(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 279 393**

(51) Int. Cl.:
H04L 9/08 (2006.01)
G06F 7/58 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Número de solicitud europea: **04740702 .8**
(86) Fecha de presentación : **06.07.2004**
(87) Número de publicación de la solicitud: **1642412**
(87) Fecha de publicación de la solicitud: **05.04.2006**

(54) Título: **Procedimiento para la transmisión de datos cifrados a través de una red de comunicaciones.**

(30) Prioridad: **07.07.2003 DE 103 30 643**

(45) Fecha de publicación de la mención BOPI:
16.08.2007

(45) Fecha de la publicación del folleto de la patente:
16.08.2007

(73) Titular/es: **SIEMENS AKTIENGESELLSCHAFT**
Wittelsbacherplatz 2
80333 München, DE

(72) Inventor/es: **Döbrich, Udo;**
Heidel, Roland y
Linzenkirchner, Edmund

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

DESCRIPCIÓN

Procedimiento para la transmisión de datos cifrados a través de una red de comunicaciones.

La invención se refiere a un procedimiento para la transmisión de datos cifrados así como a un producto de programa de ordenador correspondiente y a un sistema de comunicaciones, especialmente para los usuarios de un sistema de automatización.

Se conocen diferentes procedimientos para la transmisión de datos cifrados a partir del estado de la técnica. En principio, a este respecto, se distingue entre procedimientos de cifrado asimétricos y simétricos.

Los procedimientos de cifrado simétricos se designan también como "Clave Privada". En el caso de un cifrado simétrico, los usuarios de la comunicación tienen la misma clave secreta, que sirve tanto para el cifrado como también para el descifrado. Ejemplo de procedimientos de cifrado simétricos conocidos a partir del estado de la técnica son DES, Triple-DES, RC2, RC4, IDEA, Skipjack.

Un inconveniente común de los procedimientos de cifrado simétricos conocidos a partir del estado de la técnica es que antes del comienzo de la comunicación cifrada deben transmitirse las claves simétricas a los usuarios individuales, pudiendo retrasarse esta transmisión.

En el caso de los procedimientos de cifrado asimétricos, que se designan también como cifrado de "Clave Pública", una clave pública sirve para el cifrado. Los datos cifrados con la clave pública de un usuario solamente pueden ser descifrados con la clave privada secreta de este usuario. Los procedimientos de cifrado asimétricos conocidos son Diffie-Hellmann y RSA.

Se conoce a partir de la publicación WO 97/49213 A una generación de una clave simétrica, que se basa en datos obtenidos a partir de un proceso estocástico. Dicho más exactamente, dicha publicación da a conocer un procedimiento para la transmisión de datos con la entrada de primeros datos a partir de un proceso estocástico en al menos primeros y segundos usuarios de una red de comunicaciones. A continuación tiene lugar en cada uno de los al menos primeros y segundos usuarios una generación de una clave simétrica, sobre la base de los primeros datos y una memorización de la clave simétrica para una transmisión de datos cifrada entre los al menos primeros y segundos usuarios. Dicho procedimiento para el establecimiento de una clave criptográfica común de acuerdo con la publicación mencionada se basa en la hipótesis de que la característica de un canal de comunicación, dicho más exactamente, las impedancias del canal, se puede utilizar en los usuarios móviles como un proceso estocástico que sirve de base para la generación de las claves.

En cambio, la invención tiene el cometido de crear un procedimiento mejorado para la transmisión de datos cifrados así como un producto de programa de ordenador correspondiente y un sistema de comunicaciones para la transmisión de datos cifrados.

Los cometidos en los que se basa la invención se soluciona en cada caso con las características de las reivindicaciones independientes de la patente. Las formas de realización preferidas de la invención se indican en las reivindicaciones dependientes de la patente.

De acuerdo con la invención, para la transmisión de datos protegidos, por ejemplo a través de una red pública de comunicaciones, como Internet, se utiliza un procedimiento de cifrado simétrico. En este caso, no se lleva a cabo ninguna distribución de la clave simétrica secreta a los usuarios individuales de la red de comunicaciones, sino que la clave simétrica es generada en cada caso localmente en los usuarios individuales.

A tal fin, se introducen datos, que son tomados de un proceso estocástico, en los usuarios individuales. Sobre esta base se generan entonces en los usuarios individuales en cada caso claves simétricas idénticas localmente, que se utilizan, por lo demás, para la transmisión de datos cifrados entre los usuarios.

De acuerdo con una forma de realización preferida de la invención, los datos, que forman la base para la generación de las claves simétricas en los usuarios, son generados por medio de un generador de números aleatorios, que utiliza un proceso estocástico, como por ejemplo ruidos de resistencia o un proceso de desintegración radioactiva para la generación de números aleatorios. En comparación con los generadores de números aleatorios, que se basan en polinomios de generador, un generador de números aleatorios de este tipo tiene la ventaja de que no se trata de números pseudo-aleatorios. El polinomio del generador se puede calcular, en efecto, en principio, a través de un interventor a través de la evaluación de la comunicación de los usuarios, especialmente cuando se trata de una comunicación cíclica.

