Señor

JEFE DIVISIÓN DE NUEVAS CREACIONES

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

E. S. D.

REF: EXPEDIENTE: 06-79165

TITULO: "METODO Y APARATO PARA PROCESAR CRIPTOGRÁFICAMENTE DATOS"

ACTUACIÓN: RESPUESTA A EXAMEN DE PATENTABILIDAD

CARLOS ORLANDO MAYA RODRÍGUEZ, mayor de edad, vecino de esta ciudad, identificado con la Cédula de Ciudadanía No.17.117.818 expedida en Bogotá, Abogado titulado en ejercicio y portador de la Tarjeta Profesional No. 17.402 del Consejo Superior de la Judicatura, obrando en calidad de apoderado de la sociedad IVI SMART TECHNOLOGIES, INC. Según poder debidamente conferido y legalizado, adjunto al expediente de la referencia.

Encontrándome dentro del término legal comparezco para responder el oficio de Requerimiento No. 00955 del Examen de Patentabilidad emanado

COLOMBIA:
Carrera 13-A No. 28-38 Bufete 230
Tel (571) 341 9841 / Fax (571) 243 5423
Parque Central Bavaria
Bogotá D.C. / Colombia / Sur América

USA:
COL 12010 TM Tamayo
10000 NW 25 Th St Unit 1 L
33172-2204
MIAMI / FL, U.S.A.

E-mail: consultas@tmtamayo.net
ip@tmtamayo.com

Web: www.tmtamayo.com

de esa Oficina, del cual pedimos prórroga, con fundamento en el Artículo 45 de la Decisión 486 de 2.000 de C.A.N, damos respuesta en los siguientes términos.

3.- De la solicitud de Patente

3.1. Descripción

Atendiendo las sugerencias y observaciones del señor examinador, para atender lo señalado en el Artículo 28 de la Decisión 486, respecto de que la descripción continua con errores que inciden en la claridad de la invención, se ha corregido la memoria descriptiva, según lo señalado por el señor Examinador. Los términos "encriptar" y "desencriptar" y todos sus derivados han sido reemplazado por "cifrar" y "descifrar" y todos sus derivados. También se han realizado correcciones de manera de mantener congruencia con el pliego reivindicatorio, reemplazando el término "sistema".

Por lo tanto se presenta una nueva memoria descriptiva, la que está limitada dentro de la descripción inicial. Sin que en ningún momento se amplíe lo solicitado.

3.2.- Reivindicaciones

Para atender el requerimiento, según el Artículo 30 de la Decisión 486, el señor Examinador señala que: las reivindicaciones del pliego examinado son indefinidas porque no permiten establecer cual es la mejora aportada por el solicitante al estado de la técnica, porque no se divulga ni la forma de ejecutar o fabricar los aparatos o productos reclamados, se presenta:

se presenta un nuevo pliego reivindicatorio de 48 reivindicaciones, en reemplazo del anterior, pliego que está enteramente sustentado en la memoria descriptiva original y relacionadas con el pliego descriptivo que se aporta, por lo tanto no amplia el alcance de la invención.

Se han eliminado las reivindicaciones anteriores 1 a 35, todas ellas referidas a métodos, de modo de cumplimentar con el Artículo 15, literal e) de la Decisión 486. Las anteriores reivindicaciones 36 a 66 han sido modificadas, refiriéndose ahora claramente a "un dispositivo de cifrado/descifrado para procesar criptográficamente datos..."

(actuales reivindicaciones 1 a 29) . De la misma manera, las anteriores reivindicaciones 67 a 81 han sido modificadas, refiriéndose ahora claramente a "una tarjeta de cifrado/descifrado para procesar criptográficamente datos..." (actuales reivindicaciones 30 a 48). Mediante las presentes reivindicaciones, queda claro que la materia que se pretende proteger en la presente invención consiste en un "producto", o más bien, dos "productos", tangibles, relacionados por un único concepto inventivo.

Todas las reivindicaciones están caracterizadas y redactadas de manera de cumplir con lo solicitado por el Sr. Examinador, definiendo la materia allí reivindicada por sus características técnicas y la forma en que se relacionan sus componentes, por lo que ha sido adecuadamente renumeradas, y la dependencia de las mismas ha sido ajustada a dicha renumeración.

Por otra parte y según las modificaciones realizadas se hace necesario corregir el demás el título y resumen de la invención, en función de lo reivindicado en el nuevo pliego.

NUEVO TITULO:

"DISPOSITIVO DE CIFRADO / DESCIFRADO PARA PROCESAR DATOS CRIPTOGRÁFICAMENTE"

7- determinación del Estado de la Técnica.

En cuanto a las objeciones formuladas por el señor Examinador con respecto a la falta de nivel inventivo de la presente invención, el Solicitante el Solicitante respetuosamente desea reiterar lo siguiente:

- La patente US 6296164 está dirigida al desarrollo de un método de cifrado/descifrado para la transmisión segura de datos. La metodología de cifrado/descifrado en esta patente es distinta de la revelada en la publicación US2007/01540018, y además, no está claro si el método propuesto en esta patente es compatible con otros criptosistemas tales como DES, triple DES, etc.

- La US 5008216 describe un método para formar salientes de contacto para conectar los aparatos componentes del sustrato a los diseños de circuitos. Esta patente no está dirigida a la transmisión de datos o a el cifrado/descifrado de datos.

- Finalmente, la patente US 6160797 revela un sistema de transmisión por satélite, para la transmisión de paquetes

compatibles TCP/IP, desde una computadora cabecera de operaciones a través de una transmisión vía satélite, un satélite extraterrestre, un enlace a tierra satelital, y un iterador/receptor satelital integrado para la salida de paquetes compatibles TCP/IP a través de un puerto en el iterador/receptor sobre una computadora LAN o WAN. Esta patente no describe ningún método para el cifrado/descifrado de datos durante la transmisión.

Por lo tanto los documentos citados no afectan el nivel inventivo de la presente invención, cumpliendo así los requisitos de patentabilidad requeridos, más aún cunado se esta aportando:

- Nuevo Capítulo Descriptivo
- Nuevo Pliego Reivindicatorio
- Nuevo Resumen

Sin que se amplíe lo reclamado inicialmente.

De acuerdo con el nuevo capítulo descriptivo, nuevo pliego reivindicatorio y resumen anexos, la presente invención cumple con los requisitos de patentabilidad exigidos en el Art. 14 de la Decisión 486/2000 de la C.A.N, en el sentido de Novedad, Nivel inventivo y Aplicación Industrial.

TM TAMAYO
ROYALTIES · PATENTS · TRADEMARKS

Por lo antes expuesto, ruego a usted dar por subsanado dicho requerimiento realizado con fundamento en el articulo 45 de la Decisión 486, sin perjuicio de lo cual desde ya nos acogemos a lo dispuesto por el inciso segundo del artículo 45 de la decisión 486 de la Comunidad Andina de Naciones que a la letra dice: "(...) Cuando la oficina nacional competente estimare que ello es necesario para los fines del examen de patentabilidad, podrá notificar al solicitante dos o más veces (...)"

**NOTIFICACIONES**

Mi poderdante y yo recibiremos notificaciones en la Secretaría de su Despacho o en mi Oficina de Abogado ubicada en la Carrera 13A No. 28-38 Ofc. 230 MZ. 2 Parque Central Bavaria de la ciudad de Bogotá D.C.

Del señor Jefe,

CARLOS ORLANDO MAYA RODRÍGUEZ
No.17.117.818 expedida en Bogotá,
T.P No. 17.402 del C.S.J.

COLOMBIA:
Carrera 13-A No. 28-38 Bufete 230
Tel (571) 341 9841 / Fax (571) 243 5423
Parque Central Bavaria
Bogotá D.C. / Colombia / Sur América

USA:
COL 12010 TM Tamayo
10000 NW 25 Th St Unit 1 L
33172-2204
MIAMI / FL, U.S.A.

E-mail: consultas@tmtamayo.net
ip@tmtamayo.com

Web: www.tmtamayo.com

# DISPOSITIVO DE CIFRADO / DESCIFRADO PARA PROCESAR DATOS CRIPTOGRÁFICAMENTE

## Campo de la Invención

La presente invención se relaciona con la criptografía y con sistemas criptográficos. Más particularmente, la presente invención se relaciona con un método y sistema para procesar datos criptográficamente que incluyen una pluralidad de segmentos de datos.

## Antecedentes de la Invención

Numerosos métodos de cifrado y sistemas criptográficos (criptosistemas) se utilizan actualmente en diferentes campos. Por ejemplo, existen criptosistemas simétricos y criptosistemas asimétricos. La criptografía simétrica, que también se denomina criptografía de clave secreta, utiliza una única clave (clave secreta) para cifrar y descifrar información. La criptografía asimétrica, que también se denomina criptografía de clave pública, utiliza un par de claves: una (clave pública) para cifrar datos, y la otra (clave privada) para descifrarlos. Los algoritmos de cifrado que se encuentran actualmente disponibles incluyen, por ejemplo, el Estándar de Cifrado de Datos (DES) que es un algoritmo simétrico que emplea una cifra de bloqueo con una

única clave de 56 bits; el DES triple que es una forma segura de DES que utiliza una clave de 168 bits; el Algoritmo Internacional de Cifrado de Datos (IDEA) que es un algoritmo de cifrado de clave secreta en modo de bloqueo que utiliza una clave de 128 bits; el RC4 que es un algoritmo de llave simétrica ampliamente utilizado; el Estándar de Cifrado Avanzado (AES) que provee un esquema de cifrado más resistente con tres longitudes alternativas clave de 128 bits, de 192 bits o de 256 bits y similares.

