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 PSYCRYPT 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. 03989 del Examen de Patentabilidad emanado 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 los señalado en el Artículo 28 de la Decisión 486, respecto de que la descripción no permite identificar una forma de ejecución clara y completa de las mejoras consideradas patentables, se ha corregido la memoria descriptiva, de acuerdo a lo

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

señalado por el Señor Examinador, eliminando términos como "encripotado", o "decriptación", cambiándolos por **"encriptado" y "desencriptación".**

Las cláusulas referidas a un aparato han sido modificadas de manera de tratarse ahora de un sistema, de manera de aportar mayor claridad al alcance de la invención. También se ha modificado el término "aparato" por "sistema" en la memoria, de manera de aportar congruencia a la invención.

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 81 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.

Todas las reivindicaciones han sido convenientemente caracterizadas, de manera de complementar con lo solicitado por el Sr. Examinador.

Además, las cláusulas referidas a un aparato han sido modificadas de manera de tratarse ahora de un sistema, de manera de aportar mayor claridad al alcance de la invención. También se ha modificado el término "aparato" por "sistema" en la memoria, de manera de aportar congruencia a la invención

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 manifiesta respetuosamente lo siguiente:

La patente US 6296164 está dirigida al desarrollo de un método de encriptación/desencriptación para la transmisión segura de datos. La metodología de encriptación, desencriptación 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 US6296164 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 la encriptación / desencriptación 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

284
284

TM TAMAYO
ROYALTIES • PATENTS • TRADEMARKS

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

MÉTODO Y SISTEMA PARA PROCESAR CRIPTOGRÁFICAMENTE DATOS

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 criptográficamente datos que incluyen una pluralidad de segmentos de datos.

Antecedentes de la Invención

Numerosos métodos de métodos de encriptación 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 sola clave (clave secreta) para encriptar y desencriptar información. La criptografía asimétrica, que también se denomina criptografía de clave pública, utiliza un par de claves: una (clave pública) para encriptar datos, y la otra (clave privada) para desencriptarlos. Los algoritmos de encriptación que existen actualmente incluyen, por ejemplo, el Estándar de Encriptación de Datos (DES) que es un algoritmo simétrico que emplea una cifra de bloqueo con una sola 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 Encriptación de Datos (IDEA) que es un algoritmo de encriptación de clave secreta de modo de bloqueo que utiliza una clave de 128 bits, el RC4 que es un algoritmo de clave

simétrica ampliamente utilizado, el Estándar de Encriptación Avanzado (AES) que provee un esquema de encriptación más resistente con tres longitudes alternativas de la clave de 128 bits, de 192 bits o de 256 bits y similares.

Muchas empresas emplean un criptosistema simétrico para sus comunicaciones secretas, que utiliza un algoritmo de encriptación 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 han parecido indestructibles se están haciendo insuficientes, por ejemplo, el tamaño de la clave de 56 bits del DES ya no se considera seguro contra ataques con fuerza bruta. La utilización del mismo algoritmo de encriptación y la misma clave secreta para la comunicación durante un tiempo prolongado puede aumentar el riesgo de ataques con fuerza bruta contra el criptosistema. Sin embargo, el reemplazo del algoritmo de encriptación 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 secreta, en persona, por correo privado, y similar, entre la totalidad de las entidades que utilizan el criptosistema, y cualquier cambio en el algoritmo o la clave secreta debe también sincronizarse entre las entidades. Un criptosistema de clave de algoritmo fijo también carece de compatibilidad con otros criptosistemas que utilizan un algoritmo de encriptación diferente y/o una clave secreta diferente.

Por consiguiente, sería deseable proveer un criptosistema que realice comunicaciones y transacciones seguras que sea menos vulnerable para la fuerza bruta y otros ataques y que también tenga alta flexibilidad y compatibilidad.

Breve Descripción de la invención

Un método 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 juego de información de encriptación basado en datos contenidos en una parte predeterminada del segmento de datos que se debe encriptar, y (c) encriptar cada segmento de datos utilizando el juego de información de encriptación seleccionado para el segmento de datos. Al menos uno de un algoritmo de encriptación, una calve de encriptación, y un parámetro de encriptación 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 juego de información de encriptación, y una segunda parte predeterminada para seleccionar un segundo juego de información de encriptación, la información de encriptación incluye un algoritmo de encriptación, una calve de encriptación, y optativamente un parámetro de encriptación.

De acuerdo con un aspecto de la presente invención, un método para encriptar datos incluye (a) recibir una pluralidad de

segmentos de datos, (b1) seleccionar, para cada paquete, un primer juego de información de encriptación basado en los datos contenidos en una primera parte predeterminada del segmento de datos, (b2) seleccionar, para cada paquete, un segundo juego de información de encriptación basado en datos contenidos en una segunda parte predeterminada del segmento de datos, (c1) encriptar la segunda parte predeterminada de cada segmento de datos utilizando el primer juego de información de encriptación seleccionado para el segmento de datos, (c2) encriptar la parte restante de cada segmento de datos utilizando la segunda información de encriptación seleccionada para el segmento de datos, y (d) generar un segmento de datos encriptado para cada uno de los segmentos de datos originales, el segmento de datos encriptado tiene una primera parte predeterminada, una segunda parte predeterminada y una parte restante, al 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 encriptados de la segunda parte predeterminada del segmento de datos original, y la parte restante contiene los datos encriptados de la parte restante correspondiente del segmento de datos original.

De acuerdo con un aspecto de la presente invención, el método para desencriptar datos incluye (a) recibir datos encriptados que incluyen una pluralidad de segmentos de datos encriptados, cada uno de los segmentos de datos encriptados tiene una primera parte predeterminada, una segunda parte predeterminada, y una parte restante, la primera parte predeterminada contiene

datos originales de la primera parte predeterminada correspondiente de un segmento de datos original, la segunda parte predeterminada contiene los datos encriptados de una segunda parte predeterminada del segmento de datos original, y la parte restante contiene los datos encriptados de la parte restante correspondiente del segmento de datos original, (b1) seleccionar, para cada segmento de datos encriptado, una primera información de encriptación basada en los datos originales contenidos en la primera parte predeterminada del segmento de datos encriptado, (c1) desencriptar los datos encriptados contenidos en la segunda parte predeterminada de cada segmento de datos encriptado utilizando el primer juego de información de encriptación seleccionado para el segmento de datos encriptado, (b2) seleccionar, para cada segmento de datos encriptado, un segundo juego de información de encriptación basado en los datos desencriptados de la segunda parte predeterminada, (c2) desencriptar la parte restante de cada segmento de datos encriptado utilizando el segundo juego de información de encriptación seleccionado para el segundo segmento de datos encriptado.

