Criptografía

La criptografía (del griego κρύπτω krypto, «oculto», y γράφω graphos, «escribir», literalmente «escritura oculta») es la técnica, bien sea aplicada al arte o la ciencia, que altera las representaciones lingüísticas de un mensaje.

Objetivo

En esencia la criptografía trata de enmascarar las representaciones caligráficas de una lengua, de forma discreta. Si bien, el área de estudio científico que se encarga de ello es la Criptología.

Para ello existen distintos métodos, en donde el más común es el cifrado. Esta técnica enmascara las referencias originales de la lengua por un método de conversión gobernado por un algoritmo que permita el proceso inverso o descifrado de la información. El uso de esta u otras técnicas, permite un intercambio de mensajes que sólo puedan ser leídos por los destinatarios designados como 'coherentes'. Un destinatario coherente es la persona a la que el mensaje se le dirige con intención por parte del remitente. Así pues, el destinatario coherente conoce el discretísimo usado para el enmascaramiento del mensaje. Por lo que, o bien posee los medios para someter el mensaje criptográfico al proceso inverso, o puede razonar e inferir el proceso que lo convierta en un mensaje de acceso público. En ambos casos, no necesita usar técnicas criptoanalíticas.

Un ejemplo cotidiano de criptografía es el que usamos cuando mandamos una carta. El mensaje origen queda enmascarado por una cubierta denominada sobre, la cual declara el destinatario coherente, que además conoce el proceso inverso para hacer público el mensaje contenido en el sobre.

Hay procesos más elaborados que, por decirlo de alguna manera, el mensaje origen trata de introducir cada letra usada en un 'sobre' distinto. Por

ejemplo, la frase 'texto de prueba', pudiera estar representada por la siguiente notación cifrada: CF, F0, 114, 10E, 106, 72, F3, F6, 75, 10C, 111, 118, FB, F6, F5. El 'sobre' usado es de notación hexadecimal, si bien, el cálculo hexadecimal es de acceso público, no se puede decir que sea un mensaje discreto, ahora, si el resultado de la notación hexadecimal (como es el caso para el ejemplo) es consecuencia de la aplicación de un 'método' de cierre del 'sobre' (como lo es la cola de sellado, o el lacre en las tradicionales cartas), el destinatario debe de conocer la forma de abrirlo sin deteriorar el mensaje origen. En otras palabras, debe de conocer la contraseña. Para el ejemplo, la contraseña es '12345678'.

Conceptos

En la jerga de la criptografía, la información original que debe protegerse se denomina texto en claro o texto plano. El cifrado es el proceso de convertir el texto plano en un galimatías ilegible, denominado texto cifrado o criptograma. Por lo general, la aplicación concreta del algoritmo de cifrado (también llamado cifra) se basa en la existencia de una clave: información secreta que adapta el algoritmo de cifrado para cada uso distinto. Cifra es una antigua palabra arábiga para designar el número cero; en la Antigüedad, cuando Europa empezaba a cambiar del sistema de numeración romano al arábigo, se desconocía el cero, por lo que este resultaba misterioso, de ahí probablemente que cifrado signifique misterioso.

Las dos técnicas más sencillas de cifrado, en la criptografía clásica, son la sustitución (que supone el cambio de significado de los elementos básicos del mensaje (las letras, los dígitos o los símbolos) y la transposición (que supone una reordenación de los mismos); la gran mayoría de las cifras clásicas son combinaciones de estas dos operaciones básicas.

El descifrado es el proceso inverso que recupera el texto plano a partir del criptograma y la clave. El protocolo criptográfico especifica los detalles de

cómo se utilizan los algoritmos y las claves (y otras operaciones primitivas) para conseguir el efecto deseado. El conjunto de protocolos, algoritmos de cifrado, procesos de gestión de claves y actuaciones de los usuarios, es lo que constituyen en conjunto un criptosistema, que es con lo que el usuario final trabaja e interactúa.

Existen dos grandes grupos de cifras: los algoritmos que usan una única clave tanto en el proceso de cifrado como en el de descifrado, y los que emplean una clave para cifrar mensajes y una clave distinta para descifrarlos. Los primeros se denominan cifras simétricas, de clave simétrica o de clave privada, y son la base de los algoritmos de cifrado clásico. Los segundos se denominan cifras asimétricas, de clave asimétrica o de clave pública y forman el núcleo de las técnicas de cifrado modernas.

