

97
103

SUPERINDUSTRIA Y COMERCIO	
Radicacion : 00029649 00000002	Folios: 29
Fecha (AND): 2000-06-08 10:28:06	
Tramite : 002 PATENTES D 1 REGISTRO/ 444 REPUESTA	
Dependencia: 0020 DIVISION DE NUEVAS CREACIONES	

Señores

DIVISION DE NUEVAS CREACIONES

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Santafé de Bogotá, D.C.

02-01-03-

Re.: Expediente No. 00 - 29.649

Solicitud de Patente

En relación con la última providencia recaída en este expediente, le manifiesto lo siguiente:

- 1.- Debidamente traducidas, las copias oficiales de las solicitudes de patente básicas británicas No. 60/130.944 y 09/461.766 ya fueron acompañadas a mi escrito del 10 de Mayo del 2000.
- 2.- Se acompaña el arte final por triplicado.
- 3.- Se acompaña texto revisado de la descripción, reivindicaciones, resumen y dibujos.
- 4.- Por motivo de lo anterior, se acompaña nueva tarjeta de archivo temático.

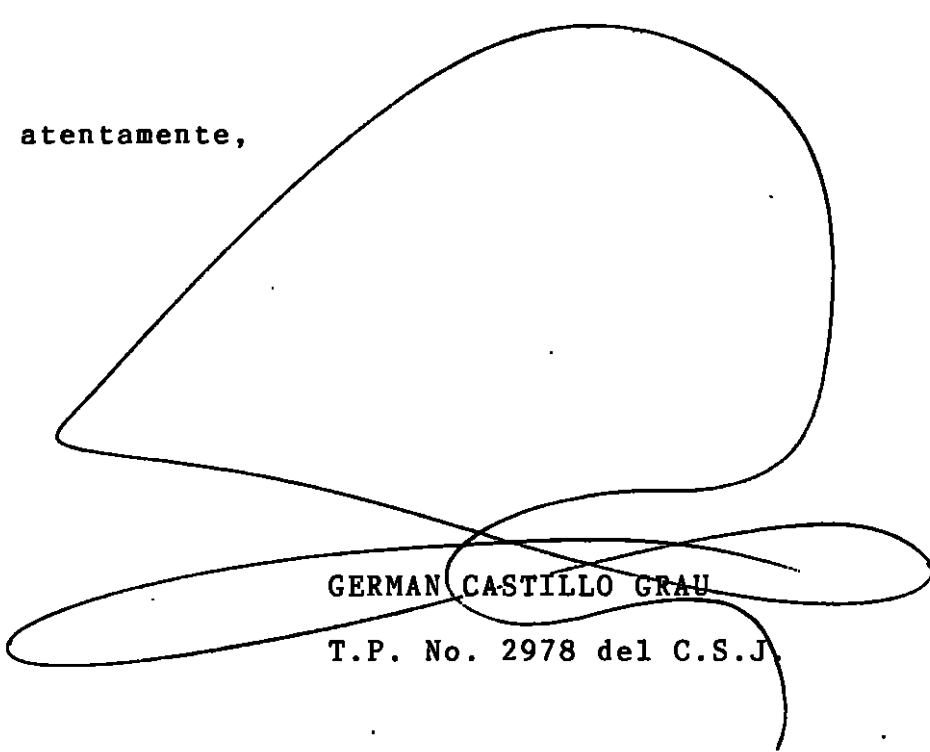
Renuncio al término faltante de traslado y le solicito ordenar la publicación del extracto.

104

Página No. 2

Expediente No. 00 - 29.649

De Ustedes atentamente,



GERMAN CASTILLO GRAU

T.P. No. 2978 del C.S.J.

aa M
105

SUPERINDUSTRIA Y COMERCIO	
Radicacion : 00029649 00000001	Folios: 63
Fecha (AMD): 2000-05-10 10:02:09	
Tramite : 002 PATENTES D 1 REGISTRO/ 329 COMPLEMEN	
Dependencia: 2020 DIVISION DE NUEVAS CREACIONES	

Señores

DIVISION DE NUEVAS CREACIONES

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Santafé de Bogotá, D.C.

Re.: Expediente No. 00 - 29.649

Solicitud de Patente

Debidamente traducidas, adjunto acompaño las solicitudes de patente básicas No. 60/130.944 y 09/461.766 las cuales le solicito agregar a este expediente para los efectos legales respectivos.

De Ustedes atentamente,

GERMAN CASTILLO GRAU

T.P. No. 2978 del C.S.J.

FORMATO DE DIGITALIZACION
RELACION DE ANEXOS

Expediente No		00079649	No de Follo
Item		No de unidades	
1	CD		✓
2	DVD		
3	REVISTA		
4	LIBRO		
5	PERIODICO		
6	DISQUETES		
7	SOBRE DE MANILA		
8	SOBRE BLANCO TAMAÑO CARTA		
9	SOBRE BLANCO TAMAÑO OFICIO	1	
10	OTROS:		
Observaciones: Acta Fm1			

101 →
106

MÉTODO Y DISPOSITIVO PARA EL CONTROL EFECTIVO DE LA LONGITUD DE CLAVE

Antecedentes

La presente invención se refiere al cifrado y en particular a un método y dispositivo para proporcionar una forma controlable y segura de determinar una clave de encriptado para utilizarse en un algoritmo de encriptado.

En los sistemas de comunicación, los datos generalmente se encriptan antes de transmitirse para asegurar privacidad e integridad de datos. El encriptado de datos se lleva a cabo en un algoritmo de encriptado. Este algoritmo de encriptado manipula o codificar los datos de transmisión utilizando otros datos, otras operaciones matemáticas y / o otros medios para realizar dicho encriptado. Por ejemplo, el algoritmo de encriptado utiliza un parámetro de datos conocido como una clave de encriptado, expresada en este documento como la variable K'_e en su proceso de inicialización. La clave de encriptado se ha creado en parte a partir una clave de cifrado o clave secreta, expresada en este documento como K_e donde K_e es conocida tanto por el dispositivo receptor como por el dispositivo transmisor para encriptar y descifrar los datos.

Los gobiernos regulan las partes y los dispositivos de comunicación de exportación que se utilizan para la encriptación y transmisión de datos, incluidos pero no limitados a software y hardware de encriptado. Tales regulaciones de exportación difieren según los diferentes países. De manera específica, los gobiernos regulan la longitud máxima de clave permitida para cifrar claves para los dispositivos de exportación. Los usuarios que transmiten y reciben datos encriptados preferirían utilizar la mejor clave posible, es decir, la clave de cifrado más larga posible para maximizar la seguridad; sin embargo, los usuarios están limitados por las regulaciones gubernamentales de la clave de cifrado.

Suponga que la tecnología actual proporciona longitudes de clave de la clave de cifrado, K_e para que esté entre 1 y 160 bytes (8 y 1.280 bits). Los gobiernos típicamente limitan la longitud máxima de clave de cifrado permitida a por ejemplo 7 bytes (56 bits).

Para ir más allá de esta longitud de clave de cifrado, un fabricante tendría que aplicar para obtener una licencia de exportación. Los dispositivos para comunicaciones, por ejemplo, teléfonos celulares, típicamente utilizan el máximo

162-6
p2

de longitud de clave permitida para un dispositivo en particular bajo las regulaciones de exportación aplicables. Por ejemplo, este parámetro podría almacenarse en la memoria de solo lectura (*READ ONLY*) *memory* (ROM). Sin embargo desde el punto de vista de fabricación, es conveniente producir dispositivos de comunicación que funcionen en diferentes países, evitando así la personalización y permitiéndole al usuario utilizar el mismo dispositivo en diferentes lugares geográficos. El fabricante preferiría producir un producto universal con un método estandarizado de encriptado que cumpla con las diferentes regulaciones establecidas por la variedad de gobiernos y también proporcionar una alto nivel de seguridad de datos.

Actualmente, una clave de encriptado K'_{c9} junto con otros parámetros públicos, como un reloj maestro, se utiliza para la inicialización de un algoritmo de encriptado. La clave de encriptado K'_{c9} utiliza la clave de cifrado, K_{c9} y un número aleatorio público, llamado *RAND*, de acuerdo con la siguiente ecuación:

$$K'_{c9}[0...15] = \begin{cases} K_c[0...L-1] \cup \text{RAND}[L...15], & L < 16, \\ K_c[0...15], & L = 16. \end{cases} \quad (EQ.1)$$

donde L es $1 \leq L \leq \min \{L^A_{\max} \text{ y } L^B_{\max}\}$ en bytes; y

donde $\text{RAND}[L...15]$ nota los L bytes hasta 15 de *RAND*.

