(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 272 130**

(21) Número de solicitud: 200402603

(51) Int. Cl.:
H04L 9/18 (2006.01)

(12) PATENTE DE INVENCIÓN B1

(22) Fecha de presentación: **28.10.2004**

(43) Fecha de publicación de la solicitud: **16.04.2007**

Fecha de la concesión: **21.02.2008**

(45) Fecha de anuncio de la concesión: **16.03.2008**

(45) Fecha de publicación del folleto de la patente: **16.03.2008**

(73) Titular/es: **Universidad de Almería**
Ctra. de Sacramento, s/n
04120 La Cañada de San Urbano, Almería, ES

(72) Inventor/es: **Novas Castellano, Nuria;**
López Ramos, Juan Antonio;
Gázquez Parra, José Antonio y
Peralta López, Justo

(74) Agente: **Carvajal y Urquijo, Isabel**

(54) Título: **Unidad cifradora/descifradora de mensajes con información digital, sistema y método de cifrado/descifrado para comunicaciones digitales en tiempo real.**

(57) Resumen:
Unidad cifradora/descifradora de mensajes con información digital, sistema y método de cifrado/descifrado para comunicaciones digitales en tiempo real.
La invención consiste en un sistema implementado en un microcontrolador o FPGA que cifra y descifra la información mediante un algoritmo de cifrado simétrico basado en una tabla de claves que es recorrida usando un generador de filtro no lineal, produciendo de esta forma una secuencia cifrante que es operada mediante una operación XOR bit bit, dando lugar de este modo palabras de mensaje cifrado o mensaje en claro, dependiendo de si la entrada es el mensaje en claro o el mensaje cifrado respectivamente y mediante la cual, un mismo mensaje puede ser cifrado de muy diferentes formas, dependiendo del momento en el que se cifra.

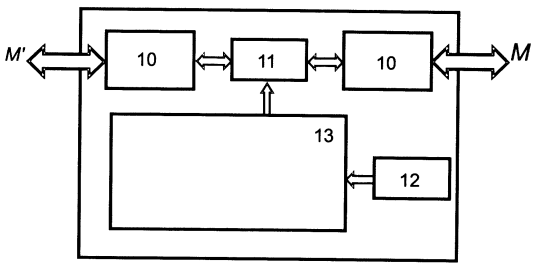

FIG. 1

ES 2 272 130 B1

DESCRIPCIÓN

Unidad cifradora/descifradora de mensajes con información digital, sistema y método de cifrado/descifrado para comunicaciones digitales en tiempo real.

Campo de la invención

El campo en el que se encuentra la presente invención es el de la protección de la información en transmisiones inalámbricas, por cable o mixtas por cable e inalámbricas.

Antecedentes de la invención

La protección de la información durante la transmisión de la misma ha sido una necesidad desde muy antiguo y más aún en el mundo civilizado actual. Son de sobra conocidos sistemas de cifrado y descifrado simétricos como DES (*Data Encryption Standard*), IDEA (*International Data Encryption Algorithm*) o más recientemente AES (*Advanced Encryption Standard*) que tratan la información por palabras, con un nivel de seguridad muy alto y una gran velocidad en las operaciones de cifrado y descifrado. Todos ellos se denominan simétricos debido a que se utiliza el mismo algoritmo para las operaciones de cifrado y descifrado y su uso en sistemas de comunicación por cable está muy extendido. Sin embargo, aunque todos ellos han demostrado su gran efectividad, presentan la debilidad de que un mismo mensaje es cifrado siempre por un mismo criptograma, lo que les hace susceptibles a ataques diferenciales y ataques de repetición por medio de mensajes grabados.

Otra importante clase de algoritmos de cifrado y descifrado son los conocidos como algoritmos de cifrado en flujo. Todos ellos cifran la información bit a bit, usualmente dígitos binarios, y en tiempo real y se basan en circuitos retro-alimentados linealmente, que proporcionan una secuencia cifrante y son muy apropiados para su implementación en hardware. La gran ventaja de los algoritmos de cifrado en flujo es que la función de cifrado varía con el tiempo y así, un mismo mensaje puede ser de varias formas distintas cifrado por varios criptogramas distintos, dependiendo del momento en el que se ha llevado a cabo la operación de cifrado. Sin embargo, su debilidad puede ponerse de manifiesto en ataques con texto en claro - texto cifrado, al obtenerse información sobre la secuencia cifrante.

Debido a las limitaciones que ofrece la transmisión por radio en transmisiones inalámbricas o híbridas por cable e inalámbricas, específicamente las derivadas del ancho de banda, se hace necesario un sistema de cifrado que tenga en cuenta todos estos aspectos.

Un ejemplo de un sistema de cifrado para comunicaciones por radio es la patente española ES-2134807 en la cual se describe un sistema en el que tanto el emisor como el receptor contienen una pluralidad de claves y un programa de selección de claves en el emisor y el receptor (el mismo en ambos). En este sistema el emisor selecciona un identificador de clave y cifra el mensaje a transmitir con la clave correspondiente a dicho identificador. Entonces transmite el mensaje cifrado junto con el identificador de clave sin cifrar. Una vez enviada la información anterior genera la siguiente clave. Para el proceso de descifrado, el receptor genera la primera clave a partir del identificador de clave y descifra el mensaje. A partir de este punto, genera la siguiente clave (idéntica a la del emisor). Este proceso se va repitiendo mientras queden mensajes por enviar. Las principales desventajas del sistema radican en:

- Pérdida de privacidad: Con el mismo dispositivo, y el identificador de clave que se transmite en abierto, se puede generar la misma secuencia de clave que el emisor y por lo tanto también podemos descifrar los mensajes transmitidos.

- Suplantación del Emisor: Si se tiene el mismo dispositivo, ya que el identificador de clave se transmite sin cifrar, se puede leer. Una vez hecho esto es posible generar con nuestro dispositivo la clave *Ki* y mandar el mensaje *Mi* cifrado con dicha clave en el instante *i* de la transmisión, es decir, cuando el receptor tenga generada la clave *Ki* para descifrar. Nótese que a partir del identificador de clave podemos generar la misma secuencia de claves que el receptor (y el emisor).

- Repetición de la transmisión: Podemos grabar la transmisión completa y volverla a enviar una vez que el Emisor ha terminado su transmisión. Con esto conseguimos que el receptor repita las acciones requeridas por el Emisor con el peligro que esto conlleva y mantenemos ocupado al receptor impidiendo una nueva comunicación por parte del emisor.

Descripción de la invención

La invención se refiere a unidad cifradora/descifradora de mensajes con información digital de acuerdo con las reivindicaciones 1 y a un sistema y método de cifrado/descifrado para comunicaciones digitales en tiempo real de acuerdo con las reivindicaciones 7 y 13, respectivamente. Realizaciones preferidas de la unidad, del sistema y del método se definen en las reivindicaciones dependientes.

Para solventar los problemas de seguridad comentados en lo anterior, se propone en esta invención un cifrado por palabras de la información y con las características del uso de varios alfabetos para el cifrado y eficiencia de los cifrados en flujo, es decir, a diferencia de los cifrados simétricos anteriormente comentados (DES, IDEA, AES) un mensaje es cifrado de muy distintas formas dependiendo del momento de la operación de cifrado. Dicha operación de

cifrado puede ser llevada a cabo en tiempo real teniendo de esta forma las ventajas de un cifrado en flujo. A diferencia de los cifrados en flujo susceptibles a ataques texto claro-texto cifrado mediante los que se puede obtener información sobre la secuencia cifrante, la invención propuesta utiliza un método de selección de claves que varía en función del tiempo dificultando en gran medida este tipo de ataques. Este método de selección de claves se transmite de forma cifrada dando una solución a los dos primeros problemas de seguridad comentados que plantea la patente mencionada.

Así, la invención se refiere a una unidad cifradora/descifradora de un mensaje original *M* que contiene información digital que comprende:

- medios de almacenamiento para almacenar, al menos, una tabla de *m* claves generadas de forma aleatoria,

- medios de generación de un descriptor de recorrido de dicha tabla de claves para determinar una clave seleccionada, cuyo descriptor de recorrido varía con el tiempo,

- medios de generación de una semilla aleatoria para definir un estado inicial del descriptor de recorrido,

- medios de ejecución de un algoritmo de cifrado/descifrado sobre dicha semilla y sobre dicho mensaje, incluyendo dicho algoritmo una operación XOR bit a bit con dicha clave seleccionada, para generar un segundo mensaje cifrado/no cifrado,

de forma que tanto la semilla aleatoria como el mensaje que contiene información digital son cifrados/descifrados por la unidad cifradora/descifradora de diferentes formas a lo largo del tiempo.

Preferiblemente, dichos medios de almacenamiento consisten en un dispositivo programable, como puede ser un dentro de la memoria interna de un microcontrolador o FPGA (*Field Programable Gate Array*), que permite la ejecución interna de procesos y no permite la lectura de información contenida en dicho dispositivo; más preferiblemente, en dichos medios de almacenamiento se almacena también el descriptor de recorrido.

