(12) SOLICITUD INTERNACIONAL PUBLICADA EN VIRTUD DEL TRATADO DE COOPERACIÓN EN MATERIA DE PATENTES (PCT)

(19) Organización Mundial de la Propiedad Intelectual
Oficina internacional

(43) Fecha de publicación internacional
28 de junio de 2012 (28.06.2012)

W I P O I P C T

(10) Número de Publicación Internacional
WO 2012/085323 A1

(51) Clasificación Internacional de Patentes:
G06F 21/00 (2006.01)

(21) Número de la solicitud internacional:
PCT/ES201 1/070898

(22) Fecha de presentación internacional:
23 de diciembre de 201 1 (23.12.201 1)

(25) Idioma de presentación: español

(26) Idioma de publicación: español

(30) Datos relativos a la prioridad:
P201031 941
24 de diciembre de 2010 (24. 12.2010) ES

(71) Solicitante *(para todos los Estados designados salvo US):* **UNIVERSIDAD POLITÉCNICA DE MADRID** [ES/ES]; C/ Ramiro de Maeztu, 7, E-28040 Madrid (ES).

(72) Inventores; e

(75) Inventores/Solicitantes *(para US solamente):* **JARA VERA, Vicente** [ES/ES]; Universidad Politécnica De Madrid, C/ Ramiro de Maeztu, 7, E-28040 Madrid (ES). **SÁNCHEZ ÁVILA, Carmen** [ES/ES]; Universidad Politécnica De Madrid, C/ Ramiro de Maeztu, 7, E-28040 Madrid (ES).

(74) Mandatario: **ARIAS SANZ, Juan;** ABG Patentes, S.L., Avenida de Burgos, 16D, Edificio Euromor, E-28036 Madrid (ES).

(81) Estados designados *(a menos que se indique otra cosa, para toda clase de protección nacional admisible):* AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Estados designados *(a menos que se indique otra cosa, para toda clase de protección regional admisible):* ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), euroasiática (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europea (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continúa en la página siguiente]

(54) Title: SYSTEM FOR SLOWING DOWN THE TRANSFER RATE OF A DEVICE BY THE CRYPTOGRAPHIC METHOD

(54) Título : SISTEMA DE RALENTIZACIÓN DE LA TASA DE TRANSFERENCIA DE UN DISPOSITIVO POR MÉTODO CRIPTOGRÁFICO

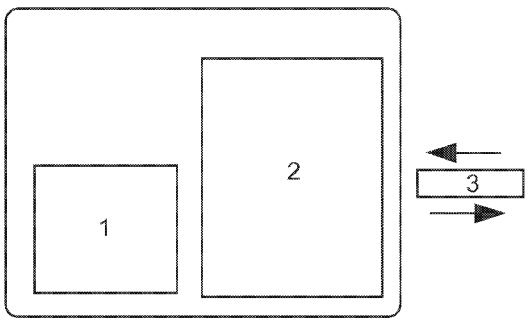

FIG. 1

(57) Abstract: The invention relates to a system for slowing down the transfer rate of a device by the cryptographic method, including: a processing means (1) configured to: select a type of encryption; encrypt information according to the type of encryption selected, including: converting the information to be encrypted into a string of numeric characters, dividing the string of characters into blocks of a variable number of characters and encrypting each of the blocks according to the type of encryption selected; and randomly generating a plurality of codes. The system additionally includes: a memory (2) that stores the plurality of codes generated, the encrypted information and the operations and intermedíate variables created by the processing means; and a means of input and output (3) configured to receive external information for carrying out the encryption tasks.

(57) Resumen:

[Continúa en la página siguiente]

WO 2012/085323 A1

Publicada:

— *con informe de búsqueda internacional (Art. 21(3))*

— *antes de la expiración del plazo para modificar las reivindicaciones y para ser republicada si se reciben modificaciones (Regla 48.2(h))*

Sistema de ralentización de la tasa de transferencia de un dispositivo por método criptográfico que comprende: unos medios de procesamiento (1) configurados para: seleccionar un tipo de cifrado; cifrar información según el tipo de cifrado seleccionado, comprendiendo: convertir la información a cifrar en una cadena de caracteres numéricos, dividir la cadena de caracteres en bloques de un número variable de caracteres y cifrar cada uno de los bloques según el tipo de cifrado seleccionado; generar aleatoriamente una pluralidad de claves; el sistema adicionalmente comprende: una memoria (2) que almacena la pluralidad de claves generadas, la información cifrada y las operaciones y variables intermedias realizadas por los medios de procesamiento; y unos medios de entrada y salida (3) configurados para recibir y enviar información del exterior para realizar las tareas de cifrado.

SISTEMA DE RALENTIZACIÓN DE LA TASA DE TRANSFERENCIA DE UN DISPOSITIVO POR MÉTODO CRIPTOGRÁFICO

CAMPO DE LA INVENCIÓN

La presente invención pertenece al campo de la criptografía.

ESTADO DE LA TÉCNICA

Hasta ahora la criptografía se ha usado en su sentido propio, cifrar con una clave y descifrar con una clave.

Son destacables los siguientes documentos relacionados con la presente invención.

El documento US2005210249-A1 ofrece un dispositivo de almacenamiento de información que es cifrado para mantener la seguridad de los contenidos y la posterior transmisión de los mismos a otros dispositivos para poder manipularlos únicamente en caso de que la autenticación sea correcta y el flujo de datos haya sido transferido completamente. No obstante, conocida la clave de acceso se tiene permiso para usar los datos y manipularlos al tiempo que se permite diseminarlos y ofrecerlos en claro a cualquiera otra persona sin el cifrado previo, vulnerando los derechos de copyright.