En el lenguaje cotidiano, la palabra código se usa de forma indistinta con cifra. En la jerga de la criptografía, sin embargo, el término tiene un uso técnico especializado: los códigos son un método de criptografía clásica que consiste en sustituir unidades textuales más o menos largas o complejas, habitualmente palabras o frases, para ocultar el mensaje; por ejemplo, "cielo azul" podría significar (atacar al amanecer). Por el contrario, las cifras clásicas normalmente sustituyen o reordenan los elementos básicos del mensaje (letras, dígitos o símbolos); en el ejemplo anterior, (rcnm arcteeaal aaa) sería un criptograma obtenido por transposición. Cuando se usa una técnica de códigos, la información secreta suele recopilarse en un libro de códigos.

Con frecuencia los procesos de cifrado y descifrado se encuentran en la literatura como encriptado y desencriptado, aunque ambos son neologismos erróneos (anglicismos de los términos ingleses encrypt y decrypt) todavía sin reconocimiento académico. Hay quien hace distinción entre cifrado/descifrado y encriptado/desencriptado según estén hablando de criptografía simétrica o asimétrica, pero la realidad es que la mayoría de los expertos hispanohablantes prefieren evitar ambos neologismos hasta el

punto de que el uso de los mismos llega incluso a discernir a los aficionados y novatos en la materia de aquellos que han adquirido más experiencia y profundidad en la misma.

Ideológicamente cifrar equivale a escribir y descifrar a leer lo escrito.

Historia de la criptografía

La historia de la criptografía es larga y abunda en anécdotas. Ya las primeras civilizaciones desarrollaron técnicas para enviar mensajes durante las campañas militares, de forma que si el mensajero era interceptado la información que portaba no corriera el peligro de caer en manos del enemigo. Posiblemente, el primer criptosistema que se conoce fuera documentado por el historiador griego Polibio: un sistema de sustitución basado en la posición de las letras en una tabla. También los romanos utilizaron sistemas de sustitución, siendo el método actualmente conocido como César, porque supuestamente Julio César lo empleó en sus campañas, uno de los más conocidos en la literatura (según algunos autores, en realidad Julio César no usaba este sistema de sustitución, pero la atribución tiene tanto arraigo que el nombre de este método de sustitución ha quedado para los anales de la historia). Otro de los métodos criptográficos utilizados por los griegos fue la escítala espartana, un método de trasposición basado en un cilindro que servía como clave en el que se enrollaba el mensaje para poder cifrar y descifrar.

En 1465 el italiano León Battista Alberti inventó un nuevo sistema de sustitución polialfabética que supuso un gran avance de la época. Otro de los criptógrafos más importantes del siglo XVI fue el francés Blaise de Vigenère que escribió un importante tratado sobre "la escritura secreta" y que diseñó una cifra que ha llegado a nuestros días asociada a su nombre. A Selenus se le debe la obra criptográfica "Cryptomenytices et Cryptographiae" (Luneburgo, 1624). Durante los siglos XVII, XVIII y XIX, el interés de los

monarcas por la criptografía fue notable. Las tropas de Felipe II emplearon durante mucho tiempo una cifra con un alfabeto de más de 500 símbolos que los matemáticos del rey consideraban inexpugnable. Cuando el matemático francés François Viète consiguió criptoanalizar aquel sistema para el rey de Francia, a la sazón Enrique IV, el conocimiento mostrado por el rey francés impulsó una queja de la corte española ante del papa Pío V acusando a Enrique IV de utilizar magia negra para vencer a sus ejércitos. Por su parte, la reina María Estuardo, reina de Escocia, fue ejecutada por su prima Isabel I de Inglaterra al descubrirse un complot de aquella tras un criptoanálisis exitoso por parte de los matemáticos de Isabel.

Durante la Primera Guerra Mundial, los alemanes usaron el cifrado ADFGVX. Este método de cifrado es similar a la del tablero de ajedrez Polibio. Consistía en una matriz de 6 x 6 utilizado para sustituir cualquier letra del alfabeto y los números 0 a 9 con un par de letras que consiste de A, D, F, G, V, o X.

Desde el siglo XIX y hasta la Segunda Guerra Mundial, las figuras más importantes fueron la del holandés Auguste Kerckhoffs y la del prusiano Friedrich Kasiski. Pero es en el siglo XX cuando la historia de la criptografía vuelve a experimentar importantes avances. En especial durante las dos contiendas bélicas que marcaron al siglo: la Gran Guerra y la Segunda Guerra Mundial. A partir del siglo XX, la criptografía usa una nueva herramienta que permitirá conseguir mejores y más seguras cifras: las máquinas de cálculo. La más conocida de las máquinas de cifrado posiblemente sea la máquina alemana Enigma: una máquina de rotores que automatizaba considerablemente los cálculos que era necesario realizar para las operaciones de cifrado y descifrado de mensajes. Para vencer al ingenio alemán, fue necesario el concurso de los mejores matemáticos de la época y un gran esfuerzo computacional. No en vano, los mayores avances tanto en el campo de la criptografía como en el del criptoanálisis no empezaron hasta entonces.