De esta forma, el mensaje original *M* o información fuente se transforme mediante operaciones XOR palabra a palabra con una lista o tabla de claves, cuyo contenido y descriptor de recorrido (de la secuencia de recorrido) están ocultos (salvo para el administrador del sistema, que realiza la programación inicial de la unidad cifradora-descifradora).

De esta forma, la invención permite la implementación de unidades cifradoras/ descifradores independientes que, conectadas a un puerto de un computador, por ejemplo USB (Universal Serial Bus) u otro tipo de puerto de comunicaciones, o conectada a cualquier otra fuente de información que necesite ser cifrada, ofrezca un elevado grado de seguridad en la información transmitida por cualquier medio (red de computadoras, por ejemplo), imposibilitando la recuperación de la información original si no se dispone de una unidad cifradora/descifradora con las mismas claves y determinador de la secuencia de recorrido que la instalada en la fuente de información que las transmitió.

Otra posibilidad que ofrece la presente invención es la implementación dentro de unidades de comunicaciones inalámbricas como son los sistemas estándares de banda ancha, *Bluetooth, Zig-bee, IEEE 802.11a-b, radiomodem* (unidad no estándar para comunicaciones de datos vía radio usualmente de gran alcance y baja-media velocidad). En este caso, tanto los algoritmos como la lista o tabla de claves y el descriptor de secuencia de recorrido de las mismas deben albergarse en la memoria interna del microcontrolador u otro dispositivo de gobierno que todos estos sistemas incorporan, por lo tanto el sistema de cifrado coexistirá conjuntamente con los algoritmos de gobierno de las comunicaciones, y el administrador del cifrado será el proveedor o fabricante de dicha unidades de comunicaciones.

De acuerdo con un aspecto de la invención, dicho descriptor de recorrido puede comprender un generador de filtro no lineal compuesto por:

- un circuito retro-alimentado linealmente *LFSR* de longitud *K* etapas, tal que 2^K es mayor o igual que la longitud de la lista *m*, y

- una función booleana con propiedad de filtro no lineal *B* para generar, a partir de las *K* etapas del circuito retroalimentado, una secuencia pseudoaleatoria de números entre uno y la longitud de la lista *m*, determinando dicha secuencia una posición en dicha lista de claves.

En este caso, la semilla aleatoria tiene *K* bits y constituye el estado inicial del circuito retro-alimentado linealmente.

Dicha semilla aleatoria puede ser obtenida a partir de un reloj de tiempo real *RTC*.

La salida del filtro no lineal puede cifrarse/descifrarse con una o más palabras obtenidas de un reloj de tiempo real *RTC*.

La invención también se refiere a un sistema de cifrado/descifrado de información digital con objeto de una transmisión segura de dicha información. Este sistema comprende:

- un emisor,

- un receptor,

- medios de transmisión de información entre dicho emisor y dicho receptor,

- una unidad cifradora/descifradora según cualquiera de las reivindicaciones 1-6 en el emisor y en receptor,

de forma que un mensaje original *M* que contiene información digital es cifrado/descifrado por la unidad cifradora/descifradora del emisor generándose un segundo mensaje cifrado/descifrado que es transmitido al receptor, y dicho segundo mensaje cifrado/descifrado es descifrado/cifrado por la unidad cifradora/descifradora del emisor y se obteniendo dicho mensaje original *M*.

Este sistema puede incluir medios de sincronización entre el emisor y el receptor; preferiblemente determinados por el acuerdo entre unidades cifradora/descifradora del emisor y receptor de un estado inicial del circuito retroalimentado. El emisor establece un estado inicial, el cual es transmitido en forma cifrada usando la propia información del mensaje cifrado.

El sistema preferiblemente asigna a cada mensaje cifrado un tiempo de caducidad predeterminado; de esta forma se soluciona el problema de repetición de la transmisión.

Es decir, una opción que aumenta el nivel de seguridad, es el cifrado temporal. El uso de un reloj de tiempo real *RTC* añade la posibilidad de cifrado temporal, es decir, cifrado dependiente del tiempo; ello implica que si se dispone de una sincronización entre los relojes de las unidades cifradoras/descifradoras, se pueden obtener mensajes cifrados que se han de descifrar en el instante que se reciben y no es posible hacerlo con posterioridad porque en este caso se emplean códigos temporales, que sólo están vigentes en un intervalo de tiempo determinado.

Dichos-medios de transmisión de la información pueden ser inalámbricos, cable o mixto.

La invención también se refiere a un método de cifrado/descifrado de un mensaje *M* que contiene información digital que comprende las etapas de:

- generar de forma aleatoria una tabla de m claves y almacenar dicha tabla en medios de almacenamiento,

- generar una semilla aleatoria para definir un estado inicial de un descriptor de recorrido,

- generar el descriptor de recorrido de dicha tabla de claves para obtener una clave seleccionada para cada momento, cuyo descriptor de recorrido varía con el tiempo,

- ejecutar un algoritmo de cifrado/descifrado sobre dicha semilla y sobre dicho mensaje, incluyendo dicho algoritmo una operación XOR bit a bit con dicha clave seleccionada de la lista de claves por el descriptor de recorrido, generando un segundo mensaje cifrado/no cifrado,

de forma que tanto la semilla aleatoria como el mensaje que contiene información digital son cifrados/descifrados por la unidad cifradora/descifradora de diferentes formas a lo largo del tiempo.

El descriptor de recorrido genera una secuencia pseudoaleatoria de números entre uno y la longitud de la lista *m*, determinando dicha secuencia una posición en dicha lista de claves correspondiente a la clave seleccionada en cada momento.

La semilla aleatoria se puede obtener a partir de un reloj de tiempo real *RTC*.

El mensaje *M* puede cifrarse/descifrarse además con una o más palabras obtenidas de un reloj de tiempo real *RTC*.

Dicha semilla puede cifrarse con una o más palabras obtenidas de un reloj de tiempo real *RTC*.

Una de las bases de esta invención consiste, por lo tanto, en el uso de unas claves y un descriptor de recorrido, los cuales no es necesario cambiar con frecuencia, pero que sólo conoce el proveedor del sistema y que nadie más puede leer, a diferencia de otros sistemas que emplean claves mas cortas, de acceso posible y que necesariamente se han de cambiar con frecuencia.

Otra buena propiedad de este método es la rapidez de los procesos de cifrado/descifrado, dado que no se realizan operaciones computacionalmente costosas (raíces, funciones transcendentes, etc.). Además, al no aumentar el tamaño de la información al ser cifrada, la velocidad de ejecución de este algoritmo de cifrado en un microcontrolador es alta, lo cual permite la ejecución en tiempo real de este proceso de cifrado y descifrado. Es decir, que el tiempo del proceso de cifrado-descifrado es menor que el tiempo de generación o transmisión de la información.

Breve descripción de los dibujos

La figura 1 representa un diagrama de una unidad cifradora/descifradora para funcionar aisladamente.

La figura 2 representa un sistema basado en microcontrolador para el gobierno de un radiomodem de comunicaciones inalámbricas en el cual se ha implementado el sistema cifrador/descifrador de forma embebida.

La figura 3 representa un generador de filtro no lineal compuesto por un circuito retroalimentado linealmente y un circuito lógico.

La figura 4 representa la estructura de un mensaje de información.

La figura 5 representa la estructura de un paquete de información por cable.

La figura 6 representa un diagrama de flujos de la etapa de sincronización.

La figura 7 representa un diagrama de flujo de la operación de cifrado del mensaje en claro.

La figura 8 representa un diagrama de flujo de la etapa de sincronización del receptor.

La figura 9 representa un diagrama de flujos de la operación de descifrado del mensaje cifrado.

Descripción de una realización preferida de la invención

Tal y como se muestra en la figura 1, la implementación física de esta invención se puede realizar de forma aislada, es decir, mediante una unidad cifradora/descifradora 1 que realice sólo las funciones de cifrador/descifrador, destinada a ser insertada, por ejemplo, dentro de un sistema de comunicaciones PC- Internet o PC-PC y permita una comunicación con un elevado grado de seguridad, y con una certeza casi absoluta de que el que no disponga de la unidad cifradora/descifradora y con las claves propias no podrá acceder a la información transmitida. En este caso, la unidad cifradora/descifradora incluye un par de puertos de entrada/salida 10, 10' por los que entra/sale la información tal y como se generó *M* (mensaje en claro) y la información tras ser cifrada *M*' (mensaje cifrado), respectivamente; así mismo incluye una unidad central de procesamiento o CPU 11, un reloj de tiempo real RTC 12 y una memoria 13, tipo ROM-Flash, para almacenamiento del algoritmo de cifrado/descifrado así como de la tabla de claves.

