Cifrado de Llave Pública

Ing. Max Alejandro Antonio Cerna Flores

Agenda

Definición

Casos de Uso

    Cifrado

    Firma Digital

Desventaja

Definición

Es un sistema criptográfico en el que las claves vienen en pares.

Una clave (la clave privada) se mantiene secreta mientras que la otra se hace pública.

Es común que un sistema de cifrado utilice un algoritmo simétrico para cifrar el mensaje, y luego un sistema de clave pública para cifrar la clave simétrica.

Casos de Uso

Firmas digitales: la clave privada se usa para firmar y la clave pública para verificar.

Cifrado: la clave pública se utiliza para cifrar y la clave privada se utiliza para descifrar.

Los sistemas de cifrado de clave pública más utilizados son RSA (para firma y cifrado), DSA (para firma) y Diffie-Hellman (para acuerdo de clave).

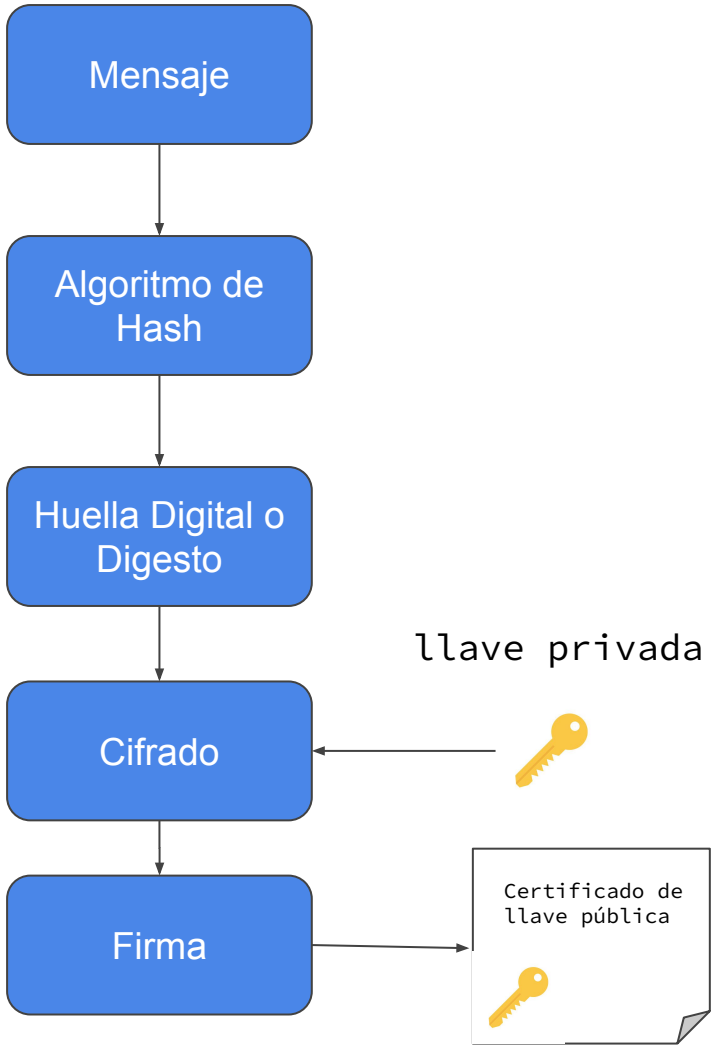
CIFRADO

Cualquier persona con una clave pública puede cifrar un mensaje, generando un texto cifrado, pero solo aquellos que conocen la clave privada correspondiente pueden descifrar el texto cifrado para obtener el mensaje original.

FIRMA DIGITAL

Un remitente puede usar una clave privada junto con un mensaje para crear una firma.

Cualquier persona con la clave pública correspondiente puede verificar si la firma coincide con el mensaje, pero un falsificador que no conoce la clave privada no puede encontrar ningún mensaje/firma que pase la verificación con la clave pública.



Desventaja

Suelen ser mucho más lentos que los algoritmos simétricos y el tamaño del mensaje que pueden cifrar es proporcional al tamaño de la clave, por lo que no se ajustan bien a los mensajes largos.

La mala elección de un algoritmo de clave asimétrica o una longitud de clave demasiado corta conlleva un riesgo de seguridad que es que se conozca la clave privada de un par.

Desventaja

Todos los esquemas de clave pública son, en teoría, susceptibles a un ataque de “fuerza bruta”.

Sin embargo, tal ataque no es práctico si la cantidad de computación necesaria para tener éxito, denominada "factor de trabajo" por Claude Shannon, está fuera del alcance de todos los atacantes potenciales.

Se puede aumentar la seguridad simplemente eligiendo una clave más larga.

Algoritmos de Cifrado de Llave Pública

Diffie-Hellman

RSA

DSA

SSL/TLS

Cifrado ElGamal

Cripto Sistema Kramer-Shoup

Funciones Hash

Curvas Elípticas

RSA

Significa Rivest, Shamir y Adleman quienes primero lo describieron públicamente.

Se conoce como el primer algoritmo apropiado tanto para firmar como para cifrar, y fue el primer gran avance en criptografía de llave pública.

Es utilizado extensamente en protocolos de comercio electrónico y se considera seguro dado a la longitud suficiente de las claves y del uso de implementaciones actualizadas.

DSA

Es un estándar para firmas digitales.

Un estándar del gobierno federal de los Estados Unidos para firmas digitales.

Es para firmas únicamente y no es un algoritmo de cifrado.

TLS/SSL

Transport Layer Security (TLS) y su predecesor, Secure Sockets Layer (SSL), son protocolos criptográficos que ofrecen seguridad para comunicaciones en redes como la Internet.

TLS y SSL cifran los segmentos de conexiones de redes en la capa de transporte de extremo a extremo.

Cifrado ElGamal

Es un algoritmo de cifrado de llave asimétrico para criptografía de llave pública basado en el acuerdo de llave Diffie-Hellman.

Fue descrito por Taher Elgamal en 1985.

Se utiliza en software libre de Guardián de Privacidad, GNU, versiones recientes de PGP, y otros cripto-sistemas.

Cripto Sistema Kramer-Shoup

Es un algoritmo de llave asimétrica y fue el primer esquema eficiente y seguro demostrado contra el ataque de texto de cifrado mediante supuestos estándares criptográficos.

Desarrollado por Ronald Cramer y Victor Shoup en 1998, es una extensión del criptosistema Elgamal.

Funciones Hash

Las funciones Hash tienen gran importancia, ya que se enfocan principalmente a solventar los problemas de la integridad de los mensajes, así como la autenticidad tanto de mensajes como de su origen.

Son funciones matemáticamente que se realizan el resumen de un documento a firmar, de manera que para ellos comprimen el documento en un único bloque de longitud fija, bloque cuyo contenido resulta ilegible y no tiene ningún sentido real.

Ejemplo: SHA-1, MD5, SHA-256

Curvas Elípticas

Es un tipo específico de criptografía de clave pública, que utiliza diferentes problemas matemáticos para generar una clave pública y otra privada con las que realizar operaciones. En el caso particular de las curvas elípticas, su utilización en algoritmos criptográficos fue propuesta por primera vez en 1985 por Victor Miller y Neil Koblitz.

En la actualidad, podemos encontrar curvas elípticas en protocolos como Bitcoin o Ethereum mediante el uso del algoritmo de firma digital ECDSA.