Algoritmos Asimétricos

Johan Steven Leguizamon Mendez

3 Diciembre 2019

1 Introducción

Los algoritmos asimétricos o clave pública se caracterizan por usar una clave para encriptar y otra para desencriptar. Una clave no se derivará de la otra. Emplean longitudes de clave mucho mayores que los simétricos. La complejidad de cálculo que comportan los hace más lentos que los algoritmos de cifrado simétricos. Por ello, los métodos asimétricos se emplean para intercambiar la clave de sesión mientras que los simétricos para el intercambio de información dentro. Si el remitente usa la clave pública del destinatario para cifrar el mensaje, una vez cifrado, sólo la clave privada del destinatario podrá descifrar este mensaje, ya que es el único que la conoce. Por lo tanto, se logra la confidencialidad del envío del mensaje, nadie salvo el destinatario puede descifrarlo.

2 Diffie-Hellman

El algoritmo de Diffie-Hellman (en honor a sus creadores, Whitfield Diffie y Martin Hellman) permite acordar una clave secreta entre dos máquinas, a través de un canal inseguro y enviando únicamente dos mensajes. La clave secreta resultante no puede ser descubierta por un atacante, aunque éste obtenga los dos mensajes enviados por el protocolo. La principal aplicación de este protocolo es acordar una clave simétrica con la que posteriormente cifrar las comunicaciones entre dos máquinas.

3 RSA

Fue creado en 1978 por Ron Rivest, Adi Shamir y Len Adleman, del Instituto Tecnológico de Massachusetts (MIT); las letras RSA son las iniciales de sus apellidos, y es el sistema criptográfico asimétrico más conocido y usado. Se basaron en el artículo de Diffie-Hellman sobre sistemas de llave pública.

para aplicar una clave secreta el RSA implementa la ecuación exponencial modular dada por $S(C)=C^d(mod n), para un CZ entonces tendríamos que la complejidad computacional de tal evento$

4 DSA

El algoritmo de firma digital (DSA, Digital Signature Algorithm) emplea un algoritmo de firma y cifrado distinto al del RSA, aunque ofrece el mismo nivel de seguridad. Lo propuso el National Institute of Standards and Technology (NIST) en 1991 y fue adoptado por los Federal Information Processing Standards (FIPS) en 1993.

5 ElGamal

Es un algoritmo basado en el intercambio de claves Diffie-Hellman, y que fue descrito por Taher ElGamal en 1984. Este algoritmo se utiliza en GNU Privacy Guard, PGP, y otros sistemas criptográficos como la generación de firmas digitales. Es bastante similar a Diffie-Hellman, constando de tres partes importantes: el generador de claves, el cifrado y descifrado.

La seguridad del algoritmo se basa en que la función utilizada es de un sólo sentido y difícil de calcular en sentido contrario mediante un logaritmo discreto (al igual que en DH). El procedimiento de cifrado (descifrado) está basado en cálculos sobre un grupo cíclico cualquiera G.

Sea n el módulo usado, los procesos de cifrado y descifrado toman tiempos de O(log n)

6 Merkie-Hellman

Merkle-Hellman (MH) fue uno de los primeros criptosistemas de llave pública y fue inventado por Ralph Merkle y Martin Hellman en 1978. El algoritmo de Merkle-Hellman está basado en el problema de la mochila de decisión (un caso especial del problema de la mochila de optimización)

7 Criptografía de curva elíptica

Es el acrónimo del inglés Elliptic Curve Cryptography, y promete una seguridad más fuerte y mejor rendimiento con claves más cortas. Estas características lo hacen ideal para el ámbito móvil, con cada vez más dispositivos. Solo para comparar: una clave ECC de 256 bits ofrece la misma seguridad que una clave de 3072 bits.

Como la clave es más corta, se necesita menos potencia informática para obtener conexiones más rápidas y seguras, ideales para dispositivos portátiles como smartphones y tabletas. Además, pese a su novedad, Symantec incorpora los certificados raíz ECC desde hace más de 5 años, así que el certificado ECC funcionará en todo su sistema.

https://www.redeszone.net/2010/11/16/criptografia-algoritmos-de-cifrado-de-clave-asimetrica/ https://www.ecured.cu/Algoritmo$_a$*simétricohttps* : *//mariiss*15.*wordpress.com*/2012/11/1 *de* − *encriptacion* − *simetrica* − *y* − *asimetrica/*