Otra posibilidad de implementación es un sistema embebido, es decir, almacenado en la memoria interna no volátil del elemento de control de un determinado sistema de comunicaciones, como se muestra en la figura 2, como por ejemplo, un módem para radio o radiomodem 20. En este caso el algoritmo de cifrado/descifrado, así como la tabla de claves y el polinomio que determina el recorrido de la tabla deben coexistir junto a los otros algoritmos del sistema de comunicaciones. Esta versión de la invención permite la comunicación inalámbrica segura. En esta realización también existen un reloj de tiempo real 12, una memoria 13 y una CPU que en este caso se encarga también de configurar el módem, controlar y proporcionar una seguridad en las comunicaciones vía radio. En este caso la información que contiene un mensaje cifrado *M*' llega cifrada a través de una antena 21, y a través del correspondiente trasnceptor de radio 22 llega al módem 20, ambos controlados por la CPU 11. La información descifrada *M* (mensaje en claro) sale por el correspondiente puerto.

Esta realización se implementa embebida en el microcontrolador de gobierno de un radiomodem para comunicaciones de datos por radio.

De acuerdo con una realización preferida de la invención, la lista o tabla de claves está integrada por *m* números de *n* bits generados aleatoriamente. Como se muestra en la figura 3, la secuencia de recorrido de claves se obtiene a partir de un circuito retro-alimentado linealmente (*LFSR, Linear Feedback Shift Register*) de *k* etapas (cada etapa se corresponde con un biestable lógico de un bit), con 2^k mayor o igual que *m* y una función de filtro *B* de orden *j* del mismo definida por una función booleana que produce como salida números entre 1 y *m*, siendo $j = log_2(m)$. Dicho *LFSR* vendrá determinado por un polinomio primitivo *A* de grado *k*, que asegura el recorrido por todos y cada uno de los elementos de la lista o tabla de claves en el proceso de cifrado-descifrado, ya que $2^j = k$. El conjunto del polinomio primitivo $[A_0 A_{k-1}]$ y función de filtro $[B_0 - B_{j-1}]$ junto con la tabla de claves determinan los elementos que preferiblemente permanecen ocultos en el sistema de cifrado.

Cuando se quiere cifrar un mensaje procedente de una fuente de información, es necesario una estructuración jerárquica del mismo para conseguir las propiedades de seguridad de este código, en particular, el tamaño o longitud del paquete deberá ser sustancialmente menor que el tamaño de la tabla de claves; por ejemplo, si la tabla de claves tiene un tamaño $m = 1024$ palabras, los paquetes no deberían tener un tamaño *p* mayor que 512 palabras. En primer lugar el mensaje original *M* de cualquier tamaño se fragmenta en un conjunto de *p* paquetes (P_0, P_1,....,P_{p-2}, P_{p-1}); cada uno de longitud *I* bytes, que corresponden con las estructuras que se cifran y transmiten independientemente; a su vez los paquetes se dividen en *b* bloques (B_0, B_1,..., B_{b-1}) de *q* palabras de longitud y *n* bits por palabra (véase figura 4).

Como se muestra en la figura 5, se genera un bloque cabecera de cada paquete P_i que se cifra y transmite en primer lugar, el cual contiene información de una semilla aleatoria (SL-SH), firmas del sistema (FO-F4), destino y tamaño del

paquete (IG-IU; LO-L4), denominado *Bloque Control de Transmisión* (*BCT*). Al final del paquete P_i, tras los bloques B_0, ... B_{b-1} que únicamente contienen información (correspondiente al mensaje a ser cifrado/descifrado), se incluye un bloque final BF que contiene información así como bits de comprobación de errores en la transmisión, tipo *Checksum* (suma de la cantidad de bits o bytes en una transmisión o un archivo que permite conocer si hubo alguna pérdida o modificación de información).

Una vez generado el BCT comienza la etapa de sincronización del emisor, tal y como se muestra en la figura 6 (en la que $\overline{SEMILLA}$ representa la semilla cifrada y $\overline{BCT}$ representa el cifrado de las palabras de control de la transmisión, BCT. Asimismo *SEMILLA*[*i*], $\overline{SEMILLA}$[*i*], BCT[*i*], $\overline{BCT}$[*i*] y, representan la palabra *i*-ésimo de la semilla, la semilla cifrada, *BCT* y el *BCT* cifrado respectivamente.

Se genera mediante un reloj de tiempo real *RTC* (*Real Time Clock*), un número aleatorio de *k* bits que sirven como semilla o estado inicial al *LFSR* del generador de filtro no lineal. Los estados del *LFSR* son usados para, mediante la función *B* de filtro no lineal, producir una sucesión de números pseudoaleatorios entre *1* y *m*, que indican las posiciones de la tabla cuyos contenidos mediante operación XOR con cada una de las palabras del *BCT*, producen el cifrado de *BCT*, denotado por $\overline{BCT}$, así como el resto de palabras del mensaje de texto en claro. A continuación se divide la semilla en palabras de longitud *n*, añadiendo si fuesen necesarios ceros a la izquierda de una de las palabras y mediante *k* bits predeterminados de $\overline{BCT}$ para ser usados como entrada de nuevo del *LFSR* el cual, mediante la función de filtro *B*, vuelve a producir una sucesión de posiciones de la tabla, cuyos elementos son sumados XOR con las palabras de la semilla para producir el cifrado de la semilla. El número de palabras en los que queda dividida la semilla es exactamente igual a la parte entera de *k/n*. De este modo transmitimos un primer mensaje cifrado que se corresponde con $\overline{BCT}$, donde los *k* primeros bits conforman el cifrado de la semilla usada para el cifrado del mensaje.

En la figura 7 se muestra el proceso de cifrado del mensaje original a enviar. El proceso es exactamente el mismo que el del cifrado de *BCT*, es decir, se suma XOR las palabras del mensaje bloque a bloque con los elementos de la tabla cuyas posiciones vienen determinadas por el *descriptor* de *recorrido*, usando como estado inicial del mismo la semilla (sin cifrar) transmitida en *BCT* cifrado; una vez completado el paquete, se transmite éste y se repite el proceso con el siguiente paquete, es decir generando un nuevo *BCT*, semilla etc., y así sucesivamente hasta completar todos los paquetes del mensaje.

En el caso particular de sistemas de comunicaciones inalámbricas, delante del bloque cabecera (*BCT*) se transmiten palabras de sincronismo y de firma del dispositivo hardware necesarias para poder realizar la sincronización entre unidades inalámbricas. El resto del proceso es el mismo que el anteriormente descrito. En comunicaciones inalámbricas, al tener mayores probabilidades de errores que en caso de cable, se suelen utilizar métodos de corrección directa de errores *FEC* (*Forward Error Correction*) que introducen redundancia de información para mejorar la tasa de fallos *BER* (*Bit Error Ratio*); en este caso cada bloque ya cifrado de *q* palabras incrementa su tamaño en *r* palabras de redundancia, que las genera automáticamente el algoritmo *FEC* y que se transmiten y reciben de forma transparente a la información fuente.

Cuando el receptor recibe un mensaje cifrado, comienza con su etapa de sincronización (cuyo diagrama de flujo se muestra en la figura 8). Para ello toma los *k* bits predeterminados de $\overline{BCT}$ para usarlos como entrada del *LFSR*, generando así una sucesión de posiciones de la tabla, cuyos elementos, sumados XOR con las palabras correspondientes a los *k* primeros bits de $\overline{BCT}$ nos proporcionarán la semilla del *LFSR* usada para cifrar el resto del *BCT*. Una vez obtenida dicha semilla se usa como entrada del *LFSR*, el cual, mediante la función de filtro no lineal *B*, produce una sucesión de posiciones de la tabla, cuyos elementos sumados XOR con el resto de palabras del $\overline{BCT}$ nos proporcionan el *BCT* original.

Una vez obtenido *BCT* y hechas las comprobaciones oportunas, comienza la etapa de descifrado del mensaje (mostrado en la figura 9), que sucesivamente bloque a bloque y paquete a paquete es totalmente simétrica a la etapa de cifrado, produciendo como salida el mensaje original.

Para aumentar el nivel de seguridad, existe la posibilidad de utilizar un cifrado/descifrado temporal. El procedimiento para el cifrado temporal consiste en lectura del año, mes, día, hora, minuto etc. en el *RTC*, y mediante una operación lógica generar una clave temporal de tamaño T bits, mediante la cual se modificará por operación XOR la semilla, la salida de la función de filtro no lineal *B* o directamente la información fuente al operarla XOR simultáneamente con la tabla de claves y la clave temporal.

Con el sistema y método de cifrado de la invención, si la longitud de la tabla de claves es suficiente y la elección del *descriptor* (polinomio *A* y función de filtro *B* que determinan el orden de recorrido de dicha tabla de claves) es adecuado, se proporciona un elevado grado de seguridad, ya que si la tabla y el *descriptor* son secretos, aún conociendo el algoritmo de cifrado, el único ataque posible es por "fuerza bruta", es decir, probando con todas las tablas de claves, descriptores de recorrido y semillas posibles. Dicho ataque no se puede realizar con los medios informáticos actuales debido a su coste en el tiempo.

