Industria y Comercio
SUPERINTENDENCIA

00 66033

SUPERINTENDENCIA Y COMERCIO
Radicacion : 00066033 00386386C
Fecha (AMD): 2000-08-30 16:52:12
Tramite : 002 PATENTES : 1 REGISTRO: 411 PRESENTAC
Dependencia: 0020 DIVISION DE NUEVAS CREACIONES
Folios: 31

TRAMITE: 02 EVENTO:01 ACTUACION: 411

DATOS DEL SOLICITANTE

(71) Nombres y Apellidos o Razón Social: **NagraCard S.A.**

No. de Identificación:

Representante Legal (Persona Jurídica):

País de Domicilio: **Suiza**

Departamento o Estado:

Dirección: **22, route de Genéve**

Ciudad: **1033 Cheseaux-sur-Lausanne**

(74) DATOS DEL APODERADO

Nombre: **EMILIO FERRERO**

Dirección y Domicilio: **Carrera 4 no. 72-35 piso 4o.,**

Ciudad: **BOGOTA COLOMBIA**

DATOS DEL INVENTOR

(72) Nombre del Inventor (es): **1- Marco SASSELLI 2- Christophe NICOLAS**
3- Michael John HILL

Identificación:

Dirección: **1-.Ch. des Roches, 1803 Chardonnes, Suiza**
2- Rue de Lausanne 29, 1028 Préverenges, Suiza
3- Route de Commugny 10, CH 1296 Coppet, Suiza.

Ciudad:

DATOS DE LA PATENTE DE INVENCION

(54) Título de la Invención: **MÉTODO DE ENCRIPTACION MULTI-MÓDULOS**

PRIORIDAD REIVINDICADA SI [X] NO [ ] TIPO DE PRIORIDAD ANDINA [ ] UNIONISTA [X]

(33) País	Fecha	No. Solicitud
CH.	30 de agosto de 1999	CH-1573/99

Convención de París.

Para Publicar a los [ ] 6 meses [ ] 12 meses [X] 18 meses a partir de la fecha de la presente solicitud

Colo: 12324-801-001-9
JJC/mrm-1

(51) CLASIFICACION INTERNACIONAL H04B 001/000 30 AGO. 2000

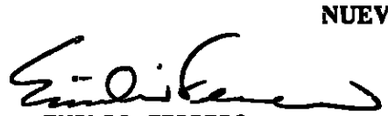
RESUMEN CON EL OBJETO Y LA FINALIDAD DE LA INVENCION

La presente invención se refiere a métodos para determinar la o las claves utilizadas por el módulo que analiza los datos que entran o salen de él en el momento de la utilización del módulo de encriptación-desencriptación Para paliar este defecto, el método multi-módulos propuesto consiste en que el módulo corriente abajo comience sus operaciones para encriptar-desencriptar cuando esté disponible una parte de los resultados del módulo corriente amba.

ANEXOS DE LA SOLICITUD

Certificado de Existencia y Representación Legal cuando el solicitante sea Persona Jurídica	☐
Los poderes debidamente otorgados, o mención de su protocolización ante la SIC	☐
Recibo de la tasa respectiva por v/r de $ 608 000 oo	☒
Recibo de la tasa por concepto de excedente de palabras en la publicación	☐
Si se reivindica prioridad Andina	
Copia de la primera solicitud	☐
Traducción oficial	☐
Si se reivindica prioridad Unionista	
Copia certificada de la primera solicitud Suiza No CH-1573/99	☒
Nota Debe presentarse dentro de los tres (3) meses, contados a partir de la fecha de radicación de la solicitud posterior	
Traducción simple	☒
Capítulo descriptivo	☒
Dibujos, planos necesarios (2 pág)	☒
Capítulo reivindicatorio	☒
Tarjeta archivo propietarios según formato	☒
Tarjeta archivo temático según formato	☒
Extracto para publicación según formato	☒
Arte final 12 x 12 cms Y 6x6 cms	☒
Otros Documentos	☐

SOLICITO LA CONCESION DE LA PATENTE DE INVENCION Y DECLARO QUE LA INVENCION ES NUEVA Y DE MI PROPIEDAD

FIRMA 

NOMBRE EMILIO FERRERO **CC** 438.019 de Usaquén **T.P No.** 31.929

WCR

MÉTODO DE ENCRIPTACIÓN MULTI-MÓDULOS

La presente invención se refiere al dominio del cifrado, o encriptación, y del descifrado o desencriptación de datos, y particularmente de datos que sean inaccesibles para personas o aparatos no autorizados en el marco de sistemas de televisión de pago. En estos sistemas los datos son cifrados en un entorno seguro protegiendo las posibilidades de cálculo importantes y denominado subsistema de codificación. A continuación los datos son enviados a través de los medios conocidos a, por lo menos, un subsistema descentralizado donde son descifrados generalmente mediante un IRD (Integrated Receiver Decoder) y una tarjeta inteligente. Una persona no autorizada podría tener libre acceso tanto a esta tarjeta inteligente como al subsistema descentralizado que coopera con ésta.

Se conoce el hecho de encadenar diversos medios de encriptación-desencriptación en un sistema de cifrado-descifrado. De ahora en adelante denominaremos encriptación-desencriptación a un medio de criptografía particular utilizado en un sistema más amplio de cifrado-descifrado.

Desde hace mucho se pretende optimizar el funcionamiento de estos sistemas desde tres puntos de vista: la rapidez, el espacio ocupado en la memoria y la seguridad. Por rapidez se entiende el tiempo necesario para descifrar los datos recibidos.

Se conocen sistemas de encriptación-desencriptación con claves simétricas. Su seguridad inherente puede ser calificada en función de varios criterios.

El primer criterio es el de la seguridad física, relativa a la facilidad o a la dificultad que supone un método de investigación para la extracción de ciertos componentes después de su eventual reemplazo por otros componentes. Estos componentes de reemplazo, , destinados a informar a la persona no autorizada de la naturaleza y del funcionamiento del sistema de cifrado-descifrado, son elegidos por ésta de manera que no sean detectados, o lo sea lo menos posible, por el resto del sistema.

Un segundo criterio se refiere a la seguridad del sistema, en la que los ataques no son intrusivos desde el punto de vista físico sino que recurren al análisis de tipo matemático. Normalmente estos ataques los llevan a cabo ordenadores de gran potencia que intentan romper los algoritmos y los códigos de cifrado

Medios para encriptar-desencriptar con claves simétricas son, por ejemplo, los sistemas denominados DES (Data Encryption Standard) Estos medios, relativamente antiguos, sólo ofrecen una seguridad del sistema y una seguridad física, ambas relativas Debido particularmente a esta razón, los DES, que a menudo poseen claves de una longitud demasiado pequeña para satisfacer las condiciones de seguridad del sistema, son reemplazados cada vez más por nuevos medios de encriptación-desencriptación o por claves más largas De manera general, estos medios de claves simétricas se sirven de los algoritmos que comprenden las series de cifrado

Otras estrategias de ataque se denominan Simple Power Analysis, y Timing Analysis En el Simple Power Analysis, se hace uso de un microprocesador encargado de encriptar o desencriptar los datos el cual está conectado a una fuente de tensión (en general de 5 Voltios) Cuando está en modo reposo lo recorre una corriente fija de intensidad i Cuando está en modo activo, la intensidad instantánea i es función, no sólo de los datos entrantes, sino también del algoritmo de encriptación En el Simple Power Analysis se mide la corriente i en función del tiempo Así, se puede deducir el tipo de algoritmo que el microprocesador efectúa

Del mismo modo, el método del Timing Analysis consiste en medir la duración del cálculo en función de una muestra presentada al módulo de desencriptación Así, la relación entre la muestra presentada y el tiempo de cálculo del resultado permite encontrar los parámetros secretos del módulo de desencriptación tales como la clave. Este sistema se describe, por ejemplo, en el documento "Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems"

publicado por Paul Kocher, Cryptography Research, 870 Market St, Suite 1088, San Francisco, CA-USA

Para mejorar la seguridad del sistema de cifrado, se han propuesto algoritmos en clave asimétricos tales como los sistemas denominados RSA (Rivest, Shamir y Adleman) Estos sistemas comprenden la generación de un par de claves emparejadas, una pública que se usa para el cifrado y otra privada que se usa para el descifrado Estos algoritmos presentan un alto nivel de seguridad tanto sistemática como física Sin embargo son más lentos que los sistemas tradicionales, sobretodo en la fase del cifrado