De acuerdo con otra forma de realización preferida, se calcula a menos un valor de medición a partir de un proceso estocástico. Por ejemplo, los datos necesarios para la generación de las claves simétricas se obtienen a partir de las posiciones binarias menos significativas del o bien de los valores de medición.

De acuerdo con otra forma de realización preferida de la invención se utiliza al menos un parámetros variable en el tiempo de un sistema de automatización como proceso estocástico. A tal fin, se contemplan, por ejemplo, diferentes valores de medición, que son suministrados por sensores del sistema de automatización, como por ejemplo temperatura, número de revoluciones, tensión, corriente, caudal, velocidad, concentración, humedad,... Los valores de medición correspondientes son estocásticos, pero pueden presentar, por ejemplo, componentes periódicos. Para la reducción de tales componentes periódicos se pueden utilizar, por ejemplo, sólo las posiciones binarias menos significativas de los valores de medición para la formación de las claves simétricas.

De acuerdo con una forma de realización preferida de la invención, se registran datos estocásticos desde al menos dos de los usuarios de una manera independiente entre sí. Los datos estocásticos registrados por uno de los usuarios son transmitidos al o a los otros usuarios. En general, cada uno de los usuarios recibe de esta manera todos los datos estocásticos. Éstos son combinados entonces entre sí, con el fin de obtener una base para la generación respectiva de la clave simétrica.

De acuerdo con otra forma de realización preferida de la invención, la transmisión de los datos, que forman la base para la generación de las claves simétricas en los usuarios, se lleva a cabo a través de una red pública, como por ejemplo Internet o una Ethernet, por ejemplo una LAN, WAN o WLAN.

De acuerdo con otra forma de realización preferi-

da de la invención, la generación de las claves se lleva a cabo en los usuarios a demanda de un usuario maestro, siendo transmitida la solicitud correspondiente a través de la red de comunicaciones hacia los usuarios. Por ejemplo, se realiza una solicitud correspondiente cuando el régimen de trabajo de la red de comunicaciones con la transmisión de datos útiles es relativamente reducido, con el fin de aprovecha la anchura de banda no utilizada para la transmisión de datos como base para la formación de las claves en los usuarios. Este modo de proceder es especialmente ventajoso cuando los usuarios se comunican a través de Internet.

En cambio, cuando se utiliza, por ejemplo Ethernet, todos los usuarios pueden "espiar" el tráfico de datos sobre la Ethernet. En este caso, la formación de la clave se puede activar en los usuarios individuales, de tal forma que el usuario maestro emite un comando de activación correspondiente sobre la Ethernet.

De acuerdo con otra forma de realización preferida de la invención, la transmisión de los datos estocásticos y la generación de las claves se lleva a cabo en los usuarios en instantes predeterminados o después de intervalos de tiempo predeterminados. En esta forma de realización, los usuarios disponen de la red de comunicaciones sobre una base de tiempo sincronizado.

De acuerdo con otra forma de realización preferida de la invención se utilizan diferentes procedimientos de cifrado simétricos por los usuarios para la generación de las claves y se generan claves simétricas diferentes correspondientes. Para la transmisión de datos cifrados se conmuta, por ejemplo, de una manera periódica entre los procedimientos de cifrado, con el fin de elevar adicionalmente la seguridad de la transmisión de los datos cifrados.

De acuerdo con otra forma de realización preferida de la invención, los datos para los diferentes procedimientos de cifrado se forman a través de diferentes combinaciones de los datos estocásticos suministrados por los usuarios individuales.

La presente invención es especialmente ventajosa para la aplicación en sistemas de automatización. Por ejemplo, los algoritmos para la formación de las claves se establecen en los usuarios individuales durante la proyección de la instalación. Los algoritmos correspondientes para la formación de las claves se mantienen secretos por los fabricantes de la instalación. Además de la protección de la transmisión de datos cifrados, existe, por lo tanto, también una protección contra la utilización de componentes no autorizados, por ejemplo de un tercer fabricante, en el sistema de automatización.

De una manera preferida, los algoritmos se memorizan en zonas protegidas de la memoria de los aparatos de automatización del sistema de automatización, por ejemplo en EPROMs o tarjetas de chips, que son introducidas por usuarios autorizados en lectores de tarjetas de los aparatos de automatización.

La aplicación de la presente invención es especialmente ventajosa para componentes enlazados entre sí a través de redes públicas de instalaciones técnicas de automatización. A través de la transmisión de datos cifrados de acuerdo con la invención entre los usuarios de una instalación técnica de automatización de este tipo se evitan intervenciones no autorizadas de terceros, especialmente también cuando se utiliza una técnica de transmisión sin hilos entre los usuarios.

De acuerdo con otra forma de realización preferida de la invención, la transmisión de datos cifrados se utiliza para los fines del mantenimiento a distancia o del llamado teleservicio de la instalación. También aquí el procedimiento de transmisión de datos de acuerdo con la invención ofrece una protección contra el espionaje de los datos transmitidos de las instalaciones o bien contra intervenciones de manipulación.

Además de una instalación técnica de automatización, la invención se puede utilizar para los fines de la telecomunicación entre usuarios o para los fines de la comunicación entre los componentes de una electrónica de automóviles, de buques, de aviones o de ferrocarriles.