De acuerdo con un ejemplo concreto, la memoria interna del microcontrolador contiene una lista o tabla de claves formadas por *1024* números de *8* bits generados aleatoriamente, así como un circuito retro-alimentado linealmente (*LFSR*) de *16* etapas (como puede observarse 2^{16} es mayor que *1024*), y una función de filtro del mismo definida

por una función que seleccione la salida de las diez primeras etapas del *LFSR*, produciendo de este modo, números pseudoaleatorios entre *0* y *1023* o equivalentemente entre *1* y *1024*. De los *2048* posibles circuitos retroalimentados linealmente con 16 etapas citados en la descripción, se toma el que viene dado por el polinomio primitivo $A = 1 + x + x^2 + x^8 + x^{13} + x^{15} + x^{16}$. Cuando una fuente de información, un PC por ejemplo, proporciona un determinado mensaje para ser transmitido, éste se envía al radiomodem a través del puerto *RS232, USB*, etc.; el radiomodem lo recibe mediante un proceso en el microcontrolador de gobierno y lo almacena en un buffer para transmisión. En dicho buffer el mensaje se divide en palabras de longitud fija *8*, los cuales, uno a uno, son sometidos al proceso de cifrado.

Para la sincronización del emisor se genera un grupo de palabras de control de la transmisión (*BCT*) que corresponde al bloque cabecera de cada paquete y que se cifra y transmite en primer lugar, el cual contiene la semilla aleatoria, firmas del sistema, destino y tamaño de del paquete (figura 5). Una vez generado el *BCT*, se genera, mediante un reloj en tiempo real *RTC* un número aleatorio no nulo de *16* bits que sirve como semilla o estado inicial al *LFSR* del generador de filtro no lineal. Los estados del *LFSR* son usados para, mediante la función de filtro no lineal, producir una sucesión de números pseudoaleatorios entre *1* y *1024*, que nos dan la posición de la tabla con la que sumamos XOR cada uno de las palabras del *BCT*, produciendo así el cifrado de *BCT*, denotado por $\overline{BCT}$, así como el resto de palabras del mensaje de texto en claro. A continuación dividimos la semilla en palabras de longitud *8*, y usaremos *16* bits predeterminados de $\overline{BCT}$, por ejemplo los dieciséis últimos para usarlos como entrada de nuevo del *LFSR*, el cual, mediante el filtro, vuelve a producir una sucesión de posiciones de la tabla, cuyos elementos son sumados XOR con las dos palabras de la semilla para producir el cifrado de la semilla. De este modo se transmite un primer mensaje cifrado que se corresponde con $\overline{BCT}$, donde los *16* primeros bits conforman el cifrado de la semilla usada para el cifrado del mensaje.

A continuación comienza el cifrado del mensaje original a enviar. El proceso es exactamente el mismo que el del cifrado de *BCT*, es decir, sumamos XOR las palabras de longitud 8 bits del mensaje con los elementos de la tabla cuyas posiciones vienen determinadas por el generador de filtro no lineal, usando como estado inicial del *LFSR* de dicho generador de filtro la semilla (sin cifrar) transmitida en *BCT* cifrado. Una vez obtenido el mensaje cifrado, se envía palabra a palabra a la unidad módem y se escribe la tarea de modulación junto con la orden a la radio de puesta en transmisión, enviándose al medio.

Cuando el receptor recibe un mensaje cifrado, el módem obtiene bloque a bloque la información, la cual es procesada por el algoritmo FEC en el caso de que esté implementada esta opción. El microcontrolador de gobierno escribe en un buffer de descifrado los bloques de información obtenidos del módem y libres de la redundancia del FEC. El primer bloque recibido es el *BCT* cifrado, $\overline{BCT}$, se toman los *16* bits predeterminados de $\overline{BCT}$, en este caso, los últimos *16*, para usarse como entrada del *LFSR*, generando así una sucesión de posiciones de la tabla, cuyos elementos, sumados XOR con las palabras correspondientes a los 16 primeros bits de $\overline{BCT}$ nos proporcionarán la semilla del *LFSR* usada para cifrar el resto del *BCT*. Una vez obtenida dicha semilla, se usa como entrada del *LFSR*, y usando las diez primeras etapas de dicho *LFSR* obtiene una sucesión de posiciones de la tabla, cuyos elementos sumados XOR con el resto de palabras del $\overline{BCT}$ nos proporcionan el *BCT* original.

Una vez obtenido *BCT*, se identifica que la firma corresponde a la del sistema y que la identificación del receptor es la correcta. También se obtiene del *BCT* la información relativa al número de palabras del paquete que completan la información necesaria para recibir el resto del paquete. Comienza entonces la etapa de descifrado, que es totalmente simétrica a la etapa de cifrado, produciendo como salida el mensaje original, el cual es enviado por el microcontrolador de gobierno al PC u otro elemento de lectura de la información.

De esta forma los mensajes que son enviados al radiomodem son cifrados antes de ser transmitidos y los que se reciben cifrados se descifran en el proceso de recepción.

REIVINDICACIONES

1. Una unidad cifradora/descifradora (1; 1') de un mensaje original *M* que contiene información digital que comprende:

- medios de almacenamiento (13) para almacenar, al menos, una tabla de m claves generadas de forma aleatoria,

- medios de generación de secuencias de recorrido, que varían con el tiempo, de dicha tabla de claves para determinar una clave seleccionada, mediante un descriptor de recorrido,

- medios de generación de una semilla aleatoria para definir un estado inicial del descriptor de recorrido,

- medios de ejecución de un algoritmo de cifrado/descifrado sobre dicha semilla y sobre dicho mensaje, incluyendo dicho algoritmo una operación XOR bit a bit con dicha clave seleccionada, para generar un segundo mensaje cifrado/no cifrado,

de forma que tanto la semilla aleatoria como el mensaje que contiene información digital son cifrados/descifrados por la unidad cifradora/descifradora de diferentes formas a lo largo del tiempo.

2. Unidad cifradora/descifradora según la reivindicación 1, **caracterizada** porque dicho descriptor de recorrido comprende un generador de filtro no lineal compuesto por:

- un circuito retro-alimentado linealmente (LFSR) de longitud *K* etapas, tal que 2^K es mayor o igual que la longitud de la lista *m*, y

- una función booleana con propiedad de filtro no lineal (B) para generar, a partir de las *K* etapas del circuito retroalimentado, una secuencia pseudoaleatoria de números entre uno y la longitud de la lista *m*.

3. Unidad cifradora/descifradora según reivindicación 2, **caracterizada** porque dicha semilla aleatoria tiene *K* bits y constituye el estado inicial del circuito retro-alimentado linealmente.

4. Unidad cifradora/descifradora según cualquiera de las reivindicaciones anteriores, **caracterizada** porque dicha semilla aleatoria es obtenida a partir de un reloj de tiempo real *RTC*(12).

5. Unidad cifradora/descifradora según cualquiera de las reivindicaciones anteriores, **caracterizada** porque dichos medios de almacenamiento (13) consisten en un dispositivo programable que permite la ejecución interna de procesos y no permite la lectura de información contenida en dicho dispositivo.

6. Unidad cifradora/descifradora según cualquiera de las reivindicaciones anteriores, **caracterizada** porque en dichos medios de almacenamiento se almacena el descriptor de recorrido.

7. Sistema de cifrado/descifrado para comunicaciones digitales en tiempo real, que comprende

- un emisor,

- un receptor,

- medios de transmisión de información entre dicho emisor y dicho receptor,

- una unidad cifradora/descifradora (1; 1') según una cualquiera de las reivindicaciones 1-6 en emisor y en receptor,

de forma que un mensaje original *M* que contiene información digital es cifrado/descifrado por la unidad cifradora/descifradora del emisor generándose un segundo mensaje cifrado/descifrado *M*' que es transmitido al receptor, y dicho segundo mensaje cifrado/descifrado es descifrado/cifrado por la unidad cifradora/descifradora del receptor y se obteniendo dicho mensaje original *M*.

8. Sistema de cifrado/descifrado según la reivindicación 7, **caracterizado** porque incluye medios de sincronización entre el emisor y el receptor.

9. Sistema de cifrado/descifrado según la reivindicación 8, **caracterizado** porque dichos medios de sincronización están determinado por el acuerdo entre unidades cifradora/descifradora del emisor y receptor de un estado inicial del circuito retroalimentado.

10. Sistema de cifrado/descifrado según cualquiera de las reivindicaciones 7-9, **caracterizado** porque dicho segundo mensaje cifrado *M*' tiene asignado un tiempo de caducidad predeterminado.

11. Sistema de cifrado/descifrado según cualquiera de las reivindicaciones 7-10, **caracterizado** porque dichos medios de transmisión de la información son inalámbricos, cable o mixto.

12. Sistema de cifrado/descifrado según cualquiera de las reivindicaciones 7-11, **caracterizado** porque la selección de las sucesivas claves utilizadas para el cifrado-descifrado del mensaje depende de los estados previos del sistema usado para generar identificadores de claves.

