(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 556 271**

(51) Int. CI.:

***H04L 29/06*** (2006.01)
***H04W 12/02*** (2009.01)
***H04W 12/10*** (2009.01)
***G06F 21/00*** (2013.01)
***H04W 88/00*** (2009.01)
***H04L 9/32*** (2006.01)
***G06F 21/60*** (2013.01)
***G06F 21/10*** (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **17.03.2009 E 09789522 (1)**

(97) Fecha y número de publicación de la concesión europea: **14.10.2015 EP 2377288**

(54) Título: **Procedimiento y aparato para transmitir y recibir datos protegidos y datos no protegidos**

(30) Prioridad:

**22.08.2008 US 91292 P**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
**14.01.2016**

(73) Titular/es:

**QUALCOMM INCORPORATED (100.0%)**
**International IP Administration 5775 Morehouse Drive**
**San Diego, California 92121-1714, US**

(72) Inventor/es:

**DHANDA, MUNGAL S. y**
**WALKE, SIMON**

(74) Agente/Representante:

**FORTEA LAGUNA, Juan José**

## DESCRIPCIÓN

Procedimiento y aparato para transmitir y recibir datos protegidos y datos no protegidos

**Antecedentes**

La invención se refiere a un procedimiento y un aparato para transmitir y recibir datos protegidos y datos no protegidos. Los datos protegidos se cifran para generar datos protegidos cifrados para su transmisión.

En sistemas de comunicaciones que requieren privacidad de datos para un usuario del sistema, las señales se cifran antes de transmitirse y son recibidas y descifradas por el equipo del usuario. Por ejemplo, datos de Internet, tal como el flujo continuo de voz o vídeo, se cifran para impedir que un usuario no autorizado de Internet acceda a los datos. En un sistema celular de comunicaciones inalámbricas, las señales de voz se cifran usando códigos de cifrado con el fin de dar privacidad a los usuarios. Las técnicas de cifrado son ampliamente conocidas y están definidas en varias normas de sistemas celulares inalámbricos. Sin embargo, en aras de un mejor entendimiento, a continuación se ofrecerá una breve explicación del cifrado.

El uso del cifrado o encriptación está ampliamente establecido en muchos tipos de sistemas de comunicaciones. El cifrado se usa para cifrar información con el fin de proporcionar mayor seguridad o confidencialidad de la información. El cifrado también impide un acceso no autorizado a la información por parte de una persona que no sea el destinatario previsto.

La información se cifra normalmente mediante un código de cifrado antes de transmitirse como datos en una señal. Un código de cifrado tiene asociada una clave de cifrado. La información cifrada solo puede obtenerse a partir de la señal transmitida usando un código de descifrado correspondiente y una clave de descifrado asociada. En algunos sistemas, la clave de cifrado es la misma que la clave de descifrado. El cifrado se usa en toda clase de aplicaciones en las que se desee seguridad en la información, por ejemplo, en comunicaciones por Internet.

Un algoritmo de cifrado reordena o cambia datos de manera que no puedan leerse o interpretarse a través de medios habituales, sino que solo puedan leerse o interpretarse usando la clave de descifrado. Solo el transmisor y el receptor saben qué clave de cifrado y qué clave de descifrado se han seleccionado para su uso por parte del transmisor y el receptor, respectivamente. En un ejemplo, los datos cifrados se obtienen mediante la suma binaria, bit a bit, de los datos de usuario y un código de cifrado o flujo de bits, generado por un algoritmo que usa la clave de cifrado.

Aunque los algoritmos de cifrado ofrecen cierto grado de seguridad, es posible descifrar un código de cifrado. Esto se consigue habitualmente entrenando, o adaptando repetidamente, un algoritmo para que realice intentos iterativos o repetidos para determinar la clave de descifrado, variando cada vez el código según el resultado del intento anterior para obtener un mejor resultado. Esto se lleva a cabo hasta que el resultado ofrezca la clave de descifrado correcta. Aunque descifrar los códigos de cifrado supone un gran esfuerzo computacional, la reciente disponibilidad de equipos informáticos baratos ha provocado que, en la actualidad, muchas personas puedan descifrar tales códigos de cifrado. Esto supone un gran riesgo para la seguridad de personas y organizaciones que necesitan enviar o recibir datos protegidos.

Los requisitos computacionales para descifrar un código de cifrado dependen, en parte, de la naturaleza de la información no cifrada antes de cifrarse. Los requisitos computacionales dependen particularmente de la aparente aleatoriedad de la información no cifrada. Por ejemplo, si la información comprende una secuencia bien definida de datos digitales que se cifran y posteriormente se envían repetidamente muchas veces en la misma señal, los requisitos computacionales son mucho menos estrictos en comparación a que si la secuencia hubiera tenido una naturaleza aleatoria o seudoaleatoria. Esto es particularmente cierto si los medios para determinar el código de cifrado conocen previamente la secuencia repetida.

Cuando se usa cifrado en sistemas inalámbricos celulares para cifrar datos para un usuario, se cifran tanto los datos de control del sistema como los datos de voz para el usuario. Los mensajes que contienen datos de control de sistema están predefinidos en el sistema y, por tanto, tienen una forma conocida y se generan en momentos conocidos. En los datos de control no hay información confidencial, privada o protegida. La información de los datos de control es solamente útil para el propio sistema y no para el usuario. Sin embargo, la información presente en las señales de voz es personal y, por lo tanto, los usuarios pueden esperar razonablemente un cierto grado de privacidad en sus conversaciones telefónicas.

La naturaleza predecible de los datos de control proporciona a los usuarios no autorizados o piratas informáticos un patrón conocido de datos en los datos cifrados, y el patrón conocido ofrece a los piratas informáticos una referencia a partir de la cual pueden determinar el código de cifrado usado y, por tanto, descifrar otras partes de los datos, incluyendo los datos privados. Por lo tanto, los piratas informáticos pueden determinar la información que necesitan con el fin de escuchar o acceder sin permiso a una conversación privada, por ejemplo. La información que va a cifrarse y enviarse en una señal debería contener, de manera idónea, poca información repetida y, más

específicamente, la señal debería contener poca información repetida que sea conocida o predecible. Esto se debe a que la información repetida puede usarse por un intruso para ajustar un algoritmo para determinar de manera no autorizada la clave de cifrado. El número de iteraciones requeridas para determinar la clave es mucho más reducido si la información transmitida contiene información repetida. Los mensajes de sistema se transmiten a muchos usuarios del sistema y tienen una secuencia de bits fija conocida.

A partir de lo anterior puede observarse que los sistemas de la técnica anterior que envían datos cifrados que contienen información predecible o conocida son mucho más vulnerables a un acceso llevado a cabo por terceras partes no autorizadas.

Se hace referencia al documento US2004/039908 A1, que describe procedimientos y aparatos para cifrar y autenticar datos, donde algunos datos se cifran y algunos datos no se cifran, pero todos los datos se autentican. Se usan módulos de enmascaramiento en un modo de cifrado de bloque parcial para indicar qué bits de un bloque de datos van a cifrarse.

Se hace referencia también al documento US2006/106802 A1, que describe un aparato y un procedimiento para permitir un acceso controlado a recursos en un servidor proveedor de recursos. Este puede cifrar o descifrar una parte de un identificador de recursos uniforme (URI), según un procedimiento sin estados para ocultar recursos y/o proporcionar soporte de control de acceso. Tras la recepción de un URI que tiene una parte cifrada se descifra la parte cifrada usando una clave predeterminada para obtener un segmento descifrado, se extrae información adicional del segmento descifrado y se forma un URI descifrado, antes de que el URI descifrado se reenvíe a un servidor proveedor de servicios. Este documento describe además el cifrado de un URI en un servidor proveedor de recursos antes de enviarse a un cliente en respuesta a una solicitud de cliente.

También se hace referencia al documento US4907275 A, que describe que en un aparato de cifrado, antes del proceso de cifrado, información que indica si bloques de texto plano van a cifrarse o no se almacena en un registro de enmascaramiento, y el número de bloques de la secuencia de bloques de texto plano se almacena en un registro de cómputo. En el proceso de cifrado, el registro de cómputo reduce su valor secuencialmente, y solo los bloques de texto plano que van a cifrarse se leen de una memoria intermedia de entrada en el orden creciente de las direcciones en función de la información almacenada en el registro de enmascaramiento. Se cifran mediante un circuito de cifrado y los bloques de texto cifrados se almacenan en una memoria intermedia de salida en las direcciones correspondientes a las direcciones de la memoria intermedia de entrada en las que se han almacenado los bloques de texto plano. Después del proceso de cifrado de los bloques de texto plano que van a cifrarse, solo los bloques de texto plano que no van a cifrarse se leen secuencialmente de la memoria intermedia de entrada en el orden creciente de las direcciones y se almacenan, sin cifrar, en la memoria intermedia de salida en las direcciones correspondientes a las direcciones de memoria intermedia de entrada en las que se han almacenado los bloques de texto plano.

Se hace referencia a la publicación "*Universal Mobile Telecommunications System (UMTS); 3G security; Security architecture (3GPP TS 33.102 version 7.1.0 Release 7); ETSI TS 133 102*" NORMAS DEL ETSI, LIS, SOPHIA ANTIPOLIS CEDEX, FRANCIA, vol. 3-SA3, n.º V7.1.0, 1 de diciembre de 2006 (01/12/2006), ISSN: 0000-0001.
Resumen de la invención

Según la presente invención se proporcionan procedimientos, aparatos y un producto de programa informático como se expone en las reivindicaciones independientes. Realizaciones preferidas de la invención se describen en las reivindicaciones dependientes.

Características adicionales de la invención se describen posteriormente de manera particular en las reivindicaciones adjuntas y, junto con las ventajas de las mismas, resultarán más evidentes tras considerar la siguiente descripción detallada de realizaciones de la invención, que se proporcionan a modo de ejemplo con referencia a los dibujos adjuntos.

**Breve descripción de los dibujos**

La Figura 1 es un diagrama esquemático de un sistema de comunicaciones para transmitir y recibir datos protegidos y datos no protegidos.

La Figura 2 es un diagrama esquemático de un validador para el sistema de la Figura 1 para validar datos en serie.

La Figura 3 es un diagrama esquemático de un validador para el sistema de la Figura 1 para validar datos en paralelo.

La Figura 4 es un diagrama de flujo que ilustra un procedimiento para transmitir y recibir datos protegidos y datos no protegidos.

La Figura 5 es un diagrama esquemático de un aparato de recepción.

La Figura 6 es un diagrama esquemático de un primer aparato de transmisión.

La Figura 7 es un diagrama de flujo que ilustra un procedimiento para transmitir, o no transmitir, datos protegidos y datos no protegidos.

La Figura 8 es un diagrama esquemático de un segundo aparato de transmisión que puede cifrar datos protegidos y datos no protegidos.

La Figura 9 es un diagrama de flujo que ilustra un procedimiento para transmitir datos protegidos y datos no protegidos.

La Figura 10 es un diagrama de un sistema de comunicaciones celular.

La Figura 11 es un diagrama de flujo que ilustra un procedimiento para establecer un enlace de comunicaciones cifrado.

La Figura 12 es un diagrama de flujo que ilustra un procedimiento para la autenticación de un abonado.

La Figura 13 es un diagrama de flujo que ilustra un procedimiento para tratar datos recibidos cifrados y no cifrados.

La Figura 14 es un diagrama de flujo que ilustra un procedimiento para enviar datos cifrados y/o datos no cifrados que puede llevarse a cabo en un equipo de infraestructura de red.

La Figura 15 es un diagrama esquemático de una parte de un receptor.

La Figura 16 es un diagrama de flujo que ilustra un procedimiento en el que datos protegidos y datos no protegidos se transmiten desde una estación base y se reciben por una estación remota.

La Figura 17 es un diagrama de flujo que ilustra un procedimiento en el que datos protegidos y datos no protegidos se transmiten desde una estación remota y se reciben por una estación base.

La Figura 18 es un diagrama de flujo que ilustra un procedimiento para recibir y descodificar datos.

La Figura 19 es un diagrama de flujo que ilustra otro procedimiento para recibir y descodificar datos.

La Figura 20 es un diagrama de flujo que ilustra un procedimiento adicional para recibir y descodificar datos.

**Descripción detallada de realizaciones de la invención**

La Figura 1 es un diagrama esquemático de un sistema de comunicaciones para transmitir y recibir datos protegidos y datos no protegidos. El sistema de comunicaciones 1100 comprende un aparato de transmisión 120 y un aparato de recepción 130. El aparato de transmisión 120 comprende una fuente de datos protegidos 101, un dispositivo de cifrado 103 acoplado a la misma y un primer transmisor 104 acoplado al dispositivo de cifrado103 y a una fuente de datos no protegidos 102. El dispositivo de cifrado 103 cifra los datos protegidos para generar datos protegidos cifrados y proporciona los datos protegidos cifrados al transmisor 104. La fuente de datos no protegidos 101 proporciona datos no protegidos al primer transmisor 104. El primer transmisor 104 transmite los datos protegidos cifrados y los datos no protegidos. En lo sucesivo, cuando se utilice el término "datos de modo mixto" en la descripción, se hará referencia a datos que comprenden datos cifrados y datos no cifrados.

El aparato de recepción 130 comprende un primer receptor 105, un dispositivo de descifrado 106 acoplado al primer receptor 105 y un validador 107 acoplado al dispositivo de descifrado 106 y al primer receptor 105. El primer receptor 105 recibe datos transmitidos por el primer transmisor 104 y proporciona los datos recibidos al dispositivo de descifrado 106 y/o al validador. El dispositivo de descifrado 106 descifra los datos recibidos para generar datos descifrados 108 y proporciona los datos descifrados 108 al validador 107.

Por tanto, el aparato de recepción 130 puede recibir, descifrar y validar los datos transmitidos. Sin embargo, el aparato de recepción también puede validar los datos recibidos sin descifrarlos, permitiendo así tratar datos no cifrados junto con datos cifrados. El validador tiene tres modos de funcionamiento. El primer modo es para tratar datos cifrados. El segundo modo es para tratar datos no cifrados, y el tercer modo es para tratar datos que comprenden datos cifrados y datos no cifrados.

El aparato de recepción 130 puede hacerse funcionar, en el primer modo de funcionamiento, para descifrar los datos

recibidos, para validar los datos descifrados con el fin de generar un primer resultado de validación y para proporcionar los datos descifrados en función del primer resultado de validación. El aparato de recepción 130 puede hacerse funcionar, en el segundo modo de funcionamiento, para validar los datos recibidos con el fin de generar un segundo resultado de validación y para proporcionar los datos recibidos en función del segundo resultado de validación. El aparato de recepción 130 puede hacerse funcionar, en el tercer modo de funcionamiento, para descifrar los datos recibidos 109 para generar datos descifrados 108, para validar los datos descifrados 108 con el fin de generar un primer resultado de validación 110 y para proporcionar los datos descifrados 108 como datos validados 111 en función del primer resultado de validación, y también para validar los datos recibidos 109 con el fin de generar un segundo resultado de validación y para proporcionar los datos recibidos en función del segundo resultado de validación. Por tanto, el tercer modo comprende el primer y el segundo modo. A continuación se describirán en detalle aparatos y procedimientos que usan las características anteriores.

La Figura 2 es un diagrama esquemático de un validador para el sistema de la Figura 1 para validar datos en serie. Los datos descifrados 201 y los datos recibidos 202 se introducen en un conmutador 203. El conmutador funciona según el primer modo descrito anteriormente para transferir los datos descifrados 201 como datos de entrada 206 a una función de validación 204. El conmutador también funciona según el segundo modo descrito anteriormente para transferir los datos recibidos 202 como datos de entrada 206 a la función de validación 204. La función de validación 204 puede hacerse funcionar para validar sus datos de entrada 206 para determinar si los datos de entrada son válidos. Por ejemplo, si los datos de entrada contienen más de un porcentaje de errores especificado, el validador determina que los datos de entrada no son válidos y genera un resultado de validación 205 que indica que los datos no son válidos. Si la determinación es que los datos de entrada son válidos, el validador genera un resultado de validación 205 que indica que los datos son válidos. El validador también proporciona los datos de entrada validados como datos validados 207. Opcionalmente, los datos de entrada 206, si se han validado, pueden usarse directamente como datos validados 207. El validador puede ser parte de un descodificador que descodifica los datos descifrados 201 o los datos recibidos 202.

En el primer modo, con el conmutador en la posición para transferir los datos descifrados como se muestra en la Figura 2, la función de validación sirve para validar los datos descifrados 201 y para generar un primer resultado de validación 205. En el segundo modo, no mostrado en la Figura 2, con el conmutador en la posición para transferir los datos recibidos, la función de validación sirve para validar los datos recibidos y para generar un segundo resultado de validación. En el tercer modo, el validador funciona tanto en el primer como en el segundo modo. Puede observarse que, como se muestra en la Figura 2, el validador funciona según el primer o el segundo modo en cualquier momento.

La Figura 3 es un diagrama esquemático de un validador para el sistema de la Figura 1 para validar datos en paralelo. Datos descifrados 301 y datos recibidos 302 se introducen en paralelo en la función de validación 303 y en la función de validación 304, respectivamente. La función de validación 303 y la función de validación 304 pueden considerarse parte de una única función de validación. La función de validación 303 funciona para validar los datos descifrados 301 para generar un primer resultado de validación 305 y datos descifrados validados, y la función de validación 304 funciona para validar los datos recibidos 302 para generar un segundo resultado de validación 306 y datos recibidos validados 308.

La Figura 4 es un diagrama de flujo que ilustra un procedimiento para transmitir y recibir datos protegidos y datos no protegidos, por ejemplo en el aparato de la Figura 1. En el bloque 701 se proporcionan datos protegidos y en el bloque 702 se proporcionan datos no protegidos. En el bloque 703 se cifran los datos protegidos para generar datos protegidos cifrados. En el bloque 704 se transmiten los datos protegidos cifrados y los datos no protegidos.

En el bloque 705, los datos transmitidos se reciben como datos recibidos. En el bloque 706 se descifran los datos recibidos para generar datos descifrados. En el bloque 707 se validan los datos descifrados para generar un primer resultado de validación. El resultado de validación indica si los datos son válidos o no. En el bloque 708 se proporcionan dos resultados diferentes dependiendo de si los datos descifrados son válidos o no. Si los datos descifrados son válidos, los datos descifrados se proporcionan en el bloque 709. Sin embargo, si los datos descifrados no son válidos, los datos descifrados no se proporcionan, como se representa mediante el bloque 710.

