(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 269 415**

(51) Int. Cl.:
G06F 7/58 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Número de solicitud europea: **01938930 .3**
(86) Fecha de presentación : **07.06.2001**
(87) Número de publicación de la solicitud: **1292882**
(87) Fecha de publicación de la solicitud: **19.03.2003**

(54) Título: **Método y dispositivo para cifrar un mensaje.**

(30) Prioridad: **07.06.2000 SE 0002158**

(45) Fecha de publicación de la mención BOPI:
01.04.2007

(45) Fecha de la publicación del folleto de la patente:
01.04.2007

(73) Titular/es: **Anoto AB.**
Emdalavägen 18
223 69 Lund, SE

(72) Inventor/es: **Thuvesholmen, Mikael;**
Edsö, Tomas;
Doré Hansen, Mads y
Skantze, Kristofer

(74) Agente: **Elzaburu Márquez, Alberto**

DESCRIPCIÓN

Método y dispositivo para cifrar un mensaje.

Campo de aplicación del invento

El presente invento se refiere en general al campo de transmitir información desde un emisor hasta un receptor. Más específicamente, el presente invento se refiere a un método y a un dispositivo para cifrar un mensaje para la transmisión segura de dicho mensaje desde un dispositivo emisor a un receptor. El invento se refiere además a un medio legible por ordenador que comprende instrucciones para llevar a un ordenador a realizar dicho método, y a un dispositivo emisor y a un sistema, respectivamente, que comprende dicho dispositivo.

Antecedentes del invento

Durante la transmisión de información desde un emisor a un receptor, por ejemplo en un sistema que incluye dispositivos manuales, existen básicamente cuatro aspectos que es necesario satisfacer para obtener una transmisión segura con respecto a autenticidad, integridad, confidencialidad y no repudio. Sin embargo, la confidencialidad, es decir, que la información se mantenga secreta durante la transmisión, es crucial en el campo de la comunicación digital, por ejemplo en transacciones financieras o en comercio exterior. Este aspecto, así como los otros aspectos, se puede cumplir mediante el uso de la criptografía.

Cuando se usa la criptografía o un algoritmo de seguridad de red basado en la criptografía, se usan datos de números aleatorios por diferentes razones y representan un papel esencial. Por ejemplo, los números aleatorios se usan frecuentemente como claves de cifrado o para la generación de claves de cifrado. Además, por definición los datos aleatorios son difíciles de determinar o de adivinar.

Los métodos normales de criptografía incluyen el cifrado simétrico y el cifrado asimétrico. Cuando se usa el cifrado simétrico, se emplea la misma clave para el cifrado y el descifrado. La clave de cifrado se usa conjuntamente con un algoritmo de cifrado, y claves diferentes resultarán en salidas diferentes del algoritmo. El grado de seguridad del mensaje cifrado depende del secreto de la clave y por tanto del número aleatorio usado como la clave o para generar la clave, no del secreto del algoritmo. Esto hace posible usar algoritmos normalizados, tales como la Norma de cifrado avanzada (en adelante AES), la Norma de cifrado de datos (en adelante DES) o la Norma internacional de cifrado de datos (en adelante IDEA). El grado de seguridad depende también de la longitud o tamaño de bits de la clave. Cuanto más larga sea la clave de cifrado, más difícil será romper el lenguaje cifrado.

Cuando se usa el cifrado asimétrico, el emisor y el receptor tienen cada uno una clave de cifrado privada y una clave de cifrado pública. Por tanto, desde el punto de vista de la confidencialidad, se consigue la autenticación y el no repudio. Los algoritmos asimétricos de cifrado comúnmente utilizados incluye, por ejemplo, el RSA (Rhivest-Shamir-Adleman) y el DH (Diffie-Hellman).

Es un problema bien sabido que las fuentes de verdaderos números aleatorios son difíciles de encontrar. Los generadores de ruidos físicos, tales como los detectores de impulsos de los eventos de radiaciones ionizantes, los tubos de descarga de gases, y los condensadores con fugas, son una fuente potencial. Sin embargo, dichos dispositivos son de una utilidad limitada en las aplicaciones de seguridad de redes. Por ejemplo, la incorporación de uno de estos dispositivos en un dispositivo de mano requerirá un diseño complejo y posiblemente voluminoso del dispositivo de mano. Además, se plantean problemas tanto con el grado de aleatoriedad como con la precisión de los números generados por tales dispositivos.

Otra solución para obtener números aleatorios para aplicaciones criptográficas es el uso de técnicas algorítmicas. Sin embargo, estos algoritmos son deterministas y por tanto producen secuencias de números que no son estadísticamente aleatorias. A estos números se hace referencia a menudo como números seudoaleatorios.

Una técnica ampliamente usada para la generación de números seudoaleatorios es el método congruencial lineal. Se obtiene una secuencia de números mediante la ecuación siguiente

$$X_{n+1} = (aX_n + b) \bmod c,$$

donde X_0 es un número inicial, es decir, la semilla aleatoria (random seed). Usualmente, en un dispositivo de mano o en un ordenador, se usan los microsegundos del reloj interno como semilla aleatoria para iniciar el algoritmo.

Un problema que se plantea con el método anteriormente mencionado es que, una vez que se ha elegido un valor, la semilla aleatoria, los números subsiguientes en la secuencia siguen de forma determinista. Ello significa que alguien que tenga conocimiento de una parte de la secuencia podría determinar teóricamente los elementos subsiguientes de la secuencia.

Es posible implementar generadores más avanzados de números aleatorios que usen el reloj interno como semilla aleatoria, por ejemplo, como el algoritmo usado en Blue-tooth. Éste y otros algoritmos similares son capaces de generar

números seudoaleatorios con características estadísticas perfeccionadas en comparación con los números generados por el método congruencial lineal. No obstante, los números seudoaleatorios todavía son de una calidad insuficiente en un sentido estadístico, es decir, cuando se considera el grado de aleatoriedad.

El artículo titulado "Stream cipher based on pseudo random number generation with optical affine transformation" por Sasaki y colaboradores, publicado en Applied Optics, Volumen 39, Nº 14, páginas 2340-2346, el 10 de mayo de 2000, describe una técnica para generar una imagen con distribución de intensidad seudoaleatoria mediante tratamiento óptico. Específicamente, se usa un tratamiento de realimentación óptico para presentar visualmente una imagen inicial en un tubo de rayos catódicos (en adelante TRC). De la imagen del TRC se forma luego una imagen en una cámara con dispositivo acoplado por carga (en adelante CCD), por medio de componentes ópticos que escinden, rotan, reflejan, convierten y recombinan la imagen, después de lo cual la imagen tratada se presenta visualmente en el TRC. Luego se repite el mismo procedimiento para un gran número de iteraciones. La imagen final de salida se usa para cifrar un mensaje de imagen mediante la adición óptica de módulo-n de la imagen final de salida al mensaje de imagen. Aparte de su evidente incapacidad de implementarse fácilmente en un dispositivo de mano, la técnica óptica conocida parece que adolece de una precisión limitada y de una velocidad lenta de tratamiento.

Por tanto, continúa planteándose el problema de encontrar un método, que se pueda implementar en un sistema que comprenda dispositivos de mano, que proporcione números aleatorios de buena calidad, de acuerdo con los criterios antes mencionados, para la generación de claves de cifrado con el fin de proveer una transmisión segura de información entre un emisor y un receptor.

En el documento US-A- 5 852 434 se describe un ejemplo de un dispositivo de mano que se refiere a un dispositivo de determinación de la posición absoluta para indicar la posición y el movimiento instantáneos de un estilete sobre una superficie formateada con un código relacionado con la posición para indicar las coordenadas X-Y.

Sumario del invento

Por tanto, un objeto del presente invento es proveer un método y un dispositivo perfeccionados para generar una clave de cifrado y para cifrar un mensaje.

Este y otros objetos se consiguen de acuerdo con el presente invento mediante la provisión de un método para cifrado de acuerdo con la reivindicación 1, un bolígrafo digital de acuerdo con la reivindicación 20, y un método para autenticación de acuerdo con la reivindicación 36. En las reivindicaciones subordinadas se definen realizaciones preferidas.

Así, el presente invento se basa en la consideración ventajosa de usar datos ópticos como semilla aleatoria para la generación de una clave de cifrado, que a su vez se usa como un algoritmo de cifrado para cifrar un mensaje. Los datos ópticos obtenidos de acuerdo con el método del presente invento presentan el grado requerido de aleatoriedad e imprevisibilidad. De hecho, se puede considerar que los datos ópticos son "verdaderamente" aleatorios. Por consiguiente, el grado de aleatoriedad es mayor, y los datos ópticos utilizados son más imprevisibles en comparación con los datos usados para semilla aleatoria en el método conocido anteriormente descrito. Por tanto, se consigue un grado perfeccionado de secreto de la clave de cifrado generada.

Tradicionalmente, se usan dos criterios distintos y no necesariamente compatibles para determinar la calidad de una secuencia de números aleatorios, la imprevisibilidad y la aleatoriedad. En una "verdadera" secuencia aleatoria, cada número es estadísticamente independiente de cualquier otro número de la secuencia, y por tanto es imprevisible. Para validar la aleatoriedad de una secuencia de números se usan dos criterios. En primer lugar, la distribución uniforme de los números aleatorios, lo que significa que la frecuencia de aparición de cada uno de los números debería ser aproximadamente la misma. En segundo lugar, la independencia entre números aleatorios, lo que significa que ningún valor de la secuencia se puede inferir de cualquiera de los demás.

De acuerdo con la realización preferida del presente invento, una superficie, o una parte de la misma, se exploran o se leen con un detector óptico, preferiblemente una cámara o un detector sensible a la luz, obteniendo de ese modo unos datos ópticos representativos de las características de la superficie leída. El detector sensible a la luz es, por ejemplo, un detector acoplado por carga (en adelante CCD), o un detector complementario de óxido-metal (en adelante CMOS). Los datos ópticos obtenidos se determinan por - y representan - los valores de al menos un parámetro óptico, que es representativo de las condiciones físicas sobre la parte de la superficie.

Preferiblemente, los datos ópticos se obtienen de una parte de una superficie provista de un patrón de código de posición, en la que el patrón de código de posición incluye marcas ópticas legibles. Cada una de dichas marcas se podría diseñar de una forma más o menos arbitraria. Sin embargo, preferiblemente el diseño de cada marca es elemental, por ejemplo en la forma de puntos redondos, como se muestra en la descripción detallada más adelante. El patrón de código de posición se implementa usando cualquier parámetro, que se podría usar para obtener símbolos del tipo anteriormente mencionado que se puedan detectar mediante un detector óptico. El hecho de que el patrón de código de posición sea óptimamente legible facilita la aplicación del patrón sobre la superficie. De acuerdo con ello, el patrón debería tener la posibilidad de reflejar luz, que no necesariamente tiene que tener una longitud de onda en el espectro visible.

Preferiblemente, el parámetro detectado y usado para la generación de la clave de cifrado es el brillo, que es una medida relativa de la intensidad de la energía de salida de una fuente luminosa que es visible para un detector óptico. En la realización preferida del presente invento, se registra el brillo de la luz que se refleja de una parte de una superficie iluminada. Por supuesto, la luz detectada no tiene que estar constituida necesariamente por luz reflejada. Se contempla también dentro del alcance del presente invento la detección de la luz emitida desde superficies luminosas, o cualquier combinación de luz emitida y luz reflejada. El brillo en la luz detectada podría depender, por ejemplo, de las variaciones en la iluminación circundante, de la calidad de la impresión del patrón, del ennegrecimiento de las marcas, y/o de la calidad de la superficie, por ejemplo, una superficie de papel. Los factores biométricos podrían tener también un impacto sobre el brillo, por ejemplo la inclinación del bolígrafo. Estos y otros factores introducen un grado considerable de aleatoriedad en los datos ópticos. Además, el hecho de que el propio detector óptico sea un generador de ruido aumentará todavía más el grado de aleatoriedad en los datos ópticos.