El documento US7434067-B1 presenta un comparador de autorizaciones de seguridad impidiendo el acceso indiscriminado y permitiendo el acceso bajo atributos personales. El comparador tiene una puerta trasera que permite el acceso al descifrado y el descifrado propiamente dicho. Pero, el comparador no está expresamente referido a contenidos y no presenta una puerta trasera que permita el acceso a los datos en claro de forma absoluta.

El documento US2008226069-A1 presenta el cifrado de datos obtenidos por dispositivos de entrada, como un teclado o cualquier otro medio similar, siendo capaz de descifrarlos mediante funciones de un módulo de procesado. No obstante, no ofrece una cuantificación de la dificultad de descifrado ni está orientado a cantidades elevadas de información de datos. En el documento US2008226069-A1 se cifran contenidos pero es posible descifrarlos de manera que pueden ser manipulados y diseminados sin control rompiendo los derechos de autoría de los mismos, aspecto que debería ser controlado.

Era por tanto deseable un sistema de ralentización de la tasa de transferencia de un dispositivo que permitiera ejercer un cierto control sobre el tiempo requerido en descifrar una información.

DESCRIPCIÓN DE LA INVENCIÓN

La invención presenta un sistema de ralentización de la tasa de transferencia de un dispositivo por método criptográfico basado en el control del tiempo de descifrado de la información. El método comprende las siguientes etapas:

1. Seleccionar el cifrado a usar:

Elección de un método de cifrado para cifrar la información en claro. El cifrado se puede seleccionar entre cifrado simétrico DES, T-DES, AES, etc. y asimétrico RSA, ElGamal, Curva Elíptica, etc.

2. Cifrar la información:

La ralentización se fijará en función de la seguridad que se quiera atribuir al documento cifrado, a la mayor o menor confidencialidad que se le quiera atribuir, y a la disposición o no disposición inmediata que se quiera conceder del mismo. Con este fin, el método aplica una dificultad de descifrado variable que se traducirá en una variación del tiempo necesario en el descifrado. Por su naturaleza, los cifrados simétricos serán más rápidos que los asimétricos.

En la etapa de cifrado, en primer lugar se convertirá el documento de información en una cadena de caracteres numéricos (binario, decimal, etc.). Si el documento es de audio o de video se puede pasar directamente a una cadena de caracteres binaria, si es un documento de texto, se puede pasar cada carácter a su carácter ASCII correspondiente, o utilizar cualquier otro sistema de conversión, y por ejemplo, pasar la cadena de caracteres a una cadena de caracteres binarios.

Para el cifrado, el documento se divide en bloques de k caracteres para cifrar cada bloque según el cifrado elegido en la etapa anterior. Una vez cifrado cada uno de los bloques éstos formarán, en conjunto, el texto cifrado.

3. Generar una pluralidad de claves:

Esta etapa es la que caracteriza el ralentizador propuesto, en ella, se genera aleatoriamente una pluralidad de claves. Si la clave de descifrado es k_j, el método generaría aleatoriamente una pluralidad de claves que junto con k_j, se entregaría al destinatario. Así la entrega consistirá en $\{k_1, k_2, ...\&_j, ...\&_{s-1}, k_s\}$. La cantidad de claves ofrecidas hará que en media -cuando "s" tiende a infinito- el destinatario tenga que

probar aproximadamente la mitad del número de claves entregadas para descifrar el documento. Por ello, para aumentar mil veces el tiempo de descifrado, el método ha de construir aleatoriamente una pluralidad de dos mil claves.

Por tanto, el método de ralentización de la tasa de transferencia de un dispositivo por método criptográfico comprende:

- seleccionar un tipo de cifrado;
- cifrar información según el tipo de cifrado seleccionado, comprendiendo: convertir la información a cifrar en una cadena de caracteres numéricos, dividir la cadena de caracteres en bloques de un número variable de caracteres y cifrar cada uno de los bloques según el tipo de cifrado seleccionado en la etapa anterior;
- generar aleatoriamente una pluralidad de claves;
- distribuir un conjunto de claves a cada destinatario, cada conjunto formado por un número variable de claves que comprende la clave de descifrado.

Preferentemente, la selección de un tipo de cifrado comprenderá la selección alternativa entre:

- cifrado simétrico, comprendiendo: DES, T-DES, AES;
- cifrado asimétrico, comprendiendo: RSA, ElGamal, Curva Elíptica.

El dispositivo que implementa el método anterior comprende:

- unos medios de procesamiento configurados para:
  - seleccionar un tipo de cifrado;
  - cifrar información según el tipo de cifrado seleccionado, comprendiendo: convertir la información a cifrar en una cadena de caracteres numéricos, dividir la cadena de caracteres en bloques de un número variable de caracteres y cifrar cada uno de los bloques según el tipo de cifrado seleccionado;
  - generar aleatoriamente una pluralidad de claves;
- una memoria que almacena la pluralidad de claves generadas, la información cifrada y las operaciones y variables intermedias realizadas por los medios de procesamiento;
- unos medios de entrada y salida configurados para recibir y enviar información del exterior para realizar las tareas de cifrado.

