(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 329 149**

(51) Int. Cl.:
H04L 9/08 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **05734559 .7**
(96) Fecha de presentación : **18.04.2005**
(97) Número de publicación de la solicitud: **1751911**
(97) Fecha de publicación de la solicitud: **14.02.2007**

(54) Título: **Método de cifrado y transferencia de datos entre un emisor y un receptor utilizando una red.**

(30) Prioridad: **24.05.2004 GB 0411560**

(45) Fecha de publicación de la mención BOPI:
23.11.2009

(45) Fecha de la publicación del folleto de la patente:
23.11.2009

(73) Titular/es: **Gcrypt Limited**
Enterprise House, 21 Buckle Street
London E1 8NN, GB

(72) Inventor/es: **Alculumbre, Michael**

(74) Agente: **Lazcano Gainza, Jesús**

DESCRIPCIÓN

Método de cifrado y transferencia de datos entre un emisor y un receptor utilizando una red.

La presente invención hace referencia a un método de cifrado y transferencia de datos entre un emisor y un receptor utilizando una red que da como resultado la transferencia de datos de manera segura.

Actualmente cada vez se envía más información sensible en formato electrónico de un emisor a un receptor. En dichas circunstancias, resulta más importante asegurar que la información no pueda ser interceptada ni leída por personas no autorizadas, es decir, la información debe transferirse de forma segura de manera que sólo emisor y receptor puedan tener acceso al contenido de la información.

En un caso, puede establecerse un enlace de conexión segura entre un emisor A y un receptor B antes de que se produzca la transferencia de datos. Sin embargo, en situaciones donde, por ejemplo, 10 personas individuales en una oficina desean comunicarse con y transferir información sensible entre ellas y a 10 personas de otra oficina remota en una forma de dos vías, existe la desventaja de tener que hacer ajustes adicionales de hardware y software para tantos enlaces de conexión segura. Además, esto conlleva recursos de tiempo y hardware considerable para mantener dichos enlaces y sus sistemas asociados de contraseñas. Esto es especialmente cierto cuando las personas de cada oficina están conectadas simultáneamente mediante alguna forma de Intranet o Ethernet y las oficinas se comunican a través de Internet. También es necesario tener un software de cifrado y descifrado en el emisor y el receptor, lo cual exige sistemas adicionales de hardware y software, y los costes asociados del mantenimiento especializado.

En otro caso, un emisor individual quiere transferir datos diferenciados a una pluralidad de receptores diferenciados. Sin embargo, esto tiene las mismas desventajas mencionadas anteriormente. En concreto, es necesario que el emisor establezca provisiones de seguridad complejas para mantener los sistemas de contraseñas seguros. Además, los sistemas adicionales de hardware y software deben establecerse para almacenar y mantener tales sistemas.

De hecho, en la era de los dispositivos pequeños y portátiles, como las PDAs, los teléfonos móviles con acceso a Internet y capacidad para emails, que tienen capacidad de procesamiento y memoria limitada, a menudo no resulta técnicamente posible tener la facilidad de conexiones seguras de dos vías donde se implican altos niveles de cifrado y descifrado.

Al tiempo que los certificados digitales pueden utilizarse para reducir la demanda sobre los recursos técnicos para emisor y receptor, implican un coste que a menudo no puede justificarse al receptor, aunque este coste sea pequeño.

Una alternativa es que el emisor cifre la información a transferir y luego envíe los datos cifrados sobre una red. Sin embargo, una vez más, el receptor debe tener recursos de procesado de hardware disponibles junto con la memoria para que el software correspondiente sea capaz de descifrar la información cifrada. Además, en situaciones donde el dispositivo del receptor tiene recursos de hardware relativamente pobres, asumir los recursos valiosos para permitir una transferencia segura de información a menudo no resulta posible.

El uso de técnicas complejas de cifrado y descifrado exige la instalación de software especial en el aparato del emisor y en el aparato del receptor. Esto es inconveniente y, además, resulta costoso. Es más, el procedimiento de instalación puede ser complejo y consume mucho tiempo, y puede provocar conflictos con otro software en su aparato correspondiente. Además, el software adicional puede exigir un nivel de capacidad de cálculo que no es viable en el aparato y puede ocupar un valioso espacio de memoria; esto es especialmente cierto en el caso de los dispositivos portátiles mencionados anteriormente.

De lo mencionado anteriormente queda claro que los métodos conocidos y los sistemas para la transferencia de datos de manera segura exigen una puesta en marcha considerable, al igual que un importante proceso informático y recursos de memoria local. Claramente esto no es adecuado para esas situaciones en las que emisor y/o receptor tienen un aparato con sólo una cantidad limitada de los recursos técnicos disponibles mencionados anteriormente.

Existe por tanto una necesidad para un método y sistema para transferir información de manera segura que pueda reducir el nivel de recursos técnicos exigidos por los aparatos del emisor y/o receptor. También, en el caso de que se utilice una clave de cifrado pública/privada, el emisor debe estar seguro de que la clave pública que cree que pertenece al receptor no haya sido sustituida por una clave pública de un intruso.

Las funciones de un método conocido para cifrar y transferir datos entre un emisor y un receptor utilizando una red se definen en la parte previa de las características de la reivindicación 1 y se conocen a partir de la US 2003/0172262 que describe un sistema seguro de comunicación para enviar datos desde un dispositivo del cliente a un receptor a través de un servidor seguro de distribución. El dispositivo del cliente cifra información utilizando una clave secreta y cifra la clave secreta utilizando una clave pública asociada con el servidor de distribución segura. La información cifrada y la clave secreta cifrada junto con los datos del receptor se envían al servidor de distribución segura que descifra la clave secreta. El servidor de distribución segura cifra entonces la clave secreta descifrada con la clave pública del receptor pretendido para mostrar una clave secreta segura específica del receptor. Esto, junto con la información cifrada, se envía posteriormente al receptor.

Las funciones que caracterizan la presente invención se definen en la parte de características de la reivindicación 1.

Preferentemente, el método incluye además establecer un enlace de comunicación entre el emisor y el servidor y enviar dicho identificador del receptor al servidor.

En una realización, el método incluye además establecer el enlace de comunicación entre el emisor y el servidor para que sea un enlace seguro.

