(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 685 123**

(21) Número de solicitud: 201700377

(51) Int. CI.:

G09C 1/00 (2006.01)
G06F 21/87 (2013.01)
H04L 9/06 (2006.01)

(12) SOLICITUD DE PATENTE A1

(22) Fecha de presentación:

31.03.2017

(43) Fecha de publicación de la solicitud:

05.10.2018

(71) Solicitantes:

GRUPREX S.L. (100.0%)
Ríos Rosas 36, 7º C
28003 Madrid ES

(72) Inventor/es:

ASENSIO ARROYO, Jesús Damaso

(74) Agente/Representante:

CAPITAN GARCÍA, Nuria

(54) Título: **Dispositivo de cifrado individual con mecanismo de protección de credenciales de usuario**

(57) Resumen:

Dispositivo que realiza la doble función de, por un lado, proteger la información de un usuario en su ordenador personal cifrando el contenido de ficheros seleccionados por el usuario y, por otro lado, las comunicaciones entre éste y contactos mediante una transformación de credenciales (login/password). El dispositivo cuenta con un microcontrolador central, que se comunica con un FPGA (dispositivo programable) que utiliza un LFSR y que utiliza una generación de una semilla o un número aleatorio que en combinación con los valores de serie de tablas numéricas para crear claves de sesión. El dispositivo cuenta también con una memoria EPROM criptográfica, un conector USB en modo esclavo para su conexión a un PC, un zócalo para memorias microSD y otro conector USB en modo maestro para conectar un teclado. El dispositivo cuenta con un exclusivo mecanismo antiapertura y con medios de destrucción en caso de intento de apertura.

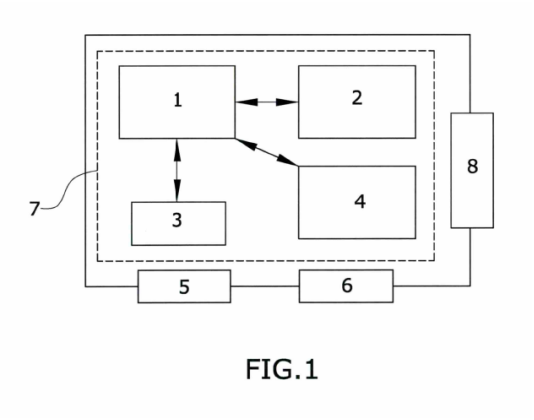

FIG.1

ES 2 685 123 A1

DESCRIPCIÓN

Dispositivo de cifrado individual con mecanismo de protección de credenciales de usuario.

Objeto de la invención

El objeto de la presente invención, tal y como el título establece, un dispositivo que realiza la doble función de, por un lado, proteger la información de un usuario en su ordenador personal cifrando el contenido de ficheros seleccionados por el usuario y, por otro lado, las comunicaciones entre éste y contactos de su grupo de confianza y también para la identificación de personas, que puede llevarse a cabo mediante una transformación de credenciales (login/password).

Caracteriza al presente dispositivo las especiales características funcionales y constructivas que presenta que realiza las funciones de cifrado individual además de permitir la protección de las credenciales (usuario y password) en el proceso de acceso a una web. Además el dispositivo cuenta con unos medios de protección en caso de robo, uso no permitido o acceso al mismo.

Se trata de un dispositivo de cifrado simétrico de uso individual y personalizado para cada usuario. El dispositivo ofrece dos tipos de cifrado simétrico, uno de ellos es un cifrado propietario exclusivamente implementado en hardware, bien en un microcontrolador o bien en un FPGA (Field Programmable Gate Array) (dispositivo programable) diseñado para este hecho y por otro lado un cifrado simétrico estándar como puede ser AES (Advanced Encryption Standard) o IDEA (International Data Encryption Algorithm). Pudiendo utilizarse cualquiera de los dos tipos de cifrado que se desee.

El dispositivo contiene un algoritmo electrónico que lleva a cabo transformadas matemáticas de las credenciales introducidas por el usuario, es decir, el Login/Password de cualquier web o entorno remoto, evitando que un troyano capaz de leer el teclado mientras el usuario teclea dichas credenciales pueda posteriormente utilizarlas para entrar en el área de acceso de dicho usuario.

El dispositivo, también está diseñado para evitar que ante el robo del mismo, un usurpador pueda utilizarlo como si del usuario legítimo se tratara. Para ello, cuando el dispositivo es conectado al PC del usuario, una aplicación de gestión que controla el dispositivo en modo “standalone” obtiene el modelo de ordenador y el número de serie de dicha aplicación, enviándolos al dispositivo, que junto a su número único de serie almacena esos datos en una memoria segura. De esta forma, se lleva a cabo un emparejamiento entre el dispositivo, la aplicación y el PC para evitar el funcionamiento en otro ordenador no perteneciente al usuario. Por supuesto, el usuario, una vez adquirido el dispositivo y en su primer uso, introduce una clave que el dispositivo almacena en su memoria segura de forma que el usuario podrá utilizar el dispositivo cuando introduzca la clave previamente seleccionada.

El dispositivo está diseñado para llevar a cabo un intercambio de claves utilizando un algoritmo de intercambio de claves asimétrico o bien mediante certificación X.509, por ejemplo. Se conecta al ordenador a través de una conexión USB en la que actúa como esclavo y posee otra entrada USB para el control de un teclado que le permite introducir datos escritos y cifrarlos antes de su llegada al ordenador. El dispositivo se caracteriza, además de lo ya comentado, por incluir un mecanismo antiapertura basado en una capa que le envuelve completamente y formada por un cristal piezoeléctrico en forma de polímero. De esta forma, el cristal es conectado al microcontrolador central del dispositivo, que contiene un algoritmo capaz de discernir entre un uso normal del dispositivo o un intento de apertura mediante las formas de onda que produce el cristal piezoeléctrico.