Para fines de ilustración, la longitud de clave de encriptado utilizable máxima en bytes, $L_{\max9}$, se supone que es de 16 bytes, aunque se podrían utilizar diferentes longitudes de clave de encriptado.

Según lo revelado por la anterior ecuación, la clave de encriptado, K'_{c9} se crea añadiendo un número aleatorio al final de la clave de cifrado, K_{c9} para completar toda la cantidad de bytes disponibles para la longitud de clave de encriptado, es decir, 16 bytes en este caso. El parámetro L representa la longitud de clave de cifrado más pequeña permitida entre dos longitudes de clave de cifrado, $L^A_{\max}$ y $L^B_{\max}$ del primer dispositivo de comunicación A y el segundo dispositivo de comunicación B fabricados bajo diferentes regulaciones gubernamentales. En otras palabras, la longitud de clave de cifrado utilizada para computar la clave de encriptado, K'_{c9} es la menor de las dos longitudes de clave de cifrado permitidas para ser utilizadas por los dispositivos A y B primero y

109
103

segundo. Los dos dispositivos pueden utilizarse en comunicaciones de encriptado con la longitud más pequeña, pero solo un dispositivo puede utilizar comunicación encriptada con la longitud de clave más grande.

Uno de los problemas con la ecuación anterior para generar la clave de encriptado, K'_{c9} es que es difícil asegurar que el hardware que implemente el algoritmo encriptado no sea alterado por el software que cancele los valores preestablecidos de L_{max} . Además, el parámetro $RAND$, al ser público, puede dársele un mal uso para alcanzar una longitud de clave efectiva y no tiene restricción, es decir K'_c tiene un número máximo de bits de clave efectivos.

Una solución alterna es reducir el espacio proporcionado para la clave de encriptado, K'_{c9} a L bytes en la memoria del dispositivo de comunicación para prevenir que el software altere la longitud. Esto se puede llevar a cabo "enmascarando" toda la cantidad de bytes disponibles menos los K bytes de la clave de cifrado, K'_c e ignorando el $RAND$. Por ejemplo, en este caso, debido a que se supone que el máximo de longitud de clave de encriptado es 16, 16 menos los L bytes que serían "enmascarados" o en otras palabras, pueden ser remplazados con ceros o con otra cadena fija. La clave de encriptado resultante, K'_{c9} consistiría entonces de K_c para los primeros L bytes y de ceros o de cualquier otra cadena fija para los próximos $16 - L$ bytes ($128 - 8L$ bits).

Sin embargo, para los valores pequeños de bytes de L resultan, por lo menos, dos consecuencias no deseadas de esta solución. Primero, durante la inicialización del algoritmo de encriptado, el algoritmo de encriptado baraja la clave de encriptado, K'_{c9} y determina un punto de partida del algoritmo de encriptado. Para lograr un encriptado fuerte, el periodo de baraja necesitaría ser incrementado por la "falta de aleatoriedad" de la cadena fija grande en los 16 menos L bytes, donde L es pequeño. A medida que baja la longitud de la parte "aleatoria" de la clave de cifrado, el algoritmo de encriptado idealmente aumentaría el periodo de baraja, o el número de iteraciones realizadas, al determinar un punto de partida de la clave de encriptado para compensar la pequeña longitud de bits "aleatorios" y lograr así un mejor encriptado. Sin embargo, el número de iteraciones que se pueden realizar está limitado por los requerimientos estrictos de cronometraje establecidos en la conmutación de transmisión / recepción. Por lo tanto, esto crea el riesgo de un encriptado débil.

Segundo, una persona no autorizada que intente descryptar los datos encriptados o realizar un "ataque de cifrado" solo necesitaría considerar o analizar

110-2
104

los primeros L bytes de la clave de cifrado, K'_c . En otras palabras, la persona no autorizada solo tendría que analizar las posibles combinaciones de datos en los L bytes en lugar de analizar la longitud de clave de encriptado utilizable máxima más grande, en este caso, 16 bytes, para los valores pequeños de L . Esto crea el riesgo de desencriptado no autorizado.

En general, un buen algoritmo de encriptado recibe como su entrada, uno de, por ejemplo, 2^{8L} posibles puntos de partida en un sistema binario. Donde L es 16 bytes, un buen algoritmo de encriptado recibiría 2^{128} posibles puntos de partida en un sistema binario. Cada una de las posibles combinaciones de los $8L$ K'_c bits definiría un punto de partida fuera de los puntos de partida 2^{8L} . Una persona no autorizada que intente desencriptar los datos cifrados tendría que ensayar hasta 2^{8L} posibles combinaciones para lograrlo. Hay muy pocos puntos de partida disponibles donde las regulaciones gubernamentales tengan longitud de clave restringida. Por ejemplo, si un gobierno restringe una longitud de clave de cifrado a un máximo de 5 bytes (40 bits), un algoritmo de encriptado tendría un número reducido de puntos de partida, es decir 2^{40} puntos de partida. Es más, si se considera el espacio, o la memoria, disponible para almacenar todos los posibles 2^{8L} puntos de partida, la tecnología actual típicamente restringe la memoria total disponible a un área específica de la memoria para almacenar el número reducido de puntos de partida y no utiliza la parte restante de la memoria. Las posiciones restantes son constantes. Así, una persona no autorizada que intente desencriptar los datos cifrados solo tendría que analizar 2^{40} puntos de partida y la persona no autorizada sabría donde estarían localizados en la memoria dichos puntos de partida.

RESUMEN

De conformidad, para vencer los problemas antes mencionados, la presente invención describe un método por el cual se genera una clave de encriptado, K'_c , el número total de posibles puntos de partida están restringidos a un subconjunto de 2^{8L} puntos de partida, donde los subconjuntos son diferentes cada vez que se genera un nuevo K'_c en el total de memoria o espacio disponible. Por consiguiente, los puntos de partida ya no están almacenados en el mismo lugar después de cada generación de una nueva clave de encriptado, K'_c .

Además, la presente invención proporciona una interfaz entre el generador de la clave de cifrado, K'_c en un sistema de comunicaciones y el dispositivo de cifrado que utiliza la clave de cifrado en los datos encriptados. La interfaz

247-105

proporciona una forma segura y controlable de limitar la longitud de clave para ajustarse a la longitud de clave efectiva establecida por las regulaciones gubernamentales al incluir una función de adición o de módulo en el cálculo de la clave de encriptado, K'_c .

Es más, la presente invención proporciona comunicaciones entre dos dispositivos que están regulados por diferentes gobiernos estableciendo distintos máximos de longitud de clave de cifrado.

Además, la presente invención proporciona una clave de encriptado, K'_c , donde la "aleatoriedad" está extendida sobre todas las posibles combinaciones de puntos de partida para entrar en el algoritmo de encriptado del dispositivo de cifrado.

Las ventajas anteriores y otras de la presente invención se llevan a cabo en una forma por un dispositivo de comunicación para determinar una clave de encriptado para ser utilizada en un algoritmo de encriptado. El dispositivo de comunicación consta de un elemento de memoria para almacenar uno o más polinomios; una pluralidad de elementos de conmutación, cada uno con una primera entrada, una segunda entrada y una salida, donde las primeras entradas del elemento de conmutación están conectadas al elemento de memoria; una pluralidad de elementos de retardo, cada uno con entrada y salida, donde la salida de un elemento de retardo está conectado a las segundas entradas del elemento de conmutación; y una pluralidad de funciones de adición o de módulo, cada una con una primera entrada, una segunda entrada y salida, donde las primeras entradas de módulo están conectadas a todos excepto una de las salidas del elemento de retardo, donde las segundas entradas de módulo están conectadas a todas excepto a una de las salidas del elemento de conmutación y donde las salidas de módulo están todas conectadas excepto una de las entradas del elemento de retardo. Los elementos de retardo pueden ser un registro de desplazamiento.