En un caso, el método incluye además establecer el enlace de comunicación entre el emisor y el servidor sujeto que el servidor compruebe la contraseña del emisor.

En otra realización, el método incluye además establecer un enlace de comunicación entre el receptor y el servidor y enviar dicho identificador del receptor al servidor.

En un caso, el método incluye además establecer un enlace de comunicación entre el receptor y el servidor para que sea un enlace seguro.

En un caso particular, el método incluye además establecer el enlace de comunicación entre el receptor y el servidor sujeto a que el servidor compruebe la contraseña del receptor.

Preferentemente, el establecimiento de la clave de cifrado específica de transferencia tiene lugar en el emisor y la clave de cifrado específica de la transferencia establecida se envía al servidor.

En otro caso, el cifrado de datos utilizando la clave de cifrado específica de la transferencia se produce en el emisor.

En una realización concreta, el emisor recibe del servidor la clave de cifrado específica de transferencia cifrada y el emisor transfiere los datos cifrados y la clave de cifrado específica de transferencia cifrada al receptor sobre la red.

En otra realización, el receptor recibe del servidor la clave de cifrado específica de transferencia descifrada y el descifrado de los datos cifrados utilizando la clave de cifrado específica de la transferencia se produce en el receptor.

En otra realización, el establecimiento de la clave de cifrado de transferencia específica se produce en el servidor.

En otro caso concreto, cifrar los datos utilizando la clave de cifrado específica de transferencia se produce en el servidor.

En una realización, el servidor transfiere los datos cifrados y la clave de cifrado específica de la transferencia cifrada al receptor sobre la red.

En otra realización, descifrar los datos cifrados utilizando la clave de cifrado específica de la transferencia descifrada se produce en el servidor y el servidor transfiere la información cifrada al receptor.

Convenientemente, el método incluye además:

- establecer un valor de código de autenticación de mensaje (MAC) para los datos anteriores a la cifrado;

- transferir el valor MAC junto con los datos cifrados y la clave de cifrado específica de la transferencia; y

- establecer un valor MAC para los datos después del descifrado y validarlo frente al valor MAC transferido.

En una realización, el cifrado de la clave de cifrado específica de transferencia utiliza uno o más métodos de cifrado de clave pública, un algoritmo blowfish, código secreto del servidor.

Según otro aspecto de la presente invención, se proporciona un método de operar un servidor para cifrar y transferir datos entre un emisor y un receptor utilizando una red, el método incluye los siguientes pasos:

- recibir del emisor un identificador del receptor;

- acceder a la información específica del receptor según el identificador del receptor enviada por el emisor y cifrar, con la información específica del receptor, una clave de cifrado específica de transferencia que se utiliza para cifrar datos;

caracterizado por

- recibir del receptor la clave de cifrado específica de la transferencia y el identificador del receptor después de que los datos cifrados y que la clave de cifrado específica de la transferencia cifrada se hayan transferido por la red para que los reciba el receptor;

- acceder a la información específica del receptor según el identificador del receptor enviada por el receptor para descifrar la clave de cifrado específica de la transferencia cifrada.

En una realización, el método de operar un servidor incluye además establecer en el servidor una clave de cifrado específica de transferencia específica a la transferencia.

En otra realización, el método para operar un servidor incluye además recibir del emisor una clave de cifrado específica de la transferencia específica a la transferencia;

y transferir la clave de cifrado específica de la transferencia cifrada al emisor.

Preferentemente, el método de operar un servidor incluye además cifrar los datos en el servidor utilizando la clave de cifrado específica de la transferencia.

En otra realización preferente, el método de operar un servidor comprende además transferir los datos cifrados y la clave de cifrado específica de la transferencia cifrada sobre la red para que lo reciba el receptor.

Preferentemente, el método de operar un servidor incluye además transferir la clave de cifrado específica de transferencia descifrada al receptor.

En otra realización, el método para operar un servidor incluye además descifrar los datos cifrados en el servidor utilizando la clave de cifrado específica de la transferencia descifrada.

Según otro aspecto de la presente invención se proporciona un medio informático para un método de cifrado y transferencia de datos entre un emisor y un receptor utilizando una red, el medio incluye:

- código informático para recibir del emisor un identificador del receptor y establecer una clave específica de cifrado específica de la transferencia a la transferencia;

- código informático para cifrar los datos utilizando la clave de cifrado específica de la transferencia;

- código informático para acceder a la información específica del receptor según el identificador del receptor enviado por el emisor y cifrando, con la información específica del receptor, dicha clave de cifrado específica de la transferencia;

- código informático para transferir los datos cifrados y la clave de cifrado específica de la transferencia cifrada sobre la red para que la reciba el receptor;

caracterizada por

- el código informático para recibir del receptor la clave de cifrado específica de la transferencia cifrada y el identificador del receptor y para acceder a la información específica de receptor según el identificador del receptor enviado por el receptor para descifrar la clave de cifrado específica de la transferencia cifrada; y

- código informático para descifrar los datos cifrados utilizando la clave de cifrado específica de la transferencia descifrada;

Un ejemplo de la presente invención se describirá detalladamente con referencia a los dibujos adjuntos, donde:

La Figura 1 muestra un diagrama esquemático de un sistema que opera un método de la presente invención cifrando y transfiriendo datos entre un emisor y un receptor utilizando una red;

La Figura 2 muestra un diagrama en bloque esquemático de los módulos operativos del servidor utilizado en la figura 1;

La Figura 3 es un diagrama de flujo que muestra los procesos involucrados en el emisor y el servidor para la presente invención y enviar datos del emisor al servidor;

La Figura 4 es un diagrama de flujo que muestra los procesos involucrados en el receptor y el servidor en respuesta a un email recibido del servidor.

Con referencia ahora a las figuras 1 y 2, estas muestran un sistema que opera una realización de un método de cifrado y transferencia de datos entre un emisor y un receptor utilizando una red. Con referencia a los dibujos, el sistema funciona para cifrar y transferir datos entre un aparato emisor 100 y un aparato receptor 200.