Las técnicas de ataque mas recientes recurren a la noción denominada DPA del inglés Differential Power Analysis Estos métodos se basan en cómputos que se pueden verificar al final de un gran numero de pruebas con la presencia de un 0 o de un 1 en una posición determinada de la clave de cifrado Son casi imposibles de destruir, lo que les confiere la característica de no poder ser detectados, y emplean al mismo tiempo la intrusión física y el análisis matemático Su funcionamiento recuerda a las técnicas de investigación de los campos petrolíferos, donde se genera una explosión potente en la superficie Los técnicos se sitúan a distancias determinadas del lugar de la explosión y con la ayuda de sondas y gracias a la reflexión de las ondas de choque en los límites de los asientos sedimentarios del subsuelo, son capaces de establecer hipótesis acerca de la composición estratigráfica del subsuelo Los ataques DPA se describen particularmente en el § 2 1 del documento "A Cautionary Note Regarding Evaluation of AES Candidates on Smart-Cards", publicado el día 1 de febrero 1999 por Suresh Chari, Charanjit Jutla, Josyula R Rao et Pankaj Rohatgi, del IBM T J Watson Research Center, Yorktown Heights, NY

La obligación de resistir a los ataques DPA obliga a utilizar los sistemas de interferencia denominados "whitening", sea en el momento de la entrada de las informaciones, sea a la salida de un algoritmo de cifrado-descifrado La técnica del whitening se describe en el § 3 5 del documento antes señalado

Además, el hecho de que las capacidades de cálculo se vean limitadas en el subsistema descentralizado de un sistema de televisión de pago crea un problema todavía no resuelto a la hora de efectuar en medida suficiente el encadenado descrito anteriormente

El objetivo de la presente invención consiste en disponer de un método de encriptación-desencriptación que resista a los métodos modernos de investigación tales como los descritos más arriba

El objetivo perseguido en la presente invención se alcanza mediante el método descrito en la parte caracterizadora de la reivindicación 1

La particularidad del método reside en el hecho de que un módulo intermediario no se activará hasta que el resultado del módulo precedente (o corriente arriba) haya terminado, sino que se activará cuando una parte de las informaciones ya estén disponibles Así, a un observador exterior no le resulta posible establecer las condiciones de entrada o de salida de este módulo

Como el proceso de descifrado interviene en el subsistema descentralizado junto con la tarjeta inteligente, esta tarjeta inteligente sólo protege las capacidades de cálculo relativamente limitadas respecto al subsistema de codificación Por ejemplo, resulta interesante utilizar en las últimas etapas del descifrado una clave asimétrica pública con un funcionamiento relativamente rápido Esto permite, por una parte, preservar las características de invulnerabilidad del sistema a la salida del proceso y, por otra parte, concentrar la capacidad de cálculo, ligada esencialmente al cifrado con ayuda de la clave privada en el subsistema de codificación

Se ha descubierto que se proporciona una seguridad complementaria con la posibilidad de concatenar, o de entrelazar parcialmente dos medios de encriptación-desencriptación que se sigan secuencialmente Se entiende por esta concatenación o entrelazamiento parcial, término que resulta de una traducción

del inglés "interleaving", aquel proceso consistente en activar la acción del segundo medio de encriptación-desencriptación de datos cuando el primer medio de encriptación-desencriptación todavía no ha terminado su trabajo con estos datos Esto permite enmascarar los datos que resultan del trabajo del primer módulo y hacerlo antes de que sean sometidos a la acción del segundo módulo.

El encadenado se puede activar desde el momento en que los datos calculados que salen del primer módulo estén parcialmente disponibles para que los trate el segundo módulo.

La invención permite prevenir los ataques antes citados combinando diversos medios de encriptación-desencriptación en un sistema de cifrado-descifrado y asociando eventualmente una concatenación o entrelazamiento parcial a la secuencia en la que se siguen estos medios

En una forma particular de realización de la invención, el sistema de cifrado-descifrado comprende un subsistema de codificación donde se utilizan secuencialmente tres algoritmos

a) un algoritmo A1 asimétrico con clave privada d1 Este algoritmo A1 crea una contraseña para los datos sin cifrar, representados por un mensaje m Esta operación proporciona un primer criptograma c1 mediante operaciones matemáticas generalmente expresadas en la profesión mediante la fórmula c1 = m exponente d1, módulo n1 En esta fórmula, n1 forma parte de la clave pública del algoritmo asimétrico A1, módulo que representa el operador matemático conocido de las congruencias en el conjunto de los enteros relativos, y donde d1 es la clave privada del algoritmo A

b) un algoritmo S simétrico que utiliza una clave secreta K Este algoritmo convierte el criptograma c1 en un criptograma c2

c) un algoritmo A2 asimétrico con clave privada d2 Este algoritmo A2 convierte el criptograma c2 en un criptograma c3 mediante la operación

matemática expresada anteriormente por la fórmula c3 = c2 exponente d2 módulo n2, en donde n2 forma parte de la clave pública del algoritmo asimétrico A2, y d2 es la clave privada del algoritmo A2

El criptograma c3 parte del subsistema de codificación y alcanza el subsistema descentralizado a través de medios conocidos En el caso de sistemas de televisión de pago, también se puede tratar de datos vídeo o de mensajes

El subsistema descentralizado utiliza, en orden inverso a lo anteriormente expuesto, tres algoritmos A1', S' y A2' Estos tres algoritmos forman parte de tres medios para encriptar y desencriptar A1-A1', S-S' y A2-A2', repartidos entre el subsistema de codificación y el subsistema descentralizado, y representando el sistema de cifrado-descifrado

d) el algoritmo A2' efectúa en c3 una operación matemática restituyendo c2 y expresada c2 = c3 exponente e2 módulo n2 En esta fórmula, el conjunto formado por e2 y n2 constituye la clave pública del algoritmo asimétrico A2-A2'

e) el algoritmo simétrico S' simétrica que utiliza la clave secreta K restituye el criptograma c1

f) el algoritmo A1' asimétrico con clave pública e1, n1 vuelve a m al efectuar la operación matemática expresada m = c1 exponente e1 módulo n1

La concatenación en el subsistema descentralizado consiste en activar la etapa de descifrado e) mientras que c2 todavía no se ha restituido completamente en la etapa anterior d), y a comenzar la etapa de descodificación f) mientras que c1 todavía no se ha restituido completamente en la etapa e La ventaja consiste en hacer fracasar un ataque que, por ejemplo, pretendiera principalmente extraer el criptograma c1 del subsistema descentralizado al final de la etapa e para compararlo con los datos no cifrados m para luego, conociendo c1 y m, atacar el algoritmo A1' tras remontar la cadena de codificación progresivamente

8

La concatenación no es necesaria en el subsistema de codificación, el cual se instala en un lugar físico seguro Sin embargo es útil en el subsistema descentralizado En el caso de la televisión de pago el IRD se instala en casa del abonado y puede ser objeto de los ataques antes descritos.

Se considera que un ataque de una combinación de tres algoritmos para desencriptar A1', S' y A2' concatenados tiene menos posibilidades de éxito que si los criptogramas c1 y c2 se reconstituyen íntegramente entre cada etapa d), e) y f) Por otro lado, el hecho de que los algoritmos A1' y A2' se utilicen con las claves públicas e1, n1 y e2, n2 hace que los medios de cálculo necesarios en el subsistema descentralizado se vean mucho más reducidos que en el subsistema de codificación

A título de ejemplo y para fijar ideas, las etapas a) y c), es decir, las etapas para encriptar con claves privadas, son 20 veces más largas que las etapas d) y f) para desencriptar con claves públicas

En una forma particular de realización de la invención derivada de la precedente, los algoritmos A1 y A2 son idénticos al igual que sus opuestos A1' y A2'

En una forma particular de realización de la invención, igualmente derivada de la precedente, se utiliza la clave pública e2 en la etapa c), n2 del algoritmo asimétrico A2 mientras que en la etapa d) se desencripta el criptograma c3 con la clave privada d2 de este algoritmo Esta forma constituye una posible alternativa cuando los recursos del subsistema descentralizado susceptibles de cálculo distan de ser alcanzados