Antecedentes de la invención

Existen algunas aproximaciones a la algoritmia utilizada por el dispositivo de esta invención. Entre las más destacadas se encuentran la patente US2006177065A1 y también la patente US20130142328A1. En el primer caso, la patente US2006177065A1 hace referencia a un sistema y método para llevar a cabo operaciones de cifrado mediante una operación XOR, una tabla numérica y en la cual se generan números aleatorios para formar una clave con los valores de la tabla. Ahora bien, lo que hace el algoritmo mencionado en esa patente es seleccionar un subconjunto de valores de la tabla numérica a través de una generación de números aleatorios pero se trata de un proceso lineal. En nuestro caso, el algoritmo que utilizamos lleva a cabo la generación no lineal de claves de forma que no se puede llevar a cabo una ingeniería inversa para intentar descubrir la clave o la forma de generación de claves de forma lineal. Tampoco protege de ataques texto claro-texto cifrado ya que en nuestro caso, si alguien no autorizado obtiene el dispositivo e intenta enviar un mensaje al dispositivo para ver la respuesta de éste y así determinar cuál puede ser la clave de cifrado, no obtendrá respuesta alguna del dispositivo debido a que dicho dispositivo se comunica exclusivamente con la aplicación en PC autorizada para ello o bien, a través de los mensajes enviados por otro dispositivo electrónico autorizado.

En el segundo caso, la patente US20130142328A1, hace referencia a un sistema y método de cifrado que utiliza claves de un solo uso pero que no se generan de la misma forma que en nuestro caso.

Los dispositivos anteriores presentan una serie de inconvenientes susceptibles de ser mejorados como por ejemplo el hecho de que en caso de quedar comprometida por un atacante la tabla numérica empleada en la encriptación, todos los dispositivos empleadores de dichas tablas deberían cambiar la tabla por una nueva. También carecen de medios de generación de claves de cifrado a través de un mecanismo de generación no lineal. Tampoco cuentan con medios que permiten detectar proceso de intentos de apertura del dispositivo y además con medios de autodestrucción de la información e incluso de parte del hardware.

Por lo tanto, es objeto de la presente invención desarrollar un dispositivo que supere los anteriores inconvenientes y que además permita realizar la doble función de por un lado, un cifrado individual y por otro lado contar con medios de protección de credenciales de usuario, desarrollando un dispositivo como el que a continuación se describe y queda recogido en su esencialidad en la reivindicación primera.

Explicación de la invención

Es un objeto de la presente invención un dispositivo de cifrado/descifrado de información, de uso individual, que está diseñado para proteger la información del ordenador de un usuario, permitiendo además del cifrado/descifrado, transformar las credenciales de un usuario (login/password) de forma que su hardware calcula el login/password real que se comprobará en el servidor correspondiente, ya sea de una entidad bancaria o de cualquier índole y que, por tanto, invalida la utilización del login/password tecleado por el usuario de modo que un keylogger o troyano capaz de leer el teclado, adquiera una información inservible si capta lo pulsado por el usuario.

El dispositivo, en este sentido y de forma exclusiva y muy característico de esta invención, puede funcionar en modo USB a través de un puerto serie virtual o mediante conexión USB pura de alto rendimiento para el caso de cifrar archivos o comunicaciones a tiempo real o bien, en modo USB HID para el caso de introducción de credencialescontando con un interruptor digital interno que le permite funcionar en el modo correspondiente, comunicación serie a través de puerto serie virtual, USB HID o USB nativo de alto rendimiento. El motivo de este

triple mecanismo de comunicación reside en que los navegadores de Internet sólo aceptan dispositivos que se comunican mediante HID (Human Interface Device). Por tanto, este dispositivo puede funcionar en los tres modos, por un lado como USB de alto rendimiento para envío de datos masivo o bien como HID para su interacción con los navegadores de Internet y, como dispositivo conectado a un puerto serie virtual.

El dispositivo comprende un microcontrolador central de alto rendimiento, que se comunica con un FPGA (dispositivo programable) que contiene un algoritmo de cifrado simétrico basado en un cifrado no lineal que utiliza un LFSR(linear feedback shift register) que se traduce como registro de desplazamiento con retroalimentación lineal y que utiliza una serie de tablas numéricas para crear claves de sesión a través de la generación de semillas aleatorias, es decir el principio de funcionamiento se basa en la generación de una semilla que no es más que un número aleatorio que en combinación con los valores de una tabla generan una clave de sesión. El dispositivo cuenta también con una memoria EPROM criptográfica que almacena de forma cifrada los datos que indica el microcontrolador central.

A modo de conexionado, el dispositivo posee un conector USB en modo esclavo para su conexión a un PC, un zócalo para memorias microSD y otro conector USB en modo maestro para conectar un teclado o una memoria USB (pen drive).

El dispositivo posee un interruptor digital interno que le permite funcionar en modo USB HID o USB normal de alto rendimiento, a través de un puerto de comunicaciones virtual, por ejemplo.

El dispositivo cuenta con un exclusivo mecanismo antiapertura basado en un polímero piezoeléctrico que rodea todo el dispositivo y que es controlado por el microcontrolador central. Así pues, en modo de utilización normal, el mecanismo piezoeléctrico emite unas ondas eléctricas que son muy distintas a aquellas que implican intento de apertura del dispositivo. El dispositivo, en ese momento y a través del controlador central, activa un mecanismo de alto voltaje que destruye el microcontrolador central y hace inservible el dispositivo eliminando además la información útil que hubiera en dicho dispositivo.

