(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 566 160**

(51) Int. CI.:

H04L 9/08 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **05.07.2010 E 10794465 (4)**

(97) Fecha y número de publicación de la concesión europea: **27.01.2016 EP 2361462**

(54) Título: **Método para generar una clave de cifrado/descifrado**

(30) Prioridad:

03.07.2009 SE 0900918
03.07.2009 US 222949 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
11.04.2016

(73) Titular/es:

KELISEC AB (100.0%)
Björn Backmans väg 2
148 32 Ösmo, SE

(72) Inventor/es:

REVELL, ELISE

DESCRIPCIÓN

Método para generar una clave de cifrado/descifrado

Campo técnico

La presente invención se refiere a un método para generar una clave de cifrado/descifrado, y especialmente para generar una clave de cifrado/descifrado de un único uso usada para cifrado simétrico, es decir en el que la misma clave se usa tanto para el cifrado como para el descifrado. La presente invención se refiere además a un programa informático que comprende medios de código para realizar el método cuando se ejecuta en un ordenador y a un producto de programa informático que comprende medios de código de programa almacenados en un medio legible por ordenador para realizar el método, cuando se ejecuta dicho producto en un ordenador.

Antecedentes

En criptografía, una clave es información que determina la salida funcional de un algoritmo criptográfico. Sin una clave, el algoritmo no tendría ningún resultado. En el cifrado, una clave especifica la transformación particular de texto en claro al texto cifrado, o viceversa durante el descifrado. También se usan claves en otros algoritmos criptográficos, tales como esquemas de firma digital y códigos de autentificación de mensajes.

Con frecuencia se dice que al diseñar sistemas de seguridad, es aconsejable suponer que un atacante puede disponer fácilmente de los detalles del algoritmo criptográfico. Este principio se conoce como el principio de Kerckhoffs y por tanto sólo el secretismo de la clave proporciona seguridad. Este principio se basa en el hecho de que es difícil mantener secretos los detalles de un algoritmo ampliamente usado. Con frecuencia es más fácil proteger una clave, ya que con frecuencia es poca información en comparación con el algoritmo de cifrado. Sin embargo, también puede ser difícil mantener secreta una clave y si el atacante obtiene la clave de alguna manera puede recuperar el mensaje original a partir de los datos cifrados.

Tal como se mencionó anteriormente, los algoritmos de cifrado que usan la misma clave tanto para el cifrado como para el descifrado se conocen como algoritmos de clave simétrica. También hay algoritmos de clave asimétrica que usan un par de claves, una para cifrar y una para descifrar. Estos algoritmos de clave asimétrica permiten hacer pública una clave mientras que la clave privada se conserva en una única ubicación. Están diseñados de modo que hallar la clave privada es extremadamente difícil, aunque se conozca la clave pública correspondiente. Un usuario de tecnología de clave pública puede publicar su clave pública, mientras se mantiene secreta su clave privada, permitiendo que cualquiera les envíe un mensaje cifrado.

Con el fin de que una clave sea “segura” junto con algoritmos de cifrado simétrico generalmente se considera que una longitud de 80 bits es lo mínimo y habitualmente se usan claves de 128 bits y se consideran muy fuertes. Las claves usadas en criptografía de clave pública tienen cierta estructura matemática. Por ejemplo, las claves públicas usadas en el sistema de RSA son el producto de dos números primos. Por tanto, los sistemas de clave pública requieren longitudes de clave más largas que los sistemas simétricos para un nivel de seguridad equivalente. La longitud de clave sugerida es de 3072 bits para sistemas basados en factorización y algoritmos discretos de números enteros que tienen el objetivo de tener una seguridad equivalente a un cifrado simétrico de 128 bits.

Tal como se mencionó anteriormente es posible generar claves con un alto grado de seguridad, si son lo bastante largas para claves basadas tanto en algoritmos simétricos como asimétricos. Sin embargo, existe un problema en la distribución de claves. Si, por ejemplo, dos partes desean comunicarse entre sí usando criptografía simétrica, primero deben decidir qué clave usar y después distribuirla de manera segura de una parte a la otra. Además, la clave tiene que mantenerse secreta por las dos partes. El riesgo de que un intruso pueda hallar la clave aumenta con el tiempo en el que la clave está en uso. Por tanto, normalmente una clave sólo es válida durante un tiempo limitado, por ejemplo seis o doce meses. Después de ese tiempo tiene que distribuirse una nueva clave.

Además, la distribución de claves para cifrado por criptografía asimétrica encuentra problemas con la distribución de claves cuando dos partes desean comunicarse entre sí. Con el fin de enviar información en ambos sentidos necesitan intercambiar claves públicas entre sí. Además, en este caso las claves tienen habitualmente un periodo de tiempo limitado durante el cual son válidas. Para una parte que se comunica con muchas partes diferentes, la gestión de la distribución de claves públicas válidas puede ser molesta. Un ejemplo típico es que la validez de una clave ha caducado cuando se necesita enviar alguna información secreta de manera urgente a otra parte o aún no se han intercambiado claves públicas.