Por lo demás, se explican en detalle formas de realización preferidas de la invención con referencia a los dibujos. En este caso:

La figura 1 muestra un diagrama de bloques de una primera forma de realización de un sistema de comunicaciones de acuerdo con la invención.

La figura 2 muestra un diagrama de flujo de una primera forma de realización del procedimiento de transmisión de datos de acuerdo con la invención.

La figura 3 muestra la generación de datos como base para la generación de claves a partir de un valor de medición.

La figura 4 muestra un diagrama de bloques de otra forma de realización de un sistema de comunicaciones de acuerdo con la invención.

La figura 5 muestra un diagrama de bloques de una forma de realización preferida de un sistema de automatización de acuerdo con la invención.

La figura 1 muestra un sistema de comunicaciones 100, en el que al menos los usuarios 102 y 104 pueden intercambiar datos a través de una red 106. En una forma de realización práctica, el sistema de comunicaciones 100 puede incluir una pluralidad de tales usuarios.

Los usuarios 102, 104 del sistema de comunicaciones 100 tienen en cada caso un programa 108 para un procedimiento de cifrado simétrico. Con la ayuda de los programas 108 se pueden formar claves simétricas sobre la base de datos de entrada, así como se pueden cifrar y descifrar datos útiles que deben transmitirse.

Los usuarios 102, 104 tienen, además, en cada caso una memoria 110 para la memorización de la clave simétrica generada a través del programa 108 respectivo.

El usuario 102 está conectado con un módulo de registro 112; el módulo de registro 112 sirve para el registro de datos estocásticos a partir de un proceso estocástico 114. En el proceso estocástico 114 se puede tratar, por ejemplo, de la señal de la tensión de una resistencia ruidosa.

Además, el usuario 102 está conectado con una fuente de datos 116. Los datos suministrados desde la fuente de datos 116 deben transmitirse desde el usuario 102 a través de la red 106 hacia el usuario 104.

Durante el funcionamiento del sistema de comunicaciones 100 se registran por el módulo de registro 112 datos estocásticos a partir del proceso estocástico 114. Los datos estocásticos son introducidos en el usuario 102. Los datos estocásticos son transmitidos desde el usuario 102 a través de la red 106 al usuario 104. Esto se lleva a cabo de una manera cifrada o descifrada.

En el usuario 102 se pone en marcha el programa

108, con el fin de generar sobre la base de los datos estocásticos suministrados por el módulo de registro 112 una clave simétrica, que se memoriza en la memoria 110. De una manera correspondiente, se pone en marcha el programa 108 en el usuario 104, con el fin de utilizar los datos estocásticos recibidos desde el usuario 102 a través de la red 106 para la generación de la misma clave simétrica, que se memoriza en la memoria 110 del usuario 104.

Cuando están presentes otros usuarios en el sistema de comunicación 100, también los otros usuarios reciben los datos estocásticos desde el usuario 102 a través de la red 106 y generan en cada caso localmente la clave simétrica con la ayuda del programa 108 respectivo.

Los datos, que son suministrados desde la fuente de datos 116 al usuario 102 se pueden transmitir ahora cifrados a través de la red 106 hacia el usuario 104. A tal fin, los datos útiles a transmitir son cifrados con la ayuda del programa 108 del usuario 102 y de la clave simétrica memorizada en la memoria 110 del usuario.

Los datos útiles cifrados son transmitidos a través de la red 106 y son recibidos por el usuario 104. Los datos son descifrados allí por el programa 108 del usuario 104 con la ayuda de la clave simétrica memorizada en la memoria 110 del usuario 104.

La generación de los datos estocásticos como base para la generación de las claves simétricas en los usuarios 102, 104 se puede realizar en este caso a través de un generador de números aleatorios estocásticos, que utiliza, por ejemplo, la tensión de salida de una resistencia ruidosa como proceso estocástico.

De una manera alternativa, se pueden utilizar también los datos suministrados por la fuente de datos 116 como datos estocásticos como base para la generación de las claves simétricas. Esto es especialmente ventajoso cuando la fuente de datos 116 suministra valores de medición de magnitudes o parámetros variables con el tiempo, por ejemplo de un sistema de automatización. Por ejemplo, determinados parámetros del proceso en un sistema de automatización de este tipo, como la temperatura, la presión, el número de revoluciones, etc. no son deterministas, sino que son más o menos aleatorios con componentes más o menos periódicos. Por lo tanto, un valor de medición correspondiente suministrado por la fuente de datos 116 se puede utilizare como dato estocástico para la generación de la clave simétrica, siendo innecesario en este caso un módulo de registro 112 separado o bien un proceso estocástico adicional 114.

La figura 2 muestra un diagrama de flujo correspondiente. En la etapa 200 se registran datos estocásticos. En este caso se puede tratar de datos estocásticos suministrados por un generador aleatorio o de los datos útiles, que son suministrados por una fuente de datos. En la etapa 202 se transmiten los datos estocásticos a los usuarios del sistema de comunicaciones. Esto se puede llevar a cabo de una manera cifrada o descifrada a través de una red pública.

