Criptografía de Clave Pública (PKC)

AB Orúe
Máster de Ciberseguridad

Características

La criptografía de clave pública resuelve la dificultad del intercambio de claves que presentan los métodos de criptografía de clave secreta. Se caracteriza por utilizar dos claves diferentes:

- Una clave pública: conocida públicamente, y cualquiera puede utilizarla para cifrar un mensaje destinado a su propietario.
- Una clave privada: guardada en secreto por su dueño y permite descifrar los mensajes que recibe.

Ambas claves están relacionadas entre sí, de tal modo que obtener la clave privada a partir de la clave pública supone resolver un problema matemático computacionalmente difícil.

Ejemplos de PKC

Los criptosistemas de clave pública más extendidos son:

- RSA (Rivest-Shamir-Adleman): Basado en la dificultad de resolver el problema de la factorización de números enteros grandes.[1]
- ElGamal: Basado en la dificultad de resolver el problema del logaritmo discreto.[2]
- Criptosistemas basados en curvas elípticas.

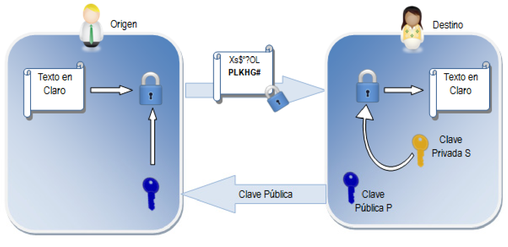

Figura 1: Protocolo de clave pública genérico

Intercambio de mensajes cifrados entre Alice y Bob:

- Alice selecciona la clave pública de Bob. Cifra el mensaje con la clave pública de Bob y lo envía.
- Bob recibe el mensaje cifrado y lo descifra usando su clave privada, solo conocida por él.

Ventajas y desventajas

Ventajas:

1. No necesita el establecimiento de una canal seguro para intercambiar la clave.
2. No aumenta del número de claves en una red.
3. Uso prolongado de la misma clave.
4. Permite el diseño fácil de protocolos de firma digital, autenticación, no repudio, integridad y confidencialidad.

Desventajas:

1. Operaciones de cifrado y descifrado lentos.
2. No es eficiente con grandes cantidades de datos.
3. Se necesitan claves de longitud larga (de 2048 a 4096 bits) para que sean seguras.
4. Las curvas elípticas de permiten usar claves más cortas para un nivel de seguridad.

Importante

El acceso a las claves públicas es fácil, lo que posibilita que un usuario conozca la clave de miles de usuarios, por lo que podría suplantarlo con relativa facilidad. La solución es firmar el mensaje, validando la pertenencia del par de claves mediante una autoridad de certificación que emita el certificado correspondiente.

Servicios de seguridad de la PKC

1. Confidencialidad: Cifrando la información solo el usuario autorizado con la clave correspondiente podrá descifrarla.
2. Autentificación: Identifica al usuario que ha enviado el mensaje.
3. Integridad: Garantiza que no se ha alterado el mensaje.
4. No repudio: Nadie excepto el emisor podría haber firmado el documento.

Los servicios de seguridad 2, 3 y 4 se alcanzan mediante la utilización de las firmas digitales. Estas últimas siempre estarán respaldadas por un infraestructura de clave pública (PKI).

Protocolo de envoltura digital

Combina la criptografía simétrica y asimétrica para alcanzar seguridad y eficiencia en las comunicaciones:
En el extremo de Alice:

1. Se cifra el mensaje m con una clave secreta k (clave de sesión) y se obtiene el criptograma c.
2. Se cifra la clave secreta k con la clave pública del destinatario y se obtiene K.
3. Se envía el criptograma c y la clave de sesión cifrada K.

En el extremo de Bob:

1. Descifra K con su clave privada y obtiene la clave k.
2. Descifra el criptograma c con la clave k y obtiene el mensaje m.

En la práctica

En la práctica se utiliza un sistema híbrido, parecido al protocolo de envoltura digital, dependiendo de lo que se necesite, si se quiere cifrar la información, se intercambia la clave y se acuerda un criptosistema de clave simétrica para cifrar/descifrar el mensaje.

Tamaño de claves vs Seguridad

Familia	Sistema	Niveles de seguridad (bits)			
Clave simétrica	Clave simétrica	**80**	**128**	**192**	**256**
Factorización enteros	RSA	1024	3072	7680	15360
Logaritmo discreto	DH, DSA, Elgamal	1024	3072	7680	15360
Curvas elípticas	ECDH, ECDSA	**160**	**256**	**384**	**512**

Figura 2: Comparación de los tamaños de clave para un nivel de seguridad dado

Conclusiones

El revolucionario concepto de la criptografía de clave pública fue primeramente descrito por Whitfield Diffie y Martín Hellman en 1976 [3]. Hoy en día no se concibe ninguna aplicación de seguridad que no incluya este tipo de criptosistema, por lo que su estudio es imprescindible para todo profesional preocupado por la seguridad de la información.

Nube de palabras

Figura 3: Nube de palabras relacionadas con los criptosistemas de clave pública

Referencias

[1] R. L. Rivest, A. Shamir, and L. Adleman.
A method for obtaining digital signatures and public-key cryptosystems.
Commun. ACM, 21(2):120–126, February 1978.

[2] T. Elgamal.
A public key cryptosystem and a signature scheme based on discrete logarithms.
IEEE Transactions on Information Theory, 31(4):469–472, Jul 1985.

[3] W. Diffie and M. Hellman.
New directions in cryptography.
IEEE Transactions on Information Theory, 22(6):644–654, Nov 1976.

Máster Ciberseguridad