(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 719 848**

(51) Int. CI.:

G07C 9/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **23.05.2012 PCT/EP2012/002176**

(87) Fecha y número de publicación internacional: **29.11.2012 WO12159742**

(96) Fecha de presentación y número de la solicitud europea: **23.05.2012 E 12729343 (9)**

(97) Fecha y número de publicación de la concesión europea: **09.01.2019 EP 2715681**

(54) Título: **Procedimiento para generar un código de desbloqueo de uso único, actualmente válido, para una cerradura electrónica**

(30) Prioridad:

25.05.2011 DE 102011103134

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
16.07.2019

(73) Titular/es:

BELOXX NEWTEC GMBH (100.0%)
Am Brögel 1a
42285 Wuppertal, DE

(72) Inventor/es:

SCHWARZE, BENJAMIN;
BOCK, PETER y
BLUNCK, MATTHIAS

(74) Agente/Representante:

CARPINTERO LÓPEZ, Mario

DESCRIPCIÓN

Procedimiento para generar un código de desbloqueo de uso único, actualmente válido, para una cerradura electrónica

La presente invención se refiere a un sistema con una cerradura electrónica, que mediante la introducción de un código de desbloqueo de uso único, actualmente válido, puede llevarse de su estado de bloqueo a su estado de desbloqueo, así como un dispositivo electrónico dispuesta de manera separada de la cerradura.

Las cerraduras electrónicas y se usan, por ejemplo, para bloquear la posición de cierre de elementos de cerradura en armarios, cajas de seguridad, casillas de correo o espacios cerrados en edificios. Mediante la introducción de un código de desbloqueo en la cerradura electrónica, ésta se puede llevar desde su estado de bloqueo que bloquea la posición de cierre a su estado de desbloqueo, en el que el elemento de cierre puede moverse manualmente a una de sus posiciones de apertura. Un código de desbloqueo de este tipo puede estar formado, por ejemplo, por una secuencia numérica.

Para aumentar la seguridad contra un accionamiento no autorizado de las cerraduras electrónicas de este tipo, o de las instalaciones equipadas con las mismas, respectivamente, se conoce el uso de códigos de desbloqueo de uso único, por cuya introducción en la cerradura, ésta puede ser llevada una sola vez de su estado de bloqueo a su estado de desbloqueo. Para posteriormente volver a llevar esta cerradura electrónica de su estado de bloqueo a su estado de desbloqueo, se requiere la introducción de un nuevo código de desbloqueo de uso único, actualmente válido.

Por el documento EP 0 767 286 A2 se conoce un sistema con una cerradura electrónica que mediante el uso de una llave electrónica con un código de desbloqueo de uso único, actualmente válido, puede llevarse de su estado de bloqueo a su estado de desbloqueo, así como un dispositivo electrónico dispuesta de manera separada de la llave. Mediante la comunicación entre la llave y el dispositivo electrónico dispuesta de manera separada, se transmite información, tal como nuevos códigos de desbloqueo y códigos de encriptación, del dispositivo electrónico dispuesta de manera separada a la llave electrónica. La comunicación entre la llave y el dispositivo electrónico dispuesta de manera separada hace que la cerradura electrónica sea vulnerable a los ataques.

El documento US 2011/0041573 A1 describe un sistema con una cerradura electrónica, que mediante la introducción de un código de desbloqueo de uso único, actualmente válido, se puede llevar de su estado de bloqueo a su estado de desbloqueo, así como un dispositivo electrónico dispuesta de manera separada de la cerradura, en lo que la cerradura electrónica y el dispositivo electrónico están configurados para generar el código de desbloqueo de uso único, actualmente válido. Debido a que no se requiere una comunicación directa entre la cerradura y el dispositivo electrónico separado, el sistema no puede ser atacado por esta vía. Sin embargo, si se conoce la encriptación, se pueden hacer deducciones sobre los futuros códigos de desbloqueo únicos que se van a generar. En particular por el lado del fabricante de la cerradura o también del propietario de la cerradura, no se puede excluir la posibilidad de un accionamiento no autorizado por empleados actuales o anteriores, o por prestadores de servicio encargados, que hayan obtenido conocimiento de la encriptación.

