(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 731 775**

(51) Int. CI.:

H04L 9/08 (2006.01)
H04L 9/32 (2006.01)
G09C 1/00 (2006.01)
G06F 21/62 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **18.04.2014 PCT/US2014/034582**

(87) Fecha y número de publicación internacional: **23.10.2014 WO14172593**

(96) Fecha de presentación y número de la solicitud europea: **18.04.2014 E 14784894 (9)**

(97) Fecha y número de publicación de la concesión europea: **20.03.2019 EP 2987267**

(54) Título: **Sistema y procedimientos de cifrado de datos**

(30) Prioridad:

18.04.2013 US 201361813186 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
19.11.2019

(73) Titular/es:

RISOFTDEV, INC. (100.0%)
1480 Moraga Road, Suite I 351
Moraga, CA 94556, US

(72) Inventor/es:

GILBERT, VINCENT, LOGAN

(74) Agente/Representante:

PADIAL MARTÍNEZ, Ana Belén

DESCRIPCIÓN

Sistema y procedimientos de cifrado de datos

CAMPO TÉCNICO:

Los aspectos de esta invención se refieren en general a la criptografía informática y, más particularmente, a un sistema mejorado y a procedimientos asociados para cifrar datos.

ANTECEDENTES DE LA TÉCNICA:

A modo de antecedentes, se han desarrollado varios procedimientos a lo largo de los años para asegurar el acceso a datos electrónicos y comunicaciones relacionadas. Un procedimiento común implica el uso de algoritmos de cifrado simétricos, que emplean una clave para cifrar y descifrar datos. La clave se utiliza de tal manera que, sin ella, los datos no se pueden descifrar fácilmente. El problema principal con este procedimiento es que cualquier persona que posea la clave puede usarla para descifrar los datos. Algunas tecnologías de ofuscación clave han intentado resolver este problema empleando un procedimiento que cifra la clave mediante una clave principal, también conocida como clave negra o clave de cifrado de clave ("KEK"). En otras palabras, la clave utilizada para cifrar los datos está auto-cifrada mediante la KEK. Sin embargo, un sistema de este tipo a menudo no es útil en diversas aplicaciones, ya que típicamente requieren hardware relativamente caro. Además, aunque este tipo de sistema tiende a funcionar bien en sistemas basados en hardware donde la "caja negra" es relativamente segura, en general no funciona bien en sistemas basados en software o entornos domésticos/de consumo, ya que el problema es dónde almacenare de forma segura la KEK. Esto se debe a que, si la KEK se ve comprometida alguna vez, hace que todas las claves emitidas sean vulnerables. Por lo tanto, muchos procedimientos de cifrado no se basan en cifrar la clave con una KEK, sino que simplemente se basan en claves generadas aleatoriamente.

Los dispositivos electrónicos, como los ordenadores, a menudo son capaces de generar secuencias aleatorias para la criptografía junto con una variedad de otros propósitos, como juegos de azar, muestreo estadístico, simulación por ordenador y otras áreas donde una secuencia aleatoria es útil para producir un resultado impredecible. Algunos dispositivos electrónicos están configurados para generar secuencias aleatorias utilizando un generador de números aleatorios de hardware, mientras que otros dependen del software. Estas técnicas basadas en software a menudo generan un número predeterminado de secuencias aleatorias. El software de esta naturaleza se conoce comúnmente como un generador de números pseudoaleatorios ("PRNG") porque no genera una secuencia verdaderamente aleatoria cuando se compara con un generador de números aleatorios de hardware típico. Hay al menos dos áreas principales donde los fallos están expuestos en la operación de cualquier PRNG. Primero, si el valor original que se usa para generar la secuencia no es lo suficientemente diversa, la secuencia pseudoaleatoria resultante es potencialmente predecible y, por lo tanto, representa un riesgo bajo la amenaza de ser adivinada. En segundo lugar, incluso si se puede producir un valor original suficientemente diverso dadas las consideraciones ambientales, si esas condiciones son capaces de ser determinadas y reproducidas, la secuencia pseudoaleatoria resultante todavía presenta un riesgo bajo la amenaza de ser adivinada. Los intentos de mejorar el estado de la técnica conocido han girado en torno a tratar de mejorar el propio PRNG por diversos medios relacionados con el aumento de la entropía de valores originales aleatorios. Sin embargo, el problema con estos tipos de soluciones es que requieren que la mejora se incorpore al PRNG que se está utilizando. Por lo tanto, existe la necesidad de aumentar la seguridad y el rendimiento de dicho PRNG sin requerir que se altere la funcionalidad del PRNG.

Un problema adicional asociado con los PRNG de la técnica anterior son las probabilidades relativas asociadas con un número o carácter particular que se incluye en el valor pseudoaleatorio. En un poco más de detalle, al generar una secuencia numérica, un PRNG debe elegir uno de los diez valores de números enteros: 0, 1, 2, 3, 4, 5, 6, 7, 8 o 9. Independientemente de los medios utilizados para generar un valor pseudoaleatorio, ese valor final debe estar dentro de este rango. Lo mismo sería cierto de los valores alfanuméricos pseudoaleatorios (es decir, 0-9 y AZ, posiblemente incluso incluyendo otros caracteres ASCII). Dependiendo de la fuerza del PRNG, una secuencia aleatoria de diez lugares podría ser tan débil como 7526435744, por ejemplo. La probabilidad de que se incluya un número aumenta a medida que aumenta la longitud de la secuencia generada. Por lo tanto, es más probable que una secuencia que sea el doble de larga incluya un número fuera de los seleccionados en la secuencia original (por ejemplo, 30820913007504796977). Esta probabilidad aumenta a medida que aumenta la longitud de la secuencia pseudoaleatoria. Además, una vez que se determina la longitud de la clave, descifrar una clave de cifrado es tan simple como ejecutar cada permutación de combinaciones de números para una clave de esa longitud.

Otro problema asociado con los algoritmos de cifrado simétricos conocidos de la técnica anterior es que, ya sea por diseño o en su implementación, no generarán nada o generarán un error o excepción cuando se intente utilizar una clave incorrecta. Esto, a su vez, facilita el uso de técnicas automatizadas o semiautomáticas de craqueo de fuerza bruta para determinar la clave correcta. Lo único que debe hacer la persona que intenta hacer el crack es ejecutar cada combinación posible de caracteres que potencialmente conforman la clave hasta que se logre una salida legible. Los algoritmos de cifrado teóricos que generarían datos legibles cuando se

presentaran con una clave incorrecta se rechazaron por no ser prácticos debido a la naturaleza desconocida de los datos que se cifraron.

Los aspectos de la presente invención se dirigen a resolver todos estos problemas y proporcionan otras ventajas relacionadas, como se describe en el siguiente sumario.

La solicitud de patente estadounidense US 2013/067551 A1 divulga un sistema que incluye una memoria operable para almacenar un identificador de cuenta de usuario asociado con una cuenta de usuario y una primera y segunda credencial de usuario, en el que la segunda credencial de usuario comprende datos de entrada de usuario capturados por un sensor. La solicitud de patente estadounidense US 2012/0063597 A1 divulga un procedimiento para intercambiar claves de sesión secretas para su uso en cifrado simétrico utilizando una tabla de números aleatorios.

DIVULGACIÓN DE LA INVENCIÓN:

La presente invención resuelve los problemas descritos anteriormente proporcionando un sistema y procedimientos asociados para cifrar datos. En al menos un modo de realización, un administrador de claves está ubicado en la memoria en al menos un dispositivo informático y está configurado para crear y administrar al menos una clave de cifrado para usar para cifrar los datos. Un al menos un archivo de clave también se encuentra en la memoria en al menos un dispositivo informático y está asociado con al menos un usuario autorizado. El archivo de clave contiene un campo de clave que comprende una secuencia de bytes pseudoaleatoria y un valor de hash único utilizado para asociar el archivo de clave al usuario. Un conjunto de caracteres base se selecciona aleatoriamente en el campo de clave, de modo que los caracteres base son un subconjunto del campo de clave. A continuación se genera una clave de cifrado al introducir los caracteres base en un algoritmo de cifrado. A continuación, los datos se cifran utilizando la clave de cifrado.

Un objetivo principal inherente al aparato y procedimiento de uso descritos anteriormente es proporcionar ventajas no enseñadas por la técnica anterior.

Otras características y ventajas de los aspectos de la presente invención se harán evidentes a partir de la siguiente descripción más detallada, tomada junto con los dibujos adjuntos, que ilustran, a modo de ejemplo, los principios de los aspectos de la invención.

