Fundamentos del cifrado

Un repaso a la historia y la evolución de los algoritmos criptográficos y el descifrado

digicert®

Índice

Introducción

El cifrado empezó a utilizarse en el 3000 a. C., pero se ha vuelto aún más indispensable ahora que Internet cada vez está más presente en nuestras vidas y que el volumen de datos que circula online a diario crece sin parar.

La intrigante historia del cifrado y los algoritmos criptográficos ha estado marcada por la batalla constante entre quienes cifran los datos (los criptógrafos) y quienes los descifran (los criptoanalistas). Los sucesivos ciclos de desarrollo de algoritmos criptográficos siempre han ido acompañados de intentos de descifrar los existentes y, cuando alguien daba con la solución, se creaba un nuevo algoritmo para sustituir el antiguo.

Este documento hace un recorrido por la historia del cifrado y sus avances técnicos más destacados, además de explicar qué requisitos deben reunir los métodos modernos.

Cómo empezó todo

Los jeroglíficos, el sistema de escritura de los egipcios, son la forma de cifrado más antigua que se conoce. Datan del 3000 a. C., y hasta el siglo XIX se pensaba que eran indescifrables. Se consideran un tipo de cifrado porque muy poca gente sabía interpretarlos.

En torno al siglo VI a. C., en la antigua Grecia surgió un nuevo método criptográfico: la escítala espartana, una cinta de pergamino que se enrollaba alrededor de un bastón (véase la Figura 1). La cinta solo podía leerse si el destinatario tenía un bastón del mismo grosor.

Este tipo de método, en el que se cambia el orden de las letras, se conoce como cifrado por transposición.

Figura 1

En el siglo I a. C. se ideó el cifrado César, uno de los métodos más famosos, que usaba con frecuencia el emperador romano Julio César. Consistía en sustituir cada letra del mensaje original con otra situada un determinado número de posiciones más adelante en el alfabeto, información que solo conocían el emisor y el destinatario del mensaje.

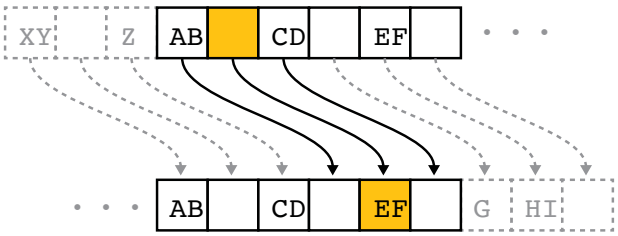

Figura 2

Este tipo de método, consistente en desplazar el abecedario un número de letras, se conoce como cifrado por desplazamiento.

Descifrar los mensajes es sencillo, pues basta con probar un máximo de 26 números, pero utilizar una permutación aleatoria permite obtener muchísimas más combinaciones (26 × 25 × 24 × .... = ¡40000000000000000000000000!), lo que complica el proceso.

Texto plano sin cifrar	ABCDEFGHIJKLMNOPQRSTUVWXYZ
Texto cifrado	SMKRATNGQJUDZLPVYOCWIBXFEH

Los métodos consistentes en modificar la secuencia de caracteres según una regla fija —como el del ejemplo anterior— se denominan «cifrado por sustitución». Es el tipo de cifrado más habitual a lo largo de la historia, y el utilizado, por ejemplo, en Enigma, una máquina de cifrado mecánica moderna en la que nos detendremos más adelante.

Sin embargo, todos los métodos por sustitución —incluido el cifrado César, más sencillo que otros— se pueden descifrar mediante el análisis de frecuencia, que recurre a parámetros lingüísticos para adivinar las letras precifradas según la frecuencia con que aparecen. Por ejemplo, en inglés:

- La letra «e» es la que se usa con más frecuencia (véase la Figura 3).
- La «q» siempre va seguida de una «u».
- Palabras como «any», «and», «the», «are», «of», «if», «is», «it» o «in» también son muy frecuentes.