Preferentemente, los medios de procesamiento seleccionarán alternativamente el tipo de cifrado entre:

- cifrado simétrico, comprendiendo: DES, T-DES, AES;
- cifrado asimétrico, comprendiendo: RSA, ElGamal, Curva Elíptica.

Debido a que el sometimiento a un distinto procesador convierte en diferente la velocidad de descifrado se hace necesario que el dispositivo tenga empotrado un procesador conocido en base al cual se haga el descifrado. Esto permite controlar el tiempo de ofrecimiento de la información interna, ya que el tiempo de descifrado viene dada por la capacidad del procesador.

Debido a que el documento cifrado pudiera tener una mayor o menor necesidad de ser ralentizado se aplica sobre él el método anterior. Cuando se desconoce la clave de descifrado, la única forma habitual de conseguir el texto en claro es probar una por una todas las claves posibles. Esto suele llevar tanto tiempo que hace inviable esta opción. Por lo tanto, situarse en el punto intermedio entre la fuerza bruta (probar todas las posibles claves) y el conocimiento de la clave (probar una sola clave), permite ralentizar el descifrado ya que se ofrece un conjunto de claves entre las cuales está la correcta. Cuantas más claves se ofrezcan, más difícil será resolver el descifrado.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

A continuación, para facilitar la comprensión de la invención, a modo ilustrativo pero no limitativo se describirá una realización de la invención que hace referencia a una figura.

La **figura 1** representa el dispositivo de ralentización de tasa de transferencia de datos por cifrado.

DESCRIPCIÓN DETALLADA DE UN MODO DE REALIZACIÓN

A continuación se detalla un modo de realización del sistema que se pretende patentar.

1. Seleccionar el cifrado a usar.

Cifrado RSA

El cifrado RSA es el método de cifrar que se usará en la realización preferente de la invención. El Algoritmo RSA, propuesto en 1978 debe su nombre a las iniciales de los apellidos de sus inventores Ron Rivest, Adi Shamir y Leonard Adleman, se basa

en la dificultad computacional de obtener los factores primos de números muy elevados. Es fácil buscar primos elevados y posteriormente multiplicarlos para crear un número mayor, pero partir de un número elevado y buscar sus factores primos es una operación sumamente compleja.

Especificaciones iniciales

Para hacer uso de este Algoritmo han de definirse una serie de estructuras. La siguiente tabla indica los pasos que han de realizarse y la forma en la que deben tratarse los elementos involucrados en los mismos, pudiendo ser dichos elementos secretos o no secretos. Los elementos secretos no deben darse a conocer, mientras que los no secretos serán públicos y deberán ofrecerse a quien los pida o precise.

1.	Dos números primos “p” y “q”	Secreto
2.	r = p*q	No Secreto
3.	$\phi(r)$ =(p-1)*(q-1)	Secreto
4.	SK (Secret Key) es la Clave Privada	Secreto
5.	PK (Public Key) es la Clave Pública	No Secreto
6.	X es el mensaje a transmitir o Plaintext	Secreto
7.	Y es el mensaje cifrado	No Secreto

El paso 3 es fácilmente deducible de la definición de la función de Euler dada la generación de "r" como producto de dos primos.

La fórmula general de dicha función es:

$$<i>(r) = r \times (1 - \frac{1}{p_1}) \times (1 - \frac{1}{p_2}) \times \ldots \times (1 - \frac{1}{p_n})$$

donde $p_1, p_2, p_3, \ldots, p_n$ son los factores primos de "r".

Esta función phi de Euler sobre "n", también llamada Indicador de Euler, ofrece como resultado el número de primos relativos que tiene "n" menores que él mismo. Así, por ejemplo, $\phi(20)=8$, ya que 20 se descompone en dos factores primos, el 2 y el 5, el primero elevado a 2, y el segundo elevado a la unidad. Son por lo tanto los siguientes los primos relativos con 20 menores que él mismo: 1, 3, 7, 9, 11, 13, 17, 19.

Las claves pública y privada presentan una fuerte relación entre ellas. Para obtener esta relación entre SK y PK se hace una extensión del Teorema de Euler:

$S\backslash a \equiv bmodr$, esto significa que para todo exponente "m", $a^m \equiv b^m \mathrm{modr}$. Esto lleva a que la fórmula de Euler, $a^{\phi(r)} \equiv \mathrm{lmodr}$ puede ser reescrita como:

$$a \rightarrow (r) \equiv I \ mod \ r$$

donde "a" es primo relativo con "r".

Además, como $a \equiv bmodr$, entonces $axc \equiv bxcmodr$, para todo elemento "c" perteneciente a los enteros.

Usando ambos resultados se puede inferir:

$$X^{m\times\phi(r)+1} \equiv X \bmod r$$

donde el texto plano X (plaintext) es primo relativo con "r" -una restricción que a continuación se indicará cómo eliminar-.

La relación entre las claves pública y privada, PK, SK, es la siguiente.