Otro tipo de criptografía es la criptografía cuántica, que usa mecánica cuántica para garantizar una comunicación segura. Permite que dos partes produzcan una cadena de bits aleatoria compartida que sólo ellas conocen, que puede usarse como clave para cifrar y descifrar mensajes. Una propiedad importante y única de la criptografía cuántica es la capacidad de los dos usuarios en comunicación de detectar la presencia de cualquier tercero que intenta conocer la clave. Esto es el resultado de un aspecto fundamental de la mecánica cuántica, es decir el proceso de medir un sistema cuántico afectará al sistema. Dado que un tercero que intenta escuchar la clave de

algún modo tiene que medirla, habrá anomalías detectables. Por tanto, la seguridad de la criptografía cuántica se basa en los fundamentos de la mecánica cuántica, al contrario que la criptografía de clave pública tradicional que se basa en la dificultad computacional de determinadas funciones matemáticas, y por tanto no puede proporcionar ninguna indicación de escuchas ni garantía de seguridad de la clave.

La criptografía cuántica sólo se usa para producir y distribuir una clave, no para transmitir ningún dato de mensaje. Entonces puede usare esta clave con cualquier algoritmo de cifrado elegido para cifrar y descifrar un mensaje, que entonces puede transmitirse por un canal de comunicación convencional.

Aunque la generación de clave con criptografía cuántica proporciona una manera muy segura de generar y distribuir una clave, también tiene un inconveniente principal. La distancia por la que puede distribuirse una clave cuántica está limitada a aproximadamente 100 kilómetros, debido a las propiedades de la mecánica cuántica.

En los documentos US 2002/0159598, WO 03/009513 y US 7 043 633 se dan a conocer soluciones adicionales de la técnica anterior.

Dados los problemas mencionados anteriormente existe una necesidad de una manera sencilla para generar y distribuir una clave criptográfica.

Sumario de invención

El problema que va a resolver la presente invención es generar una clave criptográfica, que no necesite distribuirse a los nodos que desean comunicarse entre sí, es decir en la que la clave se genera por los propios nodos.

Este problema se resuelve según un primer aspecto mediante un método para generar una clave de cifrado/descifrado, que puede usarse para una comunicación segura entre un primer nodo y un segundo nodo. El método comprende las etapas de:

enviar una petición desde el primer nodo A hasta un servidor central para configurar una comunicación segura con el segundo nodo,

enviar desde el servidor central un primer archivo de generación de clave al primer nodo y un segundo archivo de generación de clave al segundo nodo en respuesta a la petición del primer nodo,

procesar el primer archivo de generación de clave en el primer nodo y el segundo archivo de generación de clave en el segundo nodo,

generar un primer conjunto de datos intermedio en el primer nodo y un segundo conjunto de datos intermedio en el segundo nodo,

enviar el primer conjunto de datos intermedio desde el primer nodo al segundo nodo,

comparar bits del primer conjunto de datos intermedio con bits correspondientes del segundo conjunto de datos intermedio,

crear un tercer conjunto de datos intermedio nuevo basándose en la comparación bit a bit entre el primer y el segundo conjunto de datos intermedio estableciendo un primer valor si los bits comparados son iguales y un segundo valor si los bits comparados no son iguales,

enviar el tercer conjunto de datos intermedio desde el segundo nodo al primer nodo,

comparar bits del tercer conjunto de datos intermedio con los bits correspondientes del primer conjunto de datos intermedio,

generar una primera clave de cifrado basándose en la comparación bit a bit entre el tercer y el primer conjunto de datos intermedio manteniendo el valor del bit del primer conjunto de datos intermedio si el bit correspondiente del tercer conjunto de datos intermedio se establece al primer valor e ignorando el bit del primer conjunto de datos intermedio si el bit correspondiente del tercer conjunto de datos intermedio se establece al segundo valor,

generar una segunda clave de cifrado basándose en la comparación bit a bit entre el primer y el segundo conjunto de datos intermedio manteniendo el valor del bit del segundo conjunto de datos intermedio si el bit correspondiente del primer conjunto de datos intermedio es igual e ignorando el bit del segundo conjunto de datos intermedio si los bits comparados no son iguales, siendo dicha primera y segunda clave de cifrado la misma.