En el bloque 711 se validan los datos recibidos para generar un segundo resultado de validación. Los datos recibidos se proporcionan, o no se proporcionan, dependiendo del segundo resultado de validación, como se muestra en los bloques 712, 713 y 714. En un ejemplo, como se indica mediante la línea discontinua 715, los datos recibidos solo se validan en el bloque 711 siempre que se haya obtenido el primer resultado de validación, indicando el resultado de validación que los datos descifrados no son válidos. Por lo tanto, en este ejemplo, la validación de los datos descifrados y la validación de los datos recibidos se llevan a cabo en serie, una después de la otra. Una ventaja del procesamiento en serie es que no se necesario realizar la segunda validación 711 si la primera validación (bloque 707) da como resultado datos válidos (bloques 708, 709). El aparato mostrado en la Figura 2 puede usarse para el procesamiento en serie, por ejemplo. En otro ejemplo, los datos recibidos y los datos descifrados se validan en paralelo, como se indica mediante la supresión de la línea discontinua 715. Una ventaja del procesamiento en paralelo es que puede ser más rápido que el procesamiento en serie. El aparato de la Figura 3 puede usarse para el procesamiento en paralelo, por ejemplo.

El primer y el segundo resultado de validación son potencialmente útiles para el sistema, ya que proporcionan una indicación de si el aparato de recepción ha recibido los datos transmitidos y ha determinado que son válidos. Por ejemplo, en función de los resultados de validación, puede decidirse si retransmitir datos que el aparato de recepción ha determinado que no son válidos. Por lo tanto, es potencialmente útil que el aparato de recepción proporcione una señal de indicación, que indica si el aparato de recepción ha recibido los datos transmitidos y ha determinado que son válidos.

También es útil proporcionar una indicación al aparato de transmisión acerca de si el aparato de recepción puede tratar datos cifrados y datos no cifrados. En los sistemas de comunicaciones actuales, los aparatos de transmisión no tienen modo alguno de saber si el aparato de recepción puede tratar datos cifrados y datos no cifrados. Si la indicación puede proporcionarse al aparato de transmisión, el aparato de transmisión puede hacerse funcionar para transmitir datos de modo mixto, dependiendo de la indicación.

En vista de lo anterior, a continuación se describirá un aparato para proporcionar, en primer lugar, una indicación de si el aparato de recepción ha recibido los datos transmitidos y ha determinado que son válidos, y, en segundo lugar, una indicación de si el aparato de recepción puede tratar datos que comprenden datos cifrados y datos no cifrados.

La Figura 5 es un diagrama esquemático de un aparato de recepción 1000. Un receptor 1002 recibe una señal que comprende datos 1001 y proporciona datos recibidos a un dispositivo de descifrado 1003 acoplado al receptor. El dispositivo de descifrado 1003 puede hacerse funcionar para descifrar los datos recibidos para generar datos descifrados, y para proporcionar los datos descifrados a un validador 1004 acoplado al dispositivo de descifrado y al receptor. El validador 1004 puede hacerse funcionar, en un primer modo de funcionamiento, para validar los datos descifrados 1015 con el fin de generar un primer resultado de validación 1031 y para proporcionar los datos descifrados 1030 en función del primer resultado de validación. El validador 1004 puede hacerse funcionar, en un segundo modo de funcionamiento, para validar los datos recibidos 1016 con el fin de generar un segundo resultado de validación y para proporcionar los datos recibidos validados 1030 en función del segundo resultado de validación. El validador 1004 puede hacerse funcionar, en un tercer modo de funcionamiento, para validar los datos descifrados con el fin de generar un primer resultado de validación y para proporcionar los datos descifrados en función del primer resultado de validación, y también para validar los datos recibidos con el fin de generar un segundo resultado de validación y para proporcionar los datos recibidos en función del segundo resultado de validación. Por tanto, en el tercer modo, el validador funciona tanto en el primer como en el segundo modo.

Un primer dispositivo indicador 1005 está acoplado al validador 1004 y puede hacerse funcionar para proporcionar una primera señal de indicación. La señal comprende una indicación del primer y/o del segundo resultado de validación, por lo que la señal comprende una indicación de si el aparato de recepción ha recibido los datos transmitidos y ha determinado que son válidos. Un transmisor 1006 está acoplado al dispositivo indicador y puede hacerse funcionar para transmitir la primera señal de indicación 1020.

La señal de indicación 1020 puede usarse, adicionalmente o como alternativa, por el sistema para proporcionar una indicación de si el aparato de recepción puede tratar datos que comprenden datos cifrados y datos no cifrados. Por ejemplo, el aparato de transmisión puede transmitir un flujo de datos de prueba de modo mixto (que comprende datos cifrados y datos no cifrados). El aparato de recepción recibirá después en el receptor 1002 los datos de prueba transmitidos 1001 y, dependiendo de la validación de los datos de prueba en el validador 1004, transmitirá la primera señal de indicación 1020, que puede comprender una indicación CRC. El aparato de transmisión o bien transmitirá datos de modo mixto o transmitirá todos los datos cifrados, dependiendo de la primera señal de indicación 1020.

Un segundo dispositivo indicador 1007, acoplado a un microprocesador 1009, puede hacerse funcionar para proporcionar una segunda señal de indicación 1021 que comprende una indicación de si el aparato de recepción 1000 puede tratar datos que comprenden datos cifrados y datos no cifrados. Un segundo transmisor 1008 está acoplado al segundo dispositivo indicador y puede hacerse funcionar para transmitir la segunda señal de indicación 1021.

El microprocesador 1009 está acoplado a, y controla el funcionamiento de, el receptor 1002, el dispositivo de descifrado 1003, el validador 1004, el primer dispositivo indicador 1005, el primer transmisor 1006, el segundo dispositivo indicador 1007 y el segundo transmisor 1008, según datos almacenados en la memoria 1010.

El microprocesador 1009 puede hacerse funcionar para generar un mensaje y para proporcionar el mensaje al dispositivo indicador 1007 para que el mensaje pueda transmitirse por el transmisor 1008. El mensaje puede ser un mensaje de indicación de capacidad, que indica si el aparato de recepción 1000 puede tratar datos que comprenden datos cifrados y datos no cifrados. Por ejemplo, el aparato de recepción puede recibir un mensaje desde el aparato de transmisión 120 de la Figura 1, que solicita una indicación de si el aparato de recepción puede tratar datos que comprenden datos cifrados y datos no cifrados. El aparato de recepción responde transmitiendo una segunda señal de indicación, que indica si el aparato de recepción puede tratar datos que comprenden datos cifrados y datos no cifrados. El aparato de transmisión o bien envía datos de modo mixto o envía todos los datos cifrados, dependiendo de la indicación.

La Figura 6 es un diagrama esquemático de un primer aparato de transmisión 500, que corresponde al aparato de transmisión 120 de la Figura 1. El aparato de transmisión 500 incluye una fuente de datos protegidos 501 que proporciona datos protegidos a un dispositivo de cifrado 503 acoplado a la fuente de datos protegidos 501. El dispositivo de cifrado 503 cifra los datos protegidos para generar datos protegidos cifrados y proporciona los datos protegidos cifrados a un primer transmisor 504, acoplado al dispositivo de cifrado 503 y a una fuente de datos no protegidos 502. La fuente de datos no protegidos 502 proporciona datos no protegidos al primer transmisor 504. El primer transmisor 504 transmite los datos protegidos cifrados y los datos no protegidos.

El aparato de transmisión 500 comprende además un segundo receptor 510 para recibir una señal de indicación 512 que comprende una indicación de si transmitir datos protegidos cifrados y datos no protegidos no cifrados. El receptor 510 proporciona la indicación a un microprocesador 507 acoplado al receptor 510 y al transmisor 504. La señal de indicación 512 puede ser, por ejemplo, la señal de indicación 1020 mostrada en la Figura 5, comprendiendo la señal 512 una indicación de si el aparato de recepción puede tratar datos de modo mixto. En este ejemplo, el aparato de transmisión está adaptado para interpretar que la señal de indicación 512 comprende una indicación de si transmitir datos protegidos cifrados y datos no protegidos no cifrados. El microprocesador 507 interpreta la indicación recibida 520 y controla el primer transmisor 504 según la indicación. El primer transmisor 504 puede hacerse funcionar para transmitir datos protegidos cifrados y datos no protegidos no cifrados si la indicación 512 es para transmitir datos de modo mixto.

La segunda señal de indicación 1021 ilustrada en la Figura 5 puede comprender un mensaje de respuesta que se genera en respuesta a un mensaje de solicitud transmitido por el aparato de transmisión y recibido por el aparato de recepción. Por ejemplo, el aparato de transmisión puede transmitir un mensaje que solicita una indicación de si el aparato de recepción puede tratar datos de modo mixto, y el aparato de recepción responderá después transmitiendo la segunda señal de indicación que comprende un mensaje de respuesta que indica si el aparato de recepción puede tratar datos de modo mixto. El siguiente párrafo describe un procedimiento que usa señalización que puede incluir tanto el mensaje de solicitud como el mensaje de respuesta descritos anteriormente.

La Figura 7 es un diagrama de flujo que ilustra un procedimiento para transmitir, o no transmitir, datos protegidos y datos no protegidos, por ejemplo, en el aparato de la Figura 6. En el bloque 801, un aparato de recepción proporciona una señal de indicación, tal como se muestra en la Figura 5. La señal de indicación comprende una indicación de si un aparato de recepción puede tratar datos que comprenden datos cifrados y datos no cifrados, y se transmite en el bloque 802. En el bloque 803, la señal de indicación transmitida es recibida por el receptor 510 del aparato de transmisión 500 mostrado en la Figura 6. En el bloque 804 se determina si el aparato si el aparato de recepción puede tratar datos que comprenden datos cifrados y datos no cifrados, en función de la indicación. Si la determinación es SÍ, entonces los datos de modo mixto (que comprenden datos protegidos cifrados y datos no protegidos no cifrados) se transmiten en el bloque 805. Si la determinación es NO, entonces los datos de modo mixto no se transmiten. Si la determinación es NO, entonces, por ejemplo, el aparato de transmisión está adaptado para cifrar, y después transmitir, todos los datos, incluyendo los datos no protegidos.

La Figura 8 es un diagrama esquemático de un segundo aparato de transmisión 600 que puede cifrar datos protegidos y datos no protegidos. Una fuente de datos protegidos 601 puede hacerse funcionar para proporcionar datos protegidos. Una fuente de datos no protegidos 602 puede hacerse funcionar para proporcionar datos no protegidos. Un dispositivo de cifrado 603, acoplado a la fuente de datos protegidos 601 y a la fuente de datos no protegidos, puede hacerse funcionar para cifrar los datos protegidos para generar datos protegidos cifrados 610 y para cifrar los datos no protegidos para generar datos no protegidos cifrados 611. Un transmisor 604, acoplado al dispositivo de cifrado, puede hacerse funcionar para transmitir los datos protegidos cifrados y los datos no protegidos cifrados como datos transmitidos.

El aparato de transmisión 600 comprende además un segundo receptor 613 para recibir una señal de indicación 612 que comprende una indicación de si transmitir datos protegidos cifrados y datos no protegidos no cifrados. El receptor 613 proporciona la indicación a un microprocesador 607 acoplado al receptor 613 y al transmisor 604.

La señal de indicación 612 puede ser, por ejemplo, la señal de indicación 1020 mostrada en la Figura 5, comprendiendo la señal 612 una indicación de si el aparato de recepción puede tratar datos que comprenden datos cifrados y datos no cifrados. El aparato de transmisión 600 está adaptado para interpretar que la señal de indicación 1020 comprende una indicación de si transmitir datos protegidos cifrados y datos no protegidos no cifrados.

El microprocesador 607 interpreta la indicación recibida 620 y controla el transmisor según la indicación. El primer transmisor puede hacerse funcionar para transmitir los datos protegidos cifrados y los datos no protegidos si la indicación 612 es para transmitir datos protegidos cifrados y datos no protegidos no cifrados. El transmisor 604 puede hacerse funcionar para transmitir los datos protegidos cifrados 610 y los datos no protegidos cifrados 611 si la indicación no es para transmitir datos de modo mixto o si la indicación no se recibe. Esto tiene la ventaja de que un aparato de recepción puede recibir y usar los datos transmitidos cuando una indicación no se recibe y cuando los datos protegidos y los datos no protegidos se cifran como en la técnica anterior. El transmisor también puede hacerse funcionar, si no se recibe la indicación, para transmitir los datos protegidos cifrados y los datos no

protegidos cifrados, y para transmitir los datos protegidos cifrados y los datos no protegidos. Esto tiene la ventaja de que o bien el aparato de recepción mostrado en la Figura 1, o bien un aparato de recepción que puede tratar datos que comprenden datos cifrados y datos no cifrados, o bien un aparato de recepción que no es capaz de ello, puede recibir y usar los datos transmitidos si no se recibe la indicación.

La Figura 9 es un diagrama de flujo que ilustra otro procedimiento para transmitir datos protegidos y datos no protegidos. El procedimiento de la Figura 9 puede usarse en el aparato de transmisión 600 descrito anteriormente mostrado en la Figura 8. El aparato de transmisión 120 mostrado en la Figura 1, o el aparato de transmisión 500 mostrado en la Figura 6, puede adaptase para llevar a cabo el procedimiento. En el bloque 904 se proporcionan datos protegidos y en el bloque 905 se cifran los datos protegidos para generar datos protegidos cifrados. En el bloque 906 se proporcionan datos no protegidos. En el bloque 901 se proporciona una señal de indicación, proporcionando la señal de indicación una indicación de si un aparato de recepción puede tratar datos que comprenden datos cifrados y datos no cifrados. En el bloque 902 se transmite la señal de indicación. En el bloque 903 se recibe la señal de indicación transmitida. En el bloque 908 se determina si la indicación se ha recibido (SÍ) o no se ha recibido (NO).

Si la determinación es SÍ, se toma otra determinación en el bloque 909, en base a la señal de indicación, acerca de si el aparato de recepción puede tratar datos que comprenden datos cifrados y datos no cifrados. Si la determinación es SÍ, entonces en el bloque 910 se transmiten los datos protegidos cifrados del bloque 905 y los datos no protegidos no cifrados del bloque 906.

Si la determinación del bloque 909 es NO o si la determinación del bloque 908 es NO, entonces, en el bloque 907, los datos no protegidos proporcionados en en bloque 906 se cifran para generar datos no protegidos cifrados. Los datos no protegidos cifrados proporcionados por el bloque 907 y los datos protegidos cifrados proporcionados por el bloque 905 se transmiten después en el bloque 911. Opcionalmente, cuando la indicación no se recibe (es decir, cuando la determinación del bloque 908 es NO), los datos protegidos cifrados y los datos no protegidos cifrados se transmiten en el bloque 911 y, además, como se muestra mediante la línea discontinua 912, en el bloque 910 se transmiten los datos protegidos cifrados y los datos no protegidos.

La anterior descripción ilustra sistemas que comprenden disposiciones sencillas de un transmisor y un receptor. Las ideas dadas a conocer en el presente documento pueden aplicarse a sistemas más complejos con ventajas similares. Por ejemplo, las ideas pueden aplicarse a un sistema de comunicaciones celulares. La siguiente descripción ilustra cómo las ideas pueden aplicarse en un sistema de comunicaciones celulares que funciona según las normas de red de acceso radioeléctrico GSM / EDGE (GERAN) utilizadas en todo el mundo por la industria de las comunicaciones celulares y mantenidas por la organización llamada Proyecto de Asociación de Tercera Generación (3GPP).

La Figura 10 es un diagrama de un sistema de comunicaciones celulares 1100. Las estaciones base 1110, 1112 y 1114 pueden comunicarse con estaciones remotas 1120, 1122, 1124, 1126 y 1128 por medio de señales inalámbricas. Controladores de estación base 1130, 1132, 1134 y 1136 encaminan señales hacia y desde las estaciones base bajo el control de centros de conmutación móvil 1140, 1142. Los centros de conmutación móvil (MSC) 1140, 1142, están conectados a una red telefónica pública conmutada (PSTN) 1150.

Aunque las estaciones remotas son normalmente dispositivos móviles manuales (estaciones móviles, MS), muchos dispositivos inalámbricos fijos y dispositivos inalámbricos que pueden tratar datos también están incluidos en la categoría general de estación remota. Por ejemplo, una estación remota puede ser un ordenador conectado a estaciones base a través de Internet, o un terminal inalámbrico fijado a la pared de un edificio o conectado a una fuente de alimentación eléctrica, o incluso un terminal inalámbrico de una máquina expendedora para proporcionar servicios de telemetría. Un dispositivo inalámbrico que puede tratar datos puede ser, por ejemplo, un dispositivo inalámbrico capaz de permitir transacciones electrónicas para la compra de productos o servicios. El sistema de comunicaciones puede comprender solamente un único aparato de transmisión y un único aparato de recepción.

Las señales 1160 que transportan voz y/o datos pueden transferirse entre una estación remota 1120 y una estación base 1112, encaminarse después a través de la red hacia otra estación base 1114 y transferirse después entre una estación base 1112 y una estación remota 1124, permitiendo así que las estaciones remotas 1120 y 1124 se comuniquen entre sí a través del sistema de comunicaciones 1100. Como alternativa, las señales 1160 pueden transferirse entre una estación remota 1120 y otro equipo de comunicaciones de otro sistema de comunicaciones a través de la red telefónica pública conmutada 1150 (PSTN). La PSTN 1150 permite que las llamadas se encaminen entre el sistema celular móvil 1100 y otro sistema de comunicación del mismo tipo que el sistema de comunicaciones 1100 o de un tipo diferente.

En los sistemas celulares, un proceso conocido como autenticación de usuario se lleva a cabo cuando un nuevo usuario intenta acceder al sistema. Por ejemplo, un usuario del anterior sistema de comunicaciones celulares 1100 puede acceder al sistema utilizando una estación remota 1120. El objetivo de la autenticación es proteger la red contra un uso no autorizado e impedir la posibilidad de que usuarios no autorizados suplanten a usuarios autorizados.

Durante la autenticación, una clave de cifrado, usada preferiblemente para cifrar y descifrar datos de tráfico, se elige y se almacena tanto en la red como en la estación remota. Una vez que se ha establecido una clave de cifrado (descrita anteriormente), pueden tener lugar las comunicaciones entre la estación remota y otras partes de la red. El cifrado puede habilitarse o inhabilitarse por la red de comunicaciones según los requisitos de confidencialidad, según el tipo de datos que está enviándose o según el estado actual del enlace de comunicaciones entre una estación remota y la red. Por ejemplo, en sistemas celulares digitales, el cifrado se habilita para comunicaciones de voz, pero se inhabilita durante el proceso conocido como traspaso, mediante el cual una estación remota interrumpe la comunicación con una primera estación base e inicia una comunicación con una segunda estación base.