Muchas empresas emplean un criptosistema simétrico para sus comunicaciones seguras, que utiliza un algoritmo de cifrado predeterminado con la clave secreta fija tal como el DES triple o el AES. Debido a la evolución continua de la tecnología basada en computadoras, los métodos de seguridad que habían parecido indestructibles se están tornando inadecuados, por ejemplo, el tamaño de la clave de 56 bits del DES ya no se considera seguro contra ataques con generadores de claves. La utilización del mismo algoritmo de cifrado y la misma clave secreta para la comunicación durante un tiempo prolongado puede aumentar el riesgo de ataques con generadores de claves contra el criptosistema. Sin embargo, el reemplazo del algoritmo de cifrado y/o de la clave secreta en un criptosistema implementado una vez es generalmente muy costoso, ya que requiere alguna forma de

intercambio seguro de clave, ya sea en persona, por correo privado, o similares, entre la totalidad de las entidades que utilizan el criptosistema, y cualquier cambio en el algoritmo o en la clave secreta debe también sincronizarse entre las entidades. Un criptosistema de algoritmo / clave fija también carece de compatibilidad con otros criptosistemas que utilizan un algoritmo de cifrado diferente y/o una clave secreta diferente.

Por consiguiente, sería deseable proveer un criptosistema que realice comunicaciones y transacciones seguras que sea menos vulnerable a los generadores de claves y otros ataques y que también tenga alta flexibilidad y compatibilidad.

## Breve Descripción de la invención

Un dispositivo de cifrado/descifrado para procesar criptográficamente datos que incluyen una pluralidad de segmentos de datos. El proceso criptográfico incluye (a) recibir una pluralidad de segmentos de datos, (b) seleccionar, para cada segmento de datos, un conjunto de información de cifrado basado en datos contenidos en una parte predeterminada del segmento de datos que se debe cifrar, y (c) cifrar cada segmento de datos utilizando el conjunto de información de cifrado seleccionado para el segmento de datos. Al menos uno entre un algoritmo de

cifrado, una clave de cifrado, y un parámetro de cifrado se puede cambiar para cada segmento de datos basado en los datos contenidos en la parte predeterminada. La parte predeterminada puede incluir una primera parte predeterminada para seleccionar un primer conjunto de información de cifrado, y una segunda parte predeterminada para seleccionar un segundo conjunto de información de cifrado; la información de cifrado incluye un algoritmo de cifrado, una clave de cifrado y optativamente un parámetro de cifrado.

De acuerdo con un aspecto de la presente invención, un dispositivo de cifrado/descifrado para cifrar datos incluye (a) recibir una pluralidad de segmentos de datos, (b1) seleccionar, para cada paquete, un primer conjunto de información de cifrado basado en los datos contenidos en una primera parte predeterminada del segmento de datos, (b2) seleccionar, para cada paquete, un segundo conjunto de información de cifrado basado en datos contenidos en una segunda parte predeterminada del segmento de datos, (c1) cifrar la segunda parte predeterminada de cada segmento de datos utilizando el primer conjunto de información de cifrado seleccionado para el segmento de datos, (c2) cifrar la parte restante de cada segmento de datos utilizando la segunda información de cifrado seleccionada para el segmento de datos, y (d) generar un segmento de datos cifrado para cada uno de los

segmentos de datos originales; el segmento de datos cifrado tiene una primera parte predeterminada, una segunda parte predeterminada y una parte restante; la primera parte predeterminada contiene los datos originales de la primera parte predeterminada correspondiente del segmento de datos original, la segunda parte predeterminada contiene los datos cifrados de la segunda parte predeterminada correspondiente del segmento de datos original, y la parte restante contiene los datos cifrados de la parte restante correspondiente del segmento de datos original.

De acuerdo con un aspecto de la presente invención, el dispositivo de cifrado/descifrado para descifrar datos incluye (a) recibir datos cifrados que incluyen una pluralidad de segmentos de datos cifrados, cada uno de los segmentos de datos cifrados tiene una primera parte predeterminada, una segunda parte predeterminada, y una parte restante; la primera parte predeterminada contiene datos originales de una primera parte predeterminada correspondiente de un segmento de datos original, la segunda parte predeterminada contiene los datos cifrados de una segunda parte predeterminada correspondiente del segmento de datos original, y la parte restante contiene los datos cifrados de la parte restante correspondiente del segmento de datos original, (b1) seleccionar, para cada segmento de datos cifrados,

un primer conjunto de información de cifrado basada en los datos originales contenidos en la primera parte predeterminada del segmento de datos cifrado, (c1) descifrar los datos cifrados contenidos en la segunda parte predeterminada de cada segmento de datos cifrado utilizando el primer conjunto de información de cifrado seleccionado para el segmento de datos cifrados, (b2) seleccionar, para cada segmento de datos cifrado, un segundo conjunto de información de cifrado basado en los datos descifrados de la segunda parte predeterminada, (c2) descifrar la parte restante de cada segmento de datos cifrado utilizando el segundo conjunto de información de cifrado seleccionado para el segmento de datos cifrados.

De acuerdo con un aspecto de la invención, un dispositivo de cifrado/descifrado para procesar datos criptográficamente incluye (a) un medio para recibir una pluralidad de segmentos de datos, (b) un medio para seleccionar, para cada segmento de datos, un conjunto de información de cifrado basado en datos contenidos en una parte predeterminada del segmento de datos que debe cifrarse, y (c) un medio para cifrar cada segmento de datos utilizando el conjunto de información de cifrado seleccionado para el segmento de datos. El medio para seleccionar puede cambiar al menos uno de los siguientes: un algoritmo de cifrado, una clave de cifrado y

un parámetro de cifrado para cada segmento de datos basado en los datos contenidos en la parte predeterminada.

De acuerdo con un aspecto de la invención, el medio para seleccionar incluye (e) un medio para generar, para cada segmento de datos, un valor a partir de los datos contenidos en la parte predeterminada del segmento de datos, y (f) un medio para seleccionar un conjunto de información de cifrado asociado con el valor generado; el juego de información de cifrado incluye un algoritmo de cifrado, una clave de cifrado, y, optativamente, un parámetro de cifrado. El medio para generar un valor puede incluir un medio para resumir los datos contenidos en la parte predeterminada utilizando una clave de verificación o clave hash[1].

De acuerdo con un aspecto de la invención, el dispositivo de cifrado/descifrado puede además incluir un medio para proveer una tabla de cifrado que contiene un identificador del tipo de cifrado, una clave de cifrado para el tipo de cifrado y un

[1] N. del T.: traducción el término en inglés "hash" pertenece al campo de la informática y que se refiere a una función o método para generar claves o llaves que representen de manera casi unívoca a un documento, registro, archivo, etc., resumir o identificar un dato a través de la probabilidad, utilizando una *función hash* o *algoritmo hash*.

parámetro de cifrado, para cada entrada asociada con un valor generado.

De acuerdo con un aspecto de la invención, la parte predeterminada incluye una primera parte predeterminada para seleccionar un primer conjunto de información de cifrado y una segunda parte predeterminada para seleccionar un segundo conjunto de información de cifrado. Cada conjunto de información de cifrado incluye un algoritmo de cifrado, una clave de cifrado y, optativamente, un parámetro de cifrado.

De acuerdo con un aspecto de la invención, el dispositivo de cifrado/descifrado puede además incluir un medio para cifrar la segunda parte predeterminada utilizando el primer conjunto de información de cifrado y un medio para cifrar la parte restante del segmento de datos utilizando el segundo conjunto de información de cifrado.

De acuerdo con un aspecto de la invención, el dispositivo de cifrado/descifrado puede incluir además un medio para generar un segmento de datos cifrado para cada segmento de datos original; el segmento de datos cifrado tiene una primera parte predeterminada, una segunda parte predeterminada y una parte restante. La primera parte predeterminada contiene los datos

originales de la primera parte predeterminada correspondiente del segmento de datos original, la segunda parte predeterminada contiene los datos cifrados de la segunda parte predeterminada correspondiente del segmento de datos original, y la parte restante contiene los datos cifrados de la parte restante correspondiente del segmento de datos original.

De acuerdo con un aspecto de la invención el dispositivo de cifrado/descifrado puede incluir además un medio para transmitir una pluralidad de segmentos de datos cifrados como una corriente de datos cifrados. El dispositivo de cifrado/descifrado puede incluir también un medio para almacenar una pluralidad de segmentos de datos cifrados en un dispositivo de almacenamiento de datos; cada segmento de datos cifrado corresponde a un sector de datos respectivo del dispositivo de almacenamiento de datos.

De acuerdo con un aspecto de la invención, el dispositivo de cifrado/descifrado puede además incluir (a) un medio para recibir los datos cifrados que incluyen una pluralidad de segmentos de datos cifrados, (b1) un medio para seleccionar, para cada segmento de datos cifrado, un primer conjunto de información de cifrado basado en los datos contenidos en la primera parte predeterminada del segmento de datos cifrado, (c1) un medio para descifrar los datos cifrados contenidos en la segunda parte predeterminada de cada segmento de datos cifrado utilizando un

primer conjunto de información de cifrado seleccionado para el segmento de datos cifrado, (b2) seleccionar, para cada segmento de datos cifrado, un segundo conjunto de información de cifrado basado en los datos descifrados de la segunda parte predeterminada, y (c2) descifrar la parte restante de cada segmento de datos cifrado utilizando el segundo conjunto de información de cifrado seleccionado para el segmento de datos cifrado.

