INTRODUCCIÓN

INTRODUCCIÓN HISTÓRICA

Desde que el hombre es consciente de si mismo, e incluso desde antes, tiene la necesidad básica de comunicarse. De hecho la interrelación humana es una de las grandes bases del desarrollo actual. Pero es en los últimos tiempos cuando se le está dando a la comunicación la importancia que realmente tiene o en su defecto quizás se la valora demasiado. En cualquier caso, en nuestro tiempo, el valor de la comunicación queda patente y más con la aplicación de las nuevas tecnologías.

Una vez que el hombre se comunica también necesita tener una cierta privacidad en esa comunicación. Es decir, que únicamente el receptor o receptores a los que va dirigido el mensaje lo reciban.

Por lo que con esto comienza un nuevo aspecto en la comunicación, la parte que corresponde a la codificación de mensajes, encriptación, etc.

Desde tiempos antiguos se utilizan claves o códigos especiales para prevenir que personas que no son los destinatarios reales del mensaje puedan interferir e incluso modificar el contenido del mismo. Un claro ejemplo es la clave utilizada por Julio Cesar para transmitir mensajes que fueran ininteligibles cuando se interceptaran por sus enemigos. Consistía en cambiar cada letra del mensaje por la letra que estaba tres posiciones detrás en el abecedario. Por ejemplo la palabra PERRO quedaría codificada de la siguiente manera SHUUR. Pero claro esta clave es muy conocida, por lo que es totalmente inválida.

INTRODUCCIÓN A LA CRIPTOGRAFÍA

Pero no se habla de una clave, sino que los sistemas criptográficos están formados por un par de claves. Una de ellas es la que se usa para codificar el mensaje y la otra para descodificarlo. De esta forma el emisor solo tiene que conocer una clave y el receptor la otra, y el mensaje se descodificará solo con la clave apropiada. Desde este momento podemos diferenciar o hacer una primera clasificación:

- claves simétricas
- claves no simétricas

Las claves simétricas son aquellas en las que la clave que cifra y la clave que descifra son la misma. Por ejemplo, la clave utilizada por Julio César es simétrica ya que para cifrar había que rotar cada letra tres posiciones detrás en el abecedario, por lo que para descifrar había que rotar cada letra tres posiciones delante en el abecedario. Otros ejemplos basados en estos tipos de claves son los siguientes:

- claves matriciales,

cada cierto número de caracteres del mensaje se forma una fila de la matriz hasta completar el mensaje. Un vez formada la matriz se envía uno nuevo pero concatenando en este caso las filas. Un ejemplo sería el siguiente:

− mensaje: La casa es roja y verde.

− clave: 4

− matriz formada:

L	a		c
a	s	a	
e	s		r
o	j	a	
y		v	e
r	d	e	

− mensaje que se envía: Laeoyrassj dc r e

Para recuperar el mensaje bastaría con reconstruir la matriz por columnas, poniendo en cada columna un número de caracteres determinado, reconstruyendo el mensaje concatenando las filas. Para conocer la longitud de cada columna se utiliza el siguiente algoritmo:

− si el resto de la longitud del mensaje entre la clave es cero entonces el número de caracteres a poner en cada fila es el cociente de esta división.

− en caso contrario es el cociente más uno.

En nuestro ejemplo la longitud del mensaje recibido es 23 y la clave es 4, por lo que según lo anterior el número de caracteres por columna sería 5+1.

- claves matriciales desplazadas,

en este tipo de claves se conjunta la utilización de claves matriciales y de desplazamiento como la utilizada por Julio César. Para encriptar el mensaje se utilizaría primero uno de los dos métodos obteniendo un resultado al que se le aplicaría el otro método. Por este motivo la clave en este caso sería de un par de números, uno que indica la longitud de las filas de la matriz y el otro que indica el desplazamiento. Por ejemplo del caso anterior habíamos obtenido que el mensaje codificado era el siguiente.

Laeoyrassj dc r e,

por lo que al aplicarle un desplazamiento de 3 quedaría,

Ñdhrbudvvm gf u h

l clave sería pues el par (4,3).

También se podrían seguir anidando matrices y desplazamientos, es decir, crear un mensaje matricial desplazarlo, volver a crear otro mensaje matricial, etc. Pero esto conlleva la implementación de más código para descifrar el mensaje y el aumento de la clave simétrica.

Las claves no simétricas son aquellas en las que la clave con la que se cifra el mensaje, es distinta a la clave con la que se descifra el mensaje. Pero de este tipo de claves hablaremos más adelante.

AUTENTICACIÓN

¿QUÉ ES LA AUTENTICACIÓN?

En materia propiamente de autenticación lo que se pretende no es que se pueda leer el mensaje por personas ajenas, sino que se pueda asegurar la procedencia del mismo.