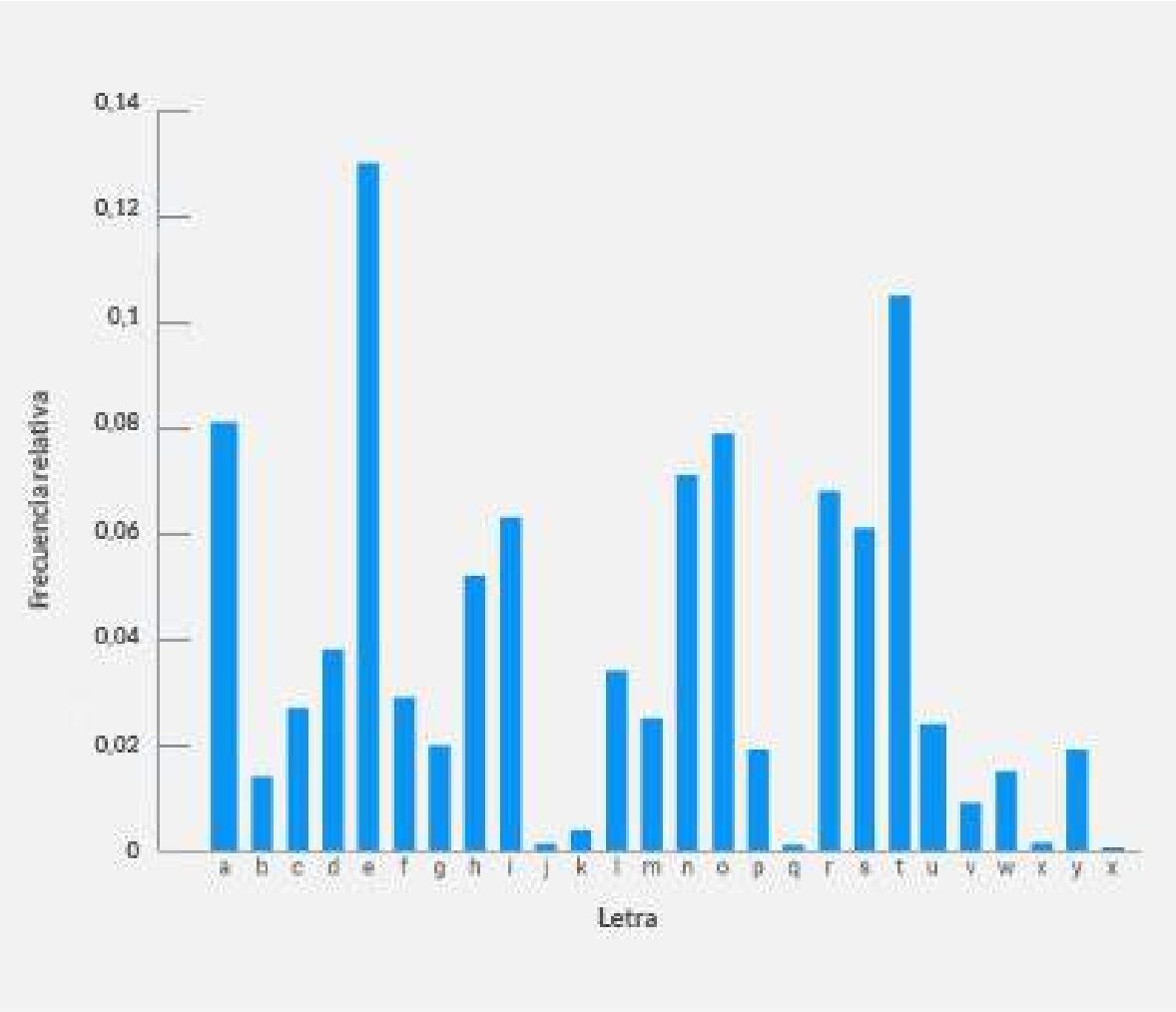

Figura 3

El renacer de la criptología

En la Edad Media, las técnicas criptográficas avanzaron notablemente debido al aumento de la actividad diplomática y del intercambio de información confidencial. Los códigos clásicos se descifraron y hubo que inventar otros nuevos.

El cifrado de María Estuardo

En el siglo XVI, María Estuardo y los conspiradores con los que se comunicaba utilizaban un «nomenclátor», sistema que, además de reemplazar letras del abecedario, sustituía frases con símbolos recogidos en un libro de códigos. Sin embargo, el sistema de sustitución de una letra por otra era rudimentario y llegó a descifrarse, razón por la cual María Estuardo fue ejecutada por traición en el castillo de Fotheringay, acusada de tramar el asesinato de la reina Isabel I de Inglaterra.