13. Método de cifrado/descifrado de un mensaje *M* que contiene información digital que comprende las etapas de:

- generar de forma aleatoria una tabla de m claves y almacenar dicha tabla en medios de almacenamiento (13),

- generar una semilla aleatoria para definir un estado inicial de un descriptor de recorrido,

- generar una secuencia de recorrido de dicha tabla de claves para obtener una clave seleccionada para cada momento, donde dicha secuencia de recorrido varia con el tiempo,

- ejecutar un algoritmo de cifrado/descifrado sobre dicha semilla y sobre dicho mensaje, incluyendo dicho algoritmo una operación XOR bit a bit con dicha clave seleccionada de la lista de claves por la secuencia de recorrido, generando un segundo mensaje cifrado/no cifrado,

de forma que tanto la semilla aleatoria como el mensaje que contiene información digital son cifrados/descifrados por la unidad cifradora/descifradora de diferentes formas a lo largo del tiempo.

14. Método según la reivindicación 13, **caracterizado** porque generar dicha secuencia de recorrido comprende generar una secuencia pseudoaleatoria de números entre uno y la longitud de la lista *m*, determinando dicha secuencia una posición en dicha lista de claves correspondiente a la clave seleccionada en cada momento.

15. Método según cualquiera de las reivindicaciones 13-14, **caracterizado** porque el proceso de cifrado/descifrado se realiza en tiempo real, es decir, que el tiempo del proceso de cifrado-descifrado es menor que el tiempo de generación o transmisión de la información.

16. Método según cualquiera de las reivindicaciones 13-15, **caracterizado** porque dicha semilla aleatoria se obtiene a partir de un reloj de tiempo real *RTC*(12).

17. Método según cualquiera de las reivindicaciones 13-16, **caracterizado** porque dicho mensaje *M* se cifra/descifra además con una o más palabras obtenidas de un reloj de tiempo real *RTC*(12).

18. Método según cualquiera de las reivindicaciones 13-17, **caracterizado** porque la salida del filtro no lineal se cifra con una o más palabras obtenidas de un reloj de tiempo real *RTC*(12).

19. Método según cualquiera de las reivindicaciones 13-18, **caracterizado** porque dicha semilla se cifra con una o más palabras obtenidas de un reloj de tiempo real *RTC*(12).

20. Método según cualquiera de las reivindicaciones 13-18, **caracterizado** porque únicamente un proveedor puede actuar como administrador del sistema y conoce y puede grabar las claves en la unidades cifradora/descifradora (1) de acuerdo con cualquiera de las reivindicaciones 1-6.

21. Método según cualquiera de las reivindicaciones 13-18, **caracterizado** porque el usuario tiene la posibilidad de grabar la tabla de claves.

