Industria y Comercio

SUPERINTENDENCIA

Delegatura de Propiedad Industrial

División de Nuevas Creaciones

PCT

SOLICITUD

PATENTE DE INVENCION

21. **EXPEDIENTE No.** 06-09165

54. **TITULO** METODO Y APARATO PARA PROCESAR CRIPTOGRAFICAMENTE DATOS.

51. **CLASIFICACION INTERNACIONAL**

71. **SOLICITANTE** PSYCRYPT, INC.

DOMICILIO CALIFORNIA, USA

74. **APODERADO** CARLOS ORLANDO MAYA RODRIGUEZ

22. **BOGOTA, D.C.,** 11 AGOSTO / 2006.

Poder, Cesión, Anexos

F.N. 13-09-2006

(FORMA P-10)

1/159

PETITORIO

Industria y Comercio
SUPERINTENDENCIA

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO
Rad: 06-079165- -00000-0000
Esp Fec: 2006-08-11 12:57:21 Dep: 2020 NUEGREACIONES
Tra: 11 PATENTE(YII
Eve: 379 FASENACIONALII
Art 411 PRESENTACION Folios: 159

FORMULARIO UNICO DE SOLICITUD DE PATENTE

PCT

ENTRADA EN FASE NACIONAL

1. SOLICITUD DE:

[X] Patente de Invención [ ] Patente de Modelo de Utilidad

[ ] Capitulo I [X] Capitulo II

2. SOLICITANTE (71)	Nombre **PSYCRYPT, INC.** Dirección Suite 213, 2635 North First Street, San Jose, CA 95139, EE UU Nacionalidad o Domicilio California, EEUU Lugar de Constitución Teléfono Fax E-mail	**IDENTIFICACION** C C [ ] NIT [ ] C E [ ] Otro [ ] Cual Número
3. REPRESENTANTE O APODERADO	Nombre **CARLOS ORLANDO MAYA RODRIGUEZ** Direccion **Cr. 13 A No 28-38, Mz 2 Bufete 245. Parque Central Bavaria** Teléfono **3419841** Fax **3368592** E-mail **pct@tmtamayo.net**	**IDENTIFICACION** C C [ ] NIT [ ] C E [ ] Otro [ ] Cual Número **17.117.818** TP **17.402**
4. INVENTOR(ES) .(72)	Nombres **WATANABE, Masashi** Dirección 49-1, Machisuji, Iwawaki, Hanoura-cho, Naka-gun, Tokushima, Japón. Nacionalidad o Domicilio Ciudadano de Japón	

5. PCT (86)

Solicitud internacional No **PCT/US2004/004117** Fecha **13/02/2004**

Publicación internacional No **WO 2005/088893 A1** Fecha **22/09/2005**

6. Título (54)
MÉTODO Y APARATO PARA PROCESAR CRIPTOGRÁFICAMENTE DATOS

7. Clasificación Internacional (51) **H04L9/00**

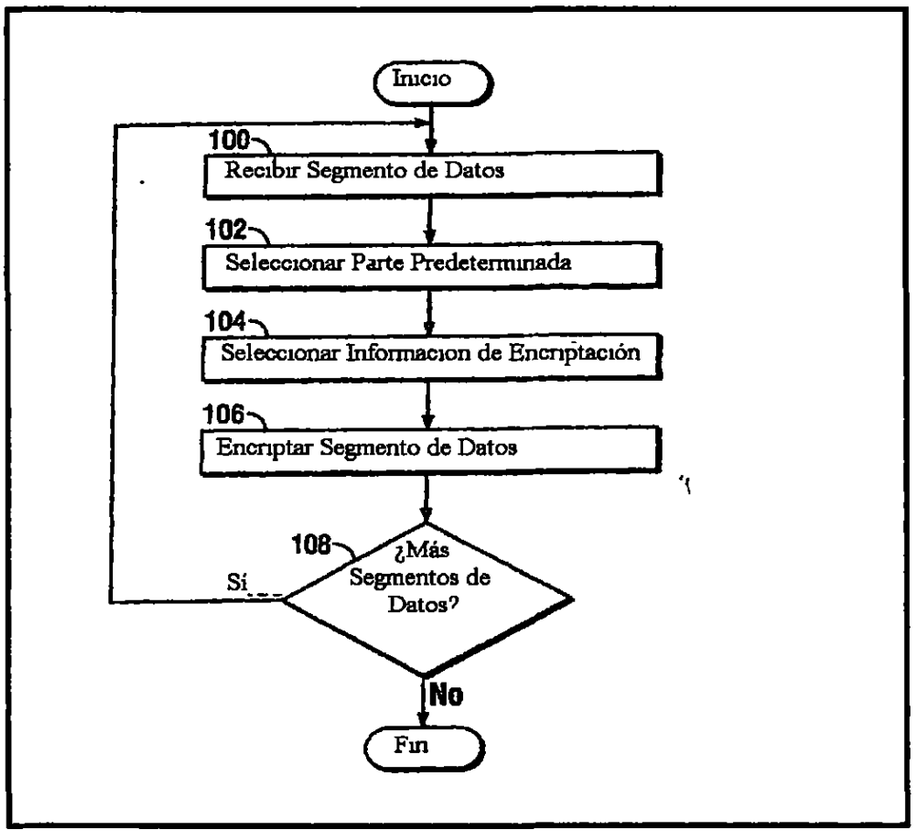
8. Prioridad Si [X] No [ ]	**(33) País de Origen**	**(32) Fecha**	**(31) Número deSolicidud**
	EE.UU	13/02/2004	PCT/US2004/004117

9. Comprobante de pago No **06 - 59,713** Fecha **AGOSTO 8/2006**

10. Anexos

- [X] Comprobante de pago de la tasa de presentacion de la solicitud
- [ ] Documento que acredita la existencia y representación legal cuando el solicitante sea persona juridica
- [ ] Poderes, si fuere el caso
- [ ] Documento de cesion del inventor al solicitante o a su causante
- [ ] Declaraciones
- [ ] Copia de la solicitud Internacional (Resumen, descripcion, reivindicaciones, dibujos)
- [X] Traduccion de la solicitud internacional al castellano (Resumen, descripción, reivindicaciones, dibujos)
- [ ] Copia del examen preliminar internacional efectuado por la Autoridad Internacional de Examen Preliminar (IPEA)
- [ ] Traduccion del examen preliminar internacional efectuado por la IPEA
- [ ] De ser el caso, copia del contrato de acceso
- [ ] De ser el caso, documento que acredite la licencia o autorización de uso de conocimientos tradicionales de las comunidades indígenas
- [ ] De ser el caso, certificado de deposito del material biologico
- [X] Arte final 12 x 12
- [ ] De ser el caso, información sobre otras solicitudes de patente o títulos obtenidos en el extrajero por el mismo titular o su causante, relacionadas parcial o totalmente con la invencion de esta solicitud
- [ ] De ser el caso, modificaciones efectuadas a la solicitud internacional
- [X] Otros (FOTOCOPIA DE LA PUBLICACION INTERNACIONAL)

11. FIGURA CARACTERISTICA



12. Solicito la concesión de la patente,

NOMBRE **CARLOS ORLANDO MAYA RODRIGUEZ**

FIRMA

C C **17.117.818** TP **17.402**

RECIBO DE CAJA APLICADO AL EXPEDIENTE No._____

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO
Rad: 06-079165- -00000-0000
Fec 2006-08-11 12 57 21 Dep 2020 NUEVCREACIONES
Tra 11 PATENTEIYII
Eve 379 FASENACIONALII
Act 411 PRESENTACION Folios 1 En

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

NIT : 800176089-2

RECIBO OFICIAL DE CAJA : 06 - 59,713
FECHA : AGOSTO 8 DE 2006

C O N S I G N A C I O N

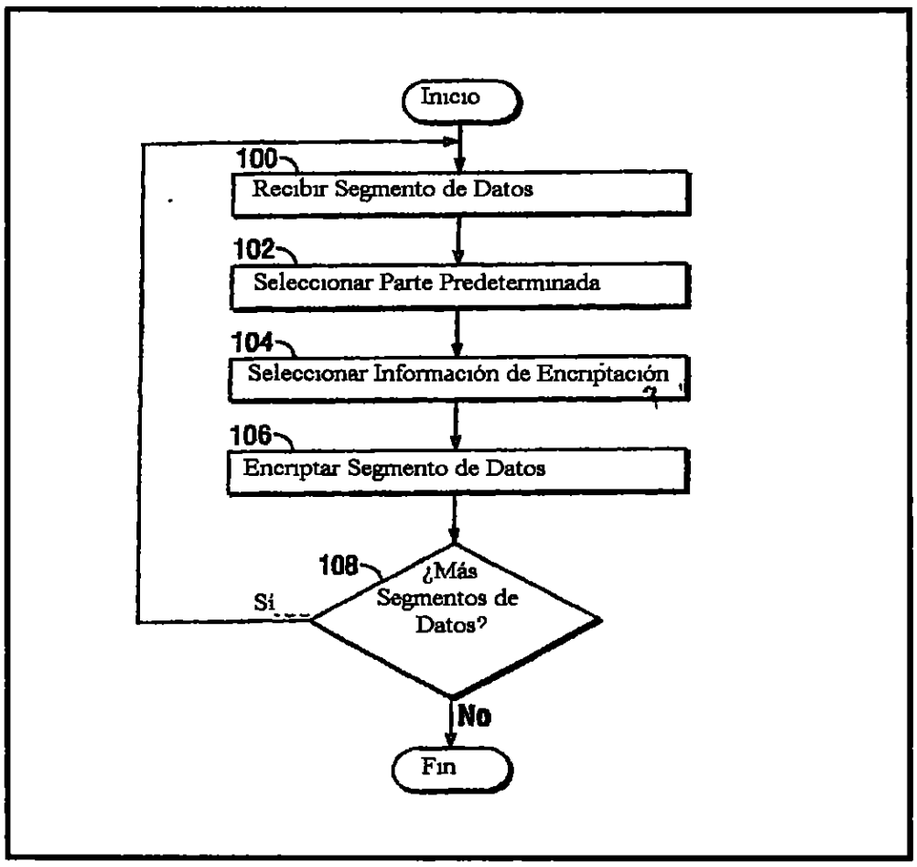
DEPOSITANTE	TIPO PAGO	BANCO	CUENTA	No. PAGO	FECHA PGO	Vr. PAGO
CARLOS TAMAYO Y ASOCIADOS	CONSIGNACION	BANCO POPULAR	050-00110-6	48873649	08/08/2006	532,000.00

C O N C E P T O

CANT.	RENTISTICO	CONCEPTO	TOTAL CONCEPTO
1	50005-01-01 SOLICITUDES	1 TRAMITES DE SOL. DE PATENTE DE IN	463,000.00
		TOTAL : $	463,000.00

SON: CUATROCIENTOS SESENTA Y TRES MIL PESOS

RESPONSABLE : _____


Inicio
100
Recibir Segmento de Datos
102
Seleccionar Parte Predeterminada
104
Seleccionar Información de Encriptación
106
Encriptar Segmento de Datos
108
¿Más Segmentos de Datos?
Si
No
Fin

Industria y Comercio
SUPERINTENDENCIA

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO
DIVISION DE NUEVAS CREACIONES
EXTRACTO PARA PUBLICACIÓN
SOLICITUD DE PATENTE DE INVENCIÓN PCT

(21) N° de solicitud	(51) Int Cl **H04L9/00**
22) Fecha de solicitud **11-08-2006**	(71)Solicitante(s) **PSYCRYPT, INC.**
(30) Prioridad (31) ***No. Prioridad*** 32) ***Fecha*** (33) ***País*** SI **PCT/US2004/004117** **13/02/2004** **US**	(72) Inventor(es) **WATANABE, Masashi**
	(74) Apoderado **CARLOS ORLANDO MAYA RODRIGUEZ**
(85) Fecha límite inicio fase nacional *13/08/06*	(87) Publicación internacional
(86) Datos relativos a la presentación de la solicitud PCT	Fecha **22 Septiembre 2005**
Fecha de presentación de la solicitud **13/02/2004**	N° publicación **WO 2005/088893 A1**
No de solicitud **PCT/US2004/004117**	

(54) Título **MÉTODO Y APARATO PARA PROCESAR CRIPTOGRÁFICAMENTE DATOS**

Reivindicación(es)

Un metodo para procesar criptográficamente datos, dicho método comprende

recibir una pluralidad de segmentos de datos,

seleccionar un juego de información de encriptación para un segmento de datos corriente que debe encriptarse basado en datos contenidos en una parte predeterminada del segmento de datos corriente,

encriptar el segmento de datos corriente utilizando el juego de información de encriptación seleccionado para el segmento de datos corriente, y

repetir dicha selección y dicha encriptacion para segmentos de datos posteriores

MÉTODO Y APARATO 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 aparato 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 descriptar 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 descriptarlos. 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 y aparato procesan 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 descriptar 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) descriptar 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 descriptados de la segunda parte predeterminada, (c2) descriptar 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 aparato 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 aparato 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 aparato 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 aparato 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 aparato puede incluir además un medio para transmitir una pluralidad de segmentos de datos encriptados como una corriente de datos encriptados. El aparato 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 aparato 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 descriptar 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 descriptados de la segunda parte predeterminada, y (c2) descriptar la parte restante de cada segmento de datos encriptado utilizando el segundo juego de información de

encripotación seleccionado para el segmento de datos encripotado.

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 descriptados 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 descriptados de la segunda parte predeterminada utilizando una clave de verificación.

De acuerdo con un aspecto de la invención, el aparato para descriptar 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 descriptar 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 aparato 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 aparato para encriptar/descriptar datos de acuerdo con una realización de la presente invención.

La Figura 1B es un diagrama de bloques que ilustra esquemáticamente una parte de descriptación de un aparato para encriptar/descriptar 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/descriptar 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 descriptar 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 descriptar 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/descriptador 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 aparato de encriptación/descriptación 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 aparato para encriptar y descriptar 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 aparato 10 para encriptar/descriptar datos de acuerdo con una realización de

la presente invención. Como se muestra en la Figura 1 A, el aparato 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 aparato 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 aparato 10 también se puede utilizar para comunicaciones seguras a través de la WAN, la Internet, red inalámbrica, y

similares. Más aún, el aparato 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 aparato 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 inicíala 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 aparato 10. La Figura 1B ilustra esquemáticamente una parte de descriptación correspondiente 10' del aparato 10 de acuerdo con una realización de la presente invención. Como se muestra en la Figura 1B, la parte de descriptación 10' puede construirse simétricamente a la parte de encriptación (Figura 1A) del aparato 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/descriptar datos de acuerdo con una realización de la presente invención. El método puede ser ejecutado por el aparato de encriptación/descriptación 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 aparato de encriptacón/descriptación 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 descriptar 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 descriptar 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 descripta 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 descriptados 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 descripta 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 descriptado (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 descriptado (146).

La Figura 13 ilustra esquemáticamente un encriptador/descriptador 150 de acuerdo con una realización de la presente invención. Como se muestra en la Figura 13, el encriptador/descriptador 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 descriptación (R) 166, y un segundo buffer de datos 168. El módulo de encriptación 156 puede ser la parte de encriptación del aparato de encriptación/descriptación 10 (módulo de encriptación 14 y el controlador 16) descrito anteriormente, y el módulo de descriptación 166 puede ser la parte de encriptación 10' del aparato de encriptación/descriptación 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/descriptador 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/descriptación para la corriente de datos correspondiente de manera tal que los datos encriptados/descriptados se combinan correctamente en los respectivos segmentos de datos encriptados/descriptados (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/descriptador de datos 150 (y el aparato de encriptación/descriptación 10) puede implementarse en una forma de tarjeta enchufable para una computadora. Dado que la totalidad de los componentes necesarios para la encriptación/descriptación se proveen en el encriptador/descriptador (tarjeta de

encriptación/descriptación), el usuario/computadora no tiene que instalar ningún programa de software específico para la encriptación1/descriptación siempre que la computadora pueda utilizar la tarjeta de encriptación/descriptación (es decir compatible con la puerta). Simplemente transmitiendo o almacenando datos a través de la tarjeta de encriptación/descriptación, 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/descriptación 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 aparato de encriptación/descriptación, debe utilizarse para descriptar los datos encriptados. El "mismo" significa que la tarjeta o aparato 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/descriptación 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/descriptación 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/descriptación puede implementarse en dispositivos lógicos programables de campo (FPLD), tales como FPGA y CPLD, la tarjeta o aparato de encriptación/descriptación 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 aparatos de encriptación/descriptación respectivos 190, 192 y 194 de acuerdo con una realización de la presente invención. Los aparatos de encriptación/descriptación 190, 192 y 194 pueden ser el aparato de encriptación/descriptación 10 o el encriptador/descriptador 150 que se describieron anteriormente. La totalidad de los aparatos de encriptación/descriptación 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 aparato de encriptación/descriptación puede utilizarse mediante más de una computadora 184 y 186. Por ejemplo, el aparato de encriptación/descriptación 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/descriptación 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.

46

REIVINDICACIONES

1. Un método para procesar criptográficamente datos, dicho método comprende:

recibir una pluralidad de segmentos de datos;

seleccionar un juego de información de encriptación para un segmento de datos corriente que debe encriptarse basado en datos contenidos en una parte predeterminada del segmento de datos corriente;

encriptar el segmento de datos corriente utilizando el juego de información de encriptación seleccionado para el segmento de datos corriente; y

repetir dicha selección y dicha encriptación para segmentos de datos posteriores.

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

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

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

47

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

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

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

5. El método de acuerdo con la reivindicación 3, que además comprende:

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 comprende:

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 comprende:

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, 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.

9. El método de acuerdo con la reivindicación 7, en donde 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, en donde 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, en donde 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 11, en donde 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, que además comprende:
encriptar la segunda parte predeterminada utilizando el primer juego de información de encriptación.

80

14. El método de acuerdo con la reivindicación 13, que además comprende:

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, que además comprende:

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, que además comprende:

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

17. El método de acuerdo con la reivindicación 15, que además comprende:

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, que además comprende:

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;

descriptar 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

descriptar 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 comprende:
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 comprende:
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 comprende:
generar un segundo valor desde los datos descriptados 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 comprende:
verificar los datos descriptados de la segunda parte predeterminada utilizando una segunda clave de verificación.

23. Un método para procesar criptográficamente datos, dicho método comprende:

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

seleccionar un juego de información de encriptación para un segmento de datos encriptado corriente que debe descriptarse basado en datos contenidos en la parte predeterminada del segmento de datos encriptado;

descriptar el segmento de datos encriptado corriente utilizando la información de encriptación seleccionada para el segmento de datos encriptado corriente; y

repetir dicha selección y dicha descriptación para segmentos de datos encriptados posteriores.

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

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

seleccionar un juego de información de encriptación asociada 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 comprende:

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

26. El método de acuerdo con la reivindicación 25, que además comprende:

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 comprende:

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 comprende:
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, 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, 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, en donde la primera parte predeterminada es un encabezamiento de Protocolo de Internet (IP) del paquete datos.

31. El método de acuerdo con la reivindicación 28, en donde 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 comprende:

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, en donde 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 27, en donde 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, en donde los datos contenidos en la parte restante del segmento de

datos encriptado utilizando el segundo juego de información de encriptación.

36. Un aparato para procesar criptográficamente datos, que comprende:

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

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

37. El aparato de acuerdo con la reivindicación 36, en donde el controlador cambia al menos uno de un algoritmo de encriptación, una clave de encriptación y un parámetro de encriptación para cada segmento de datos.

38. El aparato de acuerdo con la reivindicación 36, en donde el módulo de encriptación comprende:
una pluralidad de motores de encriptación, cada motor de encriptación corresponde a un algoritmo de encriptación respectivo diferente uno de otro.

39. El aparato de acuerdo con la reivindicación 36, en donde el módulo de encriptación además comprende:
un buffer de datos conectado a cada uno de la pluralidad de motores de encriptación.

40. El aparato de acuerdo con la reivindicación 36, en donde el controlador comprende:
un selector de datos adaptado para seleccionar una parte predeterminada de cada segmento de datos
un selector de encriptación conectado con el 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 aparato de acuerdo con la reivindicación 36, en donde el controlador además comprende:
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 aparato de acuerdo con la reivindicación 41, en donde el generador de valor está adaptado para verificar los datos contenidos en la parte predeterminada utilizando una clave de verificación.

43. El aparato de acuerdo con la reivindicación 41, en donde el controlador de encriptación comprende 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 aparato de acuerdo con la reivindicación 36, en donde la parte predeterminada de cada segmento de datos comprende:
una primera parte predeterminada, y
una segunda parte predeterminada.

45. El aparato de acuerdo con la reivindicación 44, en donde la pluralidad de segmentos de datos son paquetes de datos en una corriente de datos.

46. El aparato 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 aparato de cuerdo con la reivindicación 45, en donde la primera parte predeterminada es un encabezamiento de Protocolo de Internet (IP) del paquete de datos.

48. El aparato de acuerdo con la reivindicación 47, en donde 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 método de acuerdo con la reivindicación 44, en donde la pluralidad de segmentos de datos son sectores en un dispositivo de almacenamiento de datos.

50. El aparato de acuerdo con la reivindicación 49, en donde 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 aparato de acuerdo con la reivindicación 44, en donde el controlador comprende:

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 aparato para procesar criptográficamente datos, que comprende:

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

62

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

un controlador conectado al buffer de entrada y el módulo de encriptación, el controlador está adaptado para seleccionar un juego de información de encriptación para un segmento de datos encriptado corriente que debe descriptarse basado en datos contenidos en una parte predeterminada del segmento de datos encriptado corriente; y

un buffer de salida conectado al controlador y al módulo de descriptación, el buffer de salida está adaptado para hacer salir datos descriptados que incluyen una pluralidad de segmentos de datos descriptados.

53. El aparato de acuerdo con la reivindicación 52, en donde el módulo de descriptación comprende:

una pluralidad de motores de descriptación, cada motor de descriptación corresponde a un algoritmo de encriptación respectivo diferente uno de otro.

54. El aparato de acuerdo con la reivindicación 52, en donde el módulo de descriptación además comprende:

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

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

56. El aparato de acuerdo con la reivindicación 52, en donde el controlador además comprende:
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 aparato de acuerdo con la reivindicación 56, en donde el generador de valor está adaptado para verificar los datos contenidos en la parte predeterminada utilizando una clave de verificación

58. El aparato de acuerdo con la reivindicación 56, en donde el controlador de descriptación comprende una tabla de encriptación que contiene:
un identificador de tipo de encripotación
una clave de encriptación para el tipo de encriptación y
un parámetro de encriptación
para cada entrada asociada con un valor generado.

59. El aparato de acuerdo con la reivindicación 52, en donde la parte predeterminada de cada segmento de datos comprende:
una primera parte predeterminada y
una segunda parte predeterminada.

60. El aparato de acuerdo con la reivindicación 59, en donde la pluralidad de segmentos de datos son paquetes de datos en una corriente de datos.

61. El aparato de acuerdo con la reivindicación 60, en donde la primera parte predeterminada contiene datos para una primera capa de protocolo, 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 aparato de acuerdo con la reivindicación 60, en donde la primera parte predeterminada es un encabezamiento de Protocolo de Internet (IP) del paquete de datos.

63. El aparato de acuerdo con la reivindicación 62, en donde la segunda parte predeterminada es uno 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 método de acuerdo con la reivindicación 52, en donde la pluralidad de segmentos de datos son sectores en un dispositivo de almacenamiento de datos.

65. El aparato de acuerdo con la reivindicación 64, en donde 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 aparato de acuerdo con la reivindicación 52, en donde el controlador comprende:

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 aparato para procesar criptográficamente datos, dicho aparato comprende:

un medio para recibir una pluralidad de segmentos de datos

un medio para seleccionar un juego de información de encriptación para un segmento de datos corriente que debe encriptarse basado en datos contenidos en una parte predeterminada del segmento de datos corriente

un medio para encriptar el segmento de datos corriente utilizando el juego de información de encriptación seleccionado del segmento de datos corriente y

un medio para permitir que el medio para seleccionar y el medio para encriptar para operar en segmentos de datos posteriores.