De acuerdo con realizaciones preferidas del invento, los datos ópticos se tratan de acuerdo con un orden o esquema preprogramado y se organizan en campos de datos de una longitud predeterminada. A su vez, los campos de datos, se organizan preferiblemente en registros de datos de acuerdo con un esquema predeterminado, por ejemplo, en un orden predeterminado.

De acuerdo con una realización específica preferida del presente invento, y con el fin de perfeccionar todavía más la estocasticidad de los datos ópticos organizados en dichos registros de datos, el orden de los campos de datos dentro de los registros de datos se redispone de acuerdo con un algoritmo de redisposición cíclica. De acuerdo con el algoritmo de redisposición cíclica, el orden de los campos de datos redispuestos en los diferentes registros de datos podría diferir de uno a otro registro de datos. De ese modo, se podría usar un número de esquemas diferentes de reordenación, incluyendo el caso en el que para algunos registros de datos, el orden de los campos de datos no se haya alterado en absoluto. Preferiblemente, la reordenación cíclica se realiza mediante el desplazamiento de todos los campos de datos en cada registro de datos. Los campos de datos se podrían desplazar mediante un número de etapas que abarca desde cero, es decir, no tiene lugar desplazamiento alguno, hasta un número correspondiente al número de campos de datos en el registro de datos menos 1. Por tanto, el algoritmo de reordenación contiene información en cuanto al número de etapas en que cada campo de datos se desplaza para un registro de datos específico.

De acuerdo con una realización específica del presente invento, el orden de los campos de datos de cada registro incluido en un primer conjunto de registros de datos se redispone de acuerdo con un primer algoritmo de reordenación. De ese modo, se obtiene un prime conjunto de registro de datos redispuestos. Luego, el orden de los campos de datos de cada registro de datos de un segundo conjunto de registros de datos se redispone de acuerdo con un segundo algoritmo de reordenación, por lo que se obtiene un segundo conjunto de registros de datos redispuestos en la generación de la clave de cifrado, el primer conjunto de registros de datos redispuestos forma datos de clave y el segundo conjunto de registros de datos redispuestos forma datos de entrada, o viceversa, de la clave de cifrado usada en el algoritmo de cifrado. Alternativamente, los datos de clave y los datos de entrada forman datos de cifrado que se pueden usar como material en un proceso de cifrado. Por ejemplo, el material se puede cifrar con la clave pública del receptor, para usar como clave de cifrado o material de clave, para comprimirse a una clave de cifrado, para un algoritmo de cifrado simétrico. La ventaja del proceso de redisposición descrito es que se mejoran significativamente las características estadísticas, es decir, la aleatoriedad y la imprevisibilidad.

De acuerdo con una realización adicionalmente preferida del invento, sorprendentemente se ha averiguado que se ha obtenido un elevado grado de estocasticidad usando el algoritmo específico de reordenación explicado más adelante con mayor detalle. De hecho, los datos de salida del algoritmo de cifrado, cuando se usan los datos ópticos como semilla aleatoria y el algoritmo de reordenación descrito, constituyen un ruido uniformemente distribuido de acuerdo con los métodos estadísticos de ensayo prevalentes.

De acuerdo con una realización preferida alternativa del invento, la estocasticidad de los datos ópticos obtenidos organizados en registros de datos se mejora usando funciones resumen (hash functions). De acuerdo con esta realización, se efectúa un primer resumen sobre un conjunto de un número predeterminado de registros de datos mediante un primer algoritmo, es decir, una primera función resumen. Como entienden los expertos en la técnica, el resumen es un procedimiento iterativo que no se describirá con detalle. Por tanto, el término salida de resumen, tal como se usará en adelante en la presente memoria, se refiere al resultado de todas las iteraciones incluidas en el resumen. Así, una primera salida, es decir, una primera salida de resumen, se obtiene del primer resumen. La primera salida se usa luego como una entrada a un segundo algoritmo, que podría ser una segunda función resumen. La salida del segundo algoritmo, es decir, números aleatorios, se usa entonces, por ejemplo, como la clave de cifrado o para generar una clave de cifrado en un algoritmo de cifrado para cifrar un mensaje. No obstante, el segundo algoritmo alternativamente podría ser un algoritmo iterativo diferente de una función resumen. Por ejemplo, se podrían usar algoritmos A3 o A5, que son cifras de corriente y se usan para cifrado simétrico.

La primera función resumen introduce distorsión o ruido en los datos ópticos obtenidos usados como datos de entrada. En otras palabras, perturba las regularidades de los datos ópticos y la correlación entre campos de datos incluidos en los registros de datos. El uso de una segunda función resumen, o de un algoritmo alternativo, preferiblemente iterativo, en la primera salida mejora adicionalmente las características estadísticas de los datos y provee una distorsión adicional sobre la primera salida. De este modo, se mejoran significativamente las características estadísticas, es decir, la aleatoriedad y la imprevisibilidad, de los datos ópticos tratados usando el método de acuerdo con esta realización. El perfeccionamiento es tal que los números aleatorios generados como resultado del método de esta realización se

pueden considerar como ruido blanco uniformemente distribuido de acuerdo con los métodos prevalentes de ensayos estadísticos. Según una alternativa preferida de esta realización, se usan algoritmo de cifrado simétrico en los algoritmos primero y segundo. Mediante el uso del mismo algoritmo de cifrado para los algoritmos, se obtienen las ventajas de una implementación simplificada del código de programa de los algoritmos y un ahorro de capacidad de memoria.

Además, cuando se usa un algoritmo de cifrado simétrico, tal como el AES, para el cifrado real del mensaje, este algoritmo de cifrado se usa preferiblemente también en al menos uno de dichos algoritmos, y preferiblemente en ambos. Sin embargo, dentro del alcance del presente invento se puede concebir que se podrían usar otros y diferentes algoritmos de cifrado en cada uno de dichos algoritmos, así como para el cifrado real del mensaje. Preferiblemente, con el fin de mejorar todavía más la estocasticidad de la clave de cifrado, o de los números aleatorios usados para generar la clave de cifrado, son las propiedades estadísticas del parámetro. Esto resulta en un grado mayor de aleatoriedad e imprevisibilidad. Ejemplos de las propiedades estadísticas que se usan preferiblemente incluyen los valores mínimo, máximo y suma del parámetro detectado. Sin embargo, se pueden concebir otras propiedades estadísticas, tales como valores medios, valores de desviación típica, etc. Como observarán los expertos en la técnica, el uso de dicho cálculo de propiedades estadísticas no se limita en manera alguna a una realización específica del presente invento. Por el contrario, se podrían calcular las propiedades estadísticas de los datos ópticos y los resultados de las mismas se podrían usar para perfeccionar la estocasticidad de los datos ópticos y la clave de cifrado generada con las mismas, independientemente del método elegido para generar la clave de cifrado.

Además, los datos ópticos usados para generar una clave de cifrado podrían constituir parte del mensaje a cifrar y trasmitir. Alternativamente, los datos ópticos no constituyen parte del mensaje. Adicionalmente, la etapa de obtener datos ópticos para cifrar el mensaje se puede obtener antes de, durante, o a continuación del procedimiento de obtención del mensaje a cifrar. A título de ejemplo, el cifrado del mensaje podría tener lugar justo antes de la transmisión real del mismo. Entonces, la clave de cifrado, incluyendo la obtención de datos ópticos, tanto si los datos ópticos se extraen del mensaje como si no, se podría generar en relación con el procedimiento de cifrado. Alternativamente, la generación de la clave de cifrado se podría haber realizado antes, por ejemplo en relación con la obtención y almacenamiento del mensaje, y se usa para el cifrado una clave de cifrado guardada.

Adecuadamente, los datos ópticos usados para generar una clave de cifrado se guardan en un medio de almacenamiento antes del tratamiento de los mismos. En una realización alternativa, los datos ópticos se guardan después del tratamiento de los mismos.

Preferiblemente, se usa un algoritmo de cifrado simétrico para el cifrado real del mensaje. Hay un número de algoritmos de cifrado simétrico concebibles que son adecuados, por ejemplo AES, DES, o IDEA. El uso de un algoritmo de cifrado asimétrico, tal como el RSA, para el cifrado real del mensaje es también concebible y entra dentro del alcance del presente invento. Sin embargo, el presente invento no se limita a un algoritmo de cifrado específico.

El método del presente invento se implementa en un bolígrafo digital. Dicho bolígrafo digital comprende un detector óptico para obtener un mensaje a transmitir. por ejemplo desde una superficie provista de un patrón de código de posición como se ha descrito anteriormente. Preferiblemente, el bolígrafo digital comprende también unos medios de iluminación para iluminar una superficie a leer por el detector óptico. Los medios de iluminación y el detector óptico podrían restringirse a un intervalo limitado de longitudes de onda, de tal manera que el detector óptico principalmente detecte luz reflejada que se provee mediante los medios de iluminación. El detector óptico se usa también para obtener los datos ópticos usado para generar una clave de cifrado. Por tanto, no se requiere un detector adicional o un generador adicional de números aleatorios dentro del limitado interior del bolígrafo digital.

Adicionalmente, el bolígrafo digital comprende una unidad de tratamiento o unos medios de tratamiento para realizar las etapas del presente invento, así como todas las etapas requeridas para obtener, cifrar y transmitir un mensaje. Además, el bolígrafo digital comprende también, entre otras cosas, medios de almacenamiento adecuados para guardar datos, medios de alimentación de energía eléctrica, por ejemplo una batería, así como medios de transmisión para transmitir el mensaje a un receptor.

De acuerdo con una realización adicional del invento, se provee un detector de presión para obtener datos de presión. Como los datos de presión están relacionados con factores biométricos, tales como los movimientos de la mano, el grado de aleatoriedad de los datos de presión es elevado. Los datos de presión se pueden usar entonces en combinación con los datos ópticos como datos de números aleatorios o semilla aleatoria, en la generación de una clave de cifrado, con el fin de amplificar el grado de aleatoriedad en la semilla aleatoria.

Asimismo, de acuerdo con todavía otra realización del invento, se obtienen datos de tiempo y usan combinados con los datos ópticos como semilla aleatoria con el fin amplificar la estocasticidad de la semilla aleatoria. Aunque los datos de tiempo son deterministas por naturaleza, no disminuirá el grado de aleatoriedad de los datos combinados. Los datos de tiempo se proveen preferiblemente mediante el reloj interno de los medios de tratamiento. La semilla aleatoria así obtenida se podría usar subsiguientemente en la generación de la clave de cifrado de la manera descrita anteriormente.

Como comprenderán los expertos en la técnica, hay otras áreas relacionadas en las que se podrían utilizar los números aleatorios generados a partir de datos ópticos de acuerdo con el presente invento. Una de dichas áreas es la autenticación de un mensaje enviado o recibido.

Otra área es el transporte de claves desde un emisor a un receptor. En ese caso, los números aleatorios se cifran con una clave pública del receptor y se usan como una clave de cifrado o datos de clave, para ser comprimidos subsiguientemente a una clave de cifrado, para un algoritmo de cifrado simétrico.

Los números aleatorios se pueden usar también para generar números primos para claves RSA ó DH.

Como apreciarán los expertos en la técnica, el método y el dispositivo del presente invento, así como las realizaciones preferidas de los mismos, son adecuados para realizar como un programa de ordenador o un medio legible por ordenador, preferiblemente dentro del contenido de un bolígrafo digital.

Otros objetos y ventajas adicionales del presente invento se describen más adelante por medio de realizaciones ejemplares.