De acuerdo con un aspecto de la invención, el medio para seleccionar la primera información de cifrado puede incluir un medio para generar un primer valor a partir de los datos originales contenidos en la primera parte predeterminada del segmento de datos cifrado. El medio para generar el primer valor puede incluir un medio para resumir los datos contenidos en la primera parte predeterminada utilizando la primera clave de verificación.

De acuerdo con un aspecto de la invención, el medio para seleccionar la segunda información de cifrado puede incluir un medio para generar un segundo valor a partir de los datos descifrados de la segunda parte predeterminada del segmento de datos cifrado. El medio para generar el segundo valor puede

incluir un medio para resumir los datos descifrados de la segunda parte predeterminada utilizando una clave hash.

De acuerdo con un aspecto de la invención, el dispositivo de cifrado/descifrado para descifrar datos incluye (a) un medio para recibir una pluralidad de segmentos de datos cifrados; cada uno de los segmentos de datos cifrados tiene una parte predeterminada, (b) un medio para seleccionar, para cada segmento de datos cifrado, un conjunto de información de cifrado basado en los datos contenidos en la parte predeterminada del segmento de datos cifrado, y (c) un medio para descifrar cada segmento de datos cifrado utilizando la información de cifrado seleccionada para el segmento de datos cifrado.

De acuerdo con un aspecto de la invención, el medio para seleccionar puede incluir un medio para generar, para cada segmento de datos cifrado, un valor a partir de los datos contenidos en la parte predeterminada del segmento de datos cifrado, y un medio para seleccionar un conjunto de información de cifrado asociado con el valor generado; el conjunto de información de cifrado incluye un algoritmo de cifrado, una clave de cifrado y, optativamente, un parámetro de cifrado. El medio para generar un valor puede incluir un medio para verificar los

datos contenidos en la parte predeterminada utilizando una clave hash.

De acuerdo con un aspecto de la invención, el dispositivo puede incluir además un medio para proveer un identificador de tipo de cifrado, una clave de cifrado para el tipo de cifrado y un parámetro de cifrado asociado con un valor generado.

De acuerdo con un aspecto de la invención, la parte predeterminada puede incluir una primera parte predeterminada para seleccionar un primer juego de información de cifrado, y una segunda parte predeterminada para seleccionar un segundo juego de información de cifrado. Cada juego de información de cifrado puede incluir un algoritmo de cifrado, una clave de cifrado y, optativamente, un parámetro de cifrado.

De acuerdo con un aspecto de la invención, la primera parte predeterminada contiene datos para una primera capa de protocolo, y la segunda parte predeterminada contiene datos para una segunda capa de protocolo, en donde la primera capa de protocolo es inferior a la segunda capa de protocolo. La primera parte predeterminada puede ser un encabezamiento de Protocolo de Internet (IP) del paquete de datos. La segunda parte predeterminada puede ser una parte seleccionada de un campo de datos, un encabezamiento de Protocolo de Control de Transmisión (TCP), o un encabezamiento de Protocolo de Diagrama de Datos de Usuario (UDP) del paquete de datos.

De acuerdo con un aspecto de la invención, la primera parte predeterminada es una primera parte seleccionada en un sector en un dispositivo de almacenamiento de datos, y la segunda parte predeterminada es una segunda parte seleccionada en el sector.

De acuerdo con un aspecto de la invención, los datos contenidos en la segunda parte predeterminada de un segmento de datos cifrado se ha cifrado mediante el uso del primer conjunto de información de cifrado, y los datos contenidos en la parte restante del segmento de datos cifrado se ha cifrado mediante el uso del segundo conjunto de información de cifrado.

## Breve Descripción de los Dibujos

Los dibujos adjuntos, que se incorporan y forman parte de esta memoria descriptiva, ilustran una o más realizaciones de la presente invención y, junto con la descripción detallada, sirven para explicar los principios y las implementaciones de la invención.

En los dibujos:

La Figura 1A es un diagrama de bloques que ilustra esquemáticamente una parte de cifrado de un dispositivo de

cifrado/descifrado para cifrar/descifrar datos de acuerdo con una realización de la presente invención.

La Figura 1B es un diagrama de bloques que ilustra esquemáticamente una parte de descifrado de un dispositivo de cifrado/descifrado para cifrar/descifrar datos de acuerdo con una realización de la presente invención.

La Figura 2 es un diagrama que ilustra esquemáticamente un ejemplo de la tabla de cifrado de acuerdo con una realización de la presente invención.

La Figura 3 es un diagrama de flujo de proceso que ilustra esquemáticamente un método para cifrar/descifrar datos de acuerdo con una realización de la presente invención.

La Figura 4 es un diagrama que ilustra esquemáticamente un ejemplo de un paquete de datos en el cual la primera parte predeterminada es un encabezamiento de Protocolo de Internet (IP), y la segunda parte predeterminada es un encabezamiento de Protocolo de Control de Transmisión (TCP).

La Figura 5 es un diagrama que ilustra esquemáticamente un ejemplo de un paquete de datos en donde la primera parte

predeterminada es un encabezamiento de Protocolo de Internet (IP), y la segunda parte predeterminada es un encabezamiento de Protocolo de Diagrama de Datos de Usuario (UDP).

La Figura 6 es un diagrama que ilustra esquemáticamente un ejemplo de un paquete de datos en el cual la primera parte predeterminada es un encabezamiento de Protocolo de Internet (IP) y la segunda parte predeterminada es una parte seleccionada de un campo de datos.

La Figura 7 es un diagrama que ilustra esquemáticamente un ejemplo de la primera y segunda partes predeterminadas en un sector de un dispositivo de almacenamiento de datos.

La Figura 8 es un diagrama que ilustra esquemáticamente un ejemplo de una primera y segunda partes predeterminadas en un segmento de datos almacenado en una tarjeta de memoria en la cual el segmento de datos corresponde a los datos almacenados en cada dirección.

La Figura 9 es un diagrama de flujo de proceso que ilustra esquemáticamente un método para cifrar datos de acuerdo con una realización de la presente invención, en donde la parte

predeterminada incluye una primera parte predeterminada y una segunda parte predeterminada.

La Figura 10 es un diagrama que ilustra esquemáticamente un ejemplo de cifrado de un paquete de datos mediante la utilización del método que se muestra en la Figura 9.

La Figura 11 es un diagrama de flujo de proceso que ilustra esquemáticamente un método para descifrar datos cifrados de acuerdo con una realización de la presente invención, en donde la parte predeterminada incluye una primera parte predeterminada y una segunda parte predeterminada.

La Figura 12 es un diagrama que ilustra esquemáticamente un ejemplo de descifrado de un paquete de datos mediante el método que se muestra en la Figura 11.

La Figura 13 es un diagrama de bloques que ilustra esquemáticamente un cifrador/descifrador de datos de acuerdo con una realización de la presente invención.

La Figura 14 es un diagrama que ilustra esquemáticamente un ejemplo de aplicación del dispositivo de cifrado/descifrado para

asegurar comunicaciones a través de la Internet de acuerdo con una realización de la presente invención.

## Descripción Detallada

Las realizaciones de la presente invención se describen aquí en el contexto de un dispositivo de cifrado/descifrado para cifrar y descifrar datos que incluyen una pluralidad de segmentos de datos. Los expertos en el arte advertirán que la siguiente descripción detallada de la presente invención es sólo ilustrativa y no está destinada a ser taxativa de ningún modo. Otras realizaciones de la presente invención surgirán rápidamente para los expertos en el arte que cuenten con el beneficio de esta divulgación. A continuación, se hace referencia en detalle a implementaciones de la presente invención que se ilustran en los dibujos adjuntos. Se utilizan los mismos indicadores de referencia en todos los dibujos y en la siguiente descripción detallada para hacer referencia a las mismas partes o a partes iguales.

A efectos de mantener la claridad, no se muestran y describen todas las características habituales de las implementaciones que se describen en la presente. Naturalmente, se apreciará que en el desarrollo de cualquiera de esas implementaciones, se deberán

tomar numerosas decisiones específicas sobre la implementación para alcanzar las metas específicas del desarrollador, tales como el cumplimiento de las limitaciones relacionadas con la aplicación y la actividad comercial, y que estas metas específicas varían de una implementación a otra y de un desarrollador a otro. Más aún, se apreciará que ese esfuerzo de desarrollo podría ser complejo y consumir tiempo, pero de todos modos constituiría una tarea habitual de ingeniería para los expertos en el arte que cuentan con el beneficio de esta divulgación.

De acuerdo con una realización de la presente invención, los componentes, pasos de proceso, y/o estructuras de datos pueden implementarse a través del uso diferentes tipos de dispositivos cableados, dispositivos lógicos programables de campo (FPLD), que incluyen arreglos de compuerta programables por el usuario (FPGA) y dispositivos lógicos programables complejos (CPLD), circuitos integrados de aplicación específica (ASIC) o similares, también se pueden utilizar sin apartarse del alcance y espíritu de los conceptos inventivos que se divulgan en la presente.

En el contexto de la presente invención, el término "red" incluye redes de área local (LANs), redes de área amplia (WAN), la Internet, sistemas de televisión por cable, sistemas telefónicos,

sistemas de telecomunicaciones inalámbricas, redes de fibra óptica, redes de modo de transferencia asíncrona (ATM), redes de conmutación de tramas, sistemas de comunicaciones satelitales, y similares. Esas redes son conocidas en el arte y en consecuencia no se describen adicionalmente aquí.

