(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 664 399**

(51) Int. CI.:

G06F 21/62 (2013.01)
H04L 9/00 (2006.01)
H04L 9/08 (2006.01)
H04L 9/32 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **13.02.2015 E 15154982 (1)**

(97) Fecha y número de publicación de la concesión europea: **31.01.2018 EP 3057029**

(54) Título: **Un método y un aparato mejorados de cifrado y de autentificación**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
19.04.2018

(73) Titular/es:

WOLF, THOMAS (100.0%)
Plinganserstr. 18-B
81369 München, DE

(72) Inventor/es:

WOLF, THOMAS

(74) Agente/Representante:

DE PABLOS RIBA, Juan Ramón

Descripción

La presente invención está relacionada con un método y un aparato mejorados de cifrado y de autentificación.

En el estado anterior de la técnica las contraseñas se utilizaban generalmente para autentificar al usuario o un servicio en un ordenador. Las contraseñas también se utilizan para proteger archivos, como los archivos comprimidos ZIP.

Sin embargo, es posible saltar esa protección con contraseña probando simplemente un número arbitrario de combinaciones de bits o de caracteres, lo que también se llama ataque de fuerza bruta o simplemente un ataque de fuerza.

En el estado anterior de la técnica de cifrado hay diversos métodos disponibles para autentificar una identidad, cifrar datos, generar comprobaciones de cuentas y/o generar hashes. En estos métodos la seguridad para que no se determine una clave que se esté utilizando depende de las capacidades de los posibles atacantes. Expertos en la materia estiman que muchos de estos métodos son seguros frente al hecho de que se intente simplemente un número arbitrario de patrones de contraseñas, lo que se llama frecuentemente como ataque de fuerza bruta o ataque de fuerza. Este ataque intenta determinar una contraseña intentando todas las claves posibles. Debido a que el número de claves que se pueden probar en un periodo predeterminado puede ser muy elevado mediante el uso de ordenadores modernos o mediante clusters de ordenadores, la evaluación sobre si una clave es segura o no, la determina la longitud de la clave, que puede evaluarse por su longitud en bits. El rendimiento de los ordenadores modernos, de los superordenadores y de los clusters de ordenadores es tan alto que, dependiendo de los detalles del ataque que se haya utilizado, se puede conseguir la prueba automática de un número muy elevado de claves en un periodo que el atacante considera aceptable. En otras palabras, la seguridad de una clave es mayor cuanto más largo sea el contenido informativo en bits o cuanto más larga sea la clave. Normalmente una clave que un humano puede recordar fácilmente, sobre todo las contraseñas, está por debajo del nivel de seguridad necesario.

En el estado anterior de la técnica, los métodos son conocidos porque evitan que se prueben diferentes claves en un dispositivo informático. Estos métodos introducen, por ejemplo, un tiempo de inactividad después de haber introducido una contraseña incorrecta.

Esto reduce de manera significativa el número de claves que se pueden probar en un periodo predeterminado. Sólo se pueden poner en práctica estos métodos si la prueba la realiza una interfaz predeterminada, como puede ser un teclado o un ordenador determinado. Un ataque puede evadir el tiempo de inactividad si utiliza un clúster de ordenadores para determinar una contraseña o puede probar un número arbitrario de contraseñas desde su propio sistema informático. De ese modo, el número de claves que se prueban en un periodo predeterminado se puede maximizar. Esto ocurre sobre todo en el caso de que el atacante tenga acceso físico al archivo de datos o al ordenador.

En el estado anterior de la técnica de cifrado, los métodos están disponibles para evitar la evasiónde la complejidad del algoritmo de fuerza bruta al añadir una segunda subclave (llamada “*salt*”) a la clave del usuario antes de que se ejecuteel algoritmo de hash. De esta manera se elimina la posibilidad de utilizar tablas de hash calculadas previamente u otros métodos de simplificación.

La patente WO 02/05069 A2 divulga un método en el que se transmite un conjunto de datos digitales de un primer cliente a un servidor mediante una conexión de datos. El conjunto de datos se almacena en el servidor. Al mismo tiempo, se generan una clave maestra y una clave parcial, por ejemplo un número aleatorio, que se asignan al conjunto de datos. De esas dos claves se genera una clave

parcial. Esto se lleva a cabo de tal manera que la pareja de claves se puedan asignar a la clave maestra inequívocamente. Las dos claves forman una clave de dos partes que está enlazada a los datos digitales. La clave se añade al conjunto de datos y se transmiten de forma conjunta como un conjunto de datos a través de una conexión de datos al cliente. Por esta conexión de datos también se transfiere la segunda clave por separado del conjunto de datos digitales. A través de la conexión de datos entre el cliente y un nuevo cliente se puede transferir una copia del conjunto de datos al que está añadida la clave. De este modo, la copia en el nuevo cliente se puede autentificar como en calidad de original, siempre que la clave parcial también se transmita a través de una nueva conexión de datos al cliente. Para la autentificación propiamente dicha, el conjunto de datos digitales junto a la clave añadida, así como a la clave parcial, se transfieren al servidor a través de una conexión de datos. Ahí es donde se verifica el conjunto de datos para comprobar si es idéntico al conjunto de datos que está almacenado en el servidor. Al mismo tiempo, las claves que se han transferido se combinan a una clave de referencia, donde la clave maestraque está almacenada en el servidor verifica la clave de referencia. Si se logra la autentificación, se confirma la autentificación del conjunto de datos digitales. Después, tanto las claves como las claves maestras se declaran inválidas.