Según un segundo aspecto de la presente invención el problema se resuelve mediante un método para generar una clave de cifrado/descifrado en un primer nodo, que puede usarse para una comunicación segura entre el primer

nodo y un segundo nodo. El método según el segundo aspecto comprende las etapas de:

enviar una petición a un servidor central para configurar una comunicación segura con el segundo nodo,

recibir un primer archivo de generación de clave del servidor central en respuesta a la petición,

procesar el primer archivo de generación de clave,

generar un primer conjunto de datos intermedio,

enviar el primer conjunto de datos intermedio al segundo nodo,

recibir un tercer conjunto de datos intermedio del segundo nodo,

comparar bits del tercer conjunto de datos intermedio con bits correspondientes del primer conjunto de datos intermedio,

generar una primera clave de cifrado basándose en la comparación bit a bit entre el tercer y el primer conjunto de datos intermedio manteniendo el valor del bit del primer conjunto de datos intermedio si el bit correspondiente del tercer conjunto de datos intermedio se establece a un primer valor e ignorando el bit del primer conjunto de datos intermedio si el bit correspondiente del tercer conjunto de datos intermedio se establece a un segundo valor.

Según un tercer aspecto de la presente invención el problema se resuelve mediante un método para generar una clave de cifrado/descifrado en un segundo nodo, que puede usarse para una comunicación segura entre un primer nodo y el segundo nodo. Según el tercer aspecto el método comprende las etapas de:

recibir un segundo archivo de generación de clave de un servidor central en respuesta a una petición del primer nodo para comenzar una comunicación segura entre el primer nodo y el segundo nodo,

procesar el segundo archivo de generación de clave,

generar un segundo conjunto de datos intermedio,

recibir un primer conjunto de datos intermedio del primer nodo,

comparar bits del primer conjunto de datos intermedio con bits correspondientes del segundo conjunto de datos intermedio,

crear un tercer conjunto de datos intermedio nuevo basándose en la comparación bit a bit entre el primer y el segundo conjunto de datos intermedio estableciendo un primer valor si los bits comparados son iguales y un segundo valor si los bits comparados no son iguales,

enviar el tercer conjunto de datos intermedio al primer nodo,

generar una segunda clave de cifrado basándose en la comparación bit a bit entre el primer y el segundo conjunto de datos intermedio manteniendo el valor del bit del segundo conjunto de datos intermedio si el bit correspondiente del primer conjunto de datos intermedio es igual e ignorando el bit del segundo conjunto de datos intermedio si los bits comparados no son iguales.

Según una realización preferida de la presente invención la etapa de enviar el primer y el segundo archivo de generación de clave también comprende enviar metadatos adjuntos a cada archivo de generación de clave, respectivamente.

En aún otra realización preferida de la presente invención los metadatos comprenden una constante que va a usarse para la generación tanto de la primera como de la segunda clave de cifrado. Los metadatos también pueden comprender información sobre la longitud de clave de cifrado.

En otra realización la longitud de clave puede generarse aleatoriamente, dentro de un intervalo predeterminado.

Según un cuarto aspecto de la invención se proporciona un programa informático que comprende medios de código para realizar las etapas del método, cuando el programa se ejecuta en un ordenador.

Según un quinto aspecto de la invención se proporciona un producto de programa informático, que comprende medios de código de programa almacenados en un medio legible por ordenador para realizar las etapas del método, cuando se ejecuta dicho producto en un ordenador.

El gran beneficio de la presente invención es que la clave se genera en los nodos que desean comunicarse entre sí y por tanto no hay necesidad de distribución de clave.

Breve descripción de los dibujos

A continuación se describe la invención con referencia a los dibujos adjuntos, en los que

la figura 1 es un diagrama de flujo que muestra el método para generar una clave criptográfica según la presente invención,

la figura 2 es un ejemplo de un archivo de generación de clave enviado desde el servidor central a los nodos que desean comunicarse,

la figura 3 es un ejemplo de una constante usada para generar el primer y el segundo conjunto de datos intermedio,

la figura 4 es un ejemplo del primer conjunto de datos intermedio en el primer nodo A y el segundo conjunto de datos intermedio en el segundo nodo B,

la figura 5 es un ejemplo de un procedimiento de correspondencia entre el primer y el segundo conjunto de datos intermedio y la generación de una clave criptográfica para el segundo nodo B, y

la figura 6 es un ejemplo de la generación de una clave criptográfica para el primer nodo A.

Descripción detallada la invención

Ahora se describirá la presente invención en detalle con ayuda de diferentes realizaciones de la misma. Las realizaciones deben considerarse como ejemplos y explicativas para comprender la invención y no como limitativas.

La figura 1 muestra el método para generar una clave criptográfica según la presente invención. El método global se ejecuta mediante dos nodos A y B que desean configurar una comunicación segura entre sí usando una clave de cifrado/descifrado segura. Además, el método se ejecuta con ayuda de un servidor 2 central. En la figura 1, el primer nodo A se muestra a la izquierda y el segundo nodo B a la derecha, es decir las etapas realizadas por el primer nodo A se muestran a la izquierda de la línea discontinua y las etapas realizadas por el segundo nodo B se muestran a la derecha de la línea discontinua. En la práctica el primer nodo A puede ser un ordenador, cuyo usuario puede desear comenzar una comunicación segura con un ordenador, el segundo nodo B, en su banco. Tal como resulta evidente para un experto en la técnica, tanto el primer nodo A como el segundo nodo B pueden ser cualquier dispositivo de comunicación que deseen comunicarse entre sí.