Las ventajas anteriores y otras de la presente invención también pueden tener otra forma por medio de un método para calcular una clave de encriptado, $K'_c(x)$, para utilizarse en un algoritmo de cifrado. El método consta de pasos para obtener una clave de cifrado, $K'_c(x)$; para determinar una máxima longitud de clave de cifrado, L ; para determinar un máximo disponible de longitud de clave de encriptado, L_{max} , para obtener un polinomio $g_1(x)$, para extender los puntos de

partida de dicha clave de encriptación, $K'_c(x)$; y para calcular la clave de encriptado, $K'_c(x)$, donde $K'_c(x) = g_2^{(L)}(x)[K_c(x) \bmod g_1^{(L)}(x)]$.

442-~~8~~
106

BREVE DESCRIPCIÓN DE LOS DIBUJOS

Se puede derivar una mejor comprensión de la presente invención al referirse a la descripción detallada y reivindicaciones cuando se consideran en conjunto con las figuras donde:

La Figura 1 muestra dos dispositivos de comunicación móvil transmitiendo y recibiendo datos de acuerdo con la presente invención;

La Figura 2 muestra un esquema para computar una clave de encriptado, K'_{cs} , de acuerdo con la presente invención;

La Figura 3 muestra un registro de desplazamiento de acuerdo con el esquema de la Figura 2 en diferentes intervalos de acuerdo con la presente invención; y

La Figura 4 muestra un diagrama de bloque de un método para computar una clave de encriptado, K'_{cs} , de acuerdo con la presente invención.

DESCRIPCIÓN DETALLADA

En la siguiente descripción, por razones de la explicación y no de limitaciones, se establecen los detalles específicos, tales como circuitos particulares, componentes de circuitos, técnicas, etc., para poder proporcionar una comprensión a fondo de la presente invención. Sin embargo, será evidente para alguien experimentado en la técnica que la presente invención puede ser practicada en otras realizaciones que partan de estos detalles específicos. En otros casos, las descripciones detalladas de los métodos bien conocidos, de los dispositivos y circuitos son omitidos como para no restarle importancia a la descripción de la presente invención.

Para asegurar conformidad con una longitud de clave regulada y para mejorar el encriptado de la transmisión de datos entre dos o más dispositivos, se determina o calcula una clave de encriptado, K'_{cs} y se entra en un algoritmo de encriptado de acuerdo con la presente invención según la siguiente fórmula:

$$K'_c(x) = g_2^{(L)}(x)[K_c(x) \bmod g_1^{(L)}(x)] \quad (\text{Eq. 2})$$

113
107

donde:

L es la longitud máxima de clave de cifrado restringida en bytes y es

$1 \leq L \leq \min \{L_{\max}^A, L_{\max}^B\}$, y $\deg(g_1(x)) + \deg(g_2(x)) \leq wL$ para todos los L bytes donde w es una longitud de palabra en bits.

La clave de encriptación, K'_{ca} está escrita encima en términos de una expresión de polinomio para fines de ilustración.

Como se reveló en la Ecuación 2, la clave de encriptación, K'_{ca} se basa en parte en la clave de cifrado, K_c . La clave de cifrado, K_c , se puede obtener en cualquier forma apropiada ahora conocida o descubierta más adelante. Por ejemplo, la clave de cifrado, K_c puede ser comunicada de manera independiente a un Dispositivo A y a un Dispositivo B desde un tercer dispositivo para facilitar la encriptación y la desenscriptación. De manera alterna, el Dispositivo A puede tener una clave de cifrado, K_c almacenada y puede comunicar esto al Dispositivo B. Suponga que la tecnología actual permita una longitud de clave de cifrado que esté entre 1 y 160 bytes (8 y 1.280 bits) de longitud. Sin embargo, los gobiernos de los cuales se exportan el Dispositivo A y Dispositivo B han puesto ciertas restricciones a la longitud máxima de la clave de cifrado. Por ejemplo, suponga que el dispositivo A puede comunicarse con un máximo de longitud de clave de 5 bytes (40 bits) y que el Dispositivo B puede comunicarse con un máximo de longitud de clave de 7 bytes (56 bits). Una vez que se determina que el dispositivo A desea transmitir datos al Dispositivo B, el Dispositivo A y el Dispositivo B "negocian" una longitud de clave máxima aceptable, L en la cual los dos se pueden comunicar. Específicamente, el Dispositivo A y el Dispositivo B transmitirán y recibirán datos desde y hasta cada uno que especifique cada uno de las longitudes de clave máximas. En este ejemplo, debido a que $L_{\max}^A$ es 40 bits y $L_{\max}^B$ es 56 bits, los dispositivos "acordarán" comunicarse con un máximo de longitud de clave, L de la mínima longitud de clave, o 40 bits.

Así, de acuerdo con la presente invención, el máximo posible de longitud de clave está restringido al mínimo del máximo de las longitudes de clave entre los dispositivos A y B. Esta restricción de longitud de clave está implementada en la encriptación por medio de la función de adición o de módulo y la selección del polinomio $g_1(x)$.

En una realización ilustrada, $g_1(x)$ puede representarse como el siguiente polinomio:

$$g_1(x) = \sum_{i=0}^{wL} g_i^{(1)} x^i, \quad g_{wL} \neq 0 \quad (\text{Eq. 3})$$

donde w es igual a una longitud de palabra y L es igual al número de palabras en la clave de cifrado.

El polinomio $g_1(x)$ se crea de tal forma que el grado más alto del polinomio sea el del máximo permitido de longitud de clave en bits. Por ejemplo, si la longitud de la palabra es de 8 bits y el número de palabras es de 5, el grado más alto del polinomio $g_1(x)$ será 40. Así, el polinomio $g_1(x)$ puede ser, por ejemplo, de la siguiente manera:

$$g_1(x) = Ax^{40} + Bx^{39} + Cx^{38} + \dots + Dx + E, \quad A \neq 0 \quad (\text{Eq. 4})$$

La operación de adición o de módulo asegura que la longitud de clave sea de wL bits ya que el grado máximo de lo restante no puede exceder de uno menos que el grado más alto del dominador. En este ejemplo, la operación de computación $K_c(x) \bmod g_1^{(1)}(x)$ producirá un resultado donde el grado más alto posible es uno menos de 40, es decir 39. El resultado tiene 40 bits lo que está de conformidad con la longitud de clave máxima permitida.

El polinomio $g_1(x)$ puede accederse desde una tabla, por ejemplo, que identifica un polinomio $g_1(x)$ apropiado para un L dado. Esta tabla está preferiblemente localizada en el hardware de tal forma que los polinomios $g_1(x)$ disponibles estén seguros. Los polinomios $g_1(x)$ están protegidos de ser alterados para asegurar conformidad con las regulaciones gubernamentales. Se reconocerá que una tabla es una forma de almacenar o de obtener polinomios $g_1(x)$ pero que se pueden utilizar otras formas conocidas en la técnica.

Tal como se dijo anteriormente, un buen algoritmo de encriptado recibe como entrada, uno de los 2^{8L} posibles puntos de partida en un sistema binario, donde L es la longitud de clave máxima posible en bytes. Cada una de las

posibles combinaciones de $8L K'_c$ bits definirá uno de los puntos de partida fuera de los puntos de partida 2^{8L} . Una persona no autorizada que intente descifrar datos encriptados tendría que ensayar hasta las 2^{8L} posibles combinaciones para lograrlo.

Por ejemplo, si L es igual a 16 bytes, un buen algoritmo de encriptado recibe como entrada, uno de los posibles 2^{128} puntos de partida en un sistema binario. Cada una de las posibles combinaciones de los 128 K'_c bits definiría un punto de partida fuera de los 2^{128} puntos de partida. Una persona no autorizada que intente descifrar datos encriptados tendría que ensayar hasta 2^{128} posibles combinaciones para lograrlo.

En el ejemplo anterior con el Dispositivo A y el Dispositivo B un algoritmo de encriptado tendría un número reducido de puntos de partida debido al valor más pequeño de L que es 2^{40} puntos de partida. La tecnología actual típicamente restringe la memoria disponible total (en este caso, 2^{40} posibles puntos de partida) a un área específica de la memoria para almacenar el número reducido de puntos de partida y no utiliza la parte restante de memoria. Las posiciones restantes son constantes. Así, en este ejemplo en la tecnología actual, una persona no autorizada que intente descifrar datos encriptados solo tendría que analizar 2^{40} puntos de partida y dicha persona tendría que saber donde localizar los puntos de partida en la memoria.