El *salting* se explica en el documento de literatura no patente XP2619016 de Schneier, B.

La derivación de clave se explica en el NIST 800-132 "*Recommendation for Password Based on Key Derivation*", de diciembre de 2010.

Es objeto de la presente invención el proporcionar un método y un aparato más seguros de cifrado y de autentificación.

El objeto de la invención se consigue a través de un método de conformidad con la reivindicación número 1 o la número 2, un aparato de conformidad con la reivindicación número 6 o la número 7 y un producto de programa informático de conformidad con la reivindicación número 12.

El método innovadorpara cifrar y/o para autentificar consta del paso de enviar una solicitud de una primera combinación de bits o de caracteres en calidad de una primera subclave, así como de almacenar la primera combinación de bits o de caracteres en la memoria. De conformidad con la presente invención, se genera una segunda combinación de bits o de caracteres en calidad de una segunda subclave, donde la segunda combinación de bits o de caracteres es un patrón aleatorio o pseudoaleatorio. Tanto la primera subclave como la segunda subclave están combinadas a una clave. Los datos están cifrados con la clave. La clave también se puede utilizar como una contraseña de autentificación para autentificar en un ordenador.

En el marco de la presente invención, un ordenador es cualquier dispositivo que tenga una unidad central de procesamiento y una memoria, tales como un teléfono inteligente, una tableta, un ordenador personal, un portátil u otro dispositivo similar. La autentificación también puede incluir una autentificación en un servicio, como un programa que se ejecute en un ordenador. Por ejemplo, que se ejecute en un ordenador remoto.

La primera subclave tiene una longitud de "a" bits y la segunda subclave tiene una longitud de "b" bits. Por lo tanto, para determinar la primera subclave hay que probar las claves 2^a. Para determinar la clave que incluye la primera subclave y la segunda subclave se tienen que probar las claves 2^{a+b} en calidad de estímulos de prueba. De esta manera, el tiempo para determinar una contraseña por medio del ataque de fuerza bruta se prolonga significativamente, lo que puede impedir que los atacantes puedan utilizar el ataque de fuerza bruta.

El usuario no necesita saber la segunda subclave. El ordenador sí necesita saber la primera y/o la segunda subclaves, ya que requiere autentificación, y/o las necesitaría saber un archivo de datos que

esté protegido bajo una contraseña o una clavesólo debido a una operación de cifrado y/o de hash con el fin de verificar si la llave combinada es correcta, que no tiene que estar necesariamente en forma cifrada y/o de hash.

El método para descifrar y/o para autentificar consta del paso de enviar una solicitud para una primera combinación de bits o de caracteres en calidad de una primera subclave y para almacenar la primera combinación de bits o de caracteres en la memoria. De conformidad con la invención, hay diversos pasos que se repiten hasta que se verifique que la clave es válida. Estos son: el paso de generar una segunda combinación de bits o de caracteres en calidad de una posible segunda subclave de entre una multitud de segundas subclaves donde se selecciona la segunda combinación de bits o de caracteres del juego de todas las segundas subclaves posibles; el de combinar la primera subclave y la segunda subclave a una clave; yel de verificar si la clave es válidao no. Una vez que se verifica que la clave es válida se descifran los datos con la clave y/o la clave se utiliza como una contraseña de autentificación.

El método de descifrado genera una multitud de patrones en calidad de una segunda subclave para generar la clave que descifra los datos y/o para generar la contraseña de autentificación. De este modo, el tiempo que se necesita para descifrar los datos o para determinar la contraseña de autentificación aumenta. Este aumento de tiempo se puede considerar aceptable si se sabe la primera subclave, ya que es el usuario quien la introduce. Sin embargo, si la primera subclave la determina el ataque de fuerza bruta, el tiempo que se necesita para determinar la clave o la contraseña aumenta significativamente, ya que es el ataque de fuerza bruta el que tiene que determinar tanto la primera subclave como la segunda subclave. De esta manera, para el atacante es menos tentador determinar la clave o la contraseña.

El paso de verificar si la clave es válida o no puede conllevar el intento de descifrar los datos y/o autentificar mediante el uso de la contraseña. El método puede intentar descifrar un archivo (p. ej. un archivo comprimido ZIP) o autentificar utilizando la contraseña en un ordenador o en un servicio.

El paso de enviar una solicitud puede incluir el paso de enviar una solicitud al usuario para que introduzca la primera subclave en el ordenador.