BREVE DESCRIPCIÓN DE LOS DIBUJOS:

Los dibujos adjuntos ilustran aspectos de la presente invención. En tales dibujos:

La Figura 1 es un diagrama de arquitectura de un sistema a modo de ejemplo para cifrar datos, de acuerdo con al menos un modo de realización;

la Figura 2 es un diagrama de bloques que ilustra una estructura de datos de archivo de claves a modo de ejemplo, de acuerdo con al menos un modo de realización;

la Figura 3 es una ilustración de un campo de clave a modo de ejemplo, de acuerdo con al menos un modo de realización;

la Figura 4 es una ilustración de un valor de hash a modo de ejemplo, de acuerdo con al menos un modo de realización;

la Figura 5 es un diagrama de flujo de un procedimiento a modo de ejemplo para cifrar datos, de acuerdo con al menos un modo de realización;

la Figura 6 es una ilustración de un conjunto a modo de ejemplo de caracteres base, como se obtiene del campo de clave a modo de ejemplo, de acuerdo con al menos un modo de realización;

la Figura 7 es un diagrama de flujo de un procedimiento a modo de ejemplo para generar una secuencia de bytes pseudoaleatoria, de acuerdo con al menos un modo de realización;

la Figura 8 es una ilustración de una secuencia pseudoaleatoria a modo de ejemplo obtenida a partir de una secuencia pseudoaleatoria a modo de ejemplo larga, de acuerdo con al menos un modo de realización;

la Figura 9 es una ilustración de una parte a modo de ejemplo de datos confidenciales cifrados con un token conocido, de acuerdo con al menos un modo de realización; y

la Figura 10 es un diagrama de flujo de un procedimiento a modo de ejemplo para combatir los intentos de craqueo de fuerza bruta, de acuerdo con al menos un modo de realización.

Las figuras de dibujo descritas anteriormente ilustran aspectos de la invención en al menos uno de sus modos de realización a modo de ejemplo, que se definen con más detalle en la siguiente descripción. Las características,

elementos y aspectos de la invención a los que se hace referencia con los mismos números en diferentes figuras representan características, elementos o aspectos iguales, equivalentes o similares, de acuerdo con uno o más modos de realización.

DESCRIPCIÓN DETALLADA:

Las figuras de dibujo descritas anteriormente ilustran aspectos de la invención en al menos uno de sus modos de realización a modo de ejemplo, que se definen con más detalle en la siguiente descripción.

Volviendo ahora a la Fig. 1, se muestra un diagrama de arquitectura de un sistema a modo de ejemplo **20** para cifrar datos, de acuerdo con al menos un modo de realización. El sistema **20** comprende, en el modo de realización a modo de ejemplo, un administrador de claves **22**, un generador de números pseudoaleatorios ("PRNG") **24**, un módulo de cifrado **26**, al menos un archivo de claves **28** y al menos una aplicación de cliente **30**, cada uno residiendo en la memoria **32** en al menos un dispositivo informático **34**. Debe tenerse en cuenta que el término "memoria" pretende incluir cualquier tipo de medio de almacenamiento electrónico (o combinación de medios de almacenamiento) que se conozca o desarrolle más adelante, como discos duros locales, RAM, memoria flash, dispositivos de almacenamiento externos, red o dispositivos de almacenamiento en la nube, etc. Además, los diversos componentes del sistema **20** pueden residir en la memoria **32** en un único dispositivo informático **34**, o pueden residir por separado en dos o más dispositivos informáticos **34**. Además, el término "dispositivo informático" pretende incluir cualquier tipo de dispositivo informático conocido o desarrollado posteriormente, como ordenadores de escritorio, teléfonos inteligentes, ordenadores portátiles, tablets, dispositivos de juegos, etc.

Con referencia continua a la Fig. 1, en al menos un modo de realización, el administrador de claves **22** crea y administra una o más claves de cifrado que se utilizan para cifrar datos confidenciales **36** y permiten que solo los usuarios autorizados revelen o accedan a los datos confidenciales **36**. Como se explica más adelante, en al menos un modo de realización, el administrador de claves **22** utiliza el PRNG **24** durante ciertos pasos para crear la clave de cifrado.

En al menos un modo de realización, el módulo de cifrado **26** lleva a cabo el proceso de recibir datos confidenciales **36** y generar un token **38** para usar en su lugar. En otras palabras, utilizando la clave de cifrado asociada, el módulo de cifrado **26** genera el token **38**, cifra los datos confidenciales originales **36** y almacena los datos cifrados **40** en la memoria **32**. El token **38** es simplemente una referencia a los datos cifrados **40**; no existe una relación matemática entre el token **38** y los datos cifrados **40**. Por lo tanto, el token **38** se puede usar de manera segura en todo el sistema **20**, mientras que los datos cifrados **40** que representa permanecen almacenados en la memoria **32**. El módulo de cifrado **26** garantiza que existe una relación de uno a uno entre los datos confidenciales **36** y el token generado **38**, de modo que la integridad referencial se mantiene en todo el sistema **20**.

La al menos una aplicación de cliente **30** puede ser cualquiera de una variedad de aplicaciones o plataformas, ahora conocidas o desarrolladas posteriormente, involucradas en la recopilación, manejo o procesamiento de datos confidenciales **36** y configuradas para comunicarse con el administrador de claves **22** y el módulo de cifrado **26** para cifrar y descifrar los datos confidenciales **36**. Por ejemplo, la aplicación de cliente **30** puede ser una aplicación financiera para procesar o analizar los pagos recibidos por una empresa comercial. Otra aplicación de cliente **30** puede ser un dispositivo de punto de venta, como una caja registradora o un lector de tarjetas de pago.

Como se muestra en la Fig. 2, un modo de realización a modo de ejemplo de al menos un archivo de clave **28** se ilustra a modo de ejemplo como una estructura de datos que almacena ciertos valores asociados con una clave de cifrado. En al menos un modo de realización alternativo, el archivo de clave **28** es un archivo de texto. El archivo de clave **28** comprende, en al menos un modo de realización, una cabecera **42**, un campo de clave **44**, un valor de hash **46**, y la información de propietario **48**. La cabecera **42** contiene cierta información de versión para el archivo de clave **28**. Como se muestra en la ilustración a modo de ejemplo de la Fig. 3, el campo de clave **44** es una secuencia de bytes pseudoaleatoria. En el modo de realización a modo de ejemplo, el campo de clave **44** es generado por el PRNG **24**; sin embargo, en modos de realización alternativos, el campo de clave **44** puede generarse por cualquier otro medio adecuado, ahora conocido o desarrollado posteriormente, capaz de generar una secuencia de bytes aleatoria o pseudoaleatoria. Como se muestra en la ilustración a modo de ejemplo de la Fig. 4, el valor de hash **46** es un identificador único que se genera y bloquea el archivo de clave **28** a su propietario asociado (es decir, usuario), y al dispositivo informático de origen **34**. Sin embargo, en al menos un modo de realización, el sistema **20** proporciona una función de exportación que permite que el archivo de clave **28** sea portátil para su uso en diferentes dispositivos informáticos. Los detalles de cómo se obtiene cada uno de los campos de clave **44** y el valor de hash **46** (junto con la clave de cifrado asociada), en al menos un modo de realización, se explican a continuación. Refiriéndose nuevamente a la Fig. 2, la información del propietario **48** contiene detalles relacionados con el propietario del archivo de clave **28**, como un nombre de usuario, dirección IP, etc.

Como se mencionó anteriormente, el sistema **20** no cifra la clave de cifrado. Por lo tanto, el sistema **20** no se basa en una KEK. En su lugar, y como se ilustra en el diagrama de flujo de la Fig. 5, el administrador de claves **22** primero genera el campo de clave **44** como una secuencia de bytes, o caracteres pseudoaleatoria (**100**). En uso, en al menos un modo de realización, antes de continuar, el sistema **20** verifica si el usuario es nuevo (**102**). Para usuarios nuevos, el sistema **20** solicita al usuario que introduzca ciertas variables específicas del usuario, como un nombre de usuario y una frase de contraseña (**104**). Los datos seleccionados, como el campo de clave **44**, la frase de contraseña y otras variables ambientales y/o proporcionadas por el usuario (es decir, la fecha y/o la hora del dispositivo informático, la versión del sistema operativo, el nombre de usuario, la dirección IP, etc.) se introducen en una función hash que, a su vez, obtiene el valor de hash único **46** (**106**). Al utilizar nuevamente el sistema **20**, la identidad del usuario y los derechos de acceso asociados se verifican basándose en el valor de hash **46** (**108**). En uno de tales modos de realización, se le pide al usuario que vuelva a introducir su frase de contraseña, sobre la cual el sistema **20** realiza la función de hash usando las mismas variables para comparar el resultado con el valor de hash **46** almacenado en el archivo de clave **28** del usuario. En un modo de realización alternativo, el sistema **20** simplemente verifica si el usuario tiene un archivo de clave **28** ya almacenado en la memoria **32**.