Breve descripción de los dibujos

A continuación se describen realizaciones preferidas del invento con mayor detalle y con referencia a los dibujos adjuntos, en los que:

La Figura 1 muestra una realización de un sistema de gestión de información;

La Figura 2 muestra una realización de un dispositivo de emisión de acuerdo con el presente invento;

La Figura 3 muestra una realización de un dispositivo de emisión de acuerdo con el presente invento;

La Figura 4 presenta un diagrama de flujo que ilustra una realización de un método de acuerdo con el presente invento para cifrar un mensaje usando datos ópticos;

La Figura 5 muestra un diagrama de flujo que ilustra un algoritmo de una primera realización para aumentar la aleatoriedad en los datos ópticos usados para generar una clave de cifrado;

La Figura 6 muestra esquemáticamente el orden de los campos de datos dentro de un bloque de datos de clave y un bloque de datos de entrada antes de un procedimiento de reordenación cíclica de acuerdo con una realización del presente invento;

Las Figuras 7A y 7B muestran esquemáticamente el orden de los campos de datos dentro del bloque de datos de clave y del bloque de datos de entrada, respectivamente, después de dicho procedimiento de reordenación cíclica; y

La Figura 8 muestra un diagrama de flujo que ilustra un algoritmo de una segunda realización para aumentar la aleatoriedad en los datos de entrada usados para generar una clave de cifrado.

Descripción de realizaciones preferidas

A continuación se describe un sistema de gestión de información en el que se puede implementar este invento con referencia a la Figura 1. Después de esta presentación general de la estructura del sistema, se describirá un producto provisto de un patrón de código de posición con referencia a la Figura 2. Luego, con referencia a la Figura 3, se muestra un dispositivo de emisión, en el que se pueden implementar el método y el dispositivo del presente invento, diseñado para leer y obtener datos ópticos a partir del código de posición de la Figura 2.

Refiriéndose en primer lugar a la Figura 1, se muestra un sistema de gestión de información en el que se pueden integrar un producto de código de posición y un dispositivo de transmisión, tal como un bolígrafo digital. Hay muchas empresas interrelacionadas implicadas en el sistema de la Figura 1: compañías que fabrican los bolígrafos digitales (“fabricantes de bolígrafos”), compañías que fabrican los productos con código de posición (“fabricantes de papel”), compañías que suministran diferentes servicios por medio de unidades comercializadoras de servicios (“comercializadoras de servicios”), una compañía que administra el código de posición basándose en la base de datos de espacio virtual (“administrador de patrón”), operadores que proveen los enlaces de comunicación entre los bolígrafos digitales y las diferentes unidades (“operadores de red”), y una multitud de usuarios de bolígrafos digitales (“propietarios de bolígrafos”).

El sistema de la Figura 1 incluye una multitud de dispositivos de transmisión o bolígrafos digitales (en adelante DP) y productos de código de posición (en adelante P), de los que en la Figura 1 solamente se ha mostrado uno), una unidad de consulta (en adelante ALS), y una pluralidad de unidades comercializadoras de servicios (en adelante SH, de las que solamente se ha mostrado una en la Figura 1). Debe hacerse notar que la información se puede transmitir en cualquier modalidad adecuada desde el bolígrafo digital DP a la unidad de consulta ALS y a la unidad comercializadora de servicios SH. En una realización, se efectúa la transmisión inalámbrica de información desde el bolígrafo digital DP a una unidad de conexión de red, la cual a su vez transmite la información a la unidad de consulta ALS y a la unidad comercializadora de servicios SH, respectivamente. La unidad de conexión de red puede ser una parte integrante del bolígrafo digital DP. Alternativamente, la unidad de conexión de red puede ser un teléfono móvil o un ordenador o cualquier otra unidad adecuada con una interfaz a una red de ordenadores tal como la Internet o una red de área local

(en adelante LAN). La unidad de consulta ALS está conectada a una base de datos de espacio virtual (en adelante GSDB) que incluye datos sobre la funcionalidad de cada posición codificada por el código de posición (en adelante PC) y la compañía relacionada con cada una de dichas posiciones. La unidad de consulta ALS está conectada también a una base de datos de bolígrafo (en adelante PDB), que incluye datos sobre todos los bolígrafos digitales del sistema, tales como el identificador exclusivo de bolígrafo de cada bolígrafo y todas las configuraciones o propiedades que están relacionadas con cada bolígrafo. La base de datos de bolígrafo PDB incluye también datos relacionados con el fabricante de cada bolígrafo. Además de lo anterior, la unidad de consulta está conectada a una base de datos de eventos (en adelante GEDB), que incluye datos sobre las transacciones que tienen lugar en la unidad de consulta ALS, es decir, las solicitudes de dirección realizadas por los bolígrafos en el sistema y las respuestas de dirección contestadas a los bolígrafos, así como cualesquiera errores que se produzcan en el proceso. Como una alternativa a las bases de datos individuales que se han mostrado en la Figura 1, la unidad de consulta ALS se podría conectar a una base de datos que lo abarque todo.

El sistema incluye también una o más redes en las que los operadores de red gestionan la comunicación entre los bolígrafos digitales DP y la unidad de consulta ALS, y entre los bolígrafos digitales DP y la unidad comercializadora de servicios SH. En este sentido, el propietario de un bolígrafo ha abierto una suscripción en uno de los operadores de red. Este operador de red podría también actuar como un gestor de servicios en el sistema, por ejemplo por medio de una unidad de servidor (en adelante SP) que proporcione servicios de comunicación que permitan al propietario de un bolígrafo enviar mensajes electrónicos, por ejemplo correo electrónico, mensajes cortos (en adelante SMS) o fax, basándose en la información escrita en los productos codificados de posición P por medio del bolígrafo digital DP. La unidad de servidor SP del operador de red podría también proveer el almacenamiento en red de la información generada en este sistema, por ejemplo entradas en un calendario o agenda con posiciones codificadas. Cuando actúe como un gestor de servicios, el operador de red mantiene una base de datos de aplicaciones (en adelante ASDB) que contiene datos sobre configuraciones específicas de usuario para diferentes aplicaciones, por ejemplo una firma o una tarjeta electrónica de negocio para adjuntarlas a los mensajes por correo electrónico, dónde y cómo guardar los mensajes enviados, etc.

En la realización de la Figura 1, el sistema incluye portales de Internet que son propiedad de uno o más servidores de web que forman una interfaz con las bases de datos del sistema, uno de cuyos portales P1 se ha mostrado en la Figura 1. El portal P1 es un portal denominado portal de socio, es decir, un portal que permite a los fabricantes de bolígrafos, fabricantes de papel, comercializadores de servicios y operadores de red acceder a partes seleccionadas de las bases de datos del sistema, a través de una unidad de interfaz (en adelante IF). Un ejemplo de otro portal es uno denominado portal de propietario de bolígrafo, es decir, un portal que permite que los propietarios de bolígrafos accedan a partes seleccionadas de las bases de datos del sistema. En una realización alternativa, las funcionalidades de los dos portales se funden en un portal común.

En la comunicación entre los diferentes participantes ilustrada en la Figura 1, es deseable que la información se envíe de una forma segura, es decir, mediante el uso de cifrado y de firmas digitales. Si el bolígrafo digital DP envía información confidencial a la unidad comercializadora de servicios SH, el bolígrafo digital DP cifra la información y la unidad comercializadora de servicios SH, con el fin de descifrar la información, la descodificará. El bolígrafo digital DP puede usar cifrado simétrico o cifrado asimétrico.

En la Figura 2, se ha mostrado una parte de un producto, tal como el producto con código de posición usado en el sistema de la Figura 1, en la forma de un papel 1, provisto, en su superficie 2, de una parte 3 de código de posiciones ópticas legibles que permite una determinación de la posición. El patrón de código de posición incluye unas marcas 4, que están dispuestas metódicamente sobre la superficie 2. El solicitante propone en la solicitud de patente internacional WO 01/16691, que se ha incorporado en la presente memoria como referencia, el uso de un producto que tiene una superficie de escritura que está provisto de dicho código de posición. El código de posición, que codifica una pluralidad de posiciones sobre la superficie, permite la grabación electrónica de la información que se escribe en la superficie de escritura, por medio de un bolígrafo digital que detecta el código de posición. El código de posición puede codificar las coordenadas de un gran número de posiciones, mucho mayor que el número de posiciones requeridas en el producto. Así, el código de posición se puede ver como formando un espacio virtual que se define mediante todas las posiciones que es capaz de codificar el código de posición, por lo que las diferentes posiciones en el espacio virtual se pueden asignar para diferentes funciones y/o participantes. Debe hacerse notar que, para mayor claridad, el patrón de código de posición mostrado en la Figura 2 se ha ampliado en gran escala.

La Figura 3 muestra una representación esquemática de una realización de un dispositivo de emisión diseñado para leer, por ejemplo, un patrón de código de posición de la Figura 2. El dispositivo es un bolígrafo digital. El bolígrafo DP comprende un alojamiento 5, conformado en una forma parecida a un bolígrafo. En una parte de extremo del alojamiento 5 se ha provisto una abertura 6. La abertura está destinada a apoyarse contra - o a sujetarse a una pequeña distancia de - la superficie S de la que tiene que obtenerse información.

Dentro del alojamiento 5 se han incorporado una unidad óptica, una unidad electrónica, y una unidad de alimentación de energía eléctrica. De acuerdo con realizaciones adicionales del bolígrafo digital, dentro del alojamiento 5 podría estar incluida también una unidad de detector de presión, que se describe más adelante.

La unidad óptica comprende un diodo 7, destinado a iluminar la superficie provista del código de posición, y un detector 8 sensible a la luz, por ejemplo un detector acoplado por carga (en adelante CCD) o un detector de

semiconductor complementario de metal-óxido (en adelante CMOS), destinado a registrar imágenes bidimensionales. La unidad de alimentación de energía eléctrica es en esta realización una batería 9, instalada en un recipiente separado.

La unidad electrónica 10 comprende un dispositivo de tratamiento que incluye medios de tratamiento de imagen, medios de cifrado y un equipo de tratamiento programado para leer imágenes del detector 8 y realizar la determinación de la posición y la descodificación de la información basándose en las imágenes. Adicionalmente, el equipo de tratamiento está programado para realizar cálculos con el fin de, por ejemplo, a partir de una imagen recibida del detector, calcular las propiedades de los datos ópticos a partir de la imagen. Los datos resultantes de estos cálculos se pueden usar como datos de entrada para otros cálculos o algoritmos, tales como algoritmos de cifrado. En esta realización, se han implementado en el dispositivo de tratamiento los algoritmos AES y RSA.

Asimismo, la unidad electrónica 10 comprende una memoria o elemento de almacenamiento de datos que está destinada, por ejemplo, a guardar los datos recibidos del equipo de tratamiento o del detector, así como instrucciones de programa para el dispositivo de tratamiento.

Adicionalmente, el bolígrafo podría comprender un teclado 11, que permite el accionamiento y el control del bolígrafo. Se incluyen también un transceptor 12 para comunicación inalámbrica, por medio de ondas radioeléctricas o de luz de infrarrojos, con otros participantes del sistema de la Figura 1. Adicionalmente, se puede incluir una pantalla de presentación visual 13 para mostrar, por ejemplo, la información registrada. El teclado, el transceptor, y la pantalla de presentación visual están en comunicación con - y se controlan mediante - la unidad electrónica 10.

Hay que hacer notar que la ilustración de la Figura 3 es esquemática, y que la configuración real de las partes comprendidas dentro del bolígrafo podrían diferir de la configuración mostrada sin apartarse del alcance del presente invento.

En la realización anteriormente mencionada, el patrón de código de posición es un patrón óptico legible y, por tanto, el detector es un detector óptico. El patrón de código de posición se puede basar en un parámetro distinto de un parámetro óptico según se ha mencionado anteriormente. En ese caso, por supuesto el detector debe ser de un tipo tal que pueda leer el parámetro en cuestión.

La combinación de un bolígrafo digital y de un producto con código de posición se puede usar como un dispositivo de entrada a un ordenador, un PDA, un teléfono móvil, o un elemento similar.