En este ejemplo, el aparato emisor 100 comprende un ordenador 101 conectado a un teclado 107 y una fuente de datos 108 y un dispositivo de visualización externa 105. La fuente de datos puede incluir un lector de disco de algún tipo o una conexión de interfaz a una biblioteca de datos, la fuente de datos almacena los datos que vayan a transferirse al receptor. El ordenador 101 tiene un bus de acceso general 106 que se conecta a un microprocesador 102, una memoria 103, una interfaz de visualización 104, una interfaz de dispositivo de entrada 109 y un navegador web 110 para conectarse a Internet a través de una conexión 111.

La interfaz del visualizador 104 se conecta al dispositivo de visualización externa 105 mientras que la interfaz del dispositivo de entrada 109 se conecta al teclado 107 y la fuente de datos 108. La memoria 103 almacenará normalmente la identificación del emisor y la contraseña del emisor aunque estos puedan introducirse a través del teclado 107 en respuesta a los comandos de visualización en el dispositivo de visualización 105.

En este ejemplo, el aparato receptor 200 comprende un teléfono móvil que tiene una capacidad de Internet a través de un navegador web 210 que se conecta a Internet a través de una conexión 211.

Los datos sobre cómo se establece dicha conexión ya es muy conocida en el ámbito y no se describirá aquí. El navegador web se conecta a un bus de acceso general 206 que se conecta a un microprocesador 202, una memoria 203, una interfaz de visualización 204 y una interfaz de dispositivo de entrada 209. La interfaz de visualización 204 se conecta a un dispositivo de visualización integral 205 mientras que la interfaz del dispositivo de entrada 209 se conecta a un teclado integral 207. La memoria 203 almacenará normalmente la identificación del receptor y contraseña del receptor aunque estos pueden introducirse a través del teclado 207 en respuesta a los comandos de visualización en el dispositivo de visualización 205. El aparato 200 incluye además un cliente de email 212 para enviar y recibir emails a través de una conexión 213 a Internet.

Un servidor 300 también está conectado a Internet a través de una conexión 302. Un diagrama en bloque detallado de la estructura del servidor se muestra en la figura 2. Esta estructura del servidor se explicará en combinación con una descripción de la operación del sistema de la presente invención.

Con referencia a las figuras 1 y 2, antes del uso del sistema actual, tanto emisor como receptor se registran inicialmente con el servidor 300 y sus datos se almacenan en un módulo de la base de datos del servidor 306. En esta realización, la información almacenada incluye al menos una identificación y un contraseña para cada emisor y receptor.

El emisor desea transferir al receptor datos guardados en la fuente de datos 108. Para que el emisor transfiera los datos, el emisor tiene que conocer la identificación del receptor y la dirección web del servidor 300. Esta información puede almacenarse en la memoria 103 del emisor o puede introducirse manualmente a través del teclado 107 en respuesta a los comandos en el dispositivo de visualización 105.

Como se muestra en la figura 2, el servidor 300 incluye un servidor web 301 conectado a Internet a través de una conexión 302. El servidor web se conecta a un bus de entrada 303 y se controla por medio de un microprocesador 304. Cuando el emisor contacta con la dirección web del servidor, se establece un enlace seguro como un enlace SSL, cuyos datos son bien conocidos para los expertos en la materia. El microprocesador 304 no permite el acceso del emisor al sistema actual hasta que el módulo 305 haya completado una comprobación de contraseña junto con el acceso al módulo de la base de datos 306. Los datos de dichas comprobaciones de contraseña son muy conocidos en el ámbito y, por tanto, no se describirán aquí.

Tras la finalización de la comprobación del contraseña, el servidor 300 envía al emisor una visualización de la pantalla. Al completar esta pantalla, el emisor envía al servidor la identidad del receptor junto con los datos a transferir, que se obtienen de la fuente de datos 108. Estas entradas son activadas por los módulos hacia el borde superior de la figura.

Al recibir la identificación del receptor y los datos a enviar, el microprocesador 304 remite los datos a un módulo generador 307 de código de autenticación de mensaje (MAC). Como se conoce en la materia, dicho generador produce una parte de código que se calcula utilizando una parte o todos los datos en combinación con un algoritmo compendio criptográfico. En el caso actual, el conocido algoritmo hash MD se utiliza para generar un valor hash MD a partir de los datos. El valor hash MD se remite a un cliente de email 312 conectado a Internet a través de un enlace 316 de manera que pueda estar listo para procesar en una parte de un email.

Los datos recibidos se comprimen en un módulo 308 antes de que los cifre el módulo 309 utilizando una clave de sesión obtenida de un módulo 310. Como se conoce en la materia, la clave de sesión se genera a partir de un número aleatorio, proporcionada por un generador 311 de números aleatorios. Esta clave de sesión es específica para estos

datos y su transferencia, por tanto, se convierte en una clave de cifrado específica de transferencia. Los datos cifrados se remiten consecuentemente a un cliente de email 312 listo para procesar en una parte de un email.

La clave de sesión del módulo 310 también se cifra en el módulo 313 utilizando la clave pública de una técnica de cifrado de clave privada/clave pública, por ejemplo, el cifrado RSA, que es muy conocido en la materia. A partir de ahí, la salida desde el módulo 313 se cifra en el módulo 314 utilizando un algoritmo blowfish que incorpora la contraseña del receptor que se obtiene de la base de datos 306. Esta contraseña sale de acuerdo con la identificación del receptor remitido desde el microprocesador en el bus 315. La clave de sesión cifrada se remite al cliente de email 312 listo para procesar en una parte de un email.

El cliente email 312 procesa el valor hash MD, los datos cifrados y la clave de sesión cifrada de una manera conocida para crear un email que luego se envía a la dirección adecuada del receptor proporcionado por el microprocesador en el bus 315 después del acceso a la base de datos 306. De una manera conocida, el cliente email asigna una etiqueta única al correo electrónico y carga el envío. Una confirmación del envío del email también se envía al emisor utilizando el servidor web 301 o el cliente de email 312.

El mail que se envía por el servidor 300 puede recibirlo normalmente el cliente de email 212 del teléfono móvil 200. El contenido del mail se establece o bien para alertar al receptor sobre una transferencia de datos utilizando el sistema de la presente invención o bien activará automáticamente el navegador web 210 para iniciar un enlace de comunicación con el servidor 300. En cualquier caso, bajo el control del microprocesador 202, el receptor contacta la dirección web del servidor y un enlace seguro como se establece un enlace SSL, cuyos datos son bien conocidos para los expertos en la materia. El microprocesador el servidor 304 no permite el acceso al sistema actual hasta que un módulo 305 haya completado una comprobación de contraseña junto con el acceso al módulo de la base de datos 306. Los detalles sobre dichas comprobaciones de contraseñas son muy conocidos en la materia y, por tanto, no se describirán en el presente instrumento.

