Introducción

El término seguridad, abarca un amplio campo de áreas profesionales difíciles de enumerar. Este artículo se centra en la protección de los datos, esto incluye tanto el trasporte como su almacenamiento.

Para la salvaguardia de estos datos se utilizan las denominadas técnicas o herramientas criptográficas. Esta protección se consigue mediante métodos de redistribución del contenido de la información y/o sustitución del mismo por símbolos u otros elementos resultantes de operaciones matemáticas. Su objetivo no es disimular la existencia del mensaje, más bien se trata de ocultar su significado.

Los conceptos sobre la aplicación de las técnicas de criptografía hoy en día, aparecen como algo confuso para muchas personas. Conviven con ello, lo utilizan de distintas formas directa o indirectamente y en ocasiones sin ser totalmente conscientes de ello.

Un ejemplo sencillo es cuando aceptamos entrar en un sitio web donde existe un problema con su certificado seguridad. En esta situación puede asumirse un riesgo de consecuencias impredecibles por una simple cuestión de ignorancia.

Evolución histórica

Las primeras evidencias conocidas son los jeroglíficos tallados en algunos monumentos del Antiguo Egipto, hace más de 4500 años. No está clara la intención de los citados jeroglíficos y existe la posibilidad de que su objetivo final no tuviera nada que ver con la ocultación de un mensaje.

Los hebreos ya utilizaban una técnica de cifrado por sustitución semejante al *atbash* entre los 600 y 500 años antes de cristo. El *atbash* se emplea el libro de Jeremías.25,26 de la Biblia, donde la palabra Babilonia en hebreo: *Babel* se convierte en *SHeshash*.

En la Grecia clásica los soldados espartanos utilizaban un cifrado por trasposición basado en una escítala. La escítala consiste en un par de varas del mismo grosor (una la del emisor y la otra para el receptor), donde se enrolla un mensaje. El mensajero solo trasportaba la cinta de cuero del mensaje.

Figura 1
http://es.wikipedia.org/wiki/Esc%C3%ADtala#/media/File:Skytale.png

Otra técnica de encriptado relevante es la que desarrollo el escritor Griego Polybius, (año 200 antes de cristo). Este método se basa en la colocación del alfabeto en una red cuadrada de 5x5. El sistema consistía en hacer corresponder cada letra con sus posiciones de fila y columna. Una de las aportaciones importantes de este método es que se podía enviar un mensaje a distancia mediante señales hechas con antorchas.

Existen algunas referencias sobre las técnicas de encriptado que utilizaba Julio César para comunicarse con sus oficiales. El cifrado era del tipo de sustitución por desplazamiento de tres

caracteres del alfabeto. Hoy en día, cualquier alfabeto que esté codificado con el alfabeto desplazado manteniendo su orden se llama “cifrado de césar”.

En la época medieval es destacable en cifrado de Alberti que aparece en su tratado de 1466. Se considera el primer cifrado por sustitución polialfabético. Se trata de un disco formado por dos partes, una fija y otra interior móvil. Las partes fija y móvil disponen de 24 celdas iguales que contiene el alfabeto latino. La parte fija es en mayúsculas más los números **1**, **2**, **3** y **4**, (sin incluir la **H J K N U W Y**). La parte móvil es en minúsculas no tiene números e incluye el carácter **&**.

Figura 2
http://www.mateureka.it/wp-content/uploads/2012/11/disco-cifrante-leon-battista-alberti.jpg

El cifrado de *Playfair* fue creado por *Charles Wheatstone* en 1854. Se trata de colocar un una red cuadrada de 5x5 con una palabra clave de forma tal que no se repitan las letras. Las posiciones que quedan vacías se rellenan con las palabras restantes del alfabeto. El cifrado no es por filas y columnas, es algo más complejo, el mensaje se descompone por parejas de caracteres donde se tienen en cuenta su posición sobre la red de 5x5.

Posiblemente el método criptográfico más conocido en general, es el *Enigma*. Fue utilizado por el ejército alemán durante la Segunda Guerra Mundial. Se trata de un sistema electromecánico basado en técnica de rotores. Este sistema de encriptado fue descifrado de forma automatizada por el matemático y genio *Alan Turing.*

Tal como se ha descrito, la necesidad de preservar el contenido de un mensaje ha sido una constante desde el principio de los tiempos. En general para aplicaciones de carácter militar aunque no de forma exclusiva. Se han mostrado algunos de los más relevantes, pero existen y han existido muchos más.