A continuación, como se ilustra en la Fig. 6, el administrador de claves **22** emplea un algoritmo de extracción de claves para construir un conjunto de caracteres base **50** que se seleccionan al azar del campo de clave **44** (**110**). El conjunto de caracteres base **50** es relativamente más pequeño que el campo de clave **44**, y los caracteres particulares que se seleccionarán aleatoriamente (y preferentemente no contiguamente) del campo de clave **44** están determinados por el algoritmo de extracción de clave basándose en diversos aspectos ambientales y/o variables suministradas por el usuario. De esta manera, el archivo de clave **28** aumenta la entropía al aumentar el número de caracteres generados aleatoriamente en el campo de clave **44**, y a continuación seleccionando aleatoriamente la longitud de secuencia necesaria dentro de este grupo extendido para llegar al conjunto de caracteres base **50**. En otras palabras, el uso del archivo de clave **28** reduce en gran medida la posibilidad de que instalaciones dispares del sistema **20** dupliquen un campo de clave dado **44**. Con respecto al algoritmo de extracción de clave utilizado para construir el conjunto de caracteres base **50**, los detalles de ese algoritmo no se divulgarán en el presente documento, a fin de salvaguardar la integridad del sistema **20** y los procedimientos asociados de cifrado de datos confidenciales **36**. Además, debido a que el conjunto de caracteres base **50** no es visible, cualquier intento de ingeniería inversa del algoritmo de extracción de clave sería arduo en el mejor de los casos.

Con referencia continua a la Fig. 5, una vez construido, el conjunto de caracteres base **50** se introduce en un algoritmo de cifrado que, a su vez, obtiene la clave de cifrado (**112**). El módulo de cifrado **26** puede entonces cifrar los datos confidenciales **36** utilizando la clave de cifrado. En el modo de realización a modo de ejemplo, el administrador de claves **22** también es capaz de especificar la longitud deseada de la clave de cifrado, permitiendo que el sistema **20** genere claves de cifrado que sean compatibles con prácticamente cualquier algoritmo de cifrado para su uso en prácticamente cualquier módulo de cifrado.

También es bien sabido que, dado el tiempo, los recursos y el acceso suficientes a un sistema de cifrado particular, incluido el sistema a modo de ejemplo **20** descrito en el presente documento, un individuo o grupo de individuos dedicados podrán discernir su mecánica. Teniendo esto en cuenta, la mayoría de los algoritmos de cifrado se hacen públicos y dependen de la complejidad matemática para la ofuscación. El sistema actual **20**, por otro lado, utiliza una forma de cifrado de algoritmo ofuscado extensible, en el que el algoritmo que crea la clave de cifrado (es decir, el algoritmo de extracción de clave) está oculto. Además, se acepta que, dado el acceso a suficientes claves de cifrado, un esfuerzo dedicado podría eventualmente discernir el algoritmo de extracción de claves. Sin embargo, los elementos del algoritmo de extracción de clave son extensibles; es decir, se pueden modificar simplemente (**116**), y sin cambiar la mecánica fundamental del algoritmo de extracción de clave. Por lo tanto, dado que el algoritmo de extracción de clave debe ser utilizado por un grupo conocido, la versión actualizada del algoritmo de extracción de clave puede estar disponible para este grupo dentro de un período de tiempo predeterminado (basado en el tiempo estimado requerido para el algoritmo de extracción de clave que se va a descifrar), o cuando se determine que el algoritmo de extracción de clave está realmente comprometido (**114**). La clave de cifrado existente se exporta y se envía al usuario una nueva clave de cifrado que utiliza el algoritmo de extracción de clave actualizado. Como tal, cualquier persona que intente descifrar el algoritmo de extracción de clave se verá obligado a comenzar de nuevo. El diseño del algoritmo de extracción de clave permite un número casi ilimitado de patrones, dado el gran número y las posibles combinaciones de diversas variables ambientales y/o proporcionadas por el usuario que el algoritmo de extracción de clave podría utilizar, por no mencionar la amplia gama de valores potencialmente únicos que cada variable de este tipo podría tener.

Como se mencionó anteriormente, en al menos un modo de realización, el campo de clave **44** es generado por el PRNG **24**. En uno de tales modos de realización, como se ilustra en el diagrama de flujo de la Fig. 7, el PRNG **24** primero genera una secuencia pseudoaleatoria larga ("LPRS") **52** de números y/o caracteres (**200**). En la Fig. 8 se muestra una ilustración a modo de ejemplo del LPRS **52**. A continuación, el PRNG **24** construye una secuencia pseudoaleatoria **54** eligiendo un punto de entrada pseudoaleatorio **56** (**202**) y seleccionando un número predefinido de dígitos consecutivos (y/o caracteres) en el LPRS **52**, comenzando en el punto de entrada pseudoaleatorio **56** (**204**). Como ejemplo, y como se muestra en la ilustración a modo de ejemplo de la Fig. 8, si el PRNG **24** elige un punto de entrada pseudoaleatorio **56** de "3" y la longitud de la secuencia pseudoaleatoria **54**

debe ser "10", la resultante la secuencia pseudoaleatoria **54** obtenida a partir del LPRS **52** de la Fig. 8 sería "1043726879". Se pueden generar más secuencias pseudoaleatorias **54** según sea necesario (**206**). En otros modos de realización adicionales, el PRNG **24** construye la secuencia pseudoaleatoria **54** seleccionando un número predefinido de dígitos no consecutivos (y/o caracteres) en el LPRS **52**, comenzando en el punto de entrada pseudoaleatorio **56**. De esta manera, al almacenar el LPRS **52** en la memoria **32** y al construir la secuencia pseudoaleatoria **54** de longitud relativamente más corta, la entropía del PRNG **24** aumenta de este modo. Además, en los modos de realización en los que la memoria **32** del sistema **20** no es local al dispositivo informático **34** que aloja el PRNG **24**, el LPRS **52** forma una capa de abstracción que evita que alguien que intente adivinar la secuencia pseudoaleatoria **54** use el conocimiento del hardware del dispositivo informático **34** como base para esa suposición. En pocas palabras, en al menos un modo de realización, el LPRS **52** puede generarse en un dispositivo informático **34** y utilizarse en otro.

Una posible limitación del modo de realización descrito anteriormente del PRNG **24** es que no permite la actualización automática del LPRS **52**. En un poco más de detalle, y con una referencia continua al ejemplo de LPRS **52** de la Fig. 8, hay 90 posibles secuencias únicas pseudoaleatorias de 10 caracteres **54** que se pueden usar simplemente tomando un punto de entrada pseudoaleatorio **56** y contando 10 caracteres hacia adelante. Dado que cualquier dispositivo informático **34** utilizado para lograr esto usaría un PRNG **24** para seleccionar el punto de entrada pseudoaleatorio **56**, el número real de secuencias pseudoaleatorias únicas **54** que podrían seleccionarse antes de ver las repeticiones sería mucho menor. Para evitar esta limitación, en al menos un modo de realización, se utiliza una arquitectura extendida que permite el almacenamiento y la recuperación del conjunto de caracteres que se utilizó para crear el LPRS **52**. Esto permite la actualización periódica automática del LPRS **52**(**208**), basado en el conjunto de caracteres, lo cual reduce la probabilidad de que se repita una determinada secuencia pseudoaleatoria **54**.

Cabe señalar que, mientras que el PRNG **24** se analiza en el presente documento en el contexto del sistema de cifrado de datos a modo de ejemplo **20**, el PRNG **24** se puede utilizar por separado en cualquier otra aplicación en la que se necesita un byte pseudoaleatorio, o una serie de bytes pseudoaleatorios.