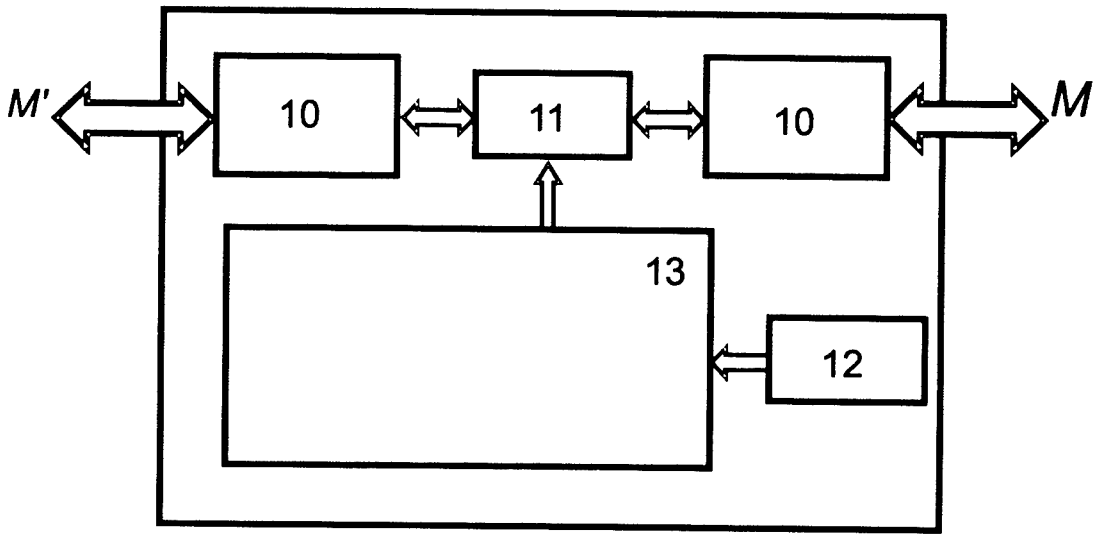

FIG. 1

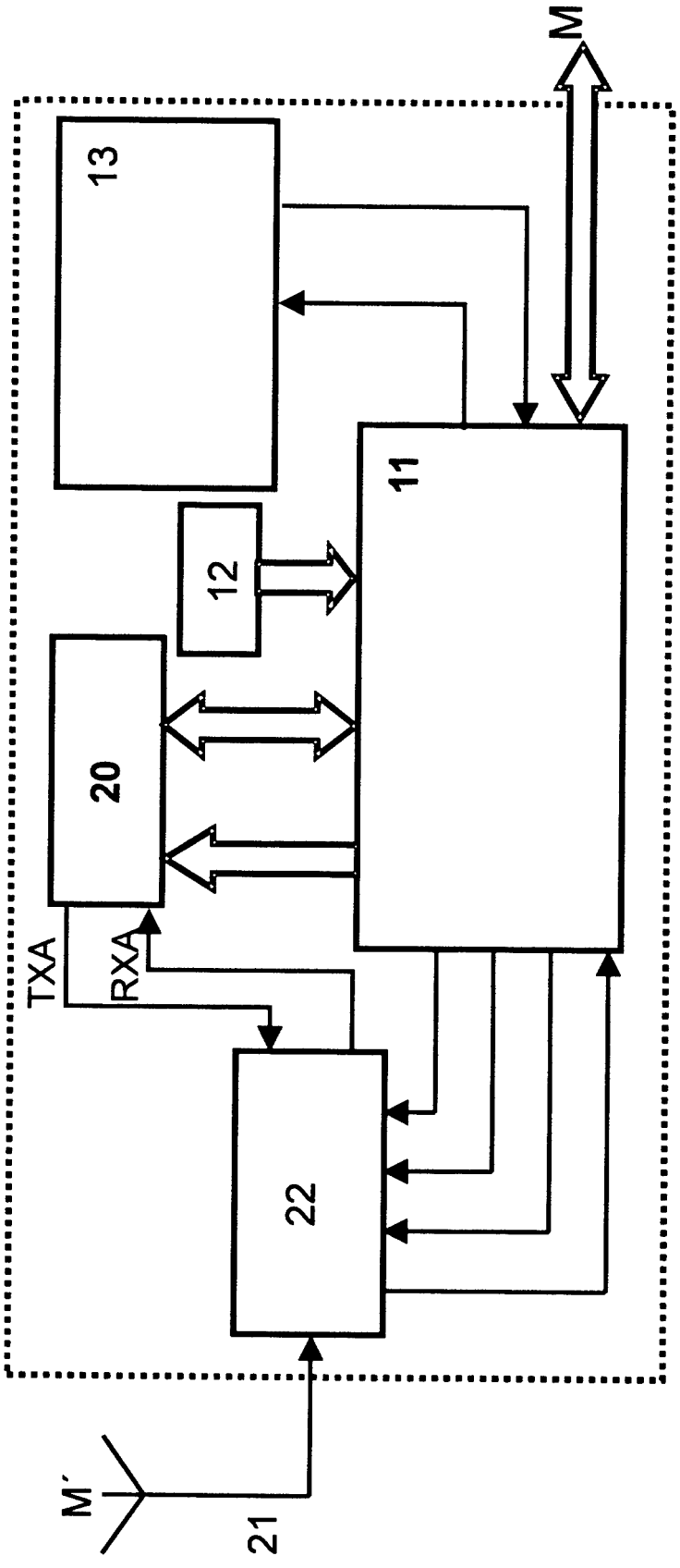

FIG. 2

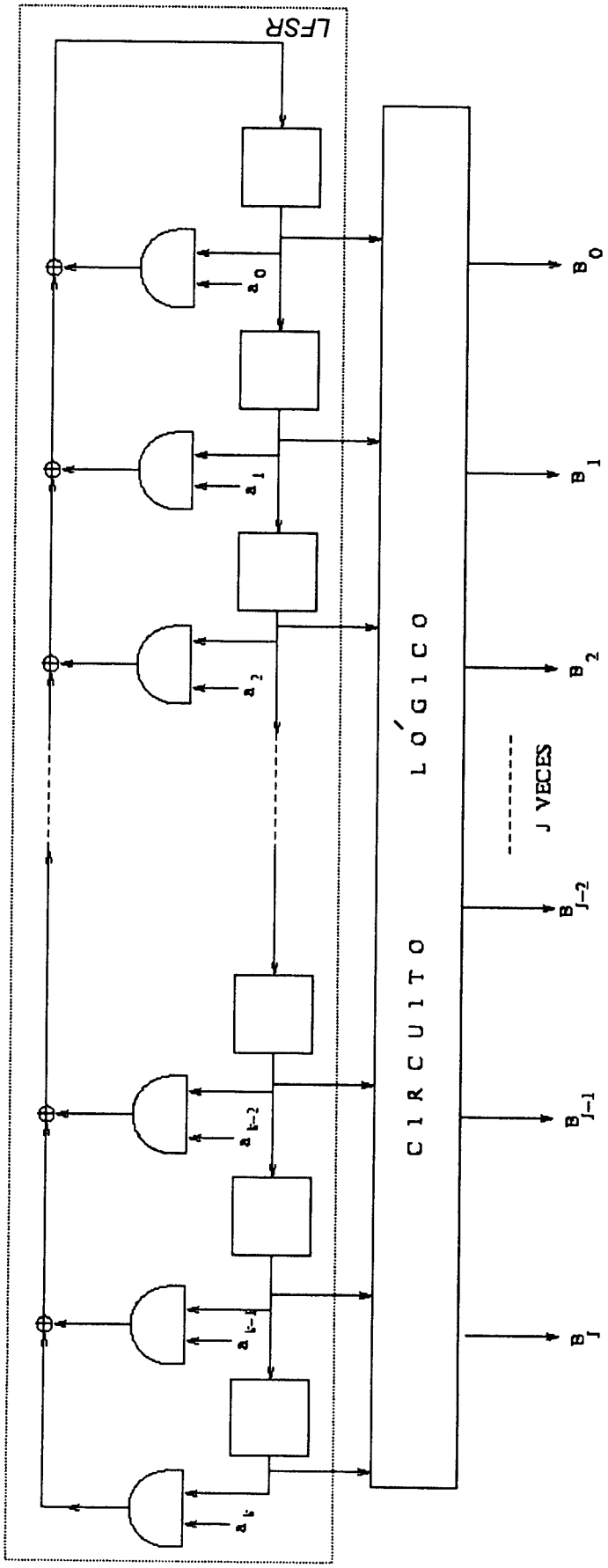
LFSR
CIRCUITO LÓGICO
J VECES
a_0
a_1
a_2
a_{k-2}
a_{k-1}
a_k
B_0
B_1
B_2
B_{J-2}
B_{J-1}
B_J