El servidor 2 central puede ser cualquier dispositivo de comunicación que puede recibir y enviar datos de una manera segura con ayuda de alguna clase de certificado de seguridad. Con el fin de que un nodo pueda usar el método de generación de clave según la presente invención, el nodo necesita estar autorizado para comunicarse con el servidor 2 central. Por tanto, el servidor 2 central mantiene un registro de todos los usuarios que están autorizados para usar el método de generación de clave. Tal como se mencionó anteriormente la comunicación entre el servidor 2 central y los nodos o viceversa es segura al usar alguna clase de certificado de seguridad. Preferiblemente, se usa un certificado X509 o similar para una comunicación segura.

Ahora se describirá el método para generar una clave de cifrado/descifrado según la presente invención mediante un ejemplo. El método comienza con que un nodo, en este ejemplo el primer nodo A, envía una petición al servidor 2 central para configurar una comunicación segura con el segundo nodo B. El servidor 2 central comprueba en primer lugar si el primer nodo A está autorizado para configurar una comunicación con el segundo nodo B y también que el segundo nodo B está autorizado para comunicarse con el servidor 2 central y el primer nodo A. Si ambos nodos están autorizados para comenzar una comunicación entre sí, el servidor 2 central, en respuesta a la petición del primer nodo A, enviará un primer archivo de generación de clave al primer nodo A y un segundo archivo de generación de clave al segundo nodo B.

La figura 2 muestra un ejemplo de un archivo de generación de clave que se envía desde el servidor central al primer nodo A y al segundo nodo B. El archivo contiene un archivo de procedimiento, que cuando se ejecuta por el primer nodo A y el segundo nodo B generará la clave de cifrado/descifrado. Dado que el procedimiento en el primer nodo A y el segundo nodo B son diferentes, lo cual se explicará a continuación, el archivo de procedimiento enviado al primer nodo A se diferencia del archivo de procedimiento enviado al segundo nodo B. Como resulta evidente a partir de la figura 2, el archivo de generación de clave también contiene metadatos M1, M2...Mn. Los metadatos pueden contener información que va a usarse para generar la clave de cifrado/descifrado y los mismos metadatos se enviarán tanto al primer nodo A como al segundo nodo B. Ejemplos de metadatos son una constante usada para generar las claves. La figura 3 muestra un ejemplo de tal constante usada para generar un primer y un segundo conjunto de datos intermedio usados durante la generación de clave. Los metadatos también pueden contener una etiqueta de tiempo que va a usarse para comparar si ambos archivos de generación de clave tienen el mismo origen.

Además, los metadatos también pueden contener información sobre la longitud de clave que va a usarse o qué bits de la clave deben usarse para generar la clave. Tal como resulta evidente para un experto en la técnica puede haber varios otros metadatos que pueden usarse con el fin de aumentar adicionalmente la seguridad del procedimiento de generación de clave.

Cuando el archivo de generación de clave se ha recibido en el primer nodo A y el segundo nodo B, cada nodo comenzará a procesar el archivo. En primer lugar, el primer nodo A generará un primer conjunto de datos intermedio y el segundo nodo B generará un segundo conjunto de datos intermedio usando el valor de la constante, tal como se representa en la figura 3. La constante contiene, en este caso, cuatro bits binarios asociados cada uno con una letra. La longitud de la constante puede variar de manera arbitraria y los bits pueden asociarse con letras, figuras, símbolos griegos, etc.

En la figura 4 se muestra un ejemplo del primer conjunto de datos intermedio para el primer nodo A y el segundo conjunto de datos intermedio para el segundo nodo B. Los conjuntos de datos intermedios se generan usando alguna clase de generador de números pseudoaleatorio conocido, usando algoritmos pseudoaleatorios tales como Blum Blum Shub, Fortuna o Mersenne twister, para generar una secuencia aleatoria, en este caso, las letras A-D. La secuencia aleatoria de las letras se muestra en el encabezado del primer y el segundo conjunto de datos intermedio en la figura 4. Por tanto, con el fin de generar el conjunto de datos intermedio en primer lugar se determina de manera pseudoaleatoria la secuencia de las letras y posteriormente se asignará el valor correcto asociado con la letra según la constante en la figura 3. Si esta asignación da como resultado la generación, por ejemplo, de sólo ceros o sólo unos para el conjunto de datos intermedio este resultado puede eliminarse por filtración y se genera una nueva secuencia aleatoria.

Dado que tanto el primer como el segundo conjunto de datos intermedio se generan de manera pseudoaleatoria, nunca serán el mismo. La longitud de los conjuntos de datos intermedios en este ejemplo es de tan sólo 8 bits con el fin de ilustrar fácilmente la presente invención en un ejemplo. Sin embargo, en la práctica, la longitud de los conjuntos de datos intermedios es normalmente de entre 64 y 2048 bits. La longitud de bits puede ser parte de los metadatos tal como se mencionó anteriormente y puede establecerse de manera aleatoria por el servidor 2 central cada vez que se realiza una nueva petición desde un nodo.