Sólo tras completar una comprobación exitosa de la contraseña, los datos cifrados, la clave de sesión cifrada y el valor hash MD contenido en el mail se envían en el enlace seguro al servidor 300 a través de un servidor web 301. Estos se activan por los módulos hacia el borde inferior de la figura.

Será obvio que si el método elegido de enviar y recibir emails es a través de mail web entonces no será necesario el cliente de email 213 separado.

En la recepción, el microprocesador 304 remite la clave de sesión cifrada a un módulo 320 que aplica un algoritmo blowfish invertido en combinación con la contraseña del receptor que se obtiene de la base de datos 306 en el bus 315 según la identificación del receptor. La salida del módulo 320 se descifra posteriormente en el módulo 321 utilizando la clave privada de la cifrado RSA utilizado para enviar datos. En virtud de estos módulos, se reproduce la clave de sesión original del módulo 310.

Los datos cifrados recibidos que están comprimidos se descifran en el módulo 323 utilizando la clave de sesión descifrada antes de ser descomprimidos en el módulo 324.

Como con el módulo 307, un valor hash MD se genera en el módulo 325 desde los datos descomprimidos y descifrados y bajo el control del microprocesador 304, el módulo 326 realiza una comprobación de comparación para validar el recién generado valor MD hash frente al valor hash MD recibido desde el receptor para asegurar que coinciden.

Suponiendo que el valor hash MD está correctamente validado en el módulo 326, los datos descifrados del módulo 324 se devuelven al receptor sobre el enlace seguro.

La Figura 3 es un diagrama de flujo que muestra los procesos implicados en el emisor y el servidor para la presente invención para enviar datos desde el emisor al servidor.

Inicialmente, el emisor desea transferir los datos específicos a un receptor específico, teniendo una identidad de receptor conocido. En el paso S1A, el emisor entra en contacto con el servidor en un intento por establecer un enlace seguro de comunicación, por ejemplo, un enlace SSL.

Establecer este enlace implica la ejecución a través de ciertos protocolos de conexión y la comprobación de contraseña mencionada anteriormente y puede asumir la forma de una visualización de una página web en un dispositivo de visualización 105, la entrada de datos de acceso adecuados en la página web y otros. Como se mencionó anteriormente, el establecimiento de dicho enlace de comunicación y la comprobación del contraseña son muy conocidas para los expertos en la materia y no se describirá detalladamente en el presente documento.

El servidor, en respuesta al contacto desde el emisor, también intenta en el paso S1B establecer el enlace de comunicación por medio de la ejecución a través de ciertos protocolos de conexión y la comprobación de contraseña mencionada anteriormente. El servidor comprobará entonces en el paso S2B para ver si se ha realizado un enlace válido, es decir, que todos los protocolos de comunicación se hayan cumplido y que todas las comprobaciones de contraseña hayan sido aprobadas. Si el enlace no se ha establecido, o si la comprobación de contraseña falló, el

servidor va al paso S3B de Error de proceso. Dicho paso puede implicar otros intentos para establecer un enlace de comunicación. Suponiendo que se establece un enlace de comunicación válido, el proceso se mueve al paso S4B para esperar la recepción de la identidad del receptor y los datos a transferir. Puede incluirse un paso de temporización en este punto, si se exige.

En el emisor se realiza una comprobación en el paso S2A para ver también si se ha realizado un enlace válido, es decir, que todos los protocolos de comunicación se hayan cumplido y que todas las comprobaciones de contraseña hayan sido aprobadas. Si el enlace no se ha establecido, o si la comprobación de contraseña falló, el emisor va al paso de Error de proceso S3A. Dicho paso puede implicar otros intentos para establecer un enlace de comunicación. Suponiendo que se establece un enlace de comunicación válido, el proceso se mueve al paso S4A para enviar la identidad del receptor y los datos a transferir. Puede incluirse un paso de temporización en este punto, si se exige.

En un ejemplo, una página web de transferencia de datos se muestra en el dispositivo de visualización 105 que exige la entrada de la identificación del receptor y la unión de los datos, por ejemplo un archivo localizado en una fuente de datos 108. La página de transferencia de datos se envía entonces al servidor 300. Será aparente que los datos a cifrar puedan introducirse directamente en la página de transferencia de datos.

El contenido de la página de transferencia de datos lo recibe el servidor 300 en el paso S4B después de que el proceso proceda al paso S5B. En este paso, el servidor produce un único valor hash MD para los datos y remite el valor al cliente de email 312, después del cual el proceso procede al paso S6B.

En el paso S6B los datos se comprimen, por ejemplo mediante zipping. Luego, en el paso S7B un número aleatorio desde el generador 311 de números aleatorios se obtiene para generar una clave de sesión que es específica a esta transferencia de datos. A partir de entonces, en el paso S8B, los datos se cifran con esta clave de sesión y luego los datos cifrados se remiten al cliente de email 312.

El proceso entonces se mueve al paso S9B en donde la clave de sesión se cifra utilizando una clave pública RSA. A partir de entonces, el proceso se mueve al paso S10B para recuperar la contraseña del receptor después del cual, en el paso S11B, el resultado del paso S9B se cifra con un algoritmo blowfish utilizando la contraseña recuperada en el paso S10B. La clave de sesión cifrada resultante se remite entonces al cliente de email 312.

En el siguiente paso S12B, se formuló un email de una manera conocida para el cliente de email 312 en un formato adecuado para ser transferido por HTML, por ejemplo por la cifrado 64 base. También puede tener un archivo adjunto HTML o un código HTML en línea para los datos cifrados y la clave de sesión cifrada. El email se envía entonces y el envío del email se carga de manera habitual, y la confirmación enviada al emisor, después de la cual finaliza el proceso.