El objetivo de la presente invención consiste en proveer un sistema para generar un código de desbloqueo de uso único, actualmente válido, para una cerradura electrónica, con el que se pueda crear una cerradura electrónica con máxima seguridad contra un accionamiento no autorizado.

Este objetivo se logra de acuerdo con la presente invención a través de un sistema del tipo mencionado al comienzo, debido a que el código de desbloqueo de uso único, actualmente válido, se genera mediante una encriptación del código de desbloqueo de uso único, actualmente válido, inmediatamente anterior, por medio de un algoritmo de encriptación, en lo que la encriptación se efectúa bajo consideración de un código de encriptación, en lo que la cerradura electrónica y el dispositivo electrónico están configurados para generar el código de encriptación a partir de un código maestro individual introducido y un código de clave almacenado en la electrónica de la cerradura incluido en un software del dispositivo electrónico. El código de desbloqueo de uso único, actualmente válido, es generado tanto por la electrónica de la cerradura como también por el dispositivo electrónico, en lo que se efectúa la misma encriptación del código de desbloqueo de uso único, actualmente válido, directamente precedente. Para el usuario del sistema es posible obtener conocimiento del código de desbloqueo de uso único, actualmente válido, a través del dispositivo electrónico dispuesta de manera separada, para luego poder introducir este código en la cerradura electrónica. Con esto no se requiere ninguna comunicación entre la cerradura y el dispositivo electrónico dispuesta de manera separada, que pudiera hacer que la cerradura se haga vulnerable al ataque de un hacker. Sin embargo, para el usuario si es posible obtener el código de desbloqueo de uso único, actualmente válido, de la cerradura a través del dispositivo electrónico dispuesta de manera separada.

El uso de acuerdo con la presente invención de un algoritmo de encriptación para generar el código de desbloqueo de uso único, actualmente válido, representa un uso muy atípico de un algoritmo de encriptación, en particular porque no se trata de hacer que una información accesible a todos sólo sea accesible para una determinada persona, de tal manera que incluso si se conoce el código de desbloqueo de uso único, actualmente válido, inicial, no se podrán sacar conclusiones sobre cuál será el siguiente código de desbloqueo de uso único, actualmente

válido, que se va a generar. Por lo tanto, un sistema de acuerdo con la presente invención se caracteriza por un alto grado de seguridad.

De acuerdo con la presente invención, el código de encriptación se genera a partir de un código maestro individual introducido y un código de clave almacenado en la electrónica de la cerradura. Esto le permite a un usuario de una cerradura electrónica generar individualmente los futuros códigos de desbloqueo de uso único mediante la introducción repetida de códigos maestros individuales. Para terceros es imposible tener conocimiento del código de desbloqueo de uso único, actualmente válido, de tal manera que no se puede producir ningún accionamiento no autorizado de una cerradura electrónica conforme a esta forma de realización, operada de acuerdo con la presente invención. Además, incluso el propio fabricante de una cerradura electrónica operada conforme a esta forma de realización del procedimiento de acuerdo con la presente invención, que tenga conocimiento del código de clave almacenado en la electrónica de la cerradura, debido a la individualización de los futuros códigos de desbloqueo de uso único que se produce mediante la introducción de los códigos maestros individuales, no podrá sacar ninguna conclusión sobre un código de desbloqueo de uso único actualmente válido o futuro. Por lo tanto, esta forma de realización sirve para crear una cerradura electrónica con un máximo nivel de seguridad contra el accionamiento no autorizado.

De acuerdo con otra forma de realización ventajosa de la presente invención, el primer código de desbloqueo de uso único, actualmente válido, después de la puesta en funcionamiento de la cerradura electrónica se genera en base a un código inicial individual introducido como código de desbloqueo de uso único, actualmente válido, directamente precedente. También con esto se logra la mayor individualización posible de los códigos de desbloqueo de uso único futuros. Esta forma de realización además ofrece la posibilidad de poder restablecer la cerradura electrónica a un estado inicial definido, en caso de que el código de desbloqueo de uso único, actualmente válido, ya no se conozca. En este caso, el usuario de la cerradura introduce nuevamente un código inicial individual y luego un código maestro individual en la cerradura electrónica. A partir de esto se genera el siguiente código de desbloqueo de uso único, actualmente válido. Preferentemente, se puede señalizar a la cerradura electrónica si el código introducido ha de ser un código inicial o un código maestro.