Tras la generación del primer y el segundo conjunto de datos intermedio, el primer nodo enviará el primer conjunto de datos intermedio al segundo nodo B sin ninguna protección, es decir de manera pública.

El segundo nodo B comparará el primer y el segundo conjunto de datos intermedio entre sí. El resultado de la comparación se denomina Correspondencia 1 en la tabla mostrada en la figura 5. El valor A y el valor B corresponden al primer y al segundo conjunto de datos intermedio, respectivamente. La comparación es una comparación bit a bit y el resultado es Verdadero si el valor para el bit del primer y el segundo conjunto de datos intermedio, respectivamente, es igual y Falso si no son iguales. El resultado, Correspondencia 1, de la comparación se usa para crear un tercer conjunto de datos intermedio nuevo, Valor 1, estableciendo un primer valor si los bits comparados son iguales y un segundo valor si los bits comparados no son iguales. En este caso se usa 1 cuando los bits comparados son iguales y se usa 0 si los bits no son iguales. Sin embargo, también puede ser lo contrario sin apartarse de la presente invención.

Entonces se envía el tercer conjunto de datos intermedio de manera pública desde el segundo nodo B al primer nodo A. Entonces el primer nodo A genera una primera clave criptográfica basándose en una comparación bit a bit entre el tercer y el primer conjunto de datos intermedio manteniendo el valor del bit del primer conjunto de datos intermedio si el bit correspondiente del tercer conjunto de datos intermedio se establece al primer valor e ignorando el bit del primer conjunto de datos intermedio si el bit correspondiente del tercer conjunto de datos intermedio se establece al segundo valor. En este caso, que se muestra en la figura 6, el primer valor corresponde a 1 y el segundo valor a 0. Tal como resulta evidente a partir de la figura 6, la clave comprende cuatro bits en lugar de los ocho bits originales, dado que se han ignorado cuatro bits durante la generación de la clave.

Tal como se mencionó anteriormente tanto el primer conjunto de datos intermedio como el tercer conjunto de datos intermedio se envían de manera pública. Aunque se intercepten es imposible que un tercero genere una clave usando estos datos, ya que el valor de un 1 en el tercer conjunto de datos no significa realmente el valor 1, sino tan sólo que el primer conjunto de datos y el segundo conjunto de datos tienen el mismo valor. Por tanto, un 1 en el tercer conjunto de datos puede ser en realidad o bien un 1 o bien un 0.

En el nodo B se genera la segunda clave criptográfica basándose en la comparación bit a bit entre el primer y el segundo conjunto de datos intermedio, véase la figura 5, manteniendo el valor del bit del segundo conjunto de datos intermedio si el bit correspondiente del primer conjunto de datos intermedio es igual e ignorando el bit del segundo conjunto de datos intermedio si los bits comparados no son iguales. Tal como puede observarse dicha primera y segunda clave criptográfica son las mismas claves. Entonces pueden usarse las claves para el cifrado/descifrado de información enviada entre el primer nodo A y el segundo nodo B. Puede usarse cualquier método de cifrado conocido junto con la clave generada mediante el método según la presente invención. Por tanto, la presente

invención no se refiere a cómo se realiza el cifrado/descifrado sino a la generación de claves criptográficas. La clave generada será válida mientras esté activa la sesión de comunicación entre el primer y el segundo nodo. Además, cuando la clave se ha generado por el primer nodo A y el segundo nodo B, los archivos de generación de clave recibidos por el servidor central se eliminarán en el nodo respectivo.

Ahora se ha descrito en detalle el método global de la presente invención. Sin embargo la presente invención también se refiere a un método para generar una clave de cifrado/descifrado en el primer nodo A. Este método es un subconjunto del método global descrito anteriormente y por tanto se describirá brevemente. El método ejecutado por el primer nodo comienza con enviar una petición al servidor 2 central para configurar una comunicación segura con el segundo nodo B. Entonces el primer nodo recibe el primer archivo de generación de clave del servidor 2 central y comienza a procesarlo. Esto generará el primer conjunto de datos intermedio, que tal como se mencionó anteriormente se envía al segundo nodo B.

Entonces el primer nodo A recibirá el tercer conjunto de datos intermedio del segundo nodo B y comparará los bits del tercer conjunto de datos intermedio con los bits correspondientes del primer conjunto de datos intermedio. El primer nodo A generará la primera clave de cifrado basándose en la comparación bit a bit entre el tercer y el primer conjunto de datos intermedio manteniendo el valor del bit del primer conjunto de datos intermedio si el bit correspondiente del tercer conjunto de datos intermedio se establece al primer valor e ignorando el bit del primer conjunto de datos intermedio si el bit correspondiente del tercer conjunto de datos intermedio se establece al segundo valor.