Si bien es cierto que las tarjetas inteligentes se utilizan mayoritariamente para desencriptar los datos, también existen tarjetas inteligentes con capacidad necesaria para efectuar operaciones de encriptación En tal caso, los ataques descritos anteriormente se dirigirán igualmente a estas tarjetas de encriptación que funcionan fuera de lugares protegidos tales como un centro de gestión Por este motivo el método según la invención se aplica igualmente a las operaciones

de encriptación en serie, es decir, que el módulo corriente abajo comienza su operación de encriptación sólo cuando una parte de las informaciones proporcionadas por el módulo corriente arriba están disponibles. Este proceso cuenta con la ventaja de entrelazar los diferentes módulos de encriptación y, como consecuencia, el resultado del módulo corriente arriba no está disponible completamente en un momento dado Además, el módulo corriente abajo no comienza sus operaciones con un resultado completo sino que lo hace por partes, lo que no permite interpretar el funcionamiento de un módulo con relación a un estado de entrada o de salida conocido

La presente invención se comprenderá más detalladamente gracias a los dibujos siguientes y que no pretenden ser limitativos, en los cuales

- la figura 1 representa las operaciones de encriptación

- la figura 2 representa las operaciones de desencriptación

- la figura 3 representa una alternativa al método de encriptación

En la figura 1, un conjunto de datos m es introducido en la cadena de encriptación Un primer elemento A1 efectúa una operación de encriptación utilizando la clave denominada privada compuesta por el exponente d1 y el módulo n1 El resultado de esta operación lo representa C1 Según el modo de funcionamiento de la invención, en el momento en que una parte del resultado C1 esté disponible, el módulo siguiente comienza su operación El módulo siguiente S efectúa su operación de encriptación con una clave secreta En cuanto se dispone parcialmente del resultado C2, éste es transmitido al módulo A2 para la tercera operación de encriptación utilizando la clave denominada privada compuesta por el exponente d2 y el módulo n2 El resultado final, denominado aquí C3, está listo para ser transmitido a través de las vías conocidas tales como la vía hertziana o por cable

La figura 2 representa el sistema para desencriptar formado por tres módulos para desencriptar A1', S', A2' similares a los que sirvieron para la encriptación, pero ordenados de forma inversa Así, se comienza primero por el módulo A2' que efectúa su operación para desencriptar tomando como base la clave denominada pública compuesta por el exponente e2 y el módulo n2 De la misma manera que para la encriptación, en el momento en que una parte del resultado C2 del módulo A2 está disponible, es transmitida al módulo S' para la segunda operación de desencriptación Para terminar con el proceso de desencriptación, el módulo A1' efectúa su operación utilizando como base la clave pública compuesta por el exponente e1 y el módulo n1

En una forma particular de la invención, las claves de los dos módulos A1 y A2 son idénticas, es decir, que la parte de encriptación, d1=d2 y n1=n2 Por analogía, en el momento de la desencriptación, e1=e2 y n1=n2 En tal caso, se habla de la clave privada d, n y de la clave pública e, n

En otra forma de la invención, ilustrada en las figuras 3 y 4, el módulo A2 utiliza la clave denominada pública en lugar de la clave denominada privada En el momento de la encriptación, la clave pública e2, n2 la utiliza el módulo A2, (ver figura 3) y en el momento de la desencriptación (ver figura 4), el módulo A2' utiliza la clave privada d2, n2 para operar A pesar de que esta configuración presenta una sobrecarga de trabajo en el conjunto de la desencriptación, la utilización de una clave privada refuerza la seguridad ofrecida por el módulo A2

El ejemplo de las figuras 3 y 4 no es restrictivo para otras combinaciones. Por ejemplo, se puede configurar el módulo A1 para que efectúe la operación para encriptar con la clave pública y para desencriptar con la clave privada

Del mismo modo, también se puede reemplazar el módulo para encriptar-desencriptar con clave secreta S mediante un módulo con clave asimétrica del mismo tipo que los módulos A1 y A2

REIVINDICACIONES

1. Método para encriptar y desencriptar, utilizando varios módulos en serie para encriptar-desencriptar, caracterizado porque el módulo para encriptar-desencriptar corriente abajo comienza su operación en el momento en que está disponible una parte del resultado del módulo para encriptar-desencriptar corriente arriba

2 Método según la reivindicación 1, caracterizado porque el módulo para desencriptar corriente abajo comienza su operación para desencriptar cuando está disponible una parte del resultado proporcionado por el módulo para desencriptar corriente arriba

3 Método según la reivindicación 1, caracterizado porque el módulo para encriptar corriente abajo comienza su operación para encriptar cuando está disponible una parte del resultado del módulo corriente arriba

4 Método según las reivindicaciones 1 a 3, caracterizado por consistir en emplear tres módulos (A1, S, A2) donde el módulo central (S) es del tipo de clave simétrica secreta (k)

5 Método según la reivindicación anterior, caracterizado porque el primer módulo (A1) y el último módulo (A2) para la encriptación y el primer módulo (A2) y el último módulo (A1) para la desencriptación son del tipo RSA de claves asimétricas privadas o públicas

6 Método según la reivindicación anterior, caracterizado porque ambos módulos (A1, A2) utilizan la clave privada (d, n, d1,n1, d2,n2) para encriptar y la clave publica (e, n, e1,n1, e2,n2) para desencriptar

7 Método según la reivindicación anterior, caracterizado porque ambos módulos (A1, A2) utilizan un mismo juego de clave privado (d, n) y público (e, n)

8 Método según la reivindicación 6, caracterizado porque ambos módulos (A1, A2) utilizan un juego diferente de claves privadas (d1,n1, d2,n2) y públicas (e1,n1, e2,n2)

9 Método según la reivindicación 5, caracterizado porque en el momento de encriptar, el último módulo (A2) utiliza la clave pública (e2,n2) y en el momento de desencriptar, el primer módulo (A2) utiliza la clave denominada privada (d2,n2)

10 Método según las reivindicaciones 1 a 3, caracterizado por consistir en emplear tres módulos (A1, A, A2) para encriptar-desencriptar de claves asimétricas

RESUMEN

Existen métodos para determinar la o las claves utilizadas por el módulo que analiza los datos que entran o salen de él en el momento de la utilización del módulo de encriptación-desencriptación Para paliar este defecto, el método multi-módulos propuesto consiste en que el módulo corriente abajo comience sus operaciones para encriptar-desencriptar cuando esté disponible una parte de los resultados del módulo corriente arriba