Texto plano	GOLDMEDALIST
Clave	OLYMPICOLYMP
Mensaje cifrado	UZJPBMFOWGEI

El cifrado de Vigenère

En el siglo XV, el italiano Leon Battista Alberti creó un prototipo para el cifrado de sustitución polialfabética (es decir, basado en varios alfabetos distintos) con el propósito de superar las deficiencias del cifrado por sustitución tradicional y poder compartir un libro de códigos de tamaño considerable. Luego surgirían otras variantes, incluida la definitiva y más eficaz, atribuida a Blaise de Vigenère: el cifrado de Vigenère, que usa una cuadrícula (el cuadro de Vigenère; véase la Figura 4) para cifrar el texto original (p. ej., «GOLD MEDALIST», medallista de oro) utilizando como clave otra palabra (p. ej., «OLYMPIC», olímpico). Aunque alguien se adueñe de la cuadrícula de conversión, le resultará muy difícil descifrar el mensaje sin conocer la clave.

	AB	CD	EF	GH	IJ	KL	MN	OP	QR	ST	UV	WX	YZ
A	AB	CD	EF	GH	IJ	KL	MN	OP	QR	ST	UV	WX	YZ
B	BC	DE	FG	HI	JK	LM	NO	PQ	RS	TU	VW	XY	ZA
C	CD	EF	GH	IJ	KL	MN	OP	QR	ST	UV	WX	YZ	AB
D	DE	FG	HI	JK	LM	NO	PQ	RS	TU	VW	XY	ZA	BC
E	EF	GH	IJ	KL	MN	OP	QR	ST	UV	WX	YZ	AB	CD
F	FG	HI	JK	LM	NO	PQ	RS	TU	VW	XY	ZA	BC	DE
G	GH	IJ	KL	MN	OP	QR	ST	UV	WX	YZ	AB	CD	EF
H	HI	JK	LM	NO	PQ	RS	TU	VW	XY	ZA	BC	DE	FG
I	IJ	KL	MN	OP	QR	ST	UV	WX	YZ	AB	CD	EF	GH
J	JK	LM	NO	PQ	RS	TU	VW	XY	ZA	BC	DE	FG	HI
K	KL	MN	OP	QR	ST	UV	WX	YZ	AB	CD	EF	GH	IJ
L	LM	NO	PQ	RS	TU	VW	XY	ZA	BC	DE	FG	HI	JK
M	MN	OP	QR	ST	UV	WX	YZ	AB	CD	EF	GH	IJ	KL
N	NO	PQ	RS	TU	VW	XY	ZA	BC	DE	FG	HI	JK	LM
O	OP	QR	ST	UV	WX	YZ	AB	CD	EF	GH	IJ	KL	MN
P	PQ	RS	TU	VW	XY	ZA	BC	DE	FG	HI	JK	LM	NO
Q	QR	ST	UV	WX	YZ	AB	CD	EF	GH	IJ	KL	MN	OP
R	RS	TU	VW	XY	ZA	BC	DE	FG	HI	JK	LM	NO	PQ
S	ST	UV	WX	YZ	AB	CD	EF	GH	IJ	KL	MN	OP	QR
T	TU	VW	XY	ZA	BC	DE	FG	HI	JK	LM	NO	PQ	RS
U	UV	WX	YZ	AB	CD	EF	GH	IJ	KL	MN	OP	QR	ST
V	VW	XY	ZA	BC	DE	FG	HI	JK	LM	NO	PQ	RS	TU
W	WX	YZ	AB	CD	EF	GH	IJ	KL	MN	OP	QR	ST	UV
X	XY	ZA	BC	DE	FG	HI	JK	LM	NO	PQ	RS	TU	VW
Y	YZ	AB	CD	EF	GH	IJ	KL	MN	OP	QR	ST	UV	WX
Z	ZA	BC	DE	FG	HI	JK	LM	NO	PQ	RS	TU	VW	XY

Figura 4

El cifrado Uesugi

En el Japón del siglo XVI se inventó un cifrado similar que también se basa en una cuadrícula de conversión. Se atribuye a Usami Sadayuki, asesor militar del señor feudal Uesugi Kenshin, quien creó una tabla de cifrado basada en un cuadrado o tablero de Polibio. Como el alfabeto tradicional japonés Iroha tiene 48 letras, se usaba una cuadrícula de 7 × 7, y cada símbolo se representaba con el número de la fila y la columna correspondientes (véase la Figura 5).