En otras palabras, si la clave de encriptado, $K'_c(x)$ resulta solo de $K_c(x) \bmod g_1^{(L)}(x)$, $K'_c(x)$ sería almacenado en un lugar específico de la memoria de acuerdo con la tecnología actual. Los otros bits serían cero o cualquier otra cadena fija. Los puntos de partida estarían ubicados en un subconjunto específico de todos los posibles puntos de partida. Sin embargo, para incrementar la fuerza del encriptado, es beneficioso tener los puntos de partida extendidos de forma más efectiva en lugar de tenerlos confinados a un subconjunto específico de bits para que la distancia mínima entre los puntos de partida sea más grande.

Este concepto de incrementar la distancia o "extender" se conoce en la técnica. Por ejemplo, la codificación de corrección de error utiliza este concepto para una aplicación diferente. Por lo tanto, para extender los puntos de partida sobre el posible rango de bit, el resultado de la operación $K_c(x) \bmod g_1^{(L)}(x)$ se multiplica por un polinomio $g_2(x)$ donde se ilustra como sería un polinomio $g_2(x)$:

$$g_2(x) = \sum_{j=0}^{n(L_{\max}-L)} g_j^{(2)} x^j \quad (Eq. 5)$$

donde w es igual al largo de la palabra, L es igual al número de palabras de la clave de cifrado y L_{max} es igual al máximo número de palabras que se utilizan en la clave de encriptado.

La multiplicación de $g_2(x)$ más el resultado de $K_c(x) \bmod g_1^{(L)}(x)$ "extenderá" el resultado de $K_c(x) \bmod g_1^{(L)}(x)$ en toda el área bit. Se seleccionará el polinomio apropiado $g_2(x)$ con base en una L dada tal como actualmente se conoce en la técnica. Esto es, para diferentes longitudes de clave, L , se seleccionan diferentes coeficientes del polinomio $g_2(x)$ para alcanzar de manera más efectiva las distancias de Hamming deseadas. Para los valores pequeños de L , un conjunto de coeficientes puede alcanzar las distancias de Hamming deseadas, mientras que para los valores grandes de L , un conjunto diferente de coeficientes sería más apropiado para alcanzar las distancias de Hamming deseadas. En el caso binario $g_2(x)$ puede encontrarse como generador de polinomio de un código de corrección de error BCH. Los polinomios $g_2(x)$ pueden ser almacenados en una tabla que relaciona los polinomios $g_2(x)$ apropiados para una L dada. Esta tabla puede ser la misma tabla en la cual $g_1(x)$ está almacenado en otra tabla. Los polinomios $g_2(x)$ pueden almacenarse bien sea en el hardware o software del dispositivo de cifrado. Se reconocerá que una tabla sirve en una forma para almacenar y recuperar polinomios $g_2(x)$ pero que otras formas conocidas por la técnica también se pueden utilizar. Por otra parte, los polinomios $g_2(x)$ se pueden obtener de la memoria en otro lugar, es decir, que no estén localizados dentro del dispositivo de cifrado.

$K'_c(x)$ resulta de la siguiente multiplicación. $K'_c(x)$ es entrada al algoritmo de encriptado para ser utilizado en datos encriptados.

La Figura 1 muestra dispositivos de comunicación móvil (100), (102) transmitiendo y recibiendo datos entre sí de acuerdo con la presente invención. Los dispositivos (100), (102) pueden ser cualquier clase dispositivo alámbrico o inalámbrico, incluyendo, sin limitarse, un teléfono celular o un computador.

La Figura 2 muestra una vista más detallada de un dispositivo de comunicación (200). El dispositivo de comunicaciones (200) incluye un elemento de memoria (202), una pluralidad de elementos de conmutación, tales como puertas AND (204), una pluralidad de elementos de retardo (206) y una pluralidad de funciones de adición o de módulo (208).

117-111

El elemento de memoria (202) almacena polinomios $g_1(x)$. El elemento de memoria (202) puede ser una tabla de despliegue o cualquier otro arreglo para almacenar información. El elemento de memoria (202) también puede almacenar polinomios $g_2(x)$. Por otra parte, los $g_2(x)$ pueden almacenarse en otro lugar dentro del dispositivo de comunicaciones (200) o pueden obtenerse de un lugar externo al dispositivo de comunicación (200), pero que sea accesible. Para fines de ilustración, el elemento de memoria (202) se describe aquí como para almacenar tanto $g_1(x)$ como $g_2(x)$. Las funciones $g_1(x)$ y $g_2(x)$ son polinomios con coeficientes específicos, por ejemplo los descritos anteriormente.

Los elementos de conmutación o las puertas AND (204) cada una tiene una primera entrada, una segunda entrada y una salida. El elemento de memoria (202) está conectado a la primera entrada de las puertas AND (204). Cada elemento de retardo (206) tiene una entrada y una salida. Los elementos de retardo (206) pueden ser implementados como un registro de desplazamiento. La salida de una de las puertas AND (204a) está conectada a la entrada de un primer elemento de retardo (206a). Las funciones de módulo (208) cada una tiene una primera entrada, una segunda entrada y una salida. Las salidas de las puertas AND (208) restantes están conectadas a las primeras entradas de las funciones de módulo (208). Las salidas de todos los elementos de retardo (206), excepto el último elemento de retardo (206b), están conectadas a las segundas entradas de las funciones de módulo (208). La salida del último elemento de retardo (206b) está conectado a la segunda entrada de las puertas AND (204). Las salidas de las funciones de módulo (208) están conectadas a las entradas de todos los elementos de retardo (206) excepto al primer elemento de retardo (206a).

Para fines ilustrativos, imagínese un esquema binario para mayor facilidad; sin embargo, aquellos expertos en la técnica apreciarán que la presente invención sea igualmente aplicable a otras representaciones de símbolo.

Inicialmente, los dispositivos de comunicación (100), (102) como los muestra la Figura 1 van a "negociar" o a comunicarse entre sí para determinar la longitud de clave de cifrado, L , que utilizan los dos dispositivos (100) y (102) para comunicarse, como se vió anteriormente. Los dispositivos (100) (102) pueden, por ejemplo, intercambiar la longitud clave de cifrado máxima respectiva de cada dispositivo. Los dispositivos (100), (102) "acuerdan" un máximo de longitud de clave de cifrado, L , seleccionando la longitud más pequeña de los dos longitudes

118 112

de clave de cifrado requeridas para cada dispositivo, en caso de que las longitudes de clave de cifrado, L , sean diferentes.

Con referencia de nuevo a la Figura 2, la primera entrada de puertas AND (204) es el polinomio binario $g_1(x)$ del elemento de memoria (202). Los primeros coeficientes $w(L_{max}-L)$ son cero y los últimos coeficientes wL pueden ser números diferentes a cero. En este caso, w es igual a la longitud de la palabra, para todas las $w \geq 1$, L es igual al número "negociado" de palabras de la clave de cifrado, para todas las $L \geq 1$, L_{max} es igual al máximo número de palabras utilizables en la clave de cifrado, para todas las $L_{max} \geq 1$. La segunda entrada de las puertas AND (204) está inicializada en cero. Así, la salida de las puertas AND (204) es cero para cada puerta que corresponda a los primeros bits $w(L_{max}-L)$. Para el último bits wL , la salida de las puertas AND (204) son una función de los coeficientes del polinomio $g_1(x)$ para cada puerta que corresponda con los últimos coeficientes wL . Cuando el coeficiente para $g_1(x)$ es 0, la puerta AND (204) se abrirá. Inversamente, cuando el coeficiente para $g_1(x)$ es 1, la puerta AND (204) se cerrará.

Los elementos de retardo (206) se inicializan con los coeficientes de la clave de cifrado, $K_c(x)$ (tal como se muestra en el registro de desplazamiento (306a) de la Figura 3). Estos coeficientes, así como las salidas de las puertas AND (204), son entradas dentro de funciones/privativas $0-(208)$ (Esto para el caso binario. Para casos diferentes al binario, estos coeficientes son entradas a otra función de adición apropiada). Las entradas iniciales de las puertas AND (204) son una cadena de ceros y de coeficientes $g_1(x)$ según se describió anteriormente. Las salidas de las funciones privativas $0-(208)$ son entrada a todas las puertas AND (206), excepto a la primera puerta AND (206a). La salida del último elemento de retardo (206b) se vuelve a alimentar en las segundas entradas de todas las puertas AND (204). Este proceso se repite a medida que los datos se desplazan, de acuerdo con los ciclos disponibles, los pulsos de reloj u otros mecanismos de cronometraje.