De acuerdo con otra forma de realización ventajosa de la presente invención, como algoritmo de encriptación se emplea AES (Advanced Encryption Standard), DES (Data Encryption Standard), Triple-DES, Blowfish, RC4 (Ron's Code 4), RC5 o RC6. Estos algoritmos de encriptación se caracterizan por un alto grado de seguridad.

Preferentemente, el código de desbloqueo de uso único, actualmente válido, es generado tanto por la electrónica de la cerradura como también por un programa que se ejecuta en el dispositivo electrónico y que es visualizado por este dispositivo electrónico, en lo que a través del programa se efectúa la misma encriptación del código de desbloqueo de uso único, válido de manera directamente precedente, que en la electrónica de la cerradura. Mediante la visualización del código de desbloqueo de uso único, actualmente válido, el usuario del sistema de acuerdo con la presente invención puede tener conocimiento del código de desbloqueo de uso único, actualmente válido, para luego poder introducirlo en la cerradura electrónica. Como dispositivo electrónico se puede emplear tanto un dispositivo electrónico móvil como también un dispositivo electrónico estacionario. Ejemplos de dispositivos móviles son los terminales de radiotelefonía móvil convencionales, ordenadores portátiles u otros dispositivos similares. Como dispositivo estacionario se puede emplear, por ejemplo, un ordenador de sobremesa (PC).

La presente invención se describe más detalladamente a continuación con referencia a los ejemplos de realización mostrados en las figuras adjuntas. En las figuras:

La Fig. 1 muestra una representación esquemática del procedimiento.

La Fig. 2 muestra una representación esquemática de un ejemplo de realización para el sistema de acuerdo con la presente invención.

La figura 1 muestran esquemáticamente el procedimiento para generar un código de desbloqueo 1 de uso único, actualmente válido. Para generar este código de desbloqueo 1 de uso único, actualmente válido, primero se usa un código maestro 2 individual, introducido en la cerradura, y un código de clave 3 almacenado en la electrónica de la cerradura, para generar un código de encriptación 4. Este código de encriptación 4 se usa para la encriptación del código de desbloqueo 5 de uso único, válido de manera inmediatamente anterior, por medio del algoritmo de encriptación 6.

La figura 2 muestran esquemáticamente un ejemplo de realización del sistema 7 de acuerdo con la presente invención, con una cerradura electrónica 9 dispuesta en un elemento de cierre 8 de una unidad de cierre no representada con mayor detalle, así como un dispositivo electrónico 10 dispuesto de manera separada, en forma de un ordenador de sobremesa (PC). Para la puesta en funcionamiento de la cerradura electrónica 9, primero el usuario de la cerradura electrónica 9 introduce un código inicial individual como código de desbloqueo de uso único, válido de manera inmediatamente anterior, en la cerradura electrónica 9. Luego el usuario introduce un código maestro individual en la cerradura. Como se muestra en la figura 1, a partir de estos códigos introducidos se genera el código de desbloqueo de uso único, actualmente válido, con el que la cerradura electrónica 9 se puede llevar de su estado de bloqueo a su estado de desbloqueo. El usuario de la cerradura electrónica 9 recibe del fabricante de la cerradura

9 un software, que se instala en el dispositivo electrónico 10. Este software comprende el mismo algoritmo de encriptación que también se encuentra almacenado en la electrónica de la cerradura 9. Además, el software comprende el mismo código de clave que también se encuentra almacenado en la electrónica de la cerradura 9. Si el usuario después de la puesta en funcionamiento de la cerradura 9 introduce en el dispositivo electrónico 10 el mismo código inicial individual y el mismo código maestro individual que ya ha introducido previamente en la cerradura 9, el software ejecutado en el dispositivo electrónico 10 genera el mismo código de desbloqueo de uso único, actualmente válido, que también ha sido generado por la cerradura electrónica 9. A través del dispositivo de visualización 11 en el dispositivo electrónico 10, el usuario puede leer el código de desbloqueo de uso único, actualmente válido, e introducirlo en la cerradura electrónica 9 para llevar la cerradura electrónica de su estado de bloqueo a su estado de desbloqueo.