Además el segundo nodo B ejecutará un subconjunto del método global, que se describirá ahora brevemente. El método para generar una clave de cifrado/descifrado en el segundo nodo B comienza con que el segundo nodo B recibe el segundo archivo de generación de clave del servidor 2 central y comienza a procesarlo. Esto generará el segundo conjunto de datos intermedio. Posteriormente el segundo nodo B recibirá el primer conjunto de datos intermedio del primer nodo A y comparará bits del primer conjunto de datos intermedio con bits correspondientes del segundo conjunto de datos intermedio. Posteriormente el segundo nodo B creará un tercer conjunto de datos intermedio nuevo basándose en la comparación bit a bit entre el primer y el segundo conjunto de datos intermedio estableciendo el primer valor si los bits comparados son iguales y el segundo valor si los bits comparados no son iguales. Entonces se envía el tercer conjunto de datos intermedio al primer nodo A.

Entonces el segundo nodo B genera la segunda clave de cifrado basándose en la comparación bit a bit entre el primer y el segundo conjunto de datos intermedio manteniendo el valor del bit del segundo conjunto de datos intermedio si el bit correspondiente del primer conjunto de datos intermedio es igual e ignorando el bit del segundo conjunto de datos intermedio si los bits comparados no son iguales.

Por tanto, con el método descrito anteriormente es posible, de una manera fácil y segura, generar claves criptográficas donde se usan, es decir en los nodos. Esto es muy beneficioso puesto que ya no existe la necesidad de distribuir claves. La clave es del tipo de un único uso y sólo será válida para una sesión de comunicación y mientras esté activa. Además, las claves se generan en dos procedimientos independientes en dos nodos separados.

Aunque se cree que el método anterior es muy seguro, la seguridad puede mejorarse adicionalmente haciendo uso de los metadatos adjuntos al archivo de generación de clave. Por ejemplo los metadatos pueden mencionar que sólo deben usarse como clave uno de cada tres o cada dos bits del resultado del procedimiento de generación de clave. Un uso similar de metadatos también puede mencionar que sólo deben leerse uno de cada tres o cada dos bits cuando el primer nodo A y el segundo nodo B se comunican entre sí durante el procedimiento de generación de clave.

Debe entenderse que aunque se ha descrito la invención con referencia a realizaciones preferidas, la invención no se limita a las mismas. Puede haber muchas otras realizaciones y variaciones que están igualmente dentro del alcance de la invención, que se define mejor mediante las reivindicaciones adjuntas.

REIVINDICACIONES

1. Método para generar una clave de cifrado/descifrado, que puede usarse para una comunicación segura entre un primer nodo (A) y un segundo nodo (B), en el que la clave generada sólo es válida para una sesión de comunicación entre el primer nodo (A) y el segundo nodo (B) y mientras esté activa la sesión de comunicación, comprendiendo dicho método las etapas de:

enviar una petición desde el primer nodo (A) a un servidor (T) central para configurar una comunicación segura con el segundo nodo (B),

enviar desde el servidor (2) central un primer archivo de generación de clave al primer nodo (A) y un segundo archivo de generación de clave al segundo nodo (B) en respuesta a la petición del primer nodo (A),

comenzar a procesar el primer archivo de generación de clave en el primer nodo (A) y el segundo archivo de generación de clave en el segundo nodo (B),

generar un primer conjunto de datos intermedio en el primer nodo (A) y un segundo conjunto de datos intermedio at el segundo nodo (B),

enviar el primer conjunto de datos intermedio del primer nodo (A) al segundo nodo (B),

comparar bits del primer conjunto de datos intermedio con bits correspondientes del segundo conjunto de datos intermedio,

crear un tercer conjunto de datos intermedio nuevo basándose en la comparación bit a bit entre el primer y el segundo conjunto de datos intermedio estableciendo un primer valor si los bits comparados son iguales y un segundo valor si los bits comparados no son iguales,

enviar el tercer conjunto de datos intermedio del segundo nodo (B) al primer nodo (A),

comparar bits del tercer conjunto de datos intermedio con los bits correspondientes del primer conjunto de datos intermedio,

generar una primera clave criptográfica basándose en la comparación bit a bit entre el tercer y el primer conjunto de datos intermedio manteniendo el valor del bit del primer conjunto de datos intermedio si el bit correspondiente del tercer conjunto de datos intermedio se establece al primer valor e ignorando el bit del primer conjunto de datos intermedio si el bit correspondiente del tercer conjunto de datos intermedio se establece al segundo valor,

generar una segunda clave criptográfica basándose en la comparación bit a bit entre el primer y el segundo conjunto de datos intermedio manteniendo el valor del bit del segundo conjunto de datos intermedio si el bit correspondiente del primer conjunto de datos intermedio es igual e ignorando el bit del segundo conjunto de datos intermedio si los bits comparados no son iguales, siendo dicha primera y segunda clave criptográfica la misma.