La Figura 11 es un diagrama de flujo que ilustra un procedimiento 1200 para establecer un enlace de comunicaciones cifrado. Este procedimiento puede usarse para una llamada de voz entre una estación remota y una estación base. La estación base y la estación remota pueden soportar diferentes algoritmos de cifrado. Durante la señalización entre la estación remota y la estación base, la estación remota transmite una señal a la estación base indicando qué algoritmos de cifrado admite (bloque 1202). Después, la red selecciona uno de estos algoritmos para su uso (bloque 1204). La estación base puede admitir más de un algoritmo a la vez, por ejemplo para comunicarse con más de una estación remota. En el bloque 1206, la estación base señaliza este algoritmo seleccionado a la estación remota. El algoritmo seleccionado es usado después por la estación remota y la estación base para comunicarse en modo cifrado (bloque 1208).

La Figura 12 es un diagrama de flujo que ilustra un procedimiento para la autenticación de un abonado. La autenticación se lleva a cabo cuando el abonado, por medio de una estación remota, trata de acceder a la red. La red almacena información relacionada con cada usuario en un registro (no mostrado). Un registro de posiciones base (HLR) está asociado a cada centro de conmutación móvil (por ejemplo, los MSC 1140, 1142 de la Figura 10) y almacena la identidad del usuario y otra información de usuario de usuarios que pertenecen al área atendida por el MSC. Un registro de posiciones de visitantes (VLR) almacena información de usuarios visitantes y que están siendo atendidos por el MSC. Cuando se requiere la autenticación de una estación remota, la red obtiene información relacionada con la seguridad a partir del HLR o el VLR correspondiente a la estación remota.

En el bloque 1301, la estación remota es identificada mediante su identidad de abonado móvil internacional (IMSI) o mediante su identidad de abonado móvil temporal (TMSI) obtenida del HLR o el VLR, respectivamente. En el bloque 1302 se obtiene información de seguridad (datos_1) aplicando un algoritmo a un número generado de manera aleatoria y a una clave de autenticación Ki. Después, los datos (datos_1) se almacenan en el VLR como parte de la información relacionada con la seguridad (bloque 1304).

En el bloque 1306, el MSC/VLR elige el valor de datos almacenado (datos_1) correspondiente a la estación remota. En el bloque 1308, la red envía una solicitud a la estación remota en relación con segundos datos almacenados (datos_2, que deberían ser idénticos a los datos_1). Después, el MSC/VLR (en el bloque 1310) prueba los datos_2 enviados desde la estación remota comparándolos con los datos almacenados (datos_1). Si (bloque 1312) los datos enviados desde la estación remota coinciden con los datos almacenados, se considera que la estación remota se ha autenticado (bloque 1314). Una vez que la estación remota se ha autenticado, pueden tener lugar comunicaciones de voz y/o datos entre la estación remota y la red. Como alternativa, si (bloque 1312) los datos enviados desde la estación remota no coinciden con los datos almacenados, la estación remota no se autentica (bloque 1316) y no pueden tener lugar comunicaciones de voz y/o de datos entre la estación remota y la red.

La Figura 13 es un diagrama de flujo que ilustra un procedimiento 1500 para tratar datos recibidos cifrados y no cifrados. El procedimiento 1500 puede llevarse a cabo en una estación remota. Un bloque de datos modulados y codificados se transmite mediante un aparato de transmisión, por ejemplo el aparato de transmisión 120 de la Figura 1, que puede estar en una estación base (BS). El bloque de datos se recibe en un aparato de recepción, por ejemplo el aparato de recepción 130 de la Figura 1, que puede estar en una estación remota, tal como una estación móvil (MS). El bloque recibido de datos se desmodula por el receptor del aparato de recepción (bloque 1501). El bloque de datos puede comprender solamente datos protegidos, o solamente datos no protegidos, pero no ambos.

En el bloque 1502 se determina si el cifrado está activado para la transmisión de los datos recibidos. En un ejemplo, si el aparato de transmisión transmite un mensaje al aparato de recepción indicando un algoritmo de cifrado seleccionado a usar, como se muestra en 1206 de la Figura 11, el aparato de recepción puede almacenar esta información y puede determinar, a partir de la información almacenada, que el cifrado está activado. En otro ejemplo, el aparato de recepción puede haber recibido un mensaje desde el aparato de transmisión, que indica al aparato de recepción que transmita y reciba datos cifrados, es decir, que funcione en el modo cifrado.

Si la determinación 1502 es que el cifrado está activado, el bloque desmodulado de datos se almacena en un medio de almacenamiento de datos (bloque 1503), que puede comprender una memoria de estado sólido. El bloque de datos almacenado se descifra (bloque 1504) y el bloque de datos descifrado se descodifica (bloque 1505). Si la determinación 1502 es que el cifrado no está activado, en el bloque 1505 el bloque de datos se descodifica sin descifrarse.

Se determina (bloque 1506) si el bloque de datos introducido en el descodificador se ha descodificado con éxito. La determinación puede comprender un indicador de comprobación de redundancia cíclica (CRC), pero puede implicar asimismo cualquier otra técnica de verificación de datos. La determinación sirve para proporcionar un resultado de validación que indica si los datos descodificados son válidos o no. La determinación tiene la misma función de proporcionar un resultado de validación como la del validador 107 de la Figura 1.

Si el bloque de datos desmodulado se cifró antes de su transmisión, entonces, siempre y cuando los datos no se hayan corrompido (por ejemplo, debido a un mal estado del enlace), la determinación en el bloque 1506 es: SÍ, el bloque de datos descodificado se ha descodificado con éxito, es decir, es válido. Después (bloque 1507), los datos válidos descodificados y una señal de indicación, por ejemplo un indicador de descodificación que puede comprender un mensaje indicador de bloque que contiene un indicador CRC, se envían a las capas superiores del protocolo de comunicaciones usado en el sistema. La señal de indicación o el indicador de descodificación indica, en este ejemplo, si los datos descodificados se han descodificado con éxito o no, es decir, son válidos o no.

Por otro lado, si el bloque de datos desmodulado comprende datos no cifrados, la determinación del bloque 1506 es NO (los datos de bloque descodificados no se han descodificado con éxito, es decir, no son válidos) y el proceso avanza hasta el bloque 1508, donde se determina de nuevo (al igual que en el anterior bloque 1502) si el cifrado está activado. Puesto que el cifrado está activado en este ejemplo, el proceso avanza hasta el bloque 1510, donde el bloque de datos que está almacenado en la memoria se descodifica. En el bloque 1511 se determina si los datos desmodulados y descodificados proporcionados por el bloque 1510 son válidos, como se ha descrito anteriormente en relación con el bloque 1506. Si la determinación del bloque 1511 es SÍ (los datos descodificados son válidos), entonces el proceso avanza hasta el bloque 1512. En el bloque 1512, los datos válidos descodificados y una señal de indicación, por ejemplo, un mensaje indicador de bloque, se envían a las capas superiores del protocolo de comunicaciones. Después, el proceso puede repetirse desde el bloque 1501, desmodulando así datos adicionales recibidos, etc.

Si la determinación del bloque 1508 es que el cifrado no está activado, el proceso avanza hasta el bloque 1509, en el que un mensaje indicador de bloque se envía a capas superiores del protocolo de comunicaciones usado en el sistema. El mensaje indicador de bloque indica que el bloque de datos recibido no puede descodificarse con éxito. Después, el proceso puede repetirse desde el bloque 1501, de manera que se desmodulan datos adicionales recibidos. El mismo bloque de datos puede retransmitirse hasta que se descodifique con éxito, o puede retransmitirse solamente una vez o un número de veces específico. Si el bloque de datos está formado por datos de voz, entonces los datos no se retransmiten generalmente, y el siguiente bloque de datos se recibe y procesa empezando por el bloque 1501 de la Figura 13.

Un bloque de datos puede transmitirse de manera que el bloque de datos puede comprender datos cifrados o datos no cifrados. Cuando se reciben datos que contienen uno o más bloques de datos cifrados y uno o más bloques de datos no cifrados, el proceso mostrado en la Figura 13 y descrito anteriormente garantiza (a) que los bloques cifrados de los datos recibidos se descifran y después se descodifican y (b) que los bloques no cifrados de los datos recibidos se descodifican sin descifrarse. Por lo tanto, cada bloque de datos introducido en el bloque 1501 puede descodificarse con éxito, tanto si el bloque está cifrado como si no, y si los múltiples bloques de datos comprenden bloques de datos cifrados y/o no cifrados. El proceso mostrado en la Figura 13 funcionará por tanto para datos que comprenden solamente datos cifrados, solamente datos no cifrados o datos de modo mixto.

El sistema puede estar dispuesto de modo que los datos de modo mixto para una estación remota solo se transmiten por la estación base siempre que la estación remota haya indicado a la estación base que la estación remota puede recibir datos cifrados y datos no cifrados cuando el cifrado está activado. Si la estación remota no ha proporcionado está indicación, entonces la estación base solo enviará datos cifrados cuando el cifrado esté activado. Por ejemplo, la estación remota proporcionará la indicación por medio de una señal de indicación que comprende un mensaje.

La siguiente tabla muestra las determinaciones tomadas en los bloques 1502, 1506, 1508 y 1511 de la Figura 13 para todos los tipos de datos recibidos (cifrados, no cifrados y de modo mixto), tanto para el caso en que no hay errores en los datos recibidos como para el caso en que hay muchos errores en los datos recibidos.

| Modo de envío de datos | Estado de error | Bloque 1502 | Bloque 1506 | Bloque 1508 | Bloque 1511 |
|---|---|---|---|---|---|
| Todos los datos están cifrados | No hay errores | sí | sí | n.a. | n.a. |
| Todos los datos están sin cifrar | No hay errores | no | sí | n.a. | n.a. |
| Datos cifrados y datos no cifrados (modo mixto) | No hay errores | sí | no | sí | sí |
| Todos los datos están cifrados | Muchos errores | sí | no | sí | no |
| Todos los datos están sin cifrar | Muchos errores | no | no | no | n.a. |
| Datos cifrados y datos no cifrados (modo mixto) | Muchos errores | sí | no | sí | no |
| (n.a. = no aplicable) | | | | | |

La Figura 14 es un diagrama de flujo que ilustra un procedimiento para enviar datos cifrados y/o datos no cifrados que puede llevarse a cabo en un equipo de infraestructura de red. Por ejemplo, el procedimiento puede llevarse a cabo en la estación base 1112 de la Figura 10. En el bloque 1410, la red transmite un mensaje de solicitud para una estación remota, solicitando a la estación remota que envíe un mensaje de indicación de capacidad. La estación remota recibe el mensaje de solicitud y responde transmitiendo un mensaje de indicación de capacidad (no mostrado).

En el bloque 1420, el mensaje de indicación de capacidad es recibido por la estación base. En el bloque 1430, la estación base determina, en función del mensaje de indicación de capacidad recibido, si la estación remota puede funcionar en el modo mixto. Si la determinación es que la estación remota puede funcionar en el modo mixto, entonces en el bloque 1450 la estación base envía un mensaje de indicación de modo mixto para la estación remota, indicando que la estación base transmitirá señales para esa estación remota en el modo mixto. El bloque 1450 puede no ser necesario, ya que la estación remota puede no necesitar el mensaje de indicación de modo mixto con el fin de funcionar para tratar datos de modo mixto. La estación remota puede actuar según el proceso mostrado en la Figura 13 y descrito anteriormente, que no requiere ningún mensaje de indicación de modo mixto procedente de la estación base. La estación remota, después de haber enviado un mensaje de indicación de capacidad a la estación base (correspondiente al bloque 1420), puede funcionar automáticamente en el modo mixto. En el bloque 1455 se activa el funcionamiento en modo mixto. En el bloque 1460, los datos protegidos se cifran y los datos no protegidos se dejan sin cifrar antes de su transmisión. En el bloque 1470 se transmiten los datos cifrados y los datos no cifrados.

El procedimiento mostrado en la Figura 14 puede llevarse a cabo en gran medida en un centro de conmutación móvil (por ejemplo, el MSC 1140, 1142 de la Figura 10). La información de cifrado puede ser solicitada por el MSC a partir del aparato receptor (por ejemplo, la estación remota a través del aparato de transmisión (por ejemplo, estación base) y después, una vez que la información es recibida por el MSC, el MSC ordena a la estación base que inicie el cifrado. La función de toma de decisiones 1430 y la función de cifrado 1445 y 1450 pueden llevarse a cabo en un controlador de estación base (por ejemplo, el BSC 1134, 1136 de la Figura 10) o en un MSC u otro equipo de red que presenta las funciones requeridas.

La Figura 15 es un diagrama esquemático de una parte de un receptor. Una señal que comprende datos modulados se introduce en el desmodulador 1605, que proporciona datos desmodulados a una primera entrada de un conmutador 1610 que tiene como segunda entrada una señal de control de conmutador 1612. La señal de control de conmutador 1612 puede tener uno de dos valores: un primer valor si se decide descifrar los datos desmodulados; y un segundo valor si se decide no descifrar los datos desmodulados sino procesar adicionalmente los datos desmodulados sin descifrarse.

Si se decide descifrar los datos desmodulados, los datos se proporcionan desde el conmutador 1610 al elemento de descifrado 1615 y se descifran mediante el elemento de descifrado 1615. Los datos descifrados se proporcionan a un descodificador 1620 y se descodifican por el descodificador 1620. Las funciones mostradas en la Figura 15 pueden implementarse en hardware, en software o en circuitos de procesamiento de señales digitales, es decir, una combinación de hardware y software.

Si se decide no descifrar los datos desmodulados, los datos se proporcionan desde el conmutador 1610 y se introducen en el descodificador 1620, sorteando así el elemento de descifrado 1615. El descodificador 1620 descodifica los datos desmodulados y proporciona datos desmodulados descodificados 1626.

Además, el descodificador 1620 proporciona una señal de indicación de descodificación 1625 que comprende una indicación de si los datos desmodulados se han descodificado con éxito o no mediante el elemento de descodificación 1620, comprendiendo la indicación, por ejemplo, un indicador de comprobación de redundancia

cíclica (CRC). Esta indicación puede usarse por el sistema para provocar la retransmisión de un bloque de datos que no se ha descodificado con éxito, como se ha descrito anteriormente.

Otra posible función del indicador de descodificación es indicar, cuando el cifrado está activado en la estación base, que los datos recibidos por la estación remota pueden ser datos de modo mixto, incluso aunque la estación remota no sepa que los datos son datos de modo mixto. Si un bloque de datos no cifrados se introduce en el elemento de descifrado, el elemento de descifrado tratará de descifrar los datos no cifrados pero no tendrá éxito y, por lo tanto, el indicador de descodificación indicará que los datos descifrados no son válidos.

La función se basa, en primer lugar, en que la estación remota trate un primer bloque de datos como si fuera un bloque de datos cifrados. La función también se basa, en segundo lugar, en tratar el primer bloque de datos como si fuera un bloque de datos no cifrados si el indicador de descodificación indica que los datos no se han descodificado con éxito. La función también se basa, en tercer lugar, en tratar bloques de datos recibidos posteriormente como si fueran datos de modo mixto si el indicador de descodificación indica que el primer bloque de datos se ha descodificado con éxito.

La posible función descrita anteriormente llevada a cabo por el indicador de descodificación (que proporciona una indicación de que los datos recibidos por la estación remota pueden ser datos de modo mixto) puede proporcionarse mediante una función alternativa en otro punto del sistema. Por ejemplo, la red (a través de la estación base) puede enviar una indicación a la estación remota de que transmitirá datos de modo mixto y, a partir de esta indicación, la estación remota puede actuar para tratar datos de modo mixto. Por ejemplo, la estación remota puede recibir la indicación y después recibir y desmodular los datos. Después, la estación remota, según la indicación y para cada bloque de datos desmodulados recibidos, (a) tratará primero el bloque como datos cifrados y (b) después tratará el mismo bloque como datos no cifrados. Asimismo, la estación remota puede llevar a cabo la operación (b) antes de la operación (a) o puede llevar a cabo las operaciones (a) y (b) en paralelo.

La Figura 16 es un diagrama de flujo que ilustra un procedimiento en el que datos protegidos y datos no protegidos se transmiten desde una estación base y se reciben por una estación remota. La estación base envía una indicación a la estación remota de que transmitirá datos de modo de mixto, recibiéndose la indicación por la estación remota (1706). El procedimiento mostrado implica descodificar datos recibidos tanto con descifrado como sin descifrado.

Un mensaje de solicitud de capacidad procedente de una estación base es recibido por la estación remota en el bloque 1702. En el bloque 1704, la estación remota responde enviando un mensaje de indicación de capacidad a la estación base. El mensaje indica si la estación remota puede o no tratar datos de modo mixto. En el bloque 1706, la estación remota recibe un mensaje de indicación de modo mixto desde la estación base, indicando el mensaje que la estación base transmitirá datos de modo mixto. Este mensaje de indicación de modo mixto lleva a cabo la función principal descrita anteriormente en el caso de la función del 'indicador de descodificación', y permite que la estación remota adapte o configure su receptor para tratar correctamente datos de modo mixto. El mensaje de indicación de modo mixto solo indicará que la estación base transmitirá datos de modo mixto si el mensaje de indicación de capacidad enviado por la estación remota indicó que la estación remota admite el funcionamiento de modo mixto. El mensaje de indicación de modo mixto puede ser, por ejemplo, parte de un mensaje ACEPTAR ACTUALIZACIÓN DE ÁREA DE ENCAMINAMIENTO para la estación remota, o puede enviarse cuando se recibe una RESPUESTA DE AUTENTICACIÓN Y CIFRADO válida desde la estación remota. El mensaje de indicación de modo mixto puede ser parte de un mensaje "INICIAR CIFRADO" modificado.

En el bloque 1708, la estación remota recibe los datos transmitidos por la estación base. Los datos comprenden normalmente datos de tráfico, por ejemplo datos de voz, y comprenden datos cifrados y datos no cifrados siempre que el mensaje de indicación de capacidad haya indicado que la estación remota admite el funcionamiento de modo mixto. En el bloque 1710, los datos recibidos se desmodulan para generar datos desmodulados adecuados para su procesamiento por medio de circuitos digitales de banda base.

En el bloque 1712, los datos desmodulados se almacenan en un primer medio de almacenamiento de datos (medio de almacenamiento de datos U), comprendiendo el medio de almacenamiento de datos, por ejemplo, una memoria digital, por ejemplo una memoria de acceso aleatorio o una memoria flash. En el bloque 1714, un parámetro variable N, que puede tener dos valores, se fija inicialmente a cero. Debe apreciarse que el parámetro variable N también puede fijarse a cero en cualquier instante de tiempo previo a la acción del bloque 1714. En el bloque 1720, los datos almacenados en el medio de almacenamiento U se descifran, por ejemplo introduciendo los datos en el elemento de descifrado 1615 mostrado en la Figura 8, para generar datos descifrados para su descodificación. En el bloque 1724, los datos descifrados se descodifican (por ejemplo, en el elemento descodificador 1620 mostrado en la Figura 15), para generar datos descifrados descodificados.

En el bloque 1750 se determina si todos los datos recibidos se han descodificado con éxito. La salida del bloque 1750 es una determinación (positiva o negativa) de si todos los datos recibidos se han descodificado con éxito para generar datos válidos. Un resultado positivo se indica como 'SÍ' en la figura.