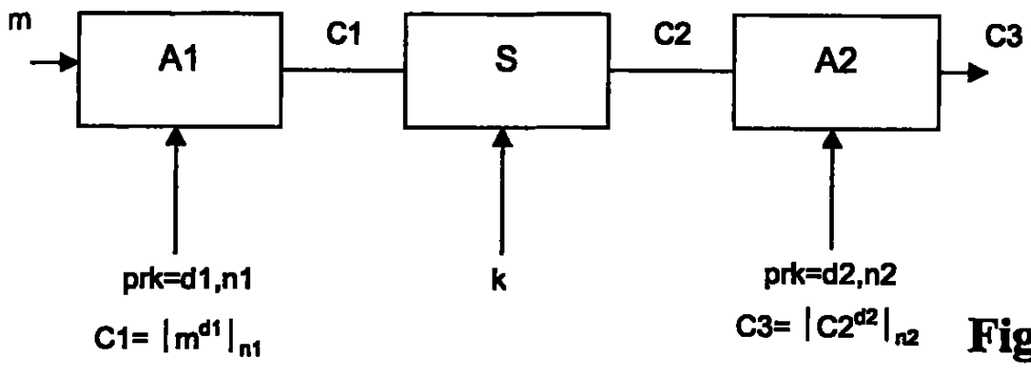

m
A1
C1
S
C2
A2
C3
prk=d1,n1
C1= |m^d1|n1
k
prk=d2,n2
C3= |C2^d2|n2

Fig. 1

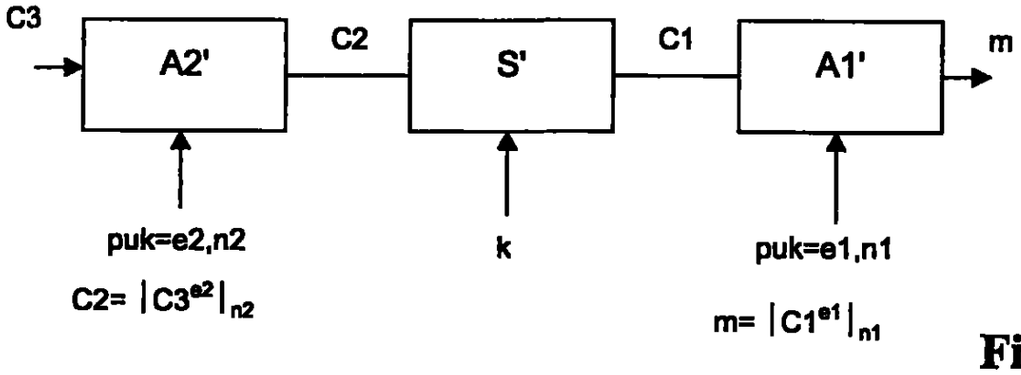

C3
A2'
C2
S'
C1
A1'
m
puk=e2,n2
C2= |C3^e2|n2
k
puk=e1,n1
m= |C1^e1|n1

Fig. 2

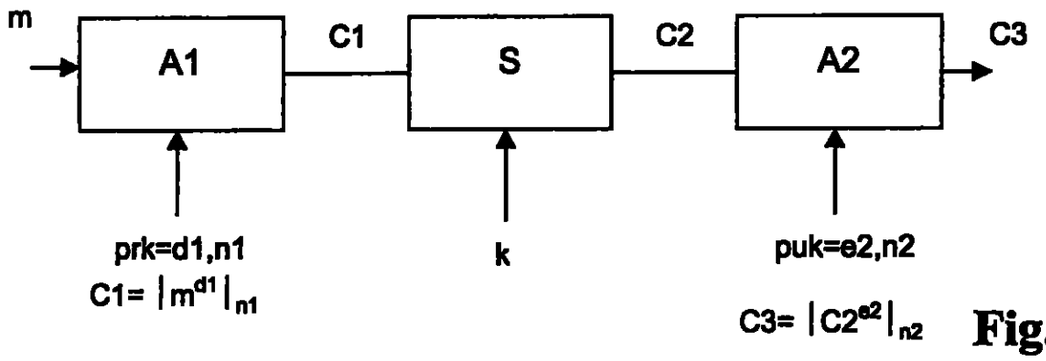

m
A1
C1
S
C2
A2
C3
prk=d1,n1
C1= |m^d1|n1
k
puk=e2,n2
C3= |C2^e2|n2

Fig. 3

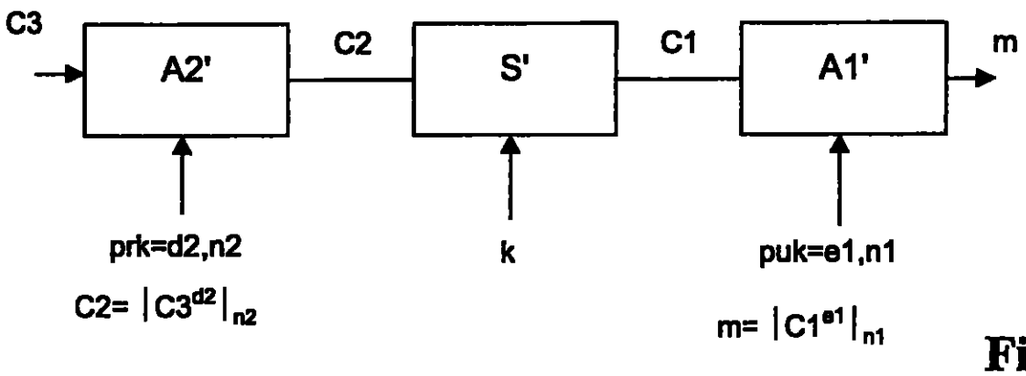

C3
A2'
C2
S'
C1
A1'
m
prk=d2,n2
C2= |C3^d2|n2
k
puk=e1,n1
m= |C1^e1|n1

Fig. 4

Se letto solo 18 pure pubblicati
2020 30 feb-2 - 2003.

SCHWEIZERISCHE EIDGENOSSENSCHAFT
CONFÉDÉRATION SUISSE
CONFEDERAZIONE SVIZZERA

Bescheinigung

Die beiliegenden Akten stimmen mit den ursprünglichen technischen Unterlagen des auf der nächsten Seite bezeichneten Patentgesuches für die Schweiz und Liechtenstein überein. Die Schweiz und das Fürstentum Liechtenstein bilden ein einheitliches Schutzgebiet. Der Schutz kann deshalb nur für beide Länder gemeinsam beantragt werden.

Attestation

Les documents ci-joints sont conformes aux pièces techniques originales de la demande de brevet pour la Suisse et le Liechtenstein spécifiée à la page suivante. La Suisse et la Principauté de Liechtenstein constituent un territoire unitaire de protection. La protection ne peut donc être revendiquée que pour l'ensemble des deux Etats.

Attestazione

Gli uniti documenti sono conformi agli atti tecnici originali della domanda di brevetto per la Svizzera e il Liechtenstein specificata nella pagina seguente. La Svizzera e il Principato di Liechtenstein formano un unico territorio di protezione. La protezione può dunque essere rivendicata solamente per l'insieme dei due Stati.

Bern, 10. Juli 2000

Eidgenössisches Institut für Geistiges Eigentum
Institut Fédéral de la Propriété Intellectuelle
Istituto Federale della Proprietà Intellettuale

Patentverfahren
Administration des brevets
Amministrazione dei brevetti

Rolf Hofstetter

Demande de brevet no 1999 1573/99

CERTIFICAT DE DEPOT (art 46 al 5 OBI)

L'Institut Fédéral de la Propriété Intellectuelle accuse réception de la demande de brevet Suisse dont le détail figure ci-dessous

Titre
Méthode d'encryptage multi-modules

Requérant
NagraCard S A
22, route de Genève
1033 Cheseaux-sur-Lausanne

Mandataire
Griffes Consulting S A
81, route de Florissant
1206 Genève

Date du dépôt 30 08 1999

Classement provisoire H03M

METHODE D'ENCRYPTAGE MULTI-MODULES

La présente invention concerne le domaine du chiffrement, ou encryptage, et du déchiffrage ou décryptage de données, et particulièrement de données devant rester inaccessibles aux personnes ou appareils non autorisés dans le cadre de systèmes de télévision à péage Dans de tels systèmes, les données sont chiffrées dans un environnement sécurisé, abritant des puissances de calcul importantes, et appelé sous-système d'encodage, puis envoyées, par des moyens connus en soi, vers au moins un sous-système décentralisé où elles sont déchiffrées, généralement au moyen d'un IRD (Integrated Receiver Decoder) et avec l'aide d'une carte à puce Cette carte à puce et le sous-système décentralisé qui coopère avec elle sont librement accessibles par une personne éventuellement non autorisée

Il est connu de chaîner divers moyens d'encryptage-décryptage dans un système de chiffrage-déchiffrage Dans toute la suite, on appellera encryptage - décryptage un moyen de cryptage particulier utilisé dans un système plus vaste de chiffrage-déchiffrage

On cherche depuis longtemps à optimiser le fonctionnement de ces systèmes du triple point de vue de la rapidité, de la place occupée en mémoire et de la sécurité La rapidité s'entend au sens du temps nécessaire pour déchiffrer les données reçues

Il est connu des systèmes d'encryptage - décryptage à clés symétriques Leur sécurité inhérente peut être qualifiée en fonction de plusieurs critères

Le premier critère est celui de la sécurité physique, relative à la facilité ou à la difficulté d'une méthode d'investigation par extraction de certains composants, suivie de leur remplacement éventuel par d'autres composants Ces composants de remplacement, destinés à renseigner la personne non autorisée sur la nature et le fonctionnement du système de chiffrage-déchiffrage, sont choisis par elle de manière à ne pas être détectés, ou le moins possible, par le reste du système

Un second critère est celui de la sécurité système, dans le cadre de laquelle les attaques ne sont pas intrusives du point de vue physique mais font appel à de l'analyse de type mathématique Typiquement, ces attaques seront menées par des ordinateurs de grande puissance qui tenteront de casser les algorithmes et les codes de chiffrement

Des moyens d'encryptage - décryptage à clés symétriques sont par exemple les systèmes appelés DES (Data Encryption Standard) Ces moyens, relativement anciens, n'offrent plus qu'une sécurité système et une sécurité physique toute relatives C'est notamment pour cette raison que de plus en plus, le DES, dont les longueurs de clés sont trop petites pour satisfaire aux conditions de sécurité système, est remplacé par des moyens d'encryptage - décryptage nouveaux ou avec des clés plus longues De manière générale, ces moyens à clés symétriques font appel à des algorithmes comprenant des rondes de chiffrement