En al menos un modo de realización, el sistema **20** emplea pasos adicionales para combatir y disminuir la probabilidad de intentos de fuerza bruta de descifrar la clave de cifrado y/o el algoritmo de extracción de clave. En resumen, como se muestra en la ilustración a modo de ejemplo de la Fig. 9, el sistema **20** incluye un token **38** al principio y al final de los datos confidenciales **36** que deben cifrarse. Debido a que el token **38** es un valor conocido y porque el token **38** se crea utilizando la misma clave de cifrado, cualquier clave de cifrado que no sea la clave utilizada para cifrar los datos confidenciales **36** (y, por lo tanto, el token **38**) no reconstruirá correctamente el token **38** tras el descifrado. De esta manera, se puede determinar fácilmente si una clave de cifrado es la clave correcta. En modos de realización adicionales, se emplean procedimientos para generar datos distintos de los datos cifrados **40**. Como resultado, ya que no hay forma de que la persona que intenta violar los datos cifrados **40** con fuerza bruta sepa si los datos que están viendo son idénticos a los datos confidenciales **36** que estaban cifrados, la cantidad de ciclos necesarios para descifrar la clave de cifrado y/o el algoritmo de extracción de clave se vuelve extremadamente alto.

En uno de tales modos de realización, como se ilustra en el diagrama de flujo de la Fig. 10, el módulo de cifrado **26** primero genera un token **38** que tiene un valor conocido (**300**) e inserta un primer a modo de ejemplo **58** del token conocido **38** al comienzo de los datos confidenciales **36** para cifrar (**302**). A continuación, se genera aleatoriamente un valor de suma de comprobación **60** (**304**). En el modo de realización a modo de ejemplo, el valor de suma de comprobación **60** es generado por el PRNG **24**, de acuerdo con el procedimiento descrito anteriormente; sin embargo, en modos de realización alternativos, el valor de suma de comprobación **60** puede generarse por cualquier otro medio adecuado, ahora conocido o desarrollado posteriormente, capaz de generar tal secuencia de bytes aleatoria o pseudoaleatoria. El valor de suma de comprobación **60** se divide luego en una primera parte **62** y una segunda parte **64** (**306**). La primera parte **62** del valor de suma de comprobación **60** se inserta después de la primera instancia **58** del token (**308**), seguida de los datos confidenciales **36** (**310**), seguida de la segunda parte **64** del valor de suma de comprobación **60** (**312**), seguida de una segunda instancia **66** del token **38** (**314**). Toda la secuencia de datos se cifra a continuación utilizando la clave de cifrado (**316**). Por lo tanto, la segunda parte **64** del valor de suma de comprobación **60**, después de los datos confidenciales **36** que se van a cifrar, tiene una relación conocida con la primera parte **62** del valor de suma de comprobación **60**. En la ilustración a modo de ejemplo de la Fig. 9, el valor de suma de comprobación **60** comprende una serie de números enteros que comienzan en la primera parte **62** y continúan en la segunda parte **64**. Esto garantiza que cualquier variación en la clave de cifrado producirá un daño detectable en el token **38** o en el valor de suma de comprobación **60**. Dado que el valor del token **38** es conocido, el módulo de cifrado **26** puede detectar si está dañado o parcialmente dañado debido a que está parcialmente descifrado. Esto permite que el módulo de cifrado **26** emplee varias técnicas para generar datos legibles pero falsos.

Para resumir, con respecto a los modos de realización a modo de ejemplo de la presente invención como se muestra y se describe en el presente documento, se apreciará que se divulga un sistema y un procedimiento para cifrar datos. Debido a que los principios de la invención pueden ponerse en práctica en una serie de configuraciones más allá de las mostradas y descritas, debe entenderse que la invención no está limitada de ninguna manera por los modos de realización a modo de ejemplo, sino que en general se dirige a un sistema y

procedimiento para cifrar datos y puede tomar numerosas formas de hacerlo sin apartarse del espíritu y alcance de la invención. Los expertos en la materia también apreciarán que la presente invención no se limita a las geometrías y materiales de construcción particulares divulgados, sino que puede implicar otras estructuras o materiales funcionalmente comparables, ahora conocidos o desarrollados posteriormente, sin apartarse del espíritu y alcance de la invención. Además, las diversas características de cada uno de los modos de realización descritos anteriormente pueden combinarse de cualquier manera lógica y se pretende que estén incluidas dentro del alcance de la presente invención.

Debe entenderse que el código lógico, los programas, los módulos, los procesos, los procedimientos y el orden en que se realizan los elementos respectivos de cada procedimiento son puramente a modo de ejemplo. Dependiendo de la implementación, pueden realizarse en cualquier orden o en paralelo, a menos que se indique lo contrario en la presente divulgación. Además, el código lógico no está relacionado, o limitado a ningún lenguaje de programación particular, y puede comprender uno o más módulos que se ejecutan en uno o más procesadores en un entorno distribuido, no distribuido o de multiprocesamiento.

El procedimiento descrito anteriormente se puede utilizar en la fabricación de chips de circuitos integrados. Los chips de circuitos integrados resultantes pueden ser distribuidos por el fabricante en forma de oblea sin procesar (es decir, como una sola oblea que tiene múltiples chips sin empaquetar), como un troquel pelado, o en forma empaquetada. En este último caso, el chip se monta en un paquete de un solo chip (como un portador de plástico, con cables que se fijan a una placa base u otro portador de nivel superior) o en un paquete de envío múltiple (como un portador de cerámica que tiene una o ambas interconexiones superficiales de interconexiones enterradas). En cualquier caso, el chip se integra con otros chips, elementos de circuitos discretos y/u otros dispositivos de procesamiento de señales como parte de uno (a) de un producto intermedio, como una placa base, o (b) y un producto final. El producto final puede ser cualquier producto que incluya chips de circuitos integrados, que van desde juguetes y otras aplicaciones de gama baja hasta productos avanzados informáticos que tienen una pantalla, un teclado u otro dispositivo de entrada y un procesador central.

Los aspectos de la presente especificación también se pueden describir de la forma siguiente:

1. Un procedimiento implementado por ordenador para cifrar datos que comprende los pasos de: implementar un administrador de claves en la memoria en al menos un dispositivo informático, estando dicho administrador de claves configurado para crear y administrar al menos una clave de cifrado para usar para cifrar los datos; implementar al menos un archivo de clave en la memoria en al menos un dispositivo informático, estando dicho archivo de clave asociado con al menos un usuario autorizado y que contiene un campo de clave que comprende una secuencia de bytes pseudoaleatoria y un valor de hash único utilizado para asociar la clave de archivo a dicho al menos un usuario; construir un conjunto de caracteres base que se seleccionan aleatoriamente en el campo de clave, siendo el conjunto de caracteres base un subconjunto del campo de clave; generar la clave de cifrado introduciendo los caracteres base en un algoritmo de cifrado; recibir los datos a cifrar; y cifrar los datos utilizando la clave de cifrado.

2. El procedimiento de acuerdo con el modo de realización 1, que comprende además el paso de generar el campo de clave, usando el administrador de claves, como una secuencia de bytes pseudoaleatoria.

3. El procedimiento de acuerdo con los modos de realización 1-2, que comprende además el paso de, al determinar que el usuario es nuevo, obtener información específica del usuario seleccionada del usuario, con dicha información que incluye al menos uno de un nombre de usuario, una frase de contraseña, una fecha actual asociada con el dispositivo informático del usuario, una hora actual asociada con el dispositivo informático del usuario, una versión del sistema operativo asociada con el dispositivo informático del usuario y una dirección IP asociada con el dispositivo informático del usuario.

4. El procedimiento de acuerdo con los modos de realización 1-3, que comprende además el paso de generar el valor de hash único introduciendo al menos una parte de la información específica del usuario en una función de hash.

5. El procedimiento de acuerdo con los modos de realización 1-4, que comprende además el paso de, al determinar que el usuario no es nuevo, verificar la identidad del usuario basándose en el valor de hash.

6. El procedimiento de acuerdo con los modos de realización 1 a 5, que comprende además los pasos de: solicitar al usuario que vuelva a introducir la frase de contraseña; realizar la función hash utilizando la misma información específica del usuario utilizada para generar previamente el valor de hash; y comparar el resultado con el valor de hash almacenado en el archivo de clave asociado con el usuario para determinar si el resultado y el valor de hash son idénticos.

7. El procedimiento de acuerdo con los modos de realización 1-6, en el que el paso de construir un conjunto de caracteres base comprende además el paso de seleccionar aleatoriamente caracteres no contiguos del campo de clave.