El bloque 1760 representa una función que fija el valor de un indicador de descodificación de bloque a un valor

particular, siendo el valor 'bien'. El indicador de descodificación de bloques solo puede tener otro valor, siendo ese otro valor 'mal', fijado por el bloque 1770. Un ejemplo de un indicador de descodificación de bloque es un indicador CRC, cuyos principios de funcionamiento son ampliamente conocidos en la técnica. Sin embargo, el indicador de descodificación de bloque puede implementarse de diferentes maneras y en ubicaciones diferentes. Por ejemplo, la estación remota puede generar un indicador que comprende una secuencia particular de datos de transmisión, solamente si los datos de descodificación se han descodificado con éxito.

Si la determinación del bloque 1750 es SÍ, en el bloque 1760 el indicador de descodificación de bloque se fija a 'BIEN'. En el bloque 1762, los datos descodificados se envían a las capas superiores del protocolo del sistema de comunicaciones y, en el bloque 1764, el indicador se envía a las capas superiores del protocolo. Después, el proceso vuelve al bloque 1708, en el que se reciben nuevos datos. Si la determinación del bloque 1750 es NO, en el bloque 1752 se determina además si el parámetro N tiene el valor uno (N=1). Si la determinación adicional es NO (es decir, si N=0), entonces, en el bloque 1754, a N se le asigna el valor 1 (es decir, N=1) y, en el bloque 1756, los datos que están almacenados en el medio de almacenamiento de datos U se descodifican por el elemento de descodificación. Después, el proceso avanza hasta la entrada del bloque 1750.

Sin embargo, si la determinación adicional es SÍ (N=1), entonces, en el bloque 1770, el indicador de descodificación de bloque se fija a 'MAL' y, en el bloque 1764, el indicador se envía a las capas superiores del protocolo. Después, el proceso vuelve al bloque 1708, en el que se reciben datos de nuevo. Normalmente, el mismo bloque de datos que se ha recibido pero que no se ha descodificado con éxito, se retransmitirá por la estación base y será recibido después por la estación remota en el bloque 1708. Esto sucederá, por ejemplo, si los datos se han descodificado sin éxito debido a un fallo genuino en el enlace, por ejemplo si las condiciones de propagación de la señal transmitida eran muy malas cuando se transmitieron algunos de los datos.

La Figura 17 es un diagrama de flujo que ilustra un procedimiento en el que datos protegidos y datos no protegidos se transmiten desde una estación remota y se reciben por una estación base. La Figura 17 muestra un ejemplo del procedimiento mostrado en la Figura 16, pero aplicado a datos de enlace ascendente en lugar de a datos de enlace descendente. Las etapas 1802, 1804 pueden no ser necesarias si ya se sabe que la estación base puede recibir datos de modo mixto. El procedimiento de la Figura 16 se lleva a cabo en una estación remota. Los datos comprenden uno o más bloques de datos transmitidos por una estación base para una estación remota (un bloque de datos de enlace descendente). Como alternativa, el procedimiento puede llevarse a cabo en una estación base para datos que comprenden uno o más bloques de datos transmitidos por una estación remota para una estación base (un bloque de datos de enlace ascendente). Los datos pueden comprender uno o más bloques de datos transmitidos por una estación remota para una estación base (un bloque de datos de enlace ascendente).

Para que la estación base transmita datos de modo mixto a la estación remota (véase la Figura 16), el mensaje de indicación de capacidad procedente de la estación remota puede incluir una indicación de que la estación remota puede tratar datos de modo mixto recibidos. Asimismo, el mensaje (véase el bloque 1706 de la Figura 16) enviado desde la estación base a la estación remota que ordena a la estación remota usar el modo cifrado puede incluir la instrucción para que la estación remota transmita datos de modo mixto.

Las Figuras 18 y 19 representan un procedimiento en el que un bloque de datos se recibe, desmodula y almacena, y los datos desmodulados son tratados por una o ambas funciones.

La Figura 18 es un diagrama de flujo que ilustra un procedimiento para recibir y descodificar datos. Una primera función F1 sirve para descifrar datos desmodulados almacenados (bloque 1930) y después para descodificar los datos descifrados (bloque 1940). Una segunda función F2 sirve para descodificar los datos desmodulados almacenados directamente sin descifrar los datos (bloque 1950).

La Figura 19 es un diagrama de flujo que ilustra otro procedimiento para recibir y descodificar datos. En este procedimiento, las funciones mostradas en la Figura 18 se llevan a cabo en orden inverso. Puede apreciarse que si se almacenan los datos desmodulados, entonces las funciones F1 y F2 pueden llevarse a cabo en serie, en cualquier orden, o en paralelo.

La Figura 20 es un diagrama de flujo que ilustra un procedimiento adicional para recibir y descodificar datos. En este procedimiento, las funciones F1 y F2 de las Figuras 18 y 19 se llevan a cabo en paralelo. Si se usa el modo mixto, entonces llevar a cabo las dos funciones F1 y F2 en paralelo puede tener la ventaja de proporcionar un procesamiento más rápido que llevando a cabo las dos funciones F1 y F2 en serie.

Haciendo referencia una vez más a la Figura 18, si todos los datos descodificados resultantes de la función F1 son válidos, no es necesario llevar a cabo la función F2. Esto solo sería el caso si todos los datos recibidos se cifran antes de la transmisión. Sin embargo, si alguno de los datos descodificados resultantes de la función F1 no es válido, la función F2 se lleva a cabo en el mismo bloque de datos. Los procesos mostrados en las Figuras 18, 19 y 20 pueden usarse para un único bloque de datos o para múltiples bloques de datos, por ejemplo una trama de datos, hasta que todos los datos, por ejemplo la trama, se hayan recibido y descodificado con un número de errores suficientemente bajo.

Haciendo referencia una vez más a la Figura 16, cada bloque funcional (por ejemplo, el 1720) puede actuar en una pluralidad de bloques o paquetes de datos antes de que el siguiente bloque funcional (por ejemplo, el 1724) actúe en la misma pluralidad de bloques. Para datos de modo mixto, los datos cifrados válidos (bloque 1724) pueden combinarse con datos desmodulados válidos (bloque 1756) para formar datos descodificados válidos combinados.

A continuación se ofrecen algunos ejemplos, a modo de referencia, de secciones de las normas 3GPP que, cuando se leen junto con la anterior descripción, pueden ayudar a entender mejor las ideas descritas en el presente documento.

Un ejemplo de la selección de una clave, mencionada anteriormente, se describe en las secciones 4.3.2 y 4.3.2b de la especificación técnica titulada "*3GPP TS 24.008 V4.17.0 (2007-09) Technical Specification 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Mobile radio interface Layer 3 specification; Core network protocols; Stage 3 (Release 4)*". Un ejemplo de un procedimiento de cifrado se describe en la especificación TS 43.020, secciones 4.2 a 4.9. (por ejemplo, datos del servicio de mensajes cortos (SMS)). Un ejemplo de un proceso para establecer un enlace de comunicaciones cifrado se describe en la sección 3.5.3 de la especificación titulada "*3GPP TS 42.009 V4.1.0 (2006-06) Technical Specification 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Security aspects (Release 4)*".

Un ejemplo del procedimiento de cifrado se describe en la especificación TS 43.020, secciones 4.2 a 4.9.

El mensaje de indicación de capacidad puede comprender un mensaje según la especificación 3GPP TS 24.008, sección 10.5.1.7, pero modificando el mensaje para incluir la indicación de capacidad de tratar datos de modo mixto, es decir, si la estación remota puede tratar datos de modo mixto que están parcialmente cifrados y parcialmente descifrados.

Las ideas descritas anteriormente pueden aplicarse a sistemas celulares que funcionan según otras normas diferentes a las normas GERAN, que utilizan cifrado para enviar datos protegidos. Tras haberse descrito su funcionamiento según las normas GERAN, la aplicación de las ideas a otras normas debería ser evidente para los expertos en la técnica. Un ejemplo de un sistema inalámbrico de comunicaciones celulares es el sistema de Acceso Radioeléctrico Terrestre Universal (UTRA), que comprende UMTS y GERAN, normalizado por el Proyecto de Asociación de Tercera Generación (3GPP). En aras de la brevedad, no se describirán más ejemplos.

Tras haberse descrito la invención haciendo referencia a las realizaciones mostradas en los dibujos adjuntos, debe entenderse que las realizaciones en cuestión son simplemente ilustrativas y que pueden realizarse modificaciones y variaciones concebidas por los expertos en la técnica sin apartarse del alcance de la invención descrita en las reivindicaciones adjuntas y equivalencias de las mismas.

**REIVINDICACIONES**

**1.** Un procedimiento para transmitir y recibir datos protegidos y datos no protegidos, que comprende:

proporcionar una señal de indicación (512, 612, 1021, 1020, 1625) que comprende una indicación de si un aparato de recepción (130, 1000) puede tratar tanto datos que comprenden datos cifrados como datos no cifrados;

transmitir la señal de indicación (512, 612, 1021, 1020, 1625);

recibir la señal de indicación (512, 612, 1021, 1020, 1625); y

proporcionar datos protegidos;

proporcionar datos no protegidos;

cifrar los datos protegidos para generar datos protegidos cifrados;

transmitir los datos protegidos cifrados y los datos no protegidos si la indicación es que el aparato de recepción (130, 1000) puede tratar tanto datos que comprenden tanto datos cifrados como datos no cifrados;

recibir datos transmitidos como datos recibidos;

descifrar los datos recibidos para generar datos descifrados;

validar los datos descifrados (108, 201, 301, 1015) para generar un primer resultado de validación (110, 205, 305, 1031) y proporcionar los datos descifrados en función del primer resultado de validación (110, 205, 305, 1031), y validar los datos recibidos para generar un segundo resultado de validación (110, 205, 306, 1031) y proporcionar los datos recibidos en función del segundo resultado de validación (110, 205, 306, 1031).

**2.** El procedimiento según la reivindicación 1, que comprende validar los datos recibidos y los datos descifrados (108, 201, 301, 1015) en paralelo.

**3.** El procedimiento según la reivindicación 1, que comprende cifrar los datos no protegidos para generar datos no protegidos cifrados y transmitir tanto los datos protegidos cifrados como los datos no protegidos cifrados, si:

la indicación es que el aparato de recepción (130, 1000) no puede tratar datos que comprenden tanto datos cifrados como datos no cifrados; o

la indicación no se recibe.

**4.** El procedimiento según la reivindicación 3, que comprende además, cuando no se recibe la indicación:

transmitir los tanto datos protegidos cifrados como los datos no protegidos cifrados; y

transmitir los tanto datos protegidos cifrados como los datos no protegidos.

**5.** Un procedimiento para transmitir datos protegidos y datos no protegidos, que comprende:

recibir una señal de indicación (512, 612, 1021, 1020, 1625) que comprende una indicación de si transmitir tanto datos protegidos cifrados como datos no protegidos no cifrados; y

proporcionar datos protegidos;

proporcionar datos no protegidos;

cifrar los datos protegidos para generar datos protegidos cifrados; y

si la indicación es transmitir tanto datos protegidos cifrados como datos no protegidos no cifrados, responder a la indicación transmitiendo los datos protegidos cifrados y los datos no protegidos no cifrados; y

si la indicación es no transmitir ni los datos protegidos cifrados ni los datos no protegidos no cifrados, cifrar los datos no protegidos para generar datos no protegidos cifrados y transmitir tanto los datos protegidos cifrados como los datos no protegidos cifrados.

**6.** El procedimiento según la reivindicación 5, que comprende cifrar los datos no protegidos para generar datos no protegidos cifrados y transmitir tanto los datos protegidos cifrados como los datos no protegidos cifrados, si la indicación no se recibe.

**7.** El procedimiento según la reivindicación 6, que comprende, si no se recibe la indicación:

transmitir tanto los datos protegidos cifrados como los datos no protegidos cifrados; y

transmitir tanto los datos protegidos cifrados como los datos no protegidos.

**8.** Un procedimiento para recibir tanto datos protegidos como datos no protegidos, comprendiendo el procedimiento:

proporcionar y transmitir una señal de indicación (512, 612, 1021, 1020, 1625), comprendiendo la señal una indicación de si un aparato de recepción (130, 1000) puede tratar tanto datos que comprenden datos cifrados como datos no cifrados;

recibir datos como datos recibidos; descifrar los datos recibidos para generar datos descifrados;

validar los datos descifrados (108, 201, 301, 1015) para generar un primer resultado de validación (110, 205, 305, 1031) y proporcionar los datos descifrados en función del primer resultado de validación (110, 205, 305, 1031), y validar los datos recibidos para generar un segundo resultado de validación (110, 205, 306, 1031) y proporcionar los datos recibidos en función del segundo resultado de validación (110, 205, 306, 1031).

**9.** El procedimiento según la reivindicación 8, que comprende validar los datos recibidos y los datos descifrados (108, 201, 301, 1015) en paralelo.

**10.** Un sistema de comunicaciones (100) para transmitir y recibir datos protegidos y datos no protegidos, que comprende:

un medio para proporcionar una señal de indicación (512, 612, 1021, 1020, 1625) que comprende una indicación de si un aparato de recepción (130, 1000) puede tratar datos que comprenden datos cifrados y datos no cifrados;

un medio para transmitir la señal de indicación (512, 612, 1021, 1020, 1625);

un medio para recibir la señal de indicación (512, 612, 1021, 1020, 1625); y

un medio para proporcionar datos protegidos;

un medio para proporcionar datos no protegidos;

un medio para cifrar los datos protegidos para generar datos protegidos cifrados;

un medio para cifrar los datos no protegidos para generar datos no protegidos cifrados;

un medio para transmitir los datos protegidos cifrados y los datos no protegidos si la indicación es que el aparato de recepción (130, 1000) puede tratar datos que comprenden tanto datos cifrados como datos no cifrados;

un medio para transmitir los datos protegidos cifrados y los datos no protegidos cifrados si la indicación es que el aparato de recepción (130, 1000) no puede tratar tanto datos que comprenden datos cifrados como datos no cifrados;

un medio para recibir datos transmitidos como datos recibidos;

un medio para descifrar los datos recibidos para generar datos descifrados (108, 201, 301, 1015); y

un medio para validar los datos descifrados (108, 201, 301, 1015) para generar un primer resultado de validación (110, 205, 305, 1031) y proporcionar los datos descifrados en función del primer resultado de validación (110, 205, 305, 1031), y validar los datos recibidos para generar un segundo resultado de validación (110, 205, 306, 1031) y proporcionar los datos recibidos en función del segundo resultado de validación (110, 205, 306, 1031).

**11.** Un aparato de transmisión (120, 500, 600) para transmitir datos protegidos y datos no protegidos, que comprende:

un medio para recibir una señal de indicación (512, 612, 1021, 1020, 1625) que comprende una indicación de si transmitir tanto datos protegidos cifrados como datos no protegidos no cifrados; y

un medio para responder a la indicación transmitiendo los datos no protegidos sin cifrar si la indicación es transmitir tanto datos protegidos cifrados como datos no protegidos no cifrados;

un medio para proporcionar datos protegidos;

un medio para proporcionar datos no protegidos;

un medio para cifrar los datos protegidos para generar datos protegidos cifrados; y

un medio para cifrar los datos no protegidos para generar datos no protegidos cifrados;

un medio para transmitir tanto los datos protegidos cifrados como los datos no protegidos si la indicación es transmitir tanto los datos protegidos cifrados como datos no protegidos no cifrados; y

un medio para transmitir los datos protegidos cifrados y los datos no protegidos cifrados si la indicación es no transmitir ni los datos protegidos cifrados ni los datos no protegidos no cifrados.

**12.** El medio para transmitir datos protegidos y datos no protegidos según la reivindicación 11, que comprende medios para:

cifrar los datos no protegidos para generar datos no protegidos cifrados y transmitir tanto los datos protegidos cifrados como los datos no protegidos cifrados, si:

la indicación es no transmitir ni los datos protegidos cifrados ni los datos no protegidos no cifrados; o
la indicación no se recibe.

**13.** Un aparato de recepción (130,1000) para recibir tanto datos protegidos como datos no protegidos, que comprende:

proporcionar y transmitir una señal de indicación (512, 612, 1021, 1020, 1625), comprendiendo la señal una indicación de si un aparato de recepción (130, 1000) puede tratar datos que comprenden datos cifrados y datos no cifrados;

medios para recibir datos como datos recibidos;

medios para descifrar los datos recibidos para generar datos descifrados (108, 201, 301, 1015); y

medios para validar los datos descifrados (108, 201, 301, 1015) para generar un primer resultado de validación (110, 205, 305, 1031) y proporcionar los datos descifrados en función del primer resultado de validación (110, 205, 305, 1031), y validar los datos recibidos para generar un segundo resultado de validación (110, 205, 306, 1031) y proporcionar los datos recibidos en función del segundo resultado de validación (110, 205, 306, 1031).

**14.** El aparato de recepción (130,1000) para recibir datos protegidos y datos no protegidos según la reivindicación 13, que comprende medios para validar los datos recibidos y los datos descifrados (108, 201, 301, 1015) en paralelo.

**15.** Un producto de programa informático, que comprende:

un medio legible por ordenador, que comprende:

código para hacer que un ordenador lleve a cabo el procedimiento según las reivindicaciones 1 a 8.