De acuerdo con un aspecto de la invención, un sistema para procesar criptográficamente datos incluye (a) un medio para recibir una pluralidad de segmentos de datos, (b) un medio para seleccionar, para cada segmento de datos, un juego de información de encriptación basado en datos contenidos en una parte predeterminada del segmento de datos que debe enecriptarse, y (c) un medio para encriptar cada segmento de datos utilizando el juego de información de encriptación

seleccionado para el segmento de datos. El medio para seleccionar puede cambiar al menos uno de un algoritmo de encriptación, una clave de encriptación, y un parámetro de encriptación 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 juego de información de encriptación asociado con el valor generado, el juego de información de encriptación incluye un algoritmo de encriptación, una clave de encriptación, y optativamene un parámetro de encriptación. El medio para generar un valor puede incluir un medio para verificar los datos contenidos en la parte predeterminada utilizando una clave de verificación.

De acuerdo con un aspecto de la invención, el sistema puede además incluir un medio para proveer una tabla de encriptación que contiene un identificador del tipo de encriptación, una clave de encriptación para el tipo de encriptación, y un parámetro de encriptación, 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 juego de información de encriptación y una segunda parte predeterminada para seleccionar un segundo

juego de información de encriptación. Cada juego de información de encriptación incluye un algoritmo de encriptación, una clave de encriptación, y optativamente un parámetro de encriptación.

De acuerdo con un aspecto de la invención, el sistema puede además incluir un medio para encriptar la segunda parte predeterminada utilizando el primer juego de información de encriptación y un medio para encriptar la parte restante del segmento de datos utilizando el segundo juego de información de encriptación.

De acuerdo con un aspecto de la invención, el sistema puede incluir además un medio para generar un segmento de datos encriptado para cada segmento de datos original, el segmento de datos encriptado 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 del segmento de datos original, la segunda parte predeterminada contiene los datos encriptados de la segunda parte predeterminada correspondiente del segmento de datos original, y la parte restante contiene los datos encriptados de la parte restante correspondiente del segmento de datos original.

De acuerdo con un aspecto de la invención el sistema puede incluir además un medio para transmitir una pluralidad de segmentos de datos encriptados como una corriente de datos encriptados. El sistema puede incluir también un medio para almacenar una pluralidad de segmentos de datos encriptados en un aparato de almacenamiento de datos, cada segmento de datos

encriptado corresponde a un sector de datos respectivo del dispositivo de almacenamiento.

De acuerdo con un aspecto de la invención, el sistema puede además incluir (a) un medio para recibir los datos encriptados que incluyen una pluralidad de segmentos de datos encriptados, (b1) un medio para seleccionar, para cada segmento de datos encriptado, un primer juego de información de encriptación basado en los datos contenidos en la primera parte predeterminada del segmento de datos encriptado, (c1) un medio para desencriptar los datos encriptados contenidos en la segunda parte predeterminada de cada segmento de datos encriptado utilizando un primer juego de información de encriptación seleccionado para el segmento de datos encriptado, (b2) seleccionar, para cada segmento de datos encriptado, un segundo juego de información de encriptación basado en los datos desencriptados de la segunda parte predeterminada, y (c2) desencriptar la parte restante de cada segmento de datos encriptado utilizando el segundo juego de información de encriptación seleccionado para el segmento de datos encriptado.

De acuerdo con un aspecto de la invención, el medio para seleccionar la primera información de encriptación 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 encriptado. El medio para generar el primer valor puede incluir un medio para verificar 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 encriptación puede incluir un medio para generar un segundo valor a partir de los datos desencriptados de la segunda parte predeterminada del segmento de datos encriptado. El medio para generar el segundo valor puede incluir un medio para verificar los datos desencriptados de la segunda parte predeterminada utilizando una clave de verificación.

De acuerdo con un aspecto de la invención, el sistema para desencriptar datos incluye (a) un medio para recibir una pluralidad de segmentos de datos encriptados, cada uno de los segmentos de datos encriptados tiene una parte predeterminada, (b) un medio para seleccionar, para cada segmento de datos encriptado, un juego de información de encriptación basado en los datos contenidos en la parte predeterminada del segmento de datos encriptado, y (c) un medio para desencriptar cada segmento de datos encriptado utilizando la información de encriptación seleccionada para el segmento de datos encriptado.

De acuerdo con un aspecto de la invención, el medio para seleccionar puede incluir un medio para generar, para cada segmento de datos encriptado, un valor a partir de los datos contenidos en la parte predeterminada del segmento de datos encriptado, y un medio para seleccionar un juego de información de encriptación asociado con el valor generado, el juego de información de encriptación incluye un algoritmo de encriptación, una clave de encriptación, y optativamente un

parámetro de encriptación. El medio para generar un valor puede incluir un medio para verificar los datos contenidos en la parte predeterminada utilizando una clave de verificación.

De acuerdo con un aspecto de la invención, el sistema puede incluir además un medio para proveer un identificador de tipo de encriptación, una clave de encriptación para el tipo de encriptación, y un parámetro de encriptación 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 encriptación, y una segunda parte predeterminada para seleccionar un segundo juego de información de encriptación. Cada juego de información de encriptación puede incluir un algoritmo de encriptación, una clave de encriptación, y optativamente un parámetro de encriptación.

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 más baja que 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 Datograma de Usuario 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 encriptado se ha encriptado utilizando el primer juego de información de encriptación, y los datos contenidos en la parte restante del segmento de datos encriptado se ha encriptado utilizando el segundo juego de información de encriptación.

Breve Descripción de los Dibujos

Los dibujos adjuntos, que se incorporan y constituyen una 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 la implementación de la invención.

En los dibujos:

La Figura 1A es un diagrama de bloques que ilustra esquemáticamente una parte de encriptación de un sistema para encriptar/desencriptar datos de acuerdo con una realización de la presente invención.

La Figura 1B es un diagrama de bloques que ilustra esquemáticamente una parte de desencriptación de un sistema para encriptar/desencriptar datos de acuerdo con una realización de la presente invención.

La Figura 2 es un diagrama que ilustra esquemáticamente un ejemplo del valor de encriptación 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 encriptar/desencriptar 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 Datagrama de Usuario.