Los ejemplos de realización descritos con referencia a las figuras sirven como explicación y no se han de interpretar como limitativos.

REIVINDICACIONES

1. Sistema (7) con una cerradura electrónica (9), que por introducción de un código de desbloqueo (1) de uso único, actualmente válido, puede llevarse de su estado de bloqueo a su estado de desbloqueo, así como con un dispositivo electrónico (10) dispuesto de manera separada de la cerradura (9), en donde la cerradura electrónica (9) y el dispositivo electrónico (10) están configurados para generar el código de desbloqueo (1) de uso único, actualmente válido, **caracterizado porque** el código de desbloqueo (1) de uso único, actualmente válido, se genera mediante una encriptación del código de desbloqueo (5) de uso único, válido de manera inmediatamente anterior, por medio de un algoritmo de encriptación (6), en donde la encriptación se efectúa teniendo en cuenta un código de encriptación (4), en donde la cerradura electrónica (9) y el dispositivo electrónico (10) están configurados para generar el código de encriptación (4) a partir de un código maestro individual introducido (2) y un código de clave (3) almacenado en la electrónica de la cerradura (9) e incluido en un software del dispositivo electrónico (10).

2. Sistema (7) de acuerdo con la reivindicación 1, **caracterizado porque** la cerradura electrónica (9) y el dispositivo electrónico (10) están configurados para determinar, después de la puesta en funcionamiento de la cerradura electrónica (9), el primer código de desbloqueo (1) de uso único, actualmente válido, teniendo en cuenta un código inicial individual introducido como código de desbloqueo de uso único, válido de manera inmediatamente anterior (5).

3. Sistema (7) de acuerdo con una de las reivindicaciones anteriores, **caracterizado porque** la cerradura electrónica (9) y el dispositivo electrónico (10) están configurados para usar como algoritmo de encriptación (6) AES, DES, Triple-DES, Blowfish, RC4, RC5 o RC6.

4. Sistema (7) de acuerdo con una de las reivindicaciones 1 a 3, **caracterizado porque** el código de desbloqueo (1) de uso único, actualmente válido, es generado tanto por la electrónica de la cerradura (9) como también por un software ejecutado en el dispositivo electrónico (10) y es visualizado por este dispositivo electrónico (10), en donde por medio del programa se efectúa la misma encriptación del código de desbloqueo de uso único, válido de manera inmediatamente anterior (5), que en la electrónica de la cerradura (9), específicamente teniendo en cuenta un código de encriptación (4) que se genera a partir de un código maestro individual introducido (2) y un código de clave (3) almacenado en la electrónica de la cerradura (9).