La Figura 1A ilustra esquemáticamente un sistema 10 para cifrar/descifrar datos de acuerdo con una realización de la presente invención. Como se muestra en la Figura 1 A, el sistema 10 incluye un buffer de entrada 12, un módulo de cifrado 14, un controlador 16 conectado al buffer de entrada 12 y al módulo de cifrado 14, y un buffer de salida 18 conectado al controlador 16 y al módulo de cifrado 14. El buffer de entrada 12 está adaptado para recibir datos que incluyen una pluralidad de segmentos de datos. Por ejemplo, esos datos pueden ser una corriente de datos que incluyen una pluralidad de paquetes de datos. Los segmentos de datos pueden también leerse desde sectores correspondientes de un medio de grabación o un dispositivo de almacenamiento de datos tal como un disco rígido, un CD ROM, un DVD, una tarjeta de memoria y similares. El módulo de cifrado 14 está adaptado para cifrar cada segmento de datos. El buffer de salida 18 separa los segmentos de datos cifrados del módulo de cifrado 14, y hace salir los datos cifrados que incluyen una pluralidad de segmentos de datos.

Por ejemplo, como se muestra en la Figura 1 A, el sistema 10 puede utilizarse entre un puerto de bus serial universal (USB) 11 y un puerto Ethernet 13, en aquel caso en que una computadora huésped se comunique a través de una LAN. El sistema 10 también se puede utilizar para comunicaciones seguras a través de la WAN, la Internet, red inalámbrica, y similares. Más aún, el sistema 10 puede utilizarse con una interfaz pequeña de sistemas de computadoras (SCSI), una interfaz de electrónica de unidades integradas/inteligentes (IDE), una interfaz de IDE mejorada, y similares, para almacenar datos seguros en dispositivos de almacenamiento masivo. El dispositivo también puede utilizarse para el otro tipo de transferencia digital de datos.

El controlador 16 está adaptado para seleccionar un conjunto de información de cifrado para cada segmento de datos basado en datos contenidos en una parte predeterminada del segmento de datos que debe cifrarse. Por ejemplo, la información de cifrado incluye un algoritmo de cifrado, una clave de cifrado, y un parámetro de cifrado tal como un vector inicial. El parámetro de cifrado puede utilizarse para establecer o iniciar el proceso de cifrado en un estado específico. Dado que la información de cifrado se selecciona basada en datos en una parte específica del segmento de datos que debe cifrarse, generalmente, al menos uno

del algoritmo de cifrado, la clave de cifrado, y el parámetro de cifrado se cambia para cada segmento de datos. En otras palabras, la información de cifrado se "autodetermina" para cada segmento de datos mediante la utilización de los datos contenidos en el segmento de datos en sí mismo. La parte predeterminada del segmento de datos puede ser un encabezamiento de cada paquete de datos, una parte seleccionada del campo de datos del paquete de datos; por ejemplo, una longitud específica de datos que empieza a un número predeterminado de bytes desde el comienzo del campo de datos. La parte predeterminada puede ser una parte seleccionada de un sector en un dispositivo de almacenamiento de datos, un campo de número o dirección de sector de cada sector en un dispositivo de almacenamiento de datos, y similares.

El módulo de cifrado 14 incluye una pluralidad de motores de cifrado 20 (20a, 20b, 20c...), cada uno corresponde a un algoritmo de cifrado que debe seleccionar el controlador 16. El módulo de cifrado 14 puede incluir además un buffer de datos 22 conectado a cada uno de la pluralidad de los motores de cifrado 20.

De acuerdo con una realización de la presente invención, que se muestra en la Figura 1A, el controlador 16 incluye un selector de datos 24, un selector de cifrado 26 conectado con el selector de

datos 24 y un controlador de cifrado 28. El selector de datos 24 está adaptado para seleccionar la parte predeterminada de cada segmento de datos. El selector de cifrado 26 está adaptado para seleccionar un conjunto de información de cifrado de acuerdo con datos contenidos en la parte predeterminada seleccionada por el selector de datos 24. El conjunto de información de cifrado incluye, por ejemplo, un algoritmo de cifrado, una clave de cifrado y, optativamente, un parámetro de cifrado. El controlador de cifrado 28 está adaptado para seleccionar y activar uno de los motores de cifrado 20 basado en la información de cifrado. Por ejemplo, si el selector de cifrado 26 selecciona un algoritmo de cifrado A, el controlador de cifrado 28 selecciona un motor de cifrado correspondiente (A) 20a y activa o inicia el motor de cifrado 20a a través de la utilización de los parámetros de cifrado. Los datos se cifran con el motor de cifrado 20a a través del uso de la clave seleccionada. Nótese que una clave diferente y/o un parámetro de cifrado diferente dan como resultado datos cifrados diferentes, aún cuando se utilice el mismo algoritmo de cifrado y por lo tanto el mismo motor de cifrado.

De acuerdo con una realización de la presente invención, el controlador 16 incluye además un generador de valor 30 conectado al selector de datos 24. El generador de valor está adaptado para generar un valor a partir de los datos contenidos en la parte

predeterminada. Por ejemplo, el generador de valor 30 puede incluir una función hash y verificar los datos mediante el uso de una clave hash para producir el valor. La clave *hash* puede preinstalarse en el generador de valor 30, o puede seleccionarse cuando el controlador 16 se programa por primera vez.

De acuerdo con una realización de la presente invención, el controlador de cifrado 26 incluye una tabla de cifrado 32. La tabla de cifrado 32 contiene un identificador de tipo de cifrado, una clave de cifrado para el tipo de cifrado, y un parámetro de cifrado tal como un vector inicial que especifica un estado de cifrado inicial del motor de cifrado, para cada entrada asociada con un valor generado por el generador de valor 30. La Figura 2 ilustra esquemáticamente un ejemplo de la tabla de cifrado 32. Como se muestra en la Figura 2, cada entrada de la tabla de cifrado 32 tiene un índice que corresponde al valor generado, por ejemplo, un valor hash, y un conjunto correspondiente de un algoritmo de cifrado (tipo de cifrado), una clave para el algoritmo de cifrado, y un vector inicial (parámetro de cifrado). El número de las entradas depende del valor generado desde la parte predeterminada. En una realización de la presente invención, una tabla de cifrado tiene 1000 entradas. Generalmente, se obtiene un valor de índice diferente de la parte predeterminada de un segmento de datos diferentes, y por lo tanto

cada segmento de datos se cifra mediante el uso de una información de cifrado diferente.

La descripción precedente es con respecto a la parte de cifrado del sistema 10. La Figura 1B ilustra esquemáticamente una parte de descifrado correspondiente 10' del sistema 10 de acuerdo con una realización de la presente invención. Como se muestra en la Figura 1B, la parte de descifrado 10' puede construirse simétricamente con respecto a la parte de cifrado (Figura 1A) del sistema 10, que incluye los motores de descifrado 20a', 20b' y 20c' en lugar de los motores de cifrado 20a, 20b y 20c, como bien lo entiende un experto en el arte sin necesidad de mayores explicaciones.

La Figura 3 ilustra esquemáticamente un método para cifrar / descifrar datos de acuerdo con una realización de la presente invención. El sistema de cifrado / descifrado 10 puede ejecutar el método. Se recibe una pluralidad de segmentos de datos, por ejemplo, al recibir una corriente de datos que incluyen una pluralidad de paquetes de datos, o leer desde un dispositivo de almacenamiento de datos que incluyen una pluralidad de sectores o direcciones de datos. Los segmentos de datos recibidos se almacenan en forma intermedia mediante un buffer de entrada. Los segmentos de datos se cifran segmento por segmento. Como se

muestra en la Figura 3, se recibe cada segmento de datos (100), y se selecciona una parte predeterminada de cada segmento de datos (102), y se selecciona un conjunto de información de cifrado según los datos contenidos en la parte predeterminada del segmento de datos que debe cifrarse (104). El segmento de datos se cifra mediante la utilización del conjunto de información de cifrado seleccionado (106). El segmento de datos siguiente se procesa de la misma forma hasta que se procesan todos los segmentos de datos del buffer de entrada (108). El conjunto de información de cifrado puede incluir un algoritmo de cifrado, una clave de cifrado y, optativamente, un parámetro de cifrado, como se describió anteriormente, y generalmente al menos uno del algoritmo de cifrado, la clave de cifrado y el parámetro de cifrado se cambian para cada segmento de datos basado en los datos contenidos en la parte predeterminada.

Como se estableció anteriormente, al seleccionar la información de cifrado, se puede generar un valor (tal como un valor hash) a partir de los datos contenidos en la parte predeterminada del segmento de datos, y el conjunto de información de cifrado se puede seleccionar mediante el uso del valor generado. El conjunto de información de cifrado puede proveerse en forma de una tabla de cifrado tal como la tabla de cifrado 32 (Figura 2) descrita anteriormente.

De acuerdo con una realización de la presente invención, la parte predeterminada incluye una primera parte predeterminada y una segunda parte predeterminada. En el caso en que el segmento de datos sea un paquete de datos, la primera parte predeterminada puede contener datos para una primera capa de protocolo, y la segunda parte predeterminada puede contener datos para una segunda capa de protocolo que es superior a la primera capa de protocolo en la jerarquía de protocolo. La primera capa de protocolo puede ser la capa de red (o capa de Internet) y la segunda capa de protocolo puede ser la capa de Transporte.