Por ejemplo, un texto y unos croquis escritos en una libreta para notas con código de posición se pueden transferir por medio del bolígrafo a un ordenador. Adicionalmente, la combinación de un bolígrafo y de un producto con código de posición permite la comunicación global, directamente desde el producto por medio del bolígrafo, mediante el código de posición sobre el producto que está asignado para dicha comunicación. Por ejemplo, la información registrada por el bolígrafo se puede transformar en un mensaje por fax, un mensaje por correo electrónico o un SMS, y luego se puede enviar desde el bolígrafo a un destinatario. Además, la combinación de un bolígrafo y un producto con código de posición se puede usar en comercio exterior. Por ejemplo, el bolígrafo digital se puede usar para pedir un artículo de un anuncio con código de posición en una revista, mediante el código de posición del anuncio que esté asignado para dicho servicio.

El concepto anterior se ha implementado en un sistema o infraestructura, que se ha mostrado en la Figura 1, y que se describe adicionalmente en las solicitudes de patente internacional del solicitante números WO 0 148 678, WO 0 148 591 y WO 0 148 685.

A continuación se presenta, en la forma de un diagrama de flujo, con referencia a la Figura 4, el método del invento para el cifrado de un mensaje basándose en la información escrita en los productos con código de posición de la Figura 2 por medio del dispositivo emisor de la Figura 3, y para proporcionar de ese modo una transmisión segura de dicho mensaje desde un dispositivo emisor a un receptor, por ejemplo en la forma de un mensaje por correo electrónico, un SMS, o un fax. Adicionalmente, el producto con código de posición y el dispositivo emisor se han incorporado preferiblemente en un sistema como el presentado en la Figura 1.

Comenzando en la etapa 410, una superficie con patrón se lee o explora mediante el detector 8, por lo que se obtiene una imagen óptica (en adelante OI). La imagen OI se guarda luego como una representación del patrón en un medio de almacenamiento de imágenes. La imagen óptica OI de los datos ópticos que representan la imagen incluye un número predeterminado de píxels. El tamaño y el número de estas representaciones de píxels, es decir, la resolución, son ajustables.

De acuerdo con una realización ejemplar, cada imagen óptica incluye 96x96 píxels. Adicionalmente, los 96x96 píxels están divididos en una matriz constituida por 16x16 elementos de imagen en la que cada elemento de imagen por consiguiente consiste en 6x6 píxels. Por supuesto, existe cualquier número de configuraciones concebibles de píxels de una imagen óptica que se pueden usar sin apartarse del alcance del presente invento.

En la etapa 420, se realiza la descodificación de la información comprendida en los datos de la imagen óptica. En la realización preferida, los datos ópticos resultantes OD comprenden información del brillo sobre la parte de la superficie que se ha leído. Los factores que tienen influencia sobre el brillo detectado ya se han descrito anteriormente.

El brillo se representa mediante valores discretos. En la realización preferida del presente invento, una superficie blanca corresponde a un valor de 255 y un superficie negra, por ejemplo una marca negra, corresponde a un valor de 0. Para aumentar la dinámica de los datos ópticos, se prefiere que cada elemento de imagen, que representa una parte de la superficie, incluya datos de al menos una marca y de al menos una parte de una superficie que rodee a las marcas.

Sin embargo, cualquiera de los valores de entrada procedentes de los detectores del bolígrafo digital, tales como presión del bolígrafo, coordenadas, tiempo, o datos análogos, se pueden usar para la generación de una clave. Estos parámetros se usan entonces en combinación con los datos ópticos OD o en combinación con diversificaciones aleatorias de ordenador.

En la etapa 430, se tratan los datos ópticos OD producidos por el detector para calcular las propiedades estadísticas específicas de los datos ópticos. De acuerdo con las realizaciones más preferidas, se calculan un valor máximo, un valor mínimo y un valor suma de la intensidad o brillo de un número de píxels, y se usan en el tratamiento continuado como datos ópticos. A los valores estadísticos calculados de ese modo se hará referencia de aquí en adelante en la presente memoria como datos ópticos tratados (en adelante POD). Este cálculo se realiza sobre cada elemento de imagen, es decir, sobre los datos ópticos OD representados en cada elemento de imagen, respectivamente. Por supuesto, existen otras propiedades preferiblemente estadísticas que se podrían calcular, tales como un valor promedio, o un valor de desviación típica.

A continuación, en la etapa 440, la secuencia resultante de datos ópticos tratados POD se organiza en grupos de bits o campos de datos. De acuerdo con la realización más preferida del presente invento, cada elemento de imagen se representa por un registro de datos (en adelante DR), y cada registro de datos consiste en cuatro campos de datos. Los dos primeros campos de datos contienen el valor suma calculado, el tercero contiene el valor mínimo calculado, y el cuarto contiene el valor máximo calculado. De ese modo, se produce una secuencia de registros de datos DR a partir de una imagen óptica, correspondiendo cada registro de datos a un elemento de imagen de la imagen. Cuando se producen los registros de datos DR, se guardan opcionalmente en un registrador cíclico, antes de usarlos como datos de número aleatorio, y se disponen en el dispositivo de tratamiento para que el equipo de tratamiento acceda a ellos cundo sea necesario, por ejemplo en la transmisión de un mensaje.

Luego, en la etapa 450, la secuencia de registros de datos DR se trata en un algoritmo con el fin de aumentar la estocasticidad de los datos ópticos tratados en los registros de datos. Esto se debe al hecho de que los datos ópticos tratados POD no son aleatorios en un cien por cien en un sentido estadístico. Por tanto, es conveniente realizar un tratamiento adicional con el fin de perfeccionar las características estadísticas de los datos ópticos, es decir, de aumentar la aleatoriedad o estocasticidad de los datos ópticos tratados, antes de que los datos ópticos tratados se usen como una semilla aleatoria. Las Figuras 5 y 8 presentan dos algoritmos diferentes de dos realizaciones alternativas del presente invento para aumentar la aleatoriedad de los datos ópticos tratados. Estos algoritmos se describen más adelante con mayor detalle.

Finalmente, en la etapa 460, se usan los datos ópticos tratados como una clave de cifrado (en adelante EK) en un algoritmo de cifrado, y se realiza el cifrado de un mensaje obtenido de la superficie con código de posición usando el bolígrafo digital.

De acuerdo con una realización alternativa, en la etapa 460 se usan los datos ópticos tratados para la autenticación de un mensaje enviado. Luego, los datos ópticos tratados se usan como datos de números aleatorios, que se cifran por medio de una clave de cifrado, por ejemplo una clave privada del bolígrafo digital, y los datos de números aleatorios cifrados se usan para la autenticación de dicho mensaje enviado.

Los algoritmos de cifrado, tal como el algoritmo de cifrado AES, usan cifrado de bloque. Una cifra de bloque, es decir, un algoritmo de cifrado que use cifrado de bloque, es un método de texto de cifrado (para producir texto en cifra) en el que una clave de cifrado y un algoritmo se aplican a un bloque de datos de una vez como un grupo en lugar de a un bit cada vez. El principal método alternativo, usado con mucha menos frecuencia, se llama el cifrado de corriente.

Hay una dificultad criptológica cuando el texto que se va a cifrar contiene datos estáticos, que no cambian de uno a otro texto. Si se usan diferentes claves de cifrado para cifrar el texto que contiene datos estáticos, un intruso podría deducir conclusiones en relación con la clave si la posición de los datos estáticos es conocida por el intruso. Para impedirlo, es común aplicar el texto cifrado del bloque cifrado anterior al bloque siguiente en la secuencia. A esta modalidad de cifrar en bloques cifrados se hace referencia a menudo como cifrado de encadenamiento de bloques cifrados (en adelante CBC). Entonces, el cifrado del bloque que incluye los datos estáticos depende de todos los bloques de texto anteriores, lo cual hace más o menos imposible sacar conclusiones relacionadas con la clave del cifrado de los datos estáticos. Para asegurar esto, un vector de iniciación obtenido de un generador aleatorio se combina con el texto del primer bloque. Por consiguiente, y de acuerdo con realizaciones preferidas del presente invento, los datos ópticos tratados se usan para formar tanto la clave de cifrado, es decir, el bloque de datos de clave, como el vector de iniciación, es decir, el bloque de datos de entrada.

Refiriéndose ahora a la Figura 5, se muestra un diagrama de flujo del método de acuerdo con un primer algoritmo preferido según el presente invento para aumentar la aleatoriedad o estocasticidad de los datos ópticos tratados y para producir números aleatorios. Debe hacerse notar que la descripción siguiente con referencia a las Figuras 5, 6, 7A, y 7B corresponde a la etapa 450 de la Figura 4.

En primer lugar, en la etapa 510, la secuencia de registros de datos, obtenida en la etapa 440 de la Figura 4, se organiza en bloques de datos, en los que cada bloque se determina o etiqueta bien como un bloque de datos de clave (en adelante KB) o bien como un bloque de datos de entrada (en adelante IB), de acuerdo con la descripción anterior. Según la realización más preferida del presente invento, cuatro registros de datos subsiguientes se organizan en un único bloque de datos. Además, un bloque de datos sí y uno no es un bloque de datos de clave KB, y los bloques de datos intermedios son bloques de datos de entrada IB.

Luego, en la etapa 520, los bloques de datos de clave KB se tratan de acuerdo con un primer algoritmo matemático, y en la etapa 530 los bloques de datos de entrada IB se tratan de acuerdo con un segundo algoritmo matemático. Los algoritmos matemáticos definen un procedimiento de reordenación cíclica o un procedimiento de desplazamiento de los campos de datos incluidos en el bloque de datos de clave KB y en el bloque de datos de entrada IB, respectivamente.

Con referencia en particular a la Figura 6, se muestra en ella el orden de los campos de datos dentro de un bloque de datos de clave KB o de un bloque de datos de entrada IB antes del procedimiento de desplazamiento. Los registros se muestran esquemáticamente como cajas divididas en cuatro elementos, representando cada elemento un campo de datos. En la realización más preferida, los campos indicados con los números 1 y 2 incluyen el valor suma de brillo, los campos indicados con el número 3 el valor mínimo, y el campo indicado con el número 4 el valor máximo. En la Tabla 1 a continuación se muestra el esquema de desplazamiento cíclico de los campos de datos incluidos en el bloque de datos de clave KB.

TABLA 1

Registro de datos	Etapas
A	0
B	3
C	2
D	1

En la figura 7A, se ha realizado el orden de los campos de datos dentro del bloque de datos de clave después del desplazamiento cíclico según se ha mostrado. Los campos de datos del primer registro de datos, registro A, conservan sus posiciones, los campos de datos dentro del segundo registro, registro B, se desplazan tres posiciones a la derecha, los campos dentro del tercer registro, registro C, se desplazan dos posiciones a la derecha, y los campos dentro del cuarto registro, registro D, se desplazan una posición a la derecha. A la salida de bloque de datos como resultado del algoritmo de reordenación para un bloque de datos de clave se hace referencia como bloque de datos de clave reordenados (en adelante RKB).

En la Tabla 2 se muestra el esquema de desplazamiento cíclico de los campos de datos incluidos en el bloque de datos de entrada IB.

TABLA 2

Registro de datos	Etapas
A	1
B	2
C	3
D	1

En la Figura 7B, se muestra el orden de los campos de datos dentro del bloque de datos de entrada después de que se ha realizado el desplazamiento cíclico, a la derecha. Los campos de datos dentro del primer registro de datos, registro A, se han desplazado una posición, los campos de datos dentro del segundo registro de datos, registro B, se han desplazado dos posiciones, los campos de datos dentro del tercer registro de datos, registro C, se han desplazado tres posiciones, y los campos de datos dentro del cuarto registro de datos, registro D, conservan sus posiciones. A la salida de bloque de datos como resultado del algoritmo de reordenación para un bloque de datos de entrada se hace referencia como un bloque de datos de entrada reordenados (en adelante RIB).