El paso de combinar la primera subclave y la segunda subclave puede conllevar concatenar la primera subclave y la segunda subclave, insertar la segunda subclave en una posición arbitraria de la primera subclave, insertar la primera subclave en una posición arbitraria de la segunda subclave, añadir la segunda subclave al final o al principio de la primera subclave, y/o entrelazar la primera subclave y la segunda subclave. La concatenación, la inserción, el entrelazado y la adición se pueden realizar a nivel de bits o de caracteres. De esta manera, incluso la seguridad de una contraseña quepueden memorizar los seres humanos puede aumentar significativamente.

La segunda subclave puede tener una longitud diferente a la de la primera subclave. Por ejemplo, la segunda subclave puede ser más corta que la primera subclave. El paso de cifrado puede conllevar el paso de generar y almacenar un valor de hash basado en una clave. El paso de descifrar puede conllevar el paso de generar un valor de hash y de comparar el valor de hash que se ha generado con un valor de hash que esté almacenado.

El objeto de la invención también se consigue por medio de un aparato de cifrado y/o de autentificación que se compone de un dispositivo de solicitud adaptadopara solicitar una primera combinación de bits o de caracteres en calidad de una primera subclave y de una memoria para almacenar la primera combinación de bits o de caracteres. De conformidad con la invención, un generador aleatorio o pseudoaleatorio está adaptado de manera que pueda generar una segunda combinación de bits o de caracteres en calidad de una segunda subclave aleatoria o pseudoaleatoria. El

aparato de cifrado también se compone de un combinador adaptado para combinar la primera subclave y la segunda subclave a una clave. Un dispositivo de cifrado del aparato de cifrado puede utilizar la clave para cifrar los datos con la clave. El aparato de cifrado se puede componer también de un generador de contraseñas adaptado para generar una contraseña basada en la clave.

El aparato de cifrado se puede configurar y utilizar como se ha mencionado anteriormente con respecto al método de cifrado.

El objeto de la invención también se soluciona mediante un aparato de cifrado y/o de autentificación que se compone de un dispositivo de solicitud adaptado para solicitar una primera combinación de bits o de caracteres en calidad de una primera subclave y de una memoria para almacenar la primera combinación de bits o de caracteres. El aparato de descifrado se compone también de un generador de juego de claves adaptado para seleccionar o generar una segunda subclave posible de entre una multitud de segundas subclaves posibles. El aparato de descifrado se puede componer de un combinador adaptado para combinar la primera subclave y la segunda subclave a una clave. El aparato de descifrado se compone también de un verificador adaptado para verificar si la clave es válida o no. El aparato de descifrado se compone también de un dispositivo de descifrado adaptado para descifrar los datos con la clave. El aparato de descifrado se compone también de un controlador adaptado para controlar el generador de juego de claves, el combinador, el verificador y el dispositivo de descifrado. El controlador indica al generador de juego de claves que genere una combinación de bits o de caracteres arbitraria en calidad de una segunda subclave del conjunto de todas las segundas subclaves posibles. Igualmente indica al combinador que combine la primera subclave y la segunda subclave a una clave,y si el verificador comprueba que la clave es válida, también indicaal dispositivo de descifrado que descifre los datos con la clave y/o que utilice la clave como una contraseña de autentificación.

El aparato de descifrado se puede adaptar y configurar como se ha mencionado anteriormente con respecto al método de descifrado.

El verificador se puede adaptar para descifrar los datos con la clave y/o para utilizar la contraseña para autentificar en un ordenador. El dispositivo de solicitud se puede adaptar para solicitar a un usuario que introduzca la primera subclave, tal como introducir la primera subclave en un dispositivo de entrada.

El combinador puede concatenar la primera subclave y la segunda subclave, insertar la segunda subclave en una posición arbitraria de la primerasubclave, añadir la segunda subclave al final o al principio de la primera subclave y/o entrelazar la primera y la segunda subclaves. La concatenación, la inserción, la adición y el entrelazado se pueden realizar a nivel de bits o de caracteres.

La segunda subclave puede tener una longitud diferente a la de la primera subclave. El dispositivo de cifrado se puede adaptar para generar un valor de hash basado en una clave. El dispositivo de descifrado se puede adaptar para generar un valor de hash a partir de una clave y para comparar ese valor de hash con un valor de hash que esté almacenado.

La segunda subclave es una parte desconocida de la clave. Esta segunda subclave se selecciona de manera aleatoria o de manera pseudoaleatoria de manera que sea más o menos similar al patrón arbitrario. Cuanto más larga sea la segunda subclave y en conformidad con su contenido informativo,esta segunda subclave se selecciona de tal manera que el número de las posibles claves que se pueden generar al combinar la primera subclave y la segunda subclave es tan elevado que inclusoutilizando un ordenador de gran rendimiento o un clúster de ordenadores, el periodo de tiempo para que se pueda ejecutar un ataque de fuerza bruta sobre la contraseña o la clave aumenta

significativamente. Se debe entender que la segunda subclave puede tener una longitud que no reduzca en exceso la facilidad de uso del usuario por un largo periodo de inactividad cuando se autentifica en un ordenador o cuando se descifra un archivo.