La Figura 4 ilustra esquemáticamente un ejemplo de un paquete de datos 34 en el cual la primera parte predeterminada es un encabezamiento de Protocolo de Internet (IP) 36, y la segunda parte predeterminada es un encabezamiento de Protocolo de Control de Transmisión (TCP) 38 del paquete de datos 34. La Figura 5 ilustra esquemáticamente un ejemplo de un paquete de datos 40 en el cual la primera parte predeterminada es un encabezamiento de Protocolo de Internet (IP) 36, y la segunda parte predeterminada es un encabezamiento de Protocolo de Diagrama de Datos de Usuario (UDP) 42 del paquete de datos 40. Se debe señalar que aunque el encabezamiento de IP 36, el encabezamiento de TCP 38, y el campo de datos de TCP posterior 44 se ilustran por separado en la

Figura 4, son contiguos en el paquete de datos 34. En forma similar, aunque el encabezamiento de IP 36, el encabezamiento de UDP 38, y el campo de datos de UDP posterior 46 se ilustran por separado en la Figura 5, son contiguos en el paquete de datos 40. Además, la información ilustrada en cada encabezamiento es a modo de ejemplo, y no taxativo de ningún modo. La totalidad de la información del encabezamiento puede utilizarse para obtener un valor (*hash*), o alguna parte de la información puede seleccionarse para generar un valor.

De acuerdo con una realización de la presente invención, la segunda parte predeterminada no se limita a un encabezamiento de TCP o de UDP, sino que puede seleccionarse de un campo de datos. La Figura 6 ilustra esquemáticamente un ejemplo de un paquete de datos 48 en el cual la primera parte predeterminada es un encabezamiento de Protocolo de Internet (IP) 36, y la segunda parte predeterminada de una parte seleccionada 52 (52a, 52b y 52c) del campo de datos 50 del paquete de datos 48. Como se muestra en la Figura 6, la parte seleccionada 52 puede dividirse y distribuirse en el campo de datos 50, y especificarse mediante un número predeterminado de bytes desde el comienzo del campo de datos 50 y una longitud de datos predeterminada. Se puede seleccionar una sola parte.

De acuerdo con una realización de la presente invención, los segmentos de datos pueden ser sectores en un dispositivo de almacenamiento tal como un disco rígido, un CD ROM, un DVD, una tarjeta de memoria u otro dispositivo de almacenamiento en masa. En este caso, la primera parte predeterminada es una primera parte seleccionada en un sector en un dispositivo de almacenamiento de datos, y la segunda parte de datos es una segunda parte seleccionada en el sector. La Figura 7 ilustra esquemáticamente ese ejemplo. En la Figura 7, la primera parte predeterminada es una primera parte seleccionada 56 en un sector 54 en un dispositivo de almacenamiento de datos, y la segunda parte predeterminada es una segunda parte seleccionada 58 (58a, 58b) en el sector 54. La Figura 8 ilustra esquemáticamente un ejemplo de una tarjeta de memoria en la cual el segmento de datos corresponde a datos almacenados en cada dirección. En ese caso, los datos pueden cifrarse dirección por dirección, y la primera parte predeterminada es una primera parte seleccionada 62 (62a, 63b) en una dirección de memoria 60, y la segunda parte predeterminada es una segunda parte seleccionada 64 en la dirección 60. Como se muestra en las Figuras 7 y 8, la primera y/o la segunda parte predeterminada pueden dividirse y distribuirse en el sector o datos en la dirección de memoria, o puede ser una sola parte.

La Figura 9 ilustra esquemáticamente un método para cifrar datos de acuerdo con una realización de la presente invención, en donde la parte predeterminada incluye una primera parte predeterminada y una segunda parte predeterminada, como se describió anteriormente. La Figura 10 ilustra esquemáticamente un ejemplo de cifrar un paquete de datos 70 mediante el método que se muestra en la Figura 9, donde el paquete de datos 70 incluye una primera parte predeterminada 72 (tal como un encabezamiento de IP) y una segunda parte predeterminada 74 (tal como un encabezamiento de TCP o una parte seleccionada del campo de datos).

Como se muestra en la Figura 9, para cada segmento de datos recibido (110), la primera parte predeterminada y la segunda parte predeterminada se seleccionan (112, 114). También con referencia a la Figura 10, la primera información de cifrado 78 se selecciona basada en los datos contenidos en la primera parte predeterminada 72 (116). Como se expuso anteriormente, esta selección 116 puede incluir, por ejemplo, obtener un valor hash a partir de la primera parte predeterminada 72 y seleccionar la primera información de cifrado mediante el uso de una tabla de cifrado que asocia el valor hash con un conjunto de información de cifrado respectivo. En forma similar, la segunda información de cifrado 79 se selecciona basada en los datos contenidos en la

segunda parte predeterminada 74 (118). Esta selección 118 puede incluir también, por ejemplo, obtener un valor hash a partir de una segunda parte predeterminada 74 y seleccionar la segunda información de cifrado mediante el uso de una tabla de cifrado que asocia el valor hash con un conjunto de información de cifrado respectivo. Una clave hash respectiva y una tabla de cifrado respectiva pueden proporcionarse para cada uno del proceso de selección 116 y 118 Por ejemplo, el controlador 16 del sistema de cifrado/descifrado 10 (Figura 1) puede incluir un primer conjunto de clave hash y la tabla de cifrado para la primera parte predeterminada, y un segundo conjunto de la clave hash y la tabla de cifrado para la segunda parte predeterminada.

Luego, la segunda parte predeterminada 74 se cifra mediante el uso de la primera información de cifrado 78 (120), y la parte restante del segmento de datos 76 se cifra mediante el uso de la segunda información de cifrado 79 (122). La parte restante 76 es la totalidad de los datos restantes en el segmento de datos diferente de la primera y segunda partes predeterminadas. Como se muestra en la Figura 10, la primera predeterminada 82 que contiene los datos originales (también denominada "texto claro"), la segunda parte predeterminada 84 que contiene datos cifrados (también denominada "texto cifrado") y la parte restante 86 que contiene datos cifrados se combinan para generar un segmento de

datos cifrado (paquete) 80 que corresponde al segmento de datos original (paquete) 70 (124). Por ejemplo, con referencia a la Figura 1, la segunda parte predeterminada puede cifrarse mediante el uso del motor de cifrado 20a, y la parte restante puede cifrarse mediante el uso del motor de cifrado 20b, y los datos cifrados respectivos se combinan con la primera parte predeterminada en el segmento de datos cifrado en el buffer de datos 22, y se envían al buffer de salida 18.

Los procesos 110 a 124 se ejecutan hasta que se cifra la totalidad de los segmentos de datos (126). Se debe señalar que los procesos de selección y cifrado se controlan de manera tal que la segunda información de cifrado 79 se selecciona antes de que los datos contenidos en la segunda parte predeterminada 74 se cifren, y los datos de texto claro para la primera parte predeterminada 84, el texto cifrado para la segunda parte predeterminada 84, y el texto cifrado para la parte restante 86 se envían al buffer de datos 22 en este orden.

Los segmentos de datos cifrados pueden transmitirse como una corriente de datos cifrada para la comunicación segura de datos, o pueden almacenarse en un dispositivo de almacenamiento de datos para impedir, por ejemplo, que la información sensible o protegida sea leída por una persona no autorizada.

La Figura 11 ilustra esquemáticamente un método para descifrar datos cifrados de acuerdo con una realización de la presente invención, en donde la parte predeterminada incluye una primera parte predeterminada y una segunda parte predeterminada. La Figura 12 ilustra esquemáticamente un ejemplo de descifrado de un paquete de datos cifrado 80 mediante el eso del método de la Figura 11, donde el paquete de datos cifrado 80 incluye una primera parte predeterminada 82 (tal como un encabezamiento de IP) y una segunda parte predeterminada 84 (tal como un encabezamiento de TCP o una parte seleccionada del campo de datos). Como se describió anteriormente, la primera parte predeterminada 82 contiene texto claro, y la segunda parte predeterminada y la parte restante 86 contienen texto cifrado.

Como se muestra en la Figura 11, para cada segmento de datos cifrado recibido (130), la primera parte predeterminada y la segunda parte predeterminada se seleccionan (132, 134). Los segmentos de datos cifrados pueden recibirse como una corriente de datos cifrada en una comunicación segura, o puede leerse desde un dispositivo de almacenamiento de datos. También con referencia a la Figura 12, la primera información de cifrado 88 se selecciona basado en los datos contenidos en la primera parte predeterminada 82 (136). En forma similar al proceso de cifrado

expuesto precedentemente, esta selección 136 puede incluir, por ejemplo, obtener un valor hash de la primera parte predeterminada 82 y seleccionar la primera información de cifrado mediante el uso de una tabla de cifrado que asocia el valor hash con un conjunto de información de cifrado respectivo. Dado que la primera parte predeterminada contiene el texto claro, la primera información de cifrado es la misma que el segmento de datos original.

Luego, la segunda parte predeterminada 84, que contiene el texto cifrado, se descifra mediante el uso de la primera información de cifrado 88 (138). La segunda información de cifrado 89 se selecciona basado en los datos descifrados 85 contenidos en la segunda parte predeterminada 84 (140). Esta selección 138 puede incluir también, por ejemplo, obtener un valor hash de los datos descifrados 85 y seleccionar la segunda información de cifrado 89 mediante el uso de una tabla de cifrado que asocia el valor hash con un conjunto de información de cifrado respectivo. Una clave hash respectiva y una tabla de cifrado respectiva pueden proporcionarse para cada uno de los procesos de selección 136 y 138.