Habrán de cumplir la relación $SK \times PK \equiv m\times\phi\{r) + 1$, lo que se puede expresar de la siguiente manera:

$$SK. \ Y.PK = \backslash \bmod \phi(r)$$

Pudiendo expresar la anterior relación como:

$$X^{SKxPK} \equiv X \bmod r$$

Cifrado y descifrado

Notando por las usuales mayúsculas inglesas de encipherment y decipherment, 'E " y "D" respectivamente, y ofreciendo en los subíndices la clave a usar, se puede expresar de manera compacta el cifrado y el descifrado del Algoritmo RSA como:

Cifrado: $E_{PK}(X) = Y \equiv X^{PK} \bmod r$

Descifrado: $D_{SK}(Y) \equiv Y^{SK} \bmod r \equiv X^{PK\times SK} \bmod r \equiv X \bmod r$

Como estas operaciones de cifrado y descifrado son conmutativas, -la razón reside en que SK*PK=PK*SK- se sigue que cifrar texto descifrado es igual que descifrar texto cifrado:

$$D_{SK}\{E_{PK}(\mathrm{X})) = E_{PK}\{D_{SK}(\mathrm{X})) \equiv X \bmod \boldsymbol{r}$$

Mejorando el Algoritmo

Hay una serie de aspectos que han de seguir considerándose, porque lo que pareciera un Algoritmo simple, encierra en su interior una serie de aspectos profundos y complejos que no pueden dejarse soslayados, de forma, que se contemplarán a continuación.

Se sabe que $X^{FK} \bmod r = (X + mxr)^{PK}$ **modr** para todo entero "m", y cualquier texto plano X, resultando que X, X+r, X+2r,X+576r,... ofrecen el mismo texto cifrado. Es decir, la función es una función tal que muchos elementos -infinitos- del conjunto inicial ofrecen una misma imagen en el conjunto final. Para restringir estas posibilidades a una función uno a uno, se deberá restringir el texto X al conjunto {0, 1, 2,.... r-1}. Esto conlleva la aplicación, tal y como se expresado previamente, de las fórmulas de cifrado y descifrado de manera biyectiva, uno contra uno.

Se ha comprobado que la realización de una serie de pautas, en el uso del Algoritmo RSA, lo hace difícil de romper, además de capacitarlo para que funcione correctamente.

a) La elección de números primos:

Han de seleccionarse dos números primos, "p" y "q", distintos entre sí. El producto r=p*q se hace público, pero ambos números primos han de permanecer en secreto, o bien eliminarse sus rastros, es decir, que sean desconocidos para cualquier persona, incluida la parte cifrante.

Los inventores del Algoritmo recomiendan como protección adicional una serie de elecciones adicionales:

1. "p" y "q" han de diferir en unos pocos dígitos, aunque sin ser demasiado cercanos.
2. Tanto (p-1) como (q-1) han de contener factores primos grandes, p' y q', respectivamente.
3. El mcd[(p-1),(q-1)] ha de ser pequeño.
4. Que (p'-1) y (q'-1) tengan factores primos grandes, p" y q" respectivamente.

b) La elección de claves:

Se ha de cumplir que $SKxPK \equiv$ **lmod^(r) ,** es decir, que el producto de la clave privada y la pública sea primo relativo con la función phi de Euler.

Además ha de ser fácil computar SK y PK. A continuación se indica cómo satisfacer estos requerimientos.

Sea d=mcd(a,n), el máximo común divisor de dos números "a" y "n". La congruencia $aX \equiv b \bmod n$ puede ser resuelta, es decir, puede encontrarse un "X" entero que la satisfaga sólo si el mcd(a,n) divide a "b". Sin entrar en la demostración de este teorema, lo que se pretende es que el mcd(a,n) divida a b. Si ese mcd(a,n)=1 , siempre ocurre que 1 dividirá a b. Luego se buscará que mcd(a,n) sea 1.

Si se hace que las dos ecuaciones d=mcd(a,n) y $aX \equiv b \bmod n$, sean en realidad 1=mcd(SK, $\phi(r)$) y $SK \times PK \equiv 1 \bmod \phi(r)$. Para lograr lo que se busca, que es que la congruencia $SK \times PK \equiv 1 \bmod \phi(r)$ se pueda resolver, es simplemente buscar en realidad que 1=mcd(SK , $\phi(r)$).

El mcd(SK , $\phi(r)$)=1 cuando SK y $\phi(r)$ no tienen factores comunes, es decir son primos relativos entre ellos.

Haciendo uso del Algoritmo de Euclides es posible encontrar un método adecuado para conocer primos relativos de un número dado, pudiendo encontrar a partir de SK el valor de PK, y viceversa, lo que completaría el algoritmo de búsqueda de las claves privada (SK) y pública (PK).

2. Cifrar la documentación:

Para cifrar un mensaje éste ha de dividirse previamente en bloques tales que no excedan el valor r-1 . De otra manera, se obtendrían funciones ambiguas al permitir representaciones diversas. Una manera de codificar un texto literario es transformando cada letra a un código numérico, ASCII, ANSI, o cualquier otro. Suponiendo A=01 , B=02,...Z=27 (incluyendo la letra Ñ como propia del alfabeto de estudio). Además podrían asignarse valores a otros signos diversos y quizás necesarios como ,)(¿!@/;.-_{}g+*~z©...por lo que se debería buscar una asignación adecuada entre cada signo y un número. Sin embargo, como ejemplo se mantendrá esta codificación, por simplicidad.

Si el mensaje es "En un lugar de la Mancha, de cuyo nombre no quiero acordarme", tras ponerlo en mayúsculas y quitar las tildes y los espacios en blanco y las comas, podría escribirse como:

[051 4221 4 12220701 1904051 201 1301 14030801 04050322261 6 14 16 13021 9051 4 16 18 2209051 9 1601 031 6 190401 19 1305].

Se eligen ahora los valores del Algoritmo. Por ejemplo, p=1 00003 y q= 1200007. El resultado de r=p*q= 120004300021 .