El aparato de cifrado y de descifrado se puede implementar por componentes discretos, tales como circuitos integrados y/o circuitos específicos de aplicación. Los componentes del aparato de cifrado y de descifrado también se pueden implementar por un ordenador que tenga un procesador y una memoria. El ordenador puede ser un ordenador de uso general, lo que incluye teléfonos móviles, tabletas, portátiles, ordenadores personales, servidores y otros dispositivos similares.

El método de cifrado y/o el método de descifrado pueden ser métodos implementados por ordenador.

La segunda subclave ("*salt*"), de conformidad con métodos del estado anterior de la técnica, es pública (está abierta) en estos métodos para la autentificación o el descifrado del usuario o del sistema. En esta invención, por el contrario, la segunda subclave no necesita estar pública para la autentificación del usuario o del sistema. Esto, por lo tanto, incrementa enormemente la dificultad de poder determinar la clave correcta mediante el ataque de fuerza bruta. Se pueden utilizar métodos que empleen una segunda subclave"*salt*" adicional además de esta invención, pero no se tiene que utilizar para que la invención funcione.

En el estado anterior de la técnica de cifrado, en relación al uso de una segunda subclave pública ("*salt*"), el procedimiento hash a veces se repite un número significativo de veces con el fin de aumentar la complejidad del paso de descifrado o de autentificación, lo que aumenta el tiempo que se necesita para probar cada clave. No obstante, este método depende de la inexistencia de un método para que el atacante simplifique sucesivas operaciones hash, lo que por lo general aún no se ha demostrado y que por ello existe controversia al respecto. En esta invención, por el contrario, la complejidad del paso de descifrado o de autentificación no aumenta como tal, sino el número de intentos de descifrado o de autentificación independientes que se necesitan. Por lo tanto, esto evita cualquier posibilidad de simplificar o acortar el proceso de descifrado o de autentificación en su conjunto mediante el uso de cualquier método de simplificación matemática o de algoritmos de los que se pueda servir el atacante.

El método de cifrado y/o el método de descifrado se puede implementar por cualquier producto de programa informático, tal como las instrucciones que están almacenadas en un soporte de datos, como puede ser un dispositivo USB, un CD o un DVD. El producto de programa informático también puede ser datos de instrucción que se pueden transmitir a través de cualquier red adecuada, como internet.

La invención se explica a continuación a través de realizaciones ilustrativas sin carácter limitativo con referencia a los dibujos adjuntos, en los que

la figura 1 es un organigrama de un método de cifrado de conformidad con la presente invención;

la figura 2 es un organigrama de un método de descifrado de conformidad con la presente invención; y

la figura 3 es un aparato de conformidad con la presente invención.

A continuación se explica la invención con referencia a las figuras que van de la 1 a la 3.

Un dispositivo de solicitud 304 envía a un usuario una solicitud 102 de una primera combinación de bits o de caracteres en calidad de una primera subclave. La solicitud se muestra en un dispositivo de salida 308. El usuario introduce la primera combinación de bits o de caracteres en calidad de una primera subclave en undispositivo de entrada 306. La primera combinación de bits o de caracteres se almacena en una memoria 310. Un generador 312 aleatorio o pseudoaleatorio genera un segunda combinación de bits o de caracteres en calidad de una segunda subclave 106, donde la segunda combinación de bits o de caracteres es un patrón aleatorio o pseudoaleatorio. Los expertos en la materia conocen estos generadores aleatorios o pseudoaleatorios y por razones de brevedad no se van a explicar con más detalle.

Un combinador 314 combina la primera subclave y la segunda subclave a una clave 108. La combinación puede incluir la concatenación de la primera subclave y de la segunda subclave. También puede incluir la inserción de la segundasubclave en una posición arbitraria de la primera subclave, así como la adición de la segunda subclave al final o al principio de la primera subclave. Además, puede incluir el entrelazado de la primera subclave y de la segunda subclave. Un dispositivo de cifrado 316 puede cifrar datos con la clave 110 y puede pasar los datos bien a un medio de almacenamiento externo o a un medio de transmisión 402. Un generador de contraseñas 318 puede introducir la contraseña como una contraseña de autentificación en un ordenador externo 404 o en un servicio que se ejecute en el mismo ordenador o en un ordenador diferente 404.