68. El aparato de acuerdo con la reivindicación 67, en donde 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 aparato de acuerdo con la reivindicación 167, en donde el medio para seleccionar comprende:
un medio para generar, para cada segmento de datos corriente, un valor a partir de datos contenidos en la parte predeterminada del segmento de datos corriente; 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 aparato de acuerdo con la reivindicación 69, en donde el medio para generar un valor comprende:
un medio para verificar los datos contenidos en la parte predeterminada utilizando una clave de verificación.

71. El aparato de acuerdo con la reivindicación 69, que además comprende:
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.

68

72. El aparato de acuerdo con la reivindicación 67, en donde la parte predeterminada comprende:

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 aparato de acuerdo con la reivindicación 72, que además comprende:

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

74. El aparato de acuerdo con la reivindicación 71, que además comprende:

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

75. El aparato de acuerdo con la reivindicación 74, que además comprende:

un medio para 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.

76. El aparato de acuerdo con la reivindicación 75, que además comprende:

un medio para transmitir una cantidad de segmentos de datos encriptados como una corriente de datos encriptados.

77. El aparato de acuerdo con la reivindicación 75, que además comprende:

un medio para almacenar una pluralidad de segmentos de datos encriptados 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.

78. El aparato de acuerdo con la reivindicación 75, que además comprende:

un medio para recibir los datos encriptados que incluye una pluralidad de segmentos de datos encriptados;

un medio para 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;

un medio para descriptar los datos encriptados contenidos en la segunda parte predeterminada de cada segmento de datos encriptado utilizando el primer juego de información de encriptación seleccionada para el segmento de datos encriptado;

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

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

78. El aparato de acuerdo con la reivindicación 78, en donde el medio para seleccionar la primera información de encriptación comprende:

un medio para generar un primer valor a partir de los datos originales contenidos en la primera parte predeterminada del segmento de datos encriptado.

80. El aparato de acuerdo con la reivindicación 79, en donde el 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.

81. El aparato de acuerdo con la reivindicación 78, en donde el medio para seleccionar la segunda información de encriptación comprende:
un medio para generar un segundo valor a partir de los datos descriptados de la segunda parte predeterminada del segmento de datos encriptado.

82. El aparato de acuerdo con la reivindicación 81, en donde el medio para verificar los datos descriptados de la segunda parte predeterminada utilizando una segunda clave de verificación.

83. Un aparato para procesar criptográficamente datos, dicho aparato 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 un juego de información de descriptación para un segmento de datos encriptado corriente que debe descriptarse basado en datos contenidos en la parte predeterminada del segmento de datos encriptado corriente,

un medio para descriptar el segmento de datos encriptado corriente utilizando la información de encriptación seleccionada para el segmento de datos encriptado corriente, y

un medio para permitir que dicho medio para seleccionar y dicho medio para descriptar operen sobre segmentos de datos encriptados posteriores.

84. El aparato de acuerdo con la reivindicación 83, en donde dicho medio para seleccionar comprende:

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

85. El aparato de acuerdo con la reivindicación 84, en donde dicho medio para generar un valor comprende:
un medio para verificar los datos contenidos en la parte predeterminada utilizando una clave de verificación.

86. El aparato de acuerdo con la reivindicación 85, que además comprende:
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.

87. El aparato de acuerdo con la reivindicación 83, en donde la parte predeterminada comprende:
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.

88. El aparato de acuerdo con la reivindicación 87, en donde los datos contenidos en la segunda parte predeterminada del segmento de datos encriptado se han encriptado utilizando el primer juego de información encriptación.

89. El aparato de acuerdo con la reivindicación 88, en donde los datos contenidos en la parte restante del segmento de datos encriptado se han encriptado utilizando el segundo juego de información encriptada.

75

RESUMEN DE LA INVENCIÓN

Un método y aparato procesa 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 debe encriptarse 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 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.

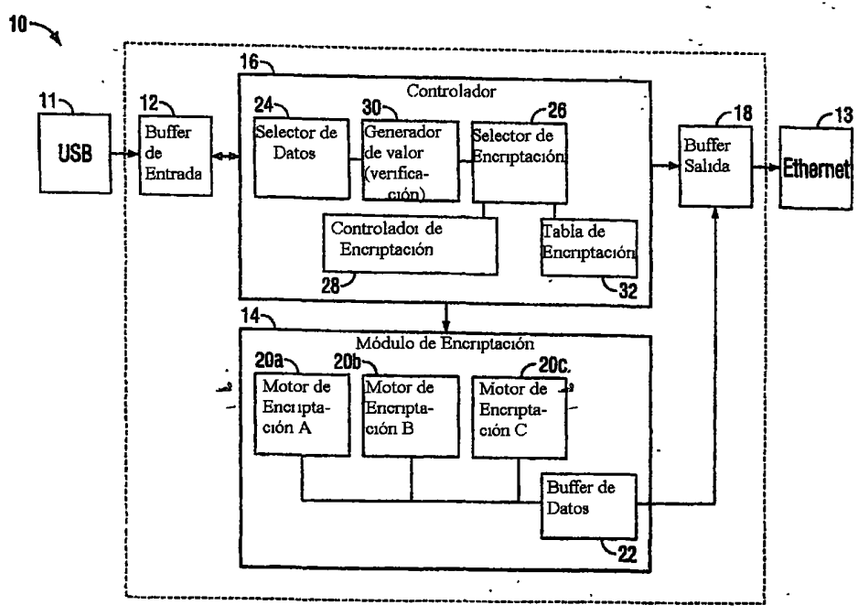

10
16
Controlador
11
USB
12
Buffer de Entrada
24
Selector de Datos
30
Generador de valor (verificación)
26
Selector de Encriptación
18
Buffer Salida
13
Ethernet
Controlador de Encriptación
28
Tabla de Encriptación
32
14
Módulo de Encriptación
20a
Motor de Encriptación A
20b
Motor de Encriptación B
20c.
Motor de Encriptación C
Buffer de Datos
22

FIG. 1A

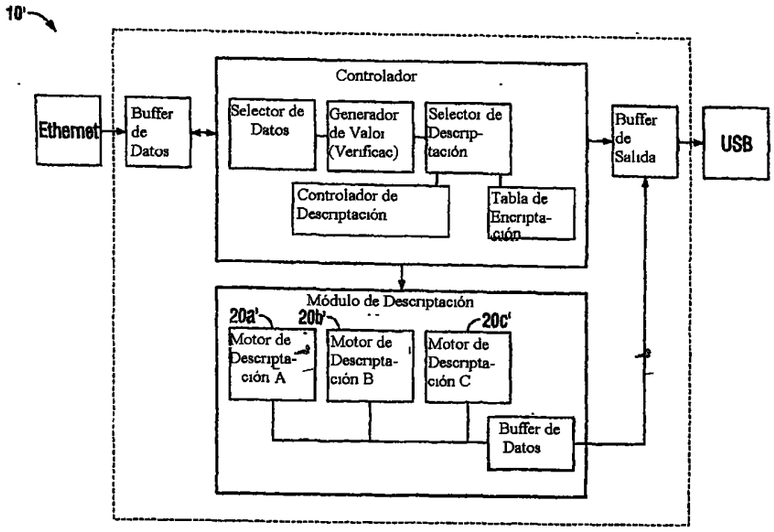

10'
Ethernet
Buffer de Datos
Controlador
Selector de Datos
Generador de Valor (Verificac)
Selector de Descrip-tación
Controlador de Descriptación
Tabla de Encripta-ción
Buffer de Salida
USB
Módulo de Descriptación
20a'
20b'
20c'
Motor de Descripta-ción A
Motor de Descripta-ción B
Motor de Descripta-ción C
Buffer de Datos

FIG. 1B

78

32

Índice	Tipo Encriptación	Clave	Vector Inicial
0	3 DES	Clave 1	5
1	AES	Clave 2	2
2	3 DES	Clave 3	7
3	IDEA	Clave 4	8
4	AES	Clave 5	3
⋮	⋮	⋮	⋮

FIG. 2

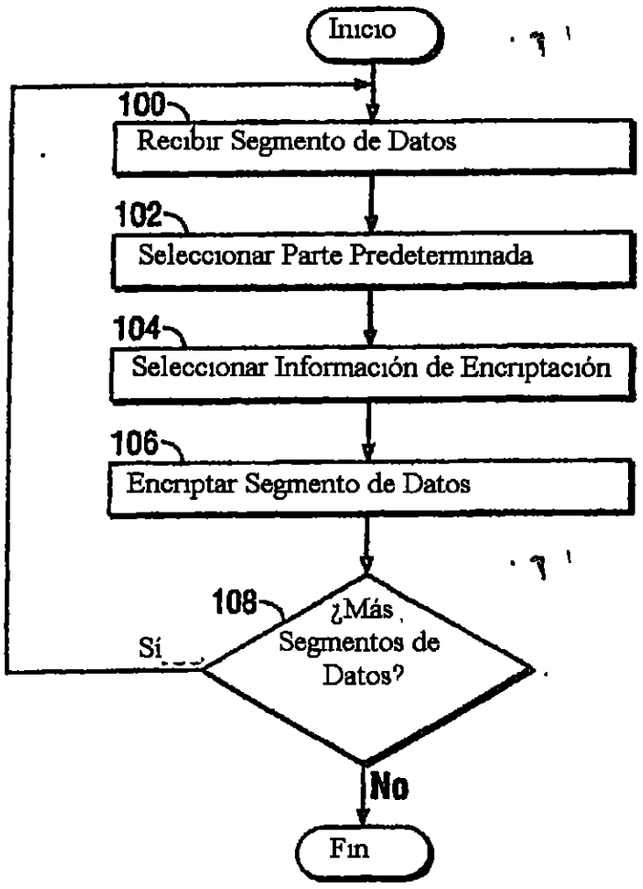
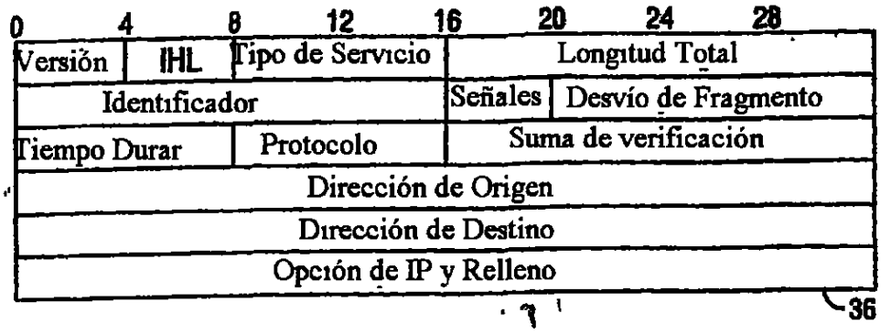


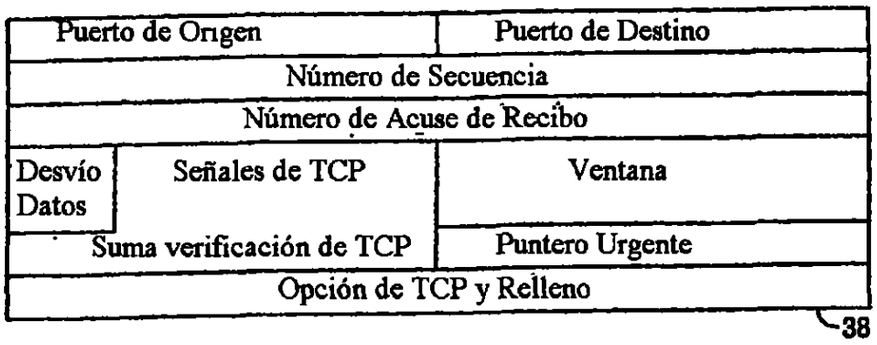
FIG. 3

34

Protocolo de IP



Encabezamiento de TCP



Datos de TCP

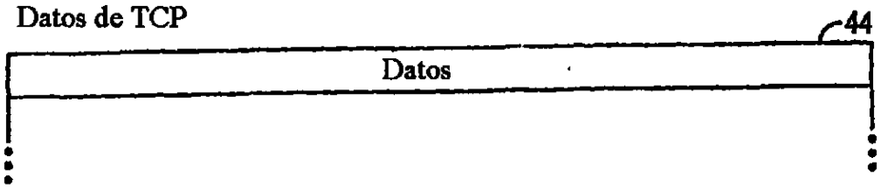


FIG. 4

80

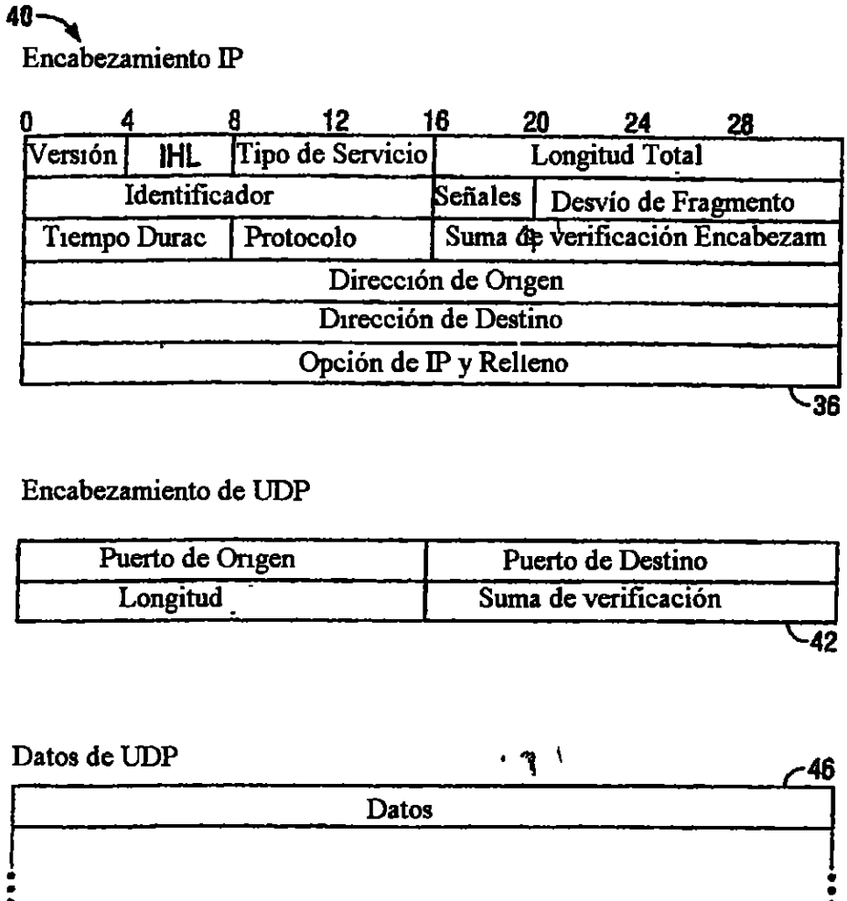

40
Encabezamiento IP
0 4 8 12 16 20 24 28
Versión
IHL
Tipo de Servicio
Longitud Total
Identificador
Señales
Desvío de Fragmento
Tiempo Durac
Protocolo
Suma de verificación Encabezam
Dirección de Origen
Dirección de Destino
Opción de IP y Relleno
36
Encabezamiento de UDP
Puerto de Origen
Puerto de Destino
Longitud
Suma de verificación
42
Datos de UDP
46
Datos

FIG. 5

81

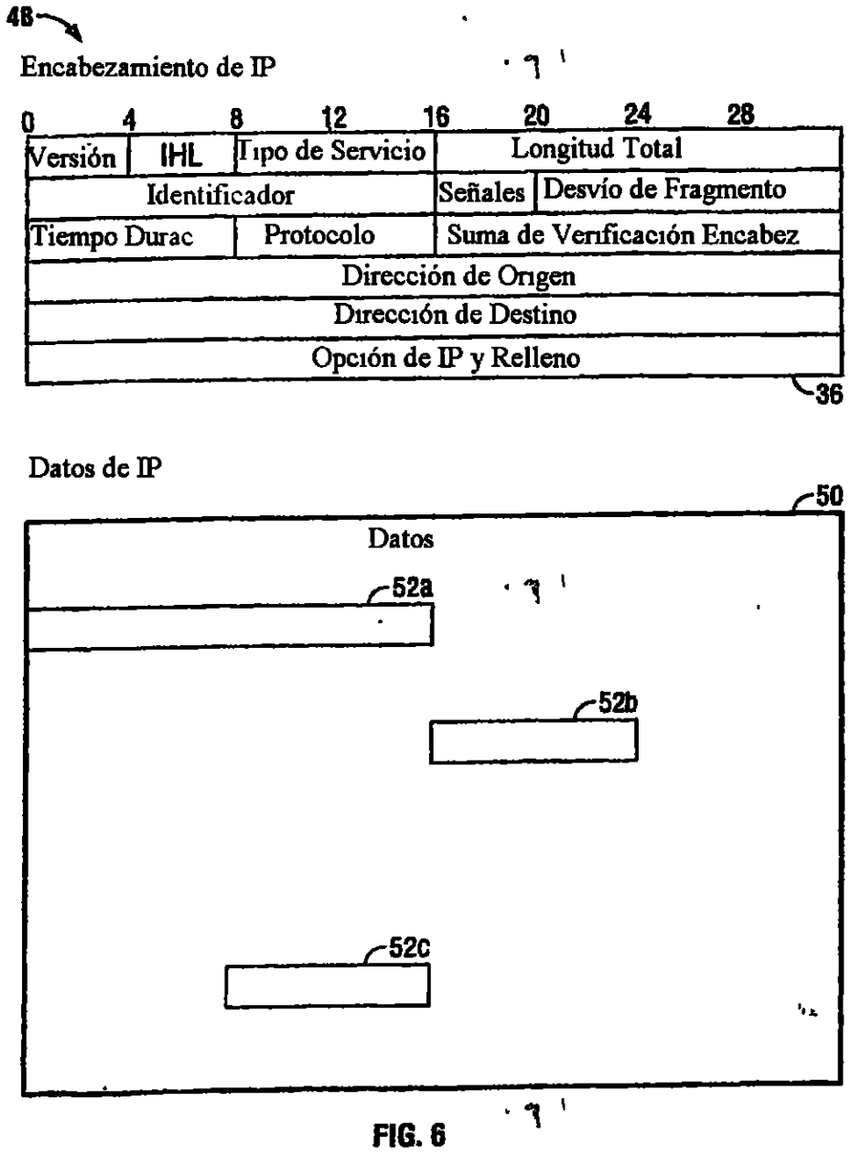

48
Encabezamiento de IP
0
4
8
12
16
20
24
28
Versión
IHL
Tipo de Servicio
Longitud Total
Identificador
Señales
Desvío de Fragmento
Tiempo Durac
Protocolo
Suma de Verificación Encabez
Dirección de Origen
Dirección de Destino
Opción de IP y Relleno
36
Datos de IP
50
Datos
52a
52b
52c

FIG. 6

82

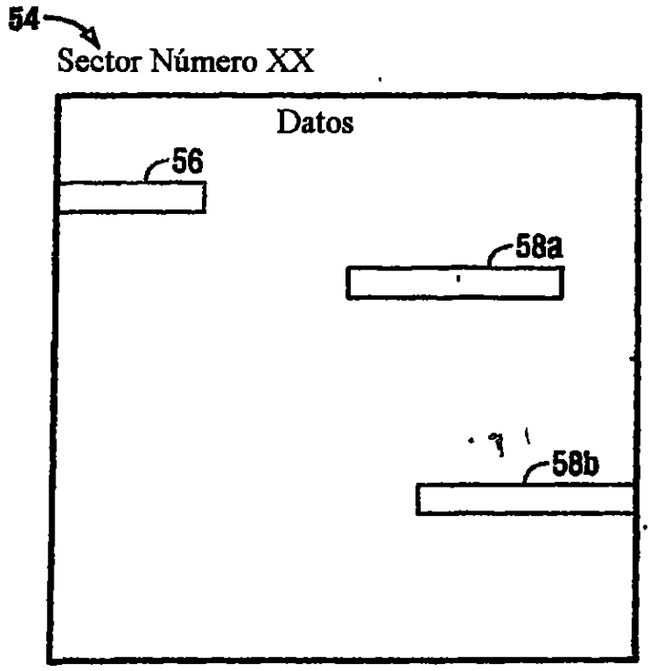

54
Sector Número XX
Datos
56
58a
58b

FIG. 7

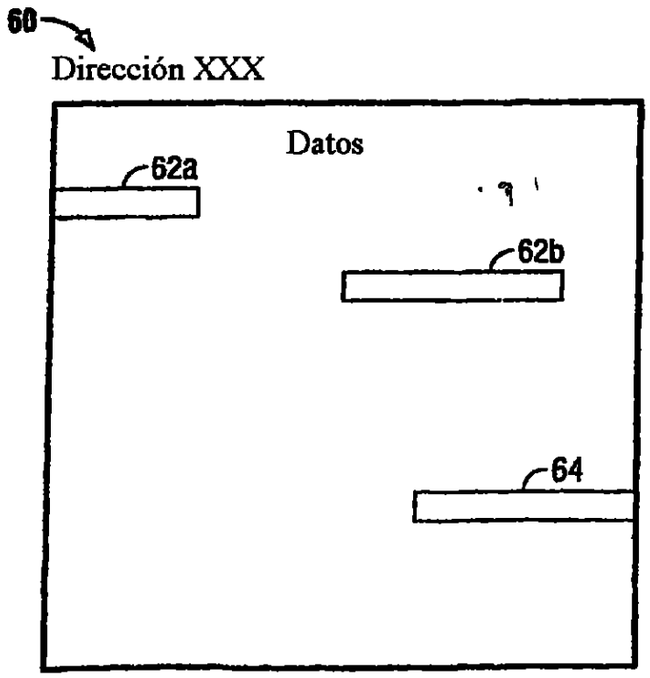

60
Dirección XXX
Datos
62a
62b
64

FIG. 8

83

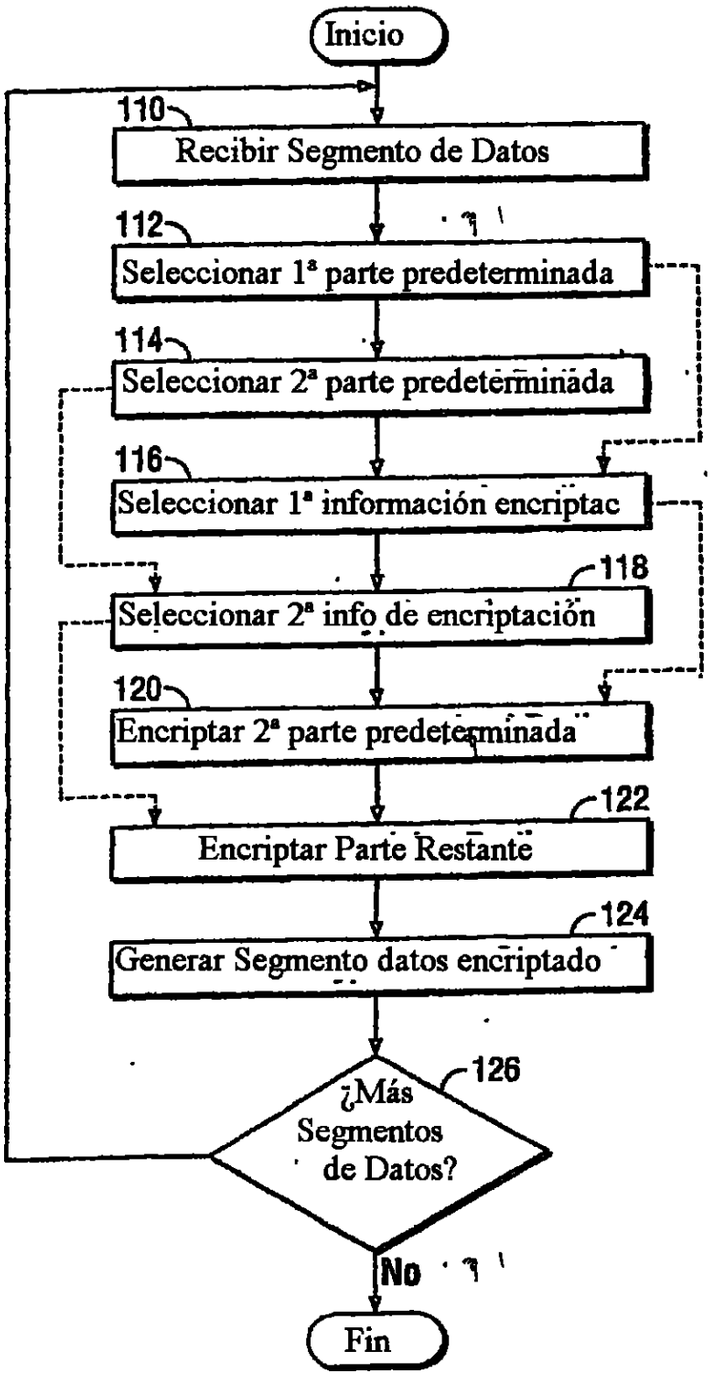

Inicio
110
Recibir Segmento de Datos
112
Seleccionar 1ª parte predeterminada
114
Seleccionar 2ª parte predeterminada
116
Seleccionar 1ª información encriptac
118
Seleccionar 2ª info de encriptación
120
Encriptar 2ª parte predeterminada
122
Encriptar Parte Restante
124
Generar Segmento datos encriptado
126
¿Más Segmentos de Datos?
No
Fin

