 Firma Electrónica España, consulte: https://goo.gl/eV2I6Z
[5] Para más información sobre ONTI, Firma Digital Argentina, consulte: https://goo.gl/ujFnK7
[6] Para más información sobre Anses, Firma Digital, consulte: https://goo.gl/UIZ8ml
[7] Para más información sobre AFIP, Firma Digital, consulte: https://goo.gl/c2dHIN

Utilización de la Firma Electrónica

A continuación se presenta una lista breve de los ambitos mas frecuentes en los que se utiliza la Firma Electrónica, tanto en el ambito público como en el ambito privado.

- Publicación de información segura en internet.
- Notificaciones oficiales del Estado (Boletín Oficial).
- Correo electrónico.
- Comercio Electrónico.
- Inscripción y Trámites en línea como servicios del Estado.
- Expedientes digitales.
- Voto Electrónico.

En resumen, la utilidad práctica de la Firma Electrónica, aporta tres características a la Seguridad de la Información: identificación del firmante (autenticación), integridad de los datos y no repudio. Estas tres características reunidas en un mismo contexto redundan en autenticidad, entendida como la certificación de la identidad y veracidad de algo.

Es un instrumento de confianza fundamental que hacen posible establecer transacciones a traves de las tecnologías de información de una forma mas eficiente y eficaz frente a de los medios tradicionales.

Se sustenta sobre los algoritmos criptograficos asimétricos y sobre el esquema jerárquico de las Autoridades de Certificación, sobre quienes recae la responsabilidad de emitir los Certificados Digitales que serán utilizados para comprobar las firmas; un Certificado Digital será tan confiable como lo sea la Autoridad de Certificación que lo emite.

Los países dotan a la Firma Electrónica de un marco jurídico, puesto que supone un medio de identificación capaz de reemplazar de forma eficaz a los metodos de identificación tradicionales. Argentina ha sido el primer país en latinoamérica en legislar la Firma Electrónica a través de la Ley N° 25.506 de Firma Digital, citada en las Referencias y cuya lectura se recomienda para profundizar sus alcances y ambito de aplicación.

Referencias

Gómez Vieites, A. (2011). *Enciclopedia de la Seguridad Informática*. (2° Ed.) Madrid, España: Ra-Ma.

López López, M. (2010). *Criptografía y seguridad en computadores*. 4° Edición. Versión 0.7.0. Lugar: Jaén, España: Universidad de Jaen.

INCIBE. (2014). *Generación y comprobación de Firma Electrónica*. España: Instituto Nacional de Ciberseguridad. Recuperado de: https://www.incibe.es/extfrontinteco/img/dnie/contenido_esquema1.jpg

Portal de Administración Electrónica. (s.f) *Los Certificados Electrónicos. Recuperado* de: http://firmaelectronica.gob.es/Home/Ciudadanos/Certificados-Electronicos.html