El aparato innovador de cifrado y de descifrado de la invención también está adaptado para descifrar datos o para proporcionar una contraseña para autentificar en un ordenador o en un servicio. El dispositivo de solicitud 304 envía una solicitud a un dispositivo de salida 308 de una primera combinación de bits o de caracteres en calidad de una primera subclave 202. El usuario puede introducir la subclave que conoce en el dispositivo de entrada 306. El dispositivo de solicitud 304 almacena la subclave en una memoria 310. El aparato de cifrado y de descifrado 302 se compone también de un verificador para verificar si una clave es válida o no y de un controlador para controlar el generador de juego de claves 326, el combinador 314 y el verificador. El controlador 324 ordena al generador de juego de claves 326 que genere una segunda combinación de bits o de caracteres en calidad de una segunda subclave 206, donde la segunda combinación de bits o de caracteres se selecciona una a una del conjunto de las segundas subclaves posibles. Acto seguido, el controlador324 ordena al combinador 314 que combine la primera subclave y la segunda subclave a una clave 210. Después, el controlador 324 ordena al verificador que verifique si la clave es válida 212 o no. Si el verificador 320 ha comprobado que la clave es válida, el controlador 324 ordena al dispositivo de descifrado 322 que descifre los datos con la clave y/o que utilice la clave como una contraseña de autentificación en un ordenador externo 404 o en un servicio que se ejecute en el mismo ordenador o en un ordenador diferente 404. El verificador 320 puede estar conectado al ordenador externo con el fin de verificar si la contraseña es válida o no y/o a un dispositivo externo 402 donde está almacenado el flujo de datos que se va a descifrar. Hay que entender que el flujo de datos que se tiene que descifrar también puede estar almacenado en el aparato de cifrado y de descifrado 302.

De conformidad con la presente invención, la seguridad de la clave aumenta, ya que un atacante tiene que probar un número exponencialmente más alto de claves en comparación con el estado anterior de la técnica que no tiene una segunda subclave desconocida. La mayor seguridad de la clave se debe a que el atacante tiene que probar un mayor número de claves, lo que el inventor de la presente invención llama “fuerza forzada”. Por consiguiente, la seguridad de la clave aumenta por el factor determinado por el tiempo de espera que el posible usuario considera aceptable con el fin de generar la segunda subclave y

de verificar la misma para autentificar e iniciar sesión en el sistema informático. El usuario conoce los a bits de la primera subclave. El aparato y el método innovadores de cifrado y de descifrado generan másb bits que se encuentran en una segunda subclave. La primera subclave y la segunda subclave están combinadas por la concatenación, por la inserción de una clave dentro de la otra, por la adición de una clave al principio o al final de la otra clave, así como por el entrelazado de las subclaves. Esto hace que el atacante tenga que probar las claves 2^{a+b}. La presente invención ofrece la ventaja de que de este modo una clave que un usuario humano memorice pueda garantizar una protección eficaz frente a un ataque de fuerza bruta.

Reivindicaciones

1. Método de autentificación, que consta de los siguientes pasos de registro:

- el envío de una solicitud de una primera combinación de bits o de caracteres en calidad de una primera subclave (102);
- el almacenamientodela primera combinación de bitso de caracteres mencionada en la memoria (104);
- la generación de una segunda combinación de bits o de caracteres en calidad de una segunda subclave (106),
  donde la segunda combinación de bits o de caracteres es un patrón aleatorio o pseudoaleatorio; y
- la combinación de la primera subclave mencionada y de la segunda subclave mencionada a una clave (108); y
- además se compone del siguiente paso:

    - el uso de la clave en calidad de una contraseña de autentificación (112);

se compone, además, de los siguientes pasos de verificación para el inicio de sesión:

- el envío de una solicitud de una primera combinación de bits o de caracteres en calidad de una primera subclave (202);
- el almacenamiento de la primera combinación de bits o de caracteres mencionada en la memoria (204);
- la repetición de los siguientes pasos hasta que se haya verificado que una clave es válida:

    - la generación de una segunda combinación de bitso de caracteres arbitraria en calidad de una segunda subclave (206) a partir del conjunto de todas las segundas subclaves posibles (208);
    - la combinación de la primera subclave mencionada y de la segunda subclave mencionada a la clave (210);
    - la verificación de si la clave es válida o no (212), por medio de la autentificación con el uso de la contraseña; y

- si se ha comprobado que la clave mencionada es válida, el uso de la clave en calidad de una contraseña de autentificación (216) en el ordenador;

donde los pasos de combinación de la primera subclave y de la segunda subclave incluyen al menos uno de los siguientes pasos:

- la concatenación de la primera subclave y de la segunda subclave;
- la inserción de la segunda subclave en una posición arbitraria de la primera subclave;

- la inserción de la primera subclave en una posición arbitraria de la segunda subclave;
- la adición de la segunda subclave al final o al principio de la primera subclave; y
- el entrelazado de la primera subclave y de la segunda subclave.

2. Método de cifrado implementado por un ordenador que consta de los siguientes pasos para el cifrado:

- el envío de una solicitud de una primera combinación de bits ode caracteres en calidad de una primera subclave (102) para el cifrado;
- el almacenamientode la primera combinación de bits o de caracteres mencionada en la memoria (104);
- la generación de una segunda combinación de bits o de caracteres en calidad de una segunda subclave (106) para el cifrado, donde la segunda combinación de bits o de caracteres es un patrón aleatorio o pseudoaleatorio; y
- la combinación de la primera subclave mencionada para el cifrado y de la segunda subclave mencionada para el cifradoa una clave (108) para el cifrado; y
- también consta de al menos uno de los siguientes pasos:

    - el cifrado de los datos con la clave (110) para el cifrado;
    - el uso de la clave para el cifrado en calidad de una contraseña de autentificación (112);

consta, además, de los siguientes pasos para el descifrado:

