(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 359 603**

(51) Int. Cl.:
H04L 9/30 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **08806126 .2**
(96) Fecha de presentación : **30.06.2008**
(97) Número de publicación de la solicitud: **2179535**
(97) Fecha de publicación de la solicitud: **28.04.2010**

(54) Título: **Método asimétrico de cifrado o de verificación de firma.**

(30) Prioridad: **06.07.2007 FR 07 56328**

(45) Fecha de publicación de la mención BOPI:
25.05.2011

(45) Fecha de la publicación del folleto de la patente:
25.05.2011

(73) Titular/es: **FRANCE TELECOM**
6 place d'Alleray
75015 Paris, FR

(72) Inventor/es: **Billet, Olivier;**
Seurin, Yannick y
Patarin, Jacques

(74) Agente: **Lehmann Novo, María Isabel**

DESCRIPCIÓN

Método asimétrico de cifrado o de verificación de firma.

La invención se refiere al campo de la criptografía. Más concretamente, la invención se refiere al cifrado de mensajes y la firma electrónica.

Se conoce, desde hace mucho tiempo, algoritmos de cifrado de mensaje, en particular algoritmos de cifrado por bloques, tales como el DES (iniciales de las palabras inglesas "*Data Encryption Standard*" que significa "Norma de Cifrado de Datos"), que utiliza una clave de 56 bits (actualmente obsoleta), o el "Triple DES" (publicado por la sociedad IBM en 1999) que utiliza tres tales claves, o también AES (iniciales de las palabras inglesas "*Advanced Encryption Standard*" que significa "Norma de Cifrado Avanzado") elegida en octubre de 2000 en Estados Unidos por el NIST *(«National Institute of Standards and Technology»)* que utiliza claves de 128, 192 o 256 bits.

La mayor parte de los algoritmos conocidos son algoritmos *simétricos*, es decir algoritmos tales que la entidad que cifra el mensaje y la entidad que lo descifra compartan una misma clave secreta. Estos algoritmos simétricos tienen, por inconveniente, que la elección de la clave, o la comunicación de la clave de una entidad a la otra, se debe realizar de forma segura para impedir que un intruso tenga conocimiento; considerando la longitud exigida para las claves (al menos 128 bits), las precauciones que ello impone son muy restrictivas.

Por lo tanto, se ha buscado construir algoritmos de cifrado *asimétricos*, es decir algoritmos tales que cualquier entidad que desee enviar un mensaje cifrado a un destinatario determinado puede utilizar una variante pública de este algoritmo, siendo la variante característica del destinatario, pero tal que sólo este destinatario sea capaz de descifrar el mensaje cifrado; se constatará que incluso el emisor del mensaje cifrado, de forma asimétrica, no puede, de forma propiamente dicha, *descifrar* este mensaje cifrado (en el supuesto de que el emisor conozca el mensaje sin cifrar desde el inicio). Al ser el algoritmo de cifrado accesible a todos, no hay ninguna precaución de seguridad a tomar al nivel de entendimiento entre el emisor de un mensaje y su destinatario.

Por otro lado, se hace constar que la mayor parte de los algoritmos *asimétricos* pueden servir tanto para el cifrado como para la firma de mensaje, siendo estos dos protocolos simplemente el inverso uno del otro. Dicho de otro modo, para el cifrado, se cifra con la clave pública y se descifra con la clave secreta, mientras que para la firma, se firma con la clave secreta y se verifica la firma con la clave pública.

En particular, en el caso de los algoritmos asimétricos en donde la clave secreta es un "truco" (tal como, por ejemplo, el algoritmo de "aceite y vinagre desequilibrados" descrito a continuación), la firma electrónica procede de la forma siguiente. En el momento de la firma de una secuencia *C* (que puede ser un condensado de un documento original), el signatario utiliza el mismo algoritmo (secreto) que si esta secuencia *C* fuera un mensaje cifrado que se tratara de descifrar. Se obtiene, así, una "firma" *M*, que se pone a la disposición del público, o de al menos un verificador, al mismo tiempo que el documento original. A continuación, para la verificación de esta firma *M*, el verificador aplica a la secuencia *M* el mismo algoritmo público que si se tratara de cifrar esta secuencia *M*; si la firma es auténtica, el verificador obtiene una secuencia idéntica a la secuencia *C*, es decir, al documento original puesto a su disposición o a su condensado.