Se fracciona el texto a cifrar de manera que no exceda el valor r-1 , o sea, 120004300020. Para cumplir con esta especificación se va a dividir el texto en los siguientes bloques de 8 dígitos:

[05142214,12220701 ,19040512,01 1301 14,03080104,05032226,16141613,02190514, 16182209,05191601 ,03161904,01 191305]

Suponiendo que SK es 60238691 159. Para calcular PK, se ha de satisfacer

$$SK \chi PK \equiv 1 \pmod{\phi(r)}$$

obteniendo un valor de PK= 671627.

A continuación, se cifran todos los elementos del texto plano, elevando cada uno de ellos a la potencia PK y calculando el valor módulo r.

Esto nos da los siguientes valores:

$$E_{PK}(X) = Y \equiv X^{PK} \bmod r$$

[83071342073,1 1341992260,92701932291 ,33584471 135,80369499959,24635225570 ,45048183052,48263380423,74143246285,1 17149080760,78437239131 ,2056963927 2], lo que configura el texto cifrado.

El proceso de descifrado consiste en tomar cada uno de los bloques cifrados, y elevarlos a SK para posteriormente sacar su resultado modular sobre r.

$$D_{SK}(Y) \equiv Y^{SK} \bmod r \equiv X^{PK \times SK} \bmod r \equiv X \bmod r$$

Aplicando estas operaciones se obtienen los valores:

[05142214,12220701 ,19040512,01 1301 14,03080104,05032226,16141613,02190514, 16182209,05191601 ,03161904,01 191305]

Si a continuación se pone cada uno de los pares de dígitos en valor literal, según el patrón A=01 , B=02,...Z=27, se obtiene el texto -tras insertar los espacios en blanco- original: "En un lugar de la Mancha, de cuyo nombre no quiero acordarme".

Sin embargo, en esta fase sólo se cifra el mensaje, no haciendo la fase descifrado. Sólo se construye el texto cifrado:

[83071342073,1 1341992260,92701932291 ,33584471 135,80369499959,24635225570 ,45048183052,48263380423,74143246285,1 17149080760,78437239131 ,2056963927 2]

3. Generar una pluralidad de claves: Rompiendo el algoritmo por fuerza bruta

Intentar romper el algoritmo de cifrado RSA por fuerza bruta supone que se divide el texto cifrado,

[83071342073,1 1341992260,92701932291 ,33584471 135,80369499959,24635225570 ,45048183052,48263380423,74143246285,1 17149080760,78437239131 ,2056963927 2]

y se intenta recuperar el texto original en claro sabiendo sólo lo que es público, que es el valor de r y de PK. Como se desconoce SK, hay que probar todos los números j desde 1 hasta r hasta encontrar el valor que tomando un fragmento cualquiera de texto cifrado, y elevado a ese valor j módulo r dé un número que puesto en letras ofrezca una sentencia coherente en un lenguaje. Debido a la enorme cantidad de valores en juego, el tiempo preciso para realizar esta operación es imposible de contemplar. Esto es un ataque de fuerza bruta.

Descifrado por ralentización

El método aquí propuesto está a medio camino entre la fuerza bruta y el conocimiento de la clave SK. En este caso al usuario se le da un conjunto de claves, generadas aleatoriamente incluyendo la correcta, por ejemplo el conjunto: {1947284219, 60238691 159, 81732781 1}. La elección de la extensión del mazo de llaves o claves dará el tiempo medio de obtención del texto en claro, por lo que se controla el descifrado del texto.

Por cada uno de estos valores SK_j, los resultados obtenidos sobre el primer y el segundo bloque del texto cifrado son los siguientes: 83071342073 y 11341992260.

Para 194728421 9, se obtiene: [39588400026, 118687772076]. No puede ser porque la primera letra no existe, "39" está fuera del abecedario.

Para 60238691 159, se obtiene: [05142214,12220701]: ENUNLUGA

Para 81732781 1, se obtiene: [68908968738,1831 1139167]: No puede ser porque la primera letra no existe, "68" está fuera del abecedario.

Con este manojo de claves queda claro que la SK es 60238691 159, ya que siempre se obtienen letras, y con un cierto sentido semántico, por lo que se aplicaría esta clave SK sobre todo el texto cifrado para obtener todo el texto completo en claro.

El resultado final es que se ha tardado tres veces más en descifrar el texto que si únicamente se dispusiera de una sola clave, la correcta. En general, lo que se suele

dar es una cantidad de claves mayor, por ejemplo 10.000, lo que hace que en media la clave correcta esté en torno a la mitad, en torno a la 5.000, de ahí que cuando se haya probado 5.000 posiblemente se haya dado con la correcta.

La posibilidad de este ralentizador estriba en suponer por ejemplo un archivo donde se sitúen varios documentos de texto, o de audio, o video, y cada uno de ellos con cierta confidencialidad mayor o menor, lo que significará que el descifrado será más lento o más rápido. Así si por ejemplo, si se tuvieran 3 documentos, uno de valor muy confidencial, otro de medio y otro de bajo, se aplicaría para cada documento una tasa de ralentización, por ejemplo de 10.000 claves para el más confidencial, de 3.000 claves para el medio, y de 100 claves para el de menor confidencialidad. Esto supondría que la documentación más sensible sería la más difícil de manejar y de disponer, siendo la menos importante en cuanto a seguridad la que más fácil va a ser descifrada.