Para la gestión del dispositivo se instala en el ordenador del usuario una aplicación software. La primera vez que el dispositivo se conecta al PC a través de la aplicación, éste solicita al usuario la introducción de una clave de acceso. Una vez introducida la clave, ésta se almacena en la memoria criptográfica del dispositivo para sus posteriores usos. Otra información que se almacena en dicha memoria es un código de la aplicación, información única del PC donde se encuentra instalada la aplicación y en la que está conectado el dispositivo. Así, si el dispositivo se ha de instalar en otro PC posteriormente, la aplicación se instalará en dicho PC, el dispositivo solicitará la clave de acceso (en este caso a modo de comprobación) al usuario y de nuevo, el dispositivo obtendrá datos de la aplicación y del PC actual, que guardará en su memoria criptográfica. De este modo, si en algún momento, el dispositivo es robado o el usuario lo pierde y alguien intenta hacer uso de él, el dispositivo conocerá que una nueva aplicación está en un nuevo PC, y si al tercer intento de introducción de la contraseña ésta no es correcta, entonces se activa el mecanismo electrónico de autodestrucción basado en alto voltaje. Si es posible, la misma aplicación del PC enviará un mensaje de alerta al centro de control correspondiente indicando el dispositivo (número de serie) que ha sufrido un intento de robo o intento de acceso no autorizado.

Salvo que se indique lo contrario, todos los elementos técnicos y científicos usados en la presente memoria poseen el significado que habitualmente entiende un experto normal en la técnica a la que pertenece esta invención. En la práctica de la presente invención se pueden usar procedimientos y materiales similares o equivalentes a los descritos en la memoria.

A lo largo de la descripción y de las reivindicaciones la palabra “comprende” y sus variantes no pretenden excluir otras características técnicas, aditivos, componentes o pasos. Para los expertos en la materia, otros objetos, ventajas y características de la invención se desprenderán en parte de la descripción y en parte de la práctica de la invención.

Breve descripción de los dibujos

Para complementar la descripción que se está realizando y con objeto de ayudar a una mejor comprensión de las características de la invención, de acuerdo con un ejemplo preferente de realización práctica de la misma, se acompaña como parte integrante de dicha descripción, un juego de dibujos en donde con carácter ilustrativo y no limitativo, se ha representado lo siguiente.

La figura 1 muestra una representación de los distintos componentes del dispositivo.

La figura 2 muestra un esquema del sistema conectado a un PC y el intercambio de información global.

La figura 3 muestra un esquema del dispositivo en modo USB HID para la transformación de credenciales electrónicamente.

La figura 4 muestra el aspecto del mecanismo antiapertura y el circuito electrónico de destrucción.

Realización preferente de la invención

A la vista de las figuras se describe seguidamente un modo de realización preferente de la invención propuesta.

En la figura 1 se pueden observar los diferentes elementos electrónicos del dispositivo. El dispositivo comprende:

- Un microcontrolador central (1) de alto rendimiento, que contienen una pluralidad de tablas.

- Un FPGA (dispositivo programable) (2) comunicado con el microcontrolador central (1), donde el FPGA (2) contiene un algoritmo de cifrado simétrico basado en un cifrado no lineal que utiliza un LFSR (linear feedback shift register) que se traduce como registro de desplazamiento con retroalimentación lineal y que utiliza la generación de una semilla o un número aleatorio que en combinación con los valores de una serie de tablas numéricas para crear claves de sesión.

- Una memoria EPROM criptográfica (3) que almacena de forma cifrada los datos que indica el microcontrolador central (1).

- Un mecanismo antiapertura (4) en conexión con el microcontrolador central (1).

- Un primer conector USB (5) esclavo para la conexión a un ordenador personal.

- Un segundo conector USB (6) maestro para teclado.

- Un mecanismo antiapertura que en una posible forma de realización está basado en un polímero piezoeléctrico (7) que rodea todo el dispositivo y que es controlado por el microcontrolador central.

- Un zócalo para una memoria micro SD (8).

En la figura 2 podemos observar el dispositivo objeto de la invención (10) conectado a un PC (9) y el flujo de datos entre aplicación y dispositivo, entre los que encontramos:

- Un primer proceso de emparejamiento (11).

- Un segundo proceso de emparejamiento (12).

- Un tercer proceso de envío (13) de archivos para almacenamiento en la memoria micro SD.

- Un cuarto proceso (14) de transformación de credenciales de usuario.

Una realización preferente de la invención se produce cuando el dispositivo actúa como máquina inteligente de cifrado/descifrado utilizando el algoritmo de cifrado simétrico basado en generación no lineal de claves. El microcontrolador central (1) del dispositivo contiene unas tablas de 1024 bytes cada una como tamaño mínimo y de 8192 bytes cada una como tamaño máximo. A través de estas tablas numéricas (se entienden como vectores unidimensionales) el dispositivo es capaz de seleccionar la clave de cifrado al mismo tiempo que cifra cada byte de información. Esto se lleva a cabo a través de un algoritmo de generación no lineal basado en LFSR. El dispositivo puede seleccionar aleatoriamente la tabla a utilizar. Una vez seleccionada la tabla, se selecciona una semilla aleatoria a través del generador de números aleatorios por hardware que incluye el microcontrolador central y también tras la medición del tiempo pasado entre la conexión del dispositivo y la llegada del primer comando de cifrado. Este mecanismo es exclusivo del dispositivo electrónico. Así, la semilla, de 16 bits se forma por la combinación de ambos números aleatorios, mecanismo también exclusivo de este dispositivo. Una vez que se ha calculado la semilla aleatoria, a través de una secuencia generada por el LFSR, se van obteniendo datos de la tabla y son precisamente estos datos los que se utilizan para el cifrado XOR con el byte correspondiente al texto plano.

Para evitar ataques típicos de estos mecanismos XOR, tales como ataque por texto plano-texto cifrado, el dispositivo no puede comunicarse con nada salvo con la aplicación instalada y previamente emparejada del ordenador del usuario.

Cuando el dispositivo ha cifrado el mensaje plano, éste es devuelto a la aplicación del PC que lo envía a su destino, generalmente otro PC con otro dispositivo de esta invención. No obstante, entre el camino suele haber un servidor que actúa como elemento de confianza entre los dispositivos y que permite llevar a cabo un control de la gestión de estos dispositivos y sus usuarios. El flujo de comunicación en el bus USB también puede securizarse para evitar un proceso de escucha.