Debe hacerse notar que se podrían usar una amplia variedad de algoritmos de desplazamiento dentro del alcance del presente invento para obtener bloques de datos de entrada y de clave reordenados o redispuestos. Sin embargo, sorprendentemente se ha averiguado que la reordenación antes descrita de los campos de datos dentro de los registros de datos incluidos en el bloque de datos de clave y en el bloque de datos de entrada aporta un perfeccionamiento particular y considerable de las propiedades estadísticas deseadas para los datos de salida de un cifrado resultante, cuando se use el resultado del procedimiento de reordenación como datos de clave y datos de entrada para el cifrado. En otras palabras, aumentan la aleatoriedad y estocasticidad de los datos de salida y la previsibilidad disminuye. De hecho, de acuerdo con los procedimientos de pruebas estadísticas reconocidos en la técnica, los datos de salida del algoritmo de cifrado, es decir, el mensaje cifrado, se pueden considerar como ruido blanco uniformemente distribuido. Este efecto inesperado se debe al hecho de que la correlación entre los datos ópticos tratados incluidos en los campos de datos dentro de un registro de datos, que a su vez se transmite a los datos de salida del algoritmo de cifrado, se perturba mediante el procedimiento de reordenación anteriormente mencionado.

Luego, en la etapa 540, los datos contenidos en los bloques de datos de clave y de entrada así reordenados se usan como la clave de cifrado, datos de clave KD, y el vector de iniciación, datos de entrada ID, respectivamente, para el algoritmo de cifrado.

Finalmente, en la etapa 550, el método se vuelve al procedimiento mostrado en la Figura 4 en la etapa 460, donde se realiza el cifrado real del mensaje usando, en esta realización preferida, el algoritmo de cifrado AES. No obstante, por supuesto se contemplan otros algoritmos de cifrado dentro del alcance del presente invento.

A continuación se describe una segunda realización preferida alternativa de un algoritmo para mejorar las características estadísticas de los datos ópticos tratados, con particular referencia a la Figura 8.

Se puede considerar que el algoritmo tiene dos partes. En la primera parte, a la que se hace referencia como actualización de semilla, se calcula una semilla aleatoria basándose en los datos ópticos tratados. En la segunda parte, a la que se hace referencia como el cálculo de números aleatorios, la semilla aleatoria así calculada se usa como datos de entrada para el cálculo de los números aleatorios que se van a usar en el algoritmo de cifrado.

Los bloques de datos que incluyen un subconjunto de la secuencia de registros de datos que contienen los datos ópticos tratados forman los datos de entrada en la parte de actualización de semilla. Los registros de datos comprenden campos de datos, preferiblemente organizados como se ha descrito anteriormente en relación con la primera realización preferida. Así, cada registro de datos incluye cuatro campos de datos, de los que los dos primeros incluyen el valor suma, el tercero el valor mínimo, y el cuarto el valor máximo, véase Figura 6.

En la etapa 810, cada bloque de datos se trata en una primera función resumen, que en esta realización es un algoritmo de cifrado, con el fin de aumentar la aleatoriedad de los registros de datos que contienen los datos ópticos tratados. La primera función resumen es, en esta realización, un algoritmo de cifrado simétrico. Los registros de datos que contienen los datos ópticos tratados se usan como la clave de cifrado, y un vector elegido arbitrariamente se usa como el vector de iniciación. Sin embargo, se prefiere que el número de unos y ceros sea sustancialmente igual y distribuido aproximadamente a lo largo de todo el vector de iniciación. Esto se puede conseguir usando la semilla anterior como el vector de iniciación para el algoritmo resumen, que eliminará el riesgo de patrones que podrían producirse debido a frecuentes actualizaciones de semilla con datos de entrada sustancialmente similares, y mejorará la calidad de la semilla aleatoria.

Luego, en la etapa 820, un proceso iterativo concatena cada salida resumen o valor resumen, (en adelante HV) y por tanto forma bloques de datos de salida resumen. Esto se debe al hecho de que un procedimiento resumen normalmente resulta en una salida que tiene un tamaño de datos que es menor, o mucho menor, que el tamaño de datos de los datos de entrada. El número de iteraciones depende del tamaño deseado de los datos de salida.

Luego se dividen los bloques de datos de salida en bloques de datos de clave y bloques de datos de semilla en la etapa 830. Los bloques de datos de clave y los bloques de datos de semilla se usan como datos de entrada en la parte del cálculo de números aleatorios. Esto se puede expresar matemáticamente como

Datos de entrada:	datos ópticos	$= SU_{2*m-1}..SU_1\ SU_D$
Cálculo:	SI_x	$= Resumen_n\ (SI_x, SU_x)$
Datos de salida:	entrada de	$= SI_{2*m-1}..SI_1, SI_0$
	semilla	$= SK_{m-1},...SK_1SK_0SD_{m-1}...SD_1SD_0$
	datos de clave	$= SK_{m-1}...SK_1SK_0$
	datos de semilla	$= SD_{m-1}...SD_1SD_0$

donde en Y/n, Y es la longitud de bits del número aleatorio a generar en la segunda etapa, y n es la longitud de bits de los datos de salida del algoritmo resumen, Resumen. Además, SU_x es el bloque x de datos de entrada, SI_x es el bloque x de datos de salida, SK_x es el bloque x de datos de clave y SD_x es el bloque x de datos de semilla. En esta realización,

el algoritmo resumen se realiza usando un algoritmo de cifrado simétrico, AES. Como entenderán los expertos en la técnica, hay un número significativo de algoritmos concebibles que se pueden usar para obtener una aleatoriedad aumentada y que se pueden implementar en lugar del algoritmo AES. La actualización de semilla se puede realizar con una actualización total de la semilla, es decir, con todos los bloques de datos incluidos en SI, o con un bloque de datos, SI_x. Esto depende de los requisitos del algoritmo de cálculo de números aleatorios en la parte dos y de la potencia de ordenador disponible.

Después, en la etapa 840, en la parte del cálculo de números aleatorios, se usan los bloques de datos de clave y los bloques de datos de semilla como datos de entrada en un segundo algoritmo, que en esta realización utiliza un algoritmo de cifrado simétrico, por ejemplo el AES. El algoritmo realizado en la etapa 840 es un algoritmo iterativo. Como se ha mencionado anteriormente, existe un número de algoritmos de cifrado alternativos que se pueden usar en dicho segundo algoritmo en lugar del AES, por ejemplo el IDEA o el DES. Alternativamente, se podrían usar los algoritmos A3 ó A5, que son cifras de corriente y se usan para cifrado simétrico. Se incluye también un contador, para la cuenta de semilla. El contador cuenta el número de veces que se ha usado el cálculo de números aleatorios desde que se actualizaron los datos de entrada en la actualización de semilla. Matemáticamente, el cálculo de números aleatorios se puede expresar como

Datos de entrada:	datos de clave	$= SK_{m-1}...SK_1SK_0$
	datos de semilla	$= SD_{m-1}...SD_1SD_0$
	cuenta de semilla	
Cálculo:	Para x desde 0 hasta (m-1)	
	1.1 PR_x	= Cifrado (clave = SK_x, entrada = SD_x)
	1.2 $SK_{(x+2)modm}$	$= SK_{(x+2)modm}$ xorPR_x
	1.3 $SD_{(x+1)modm}$	$= SD_{(x+1)modm}$ xorPR_x
	cuenta de semilla	= cuenta de semilla +1
Datos de salida:	número aleatorio	$= PR_{m-1}...PR_1PR_0$
	datos de clave	$= SK_{m-1}...SK_1SK_0$
	datos de semilla	$= SD_{m-1}....SD_1SD_0$
	cuenta de semilla	

donde PRx es un bloque x de datos de números aleatorios, xor es una operación XOR, mod es una operación de módulo, y "cifrado" es un algoritmo de cifrado simétrico. Asimismo, en la etapa de cálculo se realiza una transformación de bloque. Esta transformación aumenta más la aleatoriedad de los números aleatorios.

La transformación de las etapas 1.2 y 1.3 se podría hacer en una serie de otras formas, pero el método descrito asegura que todos los cambios en un bloque se transforman a lo largo de la mayor parte de la semilla aleatoria, y por tanto asegura una semilla aleatoria de alta calidad para el cálculo siguiente.

De acuerdo con una realización alternativa, el segundo algoritmo es una función resumen, preferiblemente usando el mismo algoritmo de cifrado simétrico que en el segundo algoritmo anteriormente descrito.

Finalmente, en la etapa 850, el método vuelve al procedimiento mostrado en la Figura 4 en la etapa 460, en la que se realiza el cifrado real del mensaje usando, en esta realización preferida, el algoritmo de cifrado AES, donde los datos de número aleatorio PRx obtenidos por medio del método anterior se usan como la clave de cifrado en la etapa 460 de la Figura 4.

Alternativamente, se efectúa un cifrado de los datos de número aleatorio PRx, por ejemplo mediante el uso de un algoritmo de cifrado asimétrico. Luego, los datos de número aleatorio cifrados se envían al receptor del mensaje cifrado. El receptor efectúa un resumen de los datos de número aleatorio cifrados y usa el valor resumen resultante como una clave de cifrado privada, que luego se usa como un algoritmo de cifrado asimétrico para el descifrado del mensaje recibido.

Aunque en la presente memoria se han mostrado y descrito realizaciones específicas a título ilustrativo y de ejemplo, los expertos en la técnica entenderán que las realizaciones específicas mostradas y descritas se podrían sustituir por una amplia variedad de realizaciones alternativas y/o equivalentes sin apartarse del alcance del presente invento. Los expertos en la técnica observarán fácilmente que el presente invento se puede implementar en una amplia variedad de realizaciones, incluyendo diversas implementaciones de hardware y software, o combinaciones de las mismas. Esta solicitud está destinada a cubrir cualesquiera adaptaciones o variaciones de las realizaciones preferidas descritas en la presente memoria. Por consiguiente, el presente invento se define mediante el texto de las reivindicaciones que se adjuntan como apéndice.

REIVINDICACIONES

1. Un método en un bolígrafo digital (en adelante DP) para cifrar un mensaje para la transmisión segura de dicho mensaje desde el bolígrafo digital (DP) a un receptor (en adelante ALS, SH, SP) **caracterizado** por las etapas de obtener el mensaje mediante el registro de imágenes de una superficie (2) provista de un patrón (3) de código de posición usando un detector óptico (8) del bolígrafo digital (DP) y la determinación de al menos una posición a partir de las imágenes;

obtener (410-420) datos ópticos para la generación de una clave de cifrado usando el detector óptico (8) del bolígrafo digital (DP), cuyos datos ópticos representan electrónicamente valores de un parámetro óptico legible por dicho detector óptico (8);

generar (430-450) exclusivamente por tratamiento electrónico en una unidad de tratamiento (10) del bolígrafo digital, la clave de cifrado,

usar dichos datos ópticos como semilla aleatoria; y

cifrar (480) dicho mensaje usando dicha clave de cifrado en un algoritmo de cifrado.

2. El método de acuerdo con la reivindicación 1, en el que se detecta el brillo en dicho parámetro óptico mediante dicho detector óptico (8).

3. El método de acuerdo con las reivindicaciones 1 ó 2, en el que la etapa (410-420) de obtener datos ópticos comprende la. etapa de obtener dichos datos ópticos a partir de una parte de una superficie (2) provista de un patrón (3) de código de posición, en el que dicho patrón (3) de código de posición incluye unas marcas ópticas legibles (4), y en el que dicho parámetro óptico es representativo de dicha parte.

4. El método de acuerdo con una cualquiera de las reivindicaciones 1 a 3, en el que la etapa (430-450) de generar una clave de cifrado comprende las etapas de

tratar (430) dichos datos ópticos de acuerdo con un esquema predeterminado,

organizar (440) dichos datos ópticos tratados en campos de datos, en los que cada campo de datos tiene un tamaño predeterminado, y

organizar (440) dichos campos de datos en un orden predeterminado en registros de datos.

5. El método de acuerdo con la reivindicación 4, en el que la etapa (430) de tratar dichos datosópticos comprende la etapa de calcular propiedades estadísticas de conjuntos de dichos valores de parámetros ópticos representados por dichos datos ópticos, por lo que dichas propiedades estadísticas constituyen dichos datos ópticos tratados.