D'autres stratégies d'attaques sont appelées Simple Power Analysis, et Timing Analysis. Dans le Simple Power Analysis, on utilise le fait qu'un microprocesseur chargé d'encrypter ou de décrypter des données est connecté à une source de tension (en général 5 Volts). Lorsqu'il est au repos, il est parcouru par un courant fixe d'intensité i Quand il est actif, l'intensité instantanée i est fonction, non seulement des données entrantes, mais aussi de l'algorithme d'encryptage Le Simple Power Analysis consiste à mesurer le courant i en fonction du temps On peut de ce fait déduire le type d'algorithme que le microprocesseur effectue

De la même manière, la méthode du Timing Analysis consiste à mesurer la durée de calcul en fonction d'un échantillon présenté au module de décryptage Ainsi, la relation entre l'échantillon présenté et le temps de calcul du résultat permet de retrouver les paramètres secrets de module de décryptage tel que la clé Un tel système est décrit par exemple dans le document "Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems" publié par Paul Kocher, Cryptography Research, 870 Market St, Suite 1088, San Francisco, CA-USA

Pour améliorer la sécurité du système de chiffrement, il a été proposé des algorithmes à clé asymétriques, tels que les systèmes dits RSA (Rivest, Shamir et Adleman) Ces systèmes comprennent la génération d'une paire de clés appariées, l'une dite publique servant au chiffrement, et l'autre dite privée servant au déchiffrement Ces algorithmes présentent un haut niveau de sécurité tant système que physique Ils sont par contre plus lents que les systèmes traditionnels, surtout au stade du chiffrement

Les techniques d'attaque les plus récentes font appel à la notion dite DPA, de l'anglais Differential Power Analysis Ces méthodes sont basées sur des supputations, vérifiables au bout d'un grand nombre d'essais, sur la présence d'un 0 ou d'un 1 dans une position donnée de la clé de chiffrement. Elles sont quasiment non destructives, ce qui leur confère une bonne indétectabilité, et font appel à la fois à une composante d'intrusion physique et à une composante d'analyse mathématique Leur fonctionnement rappelle les techniques d'investigation de champs pétrolifères, où une explosion de puissance connue est générée en surface et où des écouteurs et sondes, placés à des distances également connues du lieu de l'explosion, permettent d'émettre des suppositions sur la composition stratigraphique du sous-sol sans trop avoir à le creuser, grâce à la réflexion des ondes de choc par les limites de couches sédimentaires dans ce sous-sol Les attaques DPA sont décrites notamment dans le § 2 1 du document "A Cautionary Note Regarding Evaluation of AES Candidates on Smart-Cards", publié le 1er février 1999 par Suresh Chari, Charanjit Jutla, Josyula R Rao et Pankaj Rohatgi, de l'IBM T J Watson Research Center, Yorktown Heights, NY

L'exigence de devoir résister aux attaques DPA oblige à utiliser des systèmes de brouillage dit "whitening", soit dans les informations à l'entrée, soit en sortie d'un algorithme de chiffrement-déchiffrement La technique du whitening est décrite dans le § 3 5 du même document précité

De plus le fait que les puissances de calcul soient limitées dans le sous-système décentralisé d'un système de télévision à péage crée un problème, qui n'a jamais encore été résolu de façon satisfaisante, pour effectuer dans une mesure suffisante le chaînage décrit précédemment

Le but de la présente invention est de disposer d'une méthode d'encryptage-décrytage qui résiste aux méthodes modernes d'investigation telles que décrites ci-dessus

Le but visé par la présente invention est atteint par la méthode décrite dans la partie caractérisante de la revendication 1

La particularité de la méthode réside dans le fait qu'un module intermédiaire ne démarre pas lorsque le résultat du module précédent (ou amont) a terminé mais débute dès qu'une partie déjà des informations sont disponibles De ce fait, pour un observateur extérieur, il n'est pas possible d'établir les conditions d'entrée ou de sortie de ce module

Comme le déchiffrage intervient dans le sous-système décentralisé coopérant avec la carte à puce, cette carte à puce n'abritant que des puissances de calcul relativement limitées par rapport au sous-système d'encodage, il est par exemple intéressant d'utiliser une clé asymétrique publique, au fonctionnement relativement rapide, lors des dernières étapes du déchiffrage Ceci permet d'une part de préserver les caractéristiques d'invulnérabilité du système en sortie de processus, et d'autre part de concentrer la puissance de calcul, liée essentiellement au chiffrage à l'aide de la clé privée, dans le sous-système d'encodage

Il a été découvert qu'une sécurité supplémentaire est procurée par la possibilité de concaténer, ou d'imbriquer partiellement, deux moyens d'encryptage-décryptage qui se suivent séquentiellement On entend par cette concaténation ou imbrication partielle, qui est une traduction de l'anglais "interleaving", le procédé consistant à démarrer l'action du deuxième moyen d'encryptage-décryptage sur les données à un moment où le premier moyen d'encryptage-décryptage n'a pas encore terminé son travail sur ces mêmes données Ceci permet de masquer les données telles qu'elles résulteraient du travail du premier module et avant qu'elles ne soient soumises à l'action du deuxième module

La chaînage peut démarrer dès que des données calculées en sortie du premier module sont partiellement disponibles pour être traitées par le second module

L'invention permet de se prémunir contre les attaques précitées en combinant divers moyens d'encryptage-décryptage dans un système de chiffrage-déchiffrage, et en associant éventuellement une concaténation ou imbrication partielle à la séquence dans laquelle se suivent ces moyens

Dans une forme particulière de réalisation de l'invention, le système de chiffrage-déchiffrage comprend un sous-système d'encodage où trois algorithmes sont utilisés séquentiellement

a) un algorithme A1 asymétrique à clé privée d1 Cet algorithme A1 effectue une signature sur des données en clair, représentées par un message m, cette opération délivrant un premier cryptogramme c1, au moyen d'opérations mathématiques généralement notées dans la profession par la formule c1 = m exposant d1, modulo n1 Dans cette formule, n1 fait partie de la clé publique de l'algorithme asymétrique A1, modulo représente l'opérateur mathématique bien connu des congruences dans l'ensemble des entiers relatifs, et d1 est la clé privée de l'algorithme A

b) un algorithme S symétrique utilisant une clé secrète K Cet algorithme convertit le cryptogramme c1 en un cryptogramme c2

c) un algorithme A2 asymétrique à clé privée d2 Cet algorithme A2 convertit le cryptogramme c2 en un cryptogramme c3, au moyen de l'opération mathématique notée, comme précédemment, par c3 = c2 exposant d2 mod n2, formule dans laquelle n2 fait partie de la clé publique de l'algorithme asymétrique A2, et d2 est la clé privée de l'algorithme A2

Le cryptogramme c3 part du sous-système d'encodage et parvient au sous-système décentralisé par des moyens connus en soi Dans le cas de systèmes de télévision à péage, il peut s'agir aussi bien de données vidéo que de messages

Le sous-système décentralisé utilise, dans l'ordre inverse du précédent, trois algorithmes A1', S' et A2' Ces trois algorithmes font partie de trois moyens de cryptage-décryptage A1-A1', S-S' et A2-A2', répartis entre le sous-système d'encodage et le sous-système décentralisé, et représentant le système de chiffrage-déchiffrage

d) l'algorithme A2' effectue sur c3 une opération mathématique restituant c2 et notée c2 = c3 exposant e2 mod n2 Dans cette formule, l'ensemble constitué de e2 et n2 est la clé publique de l'algorithme asymétrique A2-A2'

e) l'algorithme symétrique S' symétrique utilisant la clé secrète K restitue le cryptogramme c1

f) l'algorithme A1' asymétrique à clé publique e1, n1 retrouve m en effectuant l'opération mathématique notée m = c1 exposant e1 mod n1

La concaténation, dans le sous-système décentralisé, consiste à démarrer l'étape de décodage e) alors que c2 n'a pas encore été totalement restitué par l'étape précédente d), et à démarrer l'étape de décodage f) alors que c1 n'a pas été totalement restitué par l'étape e. L'avantage est de déjouer une attaque qui viserait par exemple d'abord à extraire, dans le sous-système décentralisé, le cryptogramme c1 en fin d'étape e, pour le comparer avec les données en clair m, puis au moyen de c1 et de m d'attaquer l'algorithme A1', puis de remonter la chaîne de codage de proche en proche

La concaténation n'est pas nécessaire dans le sous-système d'encodage, qui est installé dans un environnement physique sécurisé Elle est par contre utile dans le sous-système décentralisé Dans le cas de la télévision à péage, l'IRD est en effet installé chez l'abonné et peut être l'objet des attaques du type prédécrit