8. El procedimiento de acuerdo con los modos de realización 1-7, en el que el paso de construir un conjunto de caracteres base comprende además el paso de seleccionar aleatoriamente caracteres del campo de clave usando un algoritmo de extracción de clave.

9. El procedimiento de acuerdo con los modos de realización 1-8, que comprende además el paso de, al determinar que el algoritmo de extracción de clave se ha comprometido, modificar el algoritmo de extracción de clave y distribuirlo al al menos un usuario autorizado.

10. El procedimiento de acuerdo con los modos de realización 1-9, que comprende además el paso de generar el campo de clave usando un generador de números pseudoaleatorios ("PRNG").

11. El procedimiento de acuerdo con los modos de realización 1-10, que comprende además los pasos de: generar una secuencia pseudoaleatoria larga ("LPRS") de bytes; y construir una secuencia pseudoaleatoria seleccionando un punto de entrada pseudoaleatorio en el LPRS y seleccionando un número predeterminado de bytes en el LPRS que comienza en el punto de entrada pseudoaleatorio.

12. El procedimiento de acuerdo con los modos de realización 1-11, en el que el paso de construir una secuencia pseudoaleatoria comprende además el paso de seleccionar un número predeterminado de bytes consecutivos en el LPRS que comienza en el punto de entrada pseudoaleatorio.

13. El procedimiento de acuerdo con los modos de realización 1-12, en el que el paso de construir una secuencia pseudoaleatoria comprende además el paso de seleccionar un número predeterminado de bytes no consecutivos en el LPRS que comienza en el punto de entrada pseudoaleatorio.

14. El procedimiento de acuerdo con los modos de realización 1-13, que comprende además el paso de implementar el PRNG en memoria en al menos un dispositivo informático.

15. El procedimiento de acuerdo con los modos de realización 1-14, que comprende además el paso de implementar al menos una aplicación de cliente en la memoria en al menos un dispositivo informático, estando dicha aplicación de cliente configurada para comunicarse con el administrador de claves y el módulo de cifrado para cifrar y descifrar la información confidencial. datos.

16. El procedimiento de acuerdo con los modos de realización 1-15, en el que el paso de cifrar los datos comprende además los pasos de: generar un token que tiene un valor conocido; insertar una primera instancia del token al comienzo de los datos; generar aleatoriamente un valor de suma de comprobación; dividir el valor de suma de comprobación en una primera parte y una segunda parte; insertar la primera parte del valor de suma de comprobación entre la primera instancia del token y el comienzo de los datos; insertar la segunda parte del valor de la suma de comprobación al final de los datos; insertar una segunda instancia del token después de la segunda parte del valor de suma de comprobación; y cifrar la secuencia completa de la primera instancia del token, la primera parte del valor de la suma de comprobación, los datos, la segunda parte del valor de la suma de comprobación y la segunda instancia del token utilizando la clave de cifrado.

17. El procedimiento de acuerdo con los modos de realización 1-16, en el que el paso de generar aleatoriamente un valor de suma de comprobación comprende además el paso de generar una serie de números enteros comenzando en la primera parte del valor de suma de verificación y continuando en la segunda parte del valor de suma de comprobación, de manera que dicha primera parte tiene una relación conocida con dicha segunda parte.

18. El procedimiento de acuerdo con los modos de realización 1-17, que comprende además el paso de, al detectar un token dañado o parcialmente dañado debido a que se ha descifrado con una clave de cifrado incorrecta, generar datos legibles pero falsos.

19. Un procedimiento implementado por ordenador para cifrar datos que comprende los pasos de: implementar un administrador de claves en la memoria en al menos un dispositivo informático, estando dicho administrador de claves configurado para crear y administrar al menos una clave de cifrado para usar para cifrar los datos; implementando al menos un archivo de clave en la memoria en al menos un dispositivo informático, estando dicho archivo de clave asociado con al menos un usuario autorizado y conteniendo un campo de clave que comprende una secuencia de bytes pseudoaleatoria y un valor de hash único utilizado para asociar el archivo de clave a dicho al menos un usuario; generar el campo de clave: generando una secuencia pseudoaleatoria larga ("LPRS") de bytes; y construyendo una secuencia pseudoaleatoria seleccionando un punto de entrada pseudoaleatorio en el LPRS y seleccionando un número predeterminado de bytes en el LPRS comenzando en el punto de entrada pseudoaleatorio; construir un conjunto de caracteres base que se seleccionan aleatoriamente en el campo de clave, siendo el conjunto de caracteres base un subconjunto del campo de clave; generar la clave de cifrado introduciendo los caracteres base en un algoritmo de cifrado; recibir los datos a cifrar; y cifrar los datos utilizando la clave de cifrado.

20. Un procedimiento implementado por ordenador para cifrar datos que comprende los pasos de: implementar un administrador de claves en la memoria en al menos un dispositivo informático, estando dicho administrador de claves configurado para crear y administrar al menos una clave de cifrado para usar para cifrar los datos; implementando al menos un archivo de clave en la memoria en al menos un dispositivo informático, estando dicho archivo de clave asociado con al menos un usuario autorizado y conteniendo un campo de clave que comprende una secuencia de bytes pseudoaleatoria y un valor de hash único utilizado para asociar el archivo de clave a dicho al menos un usuario; construir un conjunto de caracteres base que se seleccionan aleatoriamente en el campo de clave, siendo el conjunto de caracteres base un subconjunto del campo de clave; generar la clave de cifrado introduciendo los caracteres base en un algoritmo de cifrado; generar un token que tiene un valor conocido; insertar una primera instancia del token al comienzo de los datos; generar aleatoriamente un valor de suma de comprobación; dividir el valor de suma de comprobación en una primera parte y una segunda parte; insertar la primera parte del valor de suma de comprobación entre la primera instancia del token y el comienzo de los datos; insertar la segunda parte del valor de la suma de comprobación al final de los datos; insertar una segunda instancia del token después de la segunda parte del valor de suma de comprobación; y cifrar la secuencia completa de la primera instancia del token, la primera parte del valor de la suma de comprobación, los datos, la segunda parte del valor de la suma de comprobación y la segunda instancia del token utilizando la clave de cifrado.

Si bien los aspectos de la invención se han descrito con referencia a al menos un modo de realización a modo de ejemplo, los expertos en la técnica deben entender claramente que la invención no está limitada a los mismos. En lugar de eso, el alcance de la invención se debe interpretar solo en conjunto con las reivindicaciones adjuntas y se deja claro aquí que el (los) inventor(es) cree(n) que el objeto reivindicado es la invención.

REIVINDICACIONES

1. Un procedimiento implementado por ordenador para cifrar datos que comprende los pasos de:

implementar un administrador de claves en la memoria en al menos un dispositivo informático, estando dicho administrador de claves configurado para crear y administrar al menos una clave de cifrado que se usará para cifrar los datos;

implementar al menos un archivo de clave en la memoria en al menos un dispositivo informático, estando dicho archivo de clave asociado con al menos un usuario autorizado y conteniendo un campo de clave que comprende una secuencia de bytes pseudoaleatoria y un valor de hash único utilizado para asociar el archivo de clave a dicho al menos un usuario:

en el que el procedimiento se **caracteriza por**:

construir un conjunto de caracteres base (110) que se seleccionan aleatoriamente usando un algoritmo de extracción de clave del campo de clave, siendo el conjunto de caracteres base un subconjunto del campo de clave con al menos uno de esos caracteres seleccionados al azar del campo de clave que no es contiguo con al menos otro carácter seleccionado aleatoriamente del campo de clave, de tal manera que al menos un carácter seleccionado aleatoriamente y al menos otro carácter seleccionado aleatoriamente no están conectados en una secuencia ininterrumpida de caracteres dentro del campo de clave;

generar la clave de cifrado (112) introduciendo los caracteres base en un algoritmo de cifrado;

recibir los datos a cifrar y cifrar los datos utilizando la clave de cifrado.

2. El procedimiento según la reivindicación 1, que comprende además el paso de generar el campo de clave, usando el administrador de claves, como una secuencia de bytes pseudoaleatoria.

3. El procedimiento según la reivindicación 1, que comprende además el paso de, al determinar que el usuario es nuevo, obtener información específica del usuario seleccionada (104), con dicha información que incluye al menos uno de un nombre de usuario, una frase de contraseña, una fecha actual asociada con el dispositivo informático del usuario, una hora actual asociada con el dispositivo informático del usuario, una versión del sistema operativo asociada con el dispositivo informático del usuario y una dirección IP asociada con el dispositivo informático del usuario.