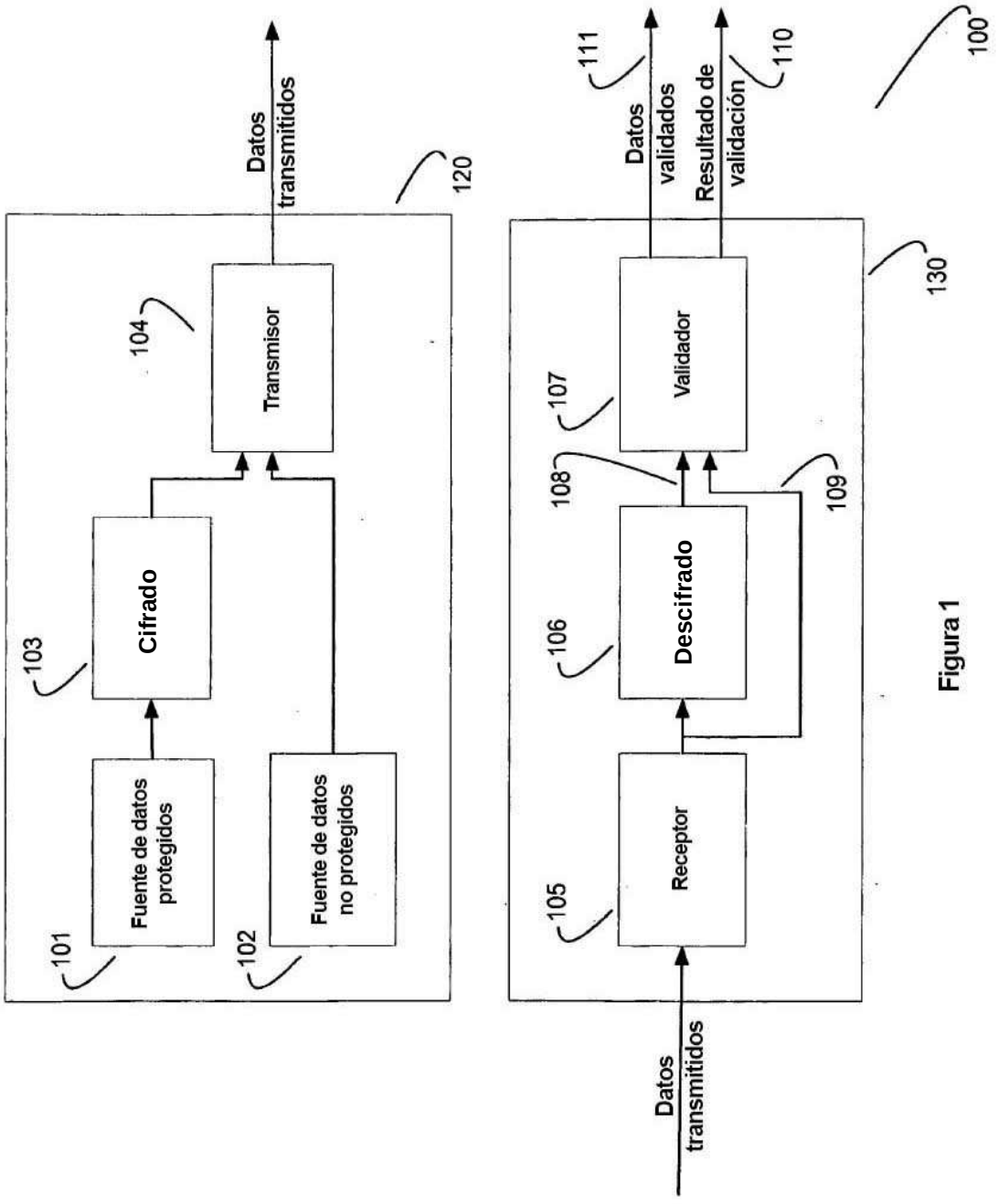
Fuente de datos protegidos
Fuente de datos no protegidos
Cifrado
Transmisor
Datos transmitidos
Receptor
Descifrado
Validador
Datos validados
Resultado de validación
101
102
103
104
105
106
107
108
109
110
111
120
130
100

Figura 1

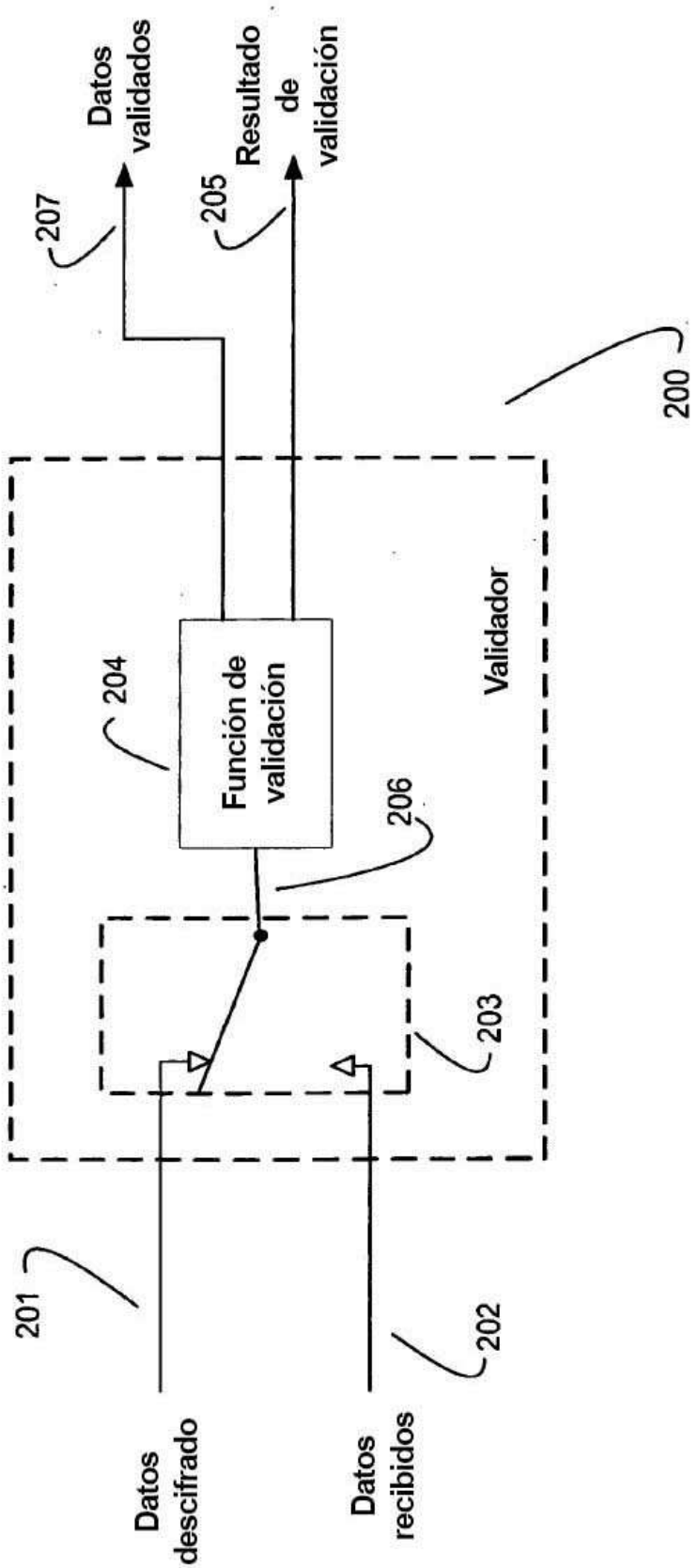
Datos validados
Resultado de validación
207
205
200
Validador
Función de validación
204
206
203
201
202
Datos descifrado
Datos recibidos

Figura 2

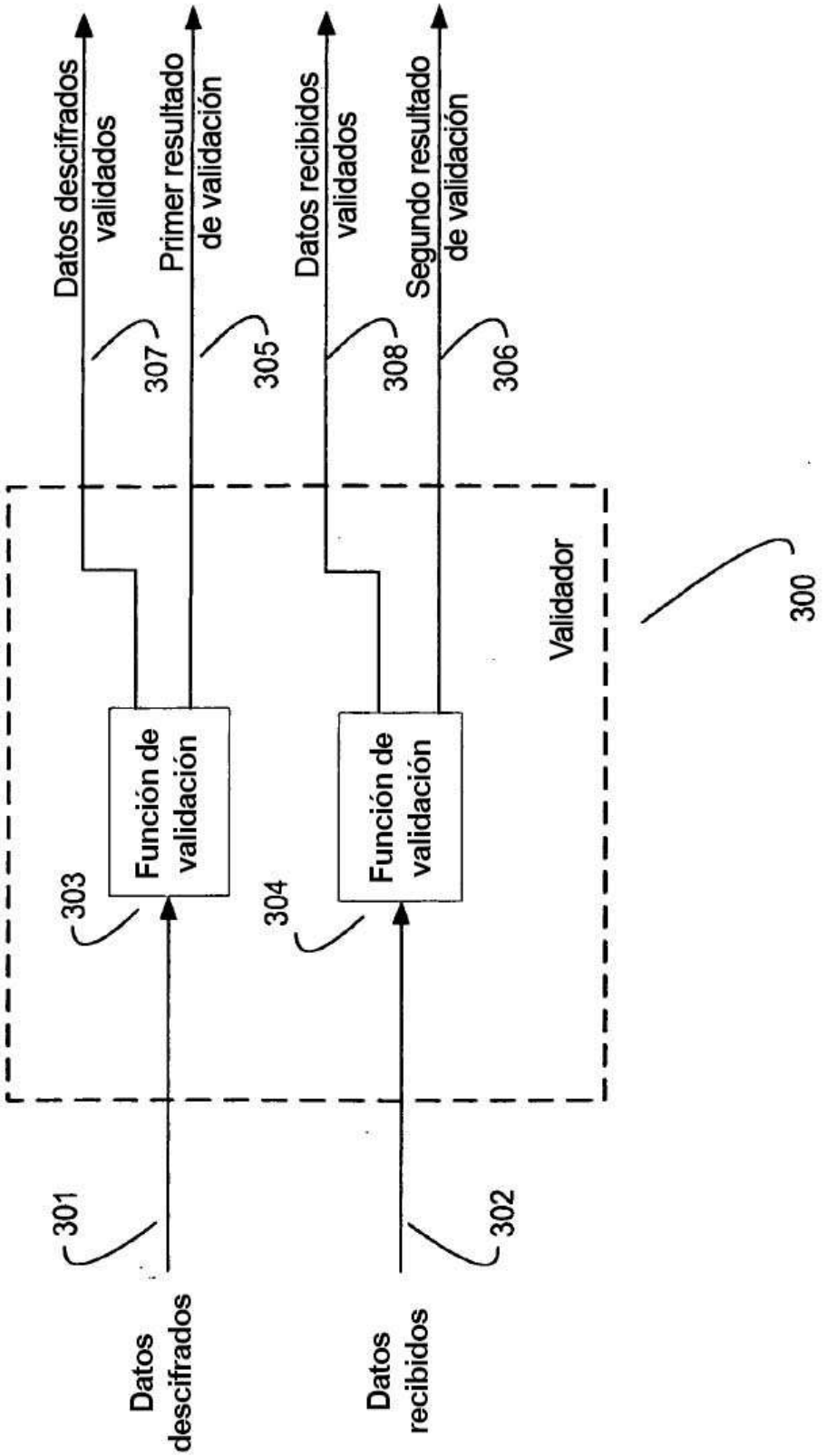
Datos descifrados validados
Primer resultado de validación
Datos recibidos validados
Segundo resultado de validación
307
305
308
306
Función de validación
Función de validación
303
304
Validador
300
301
302
Datos descifrados
Datos recibidos

Figura 3

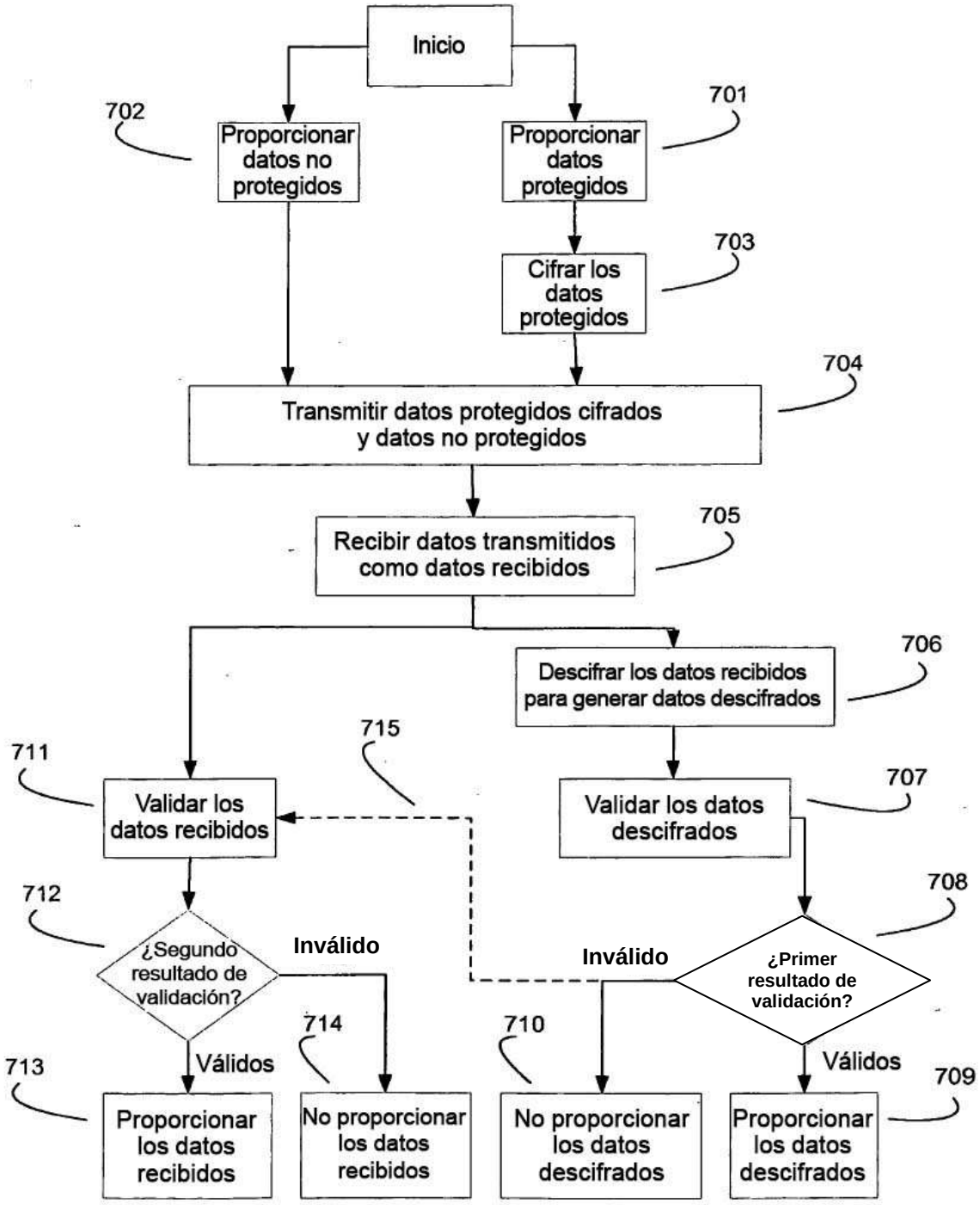
Inicio
702
Proporcionar datos no protegidos
701
Proporcionar datos protegidos
703
Cifrar los datos protegidos
704
Transmitir datos protegidos cifrados y datos no protegidos
705
Recibir datos transmitidos como datos recibidos
706
Descifrar los datos recibidos para generar datos descifrados
715
711
Validar los datos recibidos
707
Validar los datos descifrados
712
708
¿Segundo resultado de validación?
Inválido
Inválido
¿Primer resultado de validación?
714
710
713
Válidos
Válidos
709
Proporcionar los datos recibidos
No proporcionar los datos recibidos
No proporcionar los datos descifrados
Proporcionar los datos descifrados

Figura 4

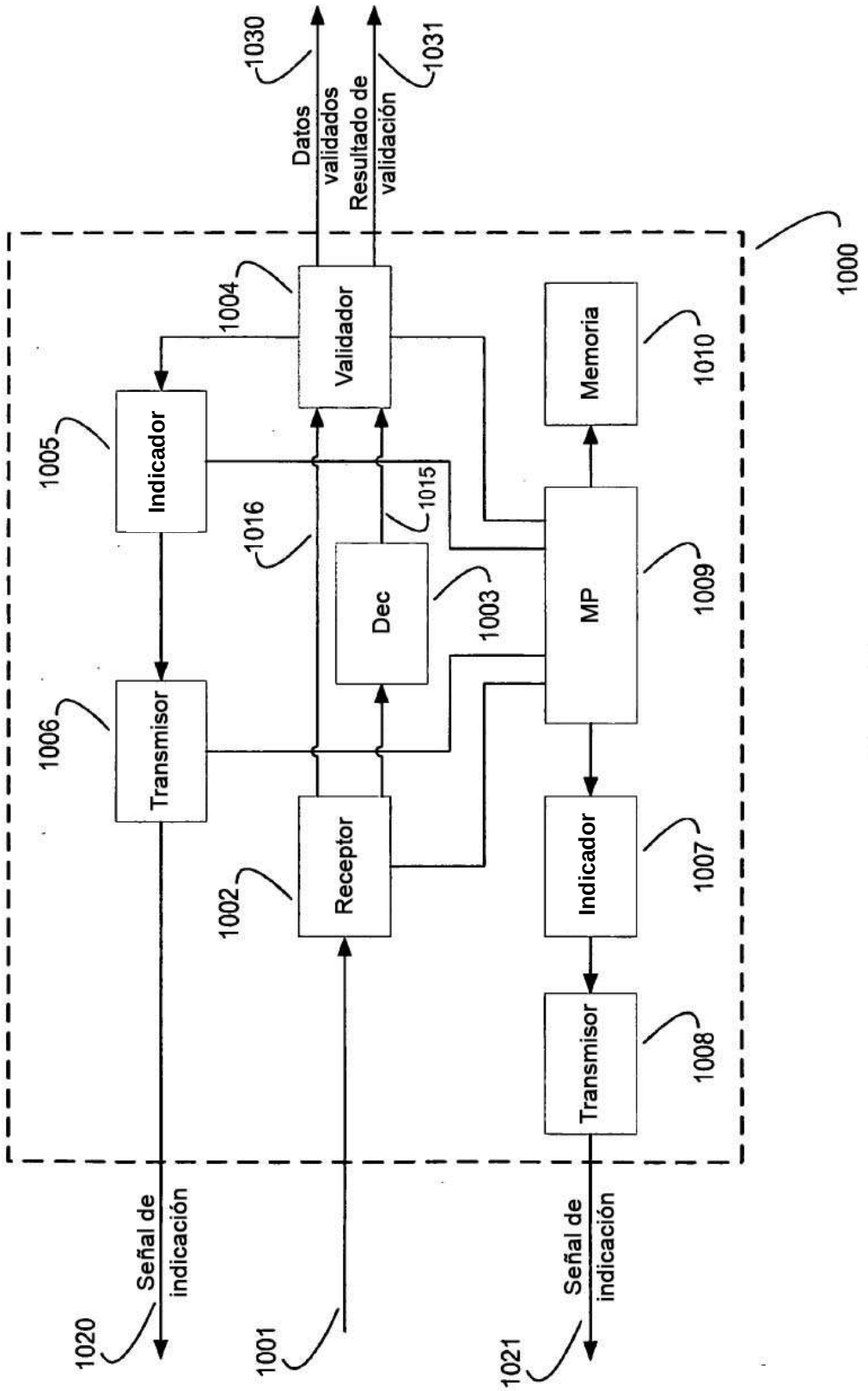
1030
Datos validados
1031
Resultado de validación
1000
1004
Validador
Memoria
1010
1005
Indicador
1015
1016
Dec
1003
MP
1009
1006
Transmisor
1002
Receptor
Indicador
1007
Transmisor
1008
Señal de indicación
1020
1001
Señal de indicación
1021