On conçoit qu'une attaque d'une combinaison de trois algorithmes de décryptage A1', S' et A2' concaténés a beaucoup moins de chances de réussir que si les cryptogrammes c1 et c2 sont intégralement reconstitués entre chaque étape d), e) et f) Par ailleurs, le fait que les algorithmes A1' et A2' soient utilisés avec des clés publiques e1, n1 et e2, n2 fait que les

moyens de calcul nécessaires dans le sous-système décentralisé sont bien plus réduits que dans le sous-système d'encodage

A titre d'exemple et pour fixer les idées, les étapes a) et c) c'est-à-dire les étapes d'encryptage avec clés privées, sont 20 fois plus longues que les étapes d) et f) de décryptage avec clés publiques

Dans une forme particulière de réalisation de l'invention, dérivée de la précédente, les algorithmes A1 et A2 sont identiques de même que leurs contreparties A1' et A2'

Dans une forme particulière de réalisation de l'invention, également dérivée de la précédente, dans l'étape c) on utilise la clé publique e2, n2 de l'algorithme asymétrique A2 alors que dans l'étape d) on décrypte le cryptogramme c3 avec la clé privée d2 de cet algorithme Cette forme constitue une alternative possible lorsque les ressources du sous-système décentralisé en puissance de calcul sont loin d'être atteintes

Bien que les cartes à puces sont utilisées majoritairement pour le décryptage des données, il existe également des cartes à puces ayant les capacités nécessaires pour effectuer des opérations de cryptage Dans ce cas, les attaques décrites plus haut vont se porter également sur ces cartes de cryptage qui fonctionnent hors d'endroits protégés tels qu'un centre de gestion C'est pourquoi la méthode selon l'invention s'applique également aux opérations de cryptage en série c'est à dire que le module aval débute son opération de cryptage dès qu'une partie des informations délivrées par le module amont sont disponibles Ce procédé à l'avantage d'imbriquer les différents modules de cryptage avec comme conséquence que le résultat du module amont n'est pas disponible complètement à un temps donné De plus, le module en aval ne débute pas ses opérations avec un résultat complet mais sur des parties ce qui rend impraticable d'interpréter le fonctionnement d'un module par rapport à un état d'entrée ou de sortie connu

La présente invention sera comprise plus en détail grâce aux dessins suivants, pris à titre non limitatifs, dans lesquels

- la figure 1 représente les opérations de cryptage
- la figure 2 représente les opérations de décryptage
- la figure 3 représente une alternative à la méthode de cryptage

Sur la figure 1, un ensemble de données m est introduit dans la chaîne de cryptage Un premier élément A1 effectue une opération de cryptage en utilisant la clé dite privée composée de l'exposent d1 et du modulo n1 Le résultat de cette opération est représenté par C1 Selon le mode de fonctionnement de l'invention, dès qu'une partie du résultat C1 est disponible, le module suivant débute son opération Ce module suivant S effectue son opération de cryptage avec une clé secrète Le résultat C2 dès que partiellement disponible est transmis au module A2 pour la troisième opération de cryptage utilisant la clé dite privée composée de l'exposant d2 et du modulo n2 Le résultat final, dénommé ici C3 est prêt pour être transmis par des voies connues tels que voie hertzienne ou par câble

La figure 2 représente le système de décryptage composé des trois modules de décryptage A1', S', A2' similaires à ceux ayant servi à l'encryptage, mais ordonné inversement Ainsi, l'on commence d'abord avec le module A2' qui effectue son opération de décryptage sur la base de la clé dite publique composées de l'exposant e2 et du modulo n2 De la même manière que pour l'encryptage, dès qu'une partie du résultat C2 du module A2' est disponible, il est transmis au module S' pour la deuxième opération de décryptage. Pour terminer le décryptage, le module A1' effectue son opération sur la base de la clé dite publique composée de l'exposent e1 et du modulo n1.

Dans une forme particulière de l'invention, les clés des deux modules A1 et A2 sont identiques, c'est-à-dire que côté encryptage, d1=d2 et n1=n2 Par analogie, lors du décryptage, e1=e2 et n1=n2. Dans ce cas, on parle de la clé privée d, n et de la clé publique e, n

Dans une autre forme de l'invention, telle qu'illustrée aux figures 3 et 4, le module A2 utilise la clé dite publique à la place de la clé dite privée Au moment de l'encryptage, la clé publique e2, n2 est utilisée par le module A2,

(voir figure 3) et lors du décryptage (voir figure 4), le module A2' utilise la clé privée d2, n2 pour opérer Bien que cette configuration présente une surcharge de travail à l'ensemble de décryptage, l'utilisation d'une clé privée renforce la sécurité offerte par le module A2

L'exemple illustré aux figures 3 et 4 n'est pas restrictif pour d'autres combinaisons Par exemple, il est possible de configurer le module A1 pour qu'il effectue l'opération d'encryptage avec la clé publique et le décryptage avec la clé privée

Il est également possible de remplacer le module d'encryptage-décryptage à clé secrète S par un module de type à clé asymétriques du même type que les module A1 et A2

REVENDICATIONS

1 Méthode de cryptage et de décryptage utilisant plusieurs modules d'encryptage-décryptage en séne, caractérisée en ce que le module d'encryptage-décryptage en aval débute son opération dès qu'une partie du résultat du module d'encryptage-décryptage amont est disponible

2 Méthode selon la revendication 1, caractérisée en ce que le module de décryptage en aval débute son opération de décryptage dès qu'une partie du résultat du module de décryptage amont est disponible

3 Méthode selon la revendication 1, caractérisée en ce que le module d'encryptage en aval débute son opération de cryptage dès qu'une partie du résultat du module amont est disponible

4 Méthode selon les revendication 1 à 3, caractérisée en ce qu'elle met en œuvre trois modules (A1, S, A2) , le module central (S) étant de type à clé symétrique secrète (k)

5 Méthode selon la revendication précédente, caractérisée en ce que le premier module (A1) et le dernier module (A2) pour l'encryptage et le premier module (A2) et le dernier module (A1) pour le décryptage sont du type RSA à clés asymétriques soit avec une clé privée et une clé publique

6 Méthode selon la revendication précédente, caractérisée en ce que les deux modules (A1, A2) utilisent la clé dite privée (d,n, d1,n1, d2,n2) pour l'encryptage et la clé dite publique (e, n, e1,n1, e2,n2) pour le décryptage

7 Méthode selon la revendication précédente, caractérisée en ce que les deux modules (A1, A2) utilisent un même jeu de clé privée (d, n) et publique (e, n)

8 Méthode selon la revendication 6, caractérisée en ce que les deux modules (A1, A2) utilisent un jeu différent de clés privée (d1,n1, d2,n2) et publique (e1, n1, e2,n2)

9 Méthode selon la revendication 5, caractérisée en ce que lors de l'encryptage, le dernier module (A2) utilise la clé dite publique (e2,n2) et lors du décryptage, le premier module (A2) utilise la clé dite privée (d2,n2)

10 Méthode selon les revendications 1 à 3, caractérisée en ce qu'elle met en œuvre trois modules (A1, A, A2) d'encryptage-décryptage à clés asymétriques

ABREGE

Lors de l'utilisation d'un module d'encryptage-décryptage, des méthodes existent pour déterminer la ou les clés utilisées par le module en analysant les données entrantes ou sortantes du module Pour pallier ce défaut, la méthode multi-modules proposées consiste à ce que le module aval débute ses opérations d'encryptage-décryptage dès qu'une partie des résultats du module amont est disponible

