VÍDEO intypedia003es

LECCIÓN 3: SISTEMAS DE CIFRA CON CLAVE PÚBLICA

AUTOR: Gonzalo Álvarez Marañón

Consejo Superior de Investigaciones Científicas, Madrid, España

BERNARDO

Hola, bienvenidos a intypedia. Conocidos ya los principios de los sistemas de clave secreta en la lección anterior, hoy analizaremos los fundamentos de la criptografía asimétrica o de clave pública. ¡Acompáñanos!

1. EL PROBLEMA DE LA DISTRIBUCIÓN DE LA CLAVE

ALICIA

Hola. Como vimos en la lección anterior, las comunicaciones utilizando criptografía simétrica o de clave secreta implican que la clave sólo la conocen el emisor y receptor del mensaje cifrado.

BERNARDO

Sí, y mi problema era cómo hacía para enviarle al destinatario la clave con la que había cifrado mi mensaje. Porque si es una persona a la que conozco y vive cerca, todavía podría quedar con ella y dársela en un pendrive. Pero si vive lejos o tuviera que enviar mensajes a muchas personas, entonces sería inmanejable.

ALICIA

Así es. Hasta mediados del siglo XX, muy pocos necesitaban realmente hacer uso de la criptografía: militares, diplomáticos y algunas empresas. Por eso tenían suficiente con la criptografía de clave simétrica. Podían gastar tiempo y dinero en distribuir las claves. Por

ejemplo los militares podían enviarlas custodiadas por soldados, los políticos podían protegerlas por fuerzas de seguridad y las grandes empresas podían contratar a agentes de seguridad.

BERNARDO

Perfecto, pero yo no puedo contratar un guardia jurado para enviarle la clave a mi amigo.

ALICIA

Claro, ahí está el problema. A finales del siglo XX cada vez era mayor la demanda del uso de la criptografía, por lo que resultaba necesario encontrar un mecanismo capaz de distribuir claves secretas de manera rápida, segura y al alcance de todos.

BERNARDO

Sí, yo ya me he encontrado con este problema. ¿Cómo enviar la clave secreta de forma segura a través de un canal inseguro?

ALICIA

Volvamos a los candados Bernardo. Pensemos en un sencillo candado con su llave. El candado representará el algoritmo de cifrado y la llave representará la clave de cifrado.

BERNARDO

Muy bien.

ALICIA

Con un candado pueden realizarse dos operaciones.

BERNARDO

Abrirlo y cerrarlo.

ALICIA

Exacto, hay una operación que la puede hacer fácilmente todo el mundo.

BERNARDO

Sí, cerrarlo. Basta con apretar el gancho hasta que haga clic.

ALICIA

Exacto. La otra operación sólo puede hacerla una persona.

BERNARDO

Abrirlo. Eso sólo lo puede hacer el que tenga la llave.

ALICIA

Todo el mundo sabe cómo cerrar el candado, basta con apretarlo, pero sólo una persona sabe cómo abrirlo, la que posea esa llave y no cualquier llave.

BERNARDO

¿Y cómo puedo enviar una clave secreta usando un candado?

ALICIA

Ahora sería muy sencillo. Imagínate que tienes la clave secreta escrita en un papel dentro de un sobre. Tu amigo tiene una caja como ésta para meterla dentro y también tiene un candado con su llave. ¿Cómo lo haríais para que tú pudieras enviarle tu clave secreta?

BERNARDO

¡Ya lo tengo! Le pediría a mi amigo que me mandase la caja junto con su candado abierto. Como todo el mundo sabe cómo cerrar un candado, yo metería dentro de la caja el sobre con mi clave secreta y cerraría el candado. De esta forma, solamente él, que es quien posee la llave, podrá abrirlo. Si alguien intercepta la caja, no podrá abrirla porque no posee la llave.

ALICIA

¡Bravo! Así es exactamente el fundamento de cómo funciona la criptografía de clave pública.

