Algoritmo asimétricos y sus funciones de encriptación y desencriptación

Michael Daniel Murillo López
Corporación Universitaria Minuto de Dios -UNIMINUTO
mmurillolo1@unimiuto.edu.co
Bogotá DC - Colombia

Resumen

Los algoritmos asimétricos son técnicas inteligentes que se usan para la protección de datos y son parte fundamental al momento de definir una seguridad de un sistema. Su uso ha permitido un gran niveles de seguridad donde es necesario garantizando privacidad e incluso anonimato. En los algoritmos asimétricos se usa un par de claves para el envío de mensajes. Las dos claves pertenecen a la misma persona que ha enviado el mensaje. Una clave es pública y se puede entregar a cualquier persona, la otra clave es privada y el propietario debe guardarla de modo que nadie tenga acceso a ella. Además, los métodos criptográficos garantizan que esa pareja de claves sólo se puede generar una vez, de modo que se puede asumir que no es posible que dos personas hayan obtenido casualmente la misma pareja de claves.

1. Introducción

Es un algoritmo que modifica los datos de un documento con el objeto de alcanzar algunas características de seguridad como autenticación, integridad y confidencialidad.

2. Que son las llaves publicas y privadas en los algoritmos asimétricos

Primero tienes que cargar el archivo de imagen desde su computadora usando el enlace de carga del menú del proyecto. Luego usando el comando 'includegraphics' podrás incluirlo en el documento. Con el entorno de figura y el comando de título podrás agregar un número y un título a la figura. Mira el código de la Figura 1 en esta sección para ver un ejemplo.

3. Tipos de Algoritmos Asimétricos

3.1. Diffie-Hellman

El algoritmo de intercambio de claves Diffie-Hellman fue publicado por primera vez en 1976 por Whitfield Diffie y Martin Hellman, aunque el algoritmo había sido inventado unos años antes por la agencia de inteligencia del gobierno británico GCHQ pero se mantuvo clasificado. En 2002, Martin Hellman sugirió que el algoritmo fuera renombrado como .[El] intercambio de claves Diffie-Hellman-Merkle.[en] reconocimiento de la contribución de Ralph Merkle a la criptografía de clave pública.

El algoritmo de intercambio de claves Diffie-Hellman resuelve el siguiente problema: Alice y Bob quieren compartir una clave secreta para, por ejemplo, un algoritmo de clave simétrica como DES o AES , pero solo pueden comunicarse a través de un canal inseguro que es escuchado por su adversario Eva. Es decir, todos los mensajes enviados entre Alice y Bob son observados por Eve.

Figura 1: Esta imagen se añadió en el menú Project.

En la figura siguiente se muestra un ejemplo de funcionamiento del protocolo Diffie-Hellman.

Los valores de “p” y “g” son públicos y cualquier atacante puede conocerlos, pero esto no supone una vulnerabilidad. Aunque un atacante conociese dichos valores y capturara los dos mensajes enviados entre las máquinas A y B, no sería capaz de averiguar la clave secreta. A continuación se muestra la información capturada por un atacante en el escenario de la Figura 46:

(ga mod p) = 8 → (5a mod 23) = 8
(gb mod p) = 19 → (5b mod 23) = 19

A partir de las ecuaciones anteriores, intentar calcular los valores de “a” y “b” es lo que se conoce como el problema del algoritmo discreto, un problema que se cree computacionalmente intratable y cuya notación es la siguiente:

a = log discg (ga mod p) = log disc 5 (8)
b = log discg (gb mod p) = log disc 5 (19)

Con los valores del ejemplo sí que es posible encontrar la solución, ya que se ha escogido un número primo “p” muy pequeño (p = 23), y se sabe que “a” y “b” son menores que “p” . Por lo tanto, para obtener los valores secretos en este ejemplo, un atacante tendría que probar sólo 22 posibles valores.