Criptografía, arte o ciencia

El periodo que va des de la antigüedad hasta el año 1949 se le denomina era de la criptografía pre-científica (Artística), de 1949-1972 criptografía científica (Shannon) y a partir del año 1976 criptografía asimétrica (Diffie-Hellman).

En el periodo que comprende la criptografía precientífica, las distintas soluciones que se aportaban eran más que suficientes, un factor importante para ello, eran los modelos sociales en los que la mayoría de la población era analfabeta. Esta circunstancia reducía enormemente la probabilidad de que alguien ajeno a los círculos donde se movía dicha información fuera capaz de descubrir su significado.

El hecho de que alguien diseñe un método para ocultar el significado de un mensaje, induce a aguzar el ingenio de algún otro a descubrir el procedimiento que se ha seguido para hacerlo. En los métodos definidos como criptografía precientífica, en la mayoría de los casos, una persona inteligente y observadora puede ser capaz de llegar a encontrar la forma de resolverlos.

La tecnología orientada a descifrar mensajes encriptados es el cripto-análisis. Esta expresión fue acuñada por *William Frederick Friedman* en 1920. A partir de la Segunda Guerra Mundial, el desarrollo de la electrónica y las computadoras permitieron crear cripto-sistemas con algoritmos cada vez más sofisticados.

Los métodos para romper códigos y cifrados son mucho más antiguos. El primer trabajo documentado de cripto-análisis lo escribió el sabio árabe del siglo IX, *Abu-Yússuf Yaqub ibn Ishaq as-Sabbah al-Kindí*, en su Manuscrito para descifrar mensajes criptográficos. Este tratado incluye una descripción del método de análisis de frecuencias.

Figura 3
http://es.wikipedia.org/wiki/An%C3%A1lisis_de_frecuencias#/media/File:Al-kindi-cryptanalysis.png

En la actualidad la mayoría de gobiernos disponen de departamentos destinados de forma exclusiva al cripto-análisis. Es una tarea de contrarreloj permanente pues, existe una gran variedad de grupos organizados que cubren todo el espectro delictivo como terrorismo, narcotráfico, mafia, etc...

Técnicas de encriptado

Tal como hemos visto las técnicas de encriptado han ido evolucionando a lo largo del tiempo. Hasta llegar al periodo de criptografía asimétrica; la seguridad estaba íntimamente ligada a la confidencialidad. Esto quiere decir que uno de los elementos esenciales de esta seguridad dependía del conocimiento privado del método y las claves.

En todos los casos tenían que compartir la misma información tanto, quien generaba el mensaje como el que lo recibía. Esto a todas luces suponía una dificultad enorme, pues era muy difícil poder asegurar que en el trasporte del mensaje y las claves (aún que viajaran por caminos distintos) nadie pudiera interceptarlos.

César: Uno de los procedimientos más clásicos de la Historia en esta disciplina, cuyo origen se sitúa en el siglo I antes de Cristo. Este sistema se basa en el método de sustitución mono alfabética, es decir, el proceso de sustitución se lleva a cabo en cada uno de los elementos del texto claro.

Tranposición: Origen y fundamento de otros sistemas de cifrado más complicados. El método de trasposición consiste en reordenar los elementos que forman el texto original, de modo que el criptograma resultante tiene los mismos elementos pero su nueva colocación impide que se pueda entender.

Gronsfeld: Este método utiliza más de un alfabeto cifrado para poner en clave el mensaje y se cambia de uno a otro según se pasa de una letra del texto en claro a otra. Es decir, que deben tenerse un conjunto de alfabetos cifrados y una forma de hacer corresponder cada letra del texto original con uno de ellos.

DES: (Data Encryption Standard) fue desarrollado por IBM a mediados de los setenta. Aunque tiene un buen diseño, su tamaño de clave de 56 bits es demasiado pequeño para los patrones de hoy. DES es un mecanismo de cifrado de datos de uso generalizado. Hay muchas implementaciones de hardware y software de DES.

AES: (*Advanced Encryption Standard*), también conocido como *Rijndael*, es un esquema de cifrado por bloques adoptado como un estándar de cifrado por el gobierno de los Estados Unidos. Este sistema de cifrado por bloques permite claves de 128, 192 y 256 bits. El AES es uno de los algoritmos más populares usados en criptografía simétrica.