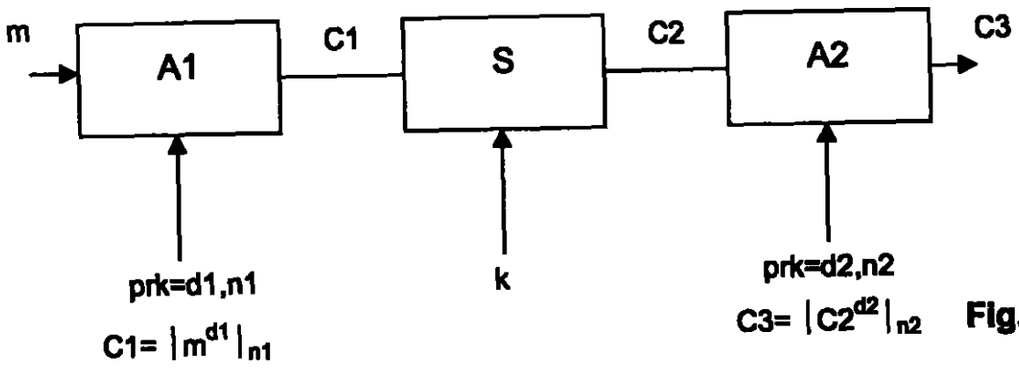

m
A1
C1
S
C2
A2
C3
prk=d1,n1
C1= |m^d1|n1
k
prk=d2,n2
C3= |C2^d2|n2

Fig. 1

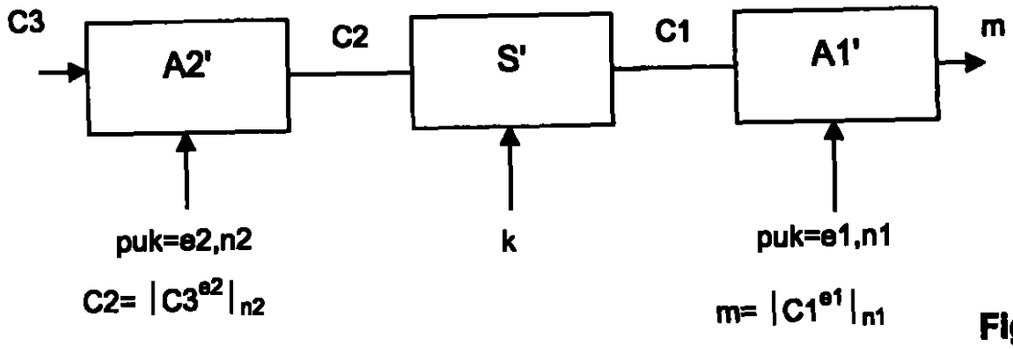

C3
A2'
C2
S'
C1
A1'
m
puk=e2,n2
C2= |C3^e2|n2
k
puk=e1,n1
m= |C1^e1|n1

Fig. 2

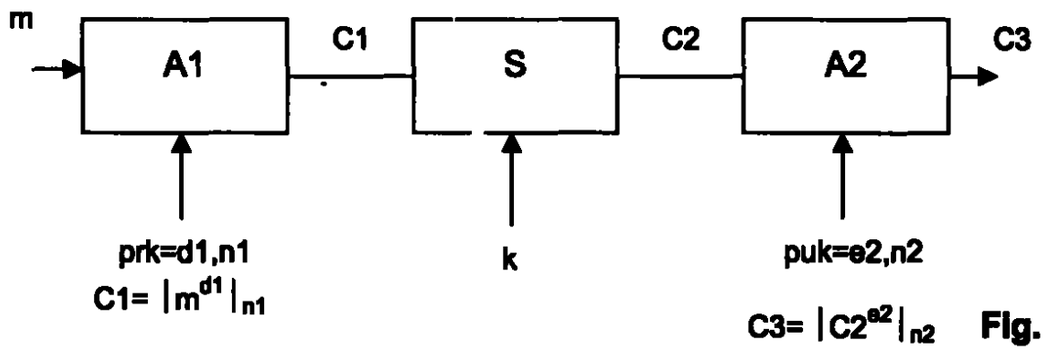

m
A1
C1
S
C2
A2
C3
prk=d1,n1
C1= |m^d1|n1
k
puk=e2,n2
C3= |C2^e2|n2

Fig. 3

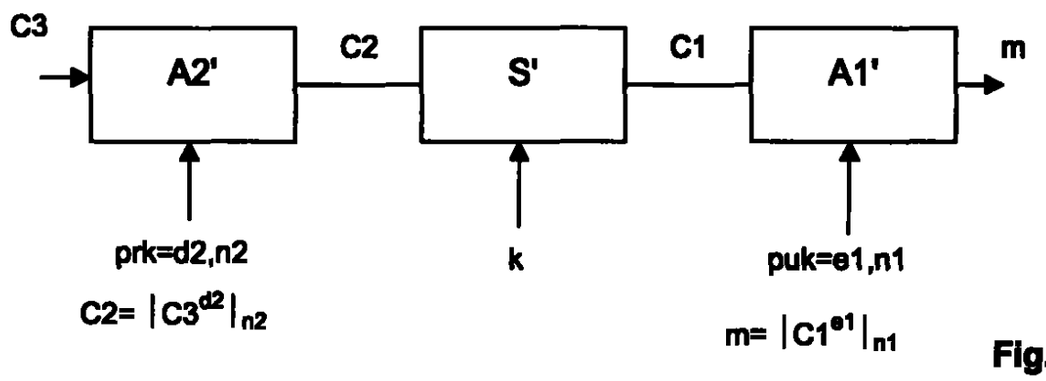

C3
A2'
C2
S'
C1
A1'
m
prk=d2,n2
C2= |C3^d2|n2
k
puk=e1,n1
m= |C1^e1|n1

Fig. 4

TRADUCCION: Se traduce la carátula y las reivindicaciones anexas a una copia de la solicitud de patente Suiza No. 1573/99 escrita en francés. Para el invento denominado: MÉTODO DE ENCRIPTAR MULTI-MÓDULOS

CONFEDERACION SUIZA

CERTIFICACION

Los documentos adjuntos están de acuerdo con los documentos originales relativos a la solicitud de patente depositada ante la Oficina de Recepción de acuerdo con el Artículo 10 del Tratado de Cooperación en Materia de Patentes (PCT)

Berna 10 de Julio de 2000.

INSTITUTO FEDERAL DE LA PROPIEDAD INTELECTUAL

El Jefe de la Sección de Patentes

(Firmado por): Rolf HOFSTETTER

Cinta y Sello de Oblea

51.

REIVINDICACI NES

1. Método para encriptar y desencriptar, utilizando varios módulos en serie para encriptar-desencriptar, caracterizado porque el módulo para encriptar-desencriptar corriente abajo comienza su operación en el momento en que está disponible una parte del resultado del módulo para encriptar-desencriptar corriente arriba

2 Método según la reivindicación 1, caracterizado porque el módulo para desencriptar corriente abajo comienza su operación para desencriptar cuando está disponible una parte del resultado proporcionado por el módulo para desencriptar corriente arriba

3 Método según la reivindicación 1, caracterizado porque el módulo para encriptar corriente abajo comienza su operación para encriptar cuando está disponible una parte del resultado del módulo corriente arriba

4 Método según las reivindicaciones 1 a 3, caracterizado por consistir en emplear tres módulos (A1, S, A2) donde el módulo central (S) es del tipo de clave simétrica secreta (k)

5 Método según la reivindicación anterior, caracterizado porque el primer módulo (A1) y el último módulo (A2) para la encriptación y el primer módulo (A2) y el último módulo (A1) para la desencriptación son del tipo RSA de claves asimétricas privadas o públicas

6 Método según la reivindicación anterior, caracterizado porque ambos módulos (A1, A2) utilizan la clave privada (d, n, d1,n1, d2,n2) para encriptar y la clave pública (e, n, e1,n1, e2,n2) para desencriptar

7 Método según la reivindicación anterior, caracterizado porque ambos módulos (A1, A2) utilizan un mismo juego de clave privado (d, n) y público (e, n)

8 Método según la reivindicación 6, caracterizado porque ambos módulos (A1, A2) utilizan un juego diferente de claves privadas (d1,n1, d2,n2) y públicas (e1,n1, e2,n2)

9 Método según la reivindicación 5, caracterizado porque en el momento de encriptar, el último módulo (A2) utiliza la clave pública (e2,n2) y en el momento de desencriptar, el primer módulo (A2) utiliza la clave denominada privada (d2,n2)

10 Método según las reivindicaciones 1 a 3, caracterizado por consistir en emplear tres módulos (A1, A, A2) para encriptar-desencriptar de claves asimétricas

[redacted]

FORMATO DE DIGITALIZACION
RELACION DE ANEXOS

Royal Technologies S.A.