El algoritmo asimétrico más conocido es, sin duda, el RSA (para una descripción detallada de RSA, véase el artículo de R.L. Rivest, A. Shamir y L.M. Adleman titulado "*Un método para obtener Firmas Digitales y Criptosistemas de claves públicas*", Communications of the ACM, volumen 21 n° 2, páginas 120 a 126, 1978). Asimismo, se conoce los algoritmos que utilizan curvas elípticas (véase, por ejemplo, el artículo de Neal Koblitz titulado "*Criptosistemas de curvas elípticas*", Mathematics of Computation, volumen n° 48, páginas 203 a 209, 1987, o el artículo de V. Miller titulado "*Uso de Curvas Elípticas en Criptografía*", CRYPTO 85, 1985). Estos algoritmos presentan el inconveniente de necesitar cálculos muy complicados.

En el sistema denominado "aceite y vinagre desequilibrado" dado a conocer por A. Kipnis, J. Patarin, y L. Goubin (véase su artículo titulado "*Sistemas de Firmas de Aceite y Vinagre desequilibrado*", EUROCRYPT 1999, páginas 206 a 222), la clave pública consiste en un sistema de *h* polinomios cuadráticos multivariados con *n* variables x_1 a x_n, con $n > h > 1$, en un cuerpo finito *K*. Estos polinomios son, por lo tanto, de la forma

$$\sum_{1 \le i \le j \le n} \alpha_k^{(ij)} x_i x_j + \sum_{1 \le i \le n} \beta_k^{(i)} x_i + \gamma_k \qquad (1 \le k \le h) ,$$

en donde los coeficientes $\alpha_k^{(ij)}, \beta_k^{(i)}$ y γ_k pertenecen a *K*.

A modo de "clave secreta", este sistema utiliza un "truco". Este truco consiste en mezclar dos tipos de variables, denominadas variables de «aceite» y variables de «vinagre», lo que permite constituir un cierto sistema de *h* ecuaciones cuadráticas multivariadas con $n = v + h$ variables, en donde el entero *v* designa el número de variables de vinagre y el entero *h* designa el número de variables de aceite. Se necesita que $v > h$; además, cada polinomio del sistema comprende todos los monomios posibles, cuyos coeficientes son determinados al azar, excluidos los monomios

constituidos por el producto de dos variables de aceite, que están ausentes. La particularidad de realización del método saca partido de que un sistema lineal aleatorio de *h* ecuaciones y *h* incógnitas presenta una gran probabilidad de tener una solución única. Fijando, de forma aleatoria, el valor de las variables de vinagre, es posible resolver el sistema lineal en las *h* variables de aceite resultante. Si, para una elección aleatoria dada de las variables de vinagre, el sistema resultante no es inversible, basta efectuar otra elección aleatoria de variables de vinagre.

Con el fin de enmascarar esta estructura al público, se aplica, a la entrada del sistema, un cambio de variables inversible de *(v+h)* variables hacia *(v+h)* variables. El sistema así transformado constituye la clave pública, mientras que el cambio de variables y el sistema original constituyen la clave secreta.

Este sistema tiene, por inconveniente, que sólo puede servir de algoritmo de firma, y no de algoritmo de cifrado. Además, es ineficaz debido a la necesidad de añadir a las variables de aceite (directamente asociadas al mensaje a firmar) un gran número de variables suplementarias (las variables de vinagre) en el momento de la firma.

Otros algoritmos asimétricos conocidos, por ejemplo el algoritmo "C*" (véase el artículo de Tsutomu Matsumoto y Hideki Imai titulado "*Public Quadratic Polynomial Tuples for Efficient Signature Verification and Message Encryption*", Eurocrypt'88, páginas 419 a 453) han sido, por sí mismos, eliminados.