Será aparente que el email contenga el valor hash MD, los datos cifrados y la clave de sesión cifrada, preferiblemente como campos ocultos. El email también incluye preferentemente un enlace HTML para permitir que el receptor se vuelva a conectar con el servidor. Este enlace se configura para enviar automáticamente los campos ocultos en la forma HTML al servidor. La cabecera del email es la cabecera del asunto elegido por el emisor, y el email se dirige a la dirección del email del receptor.

En el paso S5A el emisor recibe la confirmación del envío del email y el proceso finaliza.

La Figura 4 es un diagrama de flujo que muestra los procesos implicados en el receptor y el servidor en respuesta a un email recibido del servidor.

En el paso S101A, el receptor 200 recibe el email del servidor que contiene, entre otras cosas, los datos cifrados, la clave de sesión cifrada y el valor hash MD. El email puede descargarse o bien utilizando el webmail o utilizando el cliente de email 212 sobre el enlace 213. En el paso S102A, el receptor abre el email y entra en contacto con el servidor en un intento por establecer un enlace seguro de comunicación, por ejemplo, un enlace SSL. De una forma similar a la descrita anteriormente, establecer este enlace implica la ejecución a través de ciertos protocolos de conexión y una comprobación de contraseña similar a la comentada anteriormente en relación con el módulo 305 y puede tomar la forma de una visualización de la página web en el dispositivo de visualización 105, la entrada de los datos de acceso adecuados en la página web y otros. Como se mencionó anteriormente, el establecimiento de dicho enlace de comunicación y la comprobación de la contraseña son muy conocidos para los expertos en la materia y no se describirán detalladamente aquí.

El servidor, en respuesta al contacto desde el receptor, también intenta en el paso S101B establecer el enlace de comunicación ejecutando a través de ciertos protocolos de conexión y la comprobación de contraseña mencionada anteriormente. El servidor comprobará entonces el paso S102B para ver si se ha realizado un enlace válido, es decir, que todos los protocolos de comunicación se hayan cumplido y que todas las comprobaciones de contraseña hayan sido aprobadas. Si el enlace no se ha establecido, o si la comprobación de contraseña falló, el servidor va al paso de Error de proceso S103B. Dicho paso puede implicar otros intentos para establecer un enlace de comunicación. Suponiendo que se establece un enlace de comunicación válido, el proceso se mueve al paso S104B para esperar la recepción del receptor ID y otra información incluyendo los datos cifrados, la clave de sesión cifrada y el valor hash MD. Puede incluirse un paso de temporización en este punto, si se exige.

En el receptor se realiza una comprobación en el paso S103A para ver también si se ha realizado un enlace válido, es decir, que todos los protocolos de comunicación se hayan cumplido y que todas las comprobaciones de contraseña hayan sido aprobadas. Si el enlace no se ha establecido, o si la comprobación de contraseña falló, el emisor va al paso de Error de proceso S104A. Dicho paso puede implicar otros intentos para establecer un enlace de comunicación. Puede incluirse un paso de temporización en este punto, si se exige.

Suponiendo que se establece un enlace de comunicación válido, el proceso se mueve al paso S105A para enviar la identidad del receptor y la demás información mencionada en el párrafo anterior. Este último podrá ser en la forma de campos HTML ocultos en el email, los cuales se entregan al servidor 300. Será aparente que el protocolo para la temporización y las disposiciones para enviar las identidades, los campos ocultos, contraseñas etc, puedan variarse para encajar con situaciones particulares.

El proceso en el servidor se mueve entonces al paso S105B para recuperar la contraseña del receptor del módulo 306, después del cual, en el paso S106B, la clave de sesión cifrada se descifra con el algoritmo blowfish utilizando la contraseña recuperada en el paso S105B. El proceso se mueve entonces a un paso S107B de descifrado RSA en donde el resultado del paso S106B se descifra utilizando la clave privada del servidor. Esto provoca que se produzca la clave de sesión.

A partir de entonces, el proceso se mueve a S108B, en donde los datos aún comprimidos se descifran utilizando la clave de sesión descifrada producida en el paso S107B. Después de esto, el proceso se mueve al paso S109B para descomprimir los datos.

En el siguiente paso, S110B, el servidor produce un valor hash MD único para los datos desde el paso S109B. A partir de entonces, en el paso S111B, el valor hash MD del paso S110B se comprueba frente al valor hash MD recibido en el paso S104B. Suponiendo que el valor hash MD está validado, el proceso procede al paso S113B y ahora los datos cifrados del emisor se remiten al receptor sobre el enlace seguro. El envío de estos datos introducen y el proceso finaliza. Si el valor hash MD no puede validarse, el proceso ramifica al Error de proceso S112B. Esto puede implicar el acceso del error y el envío de un mensaje de error al receptor para indicar que los datos han podido corromperse o estar en una situación comprometida.

En el paso S106A el receptor recibe los datos de libre acceso y el proceso finaliza.

En la realización de la invención descrita anteriormente, el proceso completo de cifrado y descifrado se desarrolla en el servidor 300. Por tanto, el emisor y el receptor no necesitan ningún software especial para poder enviar o recibir datos con seguridad. En concreto, no es necesario tener el software, o utilizar la memoria del hardware y los recursos de procesado para permitir el cifrado RSA y el cifrado blowfish. Además, el acceso a las contraseñas se mantiene y el servidor no necesita mantenerse en el emisor. Además, dado que el cifrado y el descifrado se producen en el servidor, las disposiciones necesarias para el cifrado y el descifrado no las necesitará el emisor ni el receptor.

Sin embargo, la presente invención también abarca la alternativa de las funciones dentro de la casilla 317 de la figura 2 proporcionadas en el emisor. Es decir, en esta modificación, la generación de una clave de sesión desde un generador de números aleatorios y la compresión de los datos y el cifrado de los datos comprimidos con esa clave de sesión se realizan todas dentro del emisor. Sin embargo, se establece un enlace seguro con el servidor como anteriormente, pero en este caso sólo la clave de sesión generada se envía al servidor. Después de la misma comprobación de contraseña como anteriormente, los módulos S313 y S314 vuelven a generar una clave de sesión que, en este caso, se devuelven al emisor. Los datos cifrados, la clave de sesión cifrada y el valor hash se proporcionan entonces al cliente email emisor (no se muestra) que también se conecta a Internet. Este cliente email construye un email como anteriormente antes de enviarlo al receptor. Por tanto, puede verse que los pasos de S5B a S8B en la figura 3 ahora tienen lugar en el emisor. Esto puede reducir las demandas del proceso establecidas en el servidor.