La clave de cifrado, $K'_c(x)$, inicialmente se coloca en los elementos de retardo (206) (o como lo muestra un registro de desplazamiento (306a) en la Figura 3). Como se describió anteriormente, los cálculos se llevan a cabo utilizando la clave de cifrado, $K'_c(x)$. La clave de cifrado, $K'_c(x)$, se desplaza fuera de los elementos de retardo (206). La salida del último elemento de retardo (206b) es una entrada al interior de las puertas AND(204) en aquellas posiciones en donde las puertas AND -- -----

179-4
113

(204) están cerradas. Después de completar los desplazamientos $w(L_{max}-L)$, los elementos de retardo (206) contienen el resultado de la función privativa -0 , $K_c(x) \bmod g_1(L)(x)$ en el último espacio wL (como se muestra en el registro de desplazamiento (306b) en la Figura 3). Como se dijo anteriormente, este cómputo asegura que la longitud máxima de clave de cifrado, $K_c(x)$, no excede las regulaciones gubernamentales de la longitud máxima de clave permitida.

Después de terminar los desplazamientos de $w(L_{max}-L)$, $g_2(x)$ es ingresado a las puertas AND (204). En contraposición a $g_1(x)$, $g_2(x)$ es un polinomio donde los primeros coeficientes $w(L_{max}-L)$ pueden ser números diferentes a cero y los últimos coeficientes wL son ceros. El anterior proceso continúa para otros desplazamientos wL . Los bits wL que resultan de la función privativa -0 han sido "extendidos" en el área. El resultado en los elementos de retardo (206) (como se muestran en el registro de retardo (210c) en la Figura 3) es una clave de encriptado, $K'_c(x)$ que entonces se puede ingresar a un algoritmo de encriptado adecuado para encriptar datos.

Para fines ilustrativos, suponga que w es igual a 8, L es igual a 5, L_{max} es igual a 16. Suponga de nuevo que es un esquema binario para mayor facilidad.

Con referencia de nuevo a la Figura 2, la primera entrada de las puertas AND (204) es el polinomio binario $g_1(x)$ desde el elemento de memoria (202). Los primeros coeficientes $w(L_{max}-L)$, u 88, son cero y el último coeficiente wL , o 40 pueden ser números diferentes a cero. La segunda entrada de las puertas AND (204) se inicializa en cero. Así, la salida de las puertas AND (204) es cero para cada puerta correspondiente a los primeros 88 bits. Para los últimos 40 bits, las salidas de las puertas AND (204) son una función de los coeficientes del polinomio $g_1(x)$ para cada puerta correspondiente a los últimos 40 bits. Cuando el coeficiente para $g_1(x)$ es 0, la puerta AND se abrirá. Inversamente, cuando el coeficiente para $g_1(x)$ es 1, la puerta AND se cerrará.

Los elementos de retardo (206) se inicializan con los coeficientes de la clave de cifrado $K_c(x)$.—Estos coeficientes, así como las salidas de las puertas AND(204) ingresan a las funciones privativas -0 (208). (Las entradas iniciales de AND(204) son una cadena de ceros y los coeficientes $g_1(x)$ ya fueron mencionados). Las salidas de las funciones privativas -0 (208) ingresan a todas las puertas AND(206), salvo la primera puerta AND(206a).— La salida del último elemento de retardo (206b) se ingresa a todas las puertas

120 ~~114~~

AND (204) en aquellas posiciones donde las puertas AND (204) están cerradas. Este proceso se repite a medida que los datos se desplazan.

La clave de cifrado, $K_c(x)$ se localiza inicialmente en 128 elementos de retardo (206) (o en un registro de desplazamiento de 128 bits como se muestra en (306a) en la Figura 3). De acuerdo con la anterior descripción el cómputo se lleva a cabo utilizando la clave de cifrado, $K_c(x)$. La clave de cifrado, $K_c(x)$, se desplaza fuera del elemento de retardo (206). La salida del último elemento de retardo (206b) se ingresa a las puertas AND (204). Después de completar 128-40 u 88 desplazamientos, los elementos de retardo (206) contienen el resultado de la función exclusiva-o, $K_c(x) \bmod g_1^{(L)}(x)$ en los últimos 40 espacios.

Los coeficientes $g_2(x)$ entran las puertas AND (204). Los anteriores procesos continúan durante 40 desplazamientos más o por un total de 128 desplazamientos. Los 40 bits resultantes de la función exclusiva-o han sido "extendidos" en el área. El resultado en los elementos de retardo (206) (o en el registro de desplazamiento (306c) como se muestra en la Figura 3) es la clave de encriptación, $K'_c(x)$, que se puede ingresar en un algoritmo de encriptado apropiado para encriptar datos.

La Figura 4 muestra un diagrama de bloque de un método (400) para computar la clave de encriptado, K'_c , para encriptar datos de acuerdo con la presente invención. El método 400 incluye el paso para obtener una clave de cifrado, $K_c(x)$ (402). Tal como se describió anteriormente, la clave de cifrado, $K'_c(x)$ se puede obtener de varias formas conocidas en la técnica. Luego, se lleva a cabo el paso de determinar una longitud máxima de clave de cifrado, L (404). La longitud máxima de clave típicamente es un valor expresado en bytes. Los dispositivos que deseen comunicarse intercambiarán información o "negociarán" respecto a la longitud máxima de clave de cifrado con la cual cada dispositivo se puede comunicar. Típicamente, la longitud máxima de clave se establecerá a la longitud de clave más larga disponible negociada con la cual los dos dispositivos se pueden comunicar. Entonces se obtiene un polinomio $g_1(x)$ de acuerdo con el paso (406). Un polinomio $g_1(x)$ se manipula matemáticamente con la clave de cifrado, $K_c(x)$ de acuerdo con la función $K_c(x) \bmod g_1(x)$ para lograr un primer resultado. Un polinomio $g_2(x)$ se obtiene de acuerdo con el paso (408). El paso (408) extiende los puntos de partida, o incrementa la distancia de Hamming de la clave de encriptación, $K'_c(x)$. Se selecciona un polinomio apropiado $g_2(x)$ con base en los resultados del paso (404). Finalmente, se puede calcular la clave de

127 A
115
encriptación, $K'_c(x)$ de acuerdo con el paso (410) donde $K'_c(x) = g_2^{(L)}(x)[K_c(x) \bmod g_1^{(L)}(x)]$.

La presente invención ha sido descrita anteriormente con referencia a las realizaciones preferidas. Sin embargo, aquellos expertos en la técnica reconocerán que se puede hacer cambios y modificaciones sin alejarse del alcance de la presente invención. Por ejemplo, aunque la presente invención describe un método y un dispositivo donde la longitud máxima de clave de cifrado, L , es de 5 bytes, y la longitud máxima utilizable de clave de encriptado, L_{max9} , es de 16 bytes, se notará que la presente invención no está limitada a esas longitudes. Además, también se notará que los datos transmitidos y recibidos no están limitados a ningún tipo de dato en particular. Puede constituirse por voz, datos escritos u otros. Puede ser binario, ASCII o cualquier otra forma de datos. Además, los datos pueden ser transmitidos por cualquier medio conocido como por ejemplo alambre o alambres aéreos o según se descubra más adelante.

122-20
116

REIVINDICACIONES

1. Un dispositivo de comunicación para calcular una clave de cifrado, K'_{cs} manipulando una clave de cifrado, K_{cs} para utilizarse en un algoritmo de encriptado; dicho dispositivo consta de:

un elemento de memoria para almacenar uno o más polinomios;

una pluralidad de elementos de conmutación, cada uno con una primera entrada, una segunda entrada y una salida, donde dichos elementos de conmutación de primera entrada están conectados a dicho elementos de memoria;

una pluralidad de elementos de retardo, cada uno con una entrada y una salida, donde dicha salida de uno de dichos elementos de retardo está conectado a dichos elementos de segundas entradas; y

una pluralidad de funciones de adición, cada una con una primera entrada, una segunda entrada y una salida, donde:

dichas primeras entradas de funciones de adición están conectadas a todas excepto a una salida de dichos elementos de retardo,

dichas segundas entradas de función de adición están conectadas a todas excepto a una de salidas de dichos elementos, y

dichas salidas de función de adición están conectadas a todas excepto a una de dichos entradas de elementos de retardo.