7	6	5	4	3	2	1	
we	a	ya	ra	yo	chi	i	1
hi	sa	ma	mu	ta	ri	ro	2
mo	ki	ke	u	re	nu	ha	3
se	yu	fu	wi	so	ru	ni	4
su	me	ko	no	tsu	wo	ho	5
n	mi	e	o	ne	wa	he	6
	shi	te	ku	na	ka	to	7

Figura 5

El cifrado en tiempos de guerra

Durante la Primera Guerra Mundial, el desarrollo de la comunicación moderna desembocó en un aumento vertiginoso de la criptografía y el criptoanálisis.

La ruptura de las comunicaciones alemanas

Cuando a principios de 1914 Gran Bretaña declaró la guerra a Alemania, cortó el cable submarino que constituía la línea de comunicación de esta última con ultramar. Así, el ejército alemán solo podría enviar información al extranjero por radio o por la línea de cable internacional controlada por Gran Bretaña. A partir de entonces, todas las comunicaciones interceptadas se enviaban a «Room 40», una unidad de criptografía del Almirantazgo Británico que se ocupaba de descifrarlas.

El telegrama de Zimmermann

Arthur Zimmermann, ministro de Asuntos Exteriores del Imperio Alemán, había ideado un plan para evitar que los Estados Unidos de América se unieran a los Aliados en la Primera Guerra Mundial: convencer a México y Japón de que atacaran a EE. UU. Room 40 descifró un telegrama en el que se explicaban estos planes al embajador alemán en México. Sin embargo, Gran Bretaña quería evitar que Alemania creara un nuevo tipo de cifrado aún más complejo, así que no hizo público el mensaje hasta que obtuvo su versión en texto plano. Cuando finalmente salió a la luz, Estados Unidos reaccionó declarando la guerra a Alemania.

Cifrado ADFGVX

En 1918 empezó a utilizarse el cifrado ADFGVX, diseñado por el coronel del ejército alemán Fritz Nebel. Al igual que el cifrado Uesugi, empleaba un cuadrado de Polibio, con filas y columnas

encabezadas por las letras ADFGX. Cada letra de la cuadrícula se correspondía con dos letras cifradas, a las que luego se aplicaba un sistema de cifrado por transposición. Posteriormente, el cifrado ADFGX dio paso a la variante ADFGVX, con seis filas y seis columnas (véase la Figura 6).

	A	D	F	G	V	X
A	d	h	x	m	u	4
D	p	3	j	6	a	o
F	i	b	z	v	9	w
G	1	n	7	0	q	k
V	f	s	l	y	c	8
X	t	r	5	e	2	g

Figura 6

Si la clave fuera desechable, sería prácticamente imposible descifrar el código con esta cuadrícula, pero para que así fuera habría que compartir un gran número de claves, algo complicado en la primera línea de combate.

La era de Enigma

Con la llegada de las máquinas de cifrado mecánicas a principios del siglo XX, resultaba más fácil descifrar hasta los sistemas más complejos.

Un ejemplo es Enigma, una gama de máquinas portátiles y seguras inventada por el ingeniero alemán Arthur Scherbius en 1918. El ejército alemán pensaba que nadie había desentrañado aún su método de cifrado de la Primera Guerra Mundial, así que en principio consideró innecesaria la inversión que suponía adoptar la tecnología Enigma. Sin embargo, cambió de parecer cuando descubrió que no había sido así y que el trabajo de la inteligencia británica era uno de los principales motivos por los cuales había perdido la guerra.

La máquina Enigma utilizaba un sistema de cifrado de sustitución polialfabética. Contenía varios rotores (o «scramblers») con las 26 letras del alfabeto y un cuadro de conexiones que llevaba a cabo conversiones individuales de caracteres alfabéticos. Por cada letra que se tecleaba, el rotor avanzaba una posición, lo que permitía cifrar y descifrar mensajes fácilmente con una clave que cambiaba con cada letra.

Ante la amenaza de invasión por parte de Alemania, Polonia inventó su propia máquina de cifrado, llamada Bombe, pero dadas las mejoras constantes de Enigma y la posibilidad de crear cada vez más patrones de cifrado, para Polonia no resultaba rentable seguir adelante con el trabajo de criptoanálisis. En 1939, dos semanas antes de que estallara la Segunda Guerra Mundial, Polonia pasó los resultados de sus estudios y su labor de descifrado a Gran Bretaña. Con esta información, Gran Bretaña consiguió descifrar el patrón del ejército alemán para Enigma y por fin se descubrió el código Enigma.