Cifrado exponencial: Es un sistema basado en la exponenciación modular, desarrollado por *Pohlig* y *Hellman* (1978). Este método es resistente al cripto-análisis.

Existen muchos más, como ejemplo y a modo de presentación, estos son de los más conocidos y representan a la mayoría. En general los distintos métodos y algoritmos en mayor o menor medida pueden considerarse variaciones notables de sus predecesores.

Clave púbica

Rivest, *Shamir* y *Adleman* desarrollaron en 1977, un sistema criptográfico de clave pública. 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. A este sistema se le conoce como RSA y es uno de los más utilizados en la actualidad.

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 en torno a 10^{200}, y se prevé que su tamaño crezca con el aumento de la capacidad de cálculo de los ordenadores.

Existe otro sistema criptográfico de clave pública, el *ElGamal* que está fundado en un esquema de cifrado basado en problemas matemáticos de logaritmos discretos. Es un algoritmo de criptografía asimétrica basado en la idea de *Diffie-Hellman* y que funciona de una forma parecida a este algoritmo discreto.

Al igual que el RSA, el algoritmo de *ElGamal* puede ser utilizado tanto para generar firmas digitales como para cifrar o descifrar. Fue descrito por *Taher Elgamal* en 1984 y se usa en *software* GNU *Privacy Guard*, versiones recientes de PGP, y otros sistemas criptográficos. Este algoritmo no está bajo ninguna patente lo que lo hace de uso libre.

En 1991, el *National Institute of standards and Technology* del EUA propuso un estándar de firma digital y solicito comentarios públicos para la adopción del estándar propuesto. El objetivo era que las oficinas gubernamentales norte americanas tuvieran una manera normalizada de firmar sus comunicaciones. El algoritmo que se aprobó era una variante del *ElGamal*. Este estándar se conoce como DSS.

A diferencia de cualquier técnica o método de los vistos hasta ahora, donde existe una simetría en el proceso de encriptado y des-encriptado (encriptado simétrico), la clave pública es un método de encriptado asimétrico. Esto significa que existen dos claves, la llamada clave pública y la clave privada. Estas dos claves están ligadas indivisiblemente ente sí, con la particularidad de que una de ellas se hace pública.

Lo que confiere la enorme importancia a este método de encriptado, es que en todos los casos un mensaje cifrado con la clave privada solamente se descifra con la llave pública y viceversa, el mensaje cifrado con la llave publica únicamente puede des-cifrarse con la llave privada. Esta singularidad es la que permite la existencia de los certificados digitales.

Firmas digitales

Una firma digital es un recurso criptográfico que asegura al receptor de un mensaje firmado digitalmente que este, ha estado creado por el remitente y que dicho mensaje no ha sido alterado desde que fue firmado por su creador. Se trata de un método criptográfico que asocia la identidad de una persona o de un equipo informático al mensaje o documento.

Es importante no confundir el término de firma electrónica o firma digitalizada con la firma digital. La firma digital se aplica en aquellas áreas donde es importante poder verificar la autenticidad y la integridad de ciertos datos, ya que proporciona una herramienta para detectar la falsificación y la manipulación del contenido.

La firma digital debe ser susceptible a verificación por terceras partes, de tal forma que dicha comprobación permita de manera simultánea, identificar al firmante y detectar cualquier cambio en el documento digital posterior a su firma. Es importante destacar que la firma digital tendrá idéntica validez a la firma manuscrita, siempre que esté debidamente autenticada por claves u otros procedimientos seguros de acuerdo con la tecnología informática.

Existen esquemas para generar firmas digitales con clave simétrica, aunque va quedado en desuso, debido a las ventajas y seguridad que aportan los esquemas basados en las claves asimétricas tanto en el concepto como el modo de operación.

Para firmar un mensaje, el remitente utiliza su llave privada y envía el mensaje acompañado de su llave pública. El destinatario del mensaje con la llave pública que acompaña al mensaje puede comprobar la autenticidad del mismo. Mediante estas operaciones, emisor y receptor pueden estar seguros que el mensaje no ha sido alterado durante la transmisión. La Integridad es un elemento indispensable.

El término de no repudio, significa que el usuario no puede negar que él realizó una transacción firmada digitalmente ya que solo él posee la clave privada con que se generó la firma digital y el mensaje está protegido por su clave que es única y complementaria a su misma clave pública.