El receptor recibe el email en su cliente de email y puede procesar el email como en la figura 4.

Sin embargo, la presente invención también abarca la alternativa de las funciones con la casilla 322 de la figura 2 proporcionándose en el receptor una vez que el email se reciba del servidor. Es decir, en esta modificación, el descifrado de los datos, la descompresión de los datos, la generación de un valor hash MD y la validación de ahí, todo ello se llevan a cabo en el receptor. Sin embargo, se establece un enlace seguro con el servidor como anteriormente, pero en este caso sólo la clave de sesión cifrada se envía al servidor. Después de la misma comprobación de contraseña como anteriormente, los módulos S320 y S321 vuelven descifrar la clave de sesión que, en este caso, se devuelve al receptor. Los datos cifrados se descifran utilizando la clave de sesión descifrada, un valor hah MD descomprimido, generado y revisada su validez frente al valor hash MD recibido en el email. Por tanto, puede verse que los pasos de S108B a S113B en la figura 4 ahora se producen en el receptor. Esto puede reducir las demandas del proceso establecidas en el servidor.

Se apreciará que las dos modificaciones mencionadas anteriormente pueden implantarse a la vez. Sin embargo, con la presente invención, el cifrado de la clave de sesión, en combinación con la clave del receptor, tiene lugar en el servidor.

Se apreciará que un grupo de usuarios puede registrarse para recibir emails cuando se requiera. Por ejemplo, el departamento de TI de una empresa puede registrar a todos los empleados. En este caso, en el caso de que la comprobación de contraseña falle en el servidor, puede consultarse la referencia a otras contraseñas en ese grupo.

En las realizaciones de la invención que requieren un software especial instalado para el emisor o el receptor, como conocen los expertos en la materia, esto puede descargarse del servidor durante el proceso de registro y luego instalarse.

Se apreciará que desde que se exija la contraseña correcta del receptor para descifrar los datos en el algoritmo Blowfish y el descifrado correcto se compruebe eficazmente validando el valor hash MD, la comprobación del contraseña durante el enlace entre el receptor y el servidor en el paso 102A pueden eximirse, si se exige.

También se apreciará que si el descifrado no tiene éxito, el servidor 300 puede establecerse para llevar a cabo otras comprobaciones para intentar obtener la contraseña correcta, por ejemplo, buscando antiguas contraseñas del receptor e intentando cada una de ellas para descifrar los datos. Si una de los contraseñas produce el valor hash MD correcto, entonces el descifrado ha tenido éxito. Sin embargo, si ninguna de esas contraseñas funciona, entonces el receptor no es el receptor que se pretende o los datos se han corrompido durante la transferencia.

Si el receptor no tiene un contraseña y aún no está registrado en el servidor 300, el servidor puede generar un contraseña *shot* que envía al receptor a través de cualquier medio seguro y adecuado, por ejemplo, correo seguro o por medio de un enlace seguro o a través de email seguro, exigiendo al usuario que cambie su contraseña a una contraseña segura para utilizarlo a partir de entonces.

Con la presente invención, las identidades del emisor y el receptor pueden verificarse de manera que el emisor pueda enviar datos a un receptor que no tenga un software especial instalado, de manera que el receptor esté seguro del origen de los datos. Además, los intentos de cifrado y descifrado se introducen, lo que puede permitir que un emisor compruebe si un receptor ha recibido y descifrado los datos y puede permitir que el receptor compruebe si los datos que espera recibir se han entregado ya.

El aparato del emisor y del receptor puede tener muchas formas, una lista no exclusiva que incluye, por ejemplo, un ordenador, una PDA o cualquier otro dispositivo portátil, un ordenador portátil, un teléfono móvil. El servidor es preferentemente un ordenador, aunque también puede ser un tipo alternativo de dispositivo informático.

Se verá que con la presente invención, ni el emisor ni el receptor conocen la contraseña del otro, estos se conservan en el servidor. En consecuencia, el nivel de seguridad requerido por el emisor y el receptor no es tan alto como otras formas conocidas de transferir datos de una forma segura.

Con la presente invención, el servidor mantiene la información específica del receptor, como un contraseña, que utiliza el servidor en un proceso de cifrado. El servidor obtiene esta información desde una fuente de datos, el cual tiene una lista de identificaciones del receptor y la información específica del receptor, que se mantiene secreta. La información específica del receptor puede comprender una contraseña, una frase de acceso, un número PIN, un valor hash o cualquier otra información que vaya a utilizarse para verificar la identidad.

La red utilizada con la presente invención puede ser Internet, una intranet local como una red Ethernet, una red telefónica, una red radiofónica o cualquier otro tipo de red para transferir datos. Preferiblemente, cuando se utiliza Internet, una conexión SSL segura se utiliza entre el servidor y el emisor y/o entre el servidor y el receptor.

Emisor y receptor pueden identificarse al servidor a través de sus direcciones de correo electrónico (u otras direcciones de la red). Sin embargo, también pueden tener identificación de usuarios que no están relacionadas con sus direcciones de la red. El servidor puede tener una lista de direcciones de red en su base de datos y/o puede tener una lista de identificaciones de usuarios, donde la dirección de red y/o las identificaciones de usuarios están asociadas con información específica secreta del receptor.

En una realización de la presente invención, el servidor 300 puede incluir un único código secreto para el servidor y que sólo conoce el servidor. Este código secreto puede incluirse en los módulos de descifrado y cifrado blowfish. El código secreto puede utilizarse en el cifrado además de utilizar la información específica del receptor. Estos dos documentos de información pueden concatenarse simplemente para utilizarlos en el proceso de cifrado. El uso del código secreto proporciona un nivel mejorado de seguridad al sistema.

Se apreciará que el servidor no necesita retener la clave de sesión ni ningún dato enviado al receptor. Estos pueden almacenarse en una memoria volátil sobre el servidor y ser sobrescritos cuando se cifren los demás datos y claves. Esto tiene la ventaja de que el servidor no necesite tener una gran cantidad de memoria disponible para almacenar datos antiguos y posiblemente redundantes y/o las claves.