2. LA CRIPTOGRAFÍA DE CLAVE PÚBLICA

BERNARDO

Como es obvio Alicia, no usaremos candados para cifrar la información.

ALICIA

No, claro que no. Es una analogía que nos ayuda a comprender cómo funcionan los algoritmos de cifrado de clave pública. Se dispone de dos claves: una es pública y por tanto conocida por todo el mundo y la otra es privada y conocida solamente por su poseedor. Aunque cualquiera puede cifrar usando la clave pública, sólo el que posee la correspondiente clave privada podrá descifrar.

BERNARDO

Ahora veo la relación con el candado. Cualquiera puede cerrarlo, pero sólo puede abrirlo el que posea la llave.

ALICIA

Eso es. En este tipo de criptografía se utiliza una pareja de claves: una para cifrar y otra para descifrar. La clave pública debe ser conocida por todo el mundo, lo que facilita su distribución.

BERNARDO

Me interesa que todo el mundo la conozca. Así que puedo colgarla en mi página web, mandarla por correo electrónico o incluso escribirla en mi tarjeta de visita, ¿no?

ALICIA

Así es. Una vez que alguien conoce tu clave pública, puede enviarte mensajes cifrados con la seguridad de que nadie más que tú podrá descifrarlos, porque sólo tú posees la clave privada correspondiente a esa clave pública. Eso sí, la clave privada es muy importante que la mantengas en privado y sólo tú la conozcas. Nadie más.

BERNARDO

Ya entiendo. Por eso a la criptografía de clave pública se le llama también asimétrica, ¿verdad?

ALICIA

En efecto. Si cifras un mensaje con la clave pública no podrás descifrarlo usando esa misma clave pública. Necesitarás usar la clave privada. Lo que cifras con una clave, debes descifrarlo con la otra. Es lo que en matemática discreta se conoce como inversos, pero esos temas serán estudiados en otra lección.

BERNARDO

¿También puede cifrarse con la clave privada?

ALICIA

Sí, no hay por qué usar la clave pública sólo para cifrar y la privada, sólo para descifrar. También puede hacerse al revés.

BERNARDO

Un momento. Si cifro algo con mi clave privada, entonces cualquiera que conozca mi clave pública podrá descifrarlo. Y mi clave pública la puede conocer todo el mundo. Entonces, ¿qué sentido puede tener hacer una cosa así?

ALICIA

Ahí está la gracia: en que sólo tú puedes cifrar y todo el mundo puede descifrar.

BERNARDO

Pues yo sigo sin verle la gracia.

ALICIA

Como esa operación sólo puedes hacerla tú, lo interesante de esto es que entonces también puedes firmar un mensaje.

BERNARDO

¿Quieres decir que le estampo mi firma?

ALICIA

No, no esa clase de firma precisamente, más bien se trata de una firma digital. Si lo piensas bien, cifrar un mensaje con tu clave privada equivale a firmarlo porque nadie más que el poseedor de la clave privada podría haber cifrado ese mensaje.

BERNARDO

Ya entiendo. Cuando cifras algo con tu clave privada estás demostrando tu autoría: sólo tú puedes haberlo cifrado.

ALICIA

Eso es lo que se llama autenticación. Aunque cifrar con tu clave privada no proporciona confidencialidad al mensaje, es decir no le añade secreto, sí asegura la autenticación: sólo tú pudiste haberlo cifrado. Equivale por tanto a haberlo firmado.

BERNARDO

Y entonces cualquiera puede descifrarlo usando mi clave pública, lo que equivaldría a verificar mi firma.

ALICIA

Muy bien. Por eso es tan importante que tu clave privada sea privada o secreta y nunca la conozca nadie más que tú. En la práctica, debido a que los algoritmos de cifrado asimétrico son muy lentos, no suelen usarse para cifrar todo el mensaje, sino un resumen del mismo. Pero ya veremos en una próxima lección las funciones hash, las firmas digitales y cómo también proporcionan integridad a los mensajes.