Luego, la parte restante 86 del segmento de datos se descifra mediante el uso de la segunda información de cifrado 89 (142). La

parte restante 86 es la totalidad de los datos restantes del segmento de datos diferente de la primera y segunda partes predeterminadas. La primera parte predeterminada 92, la segunda parte predeterminada 94 y la parte restante 96 se combinan para generar un segmento de datos descifrados (paquete) 90 que es el mismo que el segmento de datos original (paquete) 70 (144). Los procesos 130 a 144 se ejecutan hasta que la totalidad de los segmentos de datos se han descifrado (146).

La Figura 13 ilustra esquemáticamente un cifrador/descifrador 150 de acuerdo con una realización de la presente invención. Como se muestra en la Figura 13, el cifrador/descifrador de datos incluye una parte transmisora 152 y una parte receptora 162. La parte transmisora 152 incluye un primer analizador temporizador 154, un módulo de cifrado (T) 156, y un primer buffer de datos 158. En forma similar, la parte receptora 162 incluye un segundo analizador temporizador 164, un módulo de descifrado (R) 166, y un segundo buffer de datos 168. El módulo de cifrado 156 puede ser la parte de cifrado del dispositivo de cifrado/descifrado 10 (módulo de cifrado 14 y el controlador 16) descrito anteriormente, y el módulo de descifrado 166 puede ser la parte de cifrado 10' del dispositivo de cifrado/descifrado 10 descrito anteriormente. En la parte transmisora, por ejemplo, el buffer de entrada 12 (en la Figura 1A) puede integrarse dentro del

analizador temporizador 154 de acuerdo con una implementación específica. El buffer de salida 18 (en la Figura 1A) también puede estar integrado dentro del buffer de datos 158 de acuerdo con la implementación específica. Lo mismo se aplica a la parte receptora 154.

Dado que el cifrador/descifrador de datos 150 generalmente transmite y recibe una corriente de datos (Tx y Rx), los analizadores temporizadores 154 y 164 sincronizan los procesos de cifrado/descifrado para la corriente de datos correspondiente de manera tal que los datos cifrados/descifrados se combinan correctamente en los respectivos segmentos de datos cifrados/descifrados (paquetes de datos) y se envían a los buffers de datos 158 y 168 y salen de ellos, respectivamente.

De acuerdo con una realización de la presente invención, el cifrador/descifrador de datos 150 (y el dispositivo de cifrado/descifrado 10) puede implementarse en una forma de tarjeta que se inserta en una computadora. Dado que la totalidad de los componentes necesarios para el cifrado/descifrado se proveen en el cifrador/descifrador (tarjeta de cifrado/descifrado), el usuario/computadora no tiene que instalar ningún programa de software específico para el cifrado/descifrado siempre que la computadora pueda utilizar la tarjeta de

cifrado/descifrado (es decir, que el puerto sea compatible). Simplemente almacenándola transmitir o almacenar datos a través de la tarjeta de cifrado/descifrado, los datos se cifran automáticamente y por lo tanto se transmiten a través de una red en forma segura o se almacenan en un dispositivo de almacenamiento en forma segura. La misma tarjeta de cifrado/descifrado puede utilizarse para recibir datos transmitidos o leer los datos almacenados en forma segura.

Para recibir o leer los datos cifrados, se debe usar la misma tarjeta o dispositivo de cifrado/descifrado para descifrar los datos cifrados. La "mismo" significa que la tarjeta o dispositivo es capaz de seleccionar las mismas primera y segunda parte predeterminadas de los segmentos de datos y seleccionar/obtener la misma primera y segunda información de cifrado si los datos contenidos en la parte predeterminada son los mismos. Generalmente, por ejemplo, las tarjetas de cifrado/descifrado correspondientes (comunicadoras) tienen claves hash y tablas de cifrado idénticas.

De acuerdo con una realización de la presente invención, la parte del módulo de cifrado/descifrado 170 (en la Figura 13) puede personalizarse de acuerdo con el pedido del usuario en el momento de la fabricación o de la programación inicial. Por ejemplo, dado

que la tarjeta de cifrado/descifrado puede implementarse en dispositivos lógicos programables de campo (FPLD), tales como FPGA y CPLD, la tarjeta o dispositivo de cifrado/descifrado puede programarse de acuerdo con las especificaciones del usuario (por ejemplo, el nivel de seguridad, la velocidad de transmisión, el protocolo o estándar requerido, el medio de almacenamiento específico y/o formato que debe utilizarse, etc.) con configuraciones específicas de las claves hash y las tablas de cifrado (información de cifrado).

Además, el usuario y la computadora no tienen que conocer las configuraciones, y el usuario y la computadora no tienen acceso a las configuraciones, no se puede robar esa información al usuario o a la computadora para "desbloquear el código". Más aún, el algoritmo de cifrado, la clave de cifrado y, optativamente, el parámetro de cifrado se cambian prácticamente para todos los segmentos de datos, y cuyo algoritmo, clave y parámetro que deben utilizarse son solamente "conocidos" por el segmento de datos que debe cifrarse. Dado que el algoritmo, clave y/o parámetro de cifrado se cambian automáticamente en base a ciertos datos contenidos en el segmento de datos en sí, la sincronización entre el lado transmisor y el lado receptor es innecesaria.

La Figura 14 ilustra esquemáticamente un ejemplo de aplicación de la presente invención para hace más segura la comunicación a través de Internet. Como se muestra en la Figura 14, los usuarios 180, 182, 184 pueden utilizar métodos de cifrado/descifrado respectivos 190, 192 y 194 de acuerdo con una realización de la presente invención. Los métodos de cifrado/descifrado 190, 192 y 194 pueden ser el método de cifrado/descifrado 10 o el cifrador/descifrador 150 que se describieron anteriormente. La totalidad de los sistemas de cifrado/descifrado 190, 192 y 194 se programan idénticamente y se proveen de las mismas configuraciones, por ejemplo, las mismas claves hash y tablas de cifrado. Como se muestra en la Figura 14, el método de cifrado/descifrado puede ser utilizado por más de una computadora 184 y 186. Por ejemplo, el método de cifrado/descifrado 194 puede utilizarse con un eje dentro de una LAN de manera tal que todas las transmisiones de datos desde las computadoras o el servidor conectados al eje se cifran.

De acuerdo con una realización de la presente invención, dado que el encabezamiento de IP de cada paquete de datos no se cifra, el esquema de cifrado/descifrado de una realización de la presente invención no afecta el enrutamiento o conmutación de los paquetes de datos a través de Internet u otras redes (es decir, operaciones en la capa de protocolo de red). Además, en el caso

en que algunos enrutadores pueden buscar en un campo de paquete diferente del encabezamiento de IP en la operación de enrutamiento, la primera parte predeterminada puede seleccionarse de manera tal que incluye el encabezamiento de IP y aquella parte del campo de datos que deben utilizar los enrutadores.

De acuerdo con una realización de la presente invención, como se describió anteriormente, cada segmento de datos se cifra mediante cifrado de dos niveles. Es decir, el segmento de datos diferente de la primera y segunda partes predeterminadas se cifra mediante el uso de la información contenida en la segunda parte predeterminada. Luego, la segunda parte predeterminada se cifra mediante el uso de la información contenida en la primera parte predeterminada. Por lo tanto, aunque la primera parte predeterminada contiene texto claro, la segunda parte predeterminada que contiene datos cifrados (texto cifrado) provee un nivel de seguridad adicional, ya que la segunda parte predeterminada y la parte restante se cifran generalmente mediante un algoritmo de cifrado diferente, una clave de cifrado diferente y/o un parámetro de cifrado diferente. Además, dado que el algoritmo de cifrado, la clave de cifrado, y/o el parámetro de cifrado se cambian para todos los segmentos de datos, es prácticamente imposible para un pirata informático desbloquear el código.

Si bien se han mostrado y descrito realizaciones y aplicaciones de esta invención, sería evidente para los expertos en el arte que tienen el beneficio de esta divulgación que muchas más modificaciones que las mencionadas anteriormente son posibles sin apartarse de los conceptos de la invención de la presente. La invención, en consecuencia, no debe restringirse excepto en el espíritu de las reivindicaciones anexas.

RESUMEN

Un dispositivo de cifrado/descifrado para procesar datos en forma criptográfica que incluye una pluralidad de segmentos de datos. El proceso criptográfico incluye (a) recibir una pluralidad de segmentos de datos (100), (b) seleccionar, para cada segmento de datos, un conjunto de información de cifrado en base a los datos contenidos en una parte predeterminada del segmento de datos que debe cifrarse (102, 104) y (c) cifrar dicho segmento de datos mediante el uso de un conjunto de información de cifrado que se selecciona para el segmento de datos (106). Al menos un algoritmo de cifrado, una clave de cifrado y un parámetro de cifrado se pueden cambiar para cada segmento de datos en base a los datos contenidos en la parte predeterminada. La parte predeterminada puede incluir una primera parte predeterminada para seleccionar un primer conjunto de información de cifrado y una segunda parte predeterminada para seleccionar un segundo conjunto de información de cifrado, la información de cifrado incluye un algoritmo de cifrado, una clave de cifrado y, optativamente, un parámetro de cifrado.