4. El procedimiento según la reivindicación 3, que comprende además el paso de generar el valor de hash único (106) introduciendo al menos una parte de la información específica del usuario en una función de hash.

5. El procedimiento según la reivindicación 4, que comprende además el paso de, al determinar que el usuario no es nuevo, verificar la identidad del usuario basándose en el valor de hash (108);

comprendiendo además opcionalmente el procedimiento los pasos de

pedir al usuario que vuelva a introducir la frase de contraseña;

realizar la función hash utilizando la misma información específica del usuario utilizada para generar previamente el valor de hash; y

comparar el resultado con el valor de hash almacenado en el archivo de clave asociado con el usuario para determinar si el resultado y el valor de hash son idénticos

6. El procedimiento según la reivindicación 1, que comprende además el paso de, al determinar que el algoritmo de extracción de clave ha sido comprometido, modificar el algoritmo de extracción de clave (116) y distribuirlo al menos a un usuario autorizado.

7. El procedimiento según la reivindicación 1, que comprende además el de generar el campo de clave utilizando un generador de números pseudoaleatorios ("PRNG").

8. El procedimiento según la reivindicación 7, que comprende además los pasos de: generar una secuencia pseudoaleatoria larga ("LPRS") de bytes (200); y

construir una secuencia pseudoaleatoria seleccionando un punto de entrada pseudoaleatorio en el LPRS y seleccionando un número predeterminado de bytes en el LPRS que comienza en el punto de entrada pseudoaleatorio.

9. El procedimiento según la reivindicación 8, en el que el paso de construir una secuencia pseudoaleatoria comprende además el paso de seleccionar un número predeterminado de bytes consecutivos en el LPRS que comienza en el punto de entrada pseudoaleatorio.

10. El procedimiento según la reivindicación 8, en el que el paso de construir una secuencia pseudoaleatoria comprende además el paso de seleccionar un número predeterminado de bytes no consecutivos en el LPRS que comienza en el punto de entrada pseudoaleatorio.

11. El procedimiento según la reivindicación 7, que comprende además el paso de implementar el PRNG en memoria en al menos un dispositivo informático.

12. El procedimiento según la reivindicación 1, que comprende además el paso de implementar al menos una aplicación de cliente en memoria en al menos un dispositivo informático, estando dicha aplicación de cliente

configurada para comunicarse con el administrador de claves y el módulo de cifrado para cifrar y descifrar los datos confidenciales.

13. El procedimiento según la reivindicación 1, en el que el paso de cifrar los datos comprende además los pasos de:

generar un token (300) que tiene un valor conocido;

insertar una primera instancia del token (302) al comienzo de los datos; generar aleatoriamente un valor de suma de comprobación (304);

dividir el valor de suma de comprobación (306) en una primera parte y una segunda parte;

insertar la primera parte del valor de suma de comprobación entre la primera instancia del token y el comienzo de los datos (308);

insertar la segunda parte del valor de la suma de comprobación al final de los datos (312);

insertar una segunda instancia del token después de la segunda parte del valor de suma de comprobación (314); y

cifrar la secuencia completa de la primera instancia del token, la primera parte del valor de la suma de comprobación, los datos, la segunda parte del valor de la suma de comprobación y la segunda instancia del token utilizando la clave de cifrado (316).

14. El procedimiento según la reivindicación 13, en el que el paso de generar aleatoriamente un valor de suma de comprobación comprende además el paso de generar una serie de números enteros que comienzan en la primera parte del valor de suma de comprobación y continúan en la segunda parte del valor de suma de comprobación, de manera que dicha primera parte tiene una relación conocida con dicha segunda parte.

15. El procedimiento según la reivindicación 13, que comprende además el paso de, al detectar un token dañado o parcialmente dañado debido a que se ha descifrado con una clave de cifrado incorrecta, generar datos legibles pero falsos.