FIG. 9

84

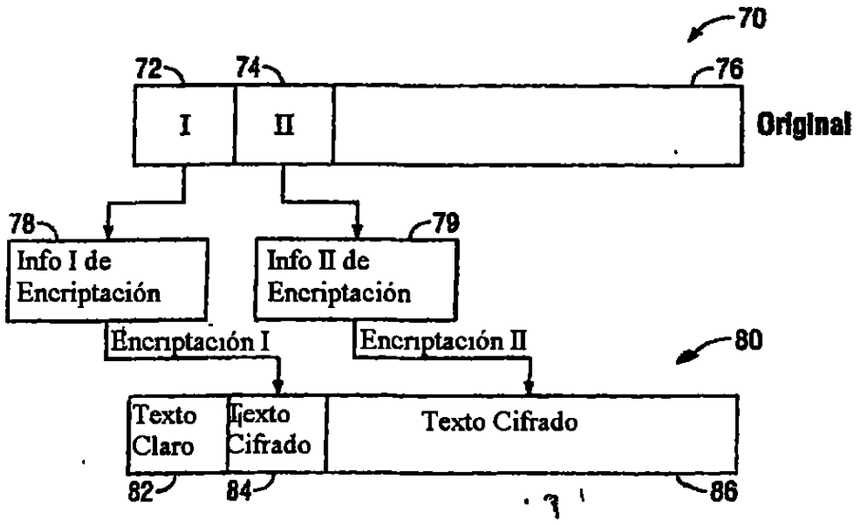

70
72
74
76
I
II
Original
78
79
Info I de Encriptación
Info II de Encriptación
Encriptación I
Encriptación II
80
Texto Claro
Texto Cifrado
Texto Cifrado
82
84
86

FIG. 10

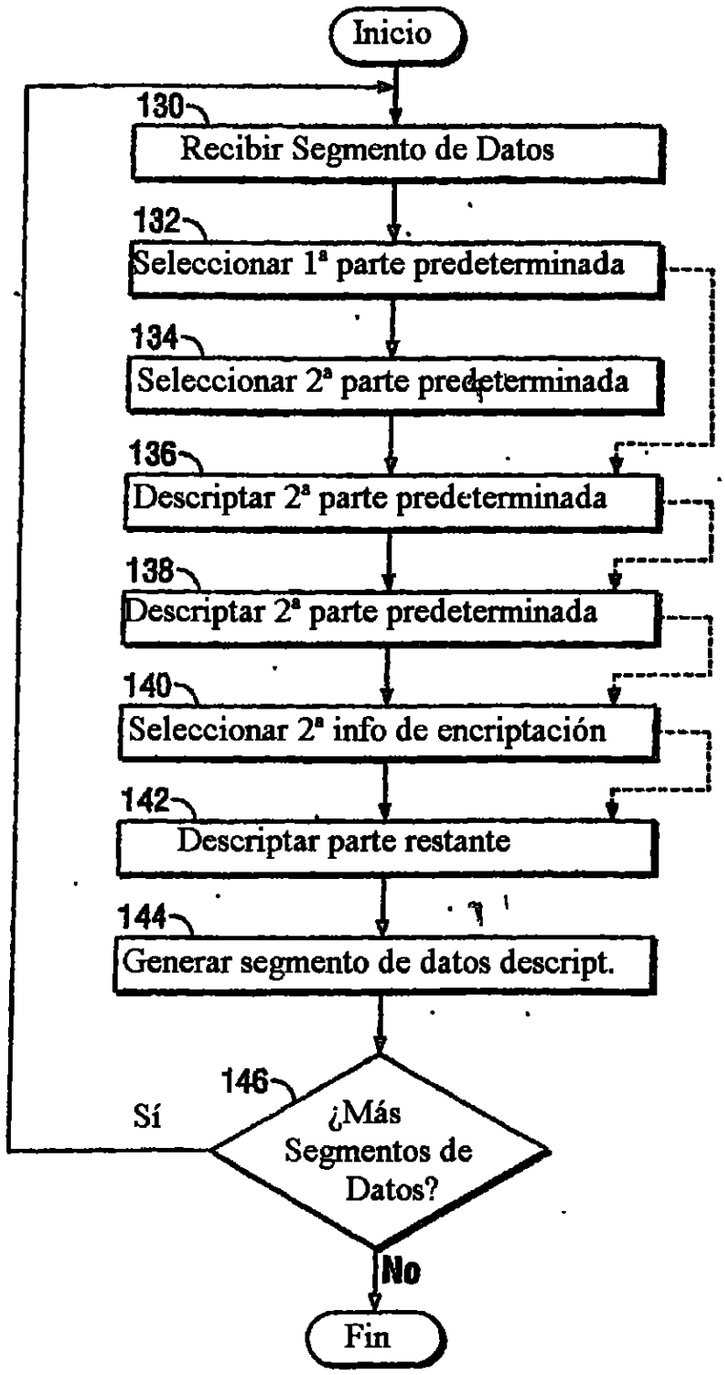

Inicio
130
Recibir Segmento de Datos
132
Seleccionar 1ª parte predeterminada
134
Seleccionar 2ª parte predeterminada
136
Descriptar 2ª parte predeterminada
138
Descriptar 2ª parte predeterminada
140
Seleccionar 2ª info de encriptación
142
Descriptar parte restante
144
Generar segmento de datos descript.
146
¿Más Segmentos de Datos?
Sí
No
Fin

FIG. 11

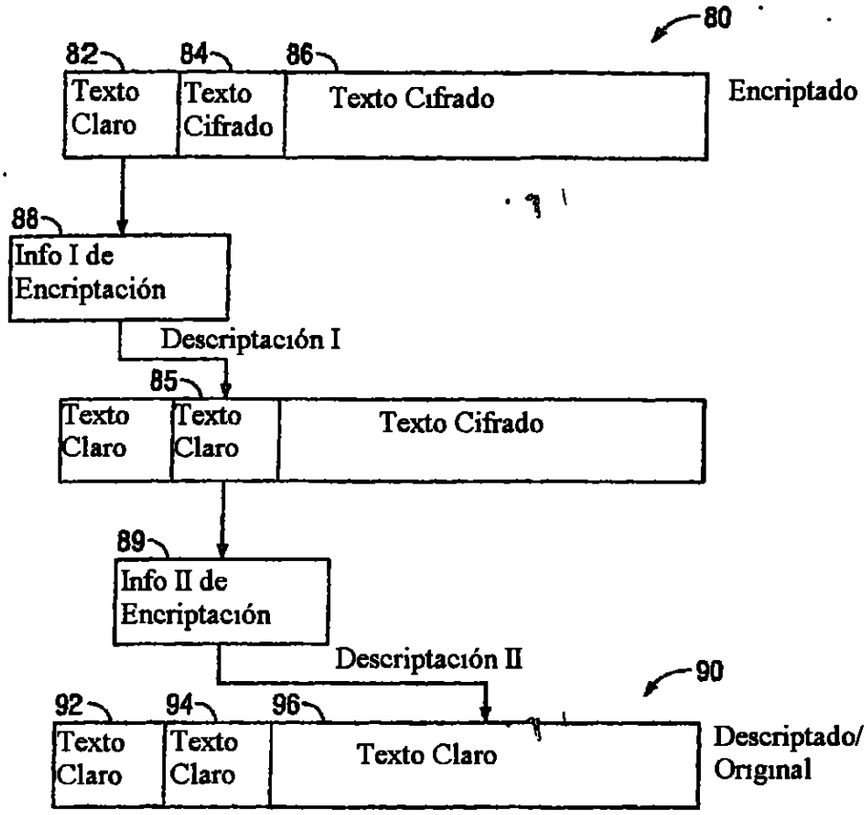

80
82
84
86
Texto Claro
Texto Cifrado
Texto Cifrado
Encriptado
88
Info I de Encriptación
Descriptación I
85
Texto Claro
Texto Claro
Texto Cifrado
89
Info II de Encriptación
Descriptación II
90
92
94
96
Texto Claro
Texto Claro
Texto Claro
Descriptado/ Original

FIG. 12

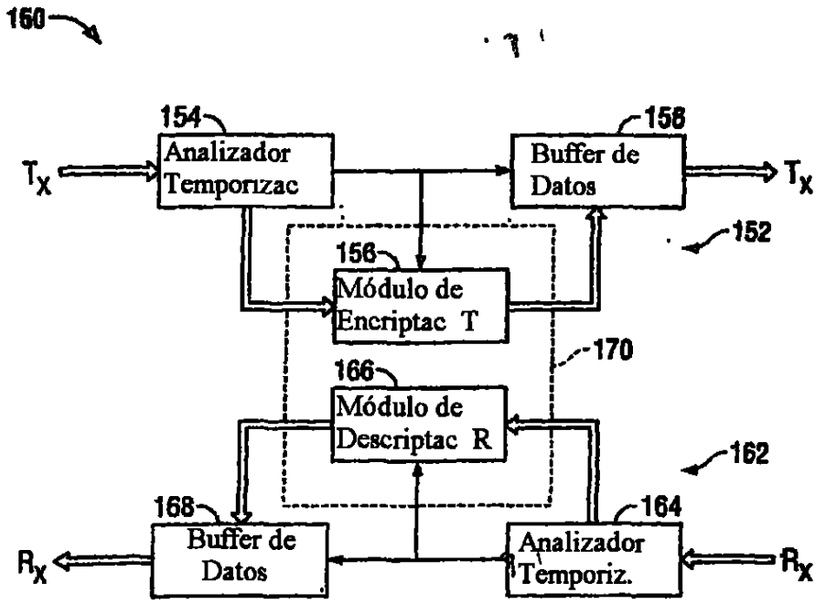

160
154
Analizador Temporizac
158
Buffer de Datos
T_X
T_X
152
156
Módulo de Encriptac T
170
166
Módulo de Descriptac R
162
168
Buffer de Datos
164
Analizador Temporiz.
R_X
R_X

FIG. 13

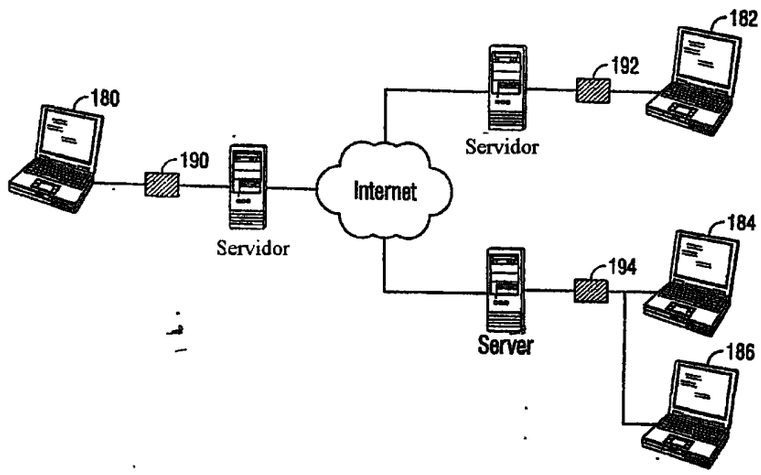

180
190
Servidor
Internet
Servidor
192
182
Server
194
184
186

FIG. 14

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
22 September 2005 (22.09.2005)

PCT

(10) International Publication Number
WO 2005/088893 A1

(51) International Patent Classification[7]: H04L 9/00

(21) International Application Number:
PCT/US2004/004117

(22) International Filing Date: 13 February 2004 (13.02.2004)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant (*for all designated States except US*): PSY-CRYPT, INC. [US/US], Suite 213, 2635 North First Street, San Jose, CA 95139 (US).

(72) Inventor; and

(75) Inventor/Applicant (*for US only*): WATANABE, Masashi [JP/JP], 49-1, Machisuji, Iwawaki, Hanoura-cho, Naka-gun, Tokushima (JP).

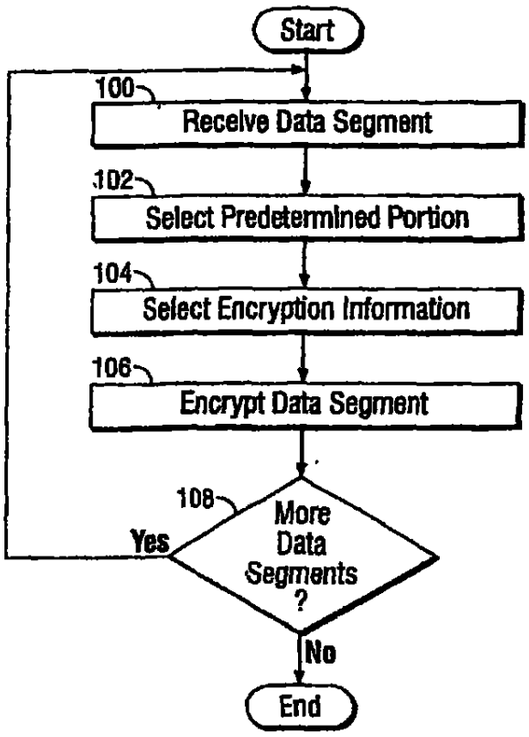
(74) Agents: RITCHIE, David, B. et al ; Thelen Reid & Priest, LLP, P.O Box 640640, San Jose, CA 95164-0640 (US).

(81) Designated States (*unless otherwise indicated, for every kind of national protection available*): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States (*unless otherwise indicated, for every kind of regional protection available*): ARIPO (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: METHOD AND APPARATUS FOR CRYPTOGRAPHICALLY PROCESSING DATA



(57) Abstract: A method and apparatus cryptographically process data including a plurality of data segments. The cryptographic process includes (a) receiving a plurality of data segments (100), (b) selecting, for each data segment, a set of encryption information based on data contained in a predetermined portion of the data segment to be encrypted (102, 104), and (c) encrypting each data segment using the set of encryption information selected for the data segment (106). At least one of an encryption algorithm, an encryption key, and an encryption parameter may be changed for each data segment based on the data contained in the predetermined portion. The predetermined portion may include a first predetermined portion for selecting a first set of encryption information, and a second predetermined portion for selecting a second set of encryption information, the encryption information including an encryption algorithm, an encryption key, and optionally an encryption parameter

WO 2005/088893 A1

Declaration under Rule 4.17:
— *of inventorship (Rule 4 17(iv)) for US only*

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

SPECIFICATION

TITLE OF INVENTION

METHOD AND APPARATUS FOR CRYPTOGRAPHICALLY PROCESSING DATA

FIELD OF THE INVENTION

[0001] The present invention relates to cryptography and cryptographic systems. More particularly, the present invention relates to a method and apparatus for cryptographically processing data including a plurality of data segments

BACKGROUND OF THE INVENTION

[0002] A number of encryption methods and cryptographic systems (cryptosystems) are currently used in various fields. For example, there are symmetric cryptosystems and asymmetric cryptosystems The symmetric cryptography, which is also referred to as secret-key cryptography, uses a single key (secret key) to encrypt and decrypt information Asymmetric cryptography, which is also referred to as public-key cryptography, uses a pair of keys. one (public key) to encrypt data, and the other (private key) to decrypt it Currently available encryption algorithms include, for example, Data Encryption Standard (DES) which is a symmetric algorithm employing a block cipher with a single 56-bit key, triple DES which is a secure form of DES using a 168-bit key, International Data Encryption Algorithm (IDEA) which is a block-mode secret-key encryption algorithm using a 128-bit key, RC4 which is a widely-used symmetric key algorithm, the Advanced Encryption Standard (AES) which provides stronger encryption scheme with alternative three key lengths of 128 bits, 192 bits, or 256 bits, and the like.

[0003] Many companies employ a symmetric cryptosystem for their secure communications, using a predetermined encryption algorithm with the fixed secret-key such as the triple DES or AES Due to the continuous evolution of computer-based technology, security methods that have seemed unbreakable are becoming inadequate, for example, the 56-bit key size of DES is no longer considered secure against brute force attacks Using the same encryption algorithm and the same secret-key for communication over long time may increase the risk of brute force attacks on the

cryptosystem However, replacing encryption algorithm and/or the secret-key in a once-implemented cryptosystem is typically very costly, since it requires some form of secure key exchange, in person, by courier, and the like, among all of the entities using the cryptosystem, and any change in the algorithm or secret key must also be synchronized among the entities. A fixed algorithm/key cryptosystem also lacks compatibility with other cryptosystems utilizing a different encryption algorithm and/or a different secret key.

[0004] Accordingly, it would be desirable to provide a cryptosystem which realizes secure communications and transactions which is less vulnerable to brute force and other attacks and also has high flexibility and compatibility.

BRIEF DESCRIPTION OF THE INVENTION

[0005] A method and apparatus cryptographically process data including a plurality of data segments The cryptographic process includes (a) receiving a plurality of data segments, (b) selecting, for each data segment, a set of encryption information based on data contained in a predetermined portion of the data segment to be encrypted, and (c) encrypting each data segment using the set of encryption information selected for the data segment At least one of an encryption algorithm, an encryption key, and an encryption parameter may be changed for each data segment based on the data contained in the predetermined portion. The predetermined portion may include a first predetermined portion for selecting a first set of encryption information, and a second predetermined portion for selecting a second set of encryption information, the encryption information including an encryption algorithm, an encryption key, and optionally an encryption parameter.

[0006] In accordance with one aspect of the present invention, a method for encrypting data includes (a) receiving a plurality of data segments, (b1) selecting, for each packet, a first set of encryption information based on data contained in a first predetermined portion of the data segment, (b2) selecting, for each packet, a second set of encryption information based on data contained in a second predetermined portion of the data segment, (c1) encrypting the second predetermined portion of each data segment

using the first set of encryption information selected for the data segment, (c2) encrypting the remaining portion of each data segment using the second encryption information selected for the data segment, and (d) generating an encrypted data segment for each of the original data segments, the encrypted data segment having a first predetermined portion, a second predetermined portion, and a remaining portion, the first predetermined portion containing the original data in the corresponding first predetermined portion of the original data segment, the second predetermined portion containing the encrypted data of the corresponding second predetermined portion of the original data segment, and the remaining portion containing the encrypted data of the corresponding remaining portion of the original data segment.

[0007] In accordance with one aspect of the present invention, the method for decrypting data includes (a) receiving an encrypted data including a plurality of encrypted data segments, each of the encrypted data segments having a first predetermined portion, a second predetermined portion, and a remaining portion, the first predetermined portion containing original data in a corresponding first predetermined portion of an original data segment, the second predetermined portion containing encrypted data of a corresponding second predetermined portion of the original data segment, and the remaining portion containing the encrypted data of the corresponding remaining portion of the original data segment, (b1) selecting, for each encrypted data segment, a first set of encryption information based on the original data contained in the first predetermine portion of the encrypted data segment, (c1) decrypting the encrypted data contained in the second predetermined portion of each encrypted data segment using the first set of encryption information selected for the encrypted data segment, (b2) selecting, for each encrypted data segment, a second set of encryption information based on the decrypted data of the second predetermined portion, (c2) decrypting the remaining portion of each encrypted data segment using the second set of encryption information selected for the encrypted data segment.

[0008] In accordance with one aspect of the invention, an apparatus for cryptographically processing data includes (a) means for receiving a plurality of data segments, (b) means for selecting, for each data segment, a set of encryption information

based on data contained in a predetermined portion of the data segment to be encrypted, and (c) means for encrypting each data segment using the set of encryption information selected for the data segment. The means for selecting may change at least one of an encryption algorithm, an encryption key, and an encryption parameter for each data segment based on the data contained in the predetermined portion.

[0009] In accordance with one aspect of the invention, the means for selecting includes (e) means for generating, for each data segment, a value from data contained in the predetermined portion of the data segment, and (f) means for selecting a set of encryption information associated with the generated value, the set of encryption information including an encryption algorithm, an encryption key, and optionally an encryption parameter The means for generating a value may include means for hashing the data contained in the predetermined portion using a hash key

[0010] In accordance with one aspect of the invention, the apparatus may further includes means for providing an encryption table containing an encryption type identifier, an encryption key for the encryption type, and an encryption parameter, for each entry associated with a generate value.

[0011] In accordance with one aspect of the invention, the predetermined portion includes a first predetermined portion for selecting a first set of encryption information, and a second predetermined portion for selecting a second set of encryption information Each set of encryption information includes an encryption algorithm, an encryption key, and optionally an encryption parameter.

[0012] In accordance with one aspect of the invention, the apparatus may further include means for encrypting the second predetermined portion using the first set of encryption information, and means for encrypting the remaining portion of the data segment using the second set of encryption information.

[0013] In accordance with one aspect of the invention, the apparatus may further include means for generating an encrypted data segment for each of the original data segments, the encrypted data segment having a first predetermined portion, a second

predetermined portion, and a remaining portion, the first predetermined portion containing the original data in the corresponding first predetermined portion of the original data segment, the second predetermined portion containing the encrypted data of the corresponding second predetermined portion of the original data segment, and the remaining portion containing the encrypted data of the corresponding remaining portion of the original data segment

[0014] In accordance with one aspect of the invention, the apparatus may further include means for transmitting a plurality of encrypted data segments as a stream of encrypted data. The apparatus may also include means for storing a plurality of encrypted data segments on a data storage device, each encrypted data segment corresponding to a respective data sector of the data storage device

[0015] In accordance with one aspect of the invention, the apparatus may further include (a) means for receiving the encrypted data including a plurality of encrypted data segments, (b1) means for selecting, for each encrypted data segment, a first set of encryption information based on data contained in the first predetermine portion of the encrypted data segment, (c1) means for decrypting the encrypted data contained in the second predetermined portion of each encrypted data segment using the first set of encryption information selected for the encrypted data segment, (b2) selecting, for each encrypted data segment, a second set of encryption information based on the decrypted data of the second predetermined portion, and (c2) decrypting the remaining portion of each encrypted data segment using the second set of encryption information selected for the encrypted data segment.

[0016] In accordance with one aspect of the invention, the means for selecting the first encryption information may include means for generating a first value from the original data contained in the first predetermined portion of the encrypted data segment. The means for generating the first value may include means for hashing the data contained in the first predetermined portion using a first hash key.

[0017] In accordance with one aspect of the invention, means for selecting the second encryption information may include means for generating a second value from the decrypted data of the second predetermined portion of the encrypted data segment. The means for generating the second value may include means for hashing the decrypted data of the second predetermined portion using a second hash key.

[0018] In accordance with one aspect of the invention, the apparatus for decrypting data includes (a) means for receiving a plurality of encrypted data segments, each of the encrypted data segments having a predetermined portion, (b) means for selecting, for each encrypted data segment, a set of encryption information based on data contained in the predetermined portion of the encrypted data segment, and (c) means for decrypting each encrypted data segment using the encryption information selected for the encrypted data segment.

[0019] In accordance with one aspect of the invention, the means for selecting may include means for generating, for each encrypted data segment, a value from data contained in the predetermined portion of the encrypted data segment, and means for selecting a set of encryption information associated with the generated value, the set of encryption information including an encryption algorithm, an encryption key, and optionally an encryption parameter. The means for generating a value may include means for hashing the data contained in the predetermined portion using a hash key.

[0020] In accordance with one aspect of the invention, the apparatus may further include means for providing an encryption type identifier, an encryption key for the encryption type, and an encryption parameter associated with a generated value.