El dispositivo portador puede comprender un medio transitorio, por ejemplo, una señal magnética o acústica, electromagnética, RF, microondas, óptica, eléctrica (por ejemplo, una señal TCP IP sobre una red IP como Internet), o un dispositivo portador como un disquete, CD ROM, disco duro, o dispositivo de memoria programable.

Al tiempo que la invención se ha descrito en términos de qué son en la actualidad sus realizaciones preferidas, quedará claro para los expertos en la materia que puedan realizarse varios cambios en las realizaciones preferentes sin salir del ámbito de la invención, que está definida por las reivindicaciones. La presente invención puede encontrar aplicación, por ejemplo, con proveedores de teléfonos móviles que puedan distribuir informes mensuales a los usuarios del teléfono móvil de manera segura, el usuario del teléfono móvil se conecta al servidor para recuperar el informe cifrado. De manera similar, los bancos pueden distribuir detalles de los pagos entrantes a sus clientes que simplemente pueden conectar al servidor como se describe anteriormente para recuperar dichos detalles, distribuyendo los detalles de manera segura.

REIVINDICACIONES

1. Un método de cifrar y transferir datos entre un emisor (100) y un receptor (200) utilizando una red, el método comprende los pasos de:

- Un servidor (300) que recibe del emisor (100) un identificador del receptor;

- Establecer una clave de cifrado específica de transferencia (310) específica para la transferencia;

- Cifrar los datos utilizando la clave de cifrado específica de la transferencia (309);

- El servidor (300) que accede a la información específica del receptor (306) según el identificador del receptor enviado por el emisor y la cifrado (314), con la información específica del receptor, dicha clave de cifrado específica de transferencia;

- Transferir los datos cifrados y la clave de cifrado específica de la transferencia cifrada sobre la red para que lo reciba el receptor (200);

Caracterizado por:

- el servidor recibe del receptor la clave de cifrado específica de la transferencia cifrada y el identificador del receptor; y

- el servidor que accede a la información específica del receptor (306) según el identificador del receptor enviado por el receptor para descifrar la clave de cifrado específica de la transferencia cifrada (320); y

- descifrar los datos cifrados utilizando la clave de cifrado específica de la transferencia descifrada (323).

2. Un método según la reivindicación 1 que incluye además establecer un enlace de comunicación (111, 302) entre el emisor y el servidor y enviar dicho identificador del receptor al servidor.

3. Un método según la reivindicación 2 que incluye además establecer el enlace de comunicación entre emisor y servidor para que sea un enlace seguro.

4. Un método según la reivindicación 2 o 3 que incluye además establecer el enlace de comunicación entre el emisor y el servidor sujeto a una revisión del servidor sobre la contraseña del emisor (305).

5. Un método según cualquier reivindicación anterior que incluye además establecer un enlace de comunicación (211, 302) entre el receptor y el servidor y enviar dicho identificador del receptor al servidor.

6. Un método según la reivindicación 5 que incluye además establecer el enlace de comunicación entre receptor y servidor para que sea un enlace seguro.

7. Un método según la reivindicación 5 o 6 que incluye además establecer el enlace de comunicación entre el receptor y el servidor sujeto a una revisión de la contraseña del receptor sobre la contraseña (305).

8. Un método según cualquier reivindicación anterior en donde el establecimiento de la clave de cifrado específica de transferencia tiene lugar en el emisor y la clave de cifrado específica de transferencia establecida se envía al servidor.

9. Un método según cualquier reivindicación anterior en donde el cifrado de datos utilizando la clave de cifrado específica de la transferencia tiene lugar en el emisor.

10. Un método según la reivindicación 9 en donde el emisor recibe del servidor la clave de cifrado específica de transferencia cifrada y el emisor transfiere los datos cifrados y la clave de cifrado específica de la transferencia cifrada al receptor sobre la red.

11. Un método según cualquiera de las reivindicaciones 1 a 7 en donde el receptor recibe del servidor la clave de cifrado específica de transferencia descifrada y el descifrado de los datos cifrados utilizando la clave de cifrado específica de la transferencia descifrada tiene lugar en el receptor.

12. Un método según cualquiera de las reivindicaciones 1 a 7 en donde el establecimiento de la clave de cifrado específica de la transferencia tiene lugar en el servidor.

13. Un método según la reivindicación 12 anterior en donde cifrar los datos utilizando la clave de cifrado específica de la transferencia tiene lugar en el servidor.

14. Un método según la reivindicación 13 en donde el servidor transfiere los datos cifrados y la clave cifrada específica de la transferencia cifrada al receptor sobre la red.

15. Un método según cualquiera de las reivindicaciones 1 a 10 y 12 a 14 en donde el descifrado de los datos cifrados utilizando la clave de cifrado específica de la transferencia descifrada tiene lugar en el servidor y el servidor transfiere los datos descifrados al receptor.

16. Un método según cualquier reivindicación anterior que incluye además:

- establecer un valor (307) de código de autenticación de mensaje (MAC) para los datos anteriores al cifrado;

- transferir el valor MAC junto con los datos cifrados y la clave de cifrado específica de la transferencia cifrada; y establecer un valor MAC (325) para los datos después de descifrarlo y validarlo (326) frente al valor MAC transferido.

17. Un método según cualquier reivindicación anterior en donde cifrar la clave de cifrado específica de la transferencia emplea uno o más métodos de cifrado de clave pública, un algoritmo blowfish, y un código secreto del servidor.

18. Un método para operar un servidor (300) para cifrar y transferir datos entre un emisor (100) y un receptor (200) utilizando una red, el método incluye los siguientes pasos:

- recibir del emisor (100) un identificador del receptor;

- acceder a la información específica del receptor (306) según el identificador del receptor enviado por el emisor y cifrar (314), con la información específica del receptor, una clave de cifrado específica de transferencia que se utiliza para cifrar datos;

Caracterizada por

- recibir del receptor (200) la clave de cifrado específica de la transferencia cifrada y el identificador del receptor después de que los datos cifrados y que la clave de cifrado específica de la transferencia cifrada se hayan transferido sobre la red para que los reciba el receptor;

Acceder a la información específica del receptor (306) según el identificador del emisor enviado por el emisor para descifrar la clave de cifrado específica de la transferencia cifrada.