Debido al esfuerzo computacional de cualquiera de los distintos algoritmos de clave pública, la firma digital de un mensaje en general, no se realiza sobre el documento completo, lo que se

hace es un resumen de longitud fija del mismo mediante un algoritmo de *hash* o huella digital. El contenido es ilegible y en ningún caso reversible, no son datos comprimidos.

Es posible que existan huellas digitales iguales para mensajes diferentes, porque una función *hash* es el resumen del mismo. Los algoritmos más utilizados son el SHA-1 y el MD5. En el caso del SHA-1 tiene 160 bits, y el MD5 128 bits, éste es bastante más rápido debido a que el número de pasos es menor. En cualquier caso los posibles objetos a resumir no tienen un tamaño límite.

El método más común de reafirmar el origen digital de los datos es a través de certificados digitales, se trata de una clave de infraestructura pública, la cual firma digitalmente la pertenencia. Ello puede usarse también para al encriptado. El origen digital solamente significa que el certificado o firma de los datos puede ser confiable por ser de alguien que posee la clave privada correspondiente al certificado firmado.

Certificados digitales

Un certificado digital es una estructura de datos que contiene información del propietario de las llaves criptográficas, la llave pública en sí y una firma digital de los dos campos anteriores que le dan validez. La firma realizada por un usuario o entidad externa leal, asegura la integridad contra una posible modificación no deseada de los datos. La confianza en el firmante se extiende al sujeto del certificado.

El certificado digital permite autentificar y garantizar la confidencialidad de las comunicaciones entre ciudadanos, empresas u otras instituciones públicas a través de las redes abiertas de comunicación. Se trata de un requisito indispensable para que las instituciones puedan ofrecer servicios seguros a través de Internet. Existen diferentes tipos de certificados digitales y distintas Autoridades de Certificación.

Por tratarse de un recurso basado en la confianza, se requiere de una Autoridad de Certificación (CA). Esta autoridad es la responsable de emitir y revocar los certificados. La entidad de confianza es la que aporta la legitimidad a la relación de una llave pública con la identidad de un usuario o servicio.

Aunque el núcleo básico de una autoridad de certificación es el par de claves criptográficas las autoridades de certificación suelen estar formadas por diversos subcomponentes o servicios, como el repositorio de certificados, el repositorio de claves, servicio seguro de historial (logs), entre otros.

También interviene la Autoridad de Registro (RA). Esta autoridad es la encargada de verificar el vínculo entre las claves públicas y la identidad de sus titulares. Un titular puede ser un Suscriptor, que es una persona física o una Entidad Final, que representa un a organismo o entidad propiamente dicha.

La información relativa a la infraestructura de clave pública se almacena en repositorios. Los dos repositorios más importantes de una infraestructura de clave púbica son: el repositorio de certificados y el de la lista de revocación de certificados (CRL). Una lista de revocación incluye

todos los certificados que por diversos motivos son inválidos antes de la fecha de caducidad de los mismos.

El encargado de comprobar la validez de los certificados digitales es la Autoridad de Validación (VA). Esta autoridad puede ser la propia autoridad de certificación o una entidad externa. Los certificados se emiten por un periodo de tiempo determinado, esta tarea recae en la Autoridad de Sellado de Tiempo (TSA). Esta parte es importante para dar cumplimiento a los servicios de no-repudio que tienen que poder establecer la existencia de los datos antes de un determinado momento.

Los métodos de certificación absolutos son imposibles, porque un certificado no puede certificarse a sí mismo. Para poder dar respuesta a esta situación se proponen distintos métodos: el modelo distribuido de confianza, el modelo plano, el modelo jerárquico, el modelo de navegación por lista de confianza y el modelo de certificado cruzado.

En el modelo distribuido de confianza, cada usuario crear un certificado que firma y distribuye a sus círculos de amistad. No ha de crearse ningún tipo de infraestructura central con una tercera entidad de confianza que de fe de la identidad de los usuarios.

El modelo plano, es el más sencillo de la infraestructura de llave púbica, que incluye a una única autoridad de certificación como tercera parte de confianza. Se trata de un certificado autofirmado donde el nombre del emisor y el titular del certificado es el mismo.