[0021] In accordance with one aspect of the invention, the predetermined portion may include a first predetermined portion for selecting a first set of encryption information, and a second predetermined portion for selecting a second set of encryption information. Each set of encryption information may include an encryption algorithm, an encryption key, and optionally an encryption parameter.

[0022] In accordance with one aspect of the invention, the first predetermined portion contains data for a first protocol layer, and the second predetermined portion contains data for a second protocol layer, wherein the first protocol layer is lower than the second protocol layer The first predetermined portion may be an Internet Protocol (IP) header of the data packet The second predetermined portion may be a selected portion of a data field, a Transmission Control Protocol (TCP) header, or a User Datagram Protocol (UDP) header of the data packet.

[0023] In accordance with one aspect of the invention, the first predetermined portion is a first selected portion in a sector in a data storage device, and the second predetermined portion is a second selected portion in the sector.

[0024] In accordance with one aspect of the invention, the data contained in the second predetermined portion of an encrypted data segment has been encrypted using the first set of encryption information, and the data contained in the remaining portion of the encrypted data segment has been encrypted using the second set of encryption information

BRIEF DESCRIPTION OF THE DRAWINGS

[0025] The accompanying drawings, which are incorporated into and constitute a part of this specification, illustrate one or more embodiments of the present invention and, together with the detailed description, serve to explain the principles and implementations of the invention.

[0026] In the drawings:

FIG 1A is a block diagram schematically illustrating an encryption part of an apparatus for encrypting/decrypting data in accordance with one embodiment of the present invention.

FIG. 1B is a block diagram schematically illustrating an decryption part of an apparatus for encrypting/decrypting data in accordance with one embodiment of the present invention

FIG 2 is a diagram schematically illustrating an example of the encryption table

in accordance with one embodiment of the present invention.

FIG 3 is a process flow diagram schematically illustrating a method for encrypting/decrypting data in accordance with one embodiment of the present invention.

FIG. 4 is a diagram schematically illustrating an example of a data packet in which the first predetermined portion is an Internet Protocol (IP) header, and the second predetermined portion is a Transmission Control Protocol (TCP) header.

FIG. 5 is a diagram schematically illustrating an example of a data packet in which the first predetermined portion is an Internet Protocol (IP) header, and the second predetermined portion is a User Datagram Protocol (UDP) header.

FIG. 6 is a diagram schematically illustrating an example of a data packet in which the first predetermined portion is an Internet Protocol (IP) header, and the second predetermined portion is a selected portion of a data field.

FIG. 7 is a diagram schematically illustrating an example of the first and second predetermined portions in a sector of a data storage device.

FIG. 8 is a diagram schematically illustrating an example of the first and second predetermined portions in a data segment stored in a memory card in which the data segment corresponds to data stored in each address.

FIG 9 is a process flow diagram schematically illustrating a method for encrypting data in accordance with one embodiment of the present invention, in which the predetermined portion includes a first predetermined portion and a second predetermined portion.

FIG. 10 is a diagram schematically illustrating an example of encrypting a data packet using the method shown in FIG. 9

FIG 11 is a process flow diagram schematically illustrating a method for decrypting encrypted data in accordance with one embodiment of the present invention, in which the predetermined portion includes a first predetermined portion and a second predetermined portion

FIG. 12 is a diagram schematically illustrating an example of decrypting a data packet using the method shown in FIG. 11

FIG. 13 is a block diagram schematically illustrating a data encryptor/decryptor in accordance with one embodiment of the present invention

FIG. 14 is a diagram schematically illustrating an example of application of the

encryption/decryption apparatus to secure communications via the Internet in accordance with one embodiment of the present invention

DETAILED DESCRIPTION

[0027] Embodiments of the present invention are described herein in the context of a method and apparatus for encrypting and decrypting data including a plurality of data segments Those of ordinary skill in the art will realize that the following detailed description of the present invention is illustrative only and is not intended to be in any way limiting. Other embodiments of the present invention will readily suggest themselves to such skilled persons having the benefit of this disclosure. Reference will now be made in detail to implementations of the present invention as illustrated in the accompanying drawings. The same reference indicators will be used throughout the drawings and the following detailed description to refer to the same or like parts.

[0028] In the interest of clarity, not all of the routine features of the implementations described herein are shown and described. It will, of course, be appreciated that in the development of any such actual implementation, numerous implementation-specific decisions must be made in order to achieve the developer's specific goals, such as compliance with application- and business-related constraints, and that these specific goals will vary from one implementation to another and from one developer to another. Moreover, it will be appreciated that such a development effort might be complex and time-consuming, but would nevertheless be a routine undertaking of engineering for those of ordinary skill in the art having the benefit of this disclosure.

[0029] In accordance with one embodiment of the present invention, the components, process steps, and/or data structures may be implemented using various types of hardwired devices, field programmable logic devices (FPLDs), including field programmable gate arrays (FPGAs) and complex programmable logic devices (CPLDs), application specific integrated circuits (ASICs), or the like, may also be used without departing from the scope and spirit of the inventive concepts disclosed herein.

[0030] In the context of the present invention, the term "network" includes local area networks (LANs), wide area networks (WANs), the Internet, cable television systems, telephone systems, wireless telecommunications systems, fiber optic networks, ATM networks, frame relay networks, satellite communications systems, and the like. Such networks are well known in the art and consequently are not further described here

[0031] FIG. 1A schematically illustrates an apparatus 10 for encrypting/decrypting data in accordance with one embodiment of the present invention. As shown in FIG. 1A, the apparatus 10 includes an input buffer 12, an encryption module 14, a controller 16 coupled to the input buffer 12 and the encryption module 14, and an output buffer 18 coupled to the controller 16 and the encryption module 14. The input buffer 12 is adapted to receive data including a plurality of data segments. For example, such data may be a data stream including a plurality of data packets. The data segments may also be read from corresponding sectors of a recording medium or data storage device such as a hard disk, CD ROM, DVD, memory card, and the like. The encryption module 14 is adapted to encrypt each data segment. The output buffer 18 buffers the encrypted data segments from the encryption module 14, and outputs encrypted data including a plurality of encrypted data segments

[0032] For example, as shown in FIG. 1A, the apparatus 10 may be used between a universal serial bus (USB) port 11 and an Ethernet port 13, in such a case where a host computer communicates via a LAN. The apparatus 10 can also be used for secure communications via WAN, the Internet, wireless network, and the like. Furthermore, the apparatus 10 may be used with a small computer system interface (SCSI), an intelligent/integrated drive electronics (IDE) interface, an enhanced IDE interface, and the like, to store secure data in mass storage devices. The apparatus may also be used for the other type of digital data transfer.

[0033] The controller 16 is adapted to select a set of encryption information for each data segment based on data contained in a predetermined portion of the data segment to be encrypted For example, the encryption information includes an encryption algorithm, an encryption key, and an encryption parameter such as an initial vector. The

encryption parameter may be used to set or initialize the encryption process to a specific state. Since the encryption information is selected based on data in a specific portion of the data segment to be encrypted, typically, at least one of the encryption algorithm, the encryption key, and the encryption parameter is changed for each data segment. In other words, the encryption information is "self-determined" for each data segment using the data contained in the data segment itself. The predetermined portion of the data segment may be a header of each data packet, a selected portion of the data field of the data packet, for example, a specific length of data starting at a predetermined number of bytes from the beginning of the data field. The predetermined portion may be a selected portion of a sector in a data storage device, a sector number or address field of each sector in a data storage device, and the like.

[0034] The encryption module **14** includes a plurality of encryption engines **20** (**20a**, **20b**, **20c**,..), each corresponding to an encryption algorithm to be selected by the controller **16**. The encryption module **14** may further include a data buffer **22** coupled to each of the plurality of encryption engines **20**.

[0035] In accordance with one embodiment of the present invention, as shown in FIG. 1A, the controller **16** includes a data selector **24**, an encryption selector **26** coupled with the data selector **24**, and an encryption controller **28**. The data selector **24** is adapted to select the predetermined portion from each data segment The encryption selector **26** is adapted to select a set of encryption information in accordance with data contained in the predetermined portion selected by the data selector **24**. The set of encryption information includes, for example, an encryption algorithm, an encryption key, and optionally an encryption parameter. The encryption controller **28** is adapted to select and activate one of the encryption engines **20** based on the encryption information. For example, if an encryption algorithm A is selected by the encryption selector **26**, the encryption controller **28** selects a corresponding encryption engine (A) **20a** and activates or initializes the encryption engine **20a** using the encryption parameters The data is encrypted by the encryption engine **20a** using the selected key. It should be noted that a different key and/or a different encryption parameter yield different encrypted data even if the same encryption algorithm and the thus same encryption engine are used.

[0036] In accordance with one embodiment of the present invention, the controller 16 further includes a value generator 30 coupled to the data selector 24. The value generator is adapted to generate a value from the data contained in the predetermined portion For example, the value generator 30 may include a hash function and hash the data using a hash key to produce the value. The hash key may be preinstalled in the value generator 30, or may be selected when the controller 16 is first programmed.

[0037] In accordance with one embodiment of the present invention, the encryption controller 26 includes an encryption table 32. The encryption table 32 contains an encryption type identifier, an encryption key for the encryption type, and an encryption parameter such as an initial vector specifying an initial encryption state of the encryption engine, for each entry associated with a value generated by the value generator 30. FIG. 2 schematically illustrates an example of the encryption table 32 As shown in FIG. 2, each entry of the encryption table 32 has an index corresponding to the generated value, for example, a hash value, and a corresponding set of an encryption algorithm (encryption type), a key for the encryption algorithm, and an initial vector (encryption parameter). The number of the entries depends on the value generated from the predetermined portion. In one embodiment of the present invention, an encryption table has about 1000 entries Typically, a different index value is derived from the predetermined portion of a different data segment, and thus each data segment is encrypted using different encryption information.

[0038] The above description is with respect to the encryption part of the apparatus 10. FIG 1B schematically illustrates a corresponding decryption part 10' of the apparatus 10 in accordance with one embodiment of the present invention. As shown in FIG. 1B, the decryption part 10' can be constructed symmetrically to the encryption part (FIG 1A) of the apparatus 10, including decryption engines 20a', 20b', and 20c' in place of the encryption engines 20a, 20b, and 20c, as is well understood by one of ordinary skill in the art without further explanation.

[0039] FIG. 3 schematically illustrates a method for encrypting/decrypting data in accordance with one embodiment of the present invention. The method may be performed by the encryption/decryption apparatus 10. A plurality of data segments are received, for example, by receiving a data stream including a plurality of data packets, or reading from a data storage device including a plurality of data sectors or addresses. The received data segments may be buffered by an input buffer The data segments are encrypted segment by segment. As shown in FIG. 3, each data segment is received (100), and a predetermined portion of each data segment is selected (102), and a set of encryption information is selected based on data contained in the predetermined portion of the data segment to be encrypted (104). The data segment is encrypted using the selected set of encryption information (106). The next data segment is processed in the same manner until all data segments in the input buffer are processed (108). The set of encryption information may include an encryption algorithm, an encryption key, and optionally an encryption parameter, as described above, ant typically at least one of the encryption algorithm, the encryption key, and the encryption parameter is changed for each data segment based the data contained in the predetermined portion.

[0040] As discussed above, in selecting the encryption information, a value (such as a hash value) may be generated from the data contained in the predetermined portion of the data segment, and the set of encryption information may be selected using the generated value. The set of encryption information may be provided in a form of an encryption table such as the encryption table 32 (FIG. 2) described above.

[0041] In accordance with one embodiment of the present invention, the predetermined portion includes a first predetermined portion and a second predetermined portion In the case where the data segment is a data packet, the first predetermined portion may contain data for a first protocol layer, and the second predetermined portion may contain data for a second protocol layer which is higher than the first protocol layer in the protocol hierarchy The first protocol layer may be the network layer (or the Internet layer), and the second protocol layer may be the Transport layer.

[0042] FIG 4 schematically illustrates an example of a data packet 34 in which the first predetermined portion is an Internet Protocol (IP) header 36, and the second predetermined portion is a Transmission Control Protocol (TCP) header 38 of the data packet 34. FIG. 5 schematically illustrates an example of a data packet 40 in which the first predetermined portion is an Internet Protocol (IP) header 36, and the second predetermined portion is a User Datagram Protocol (UDP) header 42 of the data packet 40. It should be noted that although the IP header 36, the TCP header 38, and the subsequent TCP data field 44 are illustrated separately in FIG. 4, they are contiguous in the data packet 34. Similarly, although the IP header 36, the UDP header 38, and the subsequent UDP data field 46 are illustrated separately in FIG. 5, they are contiguous in the data packet 40 In addition, the information illustrated in each header is by way of example, and not limiting in any way. All of the information in the header may be used to derive a (hash) value, or some part of the information may be selected to generate a value

[0043] In accordance with one embodiment of the present invention, the second predetermined portion is not limited to a TCP or UDP header, but may be selected from a data field FIG. 6 schematically illustrates an example of a data packet 48 in which the first predetermined portion is an Internet Protocol (IP) header 36, and the second predetermined portion is a selected portion 52 (52a, 52b, and 52c) of a data field 50 of the data packet 48. As shown in FIG. 6, the selected portion 52 may be divided and distributed in the data field 50, and specified by a predetermined number of bytes from the beginning of the data field 50 and a predetermined data length One single portion may be selected

[0044] In accordance with one embodiment of the present invention, the data segments may be sectors in a data storage device such as a hard disk, CD ROM, DVD, memory card, or other mass storage device. In this case, the first predetermined portion is a first selected portion in a sector in a data storage device, and the second predetermined portion is a second selected portion in the sector. FIG. 7 schematically illustrates such an example In FIG. 7, the first predetermined portion is a first selected portion 56 in a sector 54 in a data storage device, and the second predetermined portion

is a second selected portion 58 (58a, 58b) in the sector 54. FIG. 8 schematically illustrates an example of a memory card in which the data segment corresponds to data stored in each address. In such a case, the data may be encrypted address by address, and the first predetermined portion is a first selected portion 62 (62a, 63b) in a memory address 60, and the second predetermined portion is a second selected portion 64 in the address 60 As shown in FIGS. 7 and 8, the first and/or second predetermined portion may be divided and distributed in the sector or data in the memory address, or may be a single portion.

[0045] FIG. 9 schematically illustrates a method for encrypting data in accordance with one embodiment of the present invention, in which the predetermined portion includes a first predetermined portion and a second predetermined portion, as described above. FIG 10 schematically illustrates an example of encrypting a data packet 70 using the method shown in FIG. 9, where the data packet 70 includes a first predetermined portion 72 (such as an IP header) and a second predetermined portion 74 (such as a TCP header or a selected portion of the data field).

[0046] As shown in FIG. 9, for each data segment received (110), the first predetermined portion and the second predetermined portion are selected (112, 114). Also referring to FIG. 10, the first encryption information 78 is selected based on the data contained in the first predetermined portion 72 (116). As discussed above, this selection 116 may include, for example, deriving a hash value from the first predetermined portion 72 and selecting the first encryption information using an encryption table associating the hash value with a respective set of encryption information. Similarly, the second encryption information 79 is selected based on the data contained in the second predetermined portion 74 (118). This selection 118 may also include, for example, deriving a hash value from the second predetermined portion 74 and selecting the second encryption information using an encryption table associating the hash value with a respective set of encryption information. A respective hash key and a respective encryption table may be provided for each of the selection process 116 and 118. For example, the controller 16 of the encryption/decryption apparatus 10 (FIG 1) may include a first set of the hash key and the encryption table for the first

predetermined portion, and a second set of the hash key and the encryption table for the second predetermined portion.

[0047] Then, the second predetermined portion 74 is encrypted using the first encryption information 78 (120), and the remaining portion of the data segment 76 is encrypted using the second encryption information 79 (122). The remaining portion 76 is all of the remaining data in the data segment other than the first and second predetermined portions. As shown in FIG. 10, the first predetermined portion 82 containing the original data (also referred to as "plaintext"), the second predetermined portion 84 containing encrypted data (also referred to as "ciphertext"), and the remaining portion 86 containing encrypted data are combined to generate an encrypted data segment (packet) 80 corresponding to the original data segment (packet) 70 (124). For example, referring to FIG. 1, the second predetermined portion may be encrypted using the encryption engine 20a, and the remaining portion may be encrypted using the encryption engine 20b, and the respective encrypted data are combined with the first predetermined portion into the encrypted data segment in the data buffer 22, and sent to the output buffer 18.

[0048] The processes 110 through 124 are performed until all of the data segments are encrypted (126). It should be noted that the selection and encryption processes are controlled such that the second encryption information 79 is selected before the data contained in the second predetermined portion 74 is encrypted, and the plaintext data for the first predetermined portion 84, the ciphertext for the second predetermined portion 84, and the ciphertext for the remaining portion 86 are sent to the data buffer 22 in this order

[0049] The encrypted data segments may be transmitted as an encrypted data stream for secure data communication, or may be stored on a data storage device to prevent, for example, sensitive or protected information from being read by an unauthorized person.

[0050] FIG. 11 schematically illustrates a method for decrypting encrypted data in accordance with one embodiment of the present invention, in which the predetermined

portion includes a first predetermined portion and a second predetermined portion. FIG. 12 schematically illustrates an example of decrypting an encrypted data packet 80 using the method shown in FIG. 11, where the encrypted data packet 80 includes a first predetermined portion 82 (such as an IP header) and a second predetermined portion 84 (such as a TCP header or a selected portion of the data field). As described above, the first predetermined portion 82 contains plaintext, and the second predetermined portion and the remaining portion 86 contain ciphertext

[0051] As shown in FIG. 11, for each encrypted data segment received (130), the first predetermined portion and the second predetermined portion are selected (132, 134). The encrypted data segments may be received as an encrypted data stream in a secure communication, or may be read from a data storage device. Also referring to FIG. 12, the first encryption information 88 is selected based on the data contained in the first predetermined portion 82 (136). Similarly to the encryption process discussed above, this selection 136 may include, for example, deriving a hash value from the first predetermined portion 82 and selecting the first encryption information using an encryption table associating the hash value with a respective set of encryption information Since the first predetermined portion contains the plaintext, the first encryption information is the same as the original data segment

[0052] Then, the second predetermined portion 84, which contains the ciphertext, is decrypted using the first encryption information 88 (138). The second encryption information 89 is selected based on the decrypted data 85 contained in the second predetermined portion 84 (140). This selection 138 may also include, for example, deriving a hash value from the decrypted data 85 and selecting the second encryption information 89 using an encryption table associating the hash value with a respective set of encryption information. A respective hash key and a respective encryption table may be provided for each of the selection process 136 and 138.

[0053] Then, the remaining portion 86 of the data segment is decrypted using the second encryption information 89 (142). The remaining portion 86 is all of the remaining data of the data segment other than the first and second predetermined

portions The first predetermined portion 92, the second predetermined portion 94, and the remaining portion 96 are combined to generate an decrypted data segment (packet) 90 which is the same as the original data segment (packet) 70 (144). The processes 130 through 144 are performed until all of the encrypted data segments are decrypted (146).

[0054] FIG 13 schematically illustrates a data encryptor/decryptor 150 in accordance with one embodiment of the present invention. As shown in FIG. 13, the data encryptor/decryptor includes a transmitting portion 152 and a receiving portion 162. The transmitting portion 152 includes a first timing analyzer 154, an encryption module (T) 156, and a first data buffer 158. Similarly, the receiving portion 162 includes a second timing analyzer 164, a decryption module (R) 166, and a second data buffer 168. The encryption module 156 may be the encryption part of the encryption/decryption apparatus 10 (the encryption module 14 and the controller 16) described above, and the decryption module 166 may be the encryption part 10' of the encryption/decryption apparatus 10 described above. In the transmitting portion, for example, the input buffer 12 (in FIG. 1A) may be integrated within the timing analyzer 154 in accordance with a specific implementation. The output buffer 18 (in FIG. 1A) may also be integrated within the data buffer 158 in accordance with a specific implementation. The same applies to the receiving portion 154.

[0055] Since the data encryptor/decryptor 150 typically transmits and receives a data stream (Tx and Rx), the timing analyzers 154 and 164 synchronize the encryption/decryption processes for the corresponding data stream such that encrypted/decrypted data are properly combined into respective encrypted/decrypted data segments (data packets) and sent to and output from the data buffers 158 and 168, respectively.

[0056] In accordance with one embodiment of the present invention, the data encryptor/decryptor 150 (and the encryption/decryption apparatus 10) can be implemented in a form of a plug-in card for a computer Since all of the necessary components for encryption/decryption are provided in the data encryptor/decryptor (encryption/decryption card), the user/computer does not have to install any specific

software program for encryption/decryption so long as the computer can use the encryption/decryption card (i.e , port-compatible). By simply transmitting or storing data via the encryption/decryption card, the data is automatically encrypted and thus securely transmitted through a network or securely stored in a storage device. The same encryption/decryption card can be used to receive securely transmitted data or read the securely stored data.

[0057] To receive or read the encrypted data, the same encryption/decryption card or apparatus must be used to decrypt the encrypted data. The "same" means that the card or apparatus is capable of selecting the same predetermined first and second portions from the data segments and selecting/deriving the same first and second encryption information if the data contained in the predetermined portion is the same. Typically, for example, the corresponding (communicating) encryption/decryption cards have the identical hash keys and the identical encryption tables.

[0058] In accordance with one embodiment of the present invention, the encryption/decryption module part 170 (in FIG.13) can be customized according to the user's request at the time of manufacturing or initial programming. For example, since the encryption/decryption card can be implemented in field programmable logic devices (FPLDs), such as FPGAs and CPLDs, the encryption/decryption card or apparatus can be programmed in accordance with the user's specification (e.g., the degree of security, transmission speed, required protocol or standard, specific storage medium and/or format to be used, etc.) with specific settings of the hash keys and encryption tables (encryption information)

[0059] In addition, the user and the computer do not have to know the settings, and the settings are not accessible to the user and computer, such information cannot be stolen from the user or the computer to "crack the code." Furthermore, the encryption algorithm, the encryption key, and optionally the encryption parameter are practically changed for every data segment, and which algorithm, key, and parameter to be used are only "known" to the data segment itself to be encrypted. Since the encryption algorithm, key, and/or parameter are automatically changed based on certain data contained in the

data segment itself, synchronization between the transmitting side and the receiving side is unnecessary.

[0060] FIG. 14 schematically illustrates an example of application of the present invention to secure communications via the Internet. As shown in FIG. 14, users 180. 182, 184 can use respective encryption/decryption apparatuses 190, 192, and 194 in accordance with one embodiment of the present invention. The encryption/decryption apparatuses 190, 192, and 194 may be the encryption/decryption apparatus 10 or encryptor/decryptor 150 as described above. All of the encryption/decryption apparatuses 190, 192, and 194 are programmed identically and provided with the same settings, for example, the same hash keys and encryption tables. As shown in FIG. 14, the encryption/decryption apparatus may be used by more than one computers 184 and 186. For example, the encryption/decryption apparatus 194 may be used with a hub within a LAN such that all data transmissions from the computers or host connected to the hub are encrypted

[0061] In accordance with one embodiment of the present invention, since the IP header of each data packet is not encrypted, the encryption/decryption scheme of one embodiment of the present invention does not affect routing or switching of the data packets via the Internet or other networks (i.e., operations in the network protocol layer). In addition, in the case where some routers may possibly look into a packet field other than IP header in their routing operation, the first predetermined portion can be selected such that it includes the IP header and such portion of the data field to be used by the routers.

[0062] In accordance with one embodiment of the present invention, as described above, each data segment is encrypted using the two-level encryption That is, the data segment other than the first and second predetermined portions is encrypted using the information contained in the second predetermined portion. Then, the second predetermined portion is encrypted using the information contained in the first predetermined portion. Thus, although the first predetermined portion contains plaintext, the second predetermined portion containing encrypted data (ciphertext) provides

additional level of security, since the second predetermined portion and the remaining portion are typically encrypted by a different encryption algorithm, a different encryption key, and/or a different encryption parameter. In addition, since the encryption algorithm, the encryption key, and/or the encryption parameter are changed for every data segment, it is practically impossible to clack the code by a hacker

[0063] While embodiments and applications of this invention have been shown and described, it would be apparent to those skilled in the art having the benefit of this disclosure that many more modifications than mentioned above are possible without departing from the inventive concepts herein. The invention, therefore, is not to be restricted except in the spirit of the appended claims.