19. Un método de operar un servidor según la reivindicación 18 que además comprende establecer en el servidor (310) una clave de cifrado específica de transferencia específica a la transferencia.

20. Un método de operar un servidor de acuerdo con la reivindicación 18 que comprende además recibir del emisor una clave de cifrado específica de transferencia a la transferencia;

y transferir la clave de cifrado específica de la transferencia cifrada al emisor.

21. Un método para operar un servidor de acuerdo con una de las reivindicaciones 18 a 20 que incluye además cifrar los datos en el servidor (309) utilizando la clave de cifrado específica de la transferencia.

22. Un método de operar un servidor de acuerdo con cualquiera de las reivindicaciones 18 a 21 incluyendo transferir los datos cifrados y la clave de cifrado específica de la transferencia cifrada sobre la red para que la reciba el receptor.

23. Un método para operar un servidor de acuerdo con cualquiera de las reivindicaciones 18 a 22 que además incluye transferir al receptor la clave de cifrado específica de la transferencia descifrada.

24. Un método para operar un servidor de acuerdo con cualquiera de las reivindicaciones 18 a 22 que incluye además descifrar los datos cifrados en el servidor (323) utilizando la clave de cifrado específica de la transferencia descifrada.

25. Un medio informático para un método de cifrar y transferir datos entre un emisor (100) y un receptor (200) utilizando una red, el medio incluye:

- código informático para recibir del emisor un identificador del receptor y establecer una clave de cifrado específica de transferencia (S7B) específica a la transferencia;

- código informático para cifrar los datos utilizando la clave de cifrado específica de la transferencia (S8B);

- código informático para acceder a la información específica del receptor (S10B) según el identificador del receptor enviado por el emisor y el cifrado (S11B), con la información específica del receptor, dicha clave de cifrado específica de la transferencia;

- código informático para transferir los datos cifrados y la clave de cifrado específica de la transferencia cifrada sobre la red (S12B) para recepción por parte del receptor;

caracterizado por

- un código informático para recibir del receptor (S101B) la clave de cifrado específica de la transferencia cifrada y el identificador del receptor y para acceder a la información específica del receptor (S105B) según el identificador del receptor enviado por el receptor para describir la clave de cifrado específica de la transferencia cifrada (S106B); y

código informático para descifrar los datos cifrados (S108B) utilizando la clave de cifrado específica de la transferencia descifrada.

Visualización - 105
Interfaz de visualización - 104
Memoria - 103
Microprocesador - 102
Teclado - 107
Fuente de datos – 108
Interfaz de dispositivo de entrada -109
Navegador web – 110

INTERNET – Servidor

Teclado – 207
Interfaz de dispositivo de entrada – 209
Navegador web – 210
Cliente de email – 212
Visualización - 205
Interfaz de visualización – 204
Memoria – 203
Microprocesador 202

Figura 1.

MAC – 307
Comprimir – 308
Cifrar - 309
Cliente de email - 312
Número aleatorio – 311
Clave de sesión – 310
Cifrado RSA -313
Cifrado blowfish – 314
Comprobación de contraseña – 305
Base de datos – 306
Servidor web - 302
Microprocesador - 304
Descifrado blowfish - 320
Descifrado RSA- 321
Descifrado – 323
Descomprimir – 324
Comprobación MAC – 326
MAC – 325

Figura 2

EMISOR	SERVIDOR
INICIO	INICIO
S1A - Servidor de contacto - Protocolos de conexión - Comprobación de contraseña	S1B - Contacto del emisor - Protocolos de conexión - Comprobación de contraseña
Error de proceso – S3B ¿Suspenso? – S2A	¿Suspenso? S2B Error de proceso S3B
Enviar identificación del receptor Enviar datos al servidor	Esperar identificación y datos – S4B Generar valor hash MD Enviar a cliente de email – S5B Comprimir datos – S6B Generar clave de sesión – S7B Cifrar datos con clave de sesión – S8B Enviar a cliente de email
FIN	Cifrar clave de sesión utilizando clave pública RSA – S9B Obtener contraseña del receptor - S10B Cifrar clave de sesión utilizando algoritmo blowfish y contraseña del receptor Enviar a cliente de email – S11B Enviar email y acceder Confirmar a emisor – S12B FIN

Figura 3

RECEPTOR
INICIO

SERVIDOR
INICIO

Recibir email – S101A
- Datos cifrados
- Clave de sesión cifrada
- Valor hash MD

- Contacto del emisor- S101B
- Protocolos de conexión
- Comprobación de contraseña

S102A
- Servidor de contacto
- Protocolos de conexión
- Comprobación de contraseña

S102B – ¿Suspenso?
S103 B – Error de proceso
S104 B – Esperar identificación y datos

S103A ¿Suspenso?

Error de proceso - S104A

¿Suspenso? S103A

S105B – Obtener contraseña del receptor
S106B – Descifrar la clave de sesión utilizando el algoritmo blowfish y la contraseña del receptor
S107B – Descifrar la clave de sesión utilizando la clave privada RSA
S108B – Descifrar datos con la clave de sesión
S109 B - Descomprimir datos
S110 B Generar valor hash MD
S112B Error de proceso
S111B Validar valor hash MD
S113B Enviar datos al receptor y acceder

FIN

Enviar identificación del receptor – S105A
Enviar datos cifrados al servidor
Enviar valor hash MD
Enviar clave de sesión cifrada

Recibir datos - S106A

FIN

Figura 4

S103B
S102B

S102A
S103A
- Servidor de contacto
- Protocolos de conexión
- Comprobación de contraseña

Procesado error
S104A
Enviar identificador del receptor
Enviar datos cifrados al servidor
Enviar valor hash MD
Enviar clave de sesión cifrada

S105A

S106B

Procesado error
S104B
Espere identificación y datos
Obtener contraseña del receptor
Descifrar la clave de sesión utilizando un algoritmo blowfish y una contraseña del receptor

S107B

Descifrar la clave de sesión utilizando la clave pública RSA.

S108B

Descifrar datos con la clave de sesión

Descomprimir datos
S109B
Generar valor hash MD
S110B

S111B
S112B
S106A

Error de proceso

S113B

Recibir datos

Enviar datos al receptor y acceder

FIN

Figura 4:

FIN