6. El método de acuerdo con la reivindicación 5, en el que dichas propiedades estadísticas comprenden un valor máximo, un valor mínimo y un valor suma de dicho conjunto de valores de parámetros ópticos, y en el que las etapas (440) de organizar comprenden las etapas de

organizar dicho valor máximo en al menos un campo de datos máximos, dicho valor mínimo en al menos un campo de datos mínimos, y dicho valor suma en al menos un campo de datos suma, y

organizar dichos campos de datos máximos, mínimos y suma en un registro de datos de acuerdo con dicho orden predeterminado.

7. El método de acuerdo con una cualquiera de las reivindicaciones 4 a 6, en el que la etapa (430-450) de generar una clave de cifrado comprende además las etapas de

redisponer (520) el orden de dichos campos de datos dentro de al menos un registro de datos de una primera serie de registros de datos de acuerdo con un primer algoritmo de reordenación, obteniendo de ese modo una primera serie de registros de datos redispuestos, y

redisponer (530) el orden de dichos campos de datos dentro de al menos un registro de datos de una segunda serie de registros de datos de acuerdo con un segundo algoritmo de reordenación, obteniendo de ese modo una segunda serie de registros de datos redispuestos.

8. El método de acuerdo con la reivindicación 7, en el que una clave de cifrado comprende datos de clave y datos de entrada, y en el que la etapa (430-450) de generar una clave de cifrado comprende las etapas de

usar (540) dicha primera serie de registros de datos redispuestos como dichos datos de clave, y

usar (540) dicha segunda serie de registros de datos redispuestos como dichos datos de entrada.

9. El método de acuerdo con una cualquiera de las reivindicaciones 4 a 6, en el que la etapa (430-450) de generar una clave de cifrado comprende las etapas de

tratar un conjunto de un número predeterminado de dichos registros de datos en una primera etapa (810-820), usando una primera función resumen, obteniendo de ese modo una primera salida,

tratar dicha primera salida en una segunda etapa (830-840) usando un algoritmo iterativo, obteniendo de ese modo una segunda salida, y

usar (850) dicha segunda salida como dicha clave de cifrado o para generar dicha clave de cifrado.

10. El método de acuerdo con la reivindicación 9, en el que, en dicha segunda etapa (830-840), dicha primera salida se trata usando una segunda función resumen.

11. El método de acuerdo con las reivindicaciones 9 ó 10, en el que en dichas etapas primera y segunda (810-820, 830-840), se usan, respectivamente, un primero y un segundo algoritmos de cifrado simétrico.

12. El método de acuerdo con la reivindicación 11, en el que se usa un algoritmo de cifrado simétrico como dicho primero y como dicho segundo algoritmos de cifrado simétrico.

13. El método de acuerdo con la reivindicación 12, en el que se usa un algoritmo de cifrado simétrico como dicho algoritmo de cifrado simétrico para realizar dicha etapa (460) de cifrar dicho mensaje, y como dichos algoritmos simétricos primero y segundo.

14. El método de acuerdo con una cualquiera de las reivindicaciones precedentes, en el que la clave de cifrado comprende datos de clave y datos de entrada, cuyo método comprende además las etapas de

usar un primer subconjunto de dichos datos ópticos para generar dichos datos de clave, y

usar un segundo subconjunto de dichos datos ópticos para generar dichos datos de entrada.

15. El método de acuerdo con una cualquiera de las reivindicaciones precedentes, en el que dicho algoritmo de cifrado para cifrar dicho mensaje es un algoritmo de cifrado simétrico.

16. El método de acuerdo con la reivindicación 1, que comprende además las etapas de

obtener datos de presión usando medios de detección de presión, en el que la etapa (430-450) de generar una clave de cifrado comprende la etapa de

generar la clave de cifrado usando dichos datos de presión en combinación con dichos datos ópticos como semilla aleatoria.

17. El método de acuerdo con la reivindicación 1, que comprende además las etapas de

obtener datos de tiempo, en el que la etapa (430-450) de generar una clave de cifrado comprende la etapa de

generar la clave de cifrado usando dichos datos de tiempo combinados con dichos datos ópticos como semilla aleatoria.

18. El método de acuerdo con una cualquiera de las reivindicaciones precedentes, en el que dichas etapas se realizan en un bolígrafo digital (en adelante DP), que comprende dicho detector óptico (8) y medios de transmisión (12).

19. Un medio legible por ordenador que comprende instrucciones para llevar a un ordenador a realizar un método de acuerdo con una cualquiera de las reivindicaciones precedentes.

20. Un bolígrafo digital (DP) para cifrar un mensaje para la transmisión segura de dicho mensaje desde el bolígrafo digital (DP) a un receptor (ALS, SH, SP), **caracterizado** por un detector óptico (8) para registrar imágenes de una superficie (2) provista de un patrón (3) de código de posición;

medios de recepción (10) para recibir datos ópticos del detector óptico (8) para la generación de una clave de cifrado, cuyos datos ópticos representan electrónicamente valores de un parámetro óptico legible por dicho detector óptico (8),

medios de tratamiento (10) para generar, exclusivamente mediante tratamiento electrónico, la clave de cifrado usando dichos datos ópticos como semilla aleatoria, y para obtener dicho mensaje mediante la determinación de al menos una posición de dichas imágenes registradas;

medios de cifrado (10) para cifrar el mensaje a transmitir usando dicha clave de cifrado.

21. El bolígrafo digital de acuerdo con la reivindicación 20, en el que dichos datos ópticos se han obtenido de una parte de una superficie (2) provista de un patrón (3) de código de posición que tiene unas marcas ópticas legibles (4).

22. El bolígrafo digital de acuerdo con la reivindicación 21, en el que dichos medios de tratamiento (10) están dispuestos además para

tratar dichos datos ópticos de acuerdo con un esquema predeterminado,

organizar dichos datos ópticos tratados en campos de datos, en los que cada campo de datos tiene un tamaño predeterminado, y

organizar dichos campos de datos en un orden predeterminado en registros de datos.

23. El bolígrafo digital de acuerdo con la reivindicación 22, en el que dichos medios de tratamiento (10) están dispuestos además para calcular propiedades estadísticas de conjuntos de dichos valores de parámetros ópticos representados por dichos datos ópticos, por lo que dichas propiedades estadísticas constituyen dichos datos ópticos tratados.

24. El bolígrafo digital de acuerdo con la reivindicación 23, en el que dichas propiedades comprenden un valor máximo, un valor mínimo y un valor suma de dicho conjunto de valores de parámetros ópticos, y en el que dichos medios de tratamiento (10) están dispuestos además para organizar dicho valor máximo en al menos un campo de datos máximos, dicho valor mínimo en al menos un campo de datos mínimos, y dicho valor suma en al menos un campo de datos suma, y

organizar dichos campos de datos máximos, mínimos y suma en un registro de datos de acuerdo con dicho orden predeterminado.

25. El bolígrafo digital de acuerdo con una cualquiera de las reivindicaciones 22 a 24, en el que dichos medios de tratamiento (10) están dispuestos además para redisponer el orden de dichos campos de datos dentro de al menos un registro de datos de una primera serie de registros de datos de acuerdo con un primer algoritmo de reordenación, obteniendo de ese modo una primera serie de registros de datos redispuestos, y

redisponer el orden de dichos campos de datos dentro de al menos un registro de datos de una segunda serie de registros de datos de acuerdo con un segundo algoritmo de reordenación, obteniendo de ese modo una segunda serie de registros de datos redispuestos.

26. El bolígrafo digital de acuerdo con la reivindicación 25, en el que una clave de cifrado comprende datos de clave y datos de entrada, y en el que los medios de tratamiento (10) están dispuestos además para

usar dicha primera serie de registros de datos redispuestos como dichos datos de clave, y

usar dicha segunda serie de registros de datos redispuestos como dichos datos de entrada.

27. El bolígrafo digital de acuerdo con una cualquiera de las reivindicaciones 22 a 24, en el que los medios de tratamiento (10) están dispuestos además para

tratar un conjunto de un número predeterminado de dichos registros de datos en una primera etapa usando una primera función resumen, obteniendo de ese modo una primera salida,

tratar dicha primera salida en una segunda etapa usando un algoritmo iterativo, obteniendo de ese modo una segunda salida, y

usar dicha segunda salida como dicha clave de cifrado o para generar dicha clave de cifrado.

28. El bolígrafo digital de acuerdo con la reivindicación 27, en el que dichos medios de tratamiento (10) están dispuestos además para usar una segunda función resumen para tratar dicha primera salida en dicha segunda etapa.

29. El bolígrafo digital de acuerdo con las reivindicaciones 27 ó 28, en el que, en dichas etapas primera y segunda, se usan respectivamente un primero y un segundo algoritmo de cifrado simétrico.

30. El bolígrafo digital de acuerdo con la reivindicación 29, en el que los medios de tratamiento están dispuestos además para usar un algoritmo de cifrado simétrico como dicho primero y como dicho segundo algoritmos de cifrado simétrico.

31. El bolígrafo digital de acuerdo con la reivindicación 29, en el que se usa uno y el mismo algoritmo de cifrado simétrico por dichos medios (10) de cifrado para cifrar dicho mensaje, y por dichos medios de tratamiento (10) como dicho primero y dicho segundo algoritmos de cifrado simétrico.

32. El bolígrafo digital de acuerdo con una cualquiera de las reivindicaciones 20 a 31, en el que dichos medios de cifrado (10) están dispuestos además para cifrar dicho mensaje usando un algoritmo de cifrado simétrico.

33. El bolígrafo digital de acuerdo con una cualquiera de las reivindicaciones 20 a 32, en el que dichos medios de cifrado (10) están dispuestos además para

usar un subconjunto de dichos datos ópticos como datos de clave para dicho algoritmo de cifrado, y

usar un segundo subconjunto de dichos datos ópticos como datos de entrada para dicho algoritmo de cifrado.

34. El bolígrafo digital de acuerdo con la reivindicación 20, en el que dichos medios de recepción (10) están dispuestos además para recibir datos de presión, y en el que dichos medios de tratamiento (10) están dispuestos para generar dicha clave de cifrado usando dichos datos de presión en combinación con dichos datos ópticos.

35. El bolígrafo digital de acuerdo con la reivindicación 20, en el que dichos medios de tratamiento (10) están dispuestos además para obtener datos de tiempo, y para generar dicha clave de cifrado usando dichos datos de tiempo combinados con dichos datos ópticos.

36. Un método para la autenticación de un mensaje enviado, en el que dicho mensaje se envía desde un bolígrafo digital (DP) a un receptor (ALS, SH, SP), **caracterizado** por las etapas de

obtener el mensaje mediante el registro de imágenes de una superficie (2) provista de un patrón (3) de código de posición usando un detector óptico (8) del bolígrafo digital (DP) y la determinación de al menos una posición de las imágenes,

obtener datos ópticos para la generación de datos de números aleatorios usando el detector óptico (8) del bolígrafo digital (DP), cuyos datos ópticos representan electrónicamente valores de un parámetro óptico legibles por dicho detector óptico (8),

usar dichos datos ópticos para generar los datos de números aleatorios, exclusivamente mediante el tratamiento electrónico en una unidad de tratamiento (10) del bolígrafo digital (DP),

cifrar dichos datos de números aleatorios, y

usar dichos datos de números aleatorios para la autenticación de dicho mensaje.