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 donde 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 encriptar 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 encriptar un paquete de datos utilizando el método mostrado en la Figura 9.

La Figura 11 es un diagrama de flujo de proceso que ilustra esquemáticamente un método para desencriptar datos encriptados 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 desencriptar un paquete de datos utilizando el método mostrado en la Figura 11.

La Figura 13 es un diagrama de bloques que ilustra esquemáticamente un encriptador/desencriptador 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 sistema de encriptación/desencriptación 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 método y sistema para encriptar y desencriptar 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 se sugerirán rápidamente a los expertos en el arte que tienen el beneficio de esta invención. Ahora 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 o a partes iguales.

En aras de la claridad, no se muestran y describen todas las características habituales de las implementaciones descritas aquí. Naturalmente, se apreciará que en el desarrollo de cualquiera de esas implementaciones, deberán hacerse numerosas decisiones específicas de 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 sería un compromiso habitual de ingeniería para los expertos en el arte que tiene el beneficio de esta invención.

De acuerdo con una realización de la presente invención, los componentes, pasos de proceso, y/o estructuras de datos pueden implementarse utilizando diferentes tipos de dispositivos cableados, dispositivos lógicos programables de campo (FPLD), que incluyen matrices de compuerta programable de campo (FPGA) y dispositivos lógicos programables complejos (CPLD), circuitos integrados específicos de la aplicación (ASIC) o similares, también se pueden utilizar sin apartarse del alcance y espíritu de los conceptos de la invención descritos aquí.

En el contexto de la presente invención, el término "red" incluye redes de área local (LAN), redes de área amplia (WAN),

la Internet, sistemas de televisión por cable, sistemas telefónicos, sistemas de telecomunicaciones inalámbricas, redes de fibra óptica, redes ATM, redes de relé de cuadro, 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 encriptar/desencriptar 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 encriptación 14, un controlador 16 conectado la buffer de entrada 12 y al módulo de encriptación 14, y un buffer de salida 18 conectado al controlador 16 y al módulo de encriptación 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 similar. El módulo de encriptación 14 está adaptado para encriptar cada segmento de datos. El buffer de salida 18 separa los segmentos de datos encriptados del módulo de encriptación 14, y hace salir los datos encriptados que incluyen una pluralidad de segmentos de datos.

Por ejemplo, como se muestra en la Figura 1 A, el sistema 10 puede utilizarse entre una puerta de bus serial universal (USB) 11 y la puerta de 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 (IDE), una interfaz de IDE mejorada, y similares, para almacenar datos seguros en dispositivos de almacenamiento en masa. El sistema también puede utilizarse para el otro tipo de transferencia de datos digital.

El controlador 16 está adaptado para seleccionar un juego de información de encriptación para cada segmento de datos basado en datos contenidos en una parte predeterminada del segmento de datos que debe encriptarse. Por ejemplo, la información de encriptación incluye un algoritmo de encriptación, una clave de encriptación, y un parámetro de encriptación tal como un vector inicial. El parámetro de encriptación puede utilizarse para iniciar o inicialar el proceso de encriptación a un estado específico. Dado que la información de encriptación se selecciona basado en datos en una parte específica del segmento de datos que debe encriptarse, generalmente, al menos uno del algoritmo de encriptación, la clave de encriptación, y el parámetro de encriptación se cambia para cada segmento de datos. En otras palabras, la información de encriptación se "autodetermina" para cada segmento de datos utilizando los

datos contenidos en el segmento de datos en sí. La parte predeterminada del segmento de datos puede ser un encabezamiento de cada paquete de datos, una parte de selección 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 el 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 encriptación 14 incluye una pluralidad de motores de encriptación 20 (20a, 20b, 20c...), cada uno corresponde a un algoritmo de encriptación que debe seleccionar el controlador 16. El módulo de encriptación 14 puede incluir además un buffer de datos 22 conectado a cada uno de la pluralidad de los motores de encriptación 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 encriptación 26 conectado con el selector de datos 24 y un controlador de encriptación 28. El selector de datos 24 está adaptado para seleccionar la parte predeterminada de cada segmento de datos. El selector de encriptación 26 está adaptado para seleccionar un juego de información de encriptación de acuerdo con datos contenidos en la parte predeterminada seleccionada por el selector de datos 24. El juego de información de encriptación incluye, por ejemplo, un algoritmo de encriptación, una clave de

encriptación y optativamente un parámetro de encriptación. El controlador de encriptación 28 está adaptado para seleccionar y activar uno de los motores de encriptación 20 basado en la información de encriptación. Por ejemplo, si el selector de encriptación selecciona un algoritmo de encriptación A, el controlador de encriptación 28 selecciona un motor de encriptación correspondiente (A) 20a y activa o iniciala el motor de encriptación 20a utilizando los parámetros de encriptación. Los datos se encriptan con el motor de encriptación 20a utilizando la clave seleccionada. Se debe hacer notar que una clave diferente y/o un parámetro de encriptación diferente dan datos encriptados diferentes aún cuando se utilicen el mismo algoritmo de encriptación y por lo tanto el mismo motor de encriptación.

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 de verificación y verificar los datos utilizando una clave de verificación para producir el valor. La clave de verificación puede preinstalarse en el generador de valor 30, o puede seleccionarse cuando el controlador 16 se programa primero.

De acuerdo con una realización de la presente invención, el controlador de encriptación 26 incluye una tabla de encriptación 32. La tabla de encriptación 32 contiene un

identificador de tipo de encriptación, una clave de encriptación para el tipo de encriptación, y un parámetro de encriptación tal como un vector inicial que especifica un estado de encriptación inicial del motor de encriptación, 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 encriptación 32. Como se muestra en la Figura 2, cada entrada de la tabla de encriptación 32 tiene un índice que corresponde al valor generado, por ejemplo, un valor de verificación, y un juego correspondiente de un algoritmo de encriptación (tipo de encriptación), una clave para el algoritmo de encriptación, y un vector inicial (parámetro de encriptación). El número de las entradas depende del valor generado desde la parte predeterminada. En una realización de la presente invención, una tabla de encriptación 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 encripta utilizando una información de encriptación diferente.

La descripción precedente es con respecto a la parte de encriptación del sistema 10. La Figura 1B ilustra esquemáticamente una parte de desencriptación correspondiente 10' del sistema 10 de acuerdo con una realización de la presente invención. Como se muestra en la Figura 1B, la parte de desencriptación 10' puede construirse simétricamente a la parte de encriptación (Figura 1A) del sistema 10, que incluye los motores de encriptación 20a', 20b' y 20c' en lugar de los

motores de encriptación 20a, 20b y 20c, como lo entiende bien un experto en el arte sin mayor explicación.