La presente invención se refiere, por lo tanto, en primer lugar, un método de descifrado de un mensaje cifrado representado por una secuencia *C* o por una firma electrónica de una secuencia *C*, estando dicha secuencia *C* constituida por datos que pertenecen a un cuerpo finito *K*=GF(*q*), siendo *q*>1, en donde se tratan bloques sucesivos que comprenden cada uno (*n*·*d*) datos sucesivos de la secuencia *C*, en donde *n* y *d* son enteros predeterminados superiores a 1, comprendiendo el tratamiento de un tal bloque las etapas siguientes:

- se aplica una transformación afín inversible predeterminada t^{-1} a dicho bloque,

- el bloque resultante se interpreta como estando formado por *n* elementos sucesivos ($y_1,y_2,\ldots,y_n$) de una extensión E=GF(q^d)del cuerpo *K*,

- se calcula un *n*-uplete ($x_1,x_2,\ldots,x_n$) de elementos del cuerpo *E* resolviendo un sistema *f* de *n* polinomios predeterminados de la forma :

$$y_k = \sum_{1\le i\le j\le n} a_k^{(ij)}\, x_i^{q^{\alpha_i}}\, x_j^{q^{\beta_j}} + \sum_{1\le i\le n} b_k^{i}\, x_i^{q^{\gamma_i}} + c_k \quad (1\le k\le n)$$

en donde los coeficientes $a_k^{(ij)}$, $b_k^{(i)}$ y c_k, pertenecen a *E* y en donde los exponentes α_i, β_j y γ_i son enteros positivos o nulos,

- dicho *n*-uplete ($x_1,x_2,\ldots,x_n$) interpretado como siendo un nuevo bloque formado por (*n*·*d*) elementos sucesivos del cuerpo *K* y

- se aplica una transformación afín inversible predeterminada s^{-1} a dicho nuevo bloque.

De este modo, el método, según la invención, utiliza un procedimiento simplificado basado en:

- el reagrupamiento de los datos del bloque a tratar, que están constituidos por (*n*·*d*) elementos de un cuerpo *K*, por ejemplo bits (caso *q* = *2*) u octetos (caso de *q* = *8*), en *n* secuencias de *d* elementos,

- la identificación de cada una de estas secuencias de *d* elementos de *K* con un elemento único de una extensión (en el sentido de los cuerpos de Galois) *E* de grado *d* de *K* y

- una aplicación de E^n hacia E^n constituida por un sistema secreto *f* de *n* polinomios.

Por otro lado, se elige, como es conocido, dos transformaciones afines inversibles secretas *s* y *t*; estas transformaciones (o sus inversas s^{-1} y t^{-1} , según que se trate del cifrado o del descifrado) se aplican una a la entrada y la otra a la salida, con el fin de enmascarar el ardid operativo a los ojos del público (y, por lo tanto, de un posible intruso). Es conveniente señalar que si el público debe conocer el valor del producto (*n*·*d*) (longitud del bloque a cifrar, por ejemplo), no es necesario hacerle conocer los valores de *n* y *d* por separado.

El algoritmo de descifrado (secreto) pone en práctica el "ardid" operativo antes citado. Por lo tanto, el descifrador debe ser capaz, según la invención, de resolver un sistema de *n* ecuaciones con *n* incógnitas sobre el cuerpo *E*. Ahora bien, se sabe actualmente, en una forma de realización preferida, efectuar esta resolución en un tiempo razonable (salvo que se elija un valor excesivamente grande para *n*), en particular, por medio de los métodos de resolución que utilizan las bases de Gröbner (véase, por ejemplo, el artículo de I.A. Ajwa, Z. Liu, y P.S. Wang titulado "*Gröbner Bases Algorithm*", ICM Technical Reports, Kent State University, Kent, Ohio, USA, febrero 1995). Cada

operación de descifrado implica entonces, en particular, el cálculo de la base de Gröbner asociado al bloque de datos a descifrar .