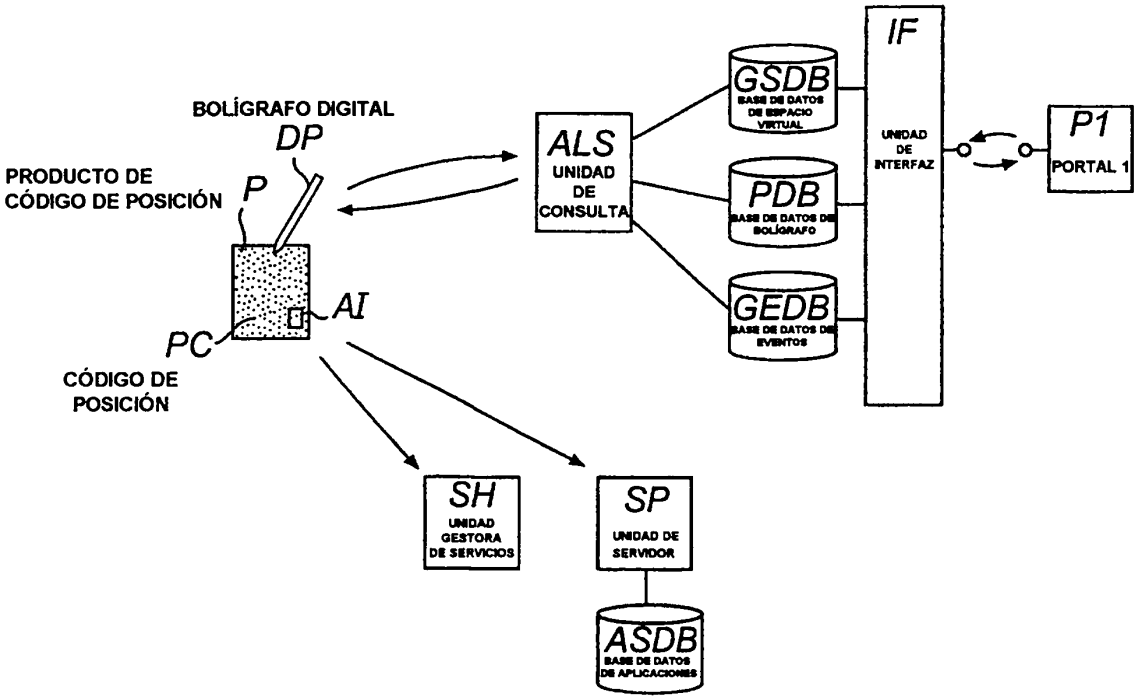
BOLÍGRAFO DIGITAL
DP
PRODUCTO DE CÓDIGO DE POSICIÓN
P
AI
PC
CÓDIGO DE POSICIÓN
ALS
UNIDAD DE CONSULTA
GSDB
BASE DE DATOS DE ESPACIO VIRTUAL
PDB
BASE DE DATOS DE BOLÍGRAFO
GEDB
BASE DE DATOS DE EVENTOS
IF
UNIDAD DE INTERFAZ
P1
PORTAL 1
SH
UNIDAD GESTORA DE SERVICIOS
SP
UNIDAD DE SERVIDOR
ASDB
BASE DE DATOS DE APLICACIONES

Fig. 1

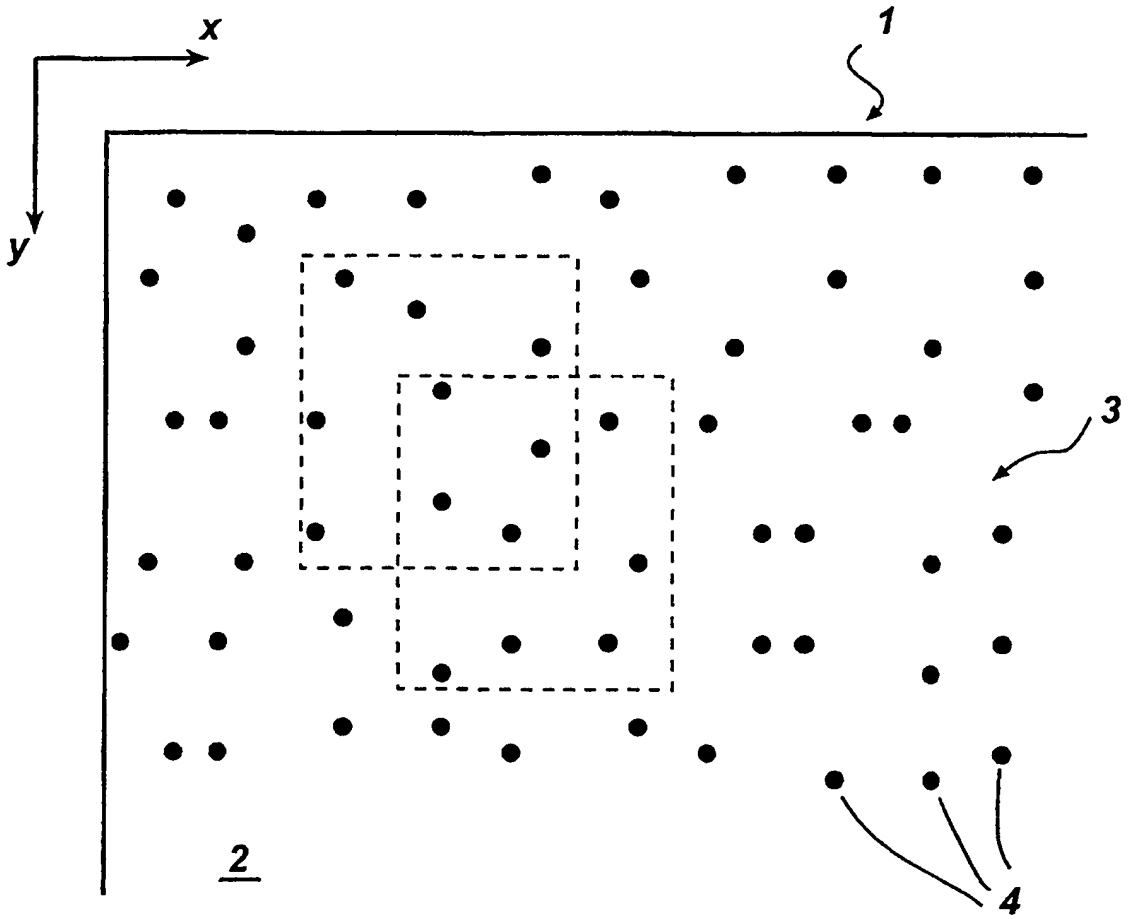

Fig. 2

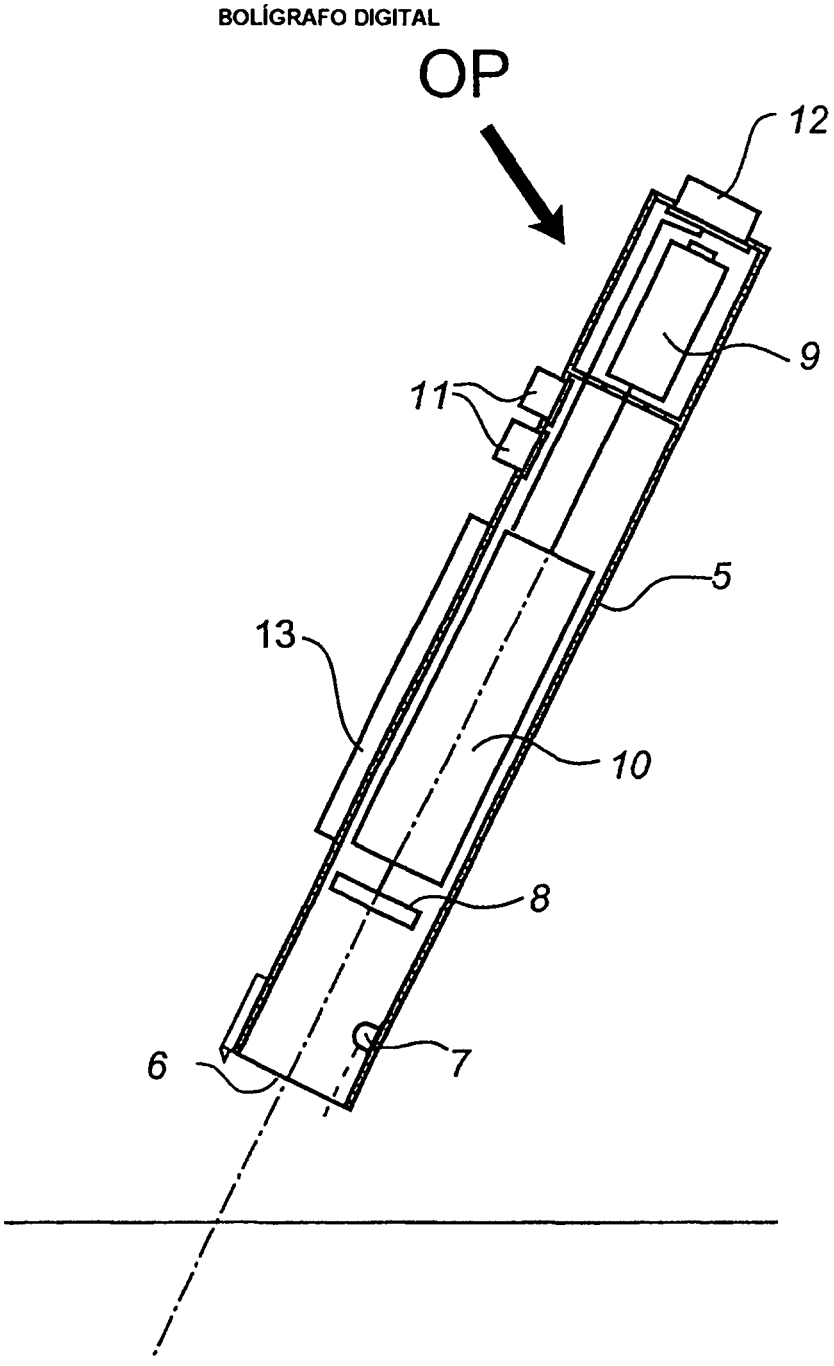

Fig. 3

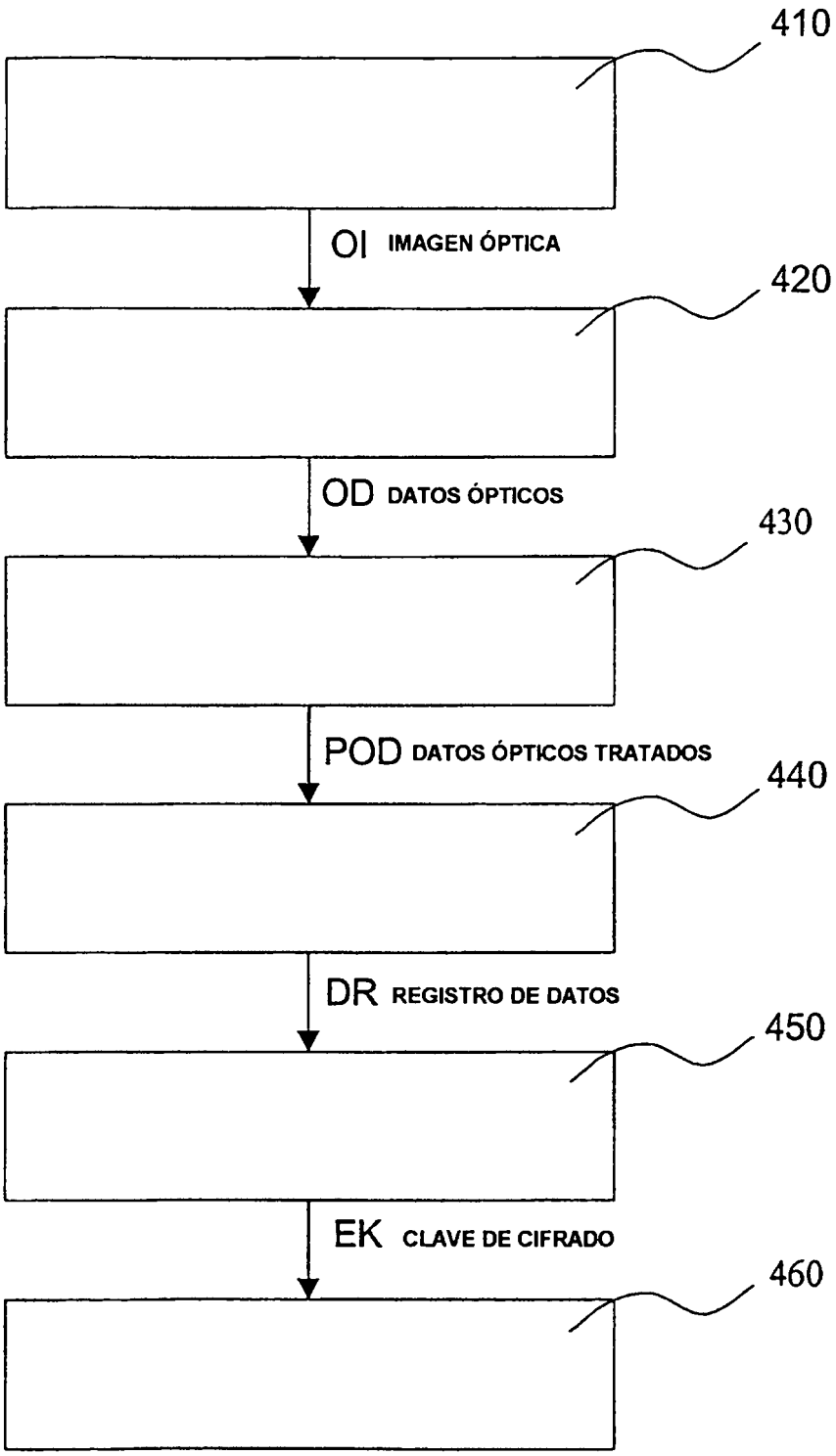
410
OI IMAGEN ÓPTICA
420
OD DATOS ÓPTICOS
430
POD DATOS ÓPTICOS TRATADOS
440
DR REGISTRO DE DATOS
450
EK CLAVE DE CIFRADO
460

