



Suite-B: La nueva oleada de algoritmos criptográficos

EL CONTINUO INCREMENTO DE LA POTENCIA DE CÁLCULO DE LOS ORDENADORES
AMENAZA CONSTANTEMENTE LAS BASES SOBRE LAS QUE SE ASIENTAN LOS SISTEMAS
CRIPTOGRÁFICOS ACTUALES



Rames Sarwat

DIRECTOR GENERAL
SMART ACCESS

Realmente no se trata de una suite de hotel, ni de un conjunto de productos de segunda categoría. Suite-B es lo último en algoritmos criptográficos, y aunque algunos de estos algoritmos existen desde hace más de dos décadas es ahora cuando comienzan a aparecer productos comerciales que los implementan y clientes que los demandan.

La base de todo sistema criptográfico es un difícil problema matemático que se considera irresoluble computacionalmente hablando. Si analizamos la situación actual de los algoritmos criptográficos nos encontramos con la siguiente situación:

- La criptografía de 40 bits, que tradicionalmente estaba sujeta al control de exportación del gobierno de EEUU, se considera hoy trivial de romper.
- La criptografía de 56 bits se consiguió romper hace algunos años con inversiones inferiores a 300.000€

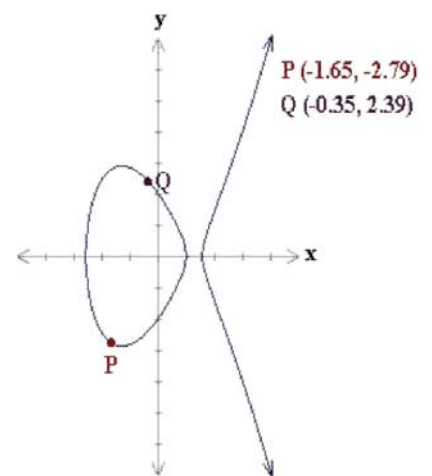
- Un *hash* 128-bits MD4, es equivalente a un algoritmo de clave simétrica de 64-bits, y ya ha sido roto.
- El *hash* 128 bits MD5 ha sido roto por un equipo chino.

Suite B es el nuevo conjunto de algoritmos criptográficos aprobados por la NSA como parte de su Programa de Modernización Criptográfica

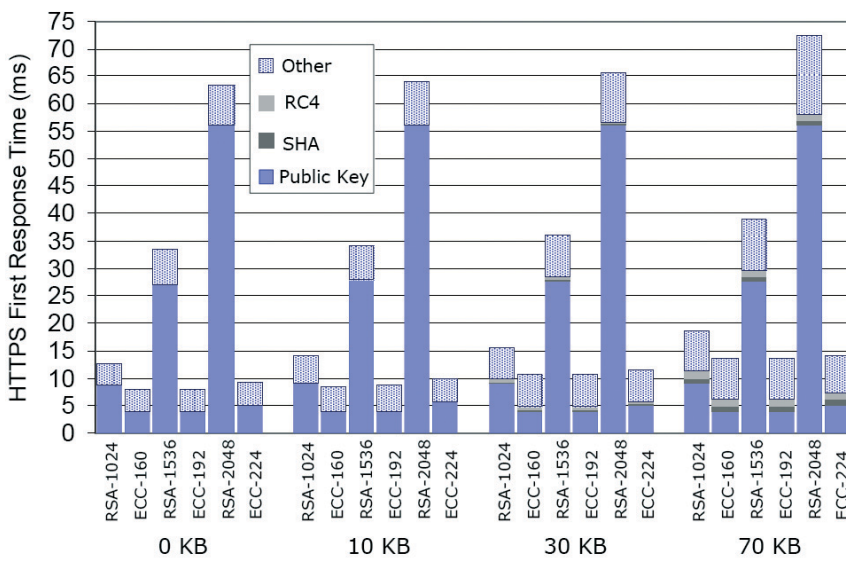
Hoy es muy frecuente ver que se aplica la criptografía de 80 bits, pero incluso ésta tiene un tiempo de vida limitado debido a que el algoritmo de *hash* SHA-1 tiene sólo una fortaleza de 280; asumiendo que el atacante pueda obtener 240 pares de cifrado, RSA-1024 se considera equivalente a una fortaleza de 280. El NIST (National Institute of Standards and Technology de Estados Unidos - agencia federal dedicada a definir estándares y tecnología especialmente en el área de seguridad y criptografía) recomienda al resto de agencias

federales de EEUU que dejen de utilizar la criptografía de 80 bits como muy tarde en el año 2010, es decir en apenas 3 años.