Figura 5

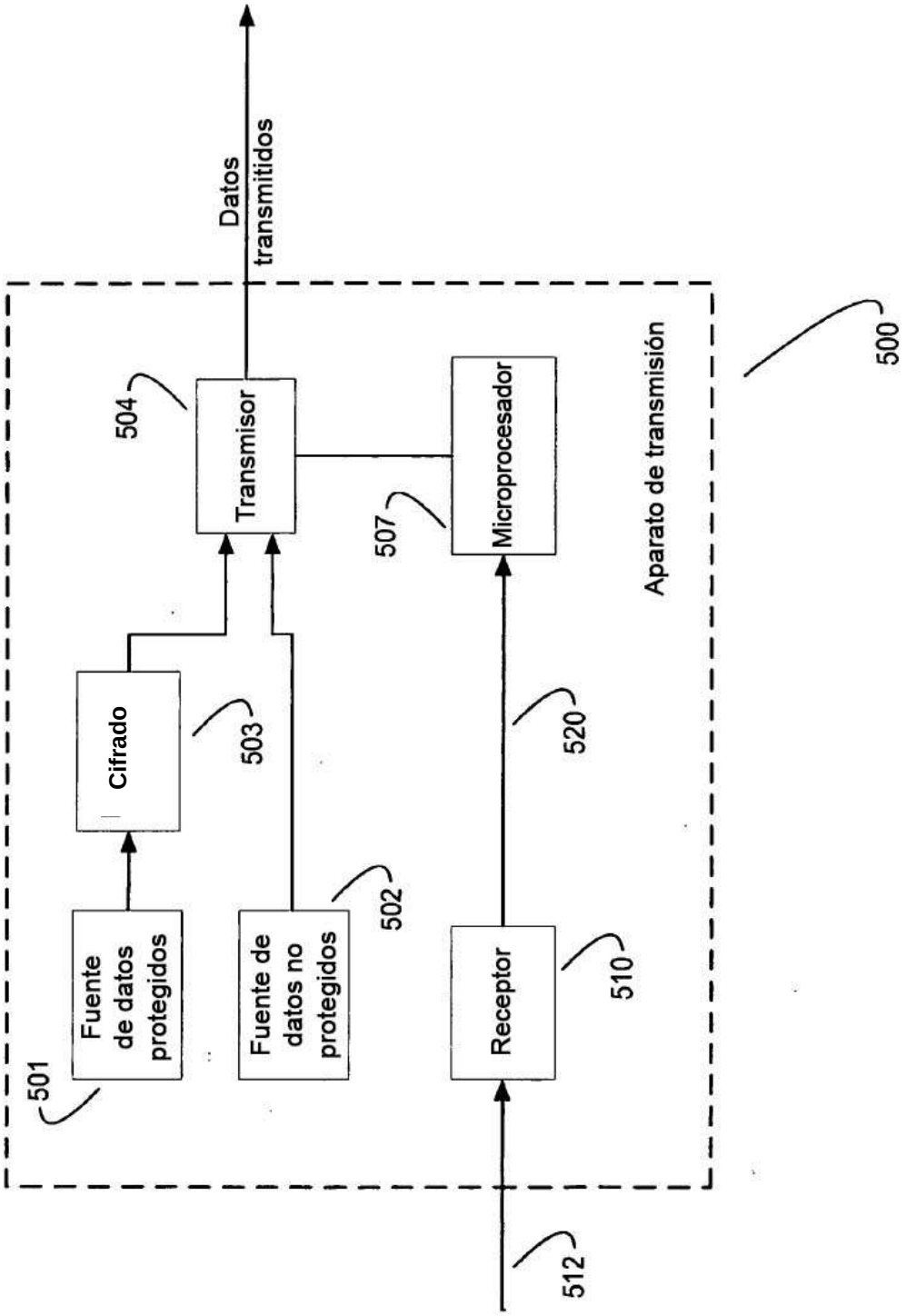
Datos transmitidos
504
Transmisor
507
Microprocesador
500
Aparato de transmisión
Cifrado
503
520
Fuente de datos protegidos
501
Fuente de datos no protegidos
502
Receptor
510
512

Figura 6

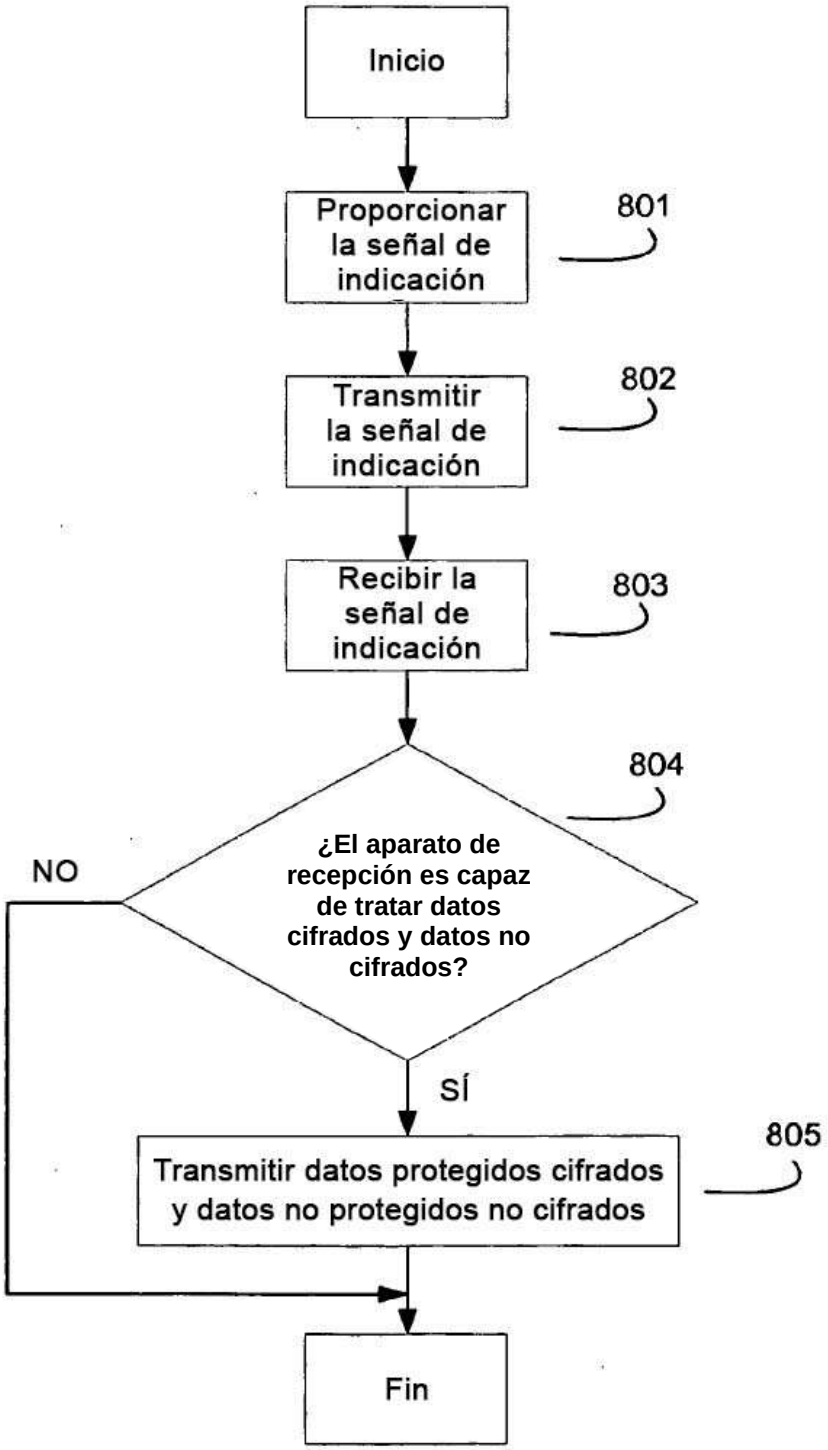
Inicio
Proporcionar la señal de indicación
801
Transmitir la señal de indicación
802
Recibir la señal de indicación
803
804
¿El aparato de recepción es capaz de tratar datos cifrados y datos no cifrados?
NO
SÍ
Transmitir datos protegidos cifrados y datos no protegidos no cifrados
805
Fin

Figura 7

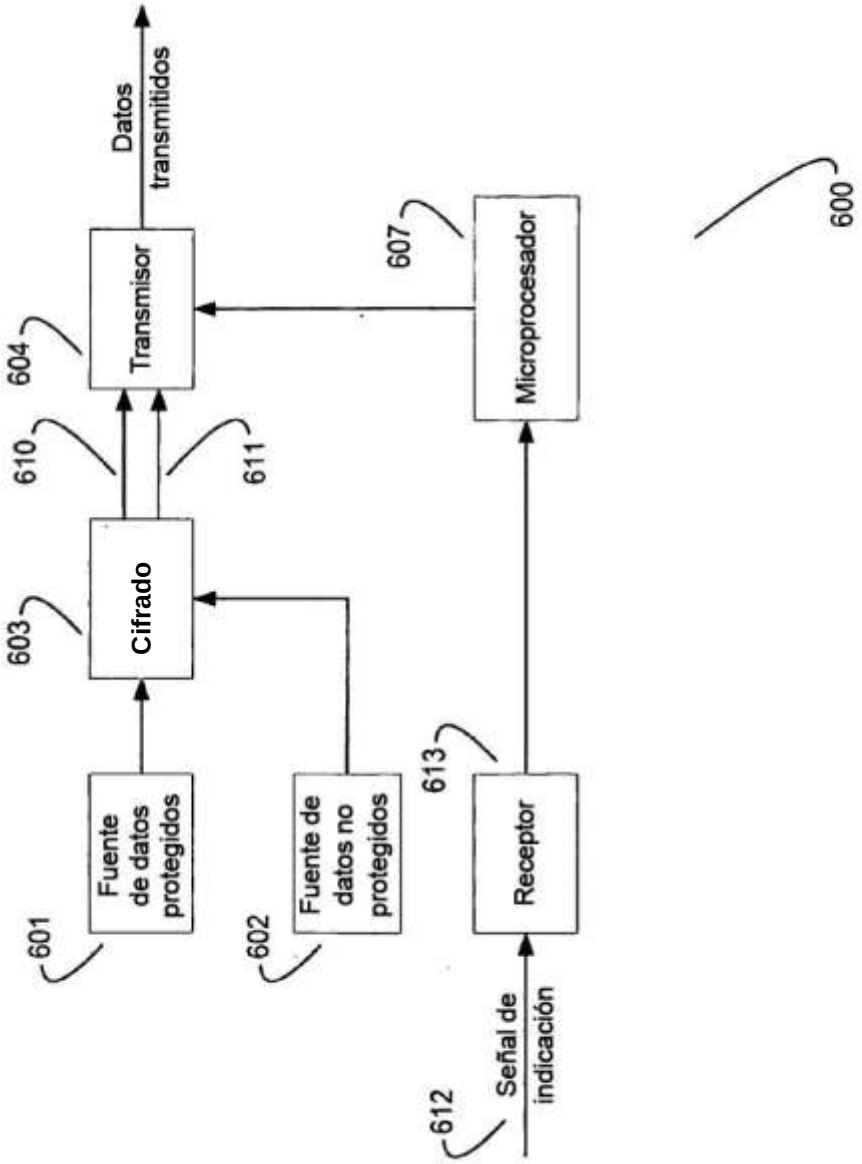
Datos transmitidos
Transmisor
Microprocesador
Cifrado
Fuente de datos protegidos
Fuente de datos no protegidos
Receptor
Señal de indicación
600
601
602
603
604
607
610
611
612
613

Figura 8

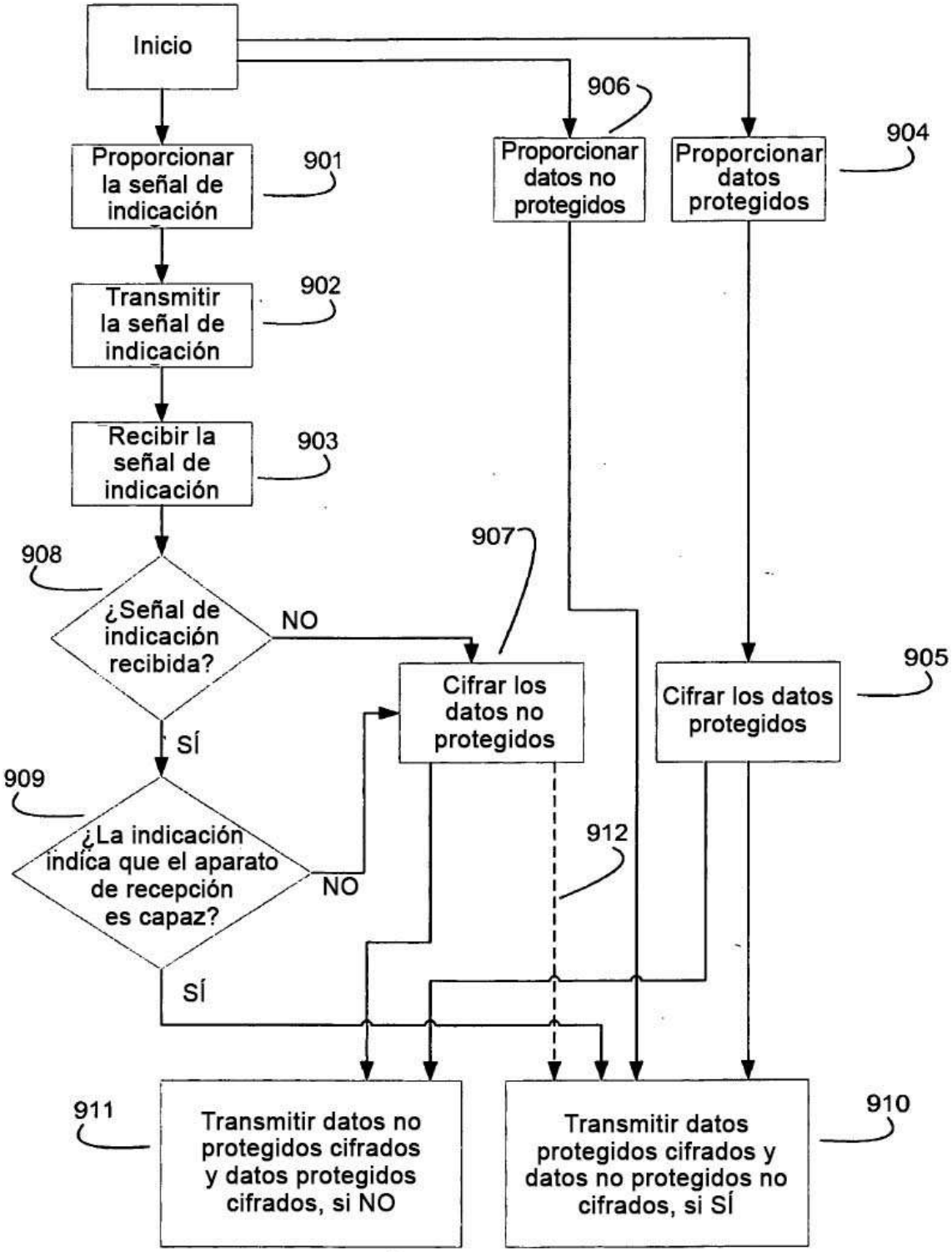
Inicio
Proporcionar la señal de indicación
901
Transmitir la señal de indicación
902
Recibir la señal de indicación
903
¿Señal de indicación recibida?
908
NO
SÍ
¿La indicación indica que el aparato de recepción es capaz?
909
NO
SÍ
906
Proporcionar datos no protegidos
904
Proporcionar datos protegidos
907
Cifrar los datos no protegidos
905
Cifrar los datos protegidos
912
911
Transmitir datos no protegidos cifrados y datos protegidos cifrados, si NO
910
Transmitir datos protegidos cifrados y datos no protegidos no cifrados, si SÍ

Figura 9

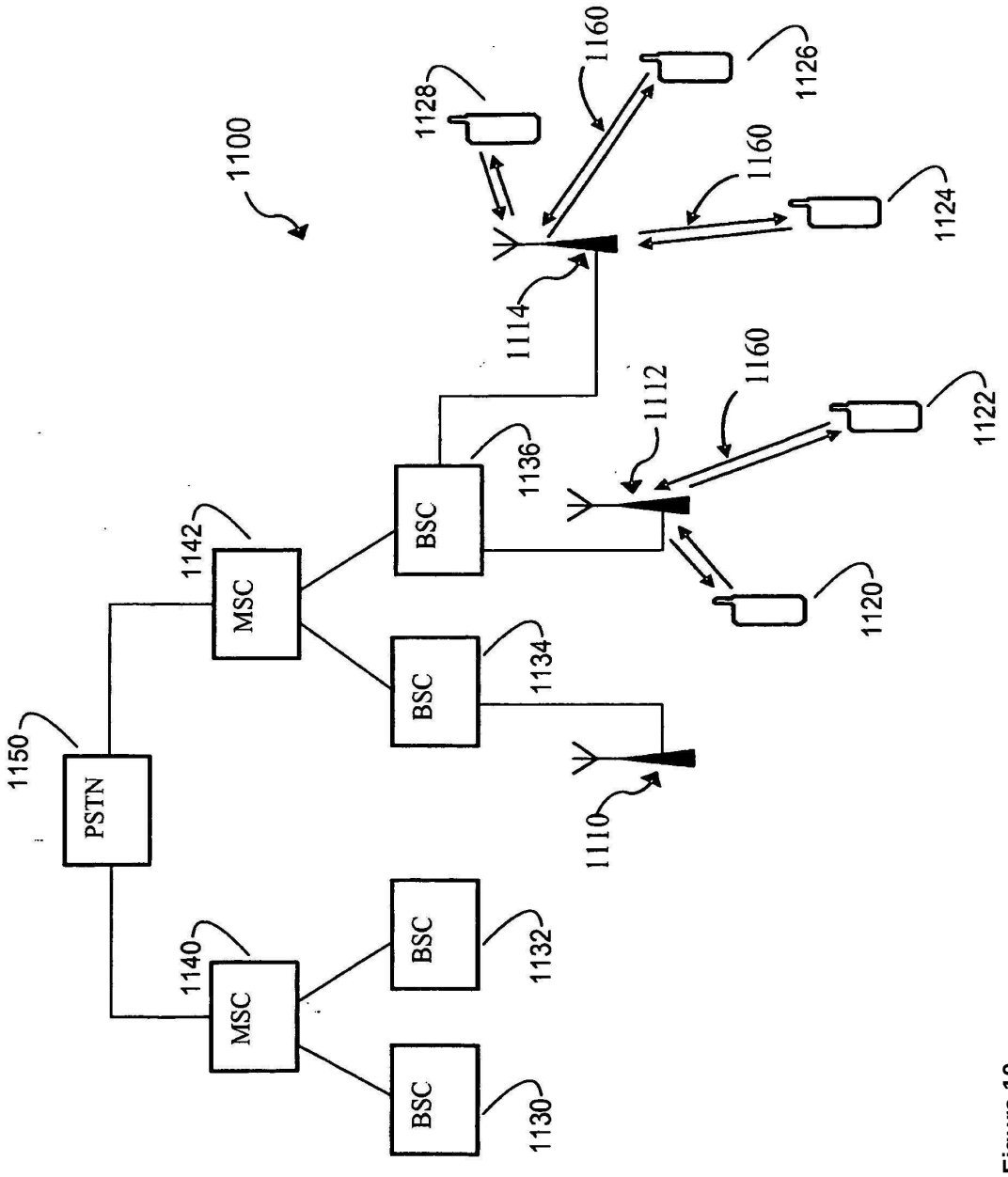
1100
1128
1160
1126
1160
1124
1114
1160
1122
1112
1136
BSC
1142
MSC
BSC
1134
1120
1150
PSTN
1110
1140
MSC
BSC
1132
BSC
1130