Así, si el documento consistente en cifrar y ralentizar fuera el primer capítulo de un libro, en concreto de "El Quijote", que empieza por "En un lugar de la Mancha...", y acaba en "vino a llamarla Dulcinea del Toboso, porque era natural del Toboso, nombre a su parecer músico y peregrino y significativo, como todos los demás que a él y a sus cosas había puesto", tiene un total de 8202 caracteres. Si se dividen en bloques de 4 letras, se obtendrán 2051 bloques, el último de los cuales sólo tendrá dos letras. Aplicando un cifrado normal, el tiempo que tarda dicha ejecución en descifrarse supone en un procesador Intel(R) Core(TM)2 CPU T5600 @ 1.83Ghz de 2.1 12,52 segundos, es decir, unos 35 minutos. Si se deseara que durara más el proceso se ofrecería un mayor número de claves. Si la cantidad de claves que se dieran fuera de {6162761 1,992991 12,76764913,8723618246,7624551234,89746841634,72364273,82 3748 1273,3248846423,34234234,234235454, 12098984823,34245,3424 1241 2,46464 6456,34242423523,656457567,878768769,989775565,891818913,83578774734,487 8742374723,3434134,87873858179,3478783478,4387865324,31573894783,3489463 24,12347893784,234782844,347878341 ,34783743343,24134512532,3423424234,34 1353515,1356436,6564564345,3454324234,234242412,43534534534,4543453,7687 967657, 194728421 9,938758234,20930353,1 02933391 1,198001 001 ,8989781 172,602 38691 159, 81732781 1,6651829934}, y cada una de ellas se probaran en este orden, al llegar a la 49° se resolvería el descifrado, lo que supone un tiempo de 108497,34 en nuestro dispositivo, es decir, algo más de 30 horas para poder disponer del primer capítulo de la novela "El Quijote".

La forma de aplicar industrialmente el sistema descrito se desprende de la propia descripción del mismo. No obstante se destaca como más relevante su aplicabilidad en la industria relacionada con los servicios de seguridad informáticos, financieros, gubernamentales, policiales y, en general en la industria relacionada con todas aquellas áreas o servicios que requieran el bloqueo de información que de partida sea disponible de manera indiscriminada. Se trata de hacer que la disponibilidad de la información esté controlada en tiempo, y si ya lo estuviera, que no esté disponible hasta que el tiempo de descifrado se haya cumplido, un tiempo que es controlado previamente.

Este control de tiempos y recursos en la disponibilidad de la información lo convierten en útil en los procesos de la ingeniería de la información, el control y salvaguarda de datos o la protección de datos, como en los derechos de autor. Así por ejemplo, la manipulación de información por parte de terceras personas pudiera ser tan costosa en tiempo y recursos por ellas que hiciera inviable su disponibilidad, pero fuera más fácil, ligera y menos costosa por el poseedor autorizado, quien poseería un conjunto de claves menor.

Una vez descrita de forma clara la invención, se hace constar que las realizaciones particulares anteriormente descritas son susceptibles de modificaciones de detalle siempre que no alteren el principio fundamental y la esencia de la invención.

REIVINDICACIONES

1.- Método de ralentización de la tasa de transferencia de un dispositivo por método criptográfico que comprende las etapas:

- seleccionar un tipo de cifrado y generar una clave de cifrado conforme al tipo de cifrado seleccionado;
- cifrar un documento de información según el tipo de cifrado seleccionado, comprendiendo esta etapa de cifrado:
  - convertir el documento de información a cifrar en una cadena de caracteres numéricos,
  - dividir la cadena de caracteres en bloques de un número determinado de caracteres; y,
  - cifrar cada uno de los bloques según el tipo de cifrado seleccionado en la etapa anterior haciendo uso de la clave generada;

caracterizado porque adicionalmente comprende las etapas:

- generar aleatoriamente un número de claves distintas a la clave ya generada y conforme al tipo de cifrado seleccionado proporcional al grado de ralentización a proporcionar;
- proveer al destinatario del documento cifrado y de un conjunto de claves, este conjunto de claves comprendiendo las claves generadas aleatoriamente en la etapa anterior y la clave de descifrado conforme al tipo de cifrado seleccionado en la primera etapa; y, esta clave situada en una posición cualquiera entre las claves generadas aleatoriamente.

2.- Método de ralentización de la tasa de transferencia de un dispositivo por método criptográfico, según la reivindicación anterior; caracterizado porque la selección de un tipo de cifrado comprende la selección alternativa entre:

- cifrado simétrico, comprendiendo: DES, T-DES, AES;
- cifrado asimétrico, comprendiendo: RSA, ElGamal, Curva Elíptica.

3.- Sistema de ralentización de la tasa de transferencia de un dispositivo por método criptográfico caracterizado porque comprende:

- unos medios de procesamiento (1):
  - configurados para seleccionar un tipo de cifrado y generar una clave de cifrado conforme al tipo de cifrado seleccionado;

- configurados para cifrar un documento de información según el tipo de cifrado seleccionado, comprendiendo esta etapa de cifrado:
  - convertir el documento de información a cifrar en una cadena de caracteres numéricos,
  - dividir la cadena de caracteres en bloques de un número determinado de caracteres; y,
  - cifrar cada uno de los bloques según el tipo de cifrado seleccionado en la etapa anterior haciendo uso de la clave generada;
- configurados para generar aleatoriamente un número de claves distintas a la clave ya generada y conforme al tipo de cifrado seleccionado proporcional al grado de ralentización a proporcionar;

- una memoria (2) adaptada para almacenar la pluralidad de claves generadas, el documento de información cifrada y las operaciones y variables intermedias realizadas por los medios de procesamiento;
- unos medios de entrada y salida (3) configurados para recibir y enviar información del exterior para realizar las tareas de cifrado.