En la figura 3 se muestra el proceso de protección de credenciales mediante el dispositivo objeto de la invención. Cuando en el acceso a una página web de un servidor (19) se nos pidan el login y el password, a través del teclado (20) se envían (15) las credenciales hacia el dispositivo de cifrado (10) en el que se produce la transformación (16) de las credenciales procediendo a continuación al envío (17) de las credenciales transformadas hacia el PC (9) y desde éste hacia el servidor web (19) a través de internet (18).

En una realización preferente de la invención, cuando un usuario accede a una página web que le solicita sus credenciales en modo Login/Password, el usuario introduce dichos parámetros. El navegador web interactúa con el dispositivo (10) en modo USB HID (electrónicamente seleccionado) y éste último procede a llevar a cabo una transformación matemática en función del tiempo utilizando el mismo algoritmo de generación no lineal. En este específico caso, se

selecciona el número de serie (único a nivel mundial) del dispositivo y a través del que se genera una semilla, seleccionando aquellos valores correspondientes en el recorrido de la tabla de claves. Se lleva a cabo finalmente una función hash segura y ese es el dato que se enviará al servidor (19) de la página web, que verificará el dato en su base de datos para dar acceso al usuario a los servicios de la web, ya sea banca online u otro tipo de web. De esta forma, se evitan ataques de tipo keylogger pero también de tipo grabación de vídeo de la pantalla del usuario, screenlogger, etc.

En la figura 4 puede observarse el mecanismo antiapertura que comprende el polímero piezoeléctrico (7) conectado con el microcontrolador central (1) mediante un puerto de entrada (21) a través del cual se analizan las señales procedentes del polímero piezoeléctrico (7), contando sobre el microcontrolador (1) con un puerto de salida (22) para activación hacia un mosfet (23) alimentado desde una batería (24).

Descrita suficientemente la naturaleza de la presente invención, así como la manera de ponerla en práctica, se hace constar que, dentro de su esencialidad, podrá ser llevada a la práctica en otras formas de realización que difieran en detalle de la indicada a título de ejemplo, y a las cuales alcanzará igualmente la protección que se recaba, siempre que no altere, cambie o modifique su principio fundamental.

REIVINDICACIONES

1. Dispositivo de cifrado individual con mecanismo de protección de credenciales de usuario caracterizado porque comprende:

- Un microcontrolador central (1) que contiene una pluralidad de tablas.

- Un FPGA (dispositivo programable) (2) comunicado con el microcontrolador central (1), donde el FPGA (2) contiene un algoritmo de cifrado simétrico basado en un cifrado no lineal que utiliza un LFSR (linear feedback shift register) que se traduce como registro de desplazamiento con retroalimentación lineal y que utiliza la generación de una semilla o un número aleatorio que en combinación con los valores de una serie de tablas numéricas para crear unas claves de sesión.

- Una memoria EPROM criptográfica (3) que almacena de forma cifrada los datos que indica el microcontrolador central (1).

- Un mecanismo de antiapertura (4) en conexión con el microcontrolador central (1) y que está basado en un polímero piezoeléctrico (7) que rodea todo el dispositivo y que es controlado por el microcontrolador central.

- Un primer conector USB (5) esclavo para la conexión a un ordenador personal.

- Un segundo conector USB (6) maestro para teclado.

- Un mecanismo antiapertura.

- Un zócalo para una memoria micro SD (8).

2. Dispositivo de cifrado individual con mecanismo de protección de credenciales de usuario según la reivindicación 1 caracterizado porque el microcontrolador central (1) del dispositivo contiene unas tablas de 1024 bytes cada una como tamaño mínimo y de 8192 bytes cada una como tamaño máximo.

3. Dispositivo de cifrado individual con mecanismo de protección de credenciales de usuario según cualquiera de las reivindicaciones anteriores caracterizado por que adicionalmente comprende un cifrado simétrico como puede ser AES (Advanced Encryption Standard) o IDEA (International Data Encryption Algorithm).

4. Dispositivo de cifrado individual con mecanismo de protección de credenciales de usuario según cualquiera de las reivindicaciones anteriores caracterizado por que el dispositivo puede funcionar en modo USB a través de un puerto serie virtual o mediante conexión USB nativa de alto rendimiento para el caso de cifrar archivos o comunicaciones a tiempo real o bien, en modo USB HID para el caso de introducción de credenciales, contando con un interruptor digital interno que le permite funcionar en el modo correspondiente, comunicación serie a través de puerto serie virtual, en modo USB HID o USB nativo de alto rendimiento.