Figura 10

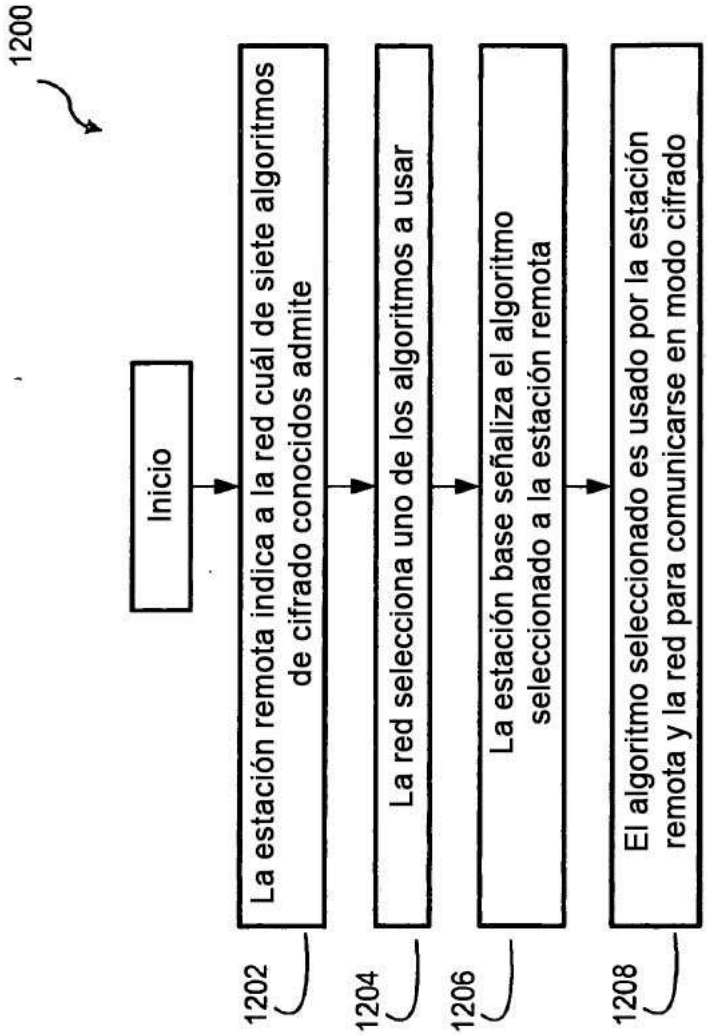
1200
Inicio
La estación remota indica a la red cuál de siete algoritmos de cifrado conocidos admite
La red selecciona uno de los algoritmos a usar
La estación base señaliza el algoritmo seleccionado a la estación remota
El algoritmo seleccionado es usado por la estación remota y la red para comunicarse en modo cifrado
1202
1204
1206
1208

Figura 11

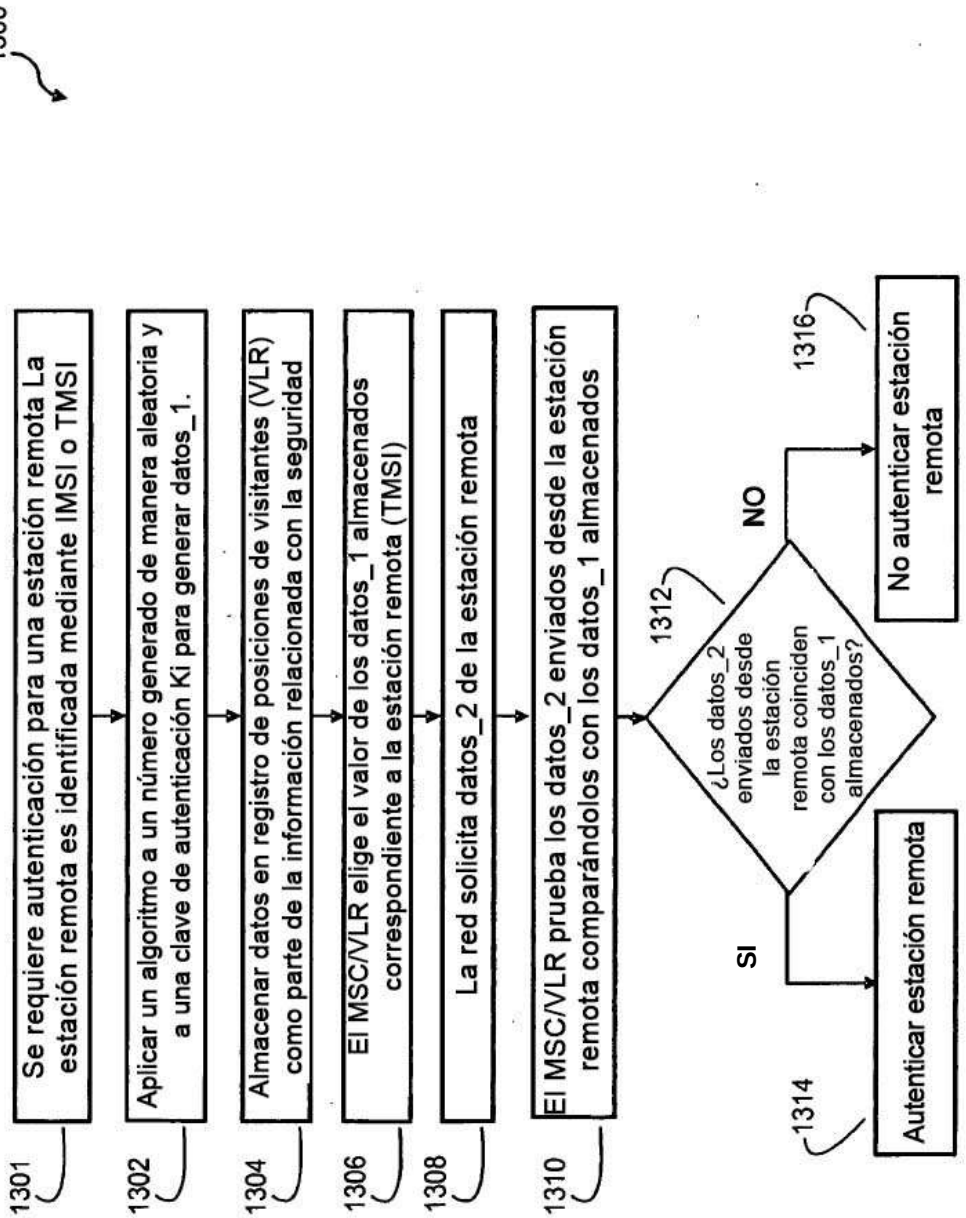
1300
1301
Se requiere autenticación para una estación remota La estación remota es identificada mediante IMSI o TMSI
1302
Aplicar un algoritmo a un número generado de manera aleatoria y a una clave de autenticación Ki para generar datos_1.
1304
Almacenar datos en registro de posiciones de visitantes (VLR) como parte de la información relacionada con la seguridad
1306
El MSC/VLR elige el valor de los datos_1 almacenados correspondiente a la estación remota (TMSI)
1308
La red solicita datos_2 de la estación remota
1310
El MSC/VLR prueba los datos_2 enviados desde la estación remota comparándolos con los datos_1 almacenados
1312
¿Los datos_2 enviados desde la estación remota coinciden con los datos_1 almacenados?
SI
NO
1314
Autenticar estación remota
1316
No autenticar estación remota

Figura 12

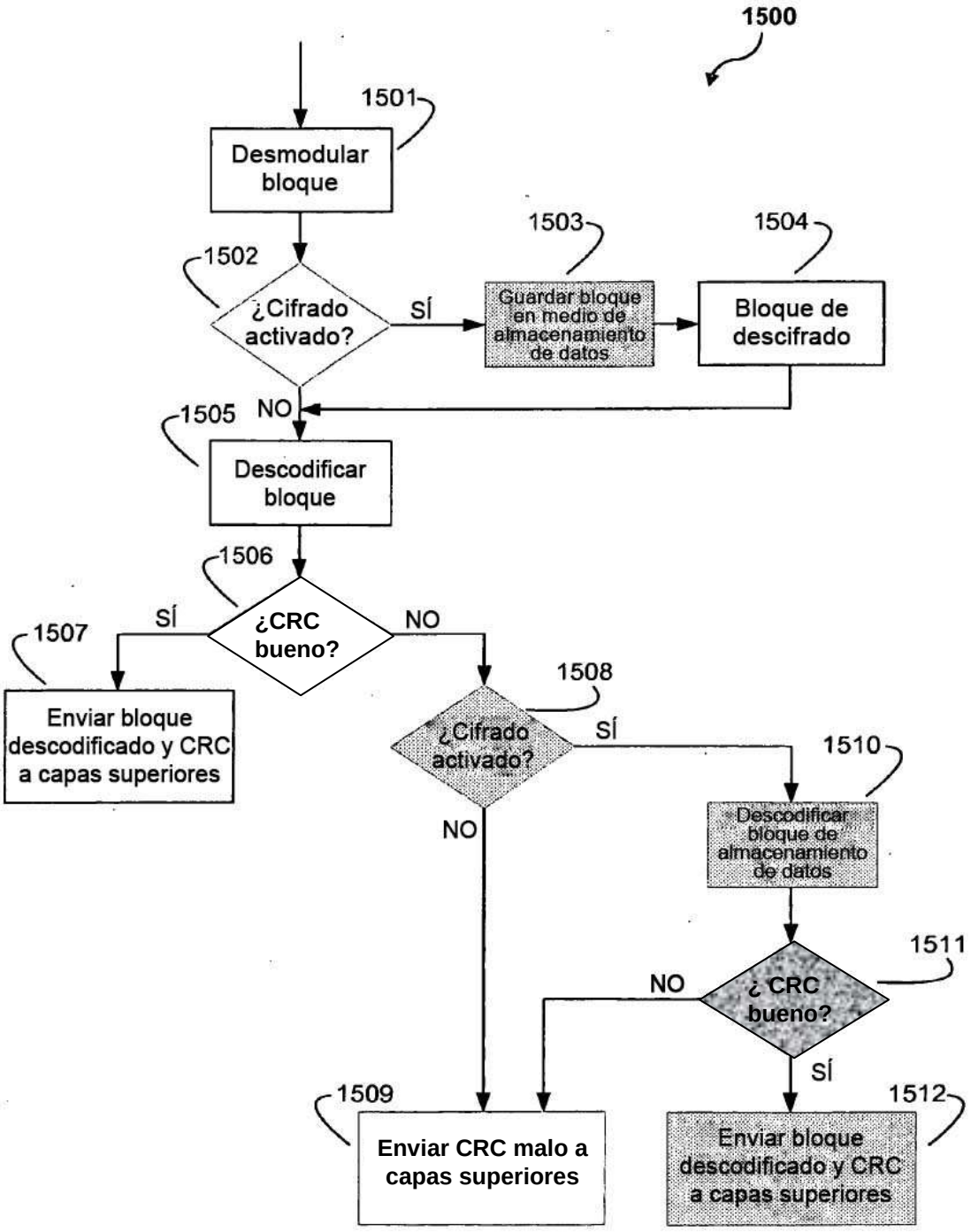
1500
1501
Desmodular bloque
1502
¿Cifrado activado?
SÍ
1503
Guardar bloque en medio de almacenamiento de datos
1504
Bloque de descifrado
NO
1505
Descodificar bloque
1506
¿CRC bueno?
SÍ
1507
Enviar bloque descodificado y CRC a capas superiores
NO
1508
¿Cifrado activado?
SÍ
1510
Descodificar bloque de almacenamiento de datos
NO
1511
¿ CRC bueno?
NO
SÍ
1509
Enviar CRC malo a capas superiores
1512
Enviar bloque descodificado y CRC a capas superiores

Figura 13

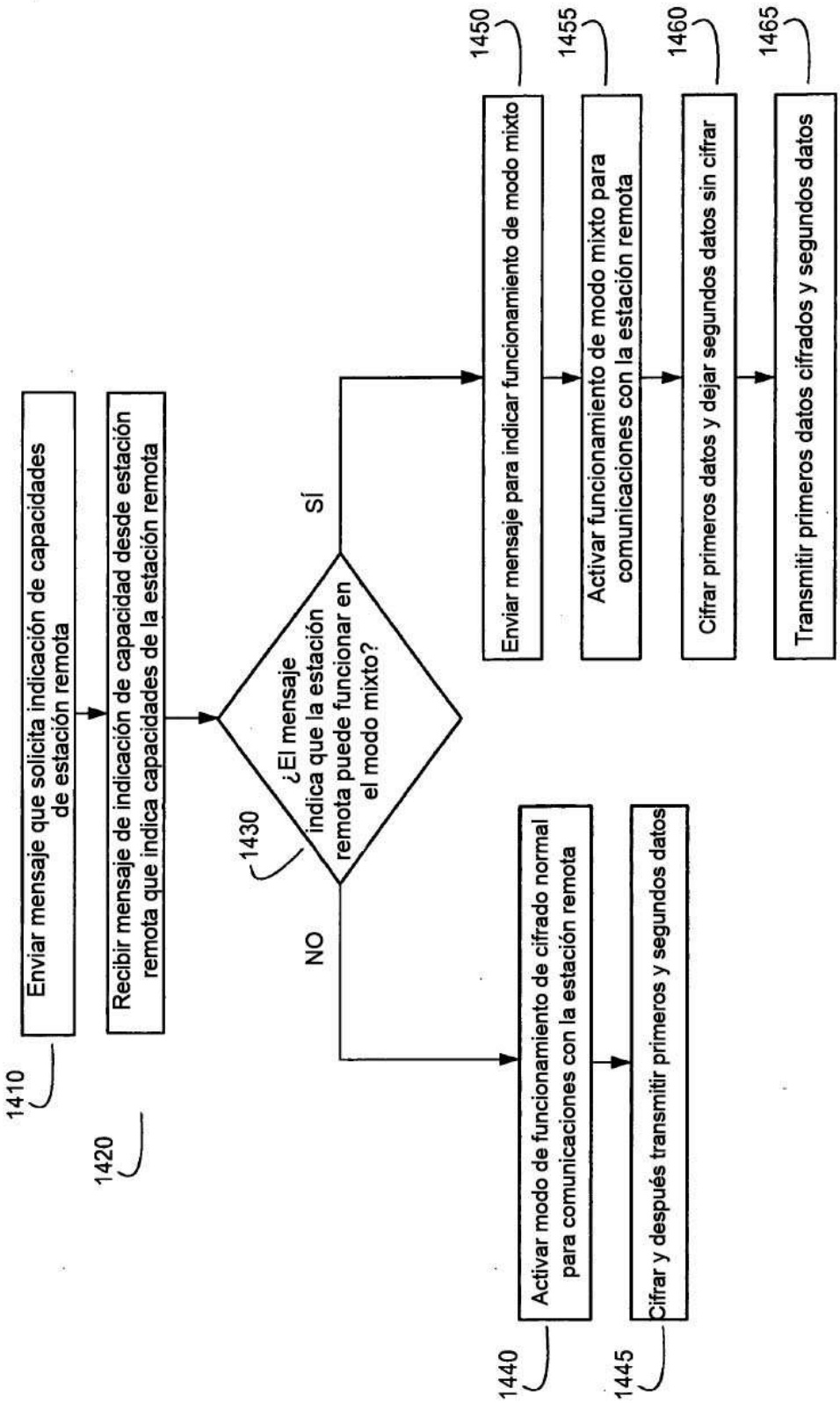
Enviar mensaje que solicita indicación de capacidades de estación remota
Recibir mensaje de indicación de capacidad desde estación remota que indica capacidades de la estación remota
¿El mensaje indica que la estación remota puede funcionar en el modo mixto?
SÍ
NO
Enviar mensaje para indicar funcionamiento de modo mixto
Activar funcionamiento de modo mixto para comunicaciones con la estación remota
Cifrar primeros datos y dejar segundos datos sin cifrar
Transmitir primeros datos cifrados y segundos datos
Activar modo de funcionamiento de cifrado normal para comunicaciones con la estación remota
Cifrar y después transmitir primeros y segundos datos
1410
1420
1430
1440
1445
1450
1455
1460
1465

Figura 14

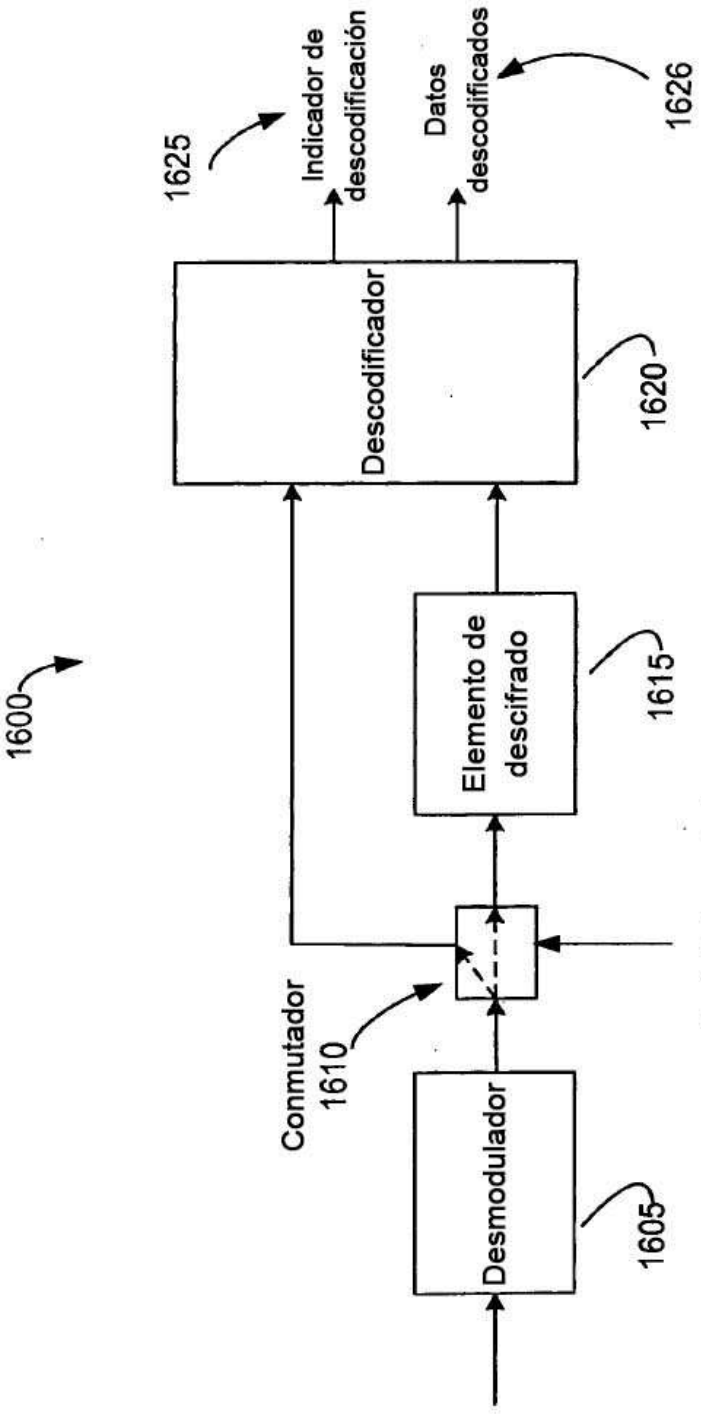
1600
Desmodulador
1605
Conmutador
1610
Señal de control
de conmutador
1612
Elemento de
descifrado
1615
Descodificador
1620
1625
Indicador de
descodificación
Datos
descodificados
1626