La información alemana obtenida al descifrarlo, conocida como «Ultra», siguió siendo un recurso importante para los Aliados hasta el final de la guerra. Sin embargo, se mantuvo el secreto para que Alemania siguiese usando Enigma con total confianza. Hasta 1974 no fue de dominio público el hecho de que el código Enigma había sido descifrado.

El comienzo de la era informática

Desde la Segunda Guerra Mundial, los instrumentos utilizados para el cifrado y el descifrado han cambiado: en lugar de máquinas mecánicas, ahora son computadoras. Debido a la rápida generalización de las computadoras en el sector privado, en esta época el cifrado se usa principalmente en transacciones comerciales corporativas, en el ámbito militar o de maneras que beneficien a la población en general.

El cifrado DES

En 1973, la Oficina Nacional de Estándares (NBS) del Ministerio de Comercio de los Estados Unidos, que luego pasaría a llamarse NIST (Instituto Nacional de Estándares y Tecnología), pidió propuestas para idear un sistema criptográfico de uso general que hiciera público el algoritmo de cifrado. En 1976, el NBS aprobó el estándar de cifrado de datos (DES), que posteriormente se convertiría en el cifrado estándar en el mundo.

Fue un momento clave en la historia de la criptografía, sobre todo en lo referente al cifrado para uso civil. Por fin las empresas disponían de una forma práctica y rentable de cifrar y descifrar la información confidencial con un método de criptografía simétrica (algo similar a lo que, en su día, había supuesto el cifrado César).

Cifrado de clave pública

Con la llegada del cifrado de clave pública, por fin se resolvió el único problema al que el cifrado César no había dado respuesta: cómo transmitir la clave. La criptografía de clave pública, presentada por primera vez en 1976 por Bailey Whitfield Diffie, Martin Hellman y Ralph Merkle, facilita las comunicaciones cifradas sin necesidad de distribuir las claves de antemano. Para ello, se emplean dos claves: una pública a la que cualquier persona tiene acceso (la que se utiliza para cifrar los datos) y otra privada que solo conoce el destinatario (la que sirve para descifrarlos).

El concepto de intercambio de claves Diffie-Hellman-Merkle utiliza una función unidireccional (la llamada aritmética modular) para mantener en secreto una conversación que transcurre en un lugar público. Este invento revolucionario echó por tierra algo que hasta entonces se había considerado uno de los principios básicos de la criptografía: que el intercambio de claves tenía que hacerse en secreto.

Sin embargo, por aquel entonces aún no se había creado una función unidireccional que permitiera el cifrado asimétrico, con claves de cifrado y descifrado distintas. Para que el cifrado de clave pública pasara de la teoría a la práctica, hubo que esperar a la invención del cifrado RSA.

El cifrado RSA

El método matemático que hizo realidad el concepto de clave pública según Diffie-Hellman fue desarrollado por tres investigadores del Instituto de Tecnología de Massachusetts: Ronald L. Rivest, Adi Shamir y Leonard M. Adleman. El nombre RSA viene, por cierto, de las iniciales de sus apellidos.

Antes de lanzarse el cifrado RSA, un criptógrafo británico ya había creado otro algoritmo de cifrado de clave pública, pero dado que los proyectos de esta naturaleza eran secreto nacional en el Reino Unido, la información no salió a la luz hasta 1997.

El cifrado RSA descompone un número dado en números primos. Estos, a su vez, se utilizan como clave pública y parte de la clave privada, como en este ejemplo:

95=5 × 19

851=23 × 37

176653=241 × 733

9831779=2011 × 4889

Debido a las características de esta factorización en números primos, sería sumamente difícil obtener la clave privada a partir de la clave pública en un plazo de tiempo realista, incluso aunque la clave pública fuera de fácil acceso. Así, se facilita el intercambio de claves de modo que solo el destinatario pueda descifrar el mensaje en Internet.

Un ejemplo es el protocolo TLS/SSL (Transport Layer Security/Secure Sockets Layer), que protege las comunicaciones entre un servidor web y un cliente. Netscape Communications lo ideó para integrarlo en Netscape Navigator, y su funcionamiento es el siguiente: en primer lugar, se emite un certificado electrónico que comprueba la identidad del servidor web o de correo; seguidamente, los mensajes se cifran con una clave simétrica (transmitida de forma segura gracias al cifrado de clave pública) para evitar que los datos se pierdan, sean interceptados o corran peligro de algún otro modo.