Por suerte, las implementaciones actuales del protocolo Diffie-Hellman utilizan números primos muy grandes, lo que impide a un atacante calcular los valores de “a” y “b” . El valor “g” no necesita ser grande, y en la práctica su valor es 2 ó 5. En el RFC 3526 aparecen publicados los números primos que deben utilizarse. A modo de ejemplo, se facilita aquí el número primo de 1024 bytes propuesto. El valor “g” utilizado es 2:

p = 28192 – 28128 – 1 + 264 x ((28062 pi) + 4743158)

3.2. DSA

(Digital Signature Algorithm en español Algoritmo de Firma Digital) es un estándar del Gobierno Federal de los Estados Unidos de América o FIPS para firmas digitales. Fue un algoritmo propuesto por el Instituto Nacional de Normas y Tecnología de los Estados Unidos para su uso en su Estándar de Firma Digital (DSS), especificado en el FIPS 186. DSA se hizo publico el 30 de Agosto de 1991, este algoritmo como su nombre lo indica, sirve para firmar y no para cifrar informacion. Una desventaja de este algoritmo es que requiere mucho mas tiempo de computo que RSA.

3.3. Cifrado El Gamal

El procedimiento de cifrado/descifrado ElGamal se refiere a un esquema de cifrado basado en el problema matemático del logaritmo discreto. Es un algoritmo de criptografía asimétrica basado en la idea de Diffie-Hellman y que funciona de una forma parecida a este algoritmo discreto.

El algoritmo de ElGamal puede ser utilizado tanto para generar firmas digitales como para cifrar o descifrar.

Fue descrito por Taher Elgamal en 19841 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.

La seguridad del algoritmo se basa en la suposición que la función utilizada es de un solo sentido debido a la dificultad de calcular un logaritmo discreto.

3.4. Criptografía de curva elíptica

Es una variante de la criptografía asimétrica o de clave pública basada en las matemáticas de las curvas elípticas. Sus autores argumentan que la CCE puede ser más rápida y usar claves más

cortas que los métodos antiguos —como RSA— al tiempo que proporcionan un nivel de seguridad equivalente. La utilización de curvas elípticas en criptografía fue propuesta de forma independiente por Neal Koblitz y Victor Miller en 1985.

3.5. Criptosistema de Merkle-Hellman

Fue uno de los primeros criptosistemas de llave pública y fue inventado por Ralph Merkle y Martin Hellman en 1978.1 Aunque sus ideas eran elegantes, y mucho más simples que RSA, no tuvo el mismo éxito que este último, debido a que MH ya fue roto,2 y además no ofrece funcionalidades para firmar.

3.6. RSA

La idea de RSA se basa en el hecho de que es difícil factorizar un número entero grande. La clave pública consta de dos números donde un número es la multiplicación de dos números primos grandes. Y la clave privada también se deriva de los mismos dos números primos. Entonces, si alguien puede factorizar el gran número, la clave privada se ve comprometida. Por lo tanto, la fuerza del cifrado depende totalmente del tamaño de la clave y si duplicamos o triplicamos el tamaño de la clave, la fuerza del cifrado aumenta exponencialmente. Las claves RSA pueden tener típicamente 1024 o 2048 bits de largo, pero los expertos creen que las claves de 1024 bits podrían romperse en un futuro próximo. Pero hasta ahora parece ser una tarea inviable.

3 Objectivos de los algoritmos Asimétricos

es suministrar la dificultad máxima al proceso de desencriptar los datos sin utilizar la llave exacta garantías de seguridad de la información en el proceso que se implemente para asegurar la información que circula diariamente por ella, algo que es de suma importancia para los desarrolladores de sistemas pues de ésto depende la confiabilidad que se le ofrezca a los usuarios.

4 Conclusion:

Los Algoritmos Asimétricos son uno de los métodos para poder proteger tu información, forma parte de la seguridad informática que cada usuario puede tener, en la información anterior podemos observar que la Algoritmos Asimétricos tiene su historia, y mediante esta podemos observar las diferentes opciones que esta nos otorga para poder cuidar nuestra información, sin embargo, en este laboratorio, me intereso el tema de cifrar archivos con algoritmos complejos ya que logra una mayor confidencialidad.

Referencias

@miscWIkipedia:2019:Online, author = Varios Autores, title = Criptografía asimétrica, year = 2019, howpublished = ürlhttps://es.wikipedia.org/wiki/Criptografurldate = 01-12-2019