- el envío de una solicitud de una primera combinación de bits o de caracteres en calidad de una primera subclave (202) para el descifrado;
- el almacenamientode la primera combinación de bits o de caracteres mencionada en la memoria (204);
- la repetición de los siguientes pasos hasta que se haya verificado que una clavede descifrado es válida:

    - la generación de una segunda combinación de bitso de caracteres arbitraria en calidad de una segunda subclave (206) para el descifrado a partirdel conjunto de todas las segundas subclaves posibles (208) para el descifrado;
    - la combinación de la primera subclave mencionada y de la segunda subclave mencionada a la clave (210) para el descifrado;
    - la verificación de si la clave para la autentificación es válida o no (212) al intentar descifrar los datos; y

- si se ha comprobado que la clave de descifrado mencionada es válida, el descifrado de los datos con la clave (214) para el descifrado;

donde los pasos referentes a la combinación de la primera subclave y de la segunda subclave conlleva al menos uno de los siguientes pasos:

- la concatenación de la primera subclave y de la segunda subclave;
- la inserción de la segunda subclave en una posición arbitraria de la primera subclave;
- la inserción de la primera subclave en una posición arbitraria de la segunda subclave;
- la adición de la segunda subclave al final o al principio de la primera subclave; y
- el entrelazado de la primera subclave y de la segunda subclave.

3. Método de conformidad con la reivindicación número 2, donde

- el paso de cifrado incluye el paso de la generación y del almacenamiento de un valor de hash basado en la clave; y/o
- el paso de descifrado incluye el paso de la generación de un valor de hash y de la comparacióndel valor de hash que se ha generado con un valor de hash que esté almacenado.

4. Método de conformidad con cualquiera de las reivindicaciones que van de la 1 a la 3, donde el paso del envío de una solicitud incluye el paso del envío de una solicitud al usuario para que introduzca la primera subclave.

5. Método de conformidad con cualquiera de las reivindicaciones que van de la 1 a la 4, donde la segunda subclave tiene una longitud diferente a la de la primera subclave.

6. Aparato de autentificación (302) implementado por un ordenador que está adaptado para autentificar, que se compone de:

- un dispositivo de solicitud (304) que está adaptado para solicitar unaprimera combinación de bits o de caracteres en calidad de una primera subclave;
- una memoria (310) para almacenar la primera combinación de bits o de caracteres mencionada;
- un generador aleatorio o pseudoaleatorio (312) que está adaptado para generar una segunda combinación de bits o de caracteres en calidad de una segunda subclave aleatoria o pseudoaleatoria; y
- un combinador (314) que está adaptado para combinar la primera subclave mencionada y la segunda subclave mencionada a una clave;
- también se compone de
    - un generador de contraseñas (318) que está adaptado para generar una contraseña basada en la clave;

- donde el dispositivo de solicitud (304) está adaptado para solicitar una primera combinación de bits o de caracteres en calidad de una primera subclave para el inicio de sesión;
- donde la memoria (310) está adaptada para almacenar la primera combinación de bits o de caracteres mencionada;
- se compone también de un generador de juego de claves (326);
- se compone también de un verificador (320) que está adaptado para verificar si la clave es válida o no; y
- se compone también de un controlador (324) que está adaptado para controlar el generador de juego de claves (326), el combinador (314) y el verificador (320) al

    - indicar al generador de juego de claves (326) que genere una segunda subclave arbitraria en calidad de una combinación de bits o de caracteres en calidad de una segunda subclave a partir del conjunto de todas las segundas subclaves posibles (208);
    - indicaral combinador (314) que combine la primera subclave mencionada y la segunda subclave mencionada a una clave;
    - indicar al verificador (320) que verifique si la clave es válida o no; y
    - si el verificador (320) ha comprobado que la clave mencionada es válida, utilizar la clave en calidad de una contraseña de autentificación en el ordenador para el inicio de sesión;

donde el combinador (314) está adaptado para al menos uno de los siguientes pasos:

- la concatenación de la primera subclave y de la segunda subclave;
- la inserción de la segunda subclave en una posición arbitraria de la primera subclave;
- la inserción de la primera subclave en una posición arbitraria de la segunda subclave;
- la adición de la segunda subclave al final o al principio de la primera subclave;
- el entrelazado de la primera subclave y de la segunda subclave.