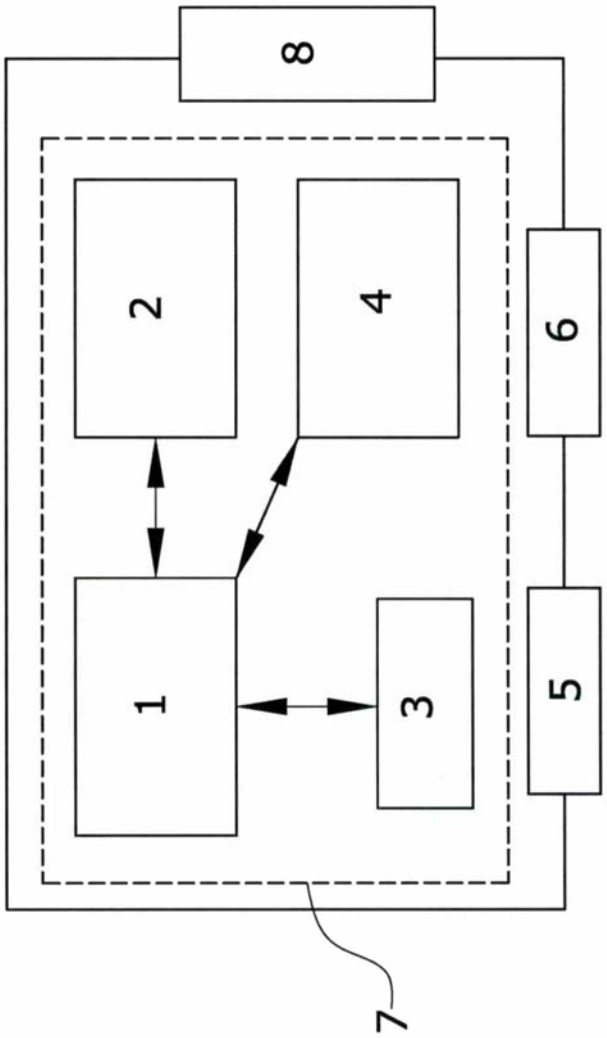

FIG.1

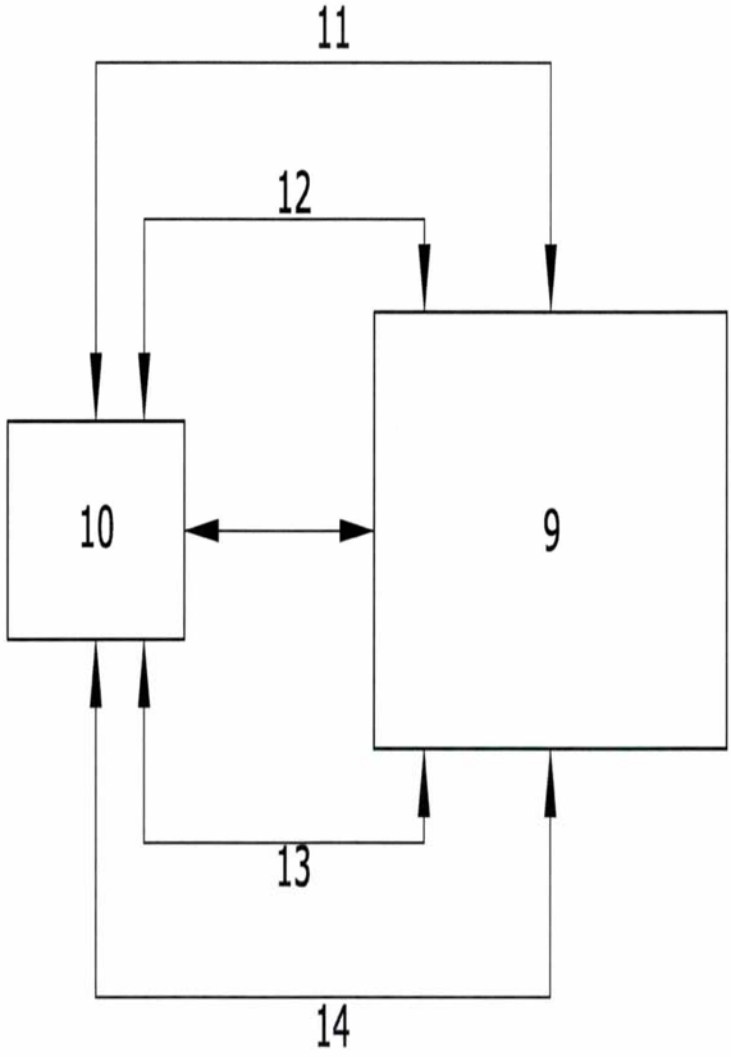

FIG.2

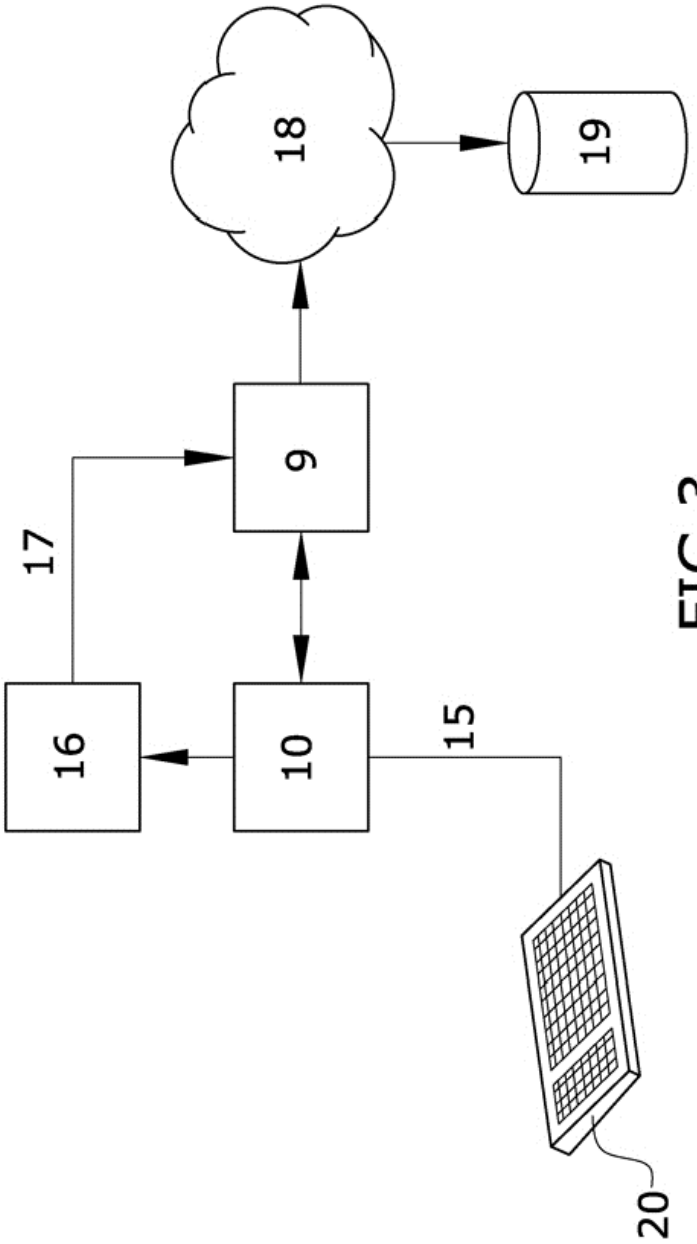

FIG.3

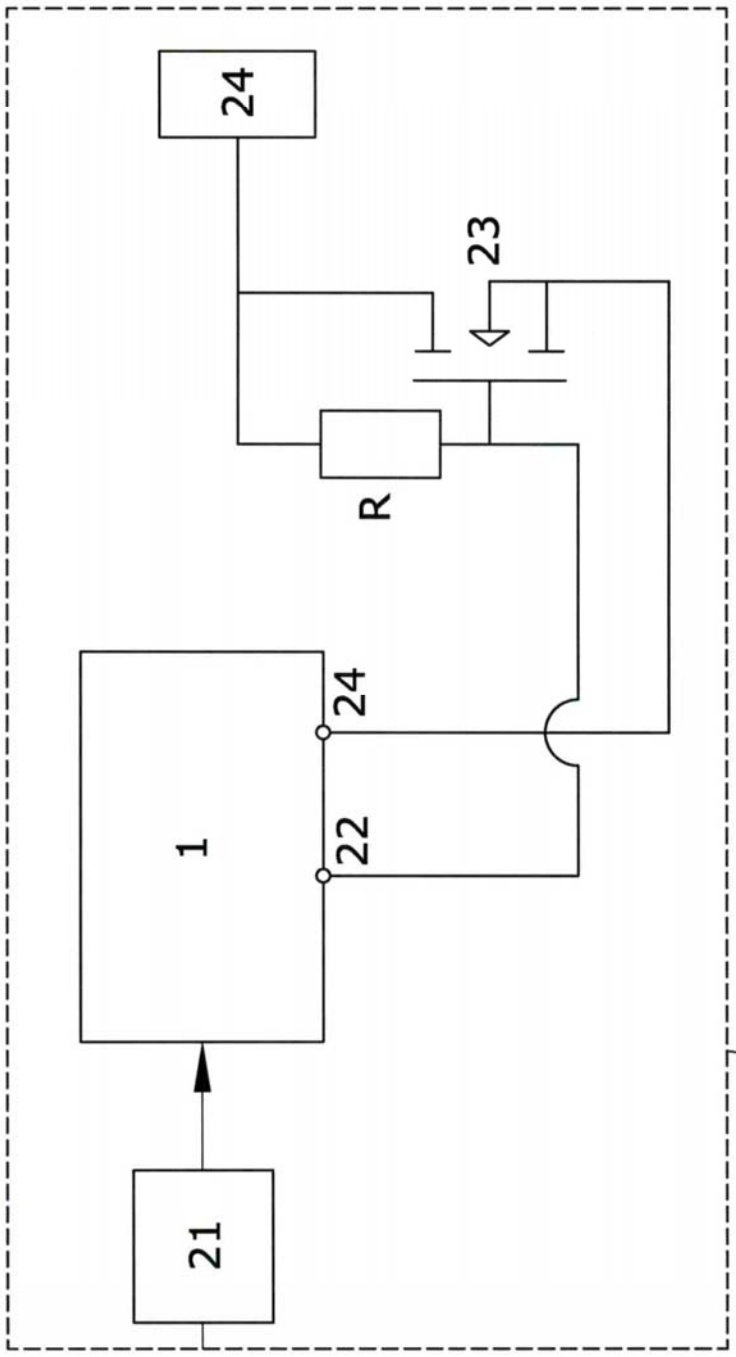

FIG.4

OFICINA ESPAÑOLA
DE PATENTES Y MARCAS

ESPAÑA

(21) N.º solicitud: 201700377

(22) Fecha de presentación de la solicitud: 31.03.2017

(32) Fecha de prioridad:

INFORME SOBRE EL ESTADO DE LA TECNICA

(51) **Int. CI. :** Ver Hoja Adicional

DOCUMENTOS RELEVANTES

Categoría	(56) **Documentos citados**	**Reivindicaciones afectadas**
Y	US 2009220083 A1 (SCHNEIDER JAMES P) 03/09/2009, párrafo [1]; párrafos [18 - 20]; párrafos [24 - 49]; párrafo [56]; párrafos [60 - 63]; párrafo [66]; Párrafo [71]; párrafo [75]; párrafo [79]; párrafos [84 - 88]; reivindicación 10, figuras 1 - 2. Figura 5,	1-4
Y	WO 9105306 A1 (UNIV SYDNEY TECH et al.) 18/04/1991, Página 1 páginas 4 - 11; reivindicaciones 1-2; reivindicaciones 20-22; reivindicaciones 32-33; reivindicación 53, figuras 1 - 2.	1-4
A	Meiser G et al. EFFICIENT IMPLEMENTATION OF ESTREAM CIPHERS ON 8-BIT AVR MICROCONTROLLERS. Industrial Embedded Systems, 2008. SIES 2008. International Symposium on, 20080611 IEEE, Piscataway, NJ, USA. Kai Huang; Bacivarov I; Hugelshofer F; Thiele L, 11/06/2008, Páginas 58 - 66 [en línea][recuperado el 2/08/2018]. Recuperado de Internet <URL: https://ieeexplore.ieee.org/abstract/document/4577681/ >, ISBN 978-1-4244-1994-4; ISBN 1-4244-1994-8. Apartados I-III	2

Categoría de los documentos citados

X: de particular relevancia
Y: de particular relevancia combinado con otro/s de la misma categoría
A: refleja el estado de la técnica
O: referido a divulgación no escrita
P: publicado entre la fecha de prioridad y la de presentación de la solicitud
E: documento anterior, pero publicado después de la fecha de presentación de la solicitud

El presente informe ha sido realizado

☒ para todas las reivindicaciones ☐ para las reivindicaciones nº:

Fecha de realización del informe	**Examinador**	**Página**
30.08.2018	J. M. Vazquez Burgos	1/6