De forma correlativa, la invención se refiere a, en segundo lugar, un método de cifrado de un mensaje representado por una secuencia *M*, o de verificación de una firma electrónica representada por una secuencia *M*, estando dicha secuencia *M* constituida por datos que pertenecen a un cuerpo finito K=GF(*q*), siendo *q>1*, en donde se trata bloques sucesivos que comprenden cada uno (*n·d*) datos sucesivos de la secuencia *M*, en donde *n* y *d* son enteros predeterminados superiores a 1, comprendiendo la construcción secreta del algoritmo de tratamiento público, de un tal bloque, las etapas siguientes:

- se aplica una transformación afín inversible predeterminada a dicho bloque,

- el bloque resultante se interpreta como estando formado por *n* elementos sucesivos ($x_1,x_2,\ldots,x_n$) de una extensión $E=GF(q^d)$ del cuerpo *K*,

- se calcula un *n*-uplete ($y_1,y_2,\ldots,y_n$) de elementos del cuerpo *E* por medio de un sistema *f* de *n* polinomios predeterminados de la forma :

$$y_k = \sum_{1\le i\le j\le n} a_k^{(ij)} x_i^{q^{\alpha_i}} x_j^{q^{\beta_j}} + \sum_{1\le i\le n} b_k^i \, x_i^{q^{\gamma_i}} + c_k \quad (1 \le k \le n)$$

en donde los coeficientes $\boldsymbol{a_k^{(ij)}}$, $\boldsymbol{b_k^{(i)}}$ y $\boldsymbol{c_k}$, pertenecen a *E* y en donde los exponentes $\boldsymbol{\alpha_i}, \boldsymbol{\beta_j}$ y $\boldsymbol{\gamma_i}$ son enteros positivos o nulos,

- dicho *n*-uplete ($y_1,y_2,\ldots,y_n$)se interpreta como siendo un nuevo bloque formado por (*n·d*) elementos sucesivos del cuerpo *K* y

- se aplica una transformación afín inversible predeterminada *t* a dicho nuevo bloque.

El algoritmo público resultante de la construcción según la invención está, por lo tanto, simplemente constituido por un endomorfismo *g* de K^{nd}, es decir, por la aplicación (polinómica, para ser más preciso) de (*n·d*) elementos de *K* hacia (*n·d*) elementos de *K* resultante de la composición $\boldsymbol{g = t \circ f \circ s.}$. En una forma de realización preferida, si el producto (*n·d*) se selecciona de bastante magnitud (preferentemente, eligiendo un gran valor para *d*), será imposible para un intruso 'destruir' este algoritmo, es decir, descifrar en un tiempo razonable un mensaje cifrado en conformidad con la invención. Además, un tal algoritmo sólo requiere, ventajosamente, una pequeña potencia de cálculo por parte del cifrador o verificador de firma.

La invención se refiere además, en tercer lugar, a un dispositivo de descifrado de un mensaje cifrado representado por una secuencia *C*, o firma electrónica de una secuencia *C*, estando dicha secuencia *C* constituida por datos que pertenecen a un cuerpo finito *K=GF*(*q*), siendo *q>1*, en donde se trata bloques sucesivos, que comprenden cada uno (*n·d*) datos sucesivos de la secuencia *C*, en donde *n* y *d* son enteros predeterminados superiores a 1, comprendiendo dicho dispositivo, con el fin de tratar un tal bloque:

- medios para aplicar una transformación afín inversible predeterminada t^{-1} a dicho bloque,

- medios para interpretar el bloque resultante como estando formado por *n* elementos sucesivos ($y_1,y_2,\ldots,y_n$) de una extensión $E=GFq^d$) del cuerpo *K*,

- medios para calcular un *n*-uplete ($x_1,x_2,\ldots x_n$) de elementos del cuerpo *E* resolviendo un sistema *f* de n polinomios predeterminados de la forma

$$y_k = \sum_{1\le i\le j\le n} a_k^{(ij)} x_i^{q^{\alpha_i}} x_j^{q^{\beta_j}} + \sum_{1\le i\le n} b_k^i \, x_i^{q^{\gamma_i}} + c_k \quad (1 \le k \le n)$$

en donde los coeficientes $\boldsymbol{a_k^{(ij)}}$, $\boldsymbol{b_k^{(i)}}$ y $\boldsymbol{c_k}$, pertenecen a *E* y en donde los exponentes $\boldsymbol{\alpha_i}, \boldsymbol{\beta_j}$ y $\boldsymbol{\gamma_i}$ son enteros positivos o nulos,

- medios para interpretar dicho *n*-uplete ($x_1,x_2,\ldots x_n$) como siendo un nuevo bloque constituido por (*n·d*) elementos sucesivos del cuerpo *K*, y

- medios para aplicar una transformación afín inversible predeterminada s^{-1} a dicho nuevo bloque.