Fig. 4

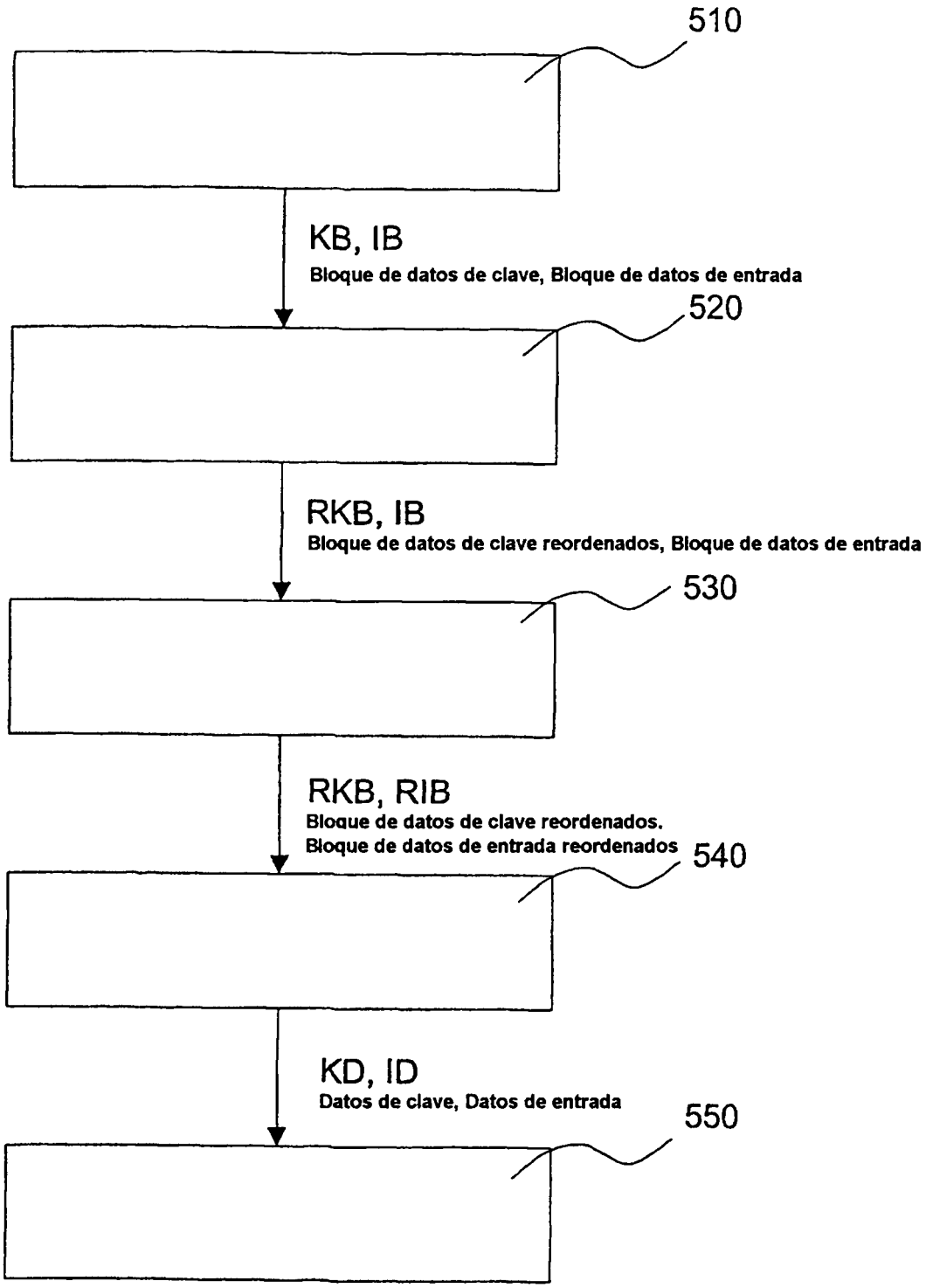
510
KB, IB
Bloque de datos de clave, Bloque de datos de entrada
520
RKB, IB
Bloque de datos de clave reordenados, Bloque de datos de entrada
530
RKB, RIB
Bloque de datos de clave reordenados.
Bloque de datos de entrada reordenados
540
KD, ID
Datos de clave, Datos de entrada
550

Fig. 5

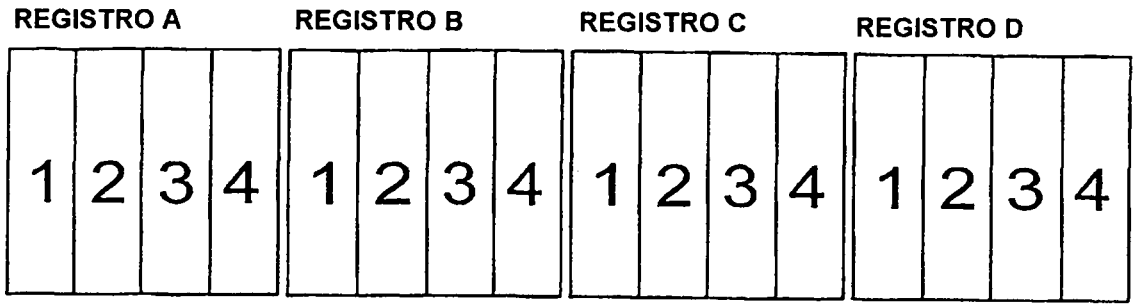

Fig. 6

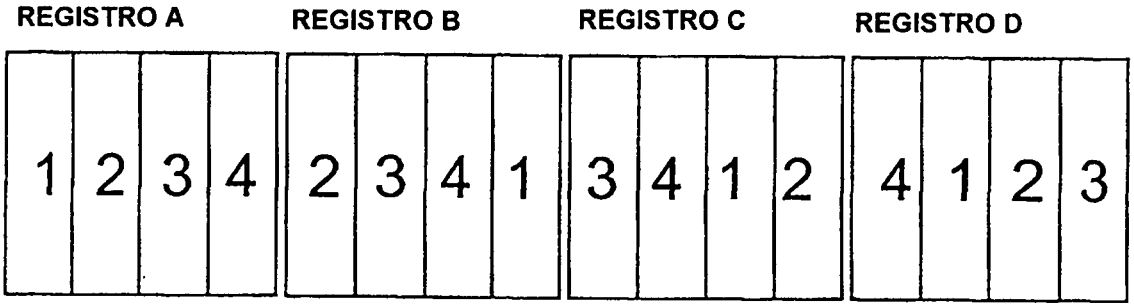

Fig. 7A

Fig. 7B

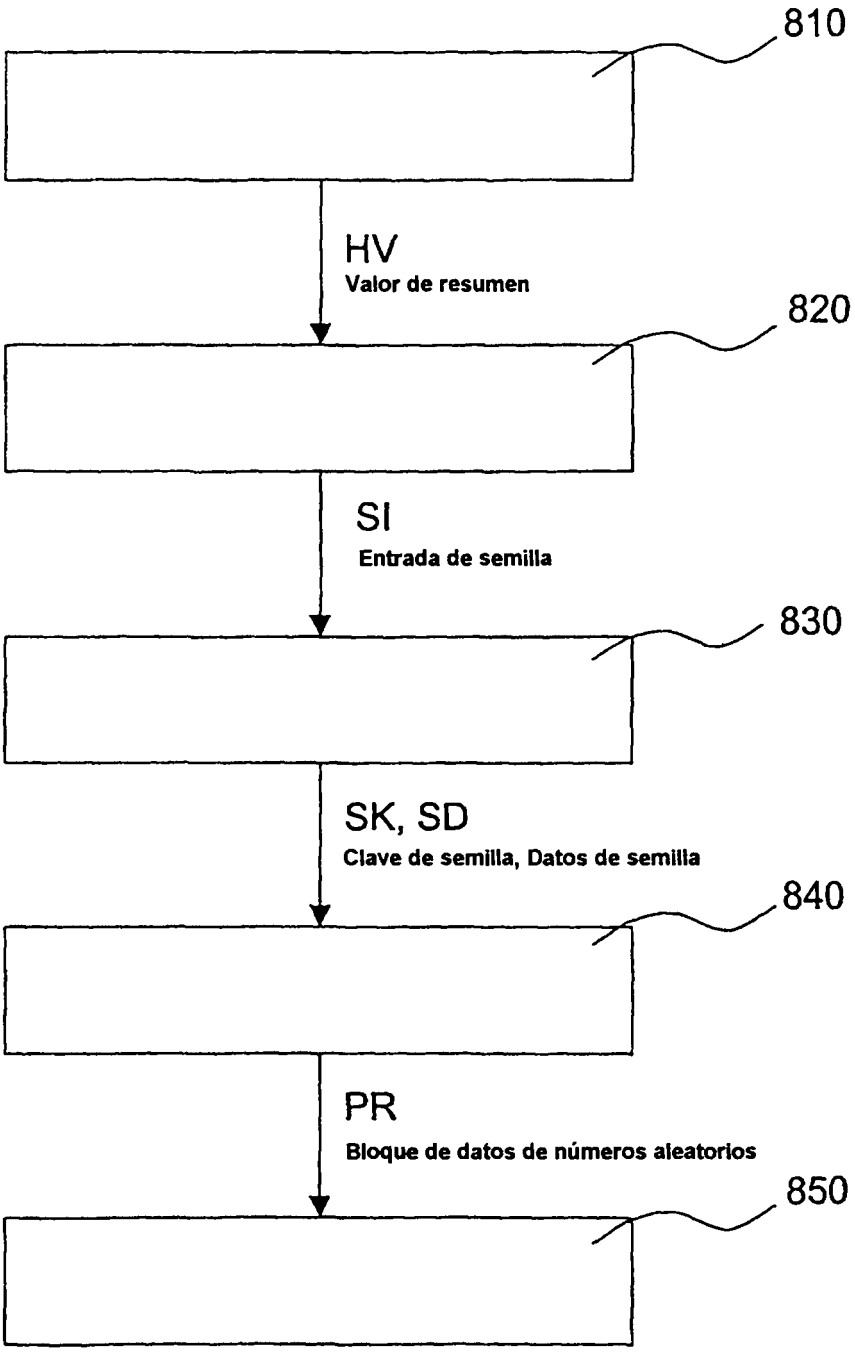
810
HV
Valor de resumen
820
SI
Entrada de semilla
830
SK, SD
Clave de semilla, Datos de semilla
840
PR
Bloque de datos de números aleatorios
850

Fig. 8