OFICINA ESPAÑOLA
DE PATENTES Y MARCAS

ESPAÑA

(21) N.º solicitud: 201700377

(22) Fecha de presentación de la solicitud: 31.03.2017

(32) Fecha de prioridad:

INFORME SOBRE EL ESTADO DE LA TECNICA

(51) **Int. Cl. :** Ver Hoja Adicional

DOCUMENTOS RELEVANTES

Categoría	(56) **Documentos citados**	**Reivindicaciones afectadas**
A	Jan Axelson. USB EMBEDDED HOSTS. THE DEVELOPER'S GUIDE. 30/11/2011 <URL: http://janaxelson.com/usb_embedded_hosts.htm >, 978-1931448246. páginas 34 - 35; ; página 179; páginas 218 - 220; páginas 229 - 231; páginas 263 - 266;	4
A	Jan Axelson. USB COMPLETE. THE DEVELOPER'S GUIDE, FIFTH EDITION. 31/03/2015 <URL: http://janaxelson.com/usbc.htm >, 978-1-931448-28-4. página 67; páginas 77 - 78;	4
A	EP 2852089 A1 (WINBOND ELECTRONICS CORP) 25/03/2015. párrafos [1 - 2]; párrafos [4 - 7]; párrafos [11 - 16]; párrafo [20]; párrafo [22]; párrafos [25 - 73]; figura 1,	1-4

Categoría de los documentos citados

X: de particular relevancia
Y: de particular relevancia combinado con otro/s de la misma categoría
A: refleja el estado de la técnica
O: referido a divulgación no escrita
P: publicado entre la fecha de prioridad y la de presentación de la solicitud
E: documento anterior, pero publicado después de la fecha de presentación de la solicitud

El presente informe ha sido realizado

☒ para todas las reivindicaciones ☐ para las reivindicaciones nº:

Fecha de realización del informe	**Examinador**	**Página**
30.08.2018	J. M. Vazquez Burgos	2/6

CLASIFICACIÓN OBJETO DE LA SOLICITUD

G09C1/00 (2006.01)
G06F21/87 (2013.01)
H04L9/06 (2006.01)

Documentación mínima buscada (sistema de clasificación seguido de los símbolos de clasificación)

G09C, G06F, H04L

Bases de datos electrónicas consultadas durante la búsqueda (nombre de la base de datos y, si es posible, términos de búsqueda utilizados)

INVENES, EPODOC, WPI, INTERNET

Fecha de Realización de la Opinión Escrita: 30.08.2018

Declaración

Novedad (Art. 6.1 LP 11/1986)	Reivindicaciones	1-4	**SI**
	Reivindicaciones		**NO**
Actividad inventiva (Art. 8.1 LP11/1986)	Reivindicaciones		**SI**
	Reivindicaciones	1-4	**NO**

Se considera que la solicitud cumple con el requisito de aplicación industrial. Este requisito fue evaluado durante la fase de examen formal y técnico de la solicitud (Artículo 31.2 Ley 11/1986).

Base de la Opinión.-

La presente opinión se ha realizado sobre la base de la solicitud de patente tal y como se publica.

1. Documentos considerados.-

A continuación se relacionan los documentos pertenecientes al estado de la técnica tomados en consideración para la realización de esta opinión.

Documento	Número Publicación o Identificación	Fecha Publicación
D01	US 2009220083 A1 (SCHNEIDER JAMES P)	03.09.2009
D02	WO 9105306 A1 (UNIV SYDNEY TECH et al.)	18.04.1991
D03	Meiser G et al.. EFFICIENT IMPLEMENTATION OF ESTREAM CIPHERS ON 8-BIT AVR MICROCONTROLLERS. Industrial Embedded Systems, 2008. SIES 2008. International Symposium on, 20080611 IEEE, Piscataway, NJ, USA. Kai Huang; Bacivarov I; Hugelshofer F; Thiele L, Páginas 58 - 66 [en línea][recuperado el 2/08/2018]. Recuperado de Internet <URL: https://ieeexplore.ieee.org/abstract/document/4577681/ >, ISBN 978-1-4244-1994-4 ; ISBN 1-4244-1994-8	11.06.2008
D04	Jan Axelson. USB EMBEDDED HOSTS. THE DEVELOPER'S GUIDE. <URL: http://janaxelson.com/usb_embedded_hosts.htm >, ISSN 978-1931448246	30.11.2011
D05	Jan Axelson. USB COMPLETE. THE DEVELOPER'S GUIDE, FIFTH EDITION. <URL: http://janaxelson.com/usbc.htm >, ISSN 978-1-931448-28-4	31.03.2015

2. Declaración motivada según los artículos 29.6 y 29.7 del Reglamento de ejecución de la Ley 11/1986, de 20 de marzo, de Patentes sobre la novedad y la actividad inventiva; citas y explicaciones en apoyo de esta declaración

El documento del estado de la técnica más próximo es D01 y divulga un dispositivo que toma un mensaje de un emisor y lo encripta, entregándolo a un receptor, donde emisor y receptor pueden tomar la forma de dispositivos o aplicaciones.

Reivindicación 1

Con el fin de ilustrar de la forma más clara posible las diferencias entre el documento D01 del estado de la técnica más próximo y la invención reivindicada en 1, se reproduce seguidamente el texto de dicha reivindicación, eliminando del mismo sus referencias originales, e insertando donde proceda las de D01. Aquellas partes del texto que pudieran no estar incluidas en D01 se señalarían entre corchetes y en negrita.