¿Cuál es entonces la solución? Parece que los algoritmos empleados en los últimos años han dejado o dejarán en breve de ser seguros. El siguiente escalón lo representan el manejo de claves RSA de 2048, como las implementadas en el nuevo DNI Electrónico. El algoritmo RSA-2048 es equivalente en fortaleza a un algoritmo de clave simétrica de 112 bits pero a su vez requiere mucha más potencia de cálculo para realizar



Elliptic curve equation: $y^2 = x^3 - 5x + 4$



últimos 150 años. Sin embargo la criptografía de curva elíptica (ECC) fue inventada en el año 1985 por Neil Koblitz de la Universidad de Washington y Victor Miller que trabajaba en IBM, tan sólo 8 años después del algoritmo RSA. Estos algoritmos han sido estudiados durante los últimos 20 años y se les reconoce su fortaleza y estabilidad de sus fundamentos matemáticos. Es interesante apuntar también que ECC ha sido estandarizada por organismos como el ISO y el IETF.

Se han definido 3 curvas y tamaños de claves: P-256, P-384 y P-521 con longitudes de claves de 256, 384 y 521 bits respectivamente. Estas curvas equivalen a claves AES de 256, 192 y 128 bits respectivamente. En general ECC es equivalente en fortaleza a RSA pero requiere menos potencia de cálculo en sus operaciones. P-256 equivale a RSA-3072, P-384 equivale a RSA-7680 y P-521 equivale a RSA-15380. El rendimiento de ECC es también proporcional a la longitud de la clave elevada al cubo, pero al emplear claves más cortas su rendimiento mejora. P-256 es más rápido que RSA-2048.

En un estudio realizado por Sun Microsystems se puede apreciar la diferencia de tiempos de respuesta sobre la implementación de diversos algoritmos para el protocolo de comunicación SSL.

El continuo incremento de la potencia de cálculo de los ordenadores amenaza constantemente las bases sobre las que se asientan los sistemas criptográficos actuales. Muchos de los sistemas operativos actuales y restante software comercial ya incorporan estos algoritmos. Parece probable que asistiremos en los próximos 2 o 3 años a una rápida migración de los algoritmos RSA a esta nueva Suite-B, que realizarán operaciones criptográficas más robustas en un menor espacio de tiempo. ♦

las operaciones. Además el anteriormente mencionado NIST vuelve a recomendar que se dejen de emplear la criptografía de 112 bits como muy tarde en el año 2030. Aunque esto es sólo una estimación basada en la previsible evolución de la potencia computacional en los próximos años. Por tanto, **la progresión de uso de los algoritmos de RSA con claves cada vez mayores, no parece sostenible.** El tiempo y potencia de cálculo requeridos a medida que crecen la longitud de las claves crece vertiginosamente. El tiempo requerido para firmar es proporcional a la longitud de la clave elevada al cubo.

Como ejemplos de la potencia de cálculo necesaria apuntamos:

- Las operaciones RSA-2048 requieren 8 veces más tiempo que sus equivalentes RSA-1024
- RSA-2048 (3DES) equivale a clave de 112 bits
- RSA-3072 equivale a una clave de 128 bits (AES)
- RSA-7680 equivale a una clave de 192 bits (AES)
- RSA-15380 equivale a una clave AES de 256 bits

A pesar de este panorama que puede parecer desolador, existen algoritmos alternativos de mayor fortaleza, que requieren menor potencia de cálculo y que se encuentran disponibles de forma comercial en la

El continuo incremento de la potencia de cálculo de los ordenadores amenaza constantemente las bases sobre las que se asientan los sistemas criptográficos actuales

actualidad. Estos algoritmos se han denominado Algoritmos Suite-B e incluyen 3 grupos de algoritmos:

- La criptografía de Curva Elíptica - Elliptical Curve Cryptography (ECC)
- El protocolo de cifrado AES - Advanced Encryption Standard
- Algoritmos de *hash* SHA-2

Las curvas elípticas son entidades algebraico/geométricas que han sido estudiadas intensivamente durante los