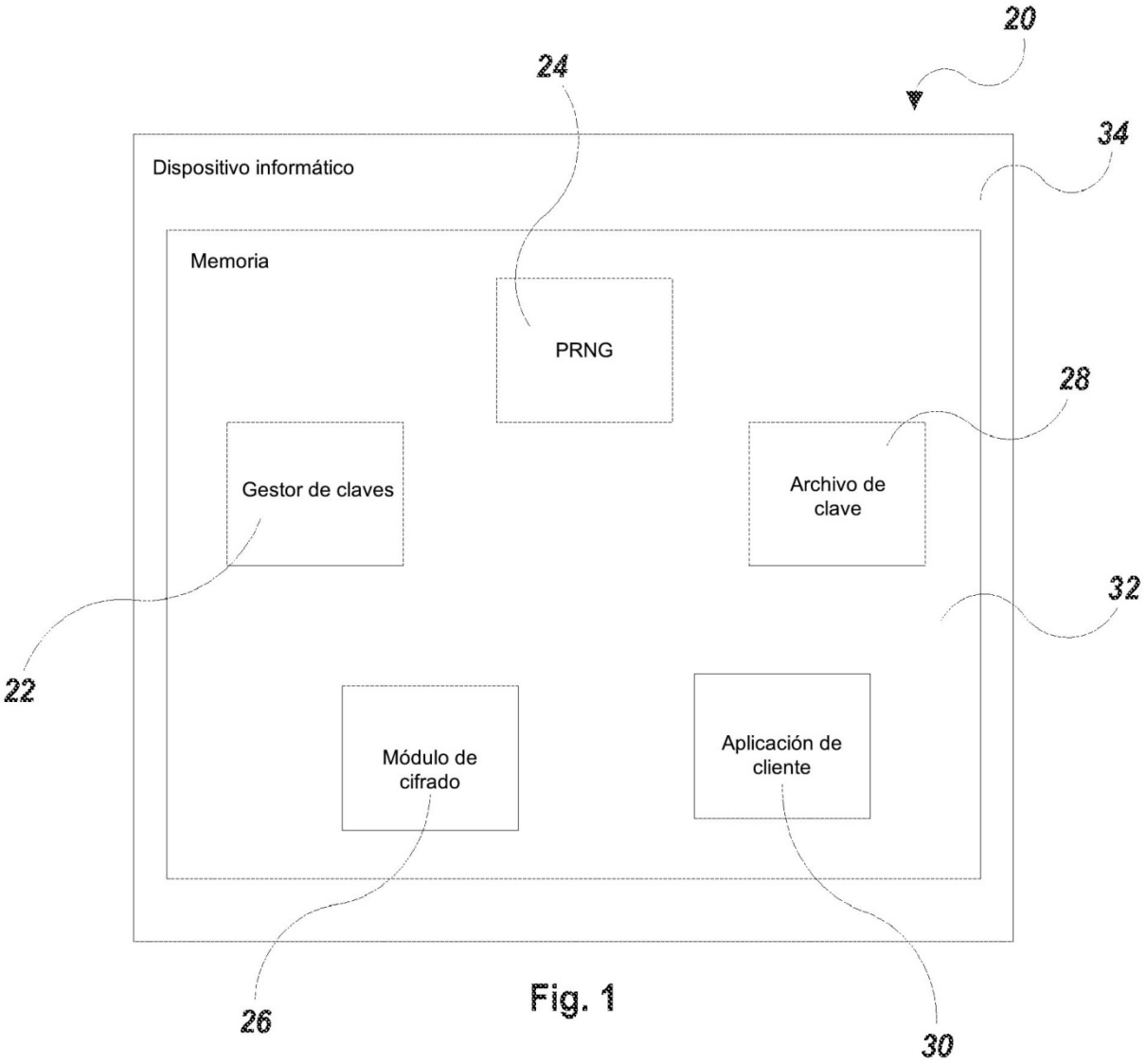

Fig. 1

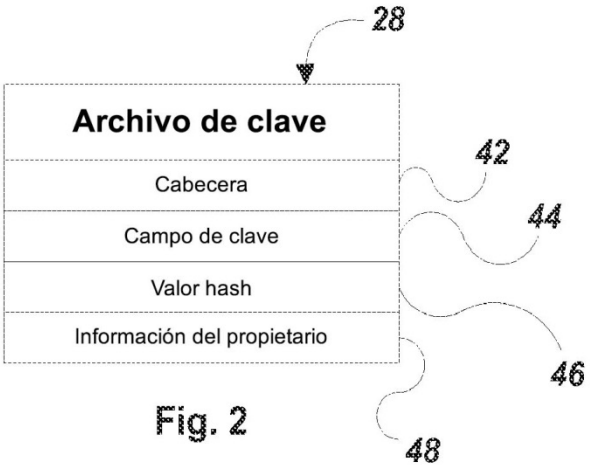

Fig. 2

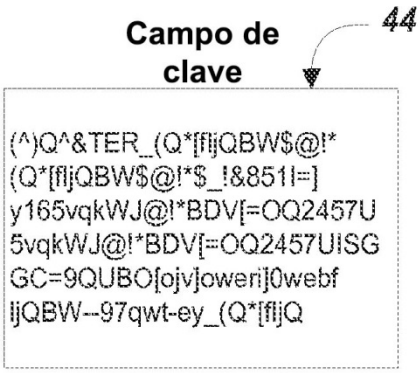

Fig. 3

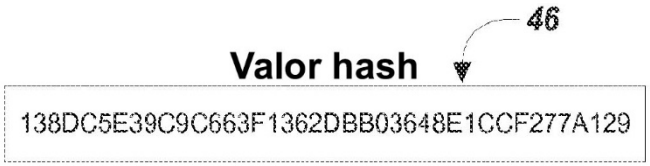
46
Valor hash
138DC5E39C9C663F1362DBB03648E1CCF277A129

Fig. 4

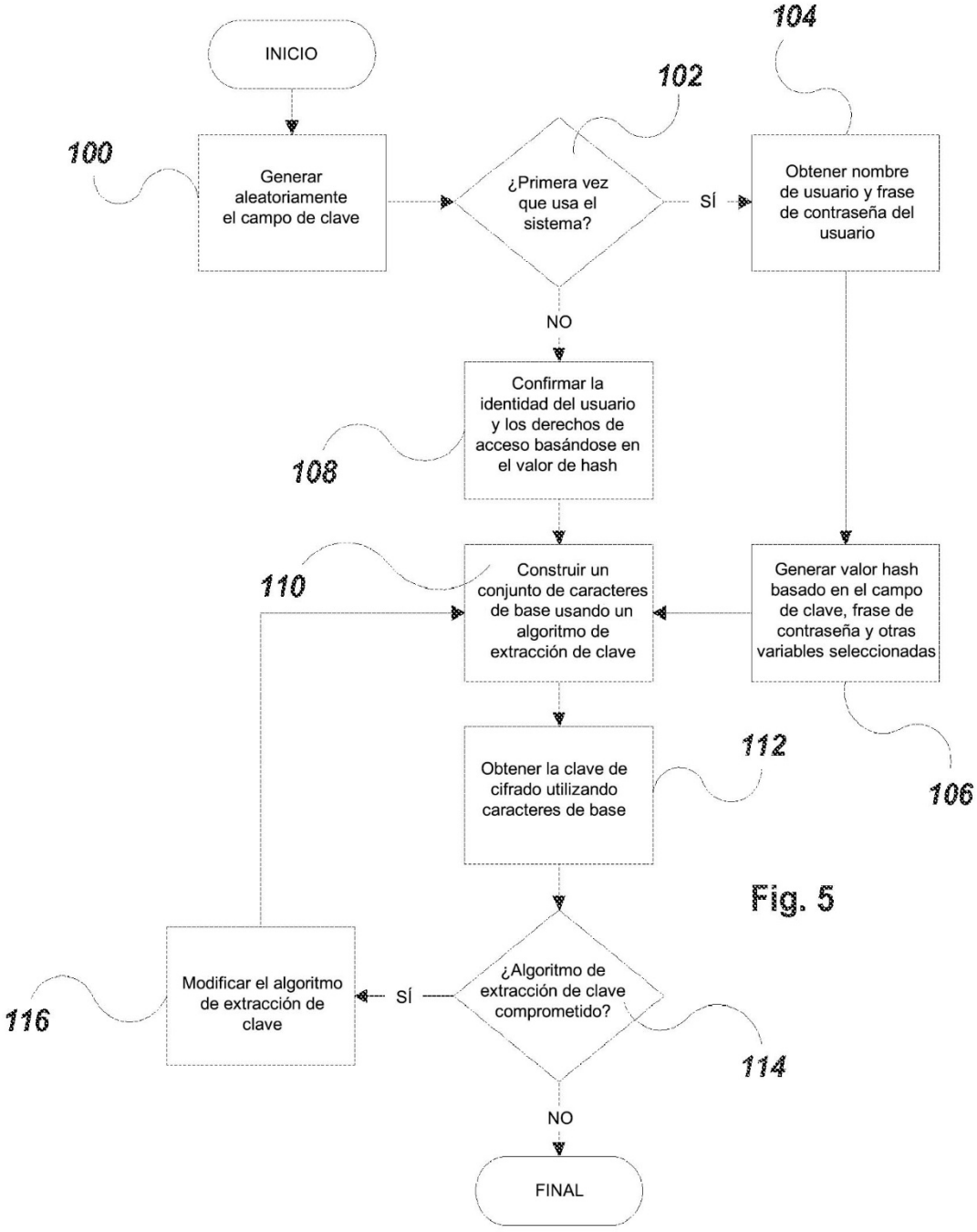
INICIO
100
Generar aleatoriamente el campo de clave
102
¿Primera vez que usa el sistema?
SÍ
104
Obtener nombre de usuario y frase de contraseña del usuario
NO
108
Confirmar la identidad del usuario y los derechos de acceso basándose en el valor de hash
110
Construir un conjunto de caracteres de base usando un algoritmo de extracción de clave
Generar valor hash basado en el campo de clave, frase de contraseña y otras variables seleccionadas
106
112
Obtener la clave de cifrado utilizando caracteres de base
¿Algoritmo de extracción de clave comprometido?
SÍ
Modificar el algoritmo de extracción de clave
116
114
NO
FINAL

Fig. 5

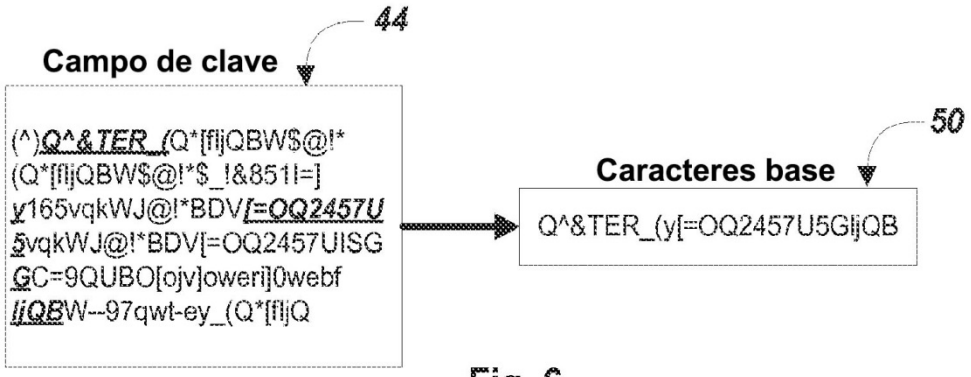
44
Campo de clave
(^)Q^&TER_(Q*[fl]QBW$@!*
(Q*[fl]QBW$@!*$_I&851I=]
y165vqkWJ@!*BDV[=OQ2457U
5vqkWJ@!*BDV[=OQ2457UISG
GC=9QUBO[ojv]oweri]0webf
//QBW--97qwt-ey_(Q*[fl]Q
50
Caracteres base
Q^&TER_(y[=OQ2457U5G]jQB