En la etapa 204 se generan localmente a través de los usuarios, sobre la base de los datos estocásticos, en cada caso claves simétricas idénticas. A tal fin, sirve un procedimiento de cifrado secreto, que está implementado en los usuarios en cada caso a través de un programa de ordenador.

Cada uno de los usuarios, que ha recibido los datos estocásticos en la etapa 202, introduce, por lo tanto, estos datos estocásticos en el programa de ordenador, con el fin de generar una clave simétrica, que es memorizada localmente por el usuario respectivo.

Por lo tanto, como resultado, todos los usuarios disponen de la clave simétrica, sin que ésta haya sido transmitida a través de la red 106. Tampoco a través del espionaje de la transmisión de los datos estocásticos a través de la red 106 un tercero puede estar en posesión de la clave, puesto que a tal fin es necesario el procedimiento de cifrado secreto o bien el programa de ordenador correspondiente. Para evitar accesos no autorizados al programa de ordenador, éste es memorizado de una manera preferida en una zona protegida de la memoria, por ejemplo en una EPROM o en una tarjeta de chip.

Después de que las claves simétricas idénticas sobre la base de los datos estocásticos han sido generadas en los usuarios individuales, se utilizan estas claves para la comunicación protegida entre los usuarios en la etapa 206.

La figura 3 muestra un ejemplo de realización para la generación de datos estocásticos como base para la generación de las claves simétricas. Por ejemplo, se suministra desde la fuente de datos 116 (ver la figura 1) un valor de medición 300, que tiene por ejemplo una longitud de 32 bits. Por ejemplo, solamente se utilizan las ocho posiciones binarias menos significativas ("Bits menos significativos" - LSB) del valor de medición 300 para la generación de las claves.

Con otras palabras, por lo tanto, las posiciones binarias menos significativas del valor de medición 300 forman valores estocásticos, que se utilizan para la generación de las claves. La utilización solamente de las posiciones binarias menos significativas del valor de medición 300 tiene en este caso, frente a la utilización del valor de medición 300 completo o solamente de las posiciones binarias más significativas ("Bits más significativos" - MSB), la ventaja de que se reducen o se eliminan porciones periódicas de la señal de medición.

La figura 4 muestra un diagrama de bloques de un sistema de comunicaciones 400. Los elementos de la figura 4, que corresponden a los elementos de la forma de realización de la figura 1, están designados con signos de referencia elevados en 300.

En la forma de realización de la figura 4, el usuario 402 está conectado con las fuentes de datos 418 y 420, que suministrar de una manera consecutiva los valores de medición a y b. El usuario 404 está conectado con la fuente de datos 422, que suministra de una manera consecutiva el valor de medición c. En el valor de medición a se trata, por ejemplo de una temperatura, en el valor de medición b se trata de un número de revoluciones y en el valor de medición c se trata de una presión.

Los usuarios 402 y 404 tienen en cada caso una memoria 424 para la memorización de los valores de medición a, b y c. Además, los usuarios 402 y 404 tienen en cada caso una memoria 426 para la memorización de las claves simétricas S1 y S2. La clave S1 es generada por el programa 408 sobre la base de una combinación de los valores de medición a y c y la clave S2 es generada sobre la base de los valores de medición a y b.

Durante el funcionamiento del sistema de comunicación 400 se generan las claves simétricas S1 y S2 en los usuarios 402 y 404 así como en otros usuarios que están constituidos, en principio, de la misma forma.

A tal fin, se memorizan los valores de medición

a, b y c, respectivamente, que son emitidos en un instante determinado por las fuentes de datos 418, 420, 422, en la memoria 424. Es decir, que el usuario 402 memoriza en su memoria 424 los valores de medición a y b y los transmite a través de la red 406 a los otros usuarios, es decir, especialmente al usuario 404, donde los valores de medición a y b son memorizados de la misma manera en la memoria 424.

Por otra parte, el usuario 404 memoriza el valor de medición c en su memoria 424 y transmite el valor de medición c a través de la red 406 a los otros usuarios, es decir, especialmente al usuario 402, donde el valor de medición c es memorizado de la misma manera en la memoria 424 respectiva. Como se explica con referencia a la figura 3, en lugar de los valores de medición completos se memorizan solamente las posiciones binarias menos significativas en la memoria 424.

El programa 408 del usuario 402 combina entre sí los valores de medición a y b, que están memorizados en la memoria 424, o bien las posiciones binarias menos significativas de estos valores de medición, colgando los bits correspondientes, por ejemplo, unos en los otros. La palabra de datos que resulta a partir de ello es utilizada por el programa 408 para generar la clave S2.

De cuerdo con ello, sobre la base de los valores de medición a y c con la ayuda del programa 408 se genera la clave S1. Las claves S1 y S2 son memorizadas en la memoria 426 del usuario 402. En principio, el mismo proceso se desarrolla en el usuario 404 así como en los otros usuarios del sistema de comunicación 400, de manera que en todos los usuarios están presentes las claves S1 y S2.

Por lo demás, se lleva a cabo una transmisión cifrada de los valores de medición a, b y c a través de la red 406, siendo utilizada la clave S1 en determinados instantes y la clave S2 en determinados instantes para la transmisión de datos cifrados. Estos instantes se pueden predefinir o se pueden controlar en función del acontecimiento. Por ejemplo, uno de los usuarios puede tener la función de un usuario maestro para el inicio de la generación de la clave o la conmutación entre las claves en los diferentes usuarios.