Según características particulares, se podrá realizar uno cualquiera de los dispositivos de descifrado o de firma sucintamente antes expuestos en el contexto de un circuito electrónico. Este circuito electrónico podrá, por ejemplo, estar constituido por un circuito programado o por un circuito integrado de lógica cableada.

La invención se refiere, además, a un medio de almacenamiento de datos inamovible o parcialmente o totalmente amovible, que comprende instrucciones de código de programa informático para la ejecución de las etapas de uno cualquiera de los métodos de cifrado o de descifrado o de firma, o de verificación de firma, sucintamente antes expuestos.

Por último, la invención se refiere, además, a un programa informático telecargable desde una red de comunicación y/o almacenado en un soporte legible por ordenador y/o ejecutable por un microprocesador. Este programa informático es notable porque comprende instrucciones para la ejecución de las etapas de uno cualquiera de los métodos de cifrado o de descifrado, o de firma o de verificación de firma, sucintamente antes expuestos, cuando se ejecuta en un ordenador.

Las ventajas ofrecidas por estos dispositivos, este medio de almacenamiento de datos y este programa informático son esencialmente los mismos que los ofrecidos por los métodos correspondientes.

Otros aspectos y ventajas de la invención parecerán evidentes a partir de la lectura de la descripción detallada siguiente de formas de realización particulares, dadas a título de ejemplos no limitativos.

Se ilustrará, en la presente descripción, el concepto de construcción de una "clave pública" según la invención. Dicho de otro modo, se dará a conocer cómo el detentador de la clave secreta puede construir el algoritmo que se utilizará por el público para tratar un bloque de datos, para los fines de cifrado o de verificación de firma. Es conveniente señalar que la elección de las funciones o valores numéricos en el ejemplo siguiente se basa esencialmente en la simplicidad de lo expuesto y no pretende reflejar valores ventajosos en el plano de una puesta en práctica de la invención.

Se toma como parámetros: $q = 2$ (por lo tanto, $K = GF(2) = \{0,1\}$ es el cuerpo de dos elementos), $d = 2,\ n = 2$, por lo que $n \cdot d = 4$. La extensión de cuerpo $E = GF(4) = \{0,1,\alpha,\beta\}$ se define con la ayuda del polinomio irreductible $X^2 + X + 1$. Se identifica, entonces, los 2-upletes de elementos de *K* con los elementos de *E* (que son, asimismo, polinomios de coeficientes en *K*) de la forma siguiente:

$$(0,0) \leftrightarrow 0 \quad (0,1) \leftrightarrow 1 \quad (1,0) \leftrightarrow \alpha \leftrightarrow X \quad (1,1) \leftrightarrow \beta \leftrightarrow 1 + X \ .$$

Se procede, a continuación, como sigue:

- extracción aleatoria de un sistema *f* de *n* = 2 polinomios con *n* = 2 variables de coeficientes en *E*=*GF*(4). Como se considera el cuerpo de 4 elementos, es inútil estimar las potencias superiores a 3, porque, en este cuerpo, cualquier elemento *X* verifica $X^4=X$. Un ejemplo de un tal sistema es :

$$\begin{cases} Y_1 = X_1 X_2 + \alpha \cdot X_1^2 + \beta \cdot X_2^2 + X_1 + \beta \\ Y_2 = \beta \cdot X_1 X_2 + X_1^2 + X_2^2 + \alpha \cdot X_2 + 1 \end{cases}$$

- extracción aleatoria de dos transformaciones afines inversibles *s* y *t* en K^4, por ejemplo (los tomamos lineales aquí por simplicidad):

$$s = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix} \text{ y } t = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}.$$

Para calcular la clave pública correspondiente, se procede como sigue. Sea (x_1,x_2,x_3,x_4) el texto a cifrar o la firma a verificar. Se calculará las salidas (y_1,y_2,y_3,y_4)en función de los datos (x_1,x_2,x_3,x_4).