Fig. 6

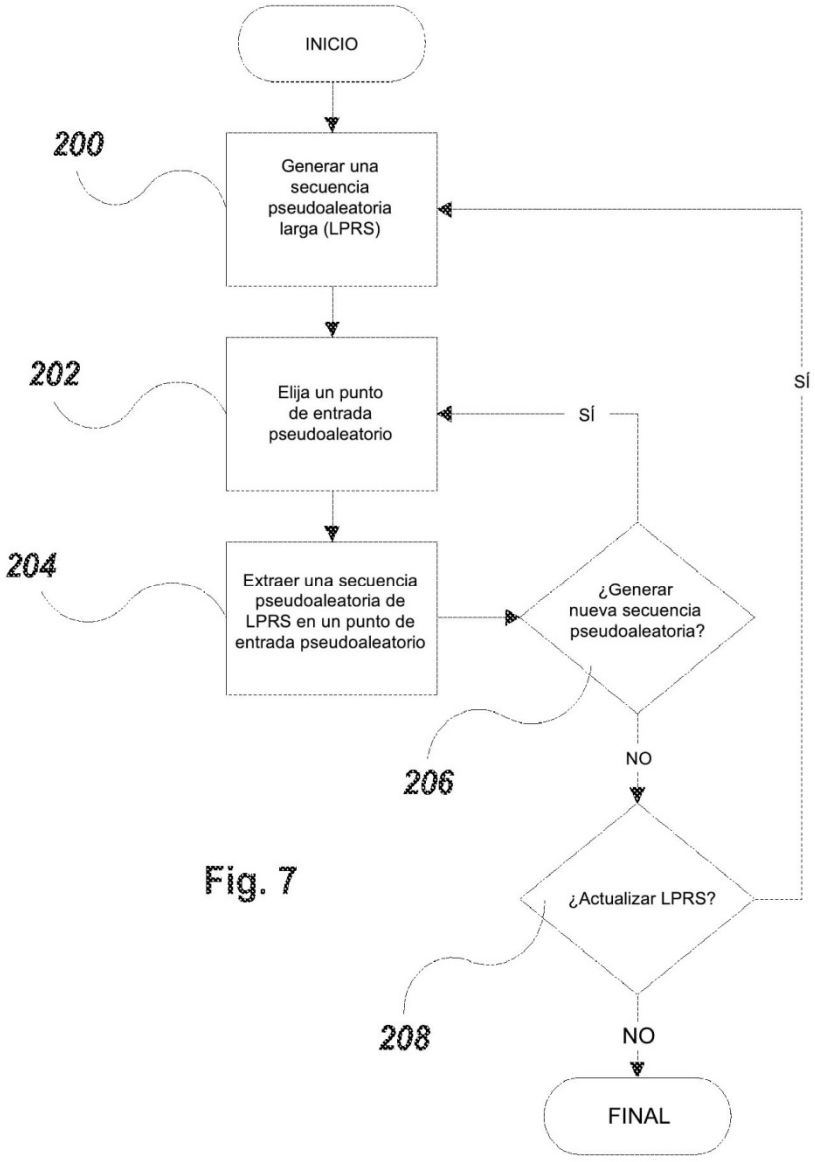
INICIO
200
Generar una secuencia pseudoaleatoria larga (LPRS)
202
Elija un punto de entrada pseudoaleatorio
SÍ
204
Extraer una secuencia pseudoaleatoria de LPRS en un punto de entrada pseudoaleatorio
¿Generar nueva secuencia pseudoaleatoria?
SÍ
206
NO
¿Actualizar LPRS?
208
NO
FINAL

Fig. 7

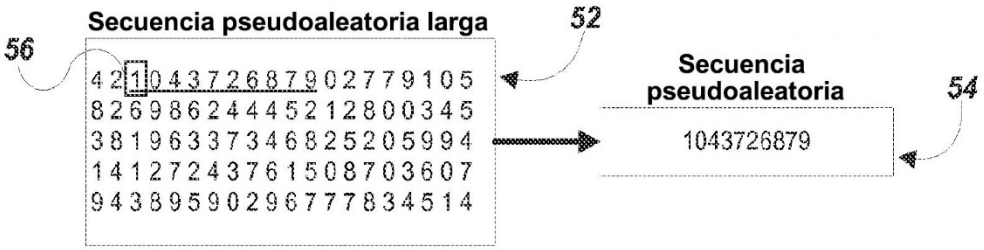

Fig. 8

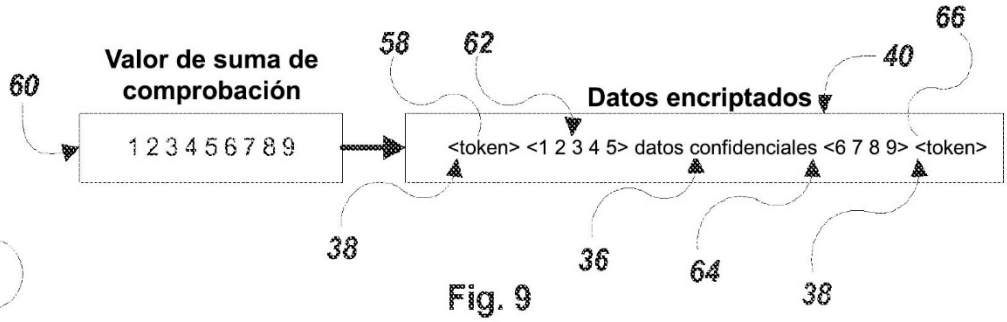

Fig. 9

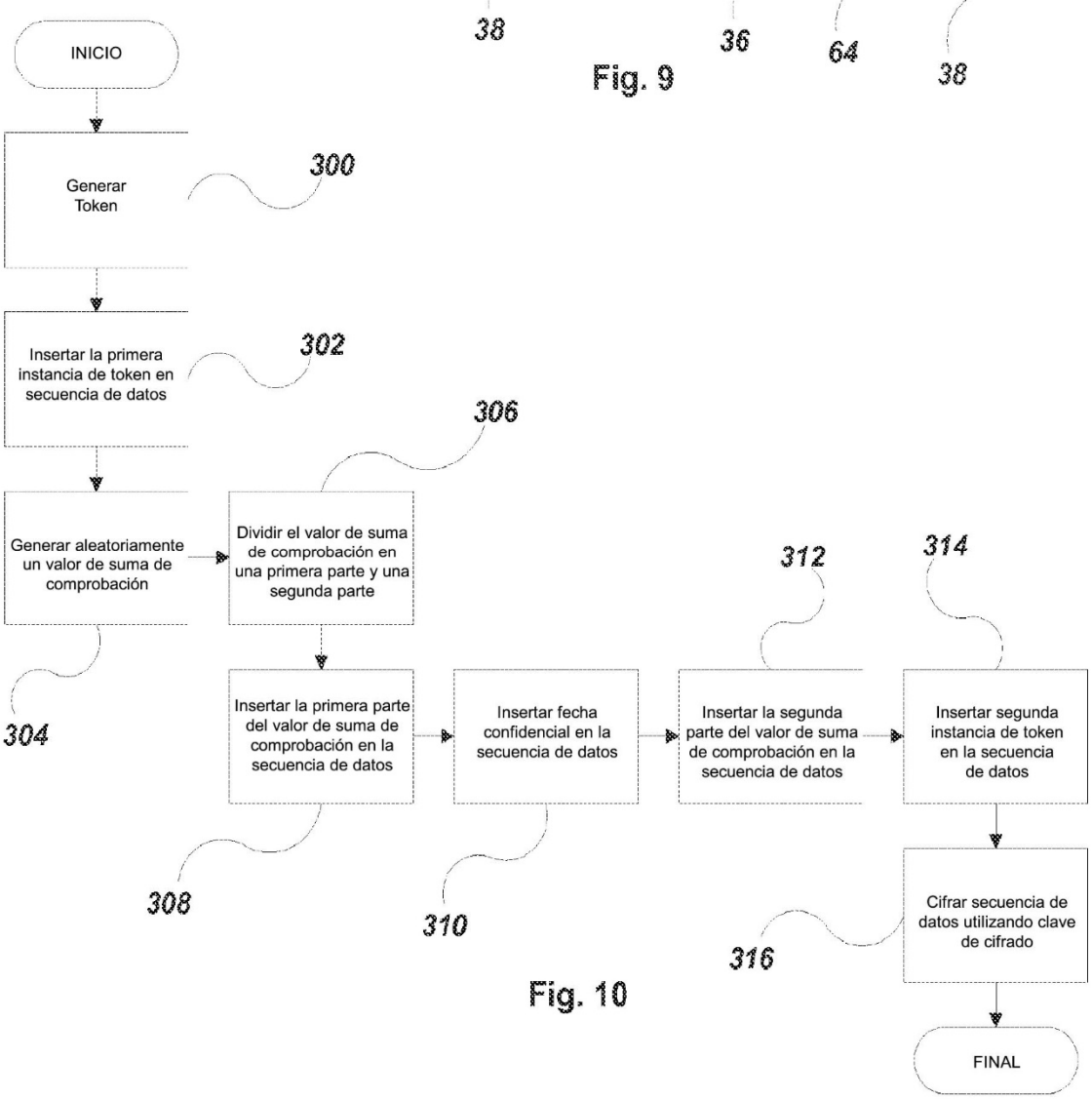

Fig. 10