Alternativas al algoritmo RSA

1. **Algoritmo de firma digital**
   El algoritmo de firma digital (DSA) es un algoritmo de cifrado aprobado y certificado por el gobierno estadounidense. Fue creado por la agencia de seguridad nacional de EE. UU. en 1991, con la idea de reemplazar al algoritmo RSA de uso estándar en la actualidad. Está al mismo nivel que la tecnología RSA en cuanto a rendimiento y seguridad, pero utiliza otro algoritmo matemático para las operaciones de firma y cifrado. Un par de claves DSA tiene el mismo tamaño que la clave RSA equivalente. Los algoritmos DSA y el RSA son igual de seguros y tienen el mismo rendimiento, pero el RSA utiliza un algoritmo matemático menos común. Aunque el algoritmo DSA utiliza claves de igual longitud que el RSA, agiliza los procesos de creación de claves y firma digital. Su única desventaja es que la verificación de claves es algo más lenta.

2. **Criptografía de curva elíptica**
   La criptografía de curva elíptica (ECC) se basa en una estructura algebraica de curvas elípticas en campos finitos. Mientras que las claves RSA se basan en la intratabilidad matemática de descomponer un número entero grande en dos o más números primos, la criptografía de curva elíptica da por sentada la imposibilidad de encontrar el logaritmo discreto de un elemento de curva elíptica aleatoria con respecto a un punto base conocido públicamente. Desde el punto de vista de la criptografía actual, una curva elíptica es una curva plana definida por un conjunto de puntos que satisfacen la ecuación $y^2 = x^3 + ax + b$, junto con un punto específico del infinito (∞). Las coordenadas deben elegirse de un campo finito fijo de características que no sean 2 ni 3, ya que de lo contrario la ecuación sería algo más complicada. Todo esto, unido a la operación de grupo de la teoría de curvas elípticas, forma un grupo abeliano, con el punto del infinito como elemento de identidad. La estructura del grupo se hereda del grupo divisor de la variedad algebraica subyacente.

   En la RSA Conference de 2005, la agencia de seguridad nacional de EE. UU. (NSA) anunció Suite B, que utiliza exclusivamente la criptografía de curva elíptica (ECC) para generar firmas digitales e intercambiar claves. Con ello se pretende proteger la información y los sistemas de seguridad nacionales (clasificados o sin clasificar).

3. **Longitudes de clave recomendadas por NIST**
   El NIST (Instituto Nacional de Estándares y Tecnología) es una agencia federal estadounidense que «colabora con el sector para desarrollar y aplicar tecnologías, medidas y normas». Sus recomendaciones son parte de las normas que cumplen los navegadores web y las autoridades de certificación.
   Usar claves más pequeñas (en lugar de otras

Minimum size (bits) of Public Keys				Key Size Ratio
Security (bits)	DSA	RSA	ECC	RSA/DSA to ECC
112	2048	2048	N/A	1:09
128	3072	3072	256-383	1:12
192	7680	7680	384-511	1:20

igual de seguras pero más largas) aumenta el rendimiento del servidor y el número de conexiones simultáneas que es posible establecer, además de reducir el uso de CPU.

Un reto que no cesa

La clave DES tiene una longitud de 56 bits, así que podría haber unas 7×10^{16} combinaciones posibles (o 2 elevado a la 56.ª potencia). En principio, podría pensarse que algo así es imposible de descifrar, pero el gran aumento en la potencia de procesamiento permitió hacerlo en 1994.

De forma similar, el algoritmo criptográfico empleado en el protocolo TLS/ SSL tampoco es imposible de descifrar; simplemente es indescifrable en un plazo de tiempo realista y con un costo asumible dada la potencia de procesamiento de la que disponemos en la actualidad. Para que clave pública TLS/SSL no corriera la misma suerte que la clave DES, se dictaminó cambiar su longitud de 1024 bits a 2048 bits. Últimamente, las empresas también se han pasado al algoritmo SHA2 para la firma digital de claves públicas con tecnología TLS/SSL, en respuesta a la normativa aplicable al sector de pagos con tarjeta (PCI-DSS).