La Figura 3 ilustra esquemáticamente un método para encriptar/desencriptar datos de acuerdo con una realización de la presente invención. El método puede ser ejecutado por el sistema de encriptación/desencriptación 10. Se recibe una pluralidad de segmentos de datos, por ejemplo, recibiendo una corriente de datos que incluyen una pluralidad de paquetes de datos, o leyendo desde un dispositivo de almacenamiento de datos que incluyen una pluralidad de sectores o direcciones de datos. Los segmentos de datos se encriptan segmento por segmento. Como se muestra en la Figura 3, se recibe cada segmento (100), y se selecciona una parte predeterminada de cada segmento de datos (102), y se selecciona un juego de información de encriptación basado en datos contenidos en la parte predeterminada del segmento de datos que debe encriptarse (104). El segmento de datos se encripta utilizando el juego de información de encriptación seleccionado (106). El segmento de datos siguiente se procesa en la misma forma hasta que se procesan todos los segmentos de datos del buffer de entrada (108). El juego de información de encriptación puede incluir un algoritmo de encriptación, una clave de encriptación, y optativamente un parámetro de encriptación, como se describió anteriormente, y generalmente al menos uno del ~~algoritmo de~~ encriptación, la clave de encriptación y el parámetro de encriptación se cambia para cada segmento de datos basado en los datos contenidos en la parte predeterminada.

Como se discutió anteriormente, al seleccionar la información de encriptación, se puede generar un valor (tal como un valor de verificación) a partir de los datos contenidos en la parte predeterminada del segmento de datos, y el juego de información de encriptación se puede seleccionar utilizando el valor generado. El juego de información de encriptación puede proveerse en una forma de una tabla de encriptación tal como la tabla de encriptación 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 más alta que la primera capa de protocolo en la jerarquía del protocolo. La primera 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 Datograma 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 le 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 (de verificación), 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 e 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 porción.

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, 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 encriptarse 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 puede 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 encriptar 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 encriptar un paquete de datos 70 utilizando el método mostrado 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 haciendo referencia a la Figura 10, la primera información de encriptación 78 se selecciona basado en los datos contenidos en la primera parte predeterminada 70 (116). Como se discutió anteriormente, esta selección 116 puede incluir, por ejemplo, obtener un valor de verificación a partir de la primera parte predeterminada 72 y seleccionar la primera información de encriptación utilizando una tabla de encriptación que asocia el valor de verificación con un juego de información de encriptación respectivo. En forma similar, la segunda información de encriptación 79 se selecciona basado en los datos contenidos en la segunda parte predeterminada 74 (118). Esta selección 118 puede incluir también, por ejemplo, obtener un valor de verificación a partir de una segunda parte predeterminada 74 y seleccionar la segunda información de encriptación utilizando una tabla de encriptación que asocia el valor de verificación con un juego de información de encriptación respectivo. Una clave de verificación respectiva y una tabla de encriptación respectiva puede proveerse para cada uno del proceso de selección 116 y 118 Por ejemplo, el controlador 16 del sistema de encriptacón/desencriptación 10 (Figura 1) puede incluir un primer juego de clave verificación

y la tabla de encriptación para la primera parte predeterminada, y un segundo juego de la clave de verificación y la tabla de encriptación para la segunda parte predeterminada.

Luego, la segunda parte predeterminada 74 se encripta utilizando la primera información de encriptación 78 (120), y la parte restante del segmento de datos 76 se encripta utilizando la segunda información de encriptación 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 encriptados (también denominada "texto cifrado") y la parte restante 86 que contiene datos encriptados se combinan para generar un segmento de datos (paquete) 80 que corresponde al segmento de datos original (paquete) 70 (124). Por ejemplo, haciendo referencia a la Figura 1, la segunda parte predeterminada puede encriptarse utilizando el motor de encriptación 20a, y la parte restante puede encriptarse utilizando el motor de encriptación 20b, y los datos encriptados respectivos se combinan con la primera parte predeterminada en el segmento de datos encriptado en el buffer de datos 22, y se envían al buffer de salida 18.

Los procesos 110 a 124 se ejecutan hasta que se encripta la totalidad de los segmentos de datos (126). Se debe señalar que los procesos de selección y encriptación se controlan de manera

tal que la segunda información de encriptación 79 se selecciona antes de que los datos contenidos en la segunda parte predeterminada 74 se encripten, 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 186 se envían al buffer de datos 22 en este orden.

Los segmentos de datos encriptados pueden transmitirse como una corriente de datos encriptada 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 desencriptar datos encriptados 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 desencriptar un paquete de datos encriptado 80 utilizando el método mostrado en la Figura 11, donde el paquete de datos encriptado 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 182 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 encriptado recibido (130), la primera parte predeterminada y la segunda parte predeterminada se seleccionan (132, 134). Los segmentos de datos encriptados pueden recibirse como una corriente de datos encriptada 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 encriptación 88 se seleccionan basado en los datos contenidos en la primera parte predeterminada 82 (136). En similar al proceso de encriptación discutido anteriormente, esta selección 136 puede incluir, por ejemplo, obtener un valor de verificación de la primera parte predeterminada 82 y seleccionar la primera información de encriptación utilizando una tabla de encriptación que asocia el valor de verificación con un juego de información de encriptación respectivo. Dado que la primera parte predeterminada contiene el texto claro, la primera información de encriptación es la misma que el segmento de datos original.

Luego, la segunda parte predeterminada 84, que contiene el texto cifrado, se desencripta utilizando la primera información de encriptación 88 (138). La segunda información de encriptación 89 se selecciona basado en los datos descritados 85 contenidos en la segunda parte predeterminada 84 (140). Esta selección 138 puede incluir también, por ejemplo, obtener un valor de verificación de los datos desencriptados 85 y seleccionar la segunda información de encriptación 89 utilizando una tabla de encriptación que asocia el valor de verificación con un juego de información de encriptación

respectivo. Una clave de verificación respectiva y una tabla de encriptación respectiva pueden proveerse para cada uno de los procesos de selección 136 y 138.

Luego, la parte restante 86 del segmento de datos se desencripta utilizando la segunda información de encriptación 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 desencriptado (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 desencriptado (146).