Ante todo

$$s(x_1, x_2, x_3, x_4) = (x_1 + x_4, x_1 + x_2 + x_3, x_1 + x_3 + x_4, x_1 + x_3) \ .$$

Para componer por f, es más cómodo interpretar los elementos de E como polinomios de coeficientes en K. De este modo, el par $(x_1 + x_4, x_1 + x_2 + x_3)$ está asociado al polinomio:

$$X_1 = (x_1 + x_4)X + (x_1 + x_2 + x_3) \ .$$

Se puede, entonces, calcular Y_1 e Y_2 efectuando multiplicaciones de polinomios, y reduciendo su módulo $X^2 + X + 1$. Después de algunos cálculos, se obtiene:

$$\begin{aligned} Y_1 &= (x_1x_2 + x_2x_3 + x_2x_4 + x_3x_4 + x_1 + x_2 + x_4 + 1)X + \\ &\quad (x_1x_2 + x_2x_3 + x_1x_3 + x_3x_4 + x_1 + x_2 + x_3 + 1) \\ Y_2 &= (x_1x_2 + x_2x_3 + x_1x_3 + x_3x_4 + x_1 + x_3)X + \\ &\quad (x_1x_3 + x_2x_4 + x_2 + x_3 + x_4 + 1) \ . \end{aligned}$$

Interpretando ello como elementos de K, se obtiene por lo tanto:

$$\begin{aligned} f \circ s(x_1, x_2, x_3, x_4) &= (x_1x_2 + x_2x_3 + x_2x_4 + x_3x_4 + x_1 + x_2 + x_4 + 1, \\ &x_1x_2 + x_2x_3 + x_1x_3 + x_3x_4 + x_1 + x_2 + x_3 + 1, \\ &x_1x_2 + x_2x_3 + x_1x_3 + x_3x_4 + x_1 + x_3, \\ &x_1x_3 + x_2x_4 + x_2 + x_3 + x_4 + 1) \ . \end{aligned}$$

No queda más que aplicar t a este quadruplete para obtener las ecuaciones expresando (y_1,y_2,y_3,y_4) en función de (x_1,x_2,x_3,x_4) se obtiene finalmente:

$$\begin{cases} y_1 = x_1x_2 + x_2 + 1 \\ y_2 = x_1x_2 + x_2x_3 + x_1x_3 + x_3x_4 + x_1 + x_2 + x_3 + 1 \\ y_3 = x_2 + 1 \\ y_4 = x_1x_2 + x_1x_3 + x_2x_3 + x_3x_4 + x_1 + x_3 \ . \end{cases}$$

Como se indicó anteriormente, la presente invención se refiere, además, a un sistema informático que pone en práctica uno cualquiera de los métodos de cifrado o de descifrado, o de firma o de verificación de firma, anteriormente descritos. Este sistema informático comprende, de forma clásica, una unidad central de proceso, que controla, mediante señales, una memoria, así como una unidad de entrada y una unidad de salida.

Además, este sistema informático se puede utilizar para ejecutar un programa informático que contiene instrucciones para la puesta en práctica del método de cifrado o de descifrado, o de firma o de verificación de firma, según la invención.

En efecto, la invención se refiere, además, a un programa informático telecargable, desde una red de comunicación, que comprende instrucciones para la ejecución de las etapas de un método de cifrado o de descifrado, o de firma o de verificación de firma, según la invención, cuando se ejecuta en un ordenador. Este programa informático se puede almacenar en un soporte legible por ordenador y puede ser ejecutable por un microprocesador.

Este programa puede utilizar cualquier lenguaje de programación, y estar bajo la forma de código fuente, código objeto, o de código intermedio entre código fuente y código objeto, tal como en una forma parcialmente compilada o en cualquier otra forma deseable.