2. El dispositivo de la Reivindicación 1, donde dichos elementos de conmutación son puertas AND.

3. El dispositivo de la Reivindicación 1, donde el elemento de memoria almacena un polinomio $g_1(x)$, donde

$$g_1(x) = \sum_{i=0}^{wL} g_i^{(1)} x^i, \quad g_{wL} \neq 0$$

y donde w es una longitud de palabra y L es un número de palabras de dicha clave de cifrado.

123 ~~123~~ 117

4. El dispositivo de la Reivindicación 3, donde el elemento de memoria almacena un polinomio $g_1(x)$, donde

$$g_2(x) = \sum_{j=0}^{w(L_{max}-L)} g_j^{(2)} x^j$$

y donde w es una longitud de palabra y L es un número de palabras de dicha clave de cifrado y L_{max} es el número máximo de palabras utilizables en la clave de encriptado, K'_c .

5. El dispositivo de la Reivindicación 4, donde dichos elementos de retardo inicialmente se cargan con dicha clave de cifrado, $K'_c(x)$.

6. El dispositivo de la Reivindicación 5, donde dicho polinomio $g_1(x)$ tiene unos primeros coeficientes $w(L_{max}-L)$ iguales a una cadena fija.

7. El dispositivo de la Reivindicación 6, donde dicho polinomio $g_2(x)$ tiene unos últimos coeficientes wL iguales a una cadena fija.

8. El dispositivo de la Reivindicación 7, donde el último wL bits de dichos elementos de retardo almacenan un resultado de $K_c(x) \bmod g_1(x)$ después de los desplazamientos $w(L_{max}-L)$.

9. El dispositivo de la Reivindicación 8, donde dichos elementos de retardo almacenan dicha clave de encriptado, K'_c , después de desplazamientos wL adicionales.

10. El dispositivo de la Reivindicación 1, donde dichos elementos de retardo son un registro de desplazamiento.

11. Un método para calcular una clave de encriptado, $K'_c(x)$, para encriptar datos que constan de los siguientes pasos:

obtener una clave de cifrado, K'_c ;

determinar una longitud de clave de cifrado máxima, L ;

determinar una longitud de clave de encriptado utilizable máxima, L_{max}

124. 2
118

obtener un polinomio $g_1(x)$;

obtener un polinomio $g_2(x)$, para extender los puntos de partida de dicha clave de encriptado, $K_c(x)$; y

calcular dicha clave de encriptado, K'_c

donde $K'_c(x) = g_2^{(L)}(x) [K_c(x) \bmod g_1^{(L)}(x)]$.

12. El método de la Reivindicación 11, además consta del paso de:

seleccionar dicho polinomio $g_2(x)$ basado en L .

13. El método de la Reivindicación 12, donde

$$g_1(x) = \sum_{i=0}^{wL} g_i^{(1)} x^i, \quad g_{wL} \neq 0$$

y donde un grado alto de dicho polinomio $g_1(x)$ es igual a wL .

14. El método de la Reivindicación 13, donde

$$g_2(x) = \sum_{j=0}^{w(L_{\max}-L)} g_j^{(2)} x^j.$$

15. El método de la Reivindicación 14, donde unos primeros coeficientes $w(L_{\max}-L)$ de $g_1(x)$ son iguales a una cadena fija.

16. El método de la Reivindicación 15, donde uno de los últimos coeficientes de $g_2(x)$ son iguales a una cadena fija.

17. El método de la Reivindicación 12, donde dicho paso de calcular se realiza utilizando una pluralidad de puertas AND, cada una con una primera entrada, una segunda entrada y una salida, una pluralidad de elementos de retardo y una pluralidad de funciones de adición.

18. El método de la Reivindicación 17, donde dicho método además consta de los siguientes pasos:

125.114-7

inicializar dichas primeras entradas de dichas puertas AND a dichos coeficientes de polinomio $g_1(x)$, e

inicializar dichas segundas entradas de dichas puertas AND en cero.

19. El método de la Reivindicación 17, donde dichos elementos de retardo son un registro de desplazamiento.

20. Un sistema para comunicar datos encriptados entre dos dispositivos de comunicación que constan de:

un primer dispositivo de comunicación con una longitud de clave de cifrado, L^A_{max} , y

un segundo dispositivo de comunicación con una segunda longitud de clave de cifrado, L^B_{max} , y

un medio para determinar la longitud de clave de cifrado máxima, L , donde $1 \leq L \leq \min \{L^A_{max}, L^B_{max}\}$;

dicho primer dispositivo consta de:

un medio para obtener polinomios $g_1(x)$ y $g_2(x)$;

un medio para obtener una función de cifrado, $K_c(x)$; y

un medio para calcular una clave de encriptado, $K'_c(x)$,

donde $K'_c(x) = g_2^{(L)}(x)[K_c(x) \bmod g_1^{(L)}(x)]$.

21. El sistema de la Reivindicación 20, donde dicho medio para calcular dicha clave de encriptado, $K'_c(x)$, consta de:

una pluralidad de puertas AND, cada una con una primera entrada, una segunda entrada y una salida, donde dichas primeras entradas de puerta están conectadas a dicho elemento de memoria;

una pluralidad de elementos de retardo, cada uno con una entrada y una salida, donde dicha salida de un elemento de retardo está conectado a dichas segundas entradas de puerta; y una pluralidad de funciones de adición, cada una con una primera entrada, una segunda entrada y una salida, donde dichas primeras entradas de funciones de adición están conectadas a todas excepto a una de dichas salidas del elemento de retardo, donde dichas segundas entradas

126. ~~10~~

de funciones de adición están conectadas a todas excepto a una de dichas salidas de puerta y donde dichas salidas de funciones de adición están conectadas a todas excepto a una de dichas entradas del elemento de retardo.

22. El sistema de la Reivindicación 21, donde dichos elementos de retardo están inicialmente cargados con dicha clave de cifrado, $K'_c(x)$.

23. El sistema de la Reivindicación 20, donde dichos medios para obtener polinomios $g_1(x)$ y $g_2(x)$ incluye recuperar dichos polinomios de un elemento de memoria contenido dentro de dicho primer dispositivo de comunicación.

24. El sistema de la Reivindicación 23, donde

$$g_1(x) = \sum_{i=0}^{wL} g_i^{(1)} x^i, \quad g_{wL} \neq 0.$$

25. El sistema de la Reivindicación 24, donde

$$g_2(x) = \sum_{j=0}^{w(L_{\max}-L)} g_j^{(2)} x^j.$$

26. el sistema de la Reivindicación 25, donde el último wL bits de dichos elementos de retardo almacenan el resultado de $K_c(x) \bmod g_1(x)$ después de desplazamientos $w(L_{\max}-L)$.

27. El sistema de la Reivindicación 26, donde dichos elementos de retardo almacenan dicha clave de encriptado, $K'_c(x)$, después de desplazamientos adicionales wL .

28. El sistema de la Reivindicación 21, donde dichos elementos de retardo son un registro de desplazamiento.

RESUMEN

La presente invención incluye un método y un dispositivo para calcular una clave de encriptado, K'_{cs} para utilizarse en la inicialización de un algoritmo de encriptado. La presente invención revela un método para calcular la clave de encriptado, $K'_c(x)$, obteniendo una clave de cifrado, $K_c(x)$, determinando una longitud máxima de clave de cifrado, L , basados en los requerimientos de los dos dispositivos que desean comunicarse y determinar una longitud de clave de encriptado máxima utilizable, L_{max} . La clave de cifrado, $K_c(x)$, luego se manipula por medio de una función de adición o por medio de una función exclusivamente de o con un polinomio $g_1(x)$. El resultado se multiplica con un polinomio $g_2(x)$, que extiende los puntos de partida de dicha clave de encriptado, $K'_c(x)$. La clave de encriptado se determina de acuerdo con $K'_c(x) = g_2^{(L)}(x) [K_c(x) \bmod g_1^{(L)}(x)]$. El método para calcular la clave de encriptado K'_{cs} asegura que no se excede una longitud máxima de clave de cifrado. Además, el método proporciona nuevos puntos de partida posibles cada vez que se genera una nueva clave de encriptado K'_{cs} .