En el modelo jerárquico, los certificados de los suscriptores y las entidades finales están firmados por una entidad externa que también se identifica con certificados emitidos por una autoridad de certificación de jerarquía superior.

El modelo de navegación por lista de confianza, es un modelo centrado en el usuario, donde cada aplicación dispone de una lista de llaves públicas de todas las autoridades de certificación en que confía. Este es un modelo que se encuentra implantado en la mayoría de navegadores WEB. La ventaja de este modelo es que cada aplicación puede escoger el confiar en un amplio conjunto de autoridades de certificación.

Modelo de certificado cruzado, utilizado cuando el titular y el emisor son autoridades de certificación distintas. Este tipo de certificados se utilizan para que una autoridad de certificación pueda certificar la identidad de otra autoridad de certificación.

Conclusión

Desde el inicio de los tiempos han existido colectivos con necesidades de intercambio de información de forma privada, destacándose los de carácter militar. En los periodos distinguidos como era de la criptografía precientífica (Artística) y posteriormente en la era de la criptografía científica, los mensajes encriptados requerían del conocimiento de las claves y comprensión de los métodos utilizados para poderlos des-cifrar. Es lo que se conoce como criptografía simétrica.

A partir del año 1977, *Rivest*, *Shamir* y *Adleman* desarrollaron lo que se conoce como clave pública o criptografía asimétrica. Esta nueva tecnología marca un antes y un después en lo

concerniente al concepto de cifrado de mensajes, siendo lo más destacable las firmas digitales y los certificados digitales. Existen una amplia variedad de nuevas aplicaciones basadas y amparadas en las infraestructuras de clave pública; pero con todo hay que tener presente que la seguridad absoluta no existe.

Referencias

Las referencias a fecha de edición de este artículo son:

http://es.wikipedia.org/wiki/Historia_de_la_criptograf%C3%ADa#Criptograf.C3.ADa_cl.C3.A1sica

http://es.wikipedia.org/wiki/Atbash

http://www.hezkuntza.ejgv.euskadi.eus/r43-573/es/contenidos/informacion/dia6_sigma/es_sigma/adjuntos/sigma_24/9_Criptografia_clasica.pdf

http://www.dma.fi.upm.es/java/matematicadiscreta/aritmeticamodular/cesar.html

http://www.livius.org/person/polybius/

http://redyseguridad.fi-p.unam.mx/proyectos/criptografia/criptografia/index.php/2-tecnicas-clasicas-de-cifrado/22-opereraciones-utilizadas/222-algoritmos-de-sustitucion?showall=&start=3

http://serdis.dis.ulpgc.es/~ii-cript/PAGINA%20WEB%20CLASICA/CRIPTOGRAFIA/POLIALFABETICAS/Cifra%20playfair.htm

http://es.wikipedia.org/wiki/Cifrado_de_Alberti

http://www.mateureka.it/notizie/grafometro-incertezza-dimensionale-disco-cifrante-le-nuove-acquisizione-del-mateureka.html

http://es.wikipedia.org/wiki/Historia_de_la_criptograf%C3%ADa#Criptograf.C3.ADa_cl.C3.A1sica

http://www.eldiario.es/turing/criptografia/alan-turing-enigma-codigo_0_226078042.html

http://es.slideshare.net/jofaan/diapositiva-criptografia

http://digital.csic.es/bitstream/10261/24545/1/Flujo_1.pdf

http://es.wikipedia.org/wiki/Criptoan%C3%A1lisis

http://e-archivo.uc3m.es/bitstream/handle/10016/6173/PFC_Patricia_Xifre_Solana.pdf?sequence=1

http://en.wikipedia.org/wiki/Al-Kindi

http://es.wikipedia.org/wiki/An%C3%A1lisis_de_frecuencias

https://s3gur1d4d1nf0rm4t1c4.wordpress.com/2008/06/04/metodos-de-encriptacion/

http://en.wikipedia.org/wiki/RSA_%28cryptosystem%29

http://ca.wikipedia.org/wiki/Advanced_Encryption_Standard

http://en.wikipedia.org/wiki/Public-key_cryptography

http://es.wikipedia.org/wiki/Firma_digital#Propiedades_necesarias

http://www.upv.es/contenidos/CD/info/711545normalc.html

http://www.certificadodigital.com.ar/download/GUsuario.pdf

http://es.wikipedia.org/wiki/Sellado_de_tiempo