En el ejemplo de realización considerado aquí, a partir de los valores de medición a, b y c se forman a través de una determinada combinación diferentes palabras de datos que, por su parte, son la base para la generación de diferentes claves simétricas. Esta combinación puede ser invariable en el tiempo o también variable con el tiempo.

La figura 5 muestra un sistema de automatización 500 con los aparatos de automatización 502, 504, 506, 6508, 510 y 512. Los aparatos de automatización 502 a 512 están conectados entre sí con un bus de datos 514. A este respecto, se puede tratar, por ejemplo, de una Ethernet. Otro aparato de automatización 516 puede intercambiar datos a través de una red pública 518 como por ejemplo Internet o una comunicación de radio móvil sin hilos.

Cada uno de los aparatos de automatización 502 a 512 y 516 tiene un programa de cifrado 520 y un programa de cifrado 522. Además, pueden estar presentes otros programas de cifrado. Los programas de cifrado 520 y 522 ponen a disposición en cada caso diferentes procedimientos de cifrado simétricos.

Además, los aparatos de automatización 502 a 512 y 516 tienen en cada caso un reloj 524. Los relojes 524 están sincronizados entre sí, de manera que se crea una base de tiempo sincronizada unitarias para el sistema de automatización 500.

Cada uno de los aparatos de automatización 502 a 512 tiene, además, una memoria 526 y una memoria 528. La memoria del aparato de automatización 502 sirve para la memorización del “valor 1”, que se emite desde un generador de valores de medición 1 correspondiente. La memoria 528 del aparato de automatización 502 sirve para la memorización del “valor 5”, que se emite desde un generador del valor de medición 5. De una manera correspondiente sucede para las memorias 526 y 528 de los otros aparatos de automatización 504 a 512, que están asociados en cada caso a determinados generadores de valores de medición, como se deduce a partir de la figura 5. Los generadores del valor de medición no se representa en la figura 5 para mayor claridad.

La palabra de datos, que sirve como base para la generación de una clave simétrica, es generada a través de una combinación predeterminada, por ejemplo a partir de la concatenación de los valores 1, 2, 3 y 4. La palabra de datos recibida a través de esta concatenación se introduce en cada caso en los programas de cifrado 520 y 522, con el fin de generar clases simétricas correspondientes.

Para la transmisión cifrada de datos entre los aparatos de automatización 502 a 512 y 516 se utilizan los programas de cifrado en una secuencia temporal previamente proyectada, es decir, que se proyecta para cada instante, si el programa de cifrado 520 ó 522 se puede utilizar para la transmisión cifrada de los datos.

En el aparato de automatización 516 se trata, por ejemplo, de un aparato de mantenimiento a distancia. También el aparato de automatización 516 recibe los valores de medición 1, 2, 3 y 4 a través de la red 518, con el fin de formar con la ayuda de los programas de cifrado 520 y 522 las claves respectivas. Las transmisión de los valores de medición desde los aparatos de automatización 502, 504 y 510 se lleva a cabo en este caso a través del bus de datos 514 y a través de la red 518 hacia el aparato de automatización 516. Después de que se ha realizado la formación de la clave, se puede llevar a cabo desde el aparato de automatización 516 un mantenimiento a distancia, siendo protegidos los datos transmitidos en este caso a través de la red 518 contra espionaje y manipulación.

La red tiene los accesos a la red 530 y 532, a través de los cuales se lleva a cabo el tráfico de datos entre el bus de datos 514 y el aparato de automatización 516. Durante la transmisión a través de la red 518 se puede llevar a cabo otro cifrado, cifrando de nuevo los datos ya cifrados. De esta manera, se eleva adicionalmente la seguridad contra ataques desde el exterior.

Esto es especialmente ventajoso cuando en la red 518 se trata de una red pública. El cifrado siguiente para la transmisión a través de la red 518 se puede llevar a cabo de una manera similar a la figura 1, adoptando el acceso a la red 530 el papel del usuario 102 y el acceso a la red 532 el papel del usuario 104.

Es especialmente ventajoso que la transmisión de datos protegidos entre los aparatos de automatización se lleve a cabo de una manera independiente de las infraestructuras generales de seguridad, como por ejemplo de consorcios centrales, sino que se basa en datos variables con el tiempo, que proceden de la instalación propiamente dicha. Otra ventaja es que en virtud

de los programas de cifrado secretos 520, 522 se lleva a cabo también una autentificación implícita de los aparatos de automatización. Los aparatos de automatización no autorizados, para los que no está autorizada la instalación, o los aparatos de automatización de fabricantes externos, que no disponen de las licencias necesarias, no tienen los programas de cifrado secretos 520, 522 y, por lo tanto, tampoco se pueden emplear en el sistema de automatización.

Para la elevación adicional de la seguridad se puede cargar en los aparatos de automatización individuales en cada caso una lista de programas de cifrado. De una manera preferida, la carga de estos programas de cifrado se lleva a cabo en el modo fuera de línea del sistema de automatización, con el fin de evitar un espionaje de los programas de cifrado. Por ejemplo, los programas de cifrado se memorizan en zonas protegidas de la memoria de EPROMs o tarjetas de chips.