CLAIMS

What is claimed is.

1. A method for cryptographically processing data, said method comprising:

receiving a plurality of data segments;

selecting, for each data segment, a set of encryption information based on data contained in a predetermined portion of the data segment to be encrypted; and

encrypting each data segment using the set of encryption information selected for the data segment.

2. The method of claim 1, wherein said selecting comprising:

changing at least one of an encryption algorithm, an encryption key, and an encryption parameter for each data segment based on the data contained in the predetermined portion.

3. The method of claim 1, wherein said selecting comprises:

generating, for each data segment, a value from data contained in the predetermined portion of the data segment; and

selecting a set of encryption information associated with the generated value, the set of encryption information including an encryption algorithm, an encryption key, and optionally an encryption parameter.

4. The method of claim 3, wherein said generating a value comprises:

hashing the data contained in the predetermined portion using a hash key.

5 The method of claim 3, further comprising:

providing an encryption table containing

an encryption type identifier;

an encryption key for the encryption type; and

an encryption parameter,

for each entry associated with a generate value.

6. The method of claim 1, wherein the predetermined portion comprises:

a first predetermined portion for selecting a first set of encryption information, the first set comprising a first encryption algorithm, a first encryption key, and optionally a first encryption parameter, and

a second predetermined portion for selecting a second set of encryption information, the second set comprising a second encryption algorithm, a second encryption key, and optionally a second encryption parameter.

7. The method of claim 6, wherein said receiving comprises:

receiving a data stream including a plurality of data packets, each data packet corresponding to a data segment

8. The method of claim 7, wherein the first predetermined portion contains data for a first protocol layer, and the second predetermined portion contains data for a second protocol layer, wherein the first protocol layer is lower than the second protocol layer.

9. The method of claim 7, wherein the first predetermined portion is an Internet Protocol (IP) header of the data packet.

10. The method of claim 9, wherein the second predetermined portion is a selected portion of a data field of the data packet

11 The method of claim 9, wherein the second predetermined portion is a Transmission Control Protocol (TCP) header of the data packet.

12 The method of claim 9, wherein the second predetermined portion is a User Datagram Protocol (UDP) header of the data packet.

13 The method of claim 6, wherein said receiving comprises:

reading the plurality of data segments from corresponding sectors in a data storage device.

14 The method of claim 13, wherein the first predetermined portion is a first selected portion in a sector in a data storage device, and the second predetermined portion is a second selected portion in the sector.

15. The method of claim 6, further comprising:

encrypting the second predetermined portion using the first set of encryption information.

16. The method of claim 15, further comprising:

encrypting the remaining portion of the data segment using the second set of encryption information

17. The method of claim 16, further comprising:

generating an encrypted data segment for each of the original data segments, the encrypted data segment having a first predetermined portion, a second predetermined portion, and a remaining portion, the first predetermined portion containing the original data in the corresponding first predetermined portion of the original data segment, the second predetermined portion containing the encrypted data of the corresponding second predetermined portion of the original data segment, and the remaining portion containing the encrypted data of the corresponding remaining portion of the original data segment.

18 The method of claim 17, further comprising:

transmitting a plurality of encrypted data segments as a stream of encrypted data.

19 The method of claim 17, further comprising:

storing a plurality of encrypted data segments on a data storage device, each encrypted data segment corresponding to a respective data sector of the data storage device

20 The method of claim 17, further comprising:

receiving the encrypted data including a plurality of encrypted data segments;

selecting, for each encrypted data segment, a first set of encryption information based on data contained in the first predetermine portion of the encrypted data segment;

decrypting the encrypted data contained in the second predetermined portion of each encrypted data segment using the first set of encryption information selected for the encrypted data segment,

selecting, for each encrypted data segment, a second set of encryption information based on the decrypted data of the second predetermined portion; and

decrypting the remaining portion of each encrypted data segment using the second set of encryption information selected for the encrypted data segment.

21. The method of claim 20, wherein said selecting the first encryption information comprises·

generating a first value from the original data contained in the first predetermined portion of the encrypted data segment

22. The method of claim 21, wherein said generating the first value comprises:

hashing the data contained in the first predetermined portion using a first hash key

23. The method of claim 20, wherein said selecting the second encryption information comprises

generating a second value from the decrypted data of the second predetermined portion of the encrypted data segment.

24. The method of claim 23, wherein said generating the second value comprises:

hashing the decrypted data of the second predetermined portion using a second hash key.

25 A method for cryptographically processing data, said method comprising:

receiving a plurality of encrypted data segments, each of the encrypted data segments having a predetermined portion,

selecting, for each encrypted data segment, a set of encryption information based on data contained in the predetermined portion of the encrypted data segment; and

decrypting each encrypted data segment using the encryption information selected for the encrypted data segment

26 The method of claim 25, wherein said selecting comprises:

generating, for each encrypted data segment, a value from data contained in the predetermined portion of the encrypted data segment; and

selecting a set of encryption information associated with the generated value, the set of encryption information including an encryption algorithm, an encryption key, and optionally an encryption parameter.

27. The method of claim 26, wherein said generating a value comprises:

hashing the data contained in the predetermined portion using a hash key.

28 The method of claim 27, further comprising:

providing an encryption table, the encryption table containing:

an encryption type identifier,

an encryption key for the encryption type; and

an encryption parameter,

for each entry associated with a generated value.

29 The method of claim 25, wherein the predetermined portion comprises:

a first predetermined portion for selecting a first set of encryption information, the first set comprising a first encryption algorithm, a first encryption key, and optionally a first encryption parameter; and

a second predetermined portion for selecting a second set of encryption information, the second set comprising a second encryption algorithm, a second encryption key, and optionally a second encryption parameter.

30 The method of claim 29, wherein said receiving comprises:

receiving an encrypted data stream including a plurality of encrypted data packets, each encrypted data packet corresponding to an encrypted data segment.

31. The method of claim 30, wherein the first predetermined portion contains data for a first protocol layer, and the second predetermined portion contains data for a second protocol layer, wherein the first protocol layer is lower than the second protocol layer.

32. The method of claim 30, wherein the first predetermined portion is an Internet Protocol (IP) header of the data packet.

33. The method of claim 32, wherein the second predetermined portion is a selected portion of a data field of the data packet.

34. The method of claim 32, wherein the second predetermined portion is a Transmission Control Protocol (TCP) header of the data packet

35 The method of claim 32, wherein the second predetermined portion is a User Datagram Protocol (UDP) header of the data packet

36. The method of claim 29, wherein said receiving comprises.

reading the plurality of encrypted data segments from corresponding sectors in a data storage device.

37. The method of claim 36, wherein the first predetermined portion is a first selected portion in a sector in a data storage device, and the second predetermined portion is a second selected portion in the sector.

38 The method of claim 29, wherein data contained in the second predetermined portion of the encrypted data segment has been encrypted using the first set of encryption information.

39. The method of claim 38, wherein data contained in the remaining portion of the encrypted data segment has been encrypted using the second set of encryption information

40 An apparatus for cryptographically processing data, comprising:

an input buffer adapted to receive data including a plurality of data segments;

an encryption module adapted to encrypt each data segment;

a controller coupled to said input buffer and said encryption module, said controller being adapted to select a set of encryption information for each data segment based on data contained in a predetermined portion of the data segment to be encrypted; and

an output buffer coupled to said controller and said encryption module, said output buffer being adapted to output encrypted data including a plurality of encrypted data segments.

41. The apparatus of claim 40, wherein said controller changes at least one of an encryption algorithm, an encryption key, and an encryption parameter for each data segment.

42. The apparatus of claim 40, wherein said encryption module comprises:

a plurality of encryption engines, each encryption engine corresponding to a respective encryption algorithm

43 The apparatus of claim 40, wherein said encryption module further comprises:

a data buffer coupled to each of the plurality of encryption engines

44. The apparatus of claim 40, wherein said controller comprises

a data selector adapted to select a predetermined portion of each data segment;

an encryption selector coupled with said data selector, adapted to select a set of encryption information in accordance with data contained in the predetermined portion, the set of encryption information including an encryption algorithm, an encryption key, and optionally an encryption parameter; and

an encryption controller adapted to select and activate an encryption engine based on the encryption information

45. The apparatus of claim 40, wherein said controller further comprises:

a value generator coupled to said data selector, adapted to generate a value from the data contained in the predetermined portion

46 The apparatus of claim 45, wherein said value generator is adapted to hash the data contained in the predetermined portion using a hash key.

47 The apparatus of claim 45, wherein said encryption controller comprises an encryption table containing

an encryption type identifier;

an encryption key for the encryption type; and

an encryption parameter,

for each entry associated with a generated value.

48. The apparatus of claim 40, wherein the predetermined portion of each data segment comprises.

a first predetermined portion; and

a second predetermined portion.

49. The apparatus of claim 48, wherein the plurality of data segments are data packets in a data stream.

50 The apparatus of claim 49, wherein the first predetermined portion contains data for a first protocol layer, and the second predetermined portion contains data for a second protocol layer, wherein the first protocol layer is lower than the second protocol layer.

51 The apparatus of claim 49, wherein the first predetermined portion is an Internet Protocol (IP) header of the data packet.

52. The apparatus of claim 51, wherein the second predetermined portion is a selected portion of a data field of the data packet.

53 The apparatus of claim 51, wherein the second predetermined portion is a Transmission Control Protocol (TCP) header of the data packet.

54. The apparatus of claim 51, wherein the second predetermined portion is a User Datagram Protocol (UDP) header of the data packet.

55. The method of claim 48, wherein the plurality of data segments are sectors in a data storage device

56 The apparatus of claim 55, wherein the first predetermined portion is a first selected portion in a sector in a data storage device, and the second predetermined portion is a second selected portion in the sector.

57. The apparatus of claim 48, wherein said controller comprises:

a first encryption table for selecting the first set of encryption information based on data contained in the first predetermined portion; and

a second encryption table for selecting the second set of encryption information based on data contained in the second predetermined portion.

58. An apparatus for cryptographically processing data, comprising:

an input buffer adapted to receive a plurality of encrypted data segments, each of the encrypted data segments having a predetermined portion,

an encryption module adapted to decrypt each encrypted data segment;

a controller coupled to said input buffer and said decryption module, said controller being adapted to select a set of encryption information for each encrypted data segment based on data contained in a predetermined portion of the encrypted data segment; and

an output buffer coupled to said controller and said decryption module, said output buffer being adapted to output decrypted data including a plurality of decrypted data segments.

59. The apparatus of claim 58, wherein said decryption module comprises:

a plurality of decryption engines, each decryption engine corresponding to a respective encryption algorithm

60. The apparatus of claim 58, wherein said decryption module further comprises:

a data buffer coupled to each of the plurality of decryption engines.

61. The apparatus of claim 58, wherein said controller comprises:

a data selector adapted to select a predetermined portion of each encrypted data segment,

a decryption selector coupled with said data selector, adapted to select a set of decryption information in accordance with data contained in the predetermined portion, the set of decryption information including an encryption algorithm, an encryption key, and optionally an encryption parameter; and

a decryption controller adapted to select and activate a decryption engine based on the encryption information.

62. The apparatus of claim 58, wherein said controller further comprises:

a value generator coupled to said data selector, adapted to generate a value from the data contained in the predetermined portion.

63 The apparatus of claim 62, wherein said value generator is adapted to hash the data contained in the predetermined portion using a hash key.

64. The apparatus of claim 62, wherein said decryption controller comprises an encryption table containing:

an encryption type identifier;

an encryption key for the encryption type; and

an encryption parameter,

for each entry associated with a generated value.

65 The apparatus of claim 58, wherein the predetermined portion of each data segment comprises:

a first predetermined portion; and

a second predetermined portion.

66. The apparatus of claim 65, wherein the plurality of data segments are data packets in a data stream

67. The apparatus of claim 66, wherein the first predetermined portion contains data for a first protocol layer, and the second predetermined portion contains data for a second protocol layer, wherein the first protocol layer is lower than the second protocol layer.

68 The apparatus of claim 66, wherein the first predetermined portion is an Internet Protocol (IP) header of the data packet.

69 The apparatus of claim 68, wherein the second predetermined portion is a selected portion of a data field of the data packet.

70 The apparatus of claim 68, wherein the second predetermined portion is a Transmission Control Protocol (TCP) header of the data packet.

71. The apparatus of claim 68, wherein the second predetermined portion is a User Datagram Protocol (UDP) header of the data packet.

72 The method of claim 58, wherein the plurality of data segments are sectors in a data storage device

73. The apparatus of claim 72, wherein the first predetermined portion is a first selected portion in a sector in a data storage device, and the second predetermined portion is a second selected portion in the sector.

74. The apparatus of claim 58, wherein said controller comprises:

a first encryption table for selecting the first set of decryption information based on data contained in the first predetermined portion, and

a second encryption table for selecting the second set of decryption information based on data contained in the second predetermined portion.

75. An apparatus for cryptographically processing data, said apparatus comprising:

means for receiving a plurality of data segments;

means for selecting, for each data segment, a set of encryption information based on data contained in a predetermined portion of the data segment to be encrypted; and

means for encrypting each data segment using the set of encryption information selected for the data segment.

76 The apparatus of claim 75, wherein said means for selecting changes at least one of an encryption algorithm, an encryption key, and an encryption parameter for each data segment based on the data contained in the predetermined portion.

77 The apparatus of claim 75, wherein said means for selecting comprises:

means for generating, for each data segment, a value from data contained in the predetermined portion of the data segment, and

means for selecting a set of encryption information associated with the generated value, the set of encryption information including an encryption algorithm, an encryption key, and optionally an encryption parameter.

78 The apparatus of claim 77, wherein said means for generating a value comprises:

means for hashing the data contained in the predetermined portion using a hash key.

79 The apparatus of claim 77, further comprising:

means for providing an encryption type identifier, an encryption key for the encryption type, and an encryption parameter associated with a generate value.

80. The apparatus of claim 75, wherein the predetermined portion comprises:

a first predetermined portion for selecting a first set of encryption information, the first set comprising a first encryption algorithm, a first encryption key, and optionally a first encryption parameter; and

a second predetermined portion for selecting a second set of encryption information, the second set comprising a second encryption algorithm, a second encryption key, and optionally a second encryption parameter.

81 The apparatus of claim 80, further comprising:

means for encrypting the second predetermined portion using the first set of encryption information.

82. The apparatus of claim 81, further comprising:

means for encrypting the remaining portion of the data segment using the second set of encryption information.

83. The apparatus of claim 82, further comprising:

means for generating an encrypted data segment for each of the original data segments, the encrypted data segment having a first predetermined portion, a second predetermined portion, and a remaining portion, the first predetermined portion containing the original data in the corresponding first predetermined portion of the original data segment, the second predetermined portion containing the encrypted data of the corresponding second predetermined portion of the original data segment, and the remaining portion containing the encrypted data of the corresponding remaining portion of the original data segment.

84 The apparatus of claim 83, further comprising:

means for transmitting a plurality of encrypted data segments as a stream of encrypted data

85. The apparatus of claim 83, further comprising:

means for storing a plurality of encrypted data segments on a data storage device, each encrypted data segment corresponding to a respective data sector of the data storage device.

86. The apparatus of claim 83, further comprising:

means for receiving the encrypted data including a plurality of encrypted data segments,

means for selecting, for each encrypted data segment, a first set of encryption information based on data contained in the first predetermine portion of the encrypted data segment;

means for decrypting the encrypted data contained in the second predetermined portion of each encrypted data segment using the first set of encryption information selected for the encrypted data segment;

means for selecting, for each encrypted data segment, a second set of encryption information based on the decrypted data of the second predetermined portion; and

means for decrypting the remaining portion of each encrypted data segment using the second set of encryption information selected for the encrypted data segment.

87 The apparatus of claim 86, wherein said means for selecting the first encryption information comprises:

means for generating a first value from the original data contained in the first predetermined portion of the encrypted data segment.

88 The apparatus of claim 87, wherein said means for generating the first value comprises:

means for hashing the data contained in the first predetermined portion using a first hash key

89. The apparatus of claim 86, wherein said means for selecting the second encryption information comprises:

means for generating a second value from the decrypted data of the second predetermined portion of the encrypted data segment.

90. The apparatus of claim 89, wherein said means for generating the second value comprises:

means for hashing the decrypted data of the second predetermined portion using a second hash key.

91 An apparatus for cryptographically processing data, said apparatus comprising:

means for receiving a plurality of encrypted data segments, each of the encrypted data segments having a predetermined portion;

means for selecting, for each encrypted data segment, a set of encryption information based on data contained in the predetermined portion of the encrypted data segment; and

means for decrypting each encrypted data segment using the encryption information selected for the encrypted data segment.

92. The apparatus of claim 91, wherein said means for selecting comprises:

means for generating, for each encrypted data segment, a value from data contained in the predetermined portion of the encrypted data segment; and

means for selecting a set of encryption information associated with the generated value, the set of encryption information including an encryption algorithm, an encryption key, and optionally an encryption parameter.

93. The apparatus of claim 92, wherein said means for generating a value comprises:

means for hashing the data contained in the predetermined portion using a hash key

94. The apparatus of claim 93, further comprising:

means for providing an encryption type identifier, an encryption key for the encryption type, and an encryption parameter associated with a generated value.

95. The apparatus of claim 91, wherein the predetermined portion comprises:

a first predetermined portion for selecting a first set of encryption information, the first set comprising a first encryption algorithm, a first encryption key, and optionally a first encryption parameter, and

a second predetermined portion for selecting a second set of encryption information, the second set comprising a second encryption algorithm, a second encryption key, and optionally a second encryption parameter.

96. The apparatus of claim 95, wherein data contained in the second predetermined portion of the encrypted data segment has been encrypted using the first set of encryption information

97 The apparatus of claim 96, wherein data contained in the remaining portion of the encrypted data segment has been encrypted using the second set of encryption information.

ABSTRACT OF THE DISCLOSURE

A method and apparatus cryptographically process data including a plurality of data segments. The cryptographic process includes (a) receiving a plurality of data segments, (b) selecting, for each data segment, a set of encryption information based on data contained in a predetermined portion of the data segment to be encrypted, and (c) encrypting each data segment using the set of encryption information selected for the data segment. At least one of an encryption algorithm, an encryption key, and an encryption parameter may be changed for each data segment based on the data contained in the predetermined portion. The predetermined portion may include a first predetermined portion for selecting a first set of encryption information, and a second predetermined portion for selecting a second set of encryption information, the encryption information including an encryption algorithm, an encryption key, and optionally an encryption parameter.

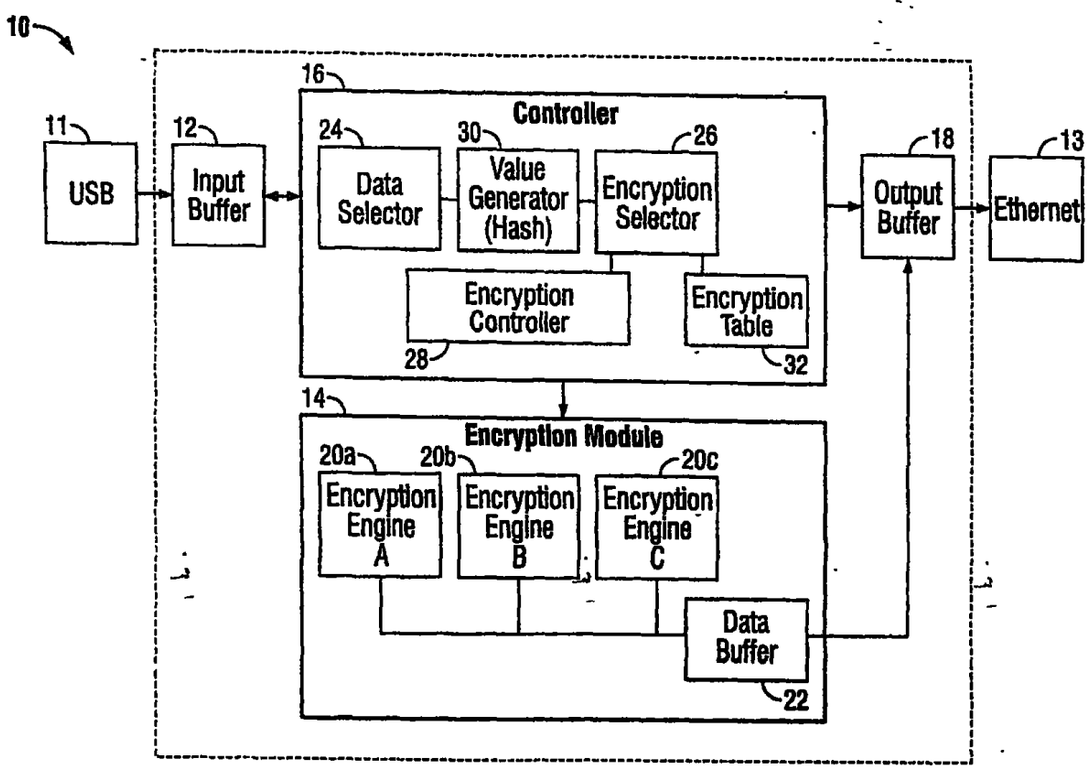


FIG. 1A

WO 2005/088893
1/13
PCT/US2004/004117

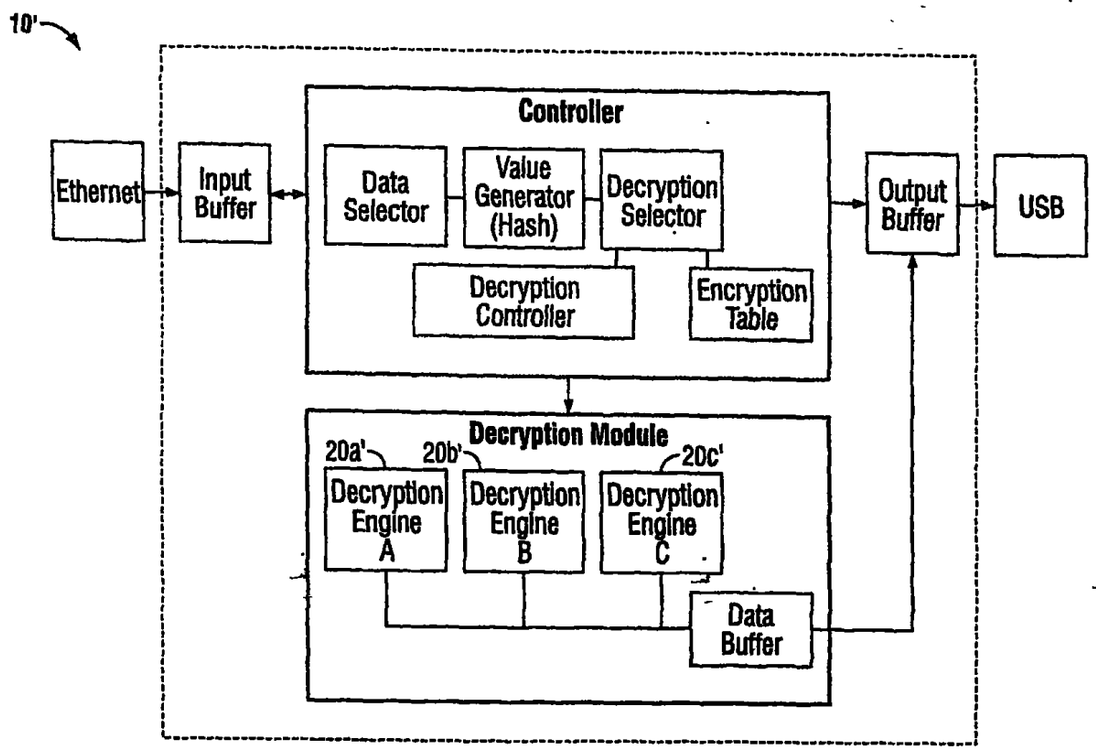

10'
Ethernet
Input Buffer
Controller
Data Selector
Value Generator (Hash)
Decryption Selector
Decryption Controller
Encryption Table
Output Buffer
USB
Decryption Module
20a'
20b'
20c'
Decryption Engine A
Decryption Engine B
Decryption Engine C
Data Buffer