Tras la conclusión de la Segunda Guerra Mundial, la criptografía tiene un desarrollo teórico importante, siendo Claude Shannon y sus investigaciones sobre teoría de la información esenciales hitos en dicho desarrollo. Además, los avances en computación automática suponen tanto una amenaza para los sistemas existentes como una oportunidad para el desarrollo de nuevos sistemas. A mediados de los años 70, el Departamento de Normas y Estándares norteamericano publica el primer diseño lógico de un cifrador que estaría llamado a ser el principal sistema criptográfico de finales de siglo: el Estándar de Cifrado de Datos o DES. En esas mismas fechas ya se empezaba a gestar lo que sería la, hasta ahora, última revolución de la criptografía teórica y práctica: los sistemas asimétricos. Estos sistemas supusieron un salto cualitativo importante, ya que permitieron introducir la criptografía en otros campos que hoy día son esenciales, como el de la firma digital.

Encriptación de Datos

Como sabemos, en un Sistema de Comunicación de Datos, es de vital importancia asegurar que la Información viaje segura, manteniendo su autenticidad, integridad, confidencialidad y el no repudio de la misma entre otros aspectos.

Estas características solo se pueden asegurar utilizando las Técnicas de Firma Digital Encriptada y la Encriptación de Datos.

Métodos de encriptación

Para poder Encriptar un dato, se pueden utilizar tres procesos matemáticos diferentes:

Algoritmo HASH

Este algoritmo efectúa un cálculo matemático sobre los datos que constituyen el documento y da como resultado un número único llamado MAC. Un mismo documento dará siempre un mismo MAC.

Algoritmos Simétricos

Utilizan una clave con la cual se encripta y desencripta el documento. Todo documento encriptado con una clave, deberá desencriptarse, en el proceso inverso, con la misma clave. Es importante destacar que la clave debería viajar con los datos, lo que hace arriesgada la operación, imposible de utilizar en ambientes donde interactúan varios interlocutores.

Algoritmos Asimétricos (RSA)

Requieren dos Claves, una Privada (única y personal, solo conocida por su dueño) y la otra llamada Pública, ambas relacionadas por una fórmula matemática compleja imposible de reproducir. El concepto de criptografía de clave pública fue introducido por Whitfield Diffie y Martin Hellman a fin de solucionar la distribución de claves secretas de los sistemas tradicionales, mediante un canal inseguro. El usuario, ingresando su PIN genera la clave Pública y Privada necesarias.

La clave Pública podrá ser distribuida sin ningún inconveniente entre todos los interlocutores. La Privada deberá ser celosamente guardada. Cuando se requiera verificar la autenticidad de un documento enviado por una persona se utiliza la Clave Publica porque el utilizó su Clave Privada.

Firma Digital

El concepto de firma digital nació como una oferta tecnológica para acercar la operatoria social usual de la firma ológrafa (manuscrita) al marco de lo que se ha dado en llamar el ciberespacio o el trabajo en redes.

Es la transformación de un mensaje utilizando un sistema de cifrado asimétrico de manera que la persona que posee el mensaje original y la clave pública del firmante, pueda establecer de forma segura, que dicha transformación se efectuó utilizando la clave privada correspondiente a la pública del firmante, y si el mensaje es el original o fue alterado desde su concepción.

Las transacciones comerciales y el hecho de tener que interactuar masiva y habitualmente por intermedio de redes de computadoras le dieron lugar al concepto. Pero sólo después que los especialistas en seguridad y los juristas comenzaran a depurarlo alcanzó un marco de situación como para ocupar un lugar en las actuaciones entre personas (jurídicas o reales).

Se intenta hacer coincidir el modelo de firma digital con los requerimientos y virtudes que debe tener una firma y así darle validez a esta mecánica. El fin es el mismo de la firma ológrafa: dar asentimiento y compromiso con el documento firmado.

El papel es el medio de almacenamiento, y el mecanismo es alguno de los tipos de impresión posibles (tinta, láser, manuscrito, etc.). Esta cualidad física le da entidad al documento, contiene sus términos, conceptos y sentidos de una manera perdurable, y al ser un elemento físico cualquier alteración dejará “señales” identificables.