Dispositivo de cifrado individual (párrafos 24-25, 62) con mecanismo de protección de credenciales de usuario caracterizado porque comprende:

- un microcontrolador central (502; párrafos 86, 88) que contiene una pluralidad de tablas.
- un FPGA (dispositivo programable) (párrafo 86) comunicado con el microcontrolador central (502), donde el FPGA contiene un algoritmo de cifrado simétrico basado en un cifrado no lineal que utiliza un LFSR (linear feedback shift register) que se traduce como registro de desplazamiento con retroalimentación lineal y que utiliza la generación de una semilla o un número aleatorio que en combinación con los valores de una serie de tablas numéricas para crear unas claves de sesión (párrafos 27, 33, 38, 40, 44).
- una memoria EPROM criptográfica (párrafos 18, 88) que almacena de forma cifrada los datos que indica el microcontrolador central (502).
- [**Un mecanismo de antiapertura en conexión con el microcontrolador central y que está basado en un polímero piezoeléctrico que rodea todo el dispositivo y que es controlado por el microcontrolador central**].
- Un primer conector USB (párrafos 27, 87) esclavo para la conexión a un ordenador personal.
- Un segundo conector USB (párrafo 87) maestro para teclado.
- [**Un mecanismo antiapertura**]
- Un zócalo para una memoria micro SD (párrafos 20, 25, 85)

El dispositivo divulgado en D01 proporciona un cifrado entre dos extremos que pueden ser entes físicos (equipos) o lógicos (aplicaciones) (párrafos 24-25, 62). Por tanto, ello incluye la posibilidad de uso individual, entre equipos o aplicaciones bajo control o supervisión de un mismo usuario. La información a transmitir puede ser de cualquier clase, y por lo tanto la posibilidad de la aplicación del dispositivo para hacer llegar unas credenciales a una aplicación es obvia para un experto en la materia.

Dado que D01 especifica que la lógica del dispositivo puede tomar la forma de varios microprocesadores, y que estos pueden ser de tipo FPGA (párrafo 86), esta posibilidad cubre el alojamiento de la lógica del LFSR en un procesador de este tipo, como una opción de implementación obvia para un experto en la materia. Lo mismo ocurre con el uso de una memoria EPROM, ya que D01 incluye la posibilidad de utilizar dicho tipo de memorias (párrafo 18). Asimismo, D01 menciona la posibilidad de conectar con memorias mediante USB, así como de conectarse con ordenadores y teclados, si bien sin concretar el tipo de conector. A este respecto, la aplicación de la conexión USB a estos dos últimos casos, constituye también una opción de implementación, obvia para un experto en la materia, habida cuenta de que la solución presentada en D01 contempla el uso de conexiones USB para la conexión de periféricos.
La diferencia entre la invención reivindicada en 1 y el dispositivo divulgado en D01 es que este último no incluye un sistema anti apertura, basado en polímeros piezoeléctricos y controlado por la lógica del dispositivo. El efecto técnico que ello tiene es que el dispositivo es vulnerable a ataques por intrusión, con el fin de desentrañar el mecanismo de encriptación/desencriptación. Y el problema técnico objetivo a resolver es del proveer al dispositivo divulgado en D01 de la capacidad de protección, detección y respuesta frente a intrusiones en el dispositivo, capaces de detectar presiones o deformaciones en su estructura, sin necesidad de recurrir a material metálico.

El documento D02 presenta un sistema de protección frente a intrusiones en equipos electrónicos, que pueden incluir aquellos dedicados a la encriptación o de desencriptación (página 4, último párrafo), mediante la cobertura de los mismos con polímeros piezoeléctricos (página 8, último párrafo - página 10; reivindicaciones 1-2, 20, 22). Tras la detección de una intrusión, el sistema puede responder conforme una lógica ejecutada por el circuito a proteger (página 7, primer párrafo).
Un experto en la materia, a la vista de las funciones de encriptación/desencriptación proporcionadas por el dispositivo divulgado en D01, y de la solución presentada en D02 para proteger, detectar y responder a intrusiones en dispositivos como el antes mencionado, no requeriría de actividad inventiva para, combinando el documento del estado de la técnica más próximo con las partes esenciales de D02, con el fin de conseguir las características reivindicadas en 1 con una expectativa razonable de éxito.

En consecuencia, a la luz de la combinación de D01 con D02 se concluye que la invención reivindicada en 1 no cumple con el requisito de actividad inventiva, tal y como este se define en el artículo 8 de la Ley de Patentes de 1986.

Reivindicaciones 2 a 4

El objeto de la reivindicación 2 concierne a las dimensiones mínimas y máximas de las tablas a almacenar en la memoria del microcontrolador. Semejante configuración constituye una opción de implementación obvia para un experto en la materia, puesto que el tamaño de las tablas dependerá de los parámetros concretos del encriptador, el tipo de almacenamiento utilizado, y de la cantidad de memoria disponible en el microcontrolador y en otras memorias auxiliares como las de tipo flash. En este sentido, dados estos grados de libertad, para un experto en la materia es obvio encontrar una solución que satisfaga el objeto de la reivindicación 2. A este respecto, el documento D03 muestra diferentes soluciones de implementación de encriptadores basados en LFSR (apartados II-III), con tablas almacenadas en la SDRAM del microcontrolador, conforme los límites reivindicados en algunos casos (II.A, II.B, tabla IV, implementación HC-128), ilustrando el grado de flexibilidad disponible a la hora de configurar la memoria de un dispositivo como el reivindicado.

Los algoritmos reivindicados en 3 están contemplados en D01 (párrafos 30, 61).

Las opciones con respecto a la conexión USB reivindicadas en 4 constituyen opciones de implementación que forman parte del conocimiento general común, como ilustran los documentos D04 (páginas 179, 229-231, 263-266) y D05 (páginas 67, 77-78). Asimismo, la conmutación por software a un modo u otro, en función de la interface exigida por el equipo conectado, es una función habitual de los sistemas operativos, por ejemplo en Windows, mediante la enumeración del dispositivo y la configuración automática para la comunicación con este, o con el concurso de identificadores para las interfaces utilizadas (documento D04, páginas 34-35, 218-220).

En consecuencia, de las consideraciones anteriores, y una vez tenidas en cuenta las correspondientes relaciones de dependencia, cabe concluir que, a la luz de la combinación de D01 con D02, las invenciones reivindicadas en 2 a 4 no cumplen con el requisito de actividad inventiva, tal y como este se define en el artículo 8 de la Ley de Patentes de 1986.