Los usuarios de comunicaciones cifradas mediante el protocolo TLS/SSL, por su parte, han tenido que actualizar los navegadores de sus computadoras, teléfonos móviles y otros dispositivos cliente, así como los navegadores web, para responder con más rapidez a los cambios en las funciones *hash* y la longitud de las claves. Sin embargo, tomar medidas que garanticen la eficacia del cifrado a largo plazo sigue siendo prioritario.

Por ejemplo, NIST se dio cuenta de las limitaciones de los certificados con claves RSA de 1024 bits utilizados en la tecnología TLS/SSL y dio orden de sustituirlos por certificados de 2048 bits antes de enero de 2014. Este cambio ayudó a combatir un amplio abanico de problemas de seguridad, ya que el aumento de la potencia informática y el desarrollo de nuevas técnicas habían hecho más frecuentes los ataques dirigidos a un tamaño de clave específico. Sin embargo, el cifrado RSA tampoco está exento de problemas: cuanto mayor es el tamaño de una clave RSA, mayor es la carga en el servidor y menos conexiones simultáneas es posible establecer. Otra opción es utilizar la criptografía de curva elíptica (ECC), que crea un par de claves (la pública y la privada) definiéndolas como si se tratara de puntos de una curva. Este sistema dificulta el robo de claves mediante ataques de fuerza bruta y, además, puede tratarse de una solución más rápida que consume menos capacidad de procesamiento que el cifrado basado en RSA.

Al igual que otros métodos criptográficos, el cifrado TLS/SSL solo seguirá siendo eficaz si los navegadores, servidores y certificados de servidor que lo usan avanzan a la par que la potencia criptográfica. Los usuarios y los proveedores deben ser conscientes de que, si no se toman medidas que garanticen una protección adecuada e ininterrumpida, las comunicaciones TLS/SSL acabarán descifrándose e Internet ya no será lo mismo.

La esperanza de un futuro mejor

Como hemos visto, la historia de la criptografía es un ciclo en el que la invención de un nuevo algoritmo va seguida de la creación de un nuevo método de descifrado. Otro gran hito dentro de esta evolución es la criptografía cuántica, que utiliza el ángulo de oscilación de un fotón para recibir los datos cifrados.

Otros métodos criptográficos son indescifrables «en un plazo de tiempo realista». Pero de la criptografía cuántica se dice que es imposible de descifrar, ya que si se interceptan los datos, cambia el ángulo de oscilación del fotón, lo que se detecta fácilmente.

Referencias

Simon Singh: «The Code Book»; Shinchosha Publishing Co., Ltd., 2001.

http://freemasonry.bcy.ca/texts/templars_cipher.html
http://www.nsa.gov/ia/programs/suiteb_cryptography/
http://www.nsa.gov/public_info/_files/cryptologic_spectrum/early_history_nsa.pdf

Si desea más información, envíe un mensaje a nuestros expertos en seguridad a contactus@digicert.com.

América

Lehi, Utah (Estados Unidos)
2801 North Thanksgiving Way, Lehi, Utah 84043, Estados Unidos

Mountain View, California (Estados Unidos)
485 Clyde Ave., Mountain View, California 94043, Estados Unidos

Asia Pacífico

Bangalore (India)
RMZ Eco World, 10th Floor, 8BCampus, Marathalli Outer Ring Road, Bangalore - 560103, India

Melbourne (Australia)
437 St Kilda Road, Melbourne, 3004, Australia

Tokio (Japón)
Ginza Six 8F, 6-10-1 Ginza Chuo-Ku, Tokio 104-0061, Japón

Europa, Oriente Medio y África

Nieuwegein (Países Bajos)
Nevelgaarde 56 Noord, 3436 ZZ Nieuwegein, Países Bajos

Ciudad del Cabo (Sudáfrica)
Gateway Building, Century Blvd & Century Way 1, Century City, 7441, Ciudad del Cabo, Sudáfrica

Dublín (Irlanda)
Block 21 Beckett Way, Park West Business Park, Dublín 12, D12 C9YE, Irlanda

San Galo (Suiza)
Poststrasse 17, San Galo, Suiza, 9000

Londres (Inglaterra)
2 Harbour Exchange Square, Suite 7.03, Londres, E14 9GE, Reino Unido

Malinas (Bélgica)
Schaliënhoevedreef 20T, 2800 Malinas, Bélgica

Múnich (Alemania)
Ismaninger Strasse 52, 81675 Múnich, Alemania

digicert®