Todo esto no es nuevo ya que lo hemos estado utilizando desde muy antiguo:

- Los reyes de la edad media sellaban sus cartas lacrándolas y poniéndoles el sello en el lacrado.
- En mensajería usual (como CORREOS, empresas como SEUR, WRW,etc.) ponemos nuestra firma en cada envío.
- En las transferencias bancarias es necesario la firma de la persona que tiene la cuenta bancaria

Y por supuesto en materia de nuevas tecnologías también hay claros ejemplos:

- En los cajeros automáticos necesitamos una tarjeta identificadora y una clave de acceso a nuestra cuenta.
- En los accesos a los edificios de una cierta importancia como La Casa Blanca, el edificio central de la ONU en Bruselas, etc. muchas veces es necesario la posesión de una tarjeta identificadora y el siguiente escaneo de las huellas digitales.
- Y más cercano a nosotros es el acceso a sistemas unix en los que cada cuenta de usuario necesita un login y una clave de entrada.

Los objetivos que se pretenden con la autenticación en el envío de mensajes son los siguientes:

- certeza de que el mensaje procede la persona que dice remitirlo.
- se asegura de que ninguna persona ajena ha podido modificar el mensaje en cuestión.
- seguridad por parte del remitente de que el receptor no podrá modificar el mensaje, y decir que es el remitente el que escribió el mensaje.

FORMAS DE AUTENTICACIÓN

Por supuesto las distintas formas de autenticación deben ser únicas, deben ser capaces de distinguir a la persona de entre las demás. Las firmas escritas son las más usuales aunque hay falsificadores expertos en la copia de firmas. Los nombres y claves de acceso a sistemas informáticos pueden ser obtenidos casi fácilmente por otros usuarios gracias a la utilización de tecnologías como analizadores de red, funciones especiales en la implementación de las tarjetas de red, etc. Los accesos a edificios con escaneo de huellas digitales pueden producir la tentación de amputar los dedos a la persona que tiene acceso por parte de otras.

Con todo queda de manifiesto que es muy difícil asegurar la veracidad de la identidad de las personas. Para ello lo que se hace es complicar el sistema de autenticación, para hacer más difícil a los que intentan hacerse pasar por quienes no son el acceso a los lugares privados o personales. Por ejemplo los detectores de huellas digitales implementan demás detección de temperatura y pulso sanguíneo para evitar la amputación y robo de los dedos.

AUTENTICACIÓN INFORMÁTICA Y FIRMAS DIGITALES

En nuestro caso se trata de verificar la identidad de las personas que acceden a los sistemas informáticos o que envían mensajes electrónicamente. Para ello se utiliza la encriptación con todo su potencial.

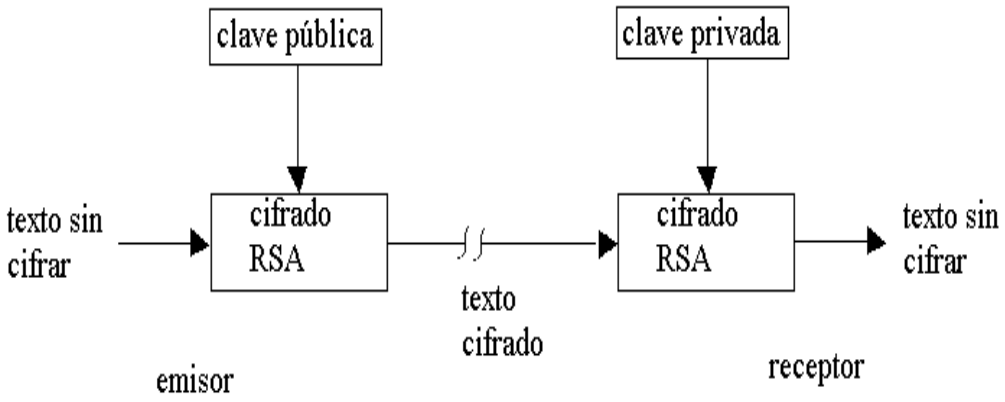
Para los mensajes o correos se utilizan las firmas digitales, que no es más que añadir al mensaje un pequeño texto cifrado

Como ya hemos dicho hay sistemas criptográficos con claves simétricas y con claves asimétricas. Nos vamos a centrar en las claves asimétricas que son aquellas que para cifrar utilizan una clave totalmente distinta que para descifrar.

CIFRADO Y AUTENTICACIÓN

El algoritmo más conocido de clave pública (asimétrica) es el RSA. Básicamente se trata de la generación de un par de números (claves), de tal forma que un mensaje cifrado con el primer número del par sólo podrá ser descifrado por el segundo número del par. Pero otra característica de este algoritmo es que la segunda clave no pude derivarse de la primera. Gracias a esto la primera clave podrá ser comunicada a cualquier persona que desee enviar un mensaje a la persona que tiene la segunda clave, sólo esta persona será capaz de descifrar el mensaje. Por esto a la primera clave se le llama clave pública y a la segunda clave privada.