4.- Sistema de ralentización de la tasa de transferencia de un dispositivo por método criptográfico, según la reivindicación 3, caracterizado porque los medios de procesamiento (1) seleccionan alternativamente el tipo de cifrado entre:

- cifrado simétrico, comprendiendo: DES, T-DES, AES;
- cifrado asimétrico, comprendiendo: RSA, ElGamal, Curva Elíptica.

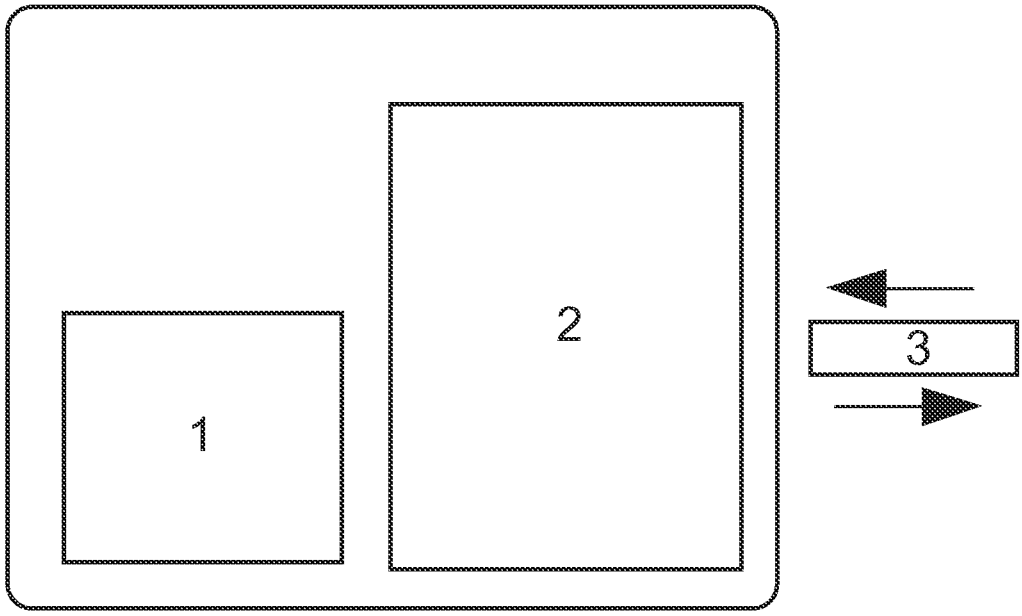

FIG. 1

INFORME DE BÚSQUEDA INTERNACIONAL

Solicitud internacional Nº

PCT/ES2011/070898

A. CLASIFICACIÓN DEL OBJETO DE LA SOLICITUD INV. G06F21/00
ADD.

De acuerdo con la Clasificación Internacional de Patentes (CIP) o según la clasificación nacional y CIP.

B. SECTORES COMPRENDIDOS POR LA BÚSQUEDA

Documentación mínima buscada (sistema de clasificación seguido de los símbolos de clasificación)

G06F

Otra documentación consultada, además de la documentación mínima, en la medida en que tales documentos formen parte de los sectores comprendidos por la búsqueda

Bases de datos electrónicas consultadas durante la búsqueda internacional (nombre de la base de datos y, si es posible, términos de búsqueda utilizados) EPQ-InternaI

C. DOCUMENTOS CONSIDERADOS RELEVANTES

Categoría*	Documentos citados, con indicación, si procede, de las partes relevantes	Relevante para las reivindicaciones N°
X	**Rivest R L et Al: "Rompecabezas Bloqueo hora y Programado Reléase Crypto ", CITACIÓN DE INTERNET, 21 de febrero 1996 (02/21/1996), XP002326370, Obtenido de la Internet: URL: http://www.es. berkeley.edu/~ daw /documentos / timelock.ps [consultado el 27/04/2005] página 3, líneas 6-25** --- - / -	**1-4**

☒ En la continuación del Recuadro C se relacionan otros documentos

☐ Los documentos de familias de patentes se indican en el Anexo

* Categorías especiales de documentos citados:

"A" documento que define el estado general de la técnica no considerado como particularmente relevante.

"E" solicitud de patente o patente anterior pero publicada en la fecha de presentación internacional o en fecha posterior.

"L" documento que puede plantear dudas sobre una reivindicación de prioridad o que se cita para determinar la fecha de publicación de otra cita o por una razón especial (como la indicada).

"O" documento que se refiere a una divulgación oral, a una utilización, a una exposición o a cualquier otro medio.

"P" documento publicado antes de la fecha de presentación internacional pero con posterioridad a la fecha de prioridad reivindicada.

"T" documento ulterior publicado con posterioridad a la fecha de presentación internacional o de prioridad que no pertenece al estado de la técnica pertinente pero que se cita por permitir la comprensión del principio o teoría que constituye la base de la invención.

"X" documento particularmente relevante; la invención reivindicada no puede considerarse nueva o que implique una actividad inventiva por referencia al documento aisladamente considerado.