**REIVINDICACIONES**

1. Un dispositivo de cifrado/descifrado para procesar criptográficamente datos, caracterizado por:

un buffer de entrada adaptado para recibir datos que incluyen una pluralidad de segmentos de datos, cada uno de los segmentos de datos encriptados tiene una parte predeterminada, en donde la parte predeterminada comprende una primera parte predeterminada, y una segunda parte predeterminada;

un módulo de cifrado adaptado para cifrar los datos contenidos la segunda parte predeterminada de cada segmento de datos, usando el primer juego de información de cifrado seleccionado para el segmentos de datos y cifrar la parte restante del segmento de datos excepto las primera y segunda partes predeterminadas, utilizando el segundo juego de información de cifrado;

un controlador conectado a dicho buffer de entrada y dicho módulo de cifrado, dicho controlador está adaptado para seleccionar un primer juego de información de cifrado para un segmento de datos corriente que debe cifrarse en base a los datos contenidos en la primera parte predeterminada del segmento de datos corriente y seleccionar un segundo juego de información de cifrado para un segmento de datos corriente que debe cifrarse en

base a los datos contenidos en la segunda parte predeterminada del segmento de datos; y

un buffer de salida conectado a dicho controlador y dicho módulo de cifrado, dicho buffer de salida está adaptado para hacer salir datos encriptados que incluyen una pluralidad de segmentos de datos cifrados.

2. El dispositivo de cifrado/descifrado de acuerdo con la reivindicación 1, caracterizado porque dicho primer juego de información de cifrado comprende:

un primer algoritmo de cifrado, una primera clave de cifrado, y optativamente un primer parámetro de cifrado.

3. El dispositivo de cifrado/descifrado de acuerdo con la reivindicación 1, caracterizado porque dicho segundo juego de información de cifrado comprende:

un segundo algoritmo de cifrado, una segunda clave de cifrado, y optativamente un segundo parámetro de cifrado.

4. El dispositivo de cifrado/descifrado de acuerdo con la reivindicación 1, en donde dicho módulo de cifrado está caracterizado porque además comprende:

un buffer de datos conectado a cada uno de la pluralidad de motores de cifrado.

5. El dispositivo de cifrado/descifrado de acuerdo con la reivindicación 1, en donde dicho controlador está caracterizado porque comprende:

un selector de datos adaptado para seleccionar, para cada segmento de datos, un primer juego de información de cifrado en base a los datos contenidos en la primera parte predeterminada del segmento de datos, y seleccionar, un segundo juego de información de cifrado en base a los datos contenidos en la segunda parte predeterminada del segmento de datos;

un selector de cifrado conectado con dicho selector de datos, adaptado para seleccionar el primer juego de información de cifrado de acuerdo con datos contenidos en la primera parte predeterminada del segmento de datos, y seleccionar el segundo juego de información de cifrado de acuerdo con datos contenidos en la segunda parte predeterminada del segmento de datos; y

un controlador de cifrado adaptado para seleccionar y activar un motor de cifrado basado en la información de cifrado.

6. El dispositivo de cifrado/descifrado de acuerdo con la reivindicación 1, en donde dicho controlador además está caracterizado por:

un generador de valor conectado a dicho selector de datos, adaptado para generar un valor a partir de los datos contenidos en la parte predeterminada.

7. El dispositivo de cifrado/descifrado de acuerdo con la reivindicación 6, caracterizado porque dicho generador de valor está adaptado para verificar los datos contenidos en la parte predeterminada utilizando una clave de verificación.

8. El dispositivo de cifrado/descifrado de acuerdo con la reivindicación 6, en donde dicho controlador de cifrado está caracterizado por una tabla de cifrado que contiene:
un identificador de tipo de cifrado
una clave de cifrado para el tipo de cifrado y
un parámetro de cifrado,
para cada entrada asociada con un valor generado.

9. El dispositivo de cifrado/descifrado de acuerdo con la reivindicación 1, caracterizado porque la pluralidad de segmentos de datos son paquetes de datos en una corriente de datos.

10. El dispositivo de cifrado/descifrado de acuerdo con la reivindicación 1, caracterizado porque la primera parte predeterminada contiene datos para una primera capa de protocolo,

y la segunda parte predeterminada contiene datos para una segunda capa de protocolo, en donde la primera capa de protocolo es más baja que la segunda capa de protocolo.

11. El dispositivo de cifrado/descifrado de acuerdo con la reivindicación 1, caracterizado porque la primera parte predeterminada es un encabezamiento de Protocolo de Internet (IP) del paquete de datos.

12. El dispositivo de cifrado/descifrado de acuerdo con la reivindicación 1, caracterizado porque la segunda parte predeterminada es una de:

una parte seleccionada de un campo de datos del paquete de datos,

un encabezamiento de Protocolo de Control de Transmisión (TCP) del paquete de datos y

un encabezamiento de Protocolo de Datograma de Usuario (UDP) del paquete de datos.

13. El dispositivo de cifrado/descifrado de acuerdo con la reivindicación 1, caracterizado porque la pluralidad de segmentos de datos son sectores en un dispositivo de almacenamiento de datos.

14. El dispositivo de cifrado/descifrado de acuerdo con la reivindicación 13, caracterizado porque la primera parte predeterminada es una primera parte seleccionada en un sector en el dispositivo de almacenamiento de datos, y la segunda parte predeterminada es una segunda parte seleccionada en el sector.

15. El dispositivo de cifrado/descifrado de acuerdo con la reivindicación 1, en donde dicho controlador está caracterizado por:

una primera tabla de cifrado para seleccionar el primer juego de información de cifrado basado en datos contenidos en la primera parte predeterminada; y

una segunda tabla de cifrado para seleccionar el segundo juego de información de cifrado basado en datos contenidos en la segunda parte predeterminada.

16. Un dispositivo de cifrado/descifrado para procesar criptográficamente datos, caracterizado por:

un buffer de entrada adaptado para recibir una pluralidad de segmentos de datos cifrados, cada uno de los segmentos de datos cifrados tiene una parte predeterminada, en donde la parte predeterminada comprende una primera parte predeterminada, y una segunda parte predeterminada;

un módulo de descifrado adaptado para descifrar los datos contenidos en la segunda parte predeterminada del segmento de datos cifrado corriente usando el primer juego de información de cifrado seleccionado para el segmento de datos cifrados, y descifrar la parte restante del segmento de datos cifrado corriente, excepto las primera y segunda partes predeterminadas usando el segundo juego de información de cifrado seleccionado para el segmento de datos cifrado;

un controlador conectado a dicho buffer de entrada y dicho módulo de descifrado, dicho controlador está adaptado para seleccionar un primer juego de información de cifrado para un segmento de datos cifrado corriente que debe descifrarse en base a datos contenidos en la primera parte predeterminada del segmento de datos cifrado corriente; y seleccionar un segundo juego de información de cifrado para un segmento de datos cifrado corriente que debe descifrarse en base a datos contenidos en la segunda parte predeterminada del segmento de datos cifrado corriente; y

un buffer de salida conectado a dicho controlador y a dicho módulo de descifrado, dicho buffer de salida está adaptado para hacer salir datos descifrados que incluyen una pluralidad de segmentos de datos descifrados.

17. El dispositivo de cifrado/descifrado de acuerdo con la reivindicación 16, en donde dicho módulo de descifrado está caracterizado porque comprende:

una pluralidad de motores de descifrado, cada motor de descifrado corresponde a un algoritmo de cifrado respectivo, diferentes entre sí.

18. El dispositivo de cifrado/descifrado de acuerdo con la reivindicación 16, en donde dicho módulo de descifrado además está caracterizado por:

un buffer de datos conectado a cada uno de la pluralidad de motores de descifrado.

19. El dispositivo de cifrado/descifrado de acuerdo con la reivindicación 16, en donde dicho controlador está caracterizado porque comprende:

un selector adaptado para seleccionar, para cada segmento de datos cifrado, seleccionar un primer juego de información de cifrado en base a datos contenidos en la primera parte predeterminada del segmento de datos cifrado; y seleccionar un segundo juego de información de cifrado en base a datos contenidos en la segunda parte predeterminada del segmento de datos cifrado;

un selector de descifrado conectado con dicho selector de datos, adaptado para seleccionar el primer juego de información de cifrado en base a datos contenidos en la primera parte predeterminada del segmento de datos cifrado; y seleccionar el segundo juego de información de cifrado en base a datos contenidos en la segunda parte predeterminada del segmento de datos cifrado; y

un controlador de descifrado adaptado para seleccionar y activar un motor de descifrado basado en la información de cifrado.

20. El dispositivo de cifrado/descifrado de acuerdo con la reivindicación 16, en donde dicho controlador además está caracterizado por:

un generador de valor conectado al selector de datos, adaptado para generar un valor a partir de los datos contenidos en la parte predeterminada.

21. El dispositivo de cifrado/descifrado de acuerdo con la reivindicación 20, caracterizado porque dicho generador de valor está adaptado para verificar los datos contenidos en la parte predeterminada utilizando una clave de verificación.

22. El dispositivo de cifrado/descifrado de acuerdo con la reivindicación 20, en donde dicho controlador de descifrado está caracterizado por una tabla de cifrado que contiene:

un identificador de tipo de cifrado;

una clave de cifrado para el tipo de cifrado; y

un parámetro de cifrado,

para cada entrada asociada con un valor generado.

23. El dispositivo de cifrado/descifrado de acuerdo con la reivindicación 16, caracterizado porque la pluralidad de segmentos de datos son paquetes de datos en una corriente de datos.