2. Método según la reivindicación 1, en el que la etapa de enviar el primer archivo de generación de clave al primer nodo (A) y el segundo archivo de generación de clave al segundo nodo (B) también comprende enviar metadatos adjuntos a cada archivo de generación de clave, respectivamente.

3. Método según la reivindicación 2, en el que los metadatos comprenden una constante que va a usarse para la generación tanto de la primera como de la segunda clave criptográfica.

4. Método según la reivindicación 2 ó 3, en el que los metadatos comprenden información sobre la longitud de clave criptográfica.

5. Método según la reivindicación 4, que comprende además la etapa de generar aleatoriamente, dentro de un intervalo predeterminado, la longitud de clave criptográfica.

6. Método para generar una clave de cifrado/descifrado en un primer nodo (A) que puede usarse para una comunicación segura entre el primer nodo (A) y un segundo nodo (B), en el que la clave generada sólo es válida para una sesión de comunicación entre el primer nodo (A) y el segundo nodo (B) y mientras esté activa la sesión de comunicación, comprendiendo dicho método las etapas de:

enviar una petición a un servidor (2) central para configurar una comunicación segura con el segundo nodo (B),

recibir un primer archivo de generación de clave del servidor (2) central en respuesta a la petición,

procesar el primer archivo de generación de clave,

generar un primer conjunto de datos intermedio,

enviar el primer conjunto de datos intermedio al segundo nodo (B),

recibir un tercer conjunto de datos intermedio del segundo nodo (B),

comparar bits del tercer conjunto de datos intermedio con bits correspondientes del primer conjunto de datos intermedio,

generar una primera clave criptográfica basándose en la comparación bit a bit entre el tercer y el primer conjunto de datos intermedio manteniendo el valor del bit del primer conjunto de datos intermedio si el bit correspondiente del tercer conjunto de datos intermedio se establece a un primer valor e ignorando el bit del primer conjunto de datos intermedio si el bit correspondiente del tercer conjunto de datos intermedio se establece a un segundo valor.

7. Método según la reivindicación 6, en el que la etapa de recibir el primer archivo de generación de clave también comprende recibir metadatos adjuntos a dicho archivo.

8. Método según la reivindicación 7, en el que los metadatos comprenden una constante que va a usarse para la generación de la primera clave criptográfica.

9. Método según la reivindicación 7 u 8, en el que los metadatos comprenden información sobre la longitud de clave criptográfica.

10. Método para generar una clave de cifrado/descifrado en un segundo nodo (B) que puede usarse para una comunicación segura entre un primer nodo (A) y el segundo nodo (B), en el que la clave generada sólo es válida para una sesión de comunicación entre el primer nodo (A) y el segundo nodo (B) y mientras esté activa la sesión de comunicación, comprendiendo dicho método las etapas de:

recibir un segundo archivo de generación de clave de un servidor (2) central en respuesta a una petición del primer nodo (A) para comenzar una comunicación segura entre el primer nodo (A) y el segundo nodo (B),

procesar el segundo archivo de generación de clave,

generar un segundo conjunto de datos intermedio,

recibir un primer conjunto de datos intermedio del primer nodo (A),

comparar bits del primer conjunto de datos intermedio con bits correspondientes del segundo conjunto de datos intermedio,

crear un tercer conjunto de datos intermedio nuevo basándose en la comparación bit a bit entre el primer y el segundo conjunto de datos intermedio estableciendo un primer valor si los bits comparados son iguales y un segundo valor si los bits comparados no son iguales,

enviar el tercer conjunto de datos intermedio al primer nodo (A),

generar una segunda clave criptográfica basándose en la comparación bit a bit entre el primer y el segundo conjunto de datos intermedio manteniendo el valor del bit del segundo conjunto de datos intermedio si el bit correspondiente del primer conjunto de datos intermedio es igual e ignorando el bit del segundo conjunto de datos intermedio si los bits comparados no son iguales.

11. Método según la reivindicación 10, en el que la etapa de recibir el segundo archivo de generación de clave también comprende recibir metadatos adjuntos a dicho archivo.

12. Método según la reivindicación 11, en el que los metadatos comprenden una constante que va a usarse para la generación de la segunda clave criptográfica.

13. Método según la reivindicación 11 ó 12, en el que los metadatos comprenden información sobre la longitud de clave criptográfica.

14. Programa informático que comprende programa de código para realizar todas las etapas según una cualquiera de las reivindicaciones 1-13, cuando se ejecuta el programa en un ordenador.

15. Producto de programa informático que comprende código de programa almacenado en un medio legible por ordenador para realizar el método según cualquiera de las reivindicaciones 1-13, cuando se ejecuta dicho código de programa en un ordenador.