Figura 15

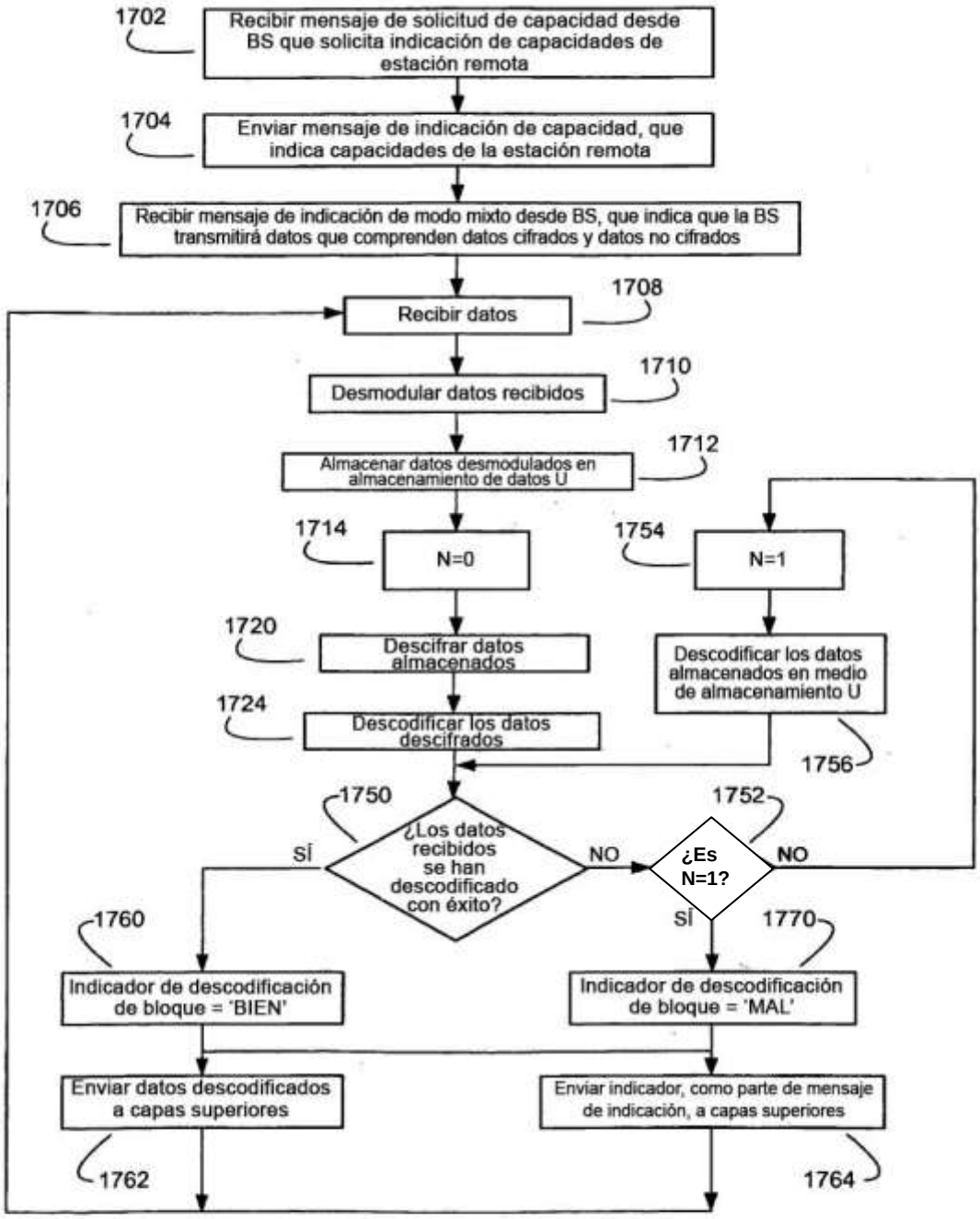
1702
Recibir mensaje de solicitud de capacidad desde BS que solicita indicación de capacidades de estación remota
1704
Enviar mensaje de indicación de capacidad, que indica capacidades de la estación remota
1706
Recibir mensaje de indicación de modo mixto desde BS, que indica que la BS transmitirá datos que comprenden datos cifrados y datos no cifrados
1708
Recibir datos
1710
Desmodular datos recibidos
1712
Almacenar datos desmodulados en almacenamiento de datos U
1714
N=0
1754
N=1
1720
Descifrar datos almacenados
1724
Descodificar los datos descifrados
Descodificar los datos almacenados en medio de almacenamiento U
1756
1750
¿Los datos recibidos se han descodificado con éxito?
SÍ
NO
1752
¿Es N=1?
NO
SÍ
1760
Indicador de descodificación de bloque = 'BIEN'
1770
Indicador de descodificación de bloque = 'MAL'
Enviar datos descodificados a capas superiores
Enviar indicador, como parte de mensaje de indicación, a capas superiores
1762
1764

Figura 16

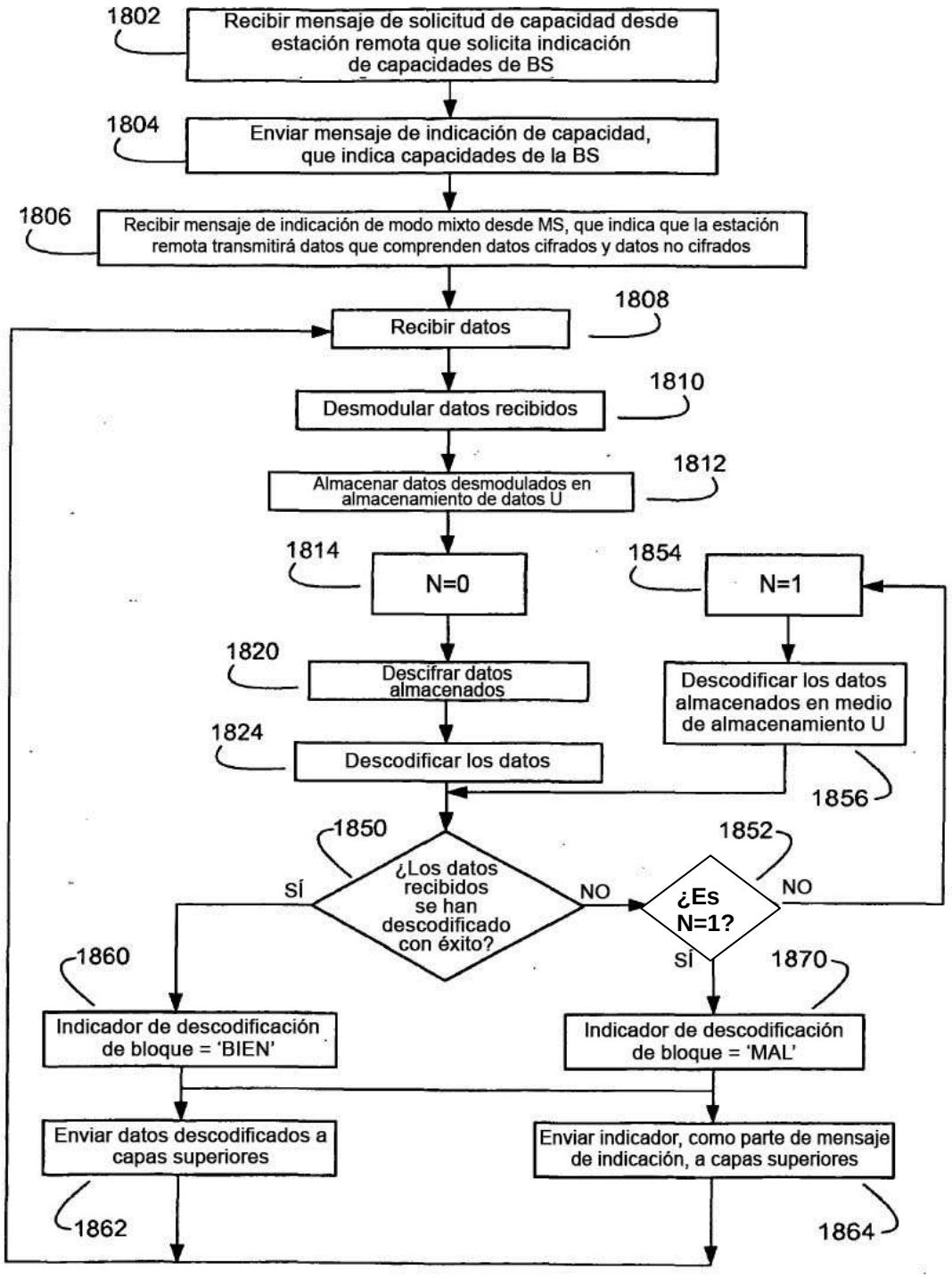
1802
Recibir mensaje de solicitud de capacidad desde estación remota que solicita indicación de capacidades de BS
1804
Enviar mensaje de indicación de capacidad, que indica capacidades de la BS
1806
Recibir mensaje de indicación de modo mixto desde MS, que indica que la estación remota transmitirá datos que comprenden datos cifrados y datos no cifrados
1808
Recibir datos
1810
Desmodular datos recibidos
1812
Almacenar datos desmodulados en almacenamiento de datos U
1814
N=0
1854
N=1
1820
Descifrar datos almacenados
1824
Descodificar los datos
Descodificar los datos almacenados en medio de almacenamiento U
1856
1850
¿Los datos recibidos se han descodificado con éxito?
SÍ
NO
1852
¿Es N=1?
NO
SÍ
1860
Indicador de descodificación de bloque = 'BIEN'
1870
Indicador de descodificación de bloque = 'MAL'
Enviar datos descodificados a capas superiores
Enviar indicador, como parte de mensaje de indicación, a capas superiores
1862
1864

Figura 17

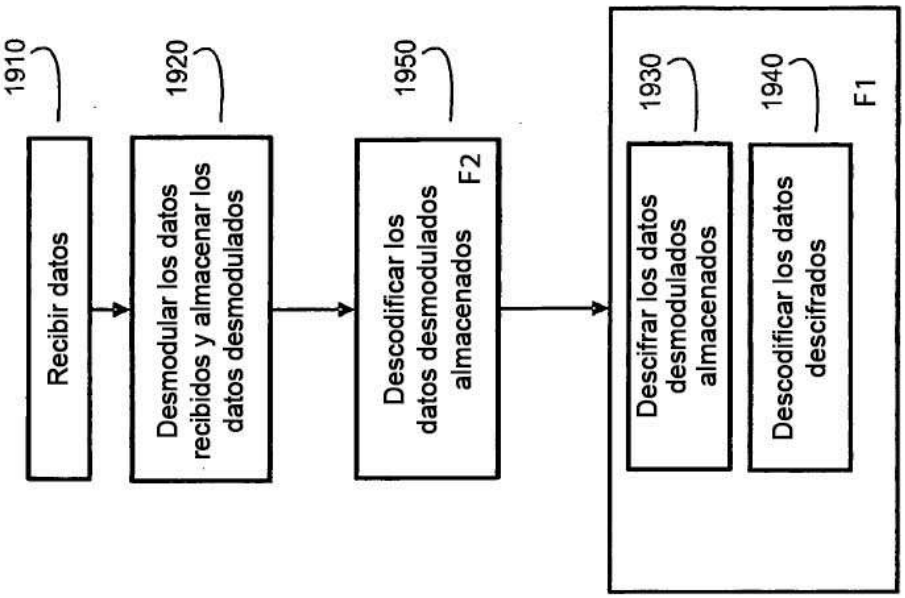


Figura 19

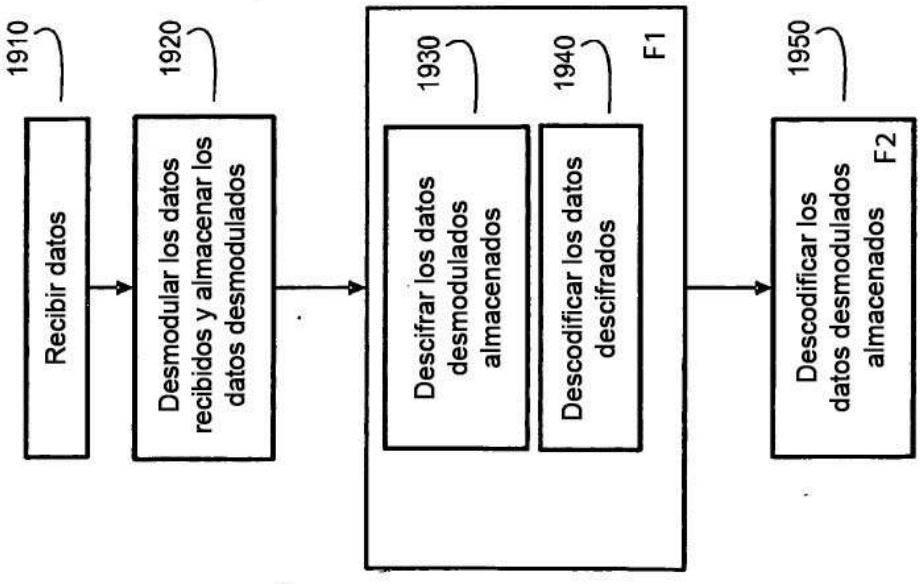


Figura 18

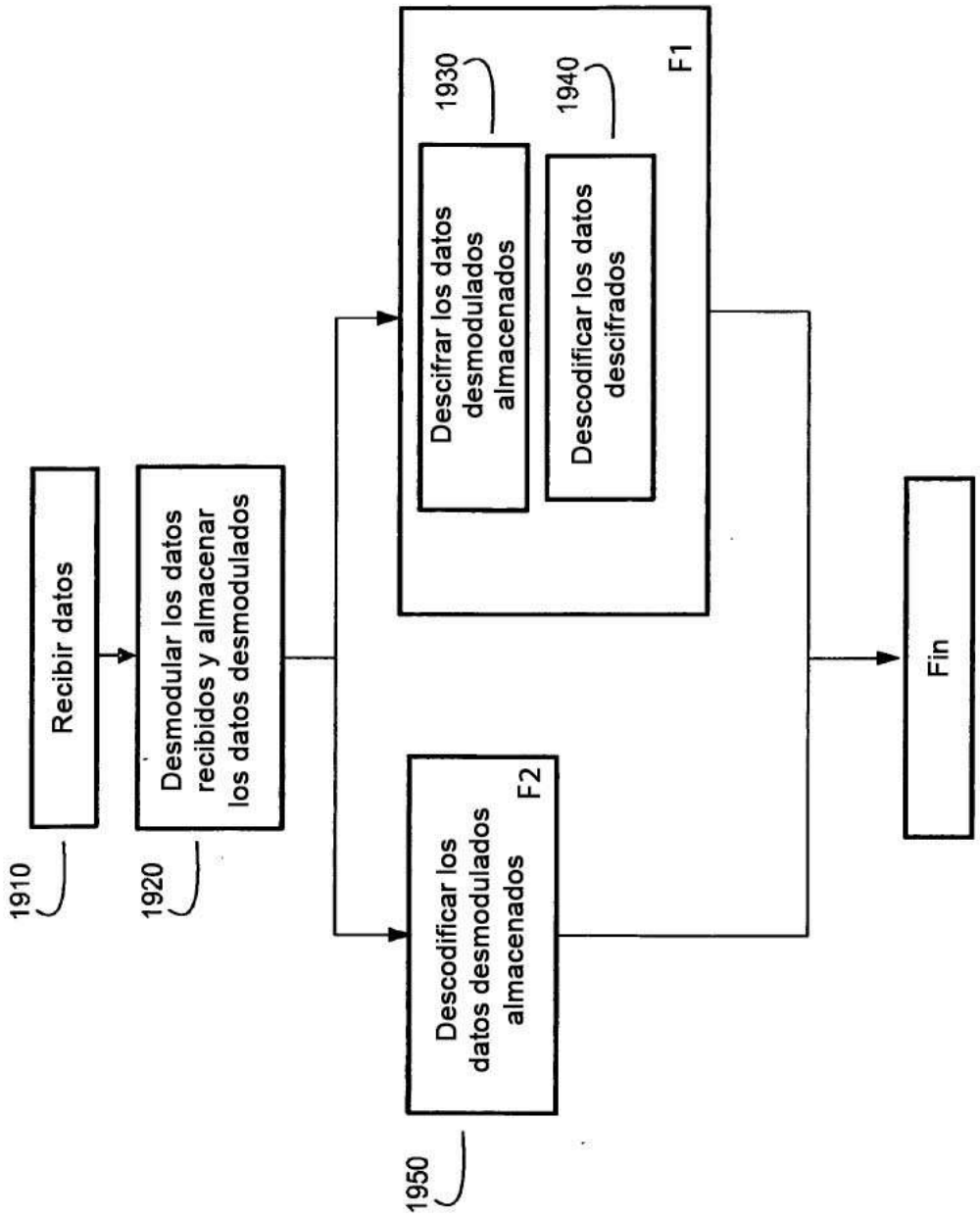
Recibir datos
1910
Desmodular los datos recibidos y almacenar los datos desmodulados
1920
F1
1930
Descifrar los datos desmodulados almacenados
1940
Descodificar los datos descifrados
F2
Descodificar los datos desmodulados almacenados
1950
Fin

Figura 20