BERNARDO

¿Y si un atacante descifra el mensaje que yo he cifrado con mi clave privada usando mi clave pública y luego lo cifra él o ella usando su clave privada, qué pasaría?

ALICIA

Cuando los destinatarios intenten verificar la firma tuya, o lo que es lo mismo descifrar usando tu clave pública, entonces se obtendrá un texto sin ningún sentido, porque no se puede descifrar un texto cifrado con una clave privada mediante una clave pública que no le corresponde. Es lo de los inversos que antes habíamos comentado.

BERNARDO

O sea, que cuando cifro algo con mi clave privada luego no puedo decir que yo no lo firmé.

ALICIA

Justo. No puedes negar haberlo firmado. Y esta propiedad del cifrado asimétrico se conoce como no repudio, ya que no podrás repudiar tus mensajes.

BERNARDO

Ya veo que es otra buena razón para mantener a salvo mi clave privada,

ALICIA

Nadie puede falsificar tu firma, siempre y cuando no conozca tu clave privada, claro. Así que ya sabes, mantenla siempre a buen recaudo.

BERNARDO

¿Cómo puedo guardarla de manera segura?

ALICIA

La pareja de claves debería guardarse por ejemplo en una tarjeta inteligente, como el DNI electrónico, aunque hay otras maneras de hacerlo.

BERNARDO

Hay algo que se me escapa: ¿cómo es posible que conociendo la clave pública no pueda descifrarse el mensaje cifrado con ella?

ALICIA

En un buen algoritmo de clave asimétrica el conocimiento de la clave pública no permite obtener ninguna información sobre la correspondiente clave privada ni descifrar el texto que con ella se ha cifrado. Para comprender cómo funcionan hay que entender primero qué son las funciones unidireccionales. En una próxima lección analizaremos este tema con detenimiento.

3. EL PROBLEMA DE LA CONFIANZA

BERNARDO

He estado reflexionando sobre el envío de mi clave secreta usando la clave pública del destinatario.

ALICIA

¿Sí?

BERNARDO

Y me ha surgido una duda. ¿Cómo sé yo que la clave pública de un usuario es en realidad la suya y no la de un atacante que la ha sustituido por la suya propia?

ALICIA

Muy perspicaz, Bernardo.

BERNARDO

Alguien podría haber interceptado la clave pública de mi amigo por el camino y haberla sustituido por la propia. Si envío mi clave secreta cifrada con esa clave pública, que en realidad es la del atacante, éste podrá descifrar sin problemas el mensaje y obtener mi clave secreta. Después podría volver a cifrarlo ahora sí con la clave pública legítima de mi amigo y mandársela. Ninguno de los dos nos daríamos cuenta de nada, mientras que el atacante se habrá hecho con la clave secreta y podrá descifrar los mensajes que cifremos con ella.

ALICIA

Muy bien, Bernardo, acabas de señalar un grave problema de la criptografía de clave pública. Lo que acabas de describir se conoce como ataque del hombre en el medio o por sus siglas en inglés man in the middle.

BERNARDO

¿Cómo puedo fiarme de que la clave pública de una persona es realmente suya y no de un impostor?

ALICIA

Es un problema de confianza. Igual que vimos lo difícil que era distribuir claves secretas de manera segura, veremos que es difícil distribuir claves públicas de manera fiable.

BERNARDO

¿Existe alguna solución?

ALICIA

Hoy en día se ha resuelto al menos parcialmente usando los certificados digitales y las infraestructuras de clave pública PKI.

BERNARDO

¿Cómo funcionan esas infraestructuras?

ALICIA

Todo eso lo veremos en próximas lecciones. Por hoy ya es suficiente. En la página Web de intypedia se encuentra documentación adicional a esta lección. ¡Adiós!

BERNARDO

¡Hasta la próxima lección!

Guión adaptado al formato intypedia a partir del documento entregado por el Dr. Gonzalo Álvarez Marañón del Consejo Superior de Investigaciones Científicas en Madrid, España.

Madrid, España, diciembre de 2010

http://www.intypedia.com

http://twitter.com/intypedia