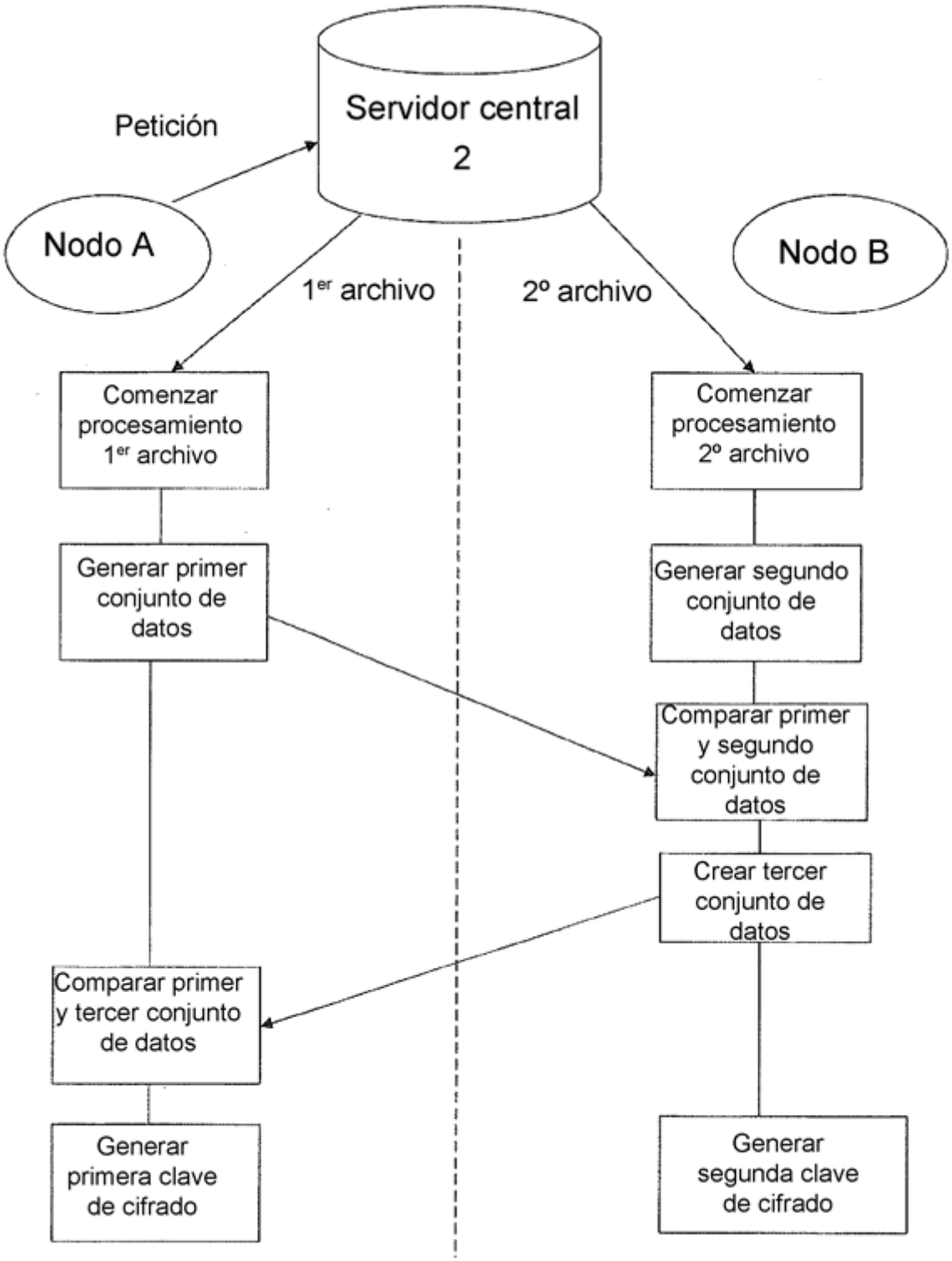
Servidor central 2
Petición
Nodo A
Nodo B
1er archivo
2º archivo
Comenzar procesamiento 1er archivo
Comenzar procesamiento 2º archivo
Generar primer conjunto de datos
Generar segundo conjunto de datos
Comparar primer y segundo conjunto de datos
Crear tercer conjunto de datos
Comparar primer y tercer conjunto de datos
Generar primera clave de cifrado
Generar segunda clave de cifrado

Fig. 1

Archivo de procedimiento	M1	M2	Mn

Fig. 2

A	B	C	D
1	0	1	0

Fig. 3

D	C	A	A	C	B	D	B
0	1	1	1	1	0	0	0

Nodo A

A	C	A	B	D	B	D	C
1	1	1	0	0	0	0	1

Nodo B

Fig. 4

Valor A	0	1	1	1	1	0	0	0
Valor B	1	1	1	0	0	0	0	1
Correspondencia 1	F	T	T	F	F	T	T	F
Valor 1	0	1	1	0	0	1	1	0
Clave B	-	1	1	-	-	0	0	-

Fig. 5

Valor A	0	1	1	1	1	0	0	0
Valor 1	0	1	1	0	0	1	1	0
Clave A	-	1	1	-	-	0	0	-

Fig. 6