122

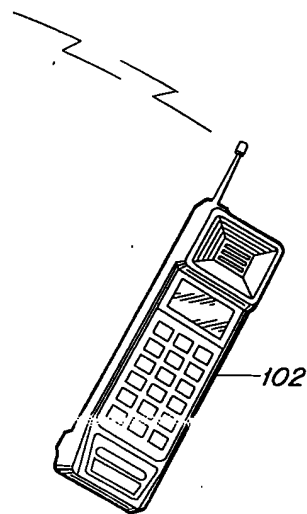
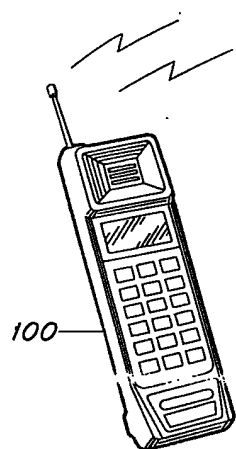
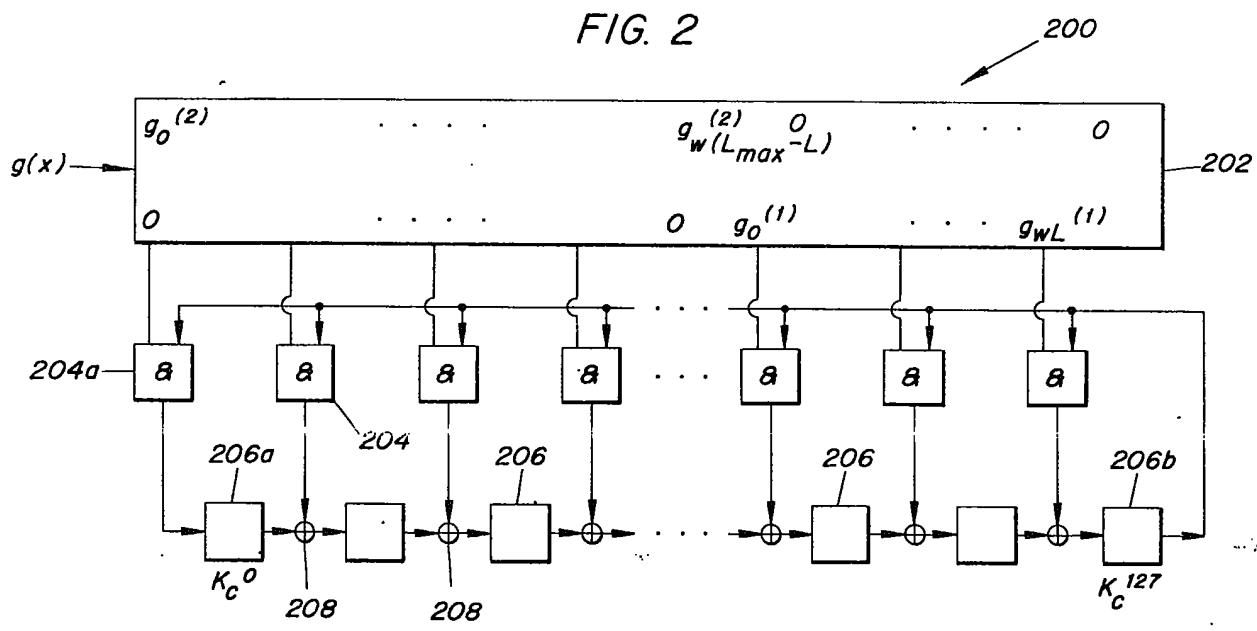