FIG. 3

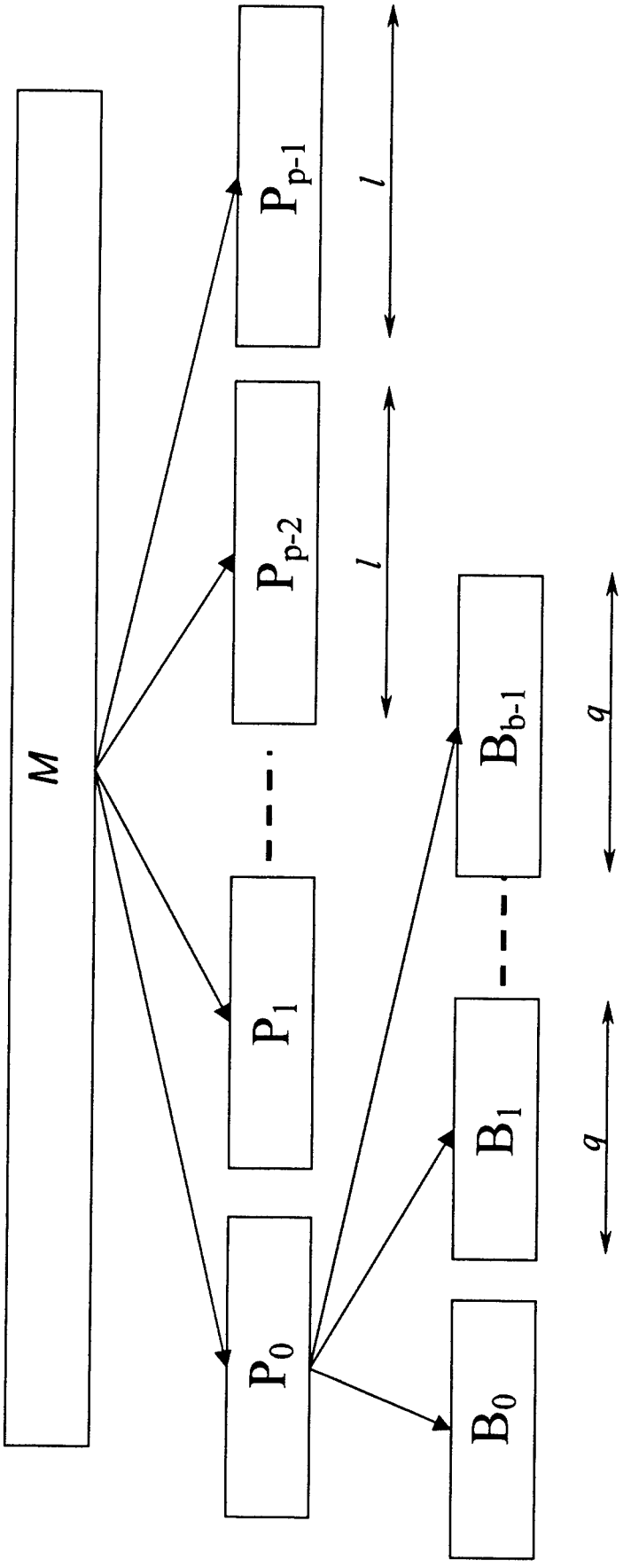

FIG. 4

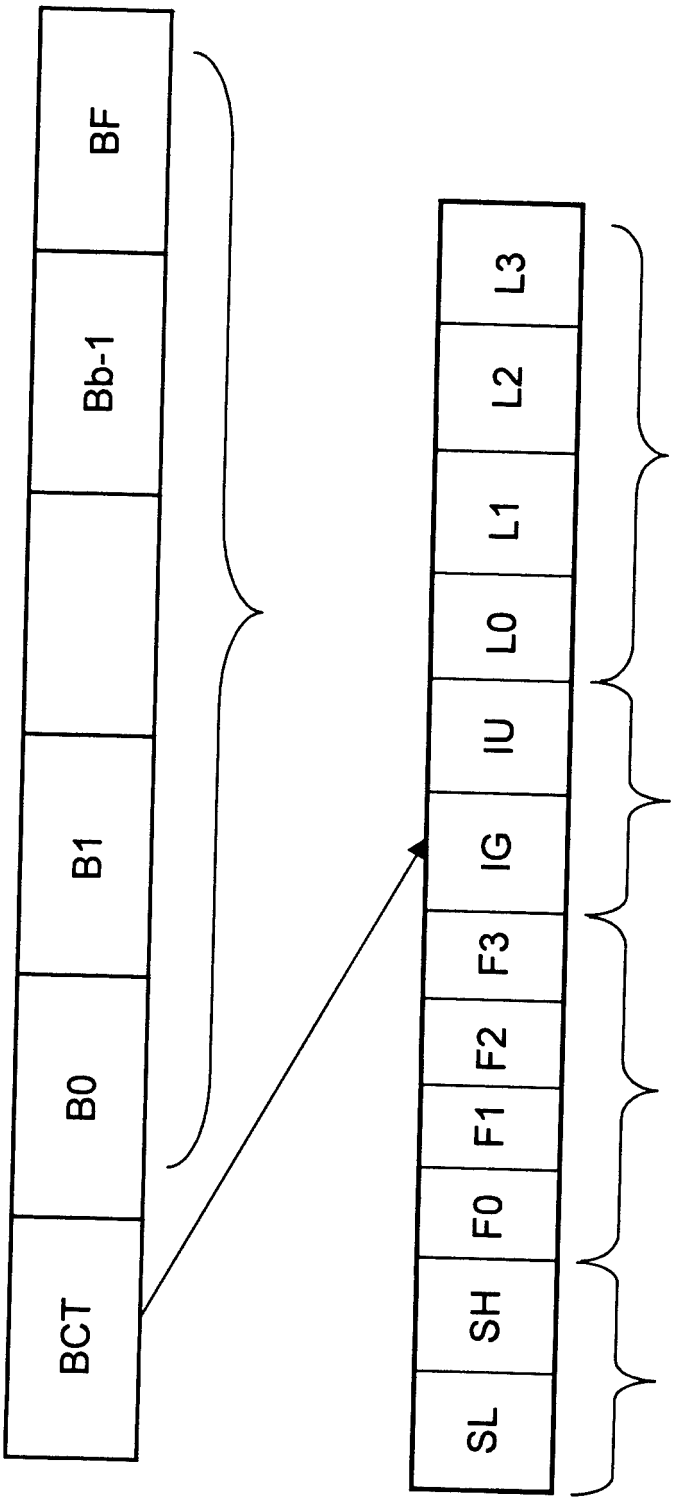

FIG. 5

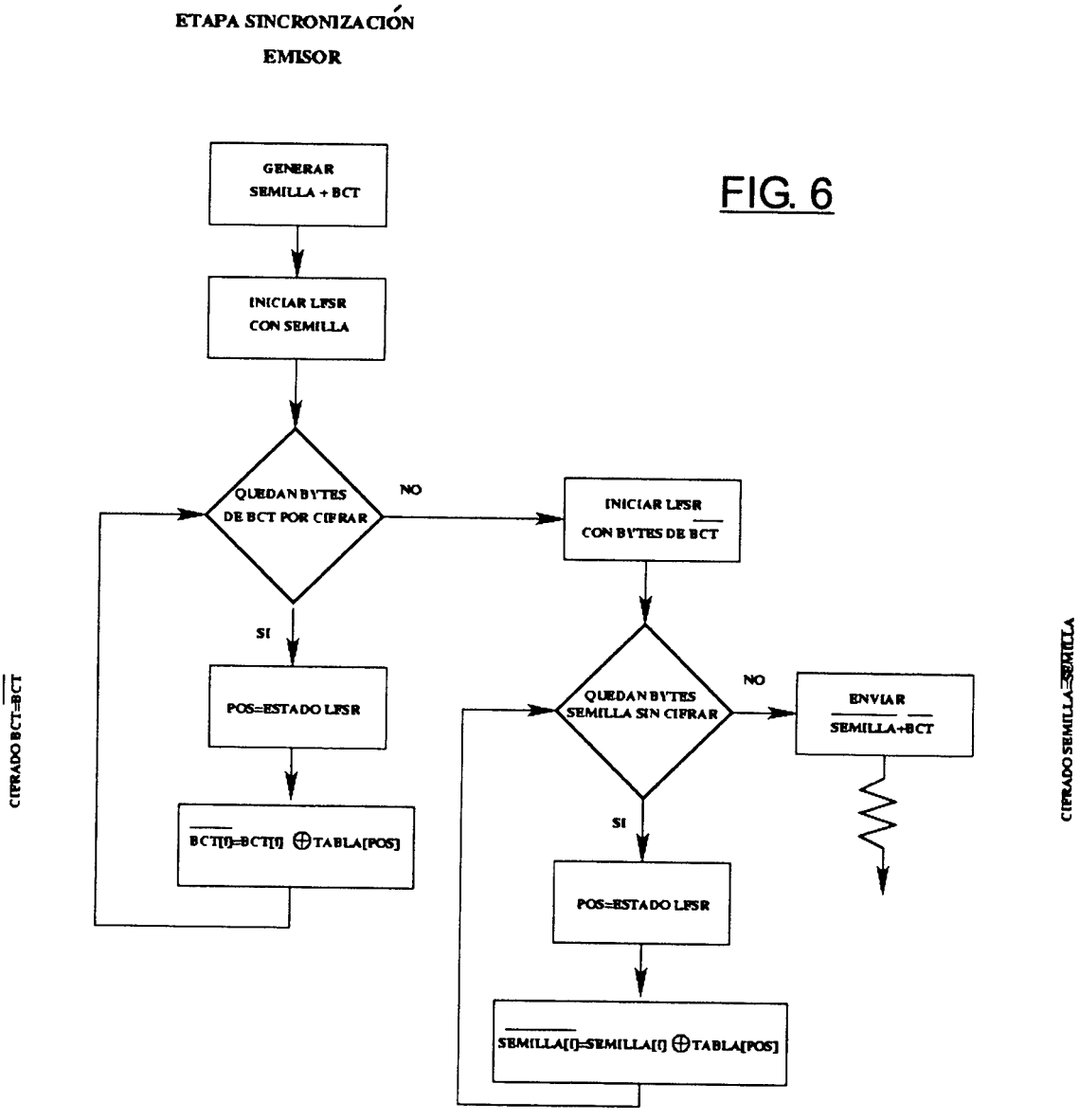
ETAPA SINCRONIZACIÓN
EMISOR
GENERAR SEMILLA + BCT
INICIAR LFSR CON SEMILLA
QUEDAN BYTES DE BCT POR CIFRAR
NO
SI
POS=ESTADO LFSR
BCT[I]=BCT[I] ⊕ TABLA[POS]
CIFRADO BCT=BCT
INICIAR LFSR CON BYTES DE BCT
QUEDAN BYTES SEMILLA SIN CIFRAR
NO
SI
ENVIAR SEMILLA+BCT
POS=ESTADO LFSR
SEMILLA[I]=SEMILLA[I] ⊕ TABLA[POS]
CIFRADO SEMILLA=SEMILLA

FIG. 6

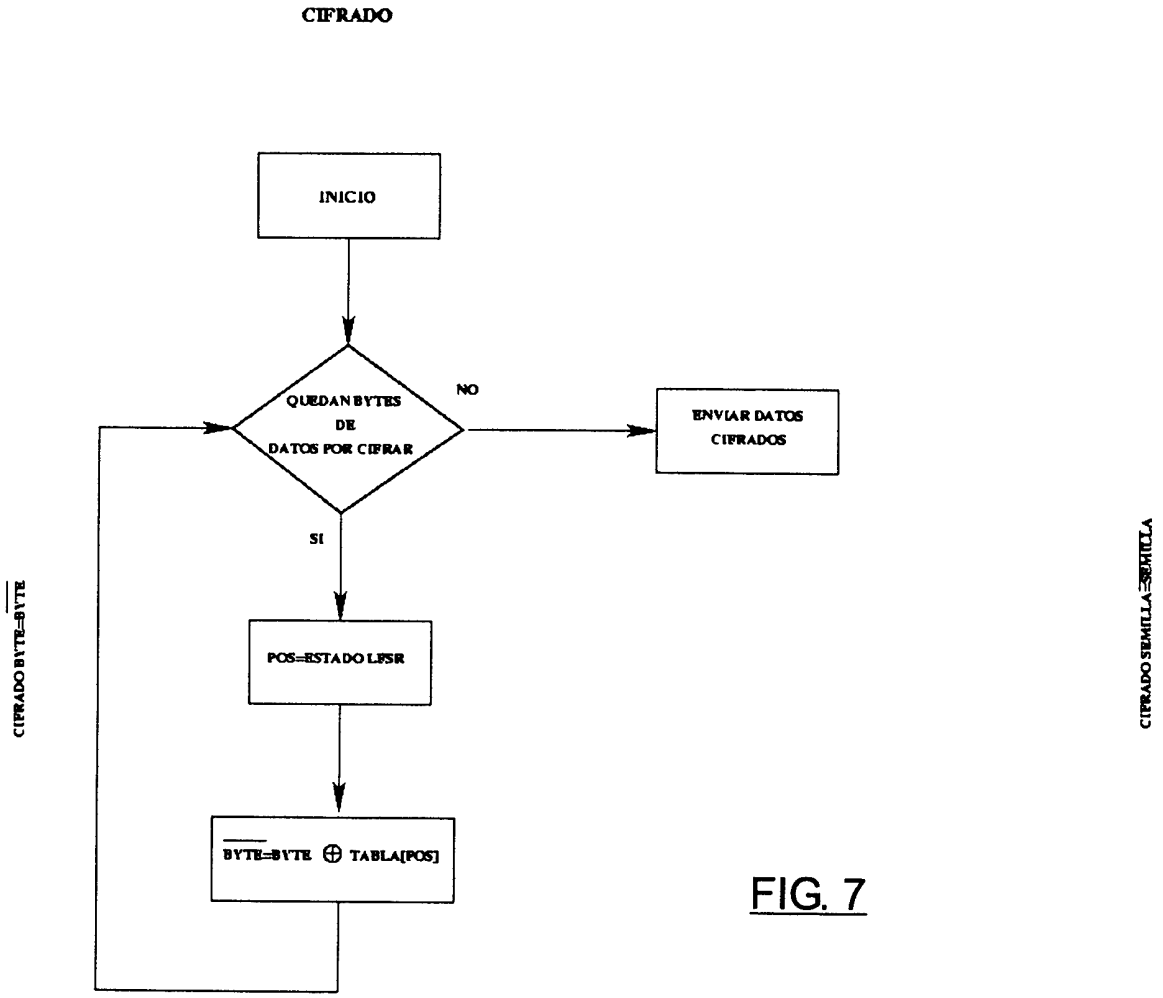
CIFRADO
INICIO
QUEDAN BYTES DE DATOS POR CIFRAR
NO
ENVIAR DATOS CIFRADOS
SI
POS=ESTADO LFSR
BYTE=BYTE ⊕ TABLA[POS]
CIFRADO BYTE=BYTE
CIFRADO SEMILLA=SEMILLA