Los instantes de conmutación para el cambio de los programas de cifrado y de las claves correspondientes se pueden determinar bajo control de instrucción por uno de los aparatos de automatización, que adopta de esta manera la función de un maestro. De una manera alternativa, los instantes de conmutación pueden estar proyectados a través de instantes absolutos predeterminados o se pueden realizar de una manera cíclica o bien periódica.

De una forma alternativa, se puede utilizar también un algoritmo alimentado por valores aleatorios de la instalación para la fijación de los instantes de cambio. Otra posibilidad es que se supervisa un régimen de carga del bus de datos 514 y se inicia la generación de las claves o bien el cambio de los programas de cifrado en un instante, en el que el régimen de carga del bus de datos 514 es reducido. Esto tiene la ventaja de que se puede utilizar la anchura de banda no usada del bus de datos 514 para la transmisión de los valores de medición a los aparatos de automatización individuales.

REIVINDICACIONES

1. Procedimiento para la transmisión de datos con las siguientes etapas:

- entrada de primeros datos desde un proceso estocástico (114) en al menos primeros y segundos usuarios (102, 104; 402, 404; 502, 504, 506, 508, 510, 512, 516) de una red de comunicaciones (100, 106; 400, 406; 500, 514, 518),
- en cada uno de los al menos primeros y segundos usuarios, la generación de una clave simétrica (S1, S2), que se basa en los primeros datos y la memorización de la clave simétrica para una transmisión de datos cifrados entre los al menos primeros y segundos usuarios,

caracterizado porque cada uno de los al menos primeros y segundos usuarios disponen de medios (108; 408) para al menos un primero y un segundo procedimiento de cifrado para la generación de claves, en el que sobre la base de los primeros datos se generan en cada caso primeras y segundas claves simétricas, respectivamente, y porque para la transmisión de datos cifrados se conmuta en secuencia temporal entre dichos primeros y segundos procedimientos de cifrado para la generación de las claves.

2. Procedimiento de acuerdo con la reivindicación 1, en el que para la generación de las primeras y segundas claves en cada uno de los primeros y segundos usuarios se forman primeros datos diferentes a través de diferente combinación de los datos estocásticos.

3. Procedimiento de acuerdo con las reivindicaciones 1 ó 2, en el que los primeros datos son transmitidos a través de la red de comunicaciones (100, 106; 400, 406; 500, 514, 518).

4. Procedimiento de acuerdo con una de las reivindicaciones anteriores, en el que los primeros datos se obtienen a través del registro de al menos un valor de medición a partir del proceso estocástico (114).

5. Procedimiento de acuerdo con una de las reivindicaciones anteriores, en el que en el proceso estocástico se trata de un parámetro variable en el tiempo de un sistema de automatización.

6. Procedimiento de acuerdo con una de las reivindicaciones anteriores, en el que los primeros datos se obtienen a partir de posiciones binarias menos significativas (LSB) de uno o varios valores de medición.

7. Procedimiento de acuerdo con una de las reivindicaciones anteriores, en el que cada uno de los al menos primeros y segundos usuarios registran datos, a partir de los cuales se forman los primeros datos.

8. Procedimiento de acuerdo con la reivindicación 7, en el que los primeros datos se forman a partir de los datos estocásticos a través de una combinación predeterminada.

9. Procedimiento de acuerdo con la reivindicación 7 u 8, en el que los datos estocásticos se transmiten a través de la red de comunicaciones (100, 106; 400, 406; 500, 514, 518).

10. Procedimiento de acuerdo con una de las reivindicaciones anteriores, en el que la generación de la clave simétrica se lleva a cabo en los usuarios a petición de un usuario maestro de la red de comunicaciones.

11. Procedimiento de acuerdo con una de las reivindicaciones anteriores, en el que la generación de la clave simétrica se lleva a cabo en instantes predeterminados o después de intervalos de tiempo predeterminados en los al menos primeros y segundos usuarios.

12. Procedimiento de acuerdo con una de las reivindicaciones anteriores, en el que la transmisión de los primeros datos o de los datos estocásticos se leva a cabo en un instante de régimen de trabajo reducido de la red de comunicaciones.

13. Procedimiento de acuerdo con una de las reivindicaciones anteriores, en el que la transmisión de los primeros datos o de los datos estocásticos se lleva a cabo con un procedimiento de cifrado asimétrico.

14. Producto de programa de ordenador, especialmente medio de memoria digital, con medios de programación para la realización de las siguientes etapas:

- entrada de primeros datos desde un proceso estocástico (114) en al menos primeros y segundos usuarios (102, 104; 402, 404; 502, 504, 506, 508, 510, 512, 516) de una red de comunicaciones (100, 106; 400, 406; 500, 514, 518),
- en cada uno de los al menos primeros y segundos usuarios, la generación de una clave simétrica (S1, S2), que se basa en los primeros datos y la memorización de la clave simétrica para una transmisión de datos cifrados entre los al menos primeros y segundos usuarios,

caracterizado porque cada uno de los al menos primeros y segundos usuarios disponen de medios (108; 408) para al menos un primero y un segundo procedimiento de cifrado para la generación de claves, en el que sobre la base de los primeros datos se generan en cada caso primeras y segundas claves simétricas, respectivamente, y porque para la transmisión de datos cifrados se conmuta en secuencia temporal entre dichos primeros y segundos procedimientos de cifrado para la generación de las claves.