FIG. 1B

32

Index	Encryption Type	Key	Initial Vector
0	3 DES	Key 1	5
1	AES	Key 2	2
2	3 DES	Key 3	7
3	IDEA	Key 4	8
4	AES	Key 5	3
⋮	⋮	⋮	⋮

FIG. 2

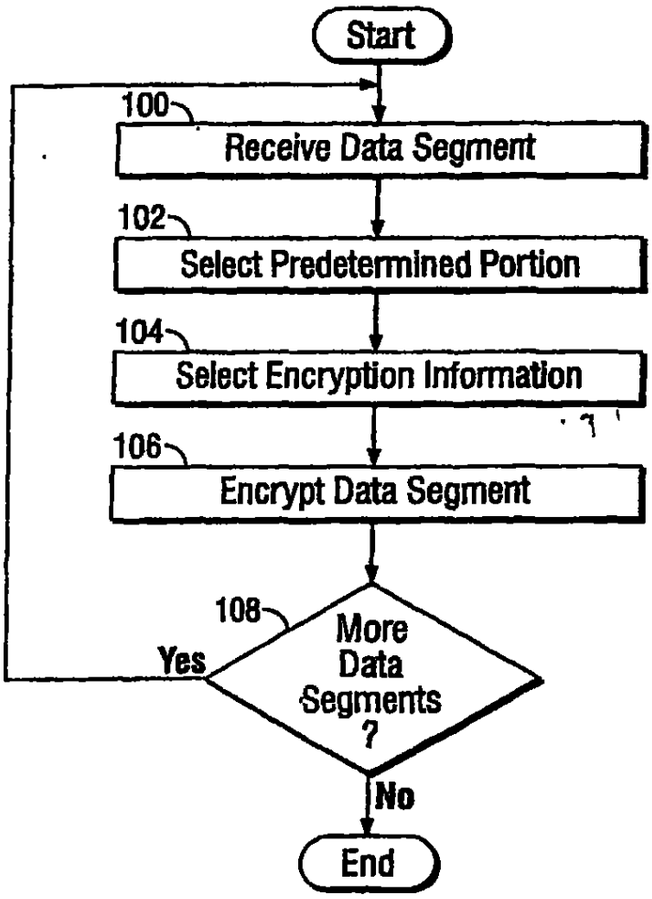


FIG. 3

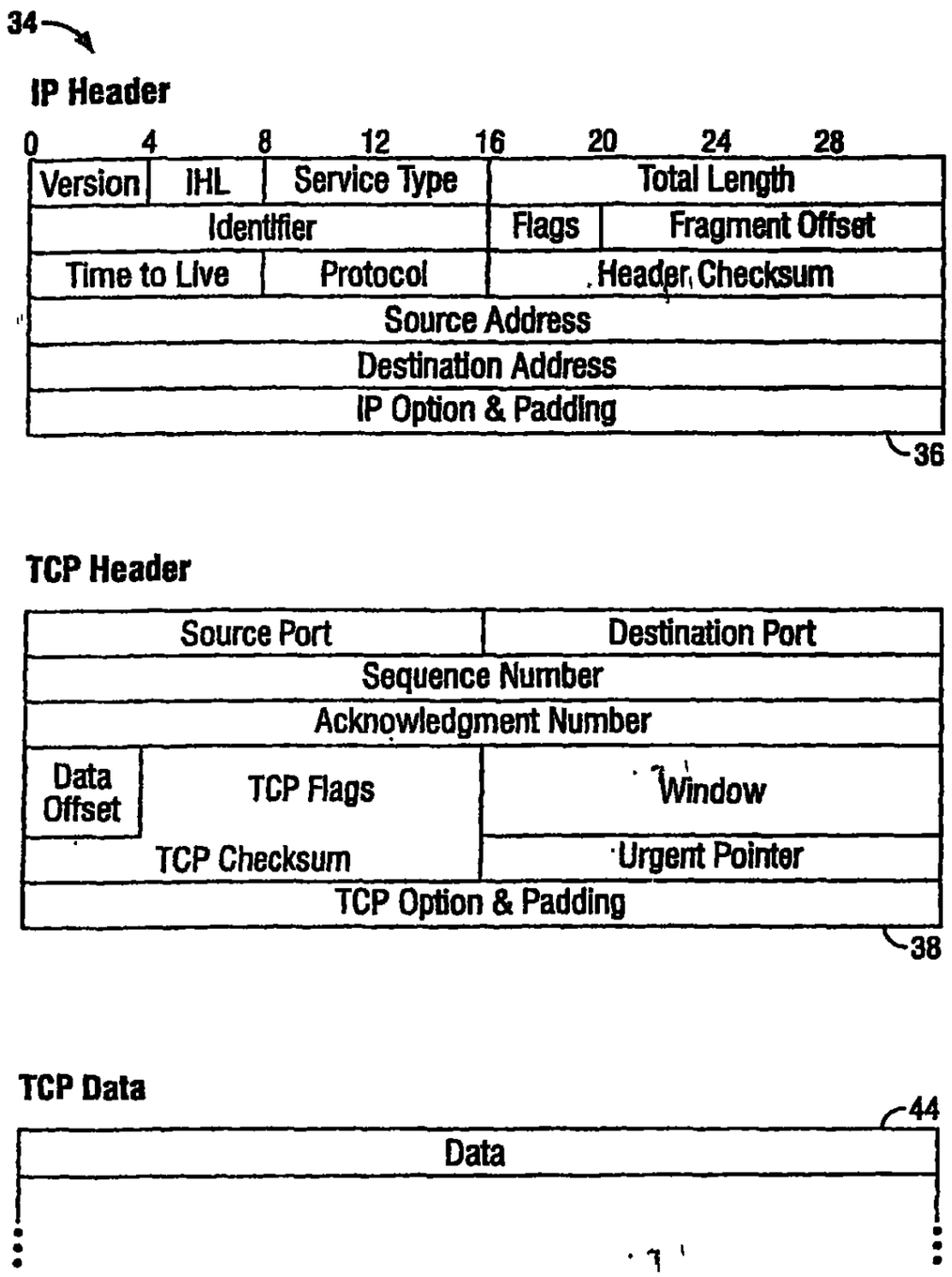

34
IP Header
0 4 8 12 16 20 24 28
Version
IHL
Service Type
Total Length
Identifier
Flags
Fragment Offset
Time to Live
Protocol
Header Checksum
Source Address
Destination Address
IP Option & Padding
36
TCP Header
Source Port
Destination Port
Sequence Number
Acknowledgment Number
Data Offset
TCP Flags
Window
TCP Checksum
Urgent Pointer
TCP Option & Padding
38
TCP Data
44
Data

FIG. 4

133

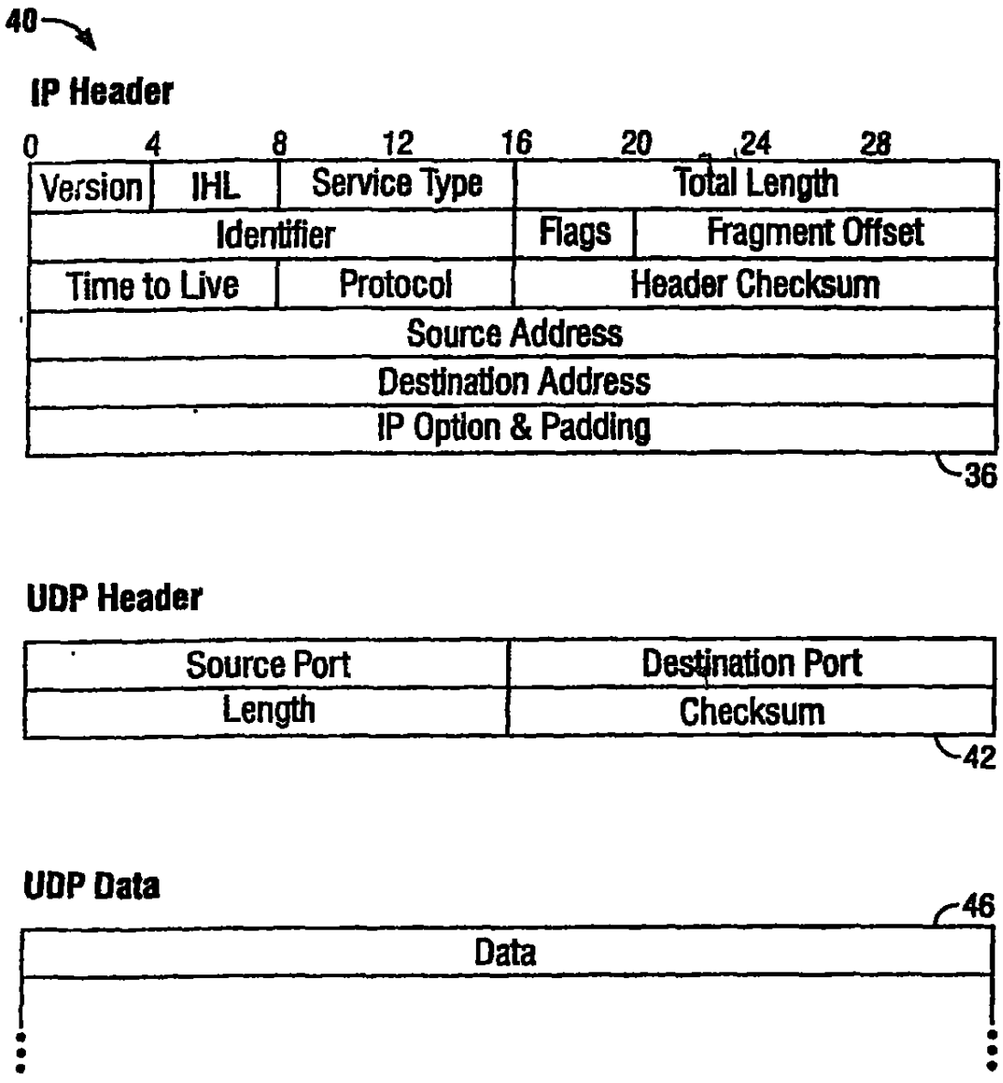

40
IP Header
0 4 8 12 16 20 24 28
Version
IHL
Service Type
Total Length
Identifier
Flags
Fragment Offset
Time to Live
Protocol
Header Checksum
Source Address
Destination Address
IP Option & Padding
36
UDP Header
Source Port
Destination Port
Length
Checksum
42
UDP Data
46
Data

FIG. 5

134

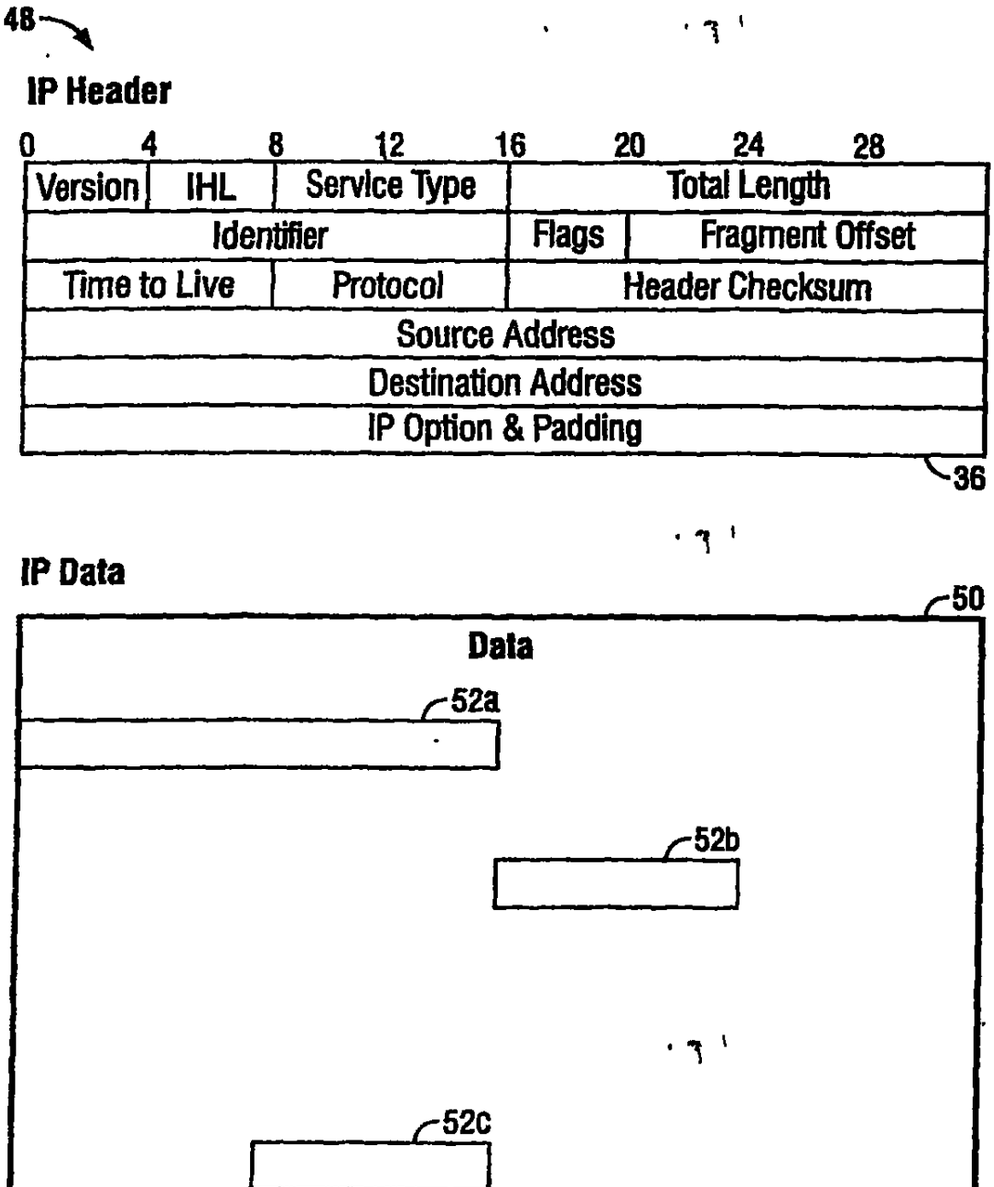

48
IP Header
0
4
8
12
16
20
24
28
Version
IHL
Service Type
Total Length
Identifier
Flags
Fragment Offset
Time to Live
Protocol
Header Checksum
Source Address
Destination Address
IP Option & Padding
36
IP Data
50
Data
52a
52b
52c

FIG. 6

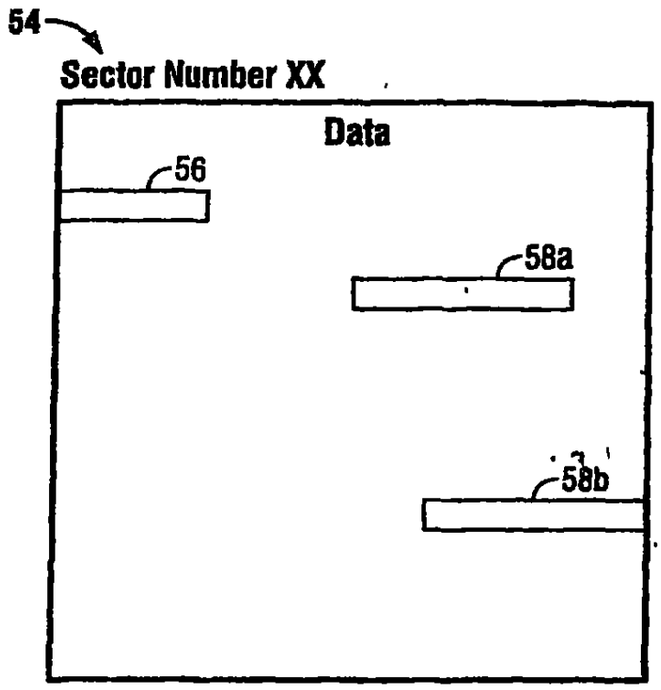

54
Sector Number XX
Data
56
58a
58b

FIG. 7

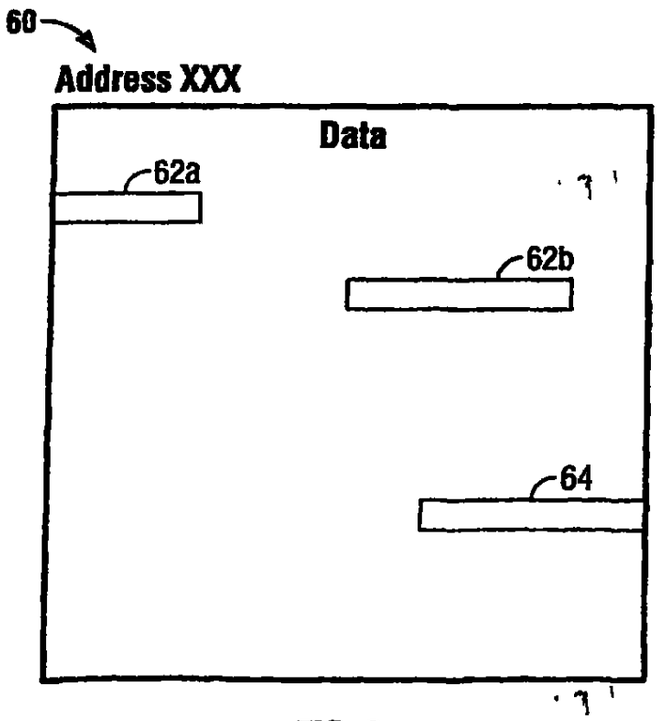

60
Address XXX
Data
62a
62b
64

FIG. 8

136

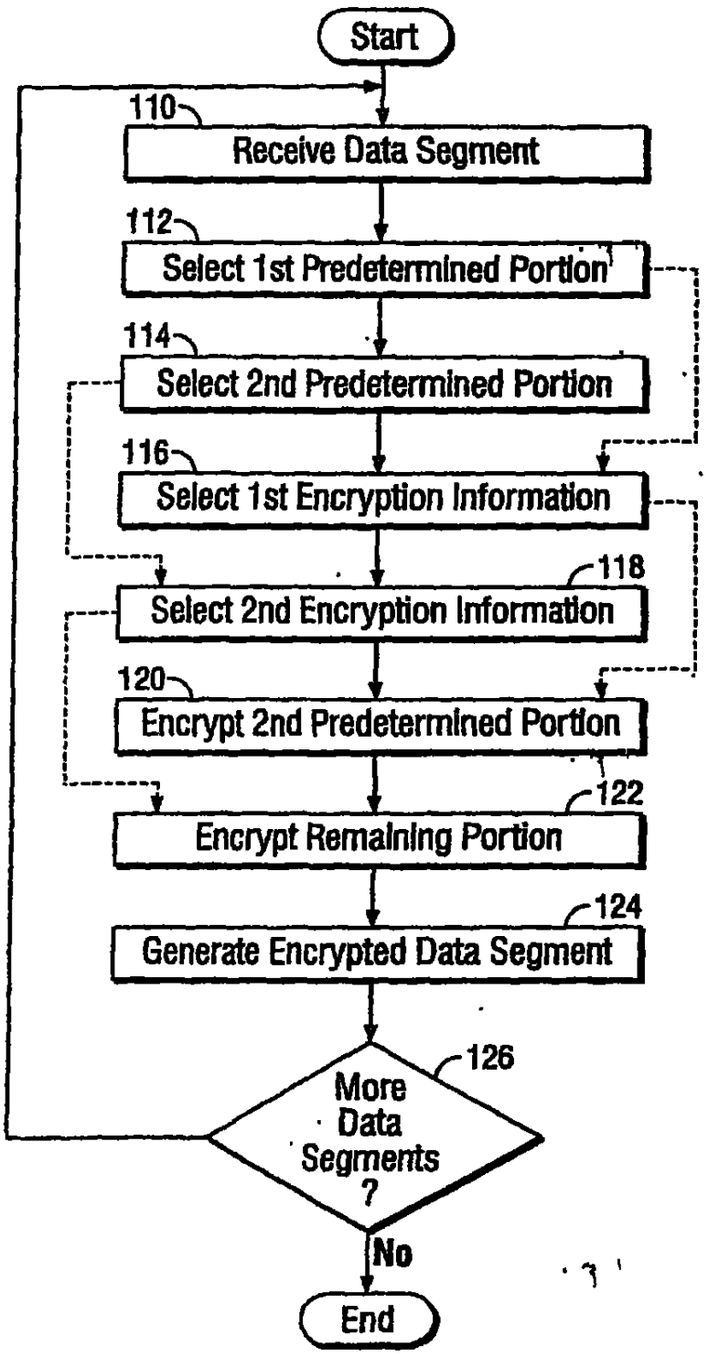

Start
110
Receive Data Segment
112
Select 1st Predetermined Portion
114
Select 2nd Predetermined Portion
116
Select 1st Encryption Information
118
Select 2nd Encryption Information
120
Encrypt 2nd Predetermined Portion
122
Encrypt Remaining Portion
124
Generate Encrypted Data Segment
126
More Data Segments ?
No
End

FIG. 9

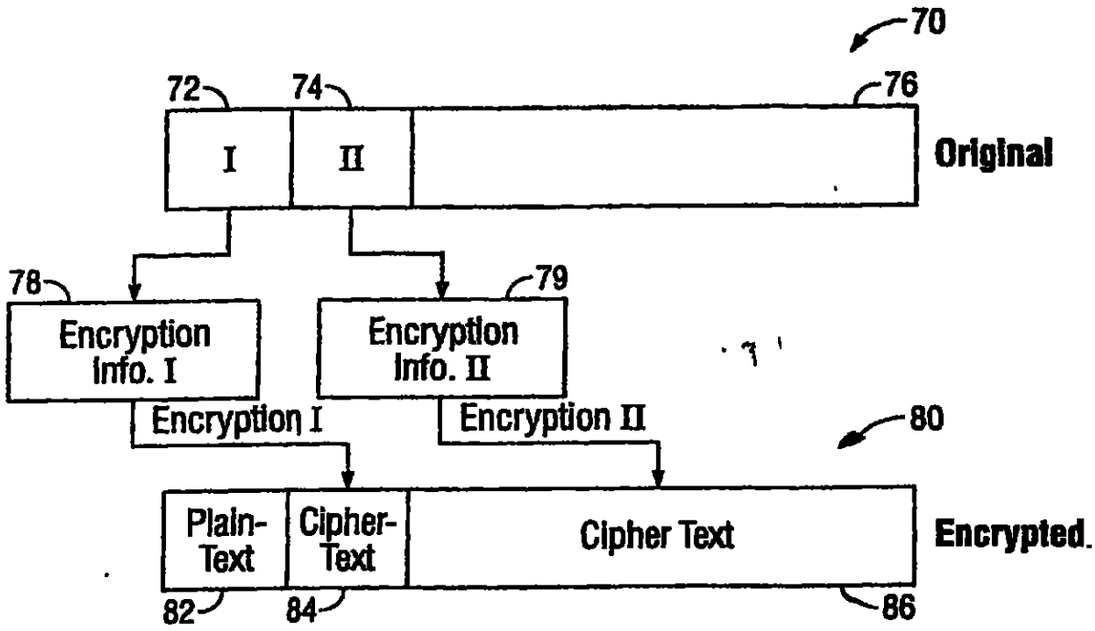

70
72
74
76
I
II
Original
78
79
Encryption Info. I
Encryption Info. II
Encryption I
Encryption II
80
Plain-Text
Cipher-Text
Cipher Text
Encrypted
82
84
86