7. Un aparato de cifrado y de descifrado (302) implementado por un ordenador que está adaptado para el cifrado y el descifrado, que se compone de:

- un dispositivo de solicitud (304) que está adaptado para solicitar una primera combinación de bits o de caracteres en calidad de una primerasubclave para el cifrado;
- una memoria (310) para almacenar la primera combinación de bits o de caracteres mencionada para el cifrado;
- un generador aleatorio o pseudoaleatorio (312) que está adaptado para generar una segunda combinación de bits o de caracteres en calidad de una segunda subclave aleatoria o pseudoaleatoria para el cifrado; y

- un combinador (314) que está adaptado para combinar la primera subclave mencionada para el cifrado y la segunda subclave mencionada para el cifradoa una clave para el cifrado;
- que se compone también de

    - un dispositivo de cifrado (316) que está adaptado para cifrar los datos con la clave para el cifrado; y/o
    - un generador de contraseñas (318) que está adaptado para generar una contraseña basada en la clave para el cifrado;

- donde el dispositivo de solicitud (304) está adaptado para solicitar una primera combinación de bits o de caracteres en calidad de una primera subclave para el descifrado;
- donde la memoria (310) está adaptada para almacenar la primera combinación de bits o de caracteres mencionada para el descifrado;
- se compone, además, de un generador de juego de claves (326);
- se compone, además, de un verificador (320) que está adaptado para verificar si la clave para el descifradoes válida o no; y
- se compone, además, de un controlador (324) que está adaptado para controlar el generador de juego de claves (326), el combinador (314), el verificador (320) y el dispositivo de descifrado (322) al

    - indicar al generador de juego de claves (326) que genere una segunda subclave arbitraria para descifrar en calidad de una combinación de bits o de caracteres a partir de un conjuntode todas las segundas subclaves posibles para el descifrado;
    - indicar al combinador (314) que combine la primera subclave mencionada para el descifrado y la segunda subclave mencionada para el descifradoa una clave para el descifrado;
    - indicar al verificador (320) que verifique si la clave para el descifradoes válida o no; y
    - si el verificador (320) ha comprobado que la clave para descifrar mencionada es válida, indicar a un dispositivo de descifrado (322) que está adaptado para descifrar los datos con la clave para el descifrado, que descifre los datos con la clave para el descifrado;

donde el combinador (314) está adaptado para al menos uno de los siguientes pasos:

- la concatenación de la primera subclave y de la segunda subclave;
- la inserción de la segunda subclave en una posición arbitraria de la primera subclave;
- la inserción de la primera subclave en una posición arbitraria de la segunda subclave;
- la adición de la segunda subclave al final o al principio de la primera subclave;

- el entrelazado de la primera subclave y de la segunda subclave.

8. Aparato (302) de conformidad con la reivindicación número 7, donde

- el dispositivo de cifrado (316) está adaptado para generar un valor de hash basado en la clave;
- el dispositivo de descifrado (322) está adaptado para generar un valor de hash basado en la clave y para comparar el valor de hash con un valor de hash que esté almacenado.

9. Aparato de descifrado (302) de conformidad con la reivindicación número 7 u 8, donde el verificador (320) está adaptado para descifrar los datos con la clave.

10. Aparato (302) de conformidad con cualquiera de las reivindicaciones que van de la 6 a la 9, donde el dispositivo de solicitud (304) está adaptado para solicitar al usuario que introduzca la primera subclave.

11. Aparato (302) de conformidad con cualquiera de las reivindicaciones que van de la 6 a la 10, donde la segunda subclave tiene una longitud diferente a la de la primera subclave.

12. Producto de programa informático que incluye instrucciones que, cuando se transfieren a un ordenador que consta de un procesador y de una memoria, ejecutan el método de conformidad con cualquiera de las reivindicaciones que van de la 1 a la 5.