15. Producto de programa de ordenador de acuerdo con la reivindicación 14, en el que los primeros datos son obtenidos a través de la detección de un valor de medición a partir del proceso estocástico (114).

16. Producto de programa de ordenador de acuerdo con la reivindicación 14 ó 15, en el que los primeros datos se obtienen a partir de posiciones binarias menos significativas (LSB) de uno o varios valores de medición.

17. Sistema de comunicaciones con al menos primeros y segundos usuarios (102, 104; 402, 404; 502, 504, 506, 508, 510, 512, 516) de una red de comunicaciones (100, 106; 400, 406; 500, 514, 518) para una transmisión de datos entre los al menos primeros y segundos usuarios, y con

- medios (112) para la entrada de primeros datos desde un proceso estocástico (114) en al menos primeros y segundos usuarios,
- en cada uno de los al menos primeros y segundos usuarios, unos medios (108; 408) para la generación de una clave simétrica, que se basa en los primeros datos y medios (110; 426; 520, 522) la memorización de

la clave simétrica para una transmisión de datos cifrados entre los al menos primeros y segundos usuarios,

caracterizado porque cada uno de los al menos primeros y segundos usuarios disponen de medios (108; 408) para al menos un primero y un segundo procedimiento de cifrado para la generación de claves, en el que sobre la base de los primeros datos se generan en cada caso primeras y segundas claves simétricas, respectivamente, y porque para la transmisión de datos cifrados se conmuta en secuencia temporal entre dichos primeros y segundos procedimientos de cifrado para la generación de las claves.

18. Sistema de comunicaciones de acuerdo con la reivindicación 17, en el que en la red de comunicaciones (100, 106; 400, 406; 500, 514, 518) se trata de una red pública.

19. Sistema de comunicaciones de acuerdo con la reivindicación 17 ó 18, en el que en la red de comunicaciones (100, 106; 400, 406; 500, 514, 518) se trata de Internet y un usuario está configurado como usuario maestro, para provocar la generación de claves en los otros usuarios a través de la transmisión de una solicitud correspondiente a través de Internet.

20. Sistema de comunicaciones de acuerdo con la reivindicación 17 ó 18, en el que en la red de comunicaciones (100, 106; 400, 406; 500, 514, 518) se trata de una Ethernet.

21. Sistema de comunicaciones de acuerdo con la reivindicación 20, en el que uno de los usuarios está configurado como usuario maestro con el fin de emitir sobre la Ethernet un comando para la activación de la generación de las claves en los usuarios.

22. Sistema de comunicaciones de acuerdo con una de las reivindicaciones anteriores 17 a 21, en el que en los al menos primeros y segundos usuarios se trata de componentes de un sistema de automatización (500).

23. Sistema de comunicaciones de acuerdo con una de las reivindicaciones anteriores 17 a 22, en el que al menos uno de los usuarios (516) está configurado para la realización de un mantenimiento a distancia.