"Y" documento particularmente relevante; la invención reivindicada no puede considerarse que implique una actividad inventiva cuando el documento se asocia a otro u otros documentos de la misma naturaleza, cuya combinación resulta evidente para un experto en la materia.

"&" documento que forma parte de la misma familia de patentes.

Fecha en que se ha concluido efectivamente la búsqueda internacional	Fecha de expedición del informe de búsqueda internacional
04 Mayo 2012	**24/05/2012**
Nombre y dirección postal de la Administración encargada de la búsqueda internacional European Patent Office P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016 N° de fax	Funcionario autorizado Mezbdi , Stephan N° de teléfono

INFORME DE BÚSQUEDA INTERNACIONAL

Solicitud internacional Nº

PCT/ES2011/070898

C (continuación). DOCUMENTOS CONSIDERADOS RELEVANTES

Categoría*	Documentos citados, con indicación, si procede, de las partes relevantes	Relevante para las reivindicaciones N°
A	various : "Proof-of-work system" , Wikipedia , **08 de diciembre 2010 (12/08/2010), XP002675282, Obtenido de la Internet:** URL: http://en .wikipedia.org/w/index.php?title=Proof-of-work_system&oldid=401209791 [retrieved on 2012-05-03] **todo el documento**	1-4

A	WO 2008/121639 Al (SANDISK CORP [US] ; J0GAND-C0UL0MB FABRICE [US]) **9 octubre 2008 (09/10/2008)** **resumen**	1-4
A	US 2004/250065 Al (BR0WNING JAMES V [US]) **9 de 2004 (09/12/2004) Diciembre** **resumen**	1-4

A	EP 1 357 455 A2 (MICROSOFT CORP [US]) **29 de octubre 2003 (29/10/2003)** **Resumen , la figura 13**	1-4

WO 2008121639	A1	09-10-2008	EP	2132677	A1	16-12-2009
			EP	2434425	A1	28-03-2012
			EP	2434426	A1	28-03-2012
			JP	2010527465	A	12-08-2010
			KR	20100014767	A	11-02-2010
			TW	200903295	A	16-01-2009
			WO	2008121639	A1	09-10-2008
US 2004250065	A1	09-12-2004	JP	2004348731	A	09-12-2004
			US	2004250065	A1	09-12-2004
EP 1357455	A2	29-10-2003	EP	1357455	A2	29-10-2003
			JP	4615832	B2	19-01-2011
			JP	2004040772	A	05-02-2004
			NO	20031645	A	17-10-2003
			US	2003195855	A1	16-10-2003

INTERNATIONAL SEARCH REPORT

International application No
PCT/ES2011/070898

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/00
ADD.

According to International Patent Classification (IPC) orto both national classification and IPC

B. FIELDS SEARCHED

Mínimum documentation searched (classification system followed by classification symbols)
G06F

Documentation searched other than mínimum documentation to the extent that such documents are ¡ncluded ¡n the fíelds searched

Electronic data base consulted during the international search (ñame of data base and, where practicable, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	RIVEST R L ET AL: "Time Lock Puzzl es and Timed Rel éase Crypto" , INTERNET CITATION, 21 February 1996 (1996-02-21) , XP002326370, Retri eved from the Internet: URL: http://www. cs.berkel ey.edu/ ~daw/papers /timel ock.ps [retri eved on 2005-04-27] page 3, l i nes 6-25	1-4

-/- ·

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which ¡s not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" documentwhich may throw doubts on priority claim(s) orwhich ¡s 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 principie ortheory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considerad novel or cannot be considerad to involve an inventive step when the document ¡s taken alone

"Y" document of particular relevance; the claimed invention cannot be considerad to involve an inventive step when the document ¡s 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
4 May 2012	24/05/2012

Ñame and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Mezbdi , Stephan

INTERNATIONAL SEARCH REPORT

International application No
PCT/ES2011/070898

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to olaim No.
A	vari ous : "Proof-of-work system" , wi ki pedi a , 8 December 2010 (2010-12-08) , XP002675282 , Retri eved from the Internet: URL: http://en .wi ki pedi a.org/w/i ndex.php?ti t i e=Proof -of -work_system&ol di d=401209791 [retri eved on 2012-05-03] the whol e document	1-4
A	W0 2008/121639 Al (SANDISK CORP [US] ; J0GAND-C0UL0MB FABRICE [US]) 9 October 2008 (2008-10-09) abstract	1-4
A	US 2004/250065 Al (BROWNING JAMES V [US]) 9 December 2004 (2004-12-09) abstract	1-4
A	EP 1 357 455 A2 (MICROSOFT CORP [US]) 29 October 2003 (2003-10-29) abstract; f i gure 13	1-4

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/ES2011/070898

Patent document cited in search report	Publioation date	Patent family member(s)	Publioation date
Wo 2008121639 Al	09-10-2008	EP 2132677 Al	16-12-2009
		EP 2434425 Al	28-03-2012
		EP 2434426 Al	28-03-2012
		JP 2010527465 A	12-08-2010
		KR 20100014767 A	11-02-2010
		TW 200903295 A	16-01-2009
		Wo 2008121639 Al	09-10-2008
US 2004250065 Al	09-12-2004	JP 2004348731 A	09-12-2004
		US 2004250065 Al	09-12-2004
EP 1357455 A2	29-10-2003	EP 1357455 A2	29-10-2003
		JP 4615832 B2	19-01-2011
		JP 2004040772 A	05-02-2004
		NO 20031645 A	17-10-2003
		US 2003195855 Al	16-10-2003