El mecanismo del RSA se puede apreciar en la siguiente figura:



Este algoritmo se basa en la elección de un par de números primos P y Q que deben ser positivos y grandes, ya que cuanto más grandes sean más dígitos tendrá otro número llamado N, y más difícil será factorizar este N en un tiempo razonable. Algunos ejemplos son los siguientes:

- N=100 dígitos se tardaría una semana
- N=150 dígitos se tardaría 1000 años
- N>200 dígitos se tardaría 1 millón de años

Pero claro estos datos se quedan anticuados casi con el paso de los días. Es decir, no se puede asegurar que, debido al enorme desarrollo de las tecnologías informáticas, el computador más rápido actual, con el que se han sacado estos datos, no sea el más lento mañana.

Ahora bien, como el receptor, el que tiene la clave privada, sabe que el mensaje recibido es de quien dice ser, ya que la clave pública ha sido comunicada y por tanto un intruso la puede obtener con relativa facilidad. Es entonces cuando entra en juego la autenticación de los mensajes.

PROBLEMAS Y SOLUCIONES DE AUTENTICACIÓN

Otra característica importante del RSA se que un mensaje cifrado con clave pública se descifra con la clave privada, como ya sabemos, pero también se puede descifrar con la clave pública un mensaje cifrado con la clave privada.

Gracias esto podemos definir un sistema de claves de tal forma que el emisor tiene la clave pública del receptor y su propia clave privada, y el receptor tiene la clave pública del emisor y su propia clave privada. Por lo que para enviar un mensaje el emisor seguiría los siguientes pasos:

- cifrar el mensaje con su clave privada.
- cifrar el mensaje con la clave pública del receptor.

Y para recibir el mensaje el receptor seguirá los siguientes pasos:

- descifrar el mensaje con su clave secreta.
- descifrar el mensaje resultante con la clave pública del emisor.

Si el receptor ha sido capaz de realizar los dos pasos con éxito sabe con bastante seguridad que el emisor es quien dice ser y por tanto el mensaje se legítimo. Aunque todo este proceso requiere un elevado gasto de procesamiento, por lo que sólo será útil para volúmenes de datos relativamente pequeños. Todo este tiempo empleado en el procesamiento depende como siempre de las ordenadores y los circuitos integrados de ayuda a la realización de todos estos cálculos.

En nuestro caso solo tenemos que verificar las identidades de los emisores de los mensajes, así que este método es el idóneo.

De forma similar lo que se suele hacer es una especie de código redundancia al mensaje que es lo que se cifra y toma el nombre de firma digital. Una vez hecho esto se envía el mensaje seguido de su código de redundancia cifrado. El receptor descifrará sólo la firma digital y hará el código de redundancia al mensaje de nuevo comparando los resultados de descifrar la firma digital y realizar la redundancia al mensaje. De esta forma se evita que el emisor rechace después el mensaje, porque en poder del receptor todavía permanece la firma cifrada con la clave privada del emisor que es el único que posee dicha clave.

Pero todo este sistema falla en cuanto que el emisor del mensaje puede, en ciertas circunstancias, decir que no ha sido él el que envió el mensaje, estas circunstancias son las siguientes:

- Si una vez enviado el mensaje el emisor hace pública su clave privada, el receptor nunca podrá demostrar que fue emisor quien envió el mensaje ya que la clave la podría haber utilizado cualquiera, incluso el receptor.
- Si el emisor cambia de clave después de enviar el mensaje, el receptor nunca podrá demostrar que fue el emisor quien envió el mensaje ya que la clave privada no es capaz de cifrar la firma del mensaje.

Cuando se habla de comunicaciones importantes como en negociaciones de contratos entre empresas, acceso a cuentas bancarias o acceso a sistemas informáticos de importancia, esto supone un enorme problema.

Esto es, imaginemos que una empresa envía un mensaje de pedido a otra por este sistema de autenticación, pero poco tiempo después la empresa que envía el pedido encuentra a otra empresa más barata. Entonces si alega que han robado en sus oficinas centrales y lo denuncia a la policía, la empresa que había recibido jamás podrá demostrar ante un juez que la otra empresa había enviado el mensaje. La empresa para rechazar que había enviado el mensaje también podría haber, simplemente cambiado de clave. Es casi inimaginable el caos que podría llegar si mentes maliciosas utilizaran este sistema para estafar a las demás personas, como en la bolsa, banca , etc.

Por esto parece necesario la existencia de una autoridad que esté por encima de los emisores y receptores, y que controle el movimiento y cambio de las claves.

Esto sugiere un nuevo sistema de autenticación en el que hay una tercer participante en la comunicación que actuará como servidor de distribución de claves. Este servidor se encargará de que cada usuario tenga su clave privada y cuando un usuario quiera comunicarse con otro usuario gestionará el protocolo de comunicación. Este protocolo será el siguiente:

- el usuario 1 pide al centro servidor que escoja una clave de sesión y que le envíe dos copias de la misma. La petición se realiza con su clave y el envío de la clave de sesión con las claves del usuario 1 y el usuario 2.
- el usuario 1 envía al usuario 2 la segunda copia para que la descifre, diciéndole que la utilice como clave de

sesión.

REDES DE COMPUTADORES

AUTENTICACIÓN Y FIRMAS DIGITALES

– 7 –