FIG. 7

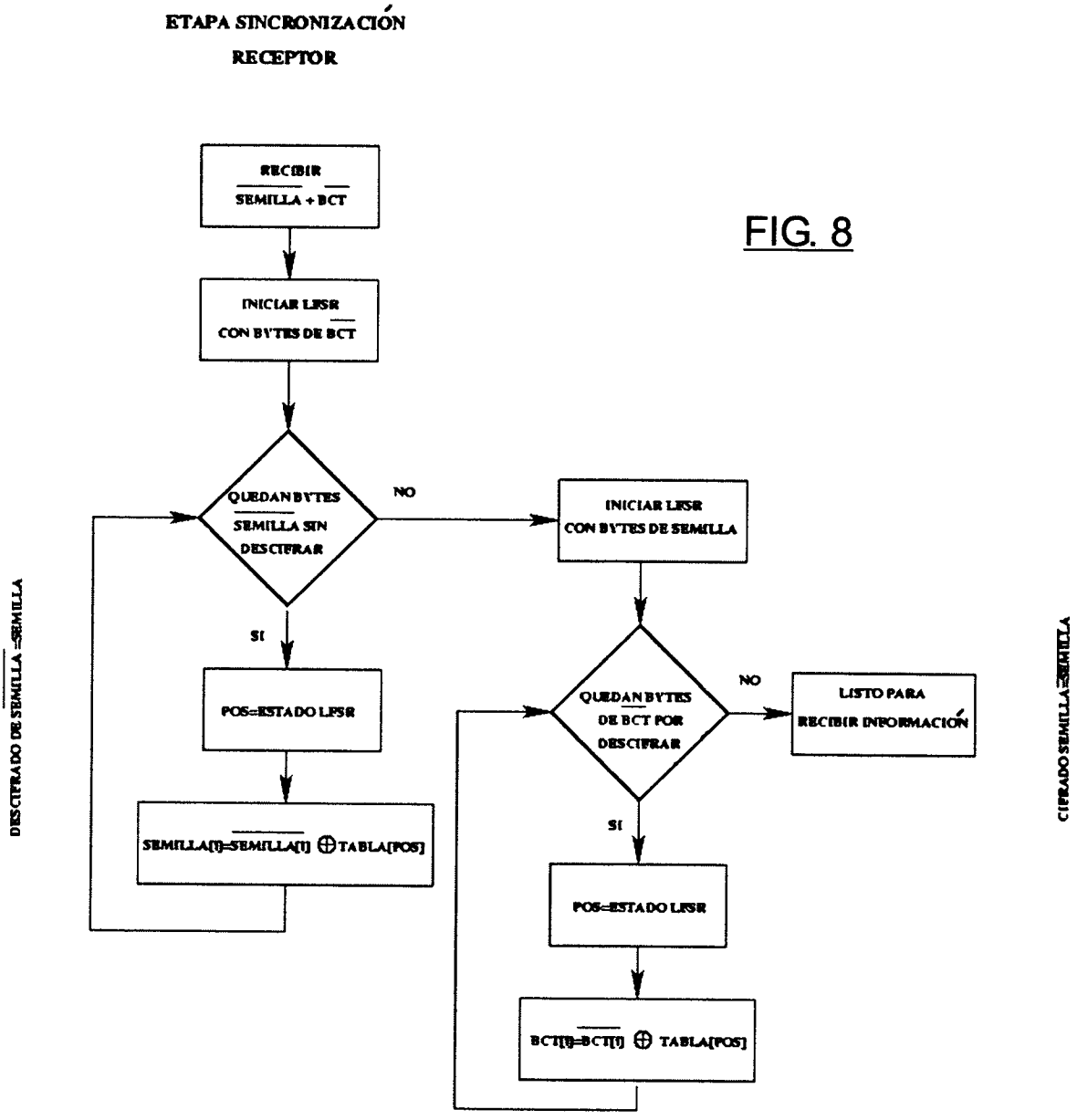
ETAPA SINCRONIZACIÓN
RECEPTOR
RECIBIR SEMILLA + BCT
INICIAR LFSR CON BYTES DE BCT
QUEDAN BYTES SEMILLA SIN DESCIFRAR
NO
SI
INICIAR LFSR CON BYTES DE SEMILLA
POS=ESTADO LFSR
SEMILLA[I]=SEMILLA[I] ⊕ TABLA[POS]
QUEDAN BYTES DE BCT POR DESCIFRAR
NO
LISTO PARA RECIBIR INFORMACIÓN
SI
POS=ESTADO LFSR
BCT[I]=BCT[I] ⊕ TABLA[POS]
DESCIFRADO DE SEMILLA =SEMILLA
CIFRADO SEMILLA=SEMILLA

FIG. 8

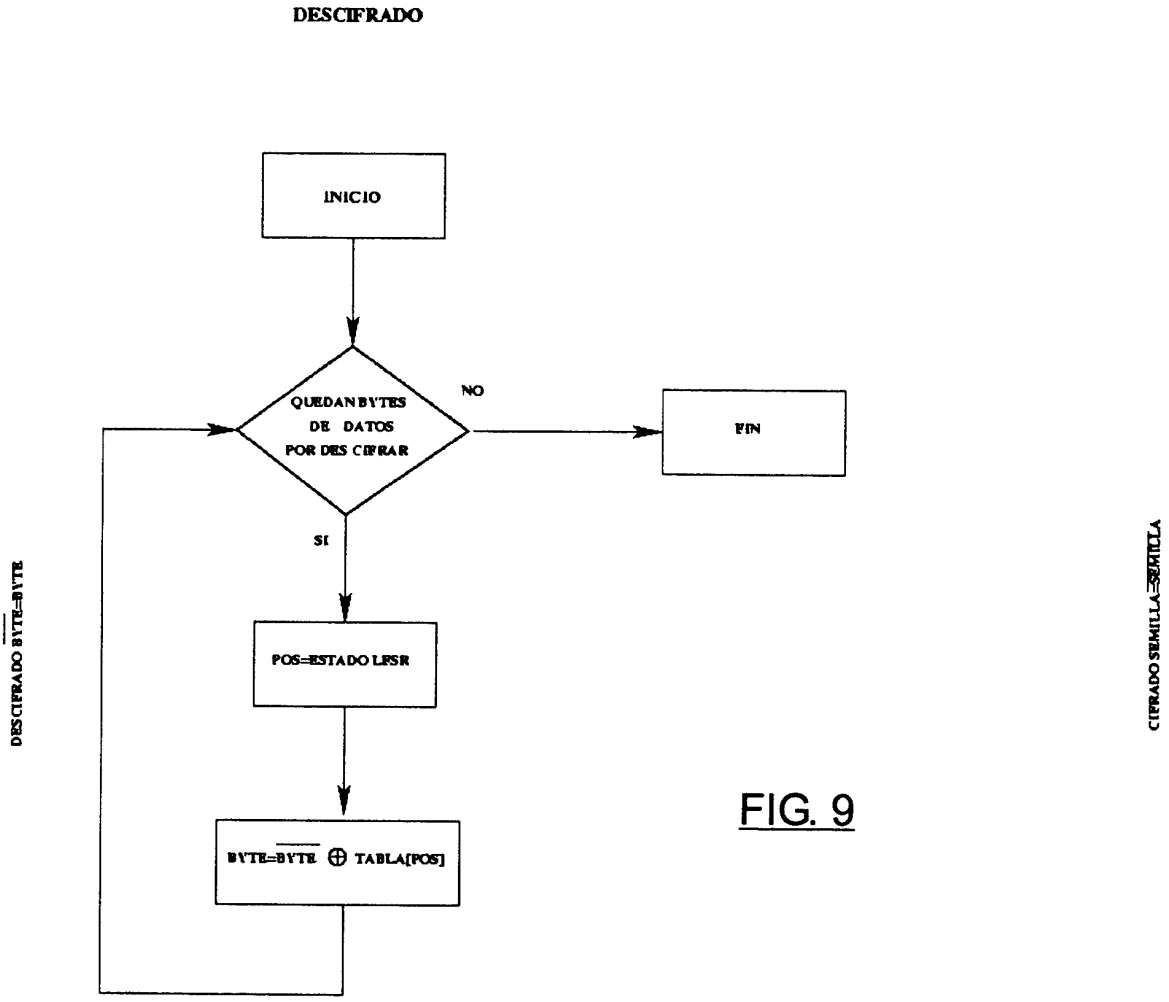
DESCIFRADO
INICIO
QUEDAN BYTES DE DATOS POR DES CIFRAR
NO
FIN
SI
POS=ESTADO LFSR
BYTE=BYTE ⊕ TABLA[POS]
DESCIFRADO BYTE=BYTE
CIFRADO SEMILLA=SEMILLA

FIG. 9

OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) ES 2 272 130

(21) Nº de solicitud: 200402603

(22) Fecha de presentación de la solicitud: **28.10.2004**

(32) Fecha de prioridad:

INFORME SOBRE EL ESTADO DE LA TÉCNICA

(51) **Int. Cl.:** ***H04L 9/18*** (2006.01)

DOCUMENTOS RELEVANTES

Categoría	Documentos citados	Reivindicaciones afectadas
A	ES 2134807 T3 (MOTOROLA) 18.05.1994, todo el documento.	1-21
A	EP 0615361 A1 (HUGHES AIRCRAFT CO) 14.09.1994, todo el documento.	1,7,13
A	WO 03049363 A1 (ERICSSON TELEFON AB L M; OLROG CHRISTIAN) 12.06.2003, todo el documento.	1,7,13

Categoría de los documentos citados

X: de particular relevancia
Y: de particular relevancia combinado con otro/s de la misma categoría
A: refleja el estado de la técnica
O: referido a divulgación no escrita
P: publicado entre la fecha de prioridad y la de presentación de la solicitud
E: documento anterior, pero publicado después de la fecha de presentación de la solicitud

El presente informe ha sido realizado

☒ para todas las reivindicaciones ☐ para las reivindicaciones nº:

Fecha de realización del informe	Examinador	Página
23.03.2007	M. Alvarez Moreno	1/1