La Figura 13 ilustra esquemáticamente un encriptador/desencriptador 150 de acuerdo con una realización de la presente invención. Como se muestra en la Figura 13, el encriptador/desencriptador 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 encriptación (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 desencriptación (R) 166, y un segundo buffer de datos 168. El módulo de encriptación 156 puede ser la parte de encriptación del sistema de encriptación/desencriptación 10 (módulo de encriptación 14 y el controlador 16) descrito anteriormente, y el módulo de

desencriptación 166 puede ser la parte de encriptación 10' del sistema de encriptación/desencriptación 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 encriptador/desencriptador de datos 150 generalmente transmite y recibe una corriente de datos (Tx y Rx), los analizadores temporizadores 154 y 164 sincronizan los procesos de encriptación/desencriptación para la corriente de datos correspondiente de manera tal que los datos encriptados/desencriptados se combinan correctamente en los respectivos segmentos de datos encriptados/desencriptados (paquetes de datos) y se envían y salen de los buffers de datos 158 y 168, respectivamente.

De acuerdo con una realización de la presente invención, el encriptador/desencriptador de datos 150 (y el sistema de encrioptación/desencriptación 10) puede implementarse en una forma de tarjeta enchufable conectable a una computadora. Dado que la totalidad de los componentes necesarios para la encriptación/desencriptación se proveen en el encriptador/desencriptador (tarjeta de encriptación/desencriptación), el usuario/computadora no tiene que instalar ningún programa de software específico para la

encriptaciónl/desencriptación siempre que la computadora pueda utilizar la tarjeta de encriptación/desencriptación (es decir compatible con la puerta). Simplemente transmitiendo o almacenando datos a través de la tarjeta de encriptación/desencriptación, los datos se encriptan automáticamente y por lo tanto se transmiten a través de una red o se almacenan con seguridad en un dispositivo de almacenamiento. La misma tarjeta de encriptación/desencriptación puede utilizarse para recibir con seguridad datos transmitidos o leer los datos almacenados con seguridad.

Para recibir o leer los datos encriptados, la misma tarjeta o sistema de encriptación/desencriptación, debe utilizarse para desencriptar los datos encriptados. El "mismo" significa que la tarjeta o sistema es capaz de seleccionar las mismas primera y segunda parte predeterminadas de los segmentos de datos y seleccionar y obtener la misma primera y segunda información de encriptación si los datos contenidos en la parte predeterminada son los mismos. Generalmente, por ejemplo, las tarjetas de encriptación/desencriptación correspondientes (comunicadoras) tienen la claves de verificación idénticas y las tablas de encriptación idénticas.

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

encriptación/desencriptación puede implementarse en dispositivos lógicos programables de campo (FPLD), tales como FPGA y CPLD, la tarjeta o sistema de encriptación/desencriptación puede programarse de acuerdo con la especificación del usuario (por ejemplo, el nivel de seguridad, la velocidad de transmisión, el protocolo o estándar requerido, el medio de almacenamiento y/o formato que debe utilizarse, etc) con ajustes específicos de las claves de verificación y las tablas de encriptación (información de encriptación).

Además, el usuario y la computadora no tienen que conocer los ajustes, y los ajustes no son accesibles para el usuario y la computadora, no se puede robar esa información al usuario o a la computadora para "romper el código". Más aún, el algoritmo de encriptación, la clave de encriptación, y optativamente el parámetro de encriptación se cambian prácticamente para todos los segmentos de datos, y cuyo algoritmo, clave y parámetro que deben utilizarse son solamente "conocidos" para el segmento de datos en sí que debe encriptarse. Dado que el algoritmo, clave y/o parámetro de encriptación se cambian automáticamente basado en ciertos datos contenidos en el segmento de datos en sí, la sincronización entre el lado transmisor y el lado receptor es innecesario.

La Figura 14 ilustra esquemáticamente un ejemplo de aplicación de la presente invención para asegurar la comunicación a través de Internet. Como se muestra en la Figura 14, los usuarios 180, 182, 184 pueden utilizar sistemas de

encriptación/desencriptación respectivos 190, 192 y 194 de acuerdo con una realización de la presente invención. Los sistemas de encriptación/desencriptación 190, 192 y 194 pueden ser el sistema de encriptación/desencriptación 10 o el encriptador/desencriptador 150 que se describieron anteriormente. La totalidad de los sistemas de encriptación/desencriptación 190, 192 y 194 se programan idénticamente y se proveen de los mismos ajustes, por ejemplo, las mismas claves de verificación y tablas de encriptación. Como se muestra en la Figura 14, el sistema de encriptación/desencriptación puede utilizarse mediante más de una computadora 184 y 186. Por ejemplo, el sistema de encriptación/desencriptación 194 puede utilizarse con un eje dentro de una LAN de manera tal que todas las transmisiones de datos desde las computadoras o huésped conectados al eje se encriptan.

De acuerdo con una realización de la presente invención, dado que el encabezamiento de IP de cada paquete de datos no se encripta, el esquema de encriptación/desencriptación de una realización de la presente invención no afecta el enrutamiento o conmutación de los paquetes de datos a través de la Internet u otras redes (es decir, operaciones en la capa de protocolo de red). Además, en el caso en que algunos enrutadores pueden posiblemente 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 encripta utilizando la encriptación de dos niveles. Es decir, el segmento de datos diferente de la primera y segunda partes predeterminadas se encripta utilizando la información contenida en la segunda parte predeterminada. Luego, la segunda parte predeterminada se encripta utilizando 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 encriptados (texto cifrado) provee un nivel de seguridad adicional, ya que la segunda parte predeterminada y la parte restante se encriptan generalmente mediante un algoritmo de encriptación diferente, una clave de encriptación diferente y/o un parámetro de encriptación diferente. Además, dado que el algoritmo de encriptación, la clave de encriptación, y/o el parámetro de encriptación se cambian para todos los segmentos de datos, es prácticamente imposible que un hacker rompa 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 invención 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.

REIVINDICACIONES

1. Un método para procesar criptográficamente datos, dicho método caracterizado por:

recibir una pluralidad de segmentos de datos;

seleccionar, para cada segmento de datos, un juego de información de encriptación en base a datos contenidos en una parte predeterminada del segmento a ser encriptado; y

encriptar cada segmento de datos utilizando el juego de información de encriptación seleccionado para el segmento de datos.

2. El método de acuerdo con la reivindicación 1, en donde dicha selección está caracterizada por:

cambiar al menos uno de un algoritmo de encriptación, una clave de encriptación, y un parámetro de encriptación para cada segmento de datos basado en los datos contenidos en la parte predeterminada.