FIG. 10

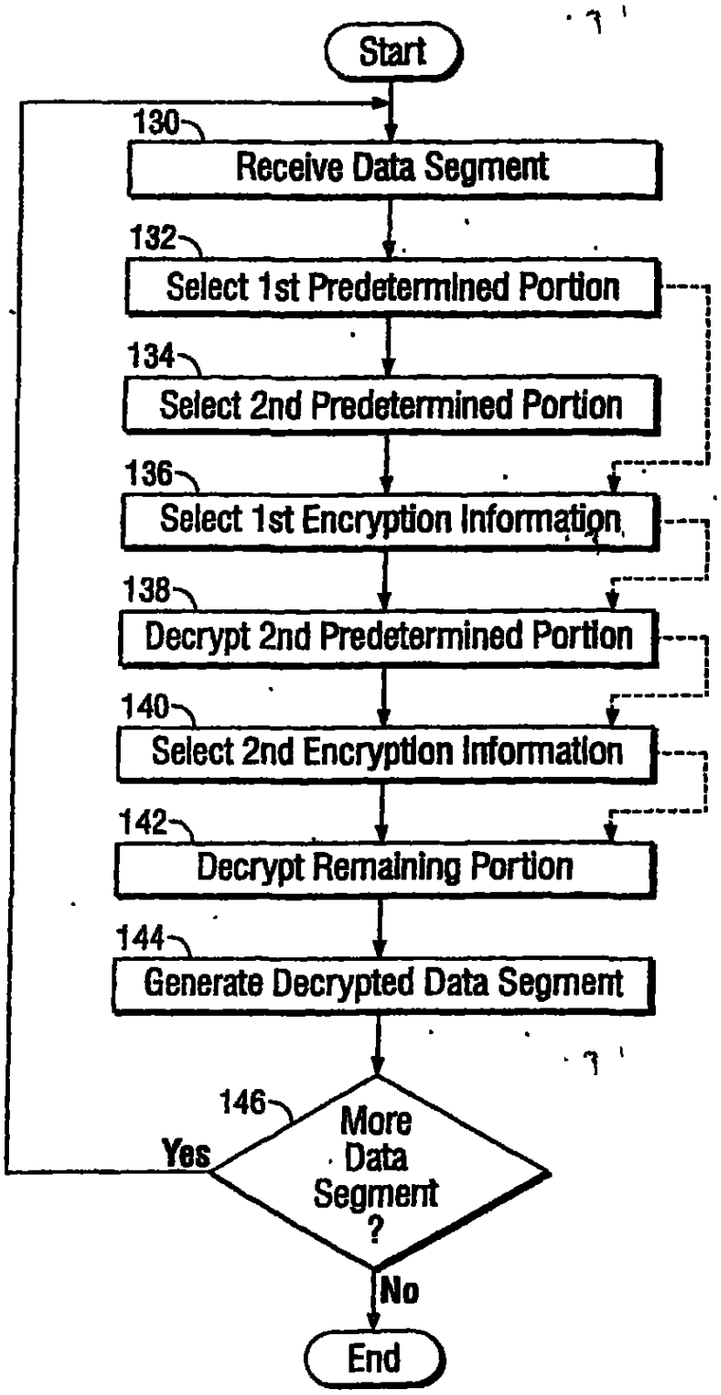

Start
130
Receive Data Segment
132
Select 1st Predetermined Portion
134
Select 2nd Predetermined Portion
136
Select 1st Encryption Information
138
Decrypt 2nd Predetermined Portion
140
Select 2nd Encryption Information
142
Decrypt Remaining Portion
144
Generate Decrypted Data Segment
146
More Data Segment ?
Yes
No
End

FIG. 11

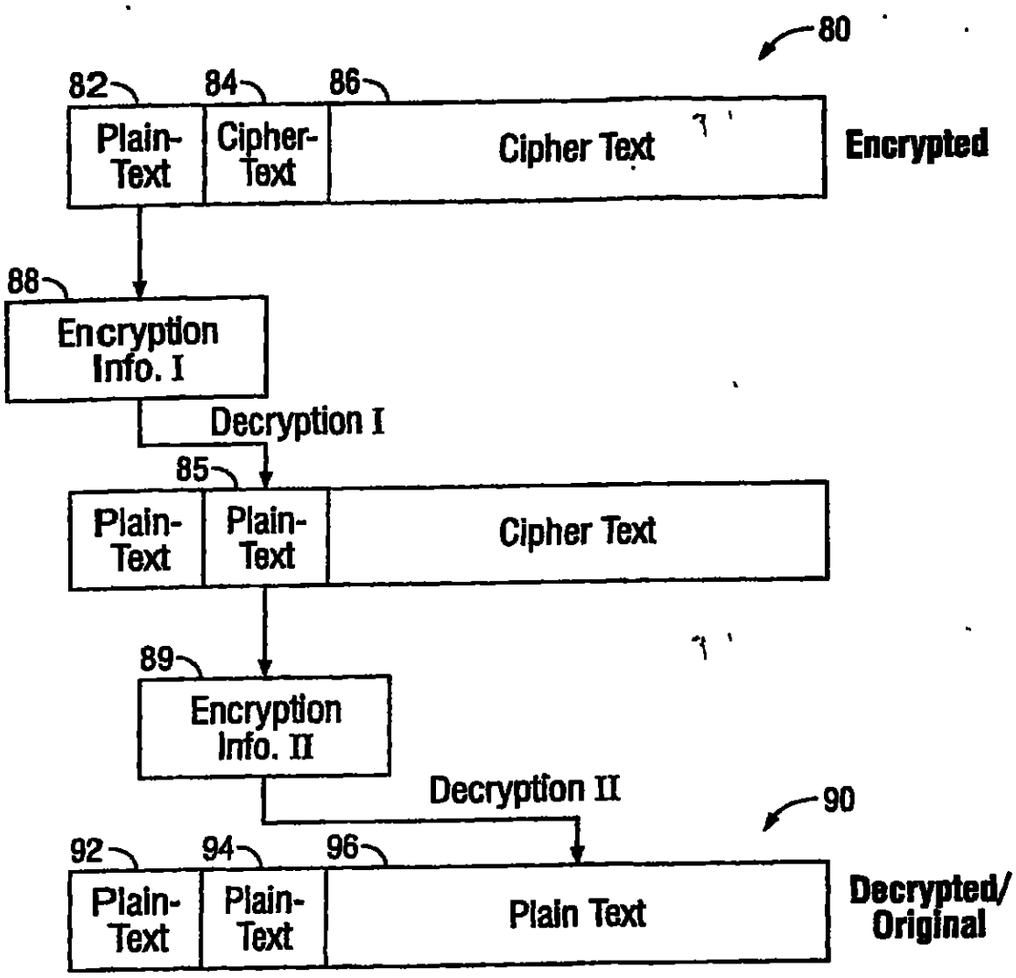

80
82
84
86
Plain-Text
Cipher-Text
Cipher Text
Encrypted
88
Encryption Info. I
Decryption I
85
Plain-Text
Plain-Text
Cipher Text
89
Encryption Info. II
Decryption II
90
92
94
96
Plain-Text
Plain-Text
Plain Text
Decrypted/ Original

FIG. 12

140

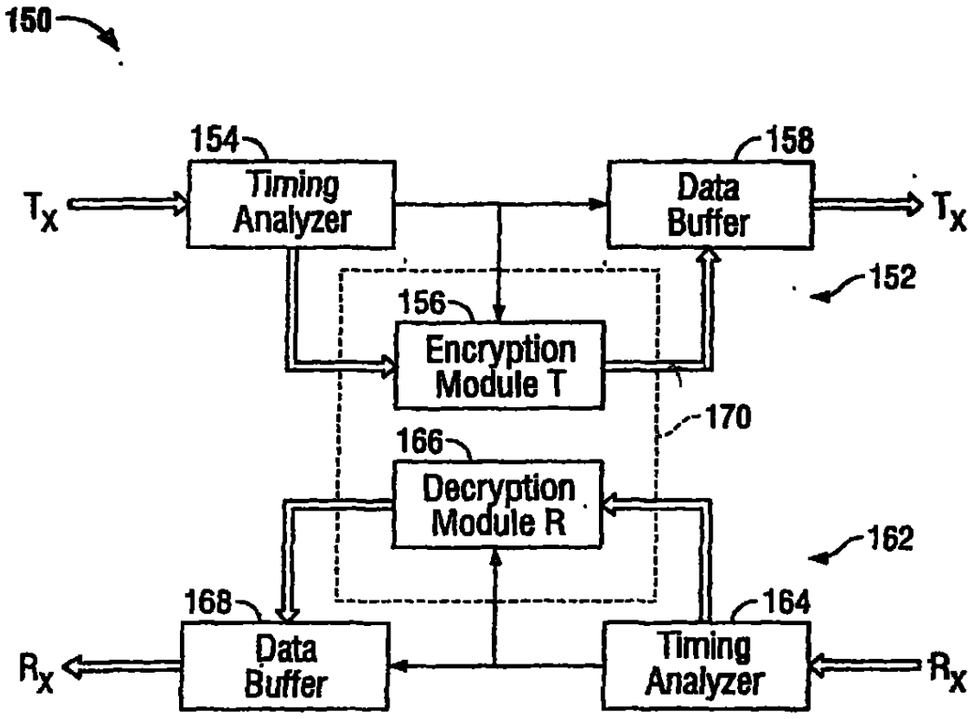

150
154
Timing Analyzer
158
Data Buffer
Tx
Tx
152
156
Encryption Module T
170
166
Decryption Module R
162
168
Data Buffer
164
Timing Analyzer
Rx
Rx

FIG. 13

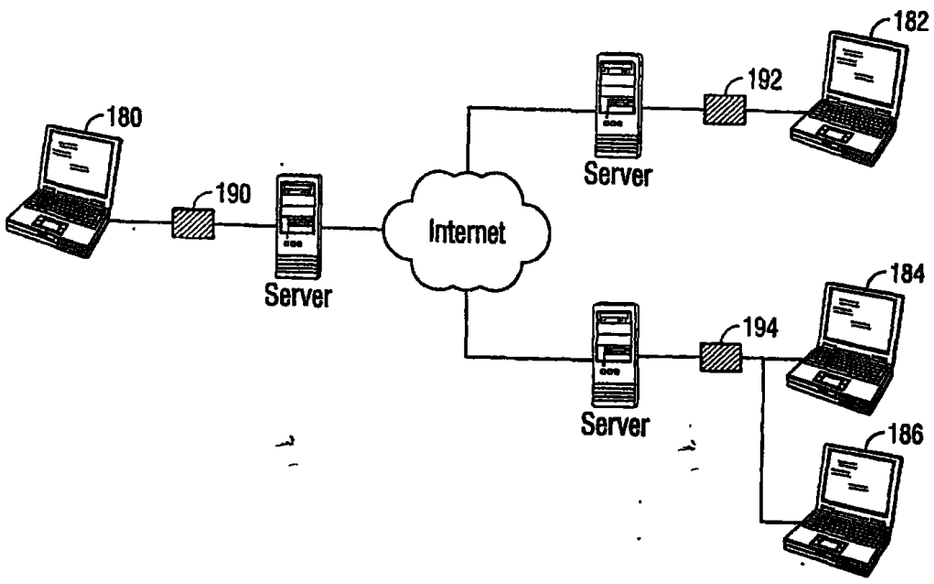


FIG. 14

142

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US04/04117

A. CLASSIFICATION OF SUBJECT MATTER
IPC(7) : H04L 9/00
US CL : 713/200
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 713/200, 164, 165, 201; 380/37, 28

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
Please See Continuation Sheet

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X --- Y	US 6,269,164 B1 (PIRES) 31 July 2001 (31 07 2001), column 6 line 62 to column 7 line 24, column 7 line 47 to column 8 line 25, column 9 line 49 to column 10 line 25; column 12, lines 40-61, column 15, lines 30-55; column 18, lines 32-67	1-7, 13-30, 36-39, 75-97 --- 8-12, 31-35
X --- Y	US 5,008,935 A (ROBERTS) 16 April 1991 (16.04 1991), column 2, lines 15-45; column 3, lines 1-64.	40-49, 55-66, 72-74 --- 50-54, 67-71
Y	US 6,160,797 A (ROBERT, III et al) 12 December 2000 (12 12 2000), column 8 line 57 to column 9 line 60	8-12, 31-35, 50-54, 67-71
A	Makki et al, The SECURE Model for Enterprise Connectivity IEEE, 2000, pages 176-182.	1-97
A	Wu et al, Communication-Friendly Encryption of Multimedia IEEE, 2002, pages 292-295.	1-97
A	Chueng et al, Implementation of Pipelined Data Encryption Standard (DES) Using Altera CPLD IEEE, 2000, pages III-17 to III-21.	1-97
A	Steward, Shawn, Practicing safe data Cellular Business, January 1997, pages 64 and 66	1-97

☒ Further documents are listed in the continuation of Box C ☐ See patent family annex.

* Special categories of cited documents
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure use exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance, the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
18 August 2004 (18 08 2004)	09 SEP 2004
Name and mailing address of the ISA/US Mail Stop PCT, Attn ISA/US Commissioner for Patents P.O Box 1450 Alexandria, Virginia 22313-1450 Facsimile No (703)305-3230	Authorized officer for Michelle F. Eason Ayaz R Sheikh Telephone No. 703-305-1373

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

PCT/US04/04117

Continuation of B. FIELDS SEARCHED Item 3:
EAST, Palm, Proquest, IEEE, Google
search terms data segements, data framgemins, data packets, packets, frame, encryption, algorithm, encryption algorithm, hash, key, encryption key, DES, IP, TCP, UDP, decryption, buffer

144

PCT

REQUEST

The undersigned requests that the present international application be processed according to the Patent Cooperation Treaty

For receiving Office use only

International Application No

International Filing Date

Name of receiving Office and "PCT International Application"

Applicant's or agent's file reference *(if desired) (12 characters maximum)* PYSC-0002/WO

Box No I TITLE OF INVENTION

METHOD AND APPARATUS FRO CRYPTOGRAPHICALLY PROCESSING DATA

Box No. II APPLICANT ☐ This person is also inventor

Name and address *(Family name followed by given name, for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below.)*

PsyCrypt, Inc
2635 North First Street
Suite 213
San Jose, California 95139
UNITED STATES OF AMERICA

Telephone No.
408-998-7156

Facsimile No
408-998-7156

Teleprinter No

Applicant's registration No with the Office

State *(that is, country)* of nationality
US

State *(that is, country)* of residence
US

This person is applicant for the purposes of ☐ all designated States ☒ all designated States except the United States of America ☐ the United States of America only ☐ the States indicated in the Supplemental Box

Box No III FURTHER APPLICANT(S) AND/OR (FURTHER) INVENTOR(S)

Name and address *(Family name followed by given name, for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below.)*

WATANABE, Masashi
49-1 Machisuji Iwawaki Hanoura-cho
Naka-gun Tokushima
JAPAN

This person is
☐ applicant only
☒ applicant and inventor
☐ inventor only *(If this check-box is marked, do not fill in below.)*

Applicant's registration No with the Office

State *(that is, country)* of nationality
JP

State *(that is, country)* of residence
JP

This person is applicant for the purposes of ☐ all designated States ☐ all designated States except the United States of America ☒ the United States of America only ☐ the States indicated in the Supplemental Box

☐ Further applicants and/or (further) inventors are indicated on a continuation sheet

Box No. IV AGENT OR COMMON REPRESENTATIVE, OR ADDRESS FOR CORRESPONDENCE

The person identified below is hereby/has been appointed to act on behalf of the applicant(s) before the competent International Authorities as. ☒ agent ☐ common representative

Name and address *(Family name followed by given name, for a legal entity, full official designation. The address must include postal code and name of country.)*

RITCHIE, David B., KREBS, Robert E., WINTERS, William; GILMER, Davis, HANISH, Marc; SCHAUB, John P., YEUNG, Adrienne; LO Thierry; ANDO, Masako ROBBINS, Steve, NIECE, William S Thelen Reid & Priest LLP, P O. BOX 640640; SAN JOSE, CALIFORNIA; UNITED STATES OF AMERICA 95164-0640

Telephone No
408.292 5800

Facsimile No
408.287.8040

Teleprinter No

Agent's registration No with the Office

☐ Address for correspondence: Mark this check-box where no agent or common representative is/has been appointed and the space above is used instead to indicate a special address to which correspondence should be sent

Box No. V DESIGNATIONS

The filing of this request constitutes under Rule 4.9(a), the designation of all Contracting States bound by the PCT on the international filing date, for the grant of every kind of protection available and, where applicable, for the grant of both regional and national patents

However,

☐ DE Germany is not designated for any kind of national protection

☐ KR Republic of Korea is not designated for any kind of national protection

☐ RU Russian Federation is not designated for any kind of national protection

(The check-boxes above may be used to exclude (irrevocably) the designations concerned in order to avoid the ceasing of the effect, under the national law, of an earlier national application from which priority is claimed See the Notes to Box No V as to the consequences of such national law provisions in these and certain other States)

Box No. VI PRIORITY CLAIM

The priority of the following earlier application(s) is hereby claimed

Filing date of earlier application *(day/month/year)*	Number of earlier application	Where earlier application is		
		national application country or Member of WTO	regional application * regional Office	international application receiving Office
item (1)				
item (2)				
item (3)				

☐ Further priority claims are indicated in the Supplemental Box

The receiving Office is requested to prepare and transmit to the International Bureau a certified copy of the earlier application(s) *(only if the earlier application was filed with the Office which for the purposes of this international application is the receiving Office)* identified above as

☐ all items ☐ item (1) ☐ item (2) ☐ item (3) ☐ other, see Supplemental Box

** Where the earlier application is an ARIPO application, indicate at least one country party to the Paris Convention for the Protection of Industrial Property or one Member of the World Trade Organization for which that earlier application was filed (Rule 4.10(b)(ii))*

Box No. VII INTERNATIONAL SEARCHING AUTHORITY

Choice of International Searching Authority (ISA) *(if two or more International Searching Authorities are competent to carry out the international search, indicate the Authority chosen the two-letter code may be used)*

ISA / US

Request to use results of earlier search; reference to that search *(if an earlier search has been carried out by or requested from the International Searching Authority)*

Date *(day/month/year)* Number Country *(or regional Office)*

Box No. VIII DECLARATIONS

The following declarations are contained in Boxes Nos VIII (i) to (v) *(mark the applicable check-boxes below and indicate in the right column the number of each type of declaration)*		Number of declarations
☐ Box No VIII (i)	Declaration as to the identity of the inventor	
☐ Box No VIII (ii)	Declaration as to the applicant's entitlement, as at the international filing date, to apply for and be granted a patent	
☐ Box No VIII (iii)	Declaration as to the applicant's entitlement, as at the international filing date, to claim the priority of the earlier application	
☒ Box No VIII (iv)	Declaration of inventorship (only for the purposes of the designation of the United States of America)	
☐ Box No VIII (v)	Declaration as to non-prejudicial disclosures or exceptions to lack of novelty	

Sheet No 3

Box No. IX CHECK LIST; LANGUAGE OF FILING

This international application contains		This international application is accompanied by the following item(s) *(mark the applicable check-boxes below and indicate in right column the number of each item)*	Number of items
(a) in paper form, the following number of sheets			
request (including declaration sheets)	3	1 ☒ fee calculation sheet	
description (excluding sequence listing and/or tables related thereto)	21	2 ☐ original separate power of attorney	
claims	16	3 ☐ original general power of attorney	
abstract	1	4 ☐ copy of general power of attorney, reference number, if any	
drawings	15	5 ☐ statement explaining lack of signature	
Sub-total number of sheets	56	6 ☐ priority document(s) identified in Box No VI as item(s)	
sequence listing		7 ☐ translation of international application into *(language)*	
tables related thereto		8 ☐ separate indications concerning deposited microorganism or other biological material	
(for both actual number of sheets if filed in paper form, whether or not also filed in computer readable form see (c) below)		9 ☐ sequence listing in computer readable form *(indicate type and number of carriers)*	
Total number of sheets	56	(i) ☐ copy submitted for the purposes of international search under Rule 13*ter* only (and not as part of the international application)	
(b) ☐ *only in computer readable form* (Section 801(a)(i))		(ii) ☐ *(only where check-box (b)(i) or (c)(i) is marked in left column)* additional copies including, where applicable, the copy for the purposes of international search under Rule 13*ter*	
(i) ☐ sequence listing		(iii) ☐ together with relevant statement as to the identity of the copy or copies with the sequence listing mentioned in left column	
(ii) ☐ tables related thereto		10 ☐ tables in computer readable form related to sequence listing *(indicate type and number of carriers)*	
(c) ☐ **also in computer readable form** (Section 801(a)(ii))		(i) ☐ copy submitted for the purposes of international search under Section 802(b-*quater*) only (and not as part of the international application)	
(i) ☐ sequence listing		(ii) ☐ *(only where check-box (b)(ii) or (c)(ii) is marked in left column)* additional copies including, where applicable, the copy for the purposes of international search under Section 802(b-*quater*)	
(ii) ☐ tables related thereto		(iii) ☐ together with relevant statement as to the identity of the copy or copies with the tables mentioned in left column	
Type and number of carriers (diskette, CD-ROM CD-R or other) on which are contained the		11 ☒ other *(specify)* Transmittal letter, post card	
☐ sequence listing			
☐ tables related thereto			
(additional copies to be indicated under items 9(ii) and/or 10(ii), in right column)			

Figure of the drawings which should accompany the abstract	3	**Language of filing of the international application**	ENGLISH

Box No. X SIGNATURE OF APPLICANT, AGENT OR COMMON REPRESENTATIVE

Next to each signature indicate the name of the person signing and the capacity in which the person signs (if such capacity is not obvious from reading the request)

DAVID B RITCHIE
REG NO 31,562

For receiving Office use only

1 Date of actual receipt of the purported international application		2 Drawings: ☐ received ☐ not received
3 Corrected date of actual receipt due to later but timely received papers or drawings completing the purported international application		
4 Date of timely receipt of the required corrections under PCT Article 11(2)		
5 International Searching Authority (if two or more are competent) ISA /	6. ☐ Transmittal of search copy delayed until search fee is paid	

For International Bureau use only

Date of receipt of the record copy by the International Bureau

147

PATENT COOPERATION TREATY

From the INTERNATIONAL SEARCHING AUTHORITY

To
DAVID B RITCHIE
THELEN REID & PRIEST LLP
PO BOX 640640
SAN JOSE, CA 95164-0640

PCT

NOTIFICATION OF TRANSMITTAL OF
THE INTERNATIONAL SEARCH REPORT
OR THE DECLARATION
(PCT Rule 44.1)

ISR 9-9-04

[redacted]	Date of Mailing (day/month/year)
	FOR FURTHER ACTION See paragraphs 1 and 4 below
International application No PCT/US04/04117	International filing date (day/month/year) 13 February 2004 (13.02.2004)
Applicant PSYCRYPT INC	

1 ☒ The applicant is hereby notified that the international search report has been established and is transmitted herewith.

Filing of amendments and statement under Article 19:
The applicant is entitled, if he so wishes, to amend the claims of the international application (see Rule 46).

When? The time limit for filing such amendments is normally two months from the date of transmittal of the international search report.

Where? Directly to the International Bureau of WIPO, 34, chemin des Colombettes, 1211 Geneva 20, Switzerland, Facsimile No. (41-22) 740 14 35.

For more detailed instructions, see the notes on the accompanying sheet.

2 ☐ The applicant is hereby notified that no international search report will be established and that the declaration under Article 17(2)(a) to that effect is transmitted herewith.

3 ☐ With regard to the protest against payment of (an) additional fee(s) under Rule 40.2, the applicant is notified that:

☐ the protest together with the decision thereon has been transmitted to the International Bureau together with the applicant's request to forward the texts of both the protest and the decision thereon to the designated Offices.

☐ no decision has been made yet on the protest; the applicant will be notified as soon as a decision is made.

4 Reminders

Shortly after 18 months from the priority date, the international application will be published by the International Bureau. If the applicant wishes to avoid or postpone publication, a notice of withdrawal of the international application, or of the priority claim, must reach the International Bureau as provided in Rules 90*bis*.1 and 90*bis*.3, respectively, before the completion of the technical preparations for international publication.

Within 19 months from the priority date, but only in respect of some designated Offices, a demand for international preliminary examination must be filed if the applicant wishes to postpone the entry into the national phase until 30 months from the priority date (in some Offices even later); otherwise, the applicant must, within 20 months from the priority date, perform the prescribed acts for entry into the national phase before those designated Offices.

In respect of other designated Offices, the time limit of 30 months (or later) will apply even if no demand is filed within 19 months.

See the Annex to Form PCT/IB/301 and for details about the applicable time limits, Office by Office, see the *PCT Applicant's Guide*, Volume II, National Chapters and the WIPO Internet site.

Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (703) 305-3230	Authorized officer for Michelle R. Eason Ayaz R. Sheikh Telephone No. 703 305-1373

Form PCT/ISA/220 (April 2002) (See notes on accompanying sheet)

Mail log_____ Date_____

CP1_____ Date_____

Exmr_____ Date_____

PATENT COOPERATION TREATY

From the INTERNATIONAL SEARCHING AUTHORITY

To
DAVID B RITCHIE
THELEN REID & PRIEST LLP
PO BOX 640640
SAN JOSE, CA 95164-0640

PCT

NOTIFICATION OF TRANSMITTAL OF THE INTERNATIONAL SEARCH REPORT OR THE DECLARATION

(PCT Rule 44.1)

	Date of Mailing (day/month/year) 09 SEP 2004
Applicant's or agent's file reference PYSC-0002/WO	FOR FURTHER ACTION See paragraphs 1 and 4 below
International application No PCT/US04/04117	International filing date (day/month/year) 13 February 2004 (13.02.2004)
Applicant PSYCRYPT, INC	

1 ☒ The applicant is hereby notified that the international search report has been established and is transmitted herewith.

Filing of amendments and statement under Article 19:
The applicant is entitled if he so wishes to amend the claims of the international application (see Rule 46).

When: The time limit for filing such amendments is normally two months from the date of transmittal of the international search report.

Where: Directly to the International Bureau of WIPO, 34 chemin des Colombettes, 1211 Geneva 20, Switzerland, Facsimile No. (41-22) 740 14 35.

For more detailed instructions, see the notes on the accompanying sheet.

2 ☐ The applicant is hereby notified that no international search report will be established and that the declaration under Article 17(2)(a) to that effect is transmitted herewith.

3 ☐ With regard to the protest against payment of (an) additional fee(s) under Rule 40.2, the applicant is notified that

☐ the protest together with the decision thereon has been transmitted to the International Bureau together with the applicant's request to forward the texts of both the protest and the decision thereon to the designated Offices.

☐ no decision has been made yet on the protest; the applicant will be notified as soon as a decision is made.

4 **Reminders**

Shortly after **18 months** from the priority date, the international application will be published by the International Bureau. If the applicant wishes to avoid or postpone publication, a notice of withdrawal of the international application, or of the priority claim, must reach the International Bureau as provided in Rules 90*bis*.1 and 90*bis*.3, respectively, before the completion of the technical preparations for international publication.

Within **19 months** from the priority date, but only in respect of some designated Offices, a demand for international preliminary examination must be filed if the applicant wishes to postpone the entry into the national phase until **30 months** from the priority date (in some Offices even later); otherwise, the applicant must, within **20 months** from the priority date, perform the prescribed acts for entry into the national phase before those designated Offices.

In respect of other designated Offices, the time limit of **30 months** (or later) will apply even if no demand is filed within 19 months.

See the Annex to Form PCT/IB/301 and, for details about the applicable time limits, Office by Office, see the *PCT Applicant's Guide*, Volume II, National Chapters and the WIPO Internet site.

Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (703)305-3230	Authorized officer Michelle R. Eason Anwar R. Sheikh Telephone No. 703-305-1373

Form PCT/ISA/220 (April 2002) *(See notes on accompanying sheet)*

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference PYSC-0002/WO	**FOR FURTHER ACTION**	see Notification of Transmittal of International Search Report (Form PCT/ISA/220) as well as, where applicable, item 5 below
International application No PCT/US04/04117	International filing date (*day/month/year*) 13 February 2004 (13 02 2004)	(Earliest) Priority Date (*day/month/year*)
Applicant PSYCRYPT INC		

This international search report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This international search report consists of a total of 4 sheets.

☒ It is also accompanied by a copy of each prior art document cited in this report.

1 **Basis of the Report**

a With regard to the **language**, the international search was carried out on the basis of the international application in the language in which it was filed, unless otherwise indicated under this item.

☐ the international search was carried out on the basis of a translation of the international application furnished to this Authority (Rule 23.1(b)).

b With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international search was carried out on the basis of the sequence listing:

☐ *contained in the international application in written form*

☐ filed together with the international application in computer readable form

☐ furnished subsequently to this Authority in written form

☐ furnished subsequently to this Authority in computer readable form

☐ the statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished

☐ the statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished

2 ☐ **Certain claims were *found unsearchable* (See Box I)**

3 ☐ **Unity of invention is lacking (See Box II)**

4 With regard to the title

☒ the text is approved as submitted by the applicant

☐ *the text has been established by this Authority to read as follows:*

5 With regard to the abstract

☐ the text is approved as submitted by the applicant

☒ the text has been established, according to Rule 38.2(b), by this Authority as it appears in Box III. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority.

6 The figure of the drawings to be published with the abstract is Figure No. 3

☒ as suggested by the applicant ☐ None of the figures

☐ because the applicant failed to suggest a figure

☐ because this figure better characterizes the invention

150

INTERNATIONAL SEARCH REPORT

International application No
PCT/US04/04117

A CLASSIFICATION OF SUBJECT MATTER
IPC(7) H04L 9/00
US CL 713/200
According to International Patent Classification (IPC) or to both national classification and IPC

B FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U S 713/200, 164, 165, 201, 380/37, 28

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
Please See Continuation Sheet

C DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document with indication, where appropriate, of the relevant passages	Relevant to claim No
X ... Y	US 6,269,164 B1 (PIRES) 31 July 2001 (31 07 2001), column 6 line 62 to column 7 line 24, column 7 line 47 to column 8 line 25 column 9 line 49 to column 10 line 25, column 12 lines 40-61, column 15, lines 30-55, column 18, lines 32-67	1-7, 13-30, 36-39, 75-97 --- 8-12, 31-35
X ... Y	US 5,008 935 A (ROBERTS) 16 April 1991 (16 04 1991), column 2, lines 15-45, column 3, lines 1-64	40-49, 55-66, 72-74 --- 50-54, 67-71
Y	US 6,160 797 A (ROBERT III et al) 12 December 2000 (12 12 2000), column 8 line 57 to column 9 line 60	8-12, 31-35, 50-54 67-71
A	Makki et al, The SECURE Model for Enterprise Connectivity IEEE, 2000 pages 176-182	1-97
A	Wu et al, Communication-Friendly Encryption of Multimedia IEEE, 2002, pages 292-295	1-97
A	Chueng et al, Implementation of Pipelined Data Encryption Standard (DES) Using Altera CPLD IEEE, 2000, pages III-17 to III-21	1-97
A	Steward, Shawn Practicing safe data Cellular Business January 1997, pages 64 and 66	1-97

☒ Further documents are listed in the continuation of Box C ☐ See patent family annex

* Special categories of cited documents
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure use exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
18 August 2004 (18 08 2004)	09 SEP 2004
Name and mailing address of the ISA/US Mail Stop PCT Attn ISA/US Commissioner for Patents P O Box 1450 Alexandria Virginia 22313 1450 Facsimile No (703)305-3230	Authorized officer for Michelle L. Siegel Ayaz R Sheikh Telephone No 703-305 1373

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

International application No

PCT/US04/04117

Box III TEXT OF THE ABSTRACT (Continuation of Item 5 of the first sheet)

The technical features mentioned in the abstract do not include a reference sign between parentheses (PCT Rule 8.1(d))

A method and apparatus cryptographically process data including a plurality of data segments. The cryptographic process includes (a) receiving a plurality of data segments (100), (b) selecting, for each data segment, a set of encryption information based on data contained in a predetermined portion of the data segment to be encrypted (102, 104), and (c) encrypting each data segment using the set of encryption information selected for the data segment (106). At least one of an encryption algorithm, an encryption key, and an encryption parameter may be changed for each data segment based on the data contained in the predetermined portion. The predetermined portion may include a first predetermined portion for selecting a first set of encryption information, and a second predetermined portion for selecting a second set of encryption information, the encryption information including an encryption algorithm, an encryption key, and optionally an encryption parameter.

INTERNATIONAL SEARCH REPORT

PCT/US04/04117

Continuation of B. FIELDS SEARCHED Item 3:
EAST, Palm, Proquest, IEEE, Google
search terms data segements data fragments data packets, packets, frame, encryption, algorithm, encryption algorithm hash key, encryption key, DES, IP, TCP, UDP, decryption buffer

153

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To
DAVID B RITCHIE
THELEN REID & PRIEST LLP
PO BOX 640640
SAN JOSE, CA 95164-0640

PCT

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43*bis* 1)

Applicant's or agent's file reference PYSC-0002/WO	Date of mailing (*day/month/year*) 09 SEP 2004 FOR FURTHER ACTION See paragraph 2 below

International application No	International filing date (*day/month/year*)	Priority date (*day/month/year*)
PCT/US04/04117	13 February 2004 (13 02 2004)	

International Patent Classification (IPC) or both national classification and IPC
IPC(7) H04L 9/00 and US Cl 713/200

Applicant
PSYCRYPT, INC

1 This opinion contains indications relating to the following items

- ☒ Box No I Basis of the opinion
- ☐ Box No II Priority
- ☐ Box No III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- ☐ Box No IV Lack of unity of invention
- ☒ Box No V Reasoned statement under Rule 43*bis* 1(a)(i) with regard to novelty, inventive step or industrial applicability, citations and explanations supporting such statement
- ☐ Box No VI Certain documents cited
- ☐ Box No VII Certain defects in the international application
- ☐ Box No VIII Certain observations on the international application

2 **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA", except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66 1*bis* (*b*) that written opinions of this International Searching Authority will not be so considered

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together where appropriate with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date whichever expires later

For further options see Form PCT/ISA/220

3 For further details, see notes to Form PCT/ISA 220

Name and mailing address of the ISA/ US Mail Stop PCT Attn ISA/US Commissioner for Patents P O Box 1450 Alexandria Virginia 22313 1450 Facsimile No (703)305-3230	Authorized officer for Ayaz R Sheikh Michelle R. Eason Telephone No 703-305-1373

Form PCT/ISA/237 (cover sheet) (January 2004)

154

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No
PCT/US04/04117

Box No. I Basis of this opinion

1 With regard to the language, this opinion has been established on the basis of the international application in the language in which it was filed, unless otherwise indicated under this item

☐ This opinion has been established on the basis of a translation from the original language into the following language _____, which is the language of a translation furnished for the purposes of international search (under Rules 12.3 and 23.1(b))

2 With regard to any nucleotide and/or amino acid sequence disclosed in the international application and necessary to the claimed invention this opinion has been established on the basis of

a type of material

☐ a sequence listing

☐ table(s) related to the sequence listing

b format of material

☐ in written format

☐ in computer readable form

c time of filing/furnishing

☐ contained in international application as filed

☐ filed together with the international application in computer readable form

☐ furnished subsequently to this Authority for the purposes of search

3 ☐ In addition in the case that more than one version or copy of a sequence listing and/or table relating thereto has been filed or furnished the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed as appropriate, were furnished

4 Additional comments

155

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No
PCT/US04/04117

Box No. V Reasoned statement under Rule 43 *bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1 Statement

Novelty (N)	Claims	NONE	YES
	Claims	1-7, 13-31, 36-48, 55-66, 72-97	NO
Inventive step (IS)	Claims	NONE	YES
	Claims	1-97	NO
Industrial applicability (IA)	Claims	1-97	YES
	Claims	NONE	NO

2 Citations and explanations

Please See Continuation Sheet

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No
PCT/US04/04117

Supplemental Box
In case the space in any of the preceding boxes is not sufficient

V. 2 Citations and Explanations.

Claims 1-7, 13-30, 36-49, 55-66 and 72-97, lack novelty under PCT Article 33(2) as being anticipated by Pires As to claims 1 25, 75 and 91, Pires discloses receiving a plurality of data segments Pires discloses selecting, for each data segment a set of encryption information based on data contained in a predetermined portion of the data segment to be encrypted Pires discloses encrypting each data segment using the set of encryption information selected for the data segment Pires discloses decrypting each encrypted data segment using the encryption information selected for the encrypted data segment

Claims 40-49, 55-66 and 72-74 lack novelty under PCT Article 33(2) as being anticipated by Roberts Roberts discloses an input buffer adapted to receive data including a plurality of data segments Roberts discloses an encryption module adapted to encrypt each data segment Roberts discloses a controller coupled to the input buffer and the encryption module Roberts discloses that the controller is adapted to select a set of encryption information for each data segment based on data contained in a predetermined portion of the data segment to be encrypted Roberts discloses an output buffer coupled to the controller and the encryption module Roberts discloses the output buffer being adapted to output encrypted data including a plurality of encrypted data segments

Claims 8-12 and 31-35 lack an inventive step under PCT Article 33(3) as being obvious over Pires in view of Robert As to claims 8-12 and 31-35 Pires does not teach that the first predetermined portion contains data for a first protocol layer, and the second predetermined portion contains data for a second protocol data Pires does not each that the first protocol layer is lower than the second protocol layer Pires does not teach that the first predetermined portion is an Internet Protocol (IP) header of the data packet Pires does not teach that the second predetermined portion is a selected portion of a data field of the data packet Pires does not teach that the second portion is a Transmission Control Protocol (TCP) header of the data packet Pires does not teach that the second predetermined portion is a User Datagram Protocol (UDP) header of the data packet Robert teaches that the first predetermined portion contains data for a first protocol layer and the second predetermined portion contains data for a second protocol data Robert teaches that the first protocol layer is lower than the second protocol layer Robert teaches that the first predetermined portion is an Internet Protocol (IP) header of the data packet Robert teaches that the second predetermined portion is a selected portion of a data field of the data packet Robert teaches that the second portion is a Transmission Control Protocol (TCP) header of the data packet Robert teaches that the second predetermined portion is a User Datagram Protocol (UDP) header of the data packet

Claims 8-12, 31-35 50-54 and 67-71 lack an inventive step under PCT Article 33(3) as being obvious over Roberts in view of Robert As to claims 8 12 and 31-35, Roberts does not teach that the first predetermined portion contains data for a first protocol layer and the second predetermined portion contains data for a second protocol data Roberts does not each that the first protocol layer is lower than the second protocol layer Roberts does not teach that the first predetermined portion is an Internet Protocol (IP) header of the data packet Roberts does not teach that the second predetermined portion is a selected portion of a data field of the data packet Roberts does not teach that the second portion is a Transmission Control Protocol (TCP) header of the data packet Roberts does not teach that the second predetermined portion is a User Datagram Protocol (UDP) header of the data packet Robert teaches that the first predetermined portion contains data for a first protocol layer and the second predetermined portion contains data for a second protocol data Robert teaches that the first protocol layer is lower than the second protocol layer Robert teaches that the first predetermined portion is an Internet Protocol (IP) header of the data packet Robert teaches that the second predetermined portion is a

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No
PCT/US04/04117

Supplemental Box
In case the space in any of the preceding boxes is not sufficient

selected portion of a data field of the data packet Robert teaches that the second portion is a Transmission Control Protocol (TCP) header of the data packet Robert teaches that the second predetermined portion is a User Datagram Protocol (UDP) header of the data packet

Claims 1-97 meet the criteria set out in PCT Article 33(4), and thus have industrial applicability because a method and apparatus cryptographically process data including a plurality of data segments can be made or used in industry

NOTES TO FORM PCT/ISA/220

These Notes are intended to give the basic instructions concerning the filing of amendments under Article 19. The Notes are based on the requirements of the Patent Cooperation Treaty, the Regulations and the Administrative Instructions under that Treaty. In case of discrepancy between these Notes and those requirements, the latter are applicable. For more detailed information, see also the *PCT Applicant's Guide*, a publication of WIPO.

In these Notes, "Article," "Rule" and "Section" refer to the provisions of the PCT, the PCT Regulations and the PCT Administrative Instructions, respectively.

INSTRUCTIONS CONCERNING AMENDMENTS UNDER ARTICLE 19

The applicant has, after having received the international search report, one opportunity to amend the claims of the international application. It should however be emphasized that, since all parts of the international application (claims, description and drawings) may be amended during the international preliminary examination procedure, there is usually no need to file amendments of the claims under Article 19 except where, e.g. the applicant wants the latter to be published for the purposes of provisional protection or has another reason for amending the claims before international publication. Furthermore, it should be emphasized that provisional protection is available in some States only.

What parts of the international application may be amended?

Under Article 19, only the claims may be amended.

During the international phase, the claims may also be amended (or further amended) under Article 34 before the International Preliminary Examining Authority. The description and drawings may only be amended under Article 34 before the International Preliminary Examining Authority.

Upon entry into the national phase, all parts of the international application may be amended under Article 28 or, where applicable, Article 41.

When? Within 2 months from the date of transmittal of the international search report or 16 months from the priority date, whichever time limit expires later. It should be noted, however, that the amendments will be considered as having been received on time if they are received by the International Bureau after the expiration of the applicable time limit but before the completion of the technical preparations for international publication (Rule 46.1).

Where not to file the amendments?

The amendments may only be filed with the International Bureau and not with the receiving Office or the International Searching Authority (Rule 46.2).

Where a demand for international preliminary examination has been/is filed, see below.

How? Either by cancelling one or more entire claims, by adding one or more new claims or by amending the text of one or more of the claims as filed.

A replacement sheet must be submitted for each sheet of the claims which, on account of an amendment or amendments, differs from the sheet originally filed.

All the claims appearing on a replacement sheet must be numbered in Arabic numerals. Where a claim is cancelled, no renumbering of the other claims is required. In all cases where claims are renumbered, they must be renumbered consecutively (Administrative Instructions, Section 205(b)).

The amendments must be made in the language in which the international application is to be published.

What documents must/may accompany the amendments?

Letter (Section 205(b)):

The amendments must be submitted with a letter.

The letter will not be published with the international application and the amended claims. It should not be confused with the "Statement under Article 19(1)" (see below, under "Statement under Article 19(1)").

The letter must be in English or French, at the choice of the applicant. However, if the language of the international application is English, the letter must be in English; if the language of the international application is French, the letter must be in French.

NOTES TO FORM PCT/ISA/220 (continued)

The letter must indicate the differences between the claims as filed and the claims as amended. It must, in particular, indicate, in connection with each claim appearing in the international application (it being understood that identical indications concerning several claims may be grouped), whether

(i) the claim is unchanged,

(ii) the claim is cancelled,

(iii) the claim is new,

(iv) the claim replaces one or more claims as filed,

(v) the claim is the result of the division of a claim as filed

The following examples illustrate the manner in which amendments must be explained in the accompanying letter:

1 [Where originally there were 48 claims and after amendment of some claims there are 51]
"Claims 1 to 29, 31, 32, 34, 35, 37 to 48 replaced by amended claims bearing the same numbers, claims 30, 33 and 36 unchanged, new claims 49 to 51 added"

2 [Where originally there were 15 claims and after amendment of all claims there are 11]
"Claims 1 to 15 replaced by amended claims 1 to 11"

3 [Where originally there were 14 claims and the amendments consist in cancelling some claims and in adding new claims]
"Claims 1 to 6 and 14 unchanged, claims 7 to 13 cancelled, new claims 15, 16 and 17 added" or
"Claims 7 to 13 cancelled, new claims 15, 16 and 17 added, all other claims unchanged"

4 [Where various kinds of amendments are made].
"Claims 1-10 unchanged, claims 11 to 13, 18 and 19 cancelled, claims 14, 15 and 16 replaced by amended claim 14, claim 17 subdivided into amended claims 15, 16 and 17; new claims 20 and 21 added"

"Statement under Article 19(1)" (Rule 46.4)

The amendments may be accompanied by a statement explaining the amendments and indicating any impact that such amendments might have on the description and the drawings (which cannot be amended under Article 19(1))

The statement will be published with the international application and the amended claims

It must be in the language in which the international application is to be published.

It must be brief, not exceeding 500 words if in English or if translated into English

It should not be confused with and does not replace the letter indicating the differences between the claims as filed and as amended. It must be filed on a separate sheet and must be identified as such by a heading, preferably by using the words "Statement under Article 19(1)."

It may not contain any disparaging comments on the international search report or the relevance of citations contained in that report. Reference to citations, relevant to a given claim, contained in the international search report may be made only in connection with an amendment of that claim

Consequence if a demand for international preliminary examination has already been filed

If, at the time of filing any amendments and any accompanying statement, under Article 19, a demand for international preliminary examination has already been submitted, the applicant must preferably, at the time of filing the amendments (and any statement) with the International Bureau, also file with the International Preliminary Examining Authority a copy of such amendments (and of any statement) and, where required, a translation of such amendments for the procedure before that Authority (see Rules 55.3(a) and 62.2, first sentence). For further information, see the Notes to the demand form (PCT/IPEA/401)

Consequence with regard to translation of the international application for entry into the national phase

The applicant's attention is drawn to the fact that, upon entry into the national phase, a translation of the claims as amended under Article 19 may have to be furnished to the designated/elected Offices, instead of, or in addition to, the translation of the claims as filed

For further details on the requirements of each designated/elected Office, see the *PCT Applicant's Guide*, Volume II

160

Comercio

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO
Rad: 06-079165- -00000-0000
Fec 2006-08-11 12:57:21 Dep 2020 NUECREACIONES
Tra 11 PATENTEIYII
Fre 379 FASENACIONALII

REQUISITOS MINIMOS PARA ADMISION
PCT

PATENTE DE INVENCION [ ] MODELO DE UTILIDAD [ ]

- Indicación de que se solicita la concesión de una patente [X]
- Datos de identificación del solicitante o de la persona que presenta la solicitud [X]
- Descripción de la invención [X]
- Dibujos de ser estos pertinentes [X]
- Comprobante de pago de las tasas establecidas [X]

COMPLETA [ ] INCOMPLETA [ ]

DISEÑO INDUSTRIAL [ ]

- Indicación de que se solicita el registro de Diseño Industrial [ ]
- Datos de identificación del solicitante o de la persona que presenta la solicitud [ ]
- Representación gráfica y fotográfica del Diseño Industrial o muestra del material que incorpora el diseño [ ]
- Comprobante de pago de las tasas establecidas [ ]

COMPLETA [ ] INCOMPLETA [ ]

ESQUEMA DE TRAZADO [ ]

- Indicación de que se solicita el registro de un Esquema de Trazado [ ]
- Datos de identificación del solicitante o de la persona que presenta la solicitud [ ]
- Representación gráfica del esquema trazado [ ]
- Comprobante de pago de las tasas establecidas [ ]

COMPLETA [ ] INCOMPLETA [ ]

Fdo B

Firma Responsable

Fecha 11-AG-1

Carrera 13 No 27-00 Piso 5, 7 y 10
Conmutador. 3 82 08 40
Fax 350 52 20
E-mail info@sic.gov.co
www.sic.gov.co
Bogotá, D.C., Colombia

REPUBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Bogotá,
2020

Doctor(a)
MAYA RODRIGUEZ CARLOS ORLANDO

REFERENCIA	Radicación No.	6 79165
	Solicitud internacional	US2004/004117
	Fecha inicio fase nacional	13/09/2006
	Trámite	11
	Evento	379
	Actuación	430
	Oficio No.	11219

Como resultado del examen de forma, realizado con fundamento en el artículo 38 de la Decisión 486 de la Comisión de la Comunidad Andina, artículo 27 del Tratado de Cooperación en Materia de Patentes (PCT), regla 51 bis del Reglamento y Circular Única de la Superintendencia de Industria y Comercio, se le comunica que:

1. Si fuere el caso, el solicitante debe adjuntar la traducción de los anexos del reporte de examen preliminar internacional (Art. 36.2.b) del tratado PCT.

2. La solicitud no contiene la copia del documento en que consta la cesión del derecho a la patente del inventor al solicitante o a su causante. (Art. 26-k) Decisión 486.

3. La solicitud no contiene el poder debidamente otorgado, con el lleno de los requisitos exigidos por los artículos 63 y subsiguientes del Código de Procedimiento Civil. Adicionalmente, deberá presentar el documento que acredita la existencia y representación legal de la sociedad solicitante, cuando ésta fuere persona jurídica.

En cumplimiento de lo dispuesto por el artículo 39 de la Decisión 486, se le requiere para que dentro del término de dos meses siguientes a la fecha de notificación del presente oficio, complete los requisitos anteriormente enunciados. En caso de no dar cumplimiento al presente requerimiento, la solicitud se considerará abandonada y perderá su prelación.

Notifíquese el presente oficio conforme a lo dispuesto en el numeral 5.2, literal e), del capítulo quinto del título primero de la Circular Unica No.10 de 2001.

ALIX CARMENZA CESPEDES DE VERGEL
Jefe de la división de Nuevas Creaciones

El anterior requerimiento fue notificado por fijación en lista de fecha 06 OCT. 2006
adpa11