28

Item		Expediente No	0906 80 33	No de Folio
			No de unidades	√
1	CD			
2	DVD			
3	REVISTA			
4	LIBRO			
5	PERIODICO			
6	DISQUETES			
7	SOBRE DE MANILA		1	
8	SOBRE BLANCO TAMAÑO CARTA			
9	SOBRE BLANCO TAMAÑO OFICIO			
10	OTROS			

Observaciones: contiene Acta final

29 31

Industria y Comercio
SUPERINTENDENCIA

SUPERINDUSTRIA Y COMERCIO
Radicacion : [illegible] Folios: 2
Fecha (RAD): [illegible] 16:52.1[illegible]
Tramite : [illegible] 1 REGISTRO/ 411 [illegible]
NIT 800176089 Dependencia: 2020 DIVISION DE [illegible] CREACIONES

RECIBO OFICIAL DE CAJA 52,340
FECHA : AGOSTO 22 DE 2000

CONSIGNACION

DEPOSITANTE	TIPO PAGO	BANCO	SUCURSAL	CUENTA	No. PAGO	Vr PAGO
CAVELIER ABOGADOS	CONSIGNACION	BANCO POPULAR	BOGOTA	050-00110-6	2079236	17,729,500.00

CONCEPTO

CANT.	RENTISTICO		CONCEPTO	TOTAL CONCEPTO
1	50005-01-01	SOLICITUDES	1 TRAMITES DE SOL DE PATENTE DE IN	608,000.00
			TOTAL . $	608,000.00

SON SEISCIENTOS OCHO MIL PESOS

RESPONSABLE ______________________

RECIBO DE CAJA APLICADO AL EXPEDIENTE No.______________________

Cdo 12[illegible]24-B01-001-9

Carrera 13 No 27-00 Pisos 5 y 10
Conmutador 334 12 21
Fax 281 31 25
Santa Fe de Bogota D C Colombia

22
30

REQUISITOS MINIMOS PARA ADMISION A TRAMITE

PATENTE DE INVENCIÓN [X] **MODELO DE UTILIDAD [ ]**

- Nombre e identificación del Solicitante 1 [X]
- Nombre e identificación del Inventor 1 [X]
- Titulo o nombre de la Invención 1 [X]
- Descripción [X]
- Reivindicaciones 11 [X]
- Resumen 13 [X]
- Comprobante de Pago 71 [X]
- Poder, cuado proceda [ ]
- Copia de la primera solicitud de patente, si reivindica prioridad, señalándola expresamente [ ]
- Firma del solicitante o apoderado [ ]

COMPLETA [ ] INCOMPLETA [ ]

DISEÑO INDUSTRIAL [ ]

- Nombre e identificación del peticionario [ ]
- Nombre e identificación del inventor o diseñador [ ]
- Indicación del género de productos para los cuales debe utilizarse [ ]
- Representación gráfica [ ]
- Comprobante de pago [ ]
- Poder, cuado proceda [ ]
- Firma del solicitante o apoderado [ ]

COMPLETA [ ] INCOMPLETA [ ]

Firma Responsable

Fecha _____

Carrera 13 No 27-00 Piso 5 y 10
Conmutador 334 12 21-2-3-4
Fax 281 31 25 e-mail info@sic.gov.co
Santa Fe de Bogotá D.C. - Colombia

DIVISION DE NUEVAS CREACIONES
PRIMER EXAMEN DE FORMA

EXPEDIENTE 00-65033
Practicado el examen jurídico de acuerdo con lo establecido en el art. 21 de la Decisión 344 se determinó que esta solicitud de Patente de Invención:

SI [ ] NO [x] **NO APLICABLE [ ] Presentó los poderes necesarios en forma correcta (Decisión 344, art. 14-a).**

SI [ ] NO [x] **NO APLICABLE [ ] Acreditó, en forma correcta, la existencia y representación de la persona jurídica solicitante (art. 14-c de la Decisión 344, literal g) del art. 4 del Decreto 117/94).**

SI [x] NO [ ] **NO APLICABLE [ ] Presentó, en forma correcta, el comprobante de pago por la tasa de presentación establecida (art. 13-f de la Decisión 344 y la Resolución 02 del 4 de Enero del 2000)**

SI [x] NO [ ] **EXTEMPORANEAMENTE [ ] Reivindicó prioridad, dentro del plazo y de acuerdo con lo previsto en el Artículo 4 del Convenio de Paris**

SI [x] NO [ ] **NO APLICABLE [ ] Presentó copia, certificada su conformidad por la Administración que recibió la solicitud de la cual reivindica prioridad, al momento de radicar la solicitud nacional**

SI [x] NO [ ] **NO APLICABLE [ ] Presentó la traducción del capítulo reivindicatorio de la solicitud de la cual se reivindica prioridad (Art. 4, D-3 Convenio de París; Concepto 5 de enero de 1999 S I.C)**

SI [ ] NO [x] **CUMPLE LOS REQUISITOS JURIDICOS**

OBSERVACIONES

En consecuencia, se conceptúa que esta solicitud

SI [ ] NO [X] **Se ajusta a los aspectos FORMALES indicados en la Decisión 344 y por tanto,**

SI [ ] NO [X] **Se recomienda PUBLICAR el extracto correspondiente.**

Bogotá, D.C , 31 de agosto del 2000

EXAMINADOR JURIDICO.
202022

DIVISIÓN NUEVAS CREACIONES

PRIMER EXAMEN DE FORMA

EXPEDIENTE Nº 2000-65.033

CONCEPTO TÉCNICO Nº 1480 **IPC:** H04N 7/16 // H04L 9/32

Practicado el examen de acuerdo a lo establecido en el Art 21 de la Decisión 344 se determinó que esta solicitud de **Patente de Invención:**

SI ☑ NO ☐	Contiene la identificación correcta del inventor (Art.8, Art 13-a)
SI ☑ NO ☐	Contiene la identificación correcta del solicitante (Artículo 13-a)
SI ☑ NO ☐	Contiene el resumen con el objeto y finalidad de la invención en forma correcta (Art 13-e)
SI ☑ NO ☐	Contiene el título o nombre de la invención en forma correcta (Art 13-b)
SI ☑ NO ☐	Contiene la descripción clara y completa de la invención (Art 13-c)
SI ☑ NO ☐	Contiene los dibujos correctos (Art 14-c junto con el literal d) del Art 4 del Dto 117 del 94)
SI ☑ NO ☐	Contiene las unidades de medida en el sistema exigido (Art 14-c junto con el Decreto 3464 del 26 de diciembre de 1980)
SI ☑ NO ☐	Contiene una o más reivindicaciones, en forma correcta, que precisen la materia para la cual se solicita la protección mediante la patente (Art 13-d)
SI ☑ NO ☐	Contiene el extracto de acuerdo con el literal c) del artículo 4 del Dto 117 /94
SI ☑ NO ☐	Contiene el arte final del dibujo característico de acuerdo con el literal c) del artículo 4 y el artículo 27 del Dto 117 /94
SI ☑ NO ☐	Contiene la tarjeta del Archivo Temático [formato P-104] en forma correcta (Art 14-c junto con el literal b) del artículo 4 del Dto 117 /94)
SI ☑ NO ☐	Contiene la tarjeta del Archivo de Propietarios [formato P-105] en forma correcta (Art 14-c junto con el literal b) del artículo 4 del Dto 117 /94)
SI ☑ NO ☐	**CUMPLE LOS REQUISITOS TÉCNICOS**

OBSERVACIONES Y OTROS SI ☐ NO ☑ ver hoja(s) anexa(s)
Los documentos aportados reúnen los requisitos técnicos mínimos, puede ordenarse la PUBLICACIÓN del extracto

Santa Fe de Bogotá, D C , 2000 09 05

202004
EXAMINADOR TÉCNICO

DIVISION DE NUEVAS CREACIONES

EXPEDIENTE 00-65033

AUTO 3062

DISPONE

ARTICULO PRIMERO: Conforme lo establece el artículo 22 de la Decisión 344 de la Comisión del Acuerdo de Cartagena, requiérese al solicitante, para que dentro del plazo de treinta (30) días hábiles siguientes a la fecha de notificación del auto, presente respuesta a las observaciones o complemente los antecedentes señalados en el examen de forma.

ARTICULO SEGUNDO: Notificar por estado el presente auto, advirtiendo que contra el no procede recurso alguno en la vía gubernativa

NOTIFIQUESE Y CUMPLASE
Dado en Bogotá D.C., a los 12 SEP 2000

EL JEFE DE LA DIVISION DE NUEVAS CREACIONES,

ALIX CARMENZA CESPEDES DE VERGEL

NOTIFICADO POR ESTADO

Bogotá D.C., 14 SET. 2000 notificado por anotación en estado de esta misma fecha

VENCIMIENTO NOTIFICACION ESTADO 27-10-00

SOLICITO PRORROGA TERMINO SI____ NO____

VENCIMIENTO TERMINO PRORROGA

202022

Carrera 13 N° 27-00 Pisos 5° y 10°
Conmutador 334 1221-2-3-4
Fax 281 3125
Santafé de Bogotá, D C. - Colombia