3. El método de acuerdo con la reivindicación 1, en donde dicha selección está caracterizada por:

generar, para cada segmento de datos, un valor a partir de datos contenidos en la parte predeterminada del segmento de datos; y

seleccionar un juego de información de encriptación asociado con el valor generado, en donde el juego de información de encriptación incluye un algoritmo de encriptación, una clave de encriptación, y optativamente un parámetro de encriptación.

4. El método de acuerdo con la reivindicación 3, en donde dicha generación de un valor está caracterizada por:

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

5. El método de acuerdo con la reivindicación 3, caracterizado además por:

proveer una tabla de encriptación que comprende:

un identificador de tipo de encriptación,

una clave de encriptación para el tipo de encriptación, y

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

6. El método de acuerdo con la reivindicación 1, en donde la parte predeterminada está caracterizada por:

una primera parte predeterminada para seleccionar un primer juego de información de encriptación, el primer juego comprende un primer algoritmo de encriptación, una primera clave de encriptación, y optativamente un primer parámetro de encriptación; y

una segunda parte predeterminada para seleccionar un segundo juego de información de encriptación, el segundo juego comprende un segundo algoritmo de encriptación, una segunda clave de encriptación y optativamente un segundo parámetro de encriptación.

7. El método de acuerdo con la reivindicación 6, en donde la recepción está caracterizada por:

recibir una corriente de datos que incluye una pluralidad de paquetes de datos, cada paquete de datos corresponde a un segmento de datos.

8. El método de acuerdo con la reivindicación 7, 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.

9. El método de acuerdo con la reivindicación 7, caracterizado porque la primera parte predeterminada es un encabezamiento de Protocolo de Internet (IP) del paquete de datos.

10. El método de acuerdo con la reivindicación 9, 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.

11. El método de acuerdo con la reivindicación 6, caracterizado porque dicha recepción comprende:
leer la pluralidad de segmentos de datos desde los sectores correspondientes en el dispositivo de almacenamiento de datos.

12. El método de acuerdo con la reivindicación 1, 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.

13. El método de acuerdo con la reivindicación 6, caracterizado además por:

encriptar la segunda parte predeterminada utilizando el primer juego de información de encriptación.

14. El método de acuerdo con la reivindicación 13, caracterizado además por:

encriptar la parte restante del segmento de datos utilizando el segundo juego de información de encriptación.

15. El método de acuerdo con la reivindicación 14, caracterizado además por:

generar un segmento de datos encriptado para cada uno de los segmentos de datos originales, el segmento de datos encriptado tiene una primera parte predeterminada, una segunda parte predeterminada y una parte restante, la primera parte predeterminada contiene los datos originales en la primera parte predeterminada correspondiente del segmento de datos original, la segunda parte predeterminada contiene los datos encriptados de la segunda parte predeterminada correspondiente del segmento de datos original, y la parte restante contiene los datos encriptados de la parte restante correspondiente del segmento de datos original.

16. El método de acuerdo con la reivindicación 15, caracterizado además por:

transmitir una pluralidad de segmentos de datos encriptados como una corriente de datos encriptados.

17. El método de acuerdo con la reivindicación 15, caracterizado además por:

almacenar una pluralidad de segmentos de datos en un dispositivo de almacenamiento de datos, cada segmento de datos encriptado corresponde a un sector de datos respectivo del dispositivo de almacenamiento de datos.

18. El método de acuerdo con la reivindicación 15, caracterizado además por:

recibir los datos encriptados que incluyen una pluralidad de segmentos de datos encriptados;

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

desencriptar los datos encriptados contenidos en la segunda parte predeterminada de cada segmento de datos encriptado utilizando el primer juego de información de encriptación seleccionado para el segmento de datos encriptado;

seleccionar, para cada segmento de datos encriptado, un segundo juego de información de encriptación basado en los datos encriptados de la segunda parte predeterminada; y

desencriptar la parte restante de cada segmento de datos encriptado utilizando el segundo juego de información de encriptación seleccionado para el segmento de datos encriptado.

19. El método de acuerdo con la reivindicación 18, en donde dicha selección de la primera información de encriptación está caracterizada por:
generar un primer valor desde lo datos originales contenidos en la primera parte predeterminada del segmento de datos encriptado.

20. El método de acuerdo con la reivindicación 19, en donde dicha generación del primer valor está caracterizada por comprender:
verificar los datos contenidos len la primera parte predeterminada utilizando una primera clave de verificación.

21. El método de acuerdo con la reivindicación 18, en donde dicha selección de la información de encriptación está caracterizada por comprender:
generar un segundo valor desde los datos desencriptados de la segunda parte predeterminada del segmento de datos encriptado.

22. El método de acuerdo con la reivindicación 21, en donde dicha generación del segundo valor está caracterizada por comprender:
verificar los datos desencriptados de la segunda parte predeterminada utilizando una segunda clave de verificación.

23. Un método para procesar criptográficamente datos, dicho método caracterizado por:

recibir una pluralidad de segmentos de datos encriptados, donde cada uno de los segmentos de datos encriptados tiene una parte predeterminada;

seleccionar, para cada segmento de datos encriptado un juego de información de encriptación basado en datos contenidos en la parte predeterminada del segmento de datos encriptado; y

desencriptar cada segmento de datos encriptado utilizando la información de encriptación seleccionada para el segmento de datos encriptado.

24. El método de acuerdo con la reivindicación 23, en donde dicha selección está caracterizada por:

generar para cada segmento de datos encriptado, un valor a partir de los datos contenidos en la parte predeterminada del segmento de datos encriptado y

seleccionar un juego de información de encriptación asociado con el valor generado, el juego de información de encriptación incluye un algoritmo de encriptación, una clave de encriptación, y optativamente un parámetro de encriptación.

25. El método de acuerdo con la reivindicación 24, en donde dicha generación de un valor está caracterizada por:

verificar los datos contenidos en la parte predeterminada utilizando una clave de verificación

26. El método de acuerdo con la reivindicación 25, caracterizado además por:

proveer una tabla de encriptación, la tabla de encriptación contiene:

un identificador de tipo de encriptación;

una clave de encriptación para el tipo de encriptación; y

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

27. El método de acuerdo con la reivindicación 23, en donde la parte predeterminada está caracterizada por :

una primera parte predeterminada para seleccionar un primer juego de información de encriptación, el primer juego comprende un primer algoritmo de encriptación, una primera clave de encriptación, y optativamente un primer parámetro de encriptación y

una segunda parte predeterminada para seleccionar un segundo juego de información de encriptación, el segundo juego comprende un segundo algoritmo de encriptación, una segunda clave de encriptación, y optativamente un segundo parámetro de encriptación.