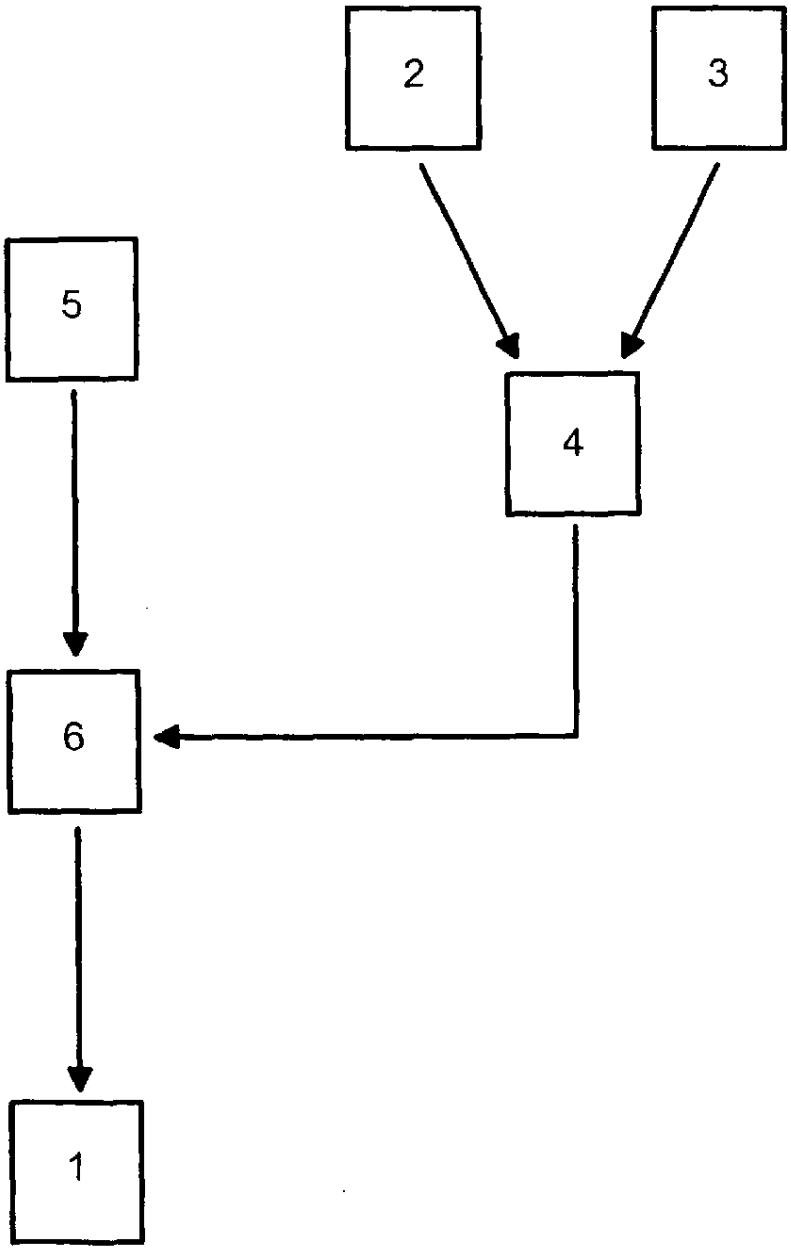

Fig. 1

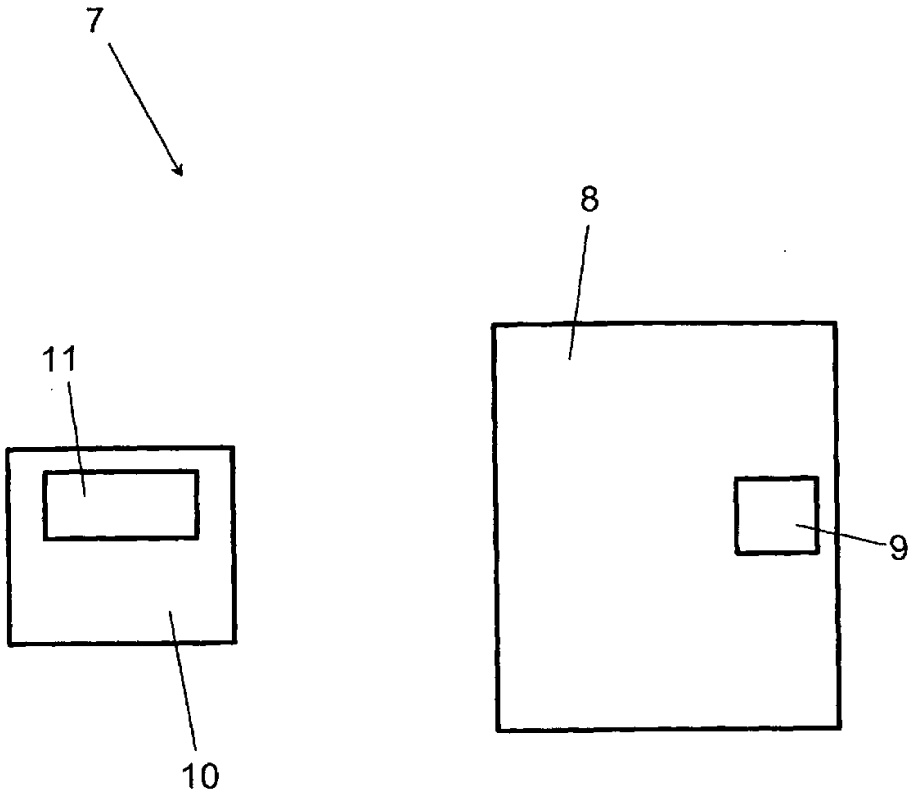

Fig. 2