La invención se refiere, además, a informaciones legibles por ordenador y que comprende instrucciones de un

programa informático, tal como fue antes descrito.

El soporte de informaciones puede ser cualquier entidad o dispositivo capaz de almacenar el programa. Por ejemplo, el soporte puede comprender un medio de almacenamiento, tal como una memoria ROM, por ejemplo un CD-ROM o una ROM de circuito microelectrónico o también un medio de registro magnético, por ejemplo un disquete ("*floppy disc*" en inglés) o un disco duro.

De otra parte, el soporte de informaciones puede ser un soporte transmisible, tal como una señal eléctrica u óptica, que se puede encaminar a través de un cable eléctrico u óptico, por radio o por otros medios. El programa, según la invención, puede ser, en particular telecargado en una red de tipo Internet.

Como variante, el soporte de informaciones puede ser un circuito integrado en donde está incorporado el programa, estando el circuito adaptado para ejecutar o para utilizarse en la ejecución de una cualquiera de los métodos según la invención.

REIVINDICACIONES

1.- Un método de descifrado de un mensaje cifrado representado por una secuencia *C*, o de firma electrónica de una secuencia *C*, estando dicha secuencia *C* constituida por datos que pertenecen a un cuerpo finito *K*=*GF*(*q*), siendo *q*>1, en donde se trata bloques sucesivos, que comprenden cada uno (*n*·*d*) datos sucesivos de la secuencia *C*, siendo *n* y *d* enteros predeterminados superiores a 1, comprendiendo el tratamiento de un tal bloque las etapas siguientes:

- se aplica una transformación afín inversible predeterminada t^{-1} a dicho bloque,

- el bloque resultante se interpreta como estando formado por *n* elementos sucesivos ($y_1,y_2,\ldots,y_n$) de una extensión $E=GF(q^d)$ del cuerpo *K*,

- se calcula un *n*-uplete ($x_1,x_2,\ldots,x_n$) de elementos del cuerpo *E* resolviendo un sistema *f* de *n* polinomios predeterminados de la forma

$$y_k = \sum_{1\le i\le j\le n} a_k^{(ij)} x_i^{q^{\alpha_i}} x_j^{q^{\beta_j}} + \sum_{1\le i\le n} b_k^{(i)} x_i^{q^{\gamma_i}} + c_k \quad (1 \le k \le n)$$

en donde los coeficientes $a_k^{(ij)}$, $b_k^{(i)}$ y c_k, pertenecen a *E* y en donde los exponentes α_i, β_j y γ_i de los enteros positivos o nulos,

- dicho *n*-uplete ($x_1,x_2,\ldots,x_n$) se interpreta como siendo un nuevo bloque formado por (*n*·*d*) elementos sucesivos del cuerpo *K* y

- se aplica una transformación afín inversible predeterminada s^{-1} a dicho nuevo bloque.

2.- El método de descifrado o de firma electrónica, según la reivindicación 1, caracterizado porque *q* es igual a 2.

3.- Método de descifrado o de firma electrónica según la reivindicación 1, caracterizado porque *q* es igual a 8.

4.- Método de cifrado de un mensaje representado por una secuencia *M*, o verificación de una firma electrónica representada por una secuencia *M*, estando dicha secuencia *M* constituida por datos que pertenecen a un cuerpo finito *K*=*GF*(*q*), siendo *q*>1, en donde se trata bloques sucesivos, comprendiendo cada uno (*n*·*d*) datos sucesivos de la secuencia *M*, en donde *n* y *d* son enteros predeterminados superiores a 1, la construcción secreta del algoritmo de tratamiento público de un tal bloque, que comprende las etapas siguientes:

- se aplica una transformación afín inversible predeterminada a dicho bloque,

- el bloque resultante se interpreta como estando formado por *n* elementos sucesivos ($x_1,x_2,\ldots,x_n$) de una extensión $E=GF(q^d)$ del cuerpo *K*,