28. El método de acuerdo con la reivindicación 27, en donde dicha recepción está caracterizada por:

recibir una corriente de datos encriptada que incluye una pluralidad de paquetes de datos encriptados, cada paquete de datos encriptados corresponde a un segmento de datos encriptado.

29. El método de acuerdo con la reivindicación 28, 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, en donde la primera capa de protocolo es más baja que la segunda capa de protocolo.

30. El método de acuerdo con la reivindicación 28, caracterizado porque la primera parte predeterminada es un encabezamiento de Protocolo de Internet (IP) del paquete datos.

31. El método de acuerdo con la reivindicación 30, 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.

32. El método de acuerdo con la reivindicación 27, en donde dicha recepción está caracterizada por:
leer la pluralidad de segmentos de datos encriptados desde sectores correspondientes en un dispositivo de almacenamiento de datos.

33. El método de acuerdo con la reivindicación 32, 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.

34. El método de acuerdo con la reivindicación 33, caracterizado porque los datos contenidos en la segunda parte predeterminada del segmento de datos encriptado se ha encriptado utilizando el primer juego de información de encriptación.

35. El método de acuerdo con la reivindicación 34, caracterizado porque los datos contenidos en la parte restante del segmento de datos encriptado utilizando el segundo juego de información de encriptación.

36. Un sistema para procesar criptográficamente datos, caracterizado por:

un buffer de entrada adaptado para recibir datos que incluyen una pluralidad de segmentos de datos,

un módulo de encriptación adaptado para encriptar cada segmento de datos,

un controlador conectado a dicho buffer de entrada y dicho módulo de encriptación, dicho controlador está adaptado para seleccionar un juego de información de encriptación para un segmento de datos corriente que debe encriptarse en base a los datos contenidos en una parte predeterminada del segmento de datos corriente y

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

37. El sistema de acuerdo con la reivindicación 1, caracterizado porque el controlador cambia al menos uno de un algoritmo de encriptación, una clave de encriptación y un parámetro de encriptación por cada segmento de datos.

38. El sistema de acuerdo con la reivindicación 36, en donde dicho módulo de encriptación está caracterizado por:
una pluralidad de motores de encriptación, cada motor de encriptación corresponde a un algoritmo de encriptación respectivo diferente uno de otro.

39. El sistema de acuerdo con la reivindicación 36, en donde dicho módulo de encriptación además está caracterizado por:
un buffer de datos conectado a cada uno de la pluralidad de motores de encriptación.

40. El sistema de acuerdo con la reivindicación 36, en donde dicho controlador está caracterizada por:
un selector de datos adaptado para seleccionar una parte predeterminada de cada segmento de datos;
un selector de encriptación conectado con dicho selector de datos, adaptado para seleccionar un juego de información de encriptación de acuerdo con datos contenidos en la parte predeterminada, el juego de información de encriptación incluye un algoritmo de encriptación, una clave de encriptación y optativamente un parámetro de encriptación; y
un controlador de encriptación adaptado para seleccionar y activar un motor de encriptación basado en la información de encriptación.

41. El sistema de acuerdo con la reivindicación 36, 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.

42. El sistema de acuerdo con la reivindicación 41, caracterizado porque el generador de valor está adaptado para verificar los datos contenidos en la parte predeterminada utilizando una clave de verificación.

43. El sistema de acuerdo con la reivindicación 41, en donde dicho controlador de encriptación está caracterizado por una tabla de encriptación que contiene:

un identificador de tipo de encriptación

una clave de encriptación para el tipo de encriptación y

un parámetro de encriptación

para cada entrada asociada con un valor generado.

44. El sistema de acuerdo con la reivindicación 36, en donde la parte predeterminada de cada segmento de datos está caracterizada por:

una primera parte predeterminada, y

una segunda parte predeterminada.

45. El sistema de acuerdo con la reivindicación 44, caracterizado porque la pluralidad de segmentos de datos son paquetes de datos en una corriente de datos.

46. El sistema de acuerdo con la reivindicación 45, en donde 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.

47. El sistema de acuerdo con la reivindicación 45, caracterizado porque la primera parte predeterminada es un encabezamiento de Protocolo de Internet (IP) del paquete de datos.

48. El sistema de acuerdo con la reivindicación 47, 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.

49. El sistema de acuerdo con la reivindicación 44, caracterizado porque la pluralidad de segmentos de datos son sectores en un dispositivo de almacenamiento de datos.

50. El sistema de acuerdo con la reivindicación 49, 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.

51. El sistema de acuerdo con la reivindicación 44, en donde dicho controlador está caracterizado por:

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

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

52. Un sistema para procesar criptográficamente datos, caracterizado por:

un buffer de entrada adaptado para recibir una pluralidad de segmentos de datos encriptados, cada uno de los segmentos de datos encriptados tiene una parte predeterminada

un módulo de encriptación adaptado para desencriptar cada segmento de datos encriptado;

un controlador conectado a dicho buffer de entrada y dicho módulo de encriptación, dicho controlador está adaptado para seleccionar un juego de información de encriptación para un segmento de datos encriptado corriente que debe desencriptarse en base a datos contenidos en una parte predeterminada del segmento de datos encriptado corriente; y

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

53. El sistema de acuerdo con la reivindicación 52, en donde dicho módulo de desencriptación está caracterizado por:
una pluralidad de motores de desencriptación, cada motor de desencriptación corresponde a un algoritmo de encriptación respectivo.

54. El sistema de acuerdo con la reivindicación 52, en donde dicho módulo de desencriptación además está caracterizado por:
un buffer de datos conectado a cada uno de la pluralidad de motores de desencriptación.

55. El sistema de acuerdo con la reivindicación 52, en donde dicho controlador está caracterizado por:
un selector adaptado para seleccionar una parte predeterminada de cada segmento de datos encriptado;
un selector de desencriptación conectado con el selector de datos, adaptado para seleccionar un juego de información de desencriptación de acuerdo con datos contenidos en la parte predeterminada, el juego de información de desencriptación incluye un algoritmo de encriptación, una clave de encriptación, y optativamente un parámetro de encriptación y
un controlador de desencriptación adaptado para seleccionar y activar un motor de desencriptación basado en la información de encriptación.