24. El dispositivo de cifrado/descifrado de acuerdo con la reivindicación 16, caracterizado porque la primera parte predeterminada contiene datos para una primera capa de protocolo, y la segunda parte predeterminada contiene datos para una segunda capa de protocolo, en donde la primera capa de protocolo es más baja que la segunda capa de protocolo.

25. El dispositivo de cifrado/descifrado de acuerdo con la reivindicación 16, caracterizado porque la primera parte predeterminada es un encabezamiento de Protocolo de Internet (IP) del paquete de datos.

26. El dispositivo de cifrado/descifrado de acuerdo con la reivindicación 25, caracterizado porque la segunda parte predeterminada es una de:

una parte seleccionada de un campo de datos del paquete de datos;

un encabezamiento de Protocolo de Control de Transmisión (TCP) del paquete de datos; y

un encabezamiento de Protocolo de Datograma de Usuario (UDP) del paquete de datos.

27. El dispositivo de cifrado/descifrado de acuerdo con la reivindicación 16, caracterizado porque la pluralidad de segmentos de datos son sectores en un dispositivo de almacenamiento de datos.

28. El dispositivo de cifrado/descifrado de acuerdo con la reivindicación 27, caracterizado porque la primera parte predeterminada es una primera parte seleccionada en un sector en un dispositivo de almacenamiento de datos, y la segunda parte predeterminada es una segunda parte seleccionada en el sector.

29. El dispositivo de cifrado/descifrado de acuerdo con la reivindicación 16, en donde dicho controlador está caracterizado porque comprende:

una primera tabla de cifrado para seleccionar el primer juego de información de cifrado basado en datos contenidos en la primera parte predeterminada; y

una segunda tabla de cifrado para seleccionar el segundo juego de información de cifrado basado en datos contenidos en la segunda parte predeterminada.

30. Una tarjeta de cifrado/descifrado para procesar criptográficamente datos, dicha tarjeta caracterizada porque comprende:

un medio para recibir una pluralidad de segmentos de datos, teniendo cada uno de los segmentos de datos una parte predeterminada, en donde la parte predeterminada comprende una primera parte predeterminada, y una segunda parte predeterminada;

un medio para seleccionar, para el segmento de datos corriente, un primer juego de información de cifrado basado en datos contenidos en la primera parte predeterminada del segmento de datos;

un medio para cifrar los datos contenidos en la segunda parte predeterminada del segmento de datos corriente utilizando

el primer juego de información de cifrado seleccionado para el segmento de datos;

un medio para seleccionar, para el segmento de datos corriente, un segundo juego de información de cifrado basado en datos contenidos en la segunda parte predeterminada del segmento de datos; y

un medio para cifrar la parte restante del segmento de datos corriente excepto las primera y segunda partes predeterminadas utilizando el segundo juego de información de cifrado seleccionado para el segmento de datos; y

un medio para permitir que dichos medios para seleccionar y dichos medios para cifrar operen sobre los siguientes segmentos de datos.

31. La tarjeta de cifrado/descifrado de acuerdo con la reivindicación 30, caracterizada porque dicho primer juego de información de cifrado comprende:

un primer algoritmo de cifrado, una primera clave de cifrado y optativamente un primer parámetro de cifrado.

32. La tarjeta de cifrado/descifrado de acuerdo con la reivindicación 30, caracterizada porque dicho segundo juego de información de cifrado comprende:

un segundo algoritmo de cifrado, una segunda clave de cifrado y optativamente un segundo parámetro de cifrado.

33. La tarjeta de cifrado/descifrado de acuerdo con la reivindicación 32, caracterizada porque dicho medio para generar un valor comprende:

un medio para verificar los datos contenidos en la parte predeterminada utilizando una clave de verificación.

34. La tarjeta de cifrado/descifrado de acuerdo con la reivindicación 30, caracterizada además por:

un medio para proveer un identificador de tipo de cifrado, una clave de cifrado para el tipo de cifrado, y un parámetro de cifrado asociado con un valor generado.

35. La tarjeta de cifrado/descifrado de acuerdo con la reivindicación 30, caracterizada además porque comprende:

un medio para cifrar la segunda parte predeterminada utilizando el primer juego de información de cifrado.

36. La tarjeta de cifrado/descifrado de acuerdo con la reivindicación 35, caracterizada además porque comprende:

un medio para cifrar la parte restante del segmento de datos utilizando el segundo juego de información de cifrado.

37. La tarjeta de cifrado/descifrado de acuerdo con la reivindicación 30, caracterizada además porque comprende:

un medio para generar, un segmento de datos encriptado para cada uno de la pluralidad de segmentos de datos recibidos antes de ser cifrados, los segmentos de datos cifrados tienen una primera parte predeterminada, una segunda parte predeterminada, y una parte remanente, la primera parte predeterminada contiene los datos originales en la correspondiente primera parte predeterminada del segmento de datos original , la segunda parte predeterminada contiene los datos cifrados de la correspondiente segunda parte predeterminada del segmento de datos original, y la parte restante contiene los datos cifrados de la correspondiente parte restante del segmento de datos original.

38. La tarjeta de cifrado/descifrado de acuerdo con la reivindicación 37, caracterizada además porque comprende:

un medio para transmitir una pluralidad de segmentos de datos cifrados como una corriente de datos cifrados.

39. La tarjeta de cifrado/descifrado de acuerdo con la reivindicación 37, caracterizada además porque comprende:

un medio para almacenar una pluralidad de segmentos de datos cifrados en un dispositivo de almacenamiento de datos, cada

segmento de datos cifrado corresponde a un sector de datos respectivo del dispositivo de almacenamiento de datos.

40. La tarjeta de cifrado/descifrado de acuerdo con la reivindicación 37, caracterizada además porque comprende:

un medio para recibir los datos cifrados que incluyen una pluralidad de segmentos de datos cifrados;

un medio para seleccionar, para cada segmento de datos cifrado, un primer juego de información de cifrado basado en datos contenidos en la primera parte predeterminada del segmento de datos cifrado;

un medio para descifrar los datos cifrados contenidos en la segunda parte predeterminada de cada segmento de datos cifrado utilizando el primer juego de información de cifrado seleccionado para el segmento de datos cifrado;

un medio para seleccionar, para cada segmento de datos cifrado, un segundo juego de información de cifrado basado en datos descifrados de la segunda parte predeterminada; y

un medio para descifrar la parte restante de cada segmento de datos cifrado utilizando el segundo juego de información de cifrado seleccionado para el segmento de datos cifrado.

41. La tarjeta de cifrado/descifrado de acuerdo con la reivindicación 40, caracterizada porque dicho medio para seleccionar la primera información de cifrado comprende:

un medio para generar un primer valor desde los datos originales contenidos en la primera parte predeterminada del segmento de datos cifrado.

42. La tarjeta de cifrado/descifrado de acuerdo con la reivindicación 41, caracterizada porque dicho medio para generar el primer valor comprende:

un medio para verificar los datos contenidos en la primera parte predeterminada utilizando una primera clave de verificación.

43. La tarjeta de cifrado/descifrado de acuerdo con la reivindicación 40, caracterizada porque dicho medio para seleccionar la segunda información de cifrado comprende:

un medio para generar un segundo valor desde los datos descifrados de la primera parte predeterminada del segmento de datos cifrado.

44. La tarjeta de cifrado/descifrado de acuerdo con la reivindicación 43, caracterizada porque dicho medio para generar el segundo valor comprende:

un medio para verificar los datos descifrados de la segunda parte predeterminada utilizando una segunda clave de verificación.

45. Una tarjeta de cifrado/descifrado para procesar criptográficamente datos, dicha tarjeta de cifrado/descifrado caracterizada porque comprende:

un medio para recibir una pluralidad de segmentos de datos cifrados, teniendo cada uno de los segmentos de datos cifrados una parte predeterminada, en donde la parte predeterminada comprende una primera parte predeterminada, y una segunda parte predeterminada;

un medio para seleccionar, para el segmento de datos cifrado corriente, un primer juego de información de cifrado basado en datos contenidos en la primera parte predeterminada del segmento de datos cifrado;

un medio para descifrar los datos contenidos en la segunda parte predeterminada del segmento de datos cifrado corriente utilizando el primer juego de información de cifrado seleccionado para el segmento de datos cifrado;

un medio para seleccionar, para el segmento de datos cifrado corriente, un segundo juego de información de cifrado basado en datos contenidos en la segunda parte predeterminada del segmento de datos cifrado; y

un medio para descifrar la parte restante del segmento de datos cifrado corriente excepto las primera y segunda partes predeterminadas utilizando el segundo juego de información de cifrado seleccionado para el segmento de datos cifrado; y

un medio para permitir que dichos medios para seleccionar y dichos medios para descifrar operen sobre los siguientes segmentos de datos cifrados.

46. La tarjeta de cifrado/descifrado de acuerdo con la reivindicación 45, caracterizada porque dicho primer juego de información de cifrado comprende un primer algoritmo de cifrado, una primera clave de cifrado, y optativamente un primer parámetro de cifrado.

47. La tarjeta de cifrado/descifrado de acuerdo con la reivindicación 46, caracterizada porque dicho segundo juego de información de cifrado comprende un segundo algoritmo de cifrado, una segunda clave de cifrado, y optativamente un segundo parámetro de cifrado.

48. La tarjeta de cifrado/descifrado de acuerdo con la reivindicación 45, caracterizada porque además comprende:

un medio para proporcionar un identificador de tipo de cifrado;

una clave de cifrado para el tipo de cifrado, y

un parámetro de cifrado, asociado con un valor generado.