- se calcula un *n*-uplete ($y_1,y_2,\ldots,y_n$) de elementos del cuerpo *E* por medio de un sistema *f* de *n* polinomios predeterminados de la forma

$$y_k = \sum_{1\le i\le j\le n} a_k^{(ij)} x_i^{q^{\alpha_i}} x_j^{q^{\beta_j}} + \sum_{1\le i\le n} b_k^{(i)} x_i^{q^{\gamma_i}} + c_k \quad (1 \le k \le n)$$

en donde los coeficientes $a_k^{(ij)}$, $b_k^{(i)}$ y c_k, pertenecen a *E* y en donde los exponentes α_i, β_j y γ_i son enteros positivos o nulos,

- dicho *n*–uplete ($y_1,y_2,\ldots,y_n$) se interpreta como siendo un nuevo bloque constituido por (*n*·*d*) elementos sucesivos del cuerpo *K* y

- se aplica una transformación afín inversible predeterminada *t* a dicho nuevo bloque.

5.- Método de cifrado o de verificación de una firma electrónica según la reivindicación 4, caracterizado porque *q* es igual a 2.

6.- Método de cifrado o de verificación de una firma electrónica, según la reivindicación 4, caracterizado porque *q* es igual a 8.

7. Dispositivo de descifrado de un mensaje cifrado representado por una secuencia *C*, o de firma electrónica de una secuencia *C*, estando dicha secuencia *C* constituida por datos que pertenecen a un cuerpo finito $K=GF(q)$, siendo $q>1$, en donde se trata bloques sucesivos, comprendiendo cada uno $(n \cdot d)$ datos sucesivos de la secuencia *C*, en donde *n* y *d* son enteros predeterminados superiores a 1, comprendiendo dicho dispositivo, con el fin de tratar un tal bloque:

- medios para aplicar una transformación afín inversible predeterminada t^{-1} a dicho bloque,

- medios para interpretar el bloque resultante como estando formado por n elementos sucesivos $(y_1,y_2,\ldots,y_n)$ de una extensión $E=GF(q^d)$ del cuerpo *K*,

- medios para calcular un *n*-uplete $(x_1,x_2,\ldots,x_n)$ de elementos del cuerpo *E* resolviendo un sistema *f* de *n* polinomios predeterminados de la forma

$$y_k = \sum_{1 \le i \le j \le n} a_k^{(ij)} x_i^{q^{\alpha_i}} x_j^{q^{\beta_j}} + \sum_{1 \le i \le n} b_k^{(i)} x_i^{q^{\gamma_i}} + c_k \quad (1 \le k \le n) \Big/ b_K^{(i)}$$

en donde los coeficientes $a_k^{(ij)}$, $b_k^{(i)}$ y c_k, pertenecen a *E* y en donde los exponentes α_i, β_j y γ_i son enteros positivos o nulos,

- medios para interpretar dicho *n*-uplete $(x_1,x_2,\ldots,x_n)$ como siendo un nuevo bloque formado por $(n \cdot d)$ elementos sucesivos del cuerpo *K* y

- medios para aplicar una transformación afín inversible predeterminada s^{-1} a dicho nuevo bloque.

8.- Dispositivo de descifrado o de firma electrónica, según la reivindicación 7, caracterizado porque *q* es igual a 2.

9.- Dispositivo de descifrado o de firma electrónica según la reivindicación 7, caracterizado porque *q* es igual a 8.

10.- Circuito electrónico, caracterizado porque comprende un dispositivo de descifrado o firma electrónica, según una cualquiera de las reivindicaciones 7 a 9.

11.- Medio de almacenamiento de datos inamovible, o parcial o totalmente amovible, que presenta instrucciones de código de programa informático para la ejecución de las etapas de un método según una cualquiera de las reivindicaciones 1 a 6.

12.- Programa informático que se puede telecargar desde una red de comunicación y/o almacenar en un soporte legible por ordenador y/o ejecutable por un microprocesador, caracterizado porque comprende instrucciones para la ejecución de las etapas del método de cifrado o de descifrado, o de firma o de verificación de firma, según una cualquiera de las reivindicaciones 1 a 6, cuando se ejecuta en un ordenador.