56. El sistema de acuerdo con la reivindicación 52, 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.

57. El sistema de acuerdo con la reivindicación 56, caracterizado porque el generador de valor está adaptado para verificar los datos contenidos en la parte predeterminada utilizando una clave de verificación

58. El sistema de acuerdo con la reivindicación 56, en donde dicho controlador de desencriptación está caracterizado por una tabla de encriptación que contiene:
un identificador de tipo de encriptación
una clave de encriptación para el tipo de encriptación y
un parámetro de encriptación
para cada entrada asociada con un valor generado.

59. El sistema de acuerdo con la reivindicación 52, en donde la parte predeterminada de cada segmento de datos está caracterizada por:
una primera parte predeterminada y
una segunda parte predeterminada.

60. El sistema de acuerdo con la reivindicación 59, caracterizado porque la pluralidad de segmentos de datos son paquetes de datos en una corriente de datos.

61. El sistema de acuerdo con la reivindicación 60, 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.

62. El sistema de acuerdo con la reivindicación 60, caracterizado porque la primera parte predeterminada es un encabezamiento de Protocolo de Internet (IP) del paquete de datos.

63. El sistema de acuerdo con la reivindicación 62, 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.

64. El sistema de acuerdo con la reivindicación 52, caracterizado porque la pluralidad de segmentos de datos son sectores en un dispositivo de almacenamiento de datos.

65. El sistema de acuerdo con la reivindicación 64, 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.

66. El sistema de acuerdo con la reivindicación 52, en donde dicho controlador está caracterizado por:

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

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

67. Un sistema para procesar criptográficamente datos, dicho sistema caracterizado porque comprende:

un medio para recibir una pluralidad de segmentos de datos

un medio para seleccionar, para cada segmento de datos, un juego de información de encriptación basado en datos contenidos en una parte predeterminada del segmento de datos a ser encriptado;

un medio para encriptar cada segmento de datos utilizando el juego de información de encriptación seleccionado del segmento de datos.

68. El sistema de acuerdo con la reivindicación 67, caracterizado porque el medio para seleccionar cambia al menos uno de un algoritmo de encriptación, una clave de encriptación y un parámetro de encriptación para cada segmento de datos basado en los datos contenidos en la parte predeterminada.

69. El sistema de acuerdo con la reivindicación 67, en donde dicho medio para seleccionar está caracterizado por:

un medio para generar, para cada segmento de datos, un va... partir de datos contenidos en la parte predeterminada del segmento de datos; y

un medio para seleccionar un juego de información de encriptación asociado con el valor generado, el juego de información de encriptación incluye un algoritmo de encriptación, una clave de encriptación y optativamente un parámetro de encriptación.

70. El sistema de acuerdo con la reivindicación 69, en donde dicho medio para generar un valor está caracterizado por:

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

71. El sistema de acuerdo con la reivindicación 69, caracterizado además por:

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

72. El sistema de acuerdo con la reivindicación 67, en donde la parte predeterminada está caracterizada por:

una primera parte predeterminada para seleccionar un primer juego de información de encriptación, el primer juego que comprende una primer algoritmo de encriptación, una primera clave de encriptación, y optativamente un primer parámetro de encriptación, y

una segunda parte predeterminada para seleccionar un segundo juego de información de encriptación, el segundo juego que comprende una segundo algoritmo de encriptación, una segunda

clave de encriptación, y optativamente un segundo parámetro de encriptación.

73. El sistema de acuerdo con la reivindicación 72, caracterizado además por:
un medio para encriptar la segunda parte predeterminada utilizando el primer juego de información de encriptación.

74. El sistema de acuerdo con la reivindicación 73, caracterizado además por:
un medio para encriptar la parte restante del segmento de datos utilizando el segundo juego de información de encriptación.

75. Un sistema para procesar criptográficamente datos, dicho sistema caracterizado porque comprende:
un medio para recibir una pluralidad de segmentos de datos encriptados, cada uno de los segmentos de datos encriptados tiene una parte predeterminada,
un medio para seleccionar, para cada segmento de datos encriptados, un juego de información de encriptación basado en datos contenidos en la parte predeterminada del segmento de datos encriptado,
un medio para desencriptar el segmento de datos encriptado utilizando la información de encriptación seleccionada para el segmento de datos encriptado.

76. El sistema de acuerdo con la reivindicación 75, en donde dicho medio para seleccionar está caracterizado por:

un medio para generar, para cada segmento de datos encriptado, un valor a partir de datos contenidos en la parte predeterminada del segmento de datos encriptado, y

un medio para seleccionar un juego de información de encriptación asociado con el valor generado, el juego de información de encriptación incluye un algoritmo de encriptación, una clave de encriptación y optativamente un parámetro de encriptación.

77. El sistema de acuerdo con la reivindicación 76, en donde dicho medio para generar un valor está caracterizado por:

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

78. El sistema de acuerdo con la reivindicación 78, caracterizado además por:

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

79. El sistema de acuerdo con la reivindicación 75, en donde la parte predeterminada está caracterizada por:

una primera parte predeterminada para seleccionar un primer juego de información de encriptación, el primer juego comprende un primer algoritmo de encriptación, una primera clave de encriptación y optativamente un primer parámetro de encriptación; y

una segunda parte predeterminada para seleccionar un segundo juego de información de encriptación, el segundo juego

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

80. El sistema de acuerdo con la reivindicación 79, caracterizado porque los datos contenidos en la segunda parte predeterminada del segmento de datos encriptado se han encriptado utilizando el primer juego de información de encriptación.

81. El sistema de acuerdo con la reivindicación 80, caracterizado porque los datos contenidos en la parte restante del segmento de datos encriptado se han encriptado utilizando el segundo juego de información de encriptación.

341

RESUMEN DE LA INVENCIÓN

Un método para procesar criptográficamente datos 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 juego de información de encriptación basado en datos contenidos en una parte predeterminada del segmento de datos que debe encriptarse (102, 140) y (c) encriptar cada segmento de datos utilizando el juego de información de encriptación seleccionado para el segmento de datos (106). Al menos uno de un algoritmo de encriptación, una clave de encriptación, y un parámetro de encriptación puede cambiarse 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 juego de información de encriptación, y una segunda parte predeterminada para seleccionar un segundo juego de información de encriptación, la información de encriptación incluye un algoritmo de encriptación, una clave de encriptación y optativamente un parámetro de encriptación.