FIG. 1

128-96

128

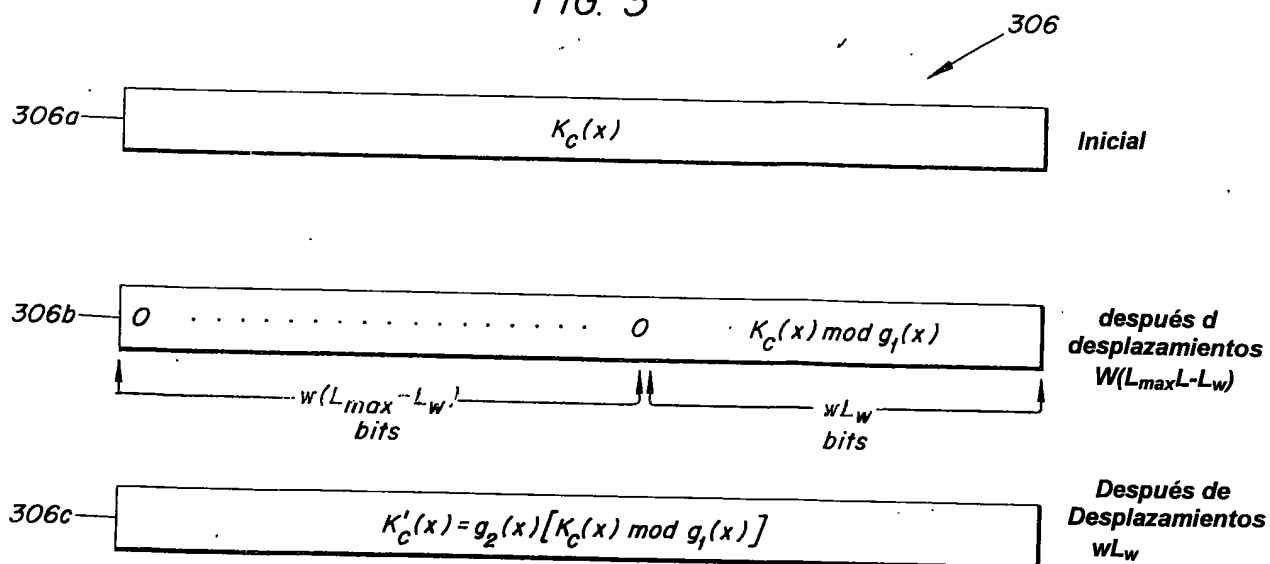
FIG. 2



129

1.5
124

FIG. 3



1.5
124

131 125

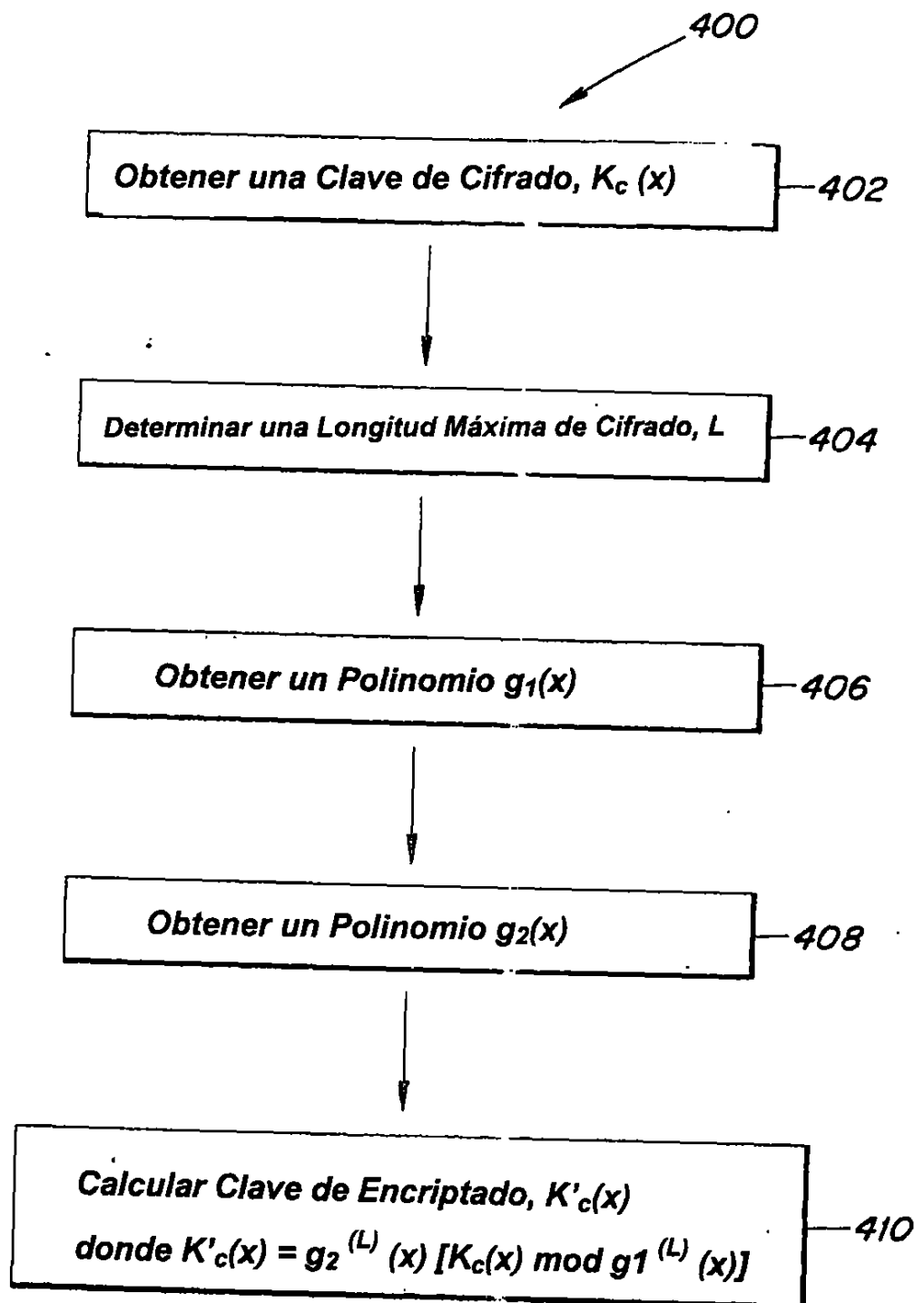


FIG. 4

folio 132 bajeto archivo temar

febrero 17/03

uz

2do. EXAMEN DE FORMA PATENTE DE INVENCION

Folio

133

Radicación no 00-29649

Concepto Técnico no . 415

Clasificación Internacional de Patentes : H04L9/28//G09C1/00

Practicado el examen de acuerdo a lo establecido en el Art. 38 de la Decisión 486 se determinó que esta solicitud de **Patente de Invención**:

- | | |
|--|---|
| SI ☒] NO ☐] | Contiene un resumen de la invención (Art.26-e). |
| SI ☒] NO ☐] | Contiene el título o nombre de la invención (Art.27-d). |
| SI ☒] NO ☐] | Contiene la descripción de la invención (Art.26-b). |
| SI ☒] NO ☐] | NO ES APLICABLE ☐] Contiene los dibujos necesarios para comprender la invención (Art.26-d) |
| SI ☒] NO ☐] | Contiene una o más reivindicaciones. (Art.26-c). |
| SI ☐] NO ☐] | NO ES APLICABLE ☒] Han sido desarrollados los productos y/o procedimientos a partir de recursos genéticos o de sus productos derivados de los que cualquiera de los Países Miembros es país de origen. (Art. 26- h). |
| SI ☐] NO ☐] | NO ES APLICABLE ☒] Los productos y/o procedimientos han sido obtenidos o desarrollados a partir de los conocimientos tradicionales de las comunidades indígenas, afroamericanas, o locales de los países miembros, de acuerdo a lo establecido en la Decisión 391 y sus modificaciones y reglamentaciones vigentes.(Art.26-i). |
| SI ☐] NO ☒] | La invención se refiere a un producto relativo a un material biológico. (Art.26-J). |
| SI ☒] NO ☐] | La prioridad coincide con la materia reivindicada. |
| SI ☒] NO ☐] | CUMPLE LOS REQUISITOS TÉCNICOS |

OBSERVACIONES Y OTROS: SI ☒] NO ☐] ver hoja(s) anexa(s)

EXAMINADOR TÉCNICO
202044

Bogotá D. C. Febrero 17 de 2003.

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

Folio 184

Concepto técnico no. 415

OBSERVACIONES

- ▣ Envía el documento mediante el cual reivindica la prioridad 60/130.944 Folios 45-56 y 09/461.766 Folios 65-102.
- ▣ Anexa la traducción del documento de prioridad 60/130.944 Folios 41-44 y 09/461.766 Folios 57-64.
- ▣ Anexa los dibujos alucivos a la invención. Folios 128-131.
- ▣ Anexa un nuevo capítulo descriptivo. Folios 106-121.
- ▣ anexa los artes finales. Folio 107.
- ▣ Anexa un nuevo capítulo reivindicatorio. Folios 122-126.

EXAMINADOR TECNICO

202044

Bogotá, Febrero 17 de 2003.

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

Folio 135

2020
Bogotá DC

Doctor(a)
GERMAN CASTILLO GRAU
Apoderado(a)

REFERENCIA:	Radicación No.	00-29649
	Trámite	002
	Evento	001
	Actuación	416
	Oficio No.	373
	Folios	001

Teniendo en cuenta que la solicitud de privilegio de patente que se tramita bajo el expediente indicado en la referencia, reúne los requisitos de forma establecidos en los artículos 26 y 27 de la Decisión 486 de la Comisión de la Comunidad Andina, y en las demás disposiciones vigentes sobre la materia, se envía el extracto de la solicitud a la Oficina de Comunicaciones para efecto de su publicación en la Gaceta de Propiedad Industrial, conforme lo establece el artículo 40 de la misma Decisión.

Cúmplase

Dado en Bogotá DC, a los

18 FEB. 2003


ALIX CARMENZA GESPEDES DE VERGEL
Jefe de la División de Nuevas Creaciones

202044

DIVISION DE NUEVAS CREACIONES

RADICACIÓN EXPEDIENTE No. 00-029649

EL EXTRACTO DE LA PRESENTE SOLICITUD DE PATENTE DE INVENCION
FUE PUBLICADO EN LA GACETA DE PROPIEDAD INDUSTRIAL No 530, DE
FECHA 31 DE JULIO DE 2003, EL TERMINO HABIL SEÑALADO POR LA LEY
EXPIRA EL 28 DE OCTUBRE DE 2003.

NOTA: Dentro del plazo de los seis (6) meses siguientes a partir de la fecha de publicación en la gaceta de Propiedad Industrial, deberá solicitar y cancelar el examen de patentabilidad so pena de que la solicitud caiga en abandono, de acuerdo con lo establecido en el Artículo 44 de la Decisión 486/2000.

SE PRESENTARON OPOSICIONES POR PARTE DE TERCEROS.

SI

NO **X**

Bogotá D.C., Febrero de 2004

131 130

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

RADICACIÓN: 0-29849

EDICTO No. 2524

**LA SECRETARÍA GENERAL AD-HOC
HACE SABER:**

Que esta Superintendencia profirió Resolución No. 2441 de 12-FEB-2004. Que el contenido de la parte resolutive es como sigue: El Superintendente de Industria y Comercio.

RESUELVE

ARTICULO PRIMERO: Declarar abandonada la solicitud de privilegio de patente de invención contenida en el expediente de la referencia.

ARTICULO SEGUNDO: Notificar personalmente el contenido de la presente resolución al doctor Germán Castillo Grau, o a quien haga sus veces, en su calidad de apoderado de Telefonaktiebolaget LM Ericsson (publ.), entregándole copia de la misma, advirtiéndole que contra ella procede el recurso de reposición interpuesto ante el Superintendente de Industria y Comercio, al momento de la notificación o dentro de los 5 días hábiles siguientes a ella.

NOTIFÍQUESE Y CUMPLASE

Dada en Bogotá, D.C., a los **12 FEB. 2004**

EL SUPERINTENDENTE DE INDUSTRIA Y COMERCIO,


JAIME DAVID ESCOBAR

Para notificar a los interesados, se fija el presente EDICTO en lugar visible al público en la SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO, por el término de (10) diez días hábiles contados a partir de las 8:30 a.m. de hoy.

Secretaría General Ad-Hoc 04-MAR-2004
Secretaría General Ad-Hoc
EDICTO No. 2524

Este edicto se desfija hoy 17-MAR-2004 a las cinco (5:00 p.m.)