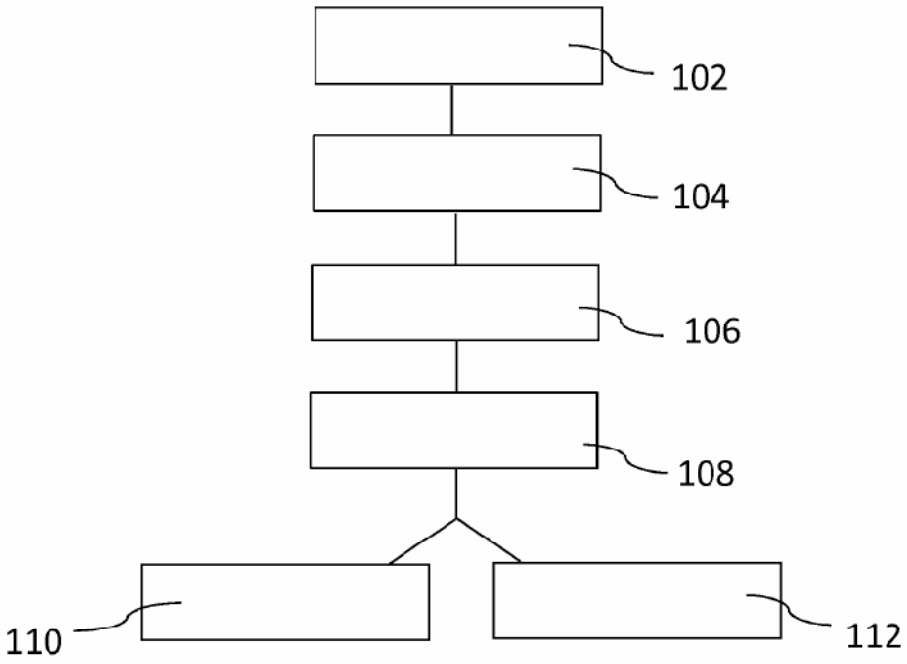

Fig. 1

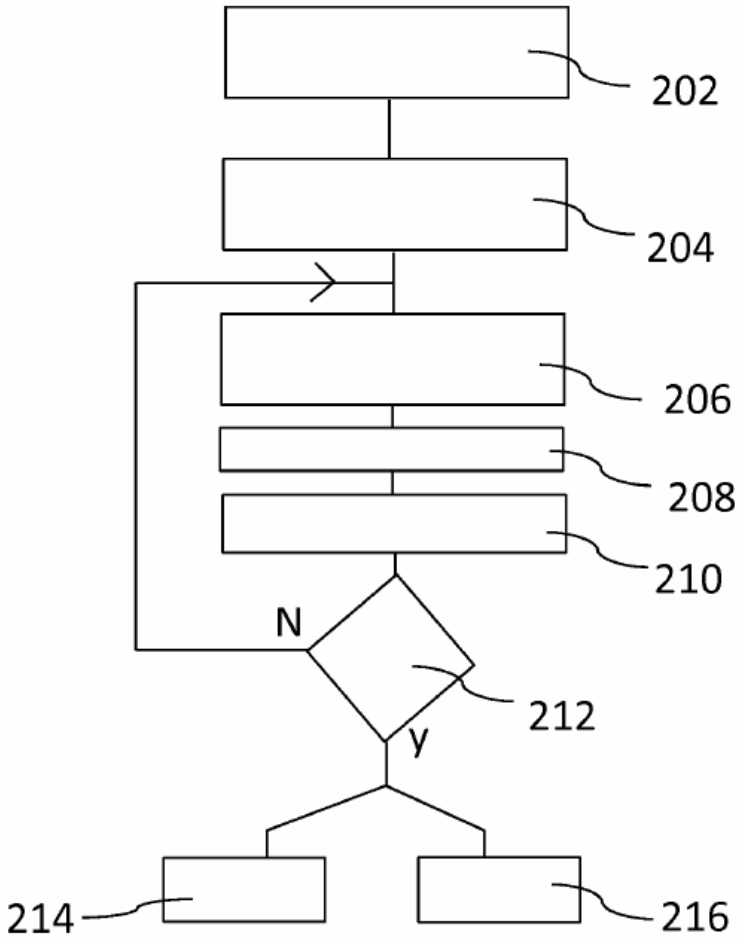

Fig. 2

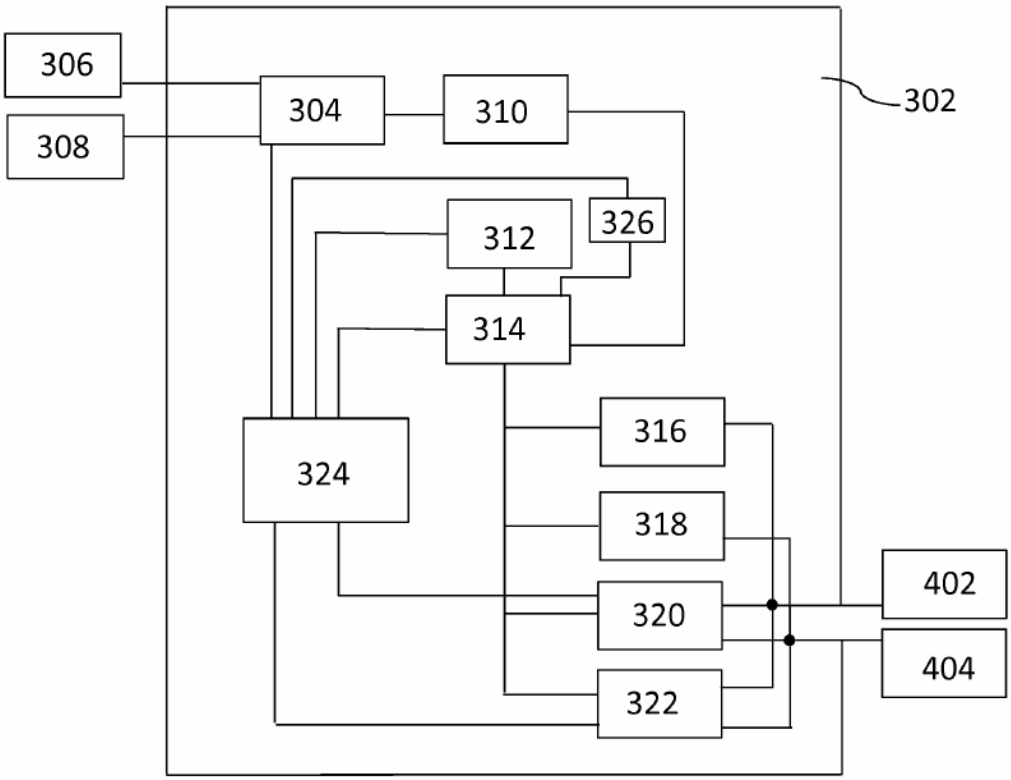

Fig. 3