Pero estas mismas cualidades traen aparejados inconvenientes que el uso de sistemas de computación podría evitar. Ciertamente los papeles ocupan lugar y pesan demasiado, resulta complejo y molesto buscar información en ellos (requiriendo de la acción humana ya sea al archivarlos y/o al rescatarlos), y el compartir los documentos también resulta inconveniente.

Ventajas

- ✓ Integridad de la información: la integridad del documento es una protección contra la modificación de los datos en forma intencional o accidental. El emisor protege el documento, incorporándole a ese un valor de control de integridad, que corresponde a un valor único, calculado a partir del contenido del mensaje al momento de su creación. El receptor deberá efectuar el mismo cálculo sobre el documento recibido y comparar el valor calculado con el enviado por el emisor. De coincidir, se concluye que el documento no ha sido modificado durante la transferencia.
- ✓ Autenticidad del origen del mensaje*:* este aspecto de seguridad protege al receptor del documento, garantizándole que dicho mensaje ha sido generado por la parte identificada en el documento como emisor del mismo, no pudiendo alguna otra entidad suplantar a un usuario del sistema. Esto se logra mediante la inclusión en el documento transmitido de un valor de autenticación (MAC, Message autentication code). El valor depende tanto del contenido del documento como de la clave secreta en poder del emisor.
- ✓ No repudio del origen*:* el no repudio de origen protege al receptor del documento de la negación del emisor de haberlo enviado. Este aspecto de seguridad es más fuerte que los anteriores ya que el emisor no puede negar bajo ninguna circunstancia que ha generado dicho mensaje, transformándose en un medio de prueba inequívoco respecto de la responsabilidad del usuario del sistema.

Aspectos técnicos

A diferencia de la firma manuscrita, que es un trazo sobre un papel, la firma digital consiste en el agregado de un apéndice al texto original, siendo este apéndice, en definitiva, la firma digital; al conjunto formado por el documento original más la firma digital se lo denominará mensaje.

Este apéndice o firma digital es el resultado de un cálculo que se realiza sobre la cadena binaria del texto original.

En este cálculo están involucrados el documento mismo y una clave privada (que, generalmente, pertenece al sistema de clave pública-privada o sistema asimétrico) la cual es conocida sólo por el emisor o autor del mensaje, lo que da como resultado que para cada mensaje se obtenga una firma distinta, es decir, a diferencia de la firma tradicional, la firma digital cambia cada vez con cada mensaje, porque la cadena binaria de cada documento será distinta de acuerdo a su contenido.

A través de este sistema podemos garantizar completamente las siguientes propiedades de la firma tradicional:

- ✓ Quien firma reconoce el contenido del documento, que no puede modificarse con posterioridad (integridad).
- ✓ Quien lo recibe verifica con certeza que el documento procede del firmante. No es posible modificar la firma (autenticidad).
- ✓ El documento firmado tiene fuerza legal. Nadie puede desconocer haber firmado un documento ante la evidencia de la firma (no repudio).

Este sistema utiliza dos claves diferentes: una para cifrar y otra para descifrar. Una es la clave pública, que efectivamente se publica y puede ser conocida por cualquier persona; otra, denominada clave privada, se mantiene en absoluto secreto ya que no existe motivo para que nadie más

que el autor necesite conocerla y aquí es donde reside la seguridad del sistema.

Ambas claves son generadas al mismo tiempo con un algoritmo matemático y guardan una relación tal entre ellas que algo que es encriptado con la privada, solo puede ser desencriptado por la clave pública.

Resumiendo, la clave privada es imprescindible para descifrar criptogramas y para firmar digitalmente, mientras que la clave pública debe usarse para encriptar mensajes dirigidos al propietario de la clave privada y para verificar su firma.

Si bien no se trata de un tema estrictamente técnico, es conveniente aclarar que en tiempo de generación de cada par de claves, pública y privada, podría intervenir otra clave que es la de la Autoridad Certificante que provee la garantía de autenticidad del par de claves generadas, así como también, su pertenencia a la persona cuya propiedad se atribuye.

Este esquema se utiliza en intercambios entre entidades cuando se trata de transferencias electrónicas de dinero, órdenes de pago, etc. donde es indispensable que las transacciones cumplan con los requisitos de seguridad enunciados anteriormente (integridad, autenticidad y no repudio del origen), pero no se satisface el concepto de confidencialidad de la información (secreto).