FIG 1

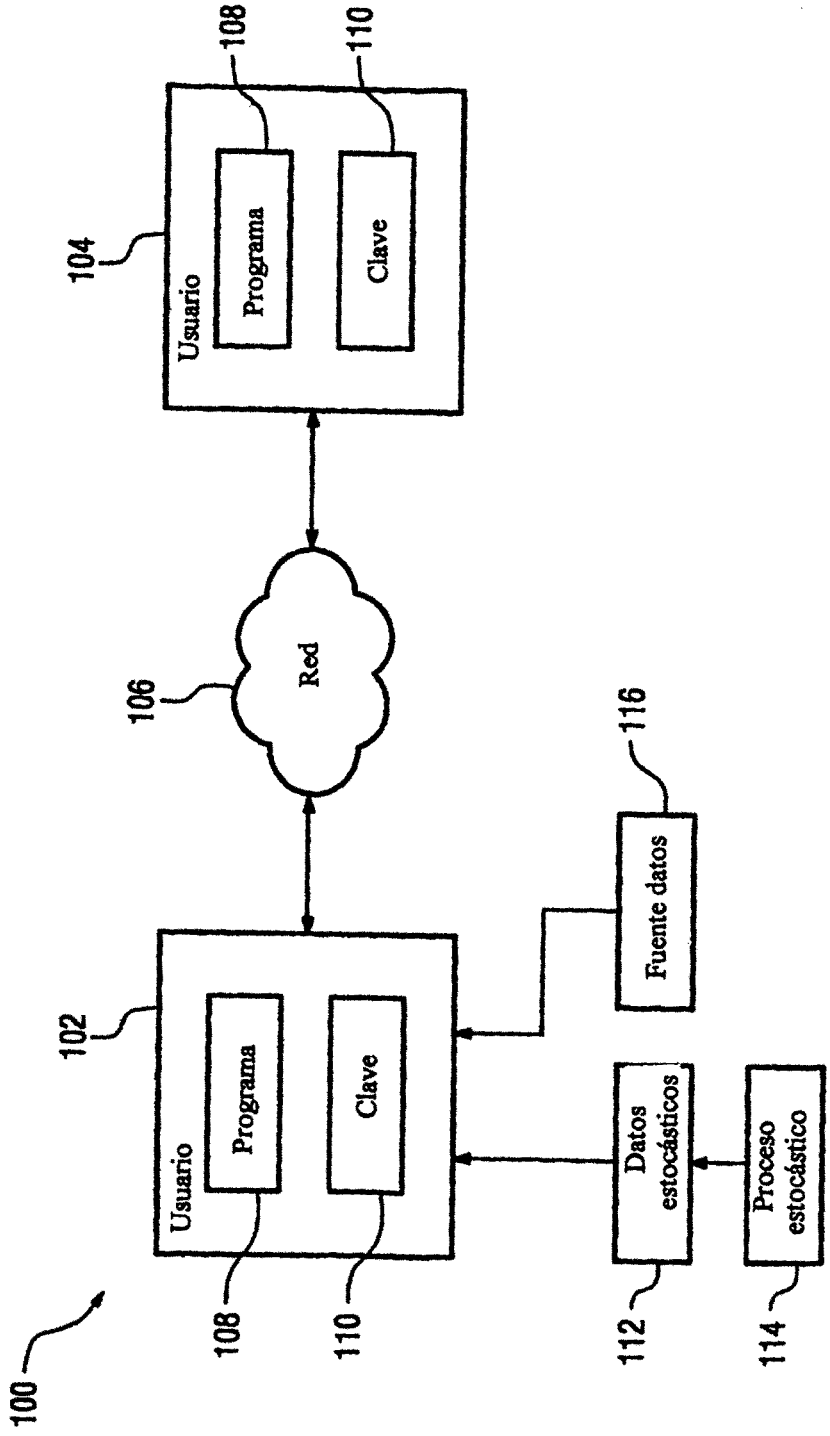

100
102
Usuario
Programa
Clave
104
Usuario
Programa
Clave
106
Red
108
110
108
110
112
114
116
Fuente datos
Datos estocásticos
Proceso estocástico

FIG 2

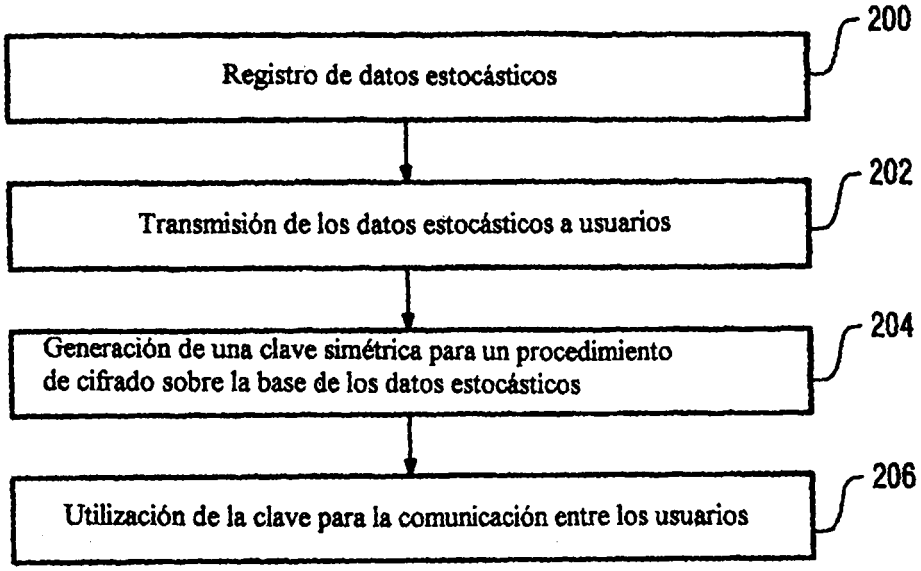

Registro de datos estocásticos
200
Transmisión de los datos estocásticos a usuarios
202
Generación de una clave simétrica para un procedimiento de cifrado sobre la base de los datos estocásticos
204
Utilización de la clave para la comunicación entre los usuarios
206

FIG 3

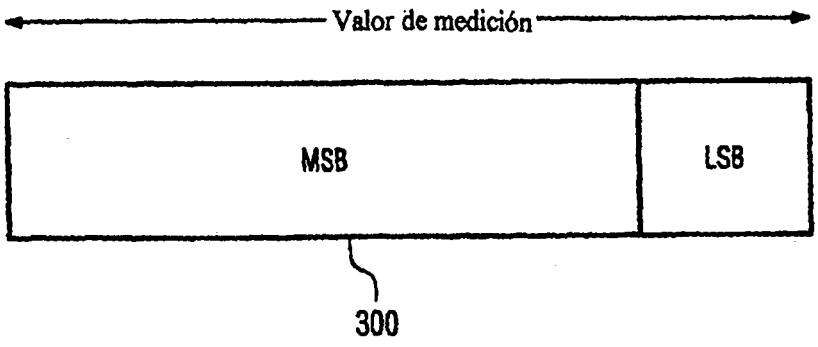
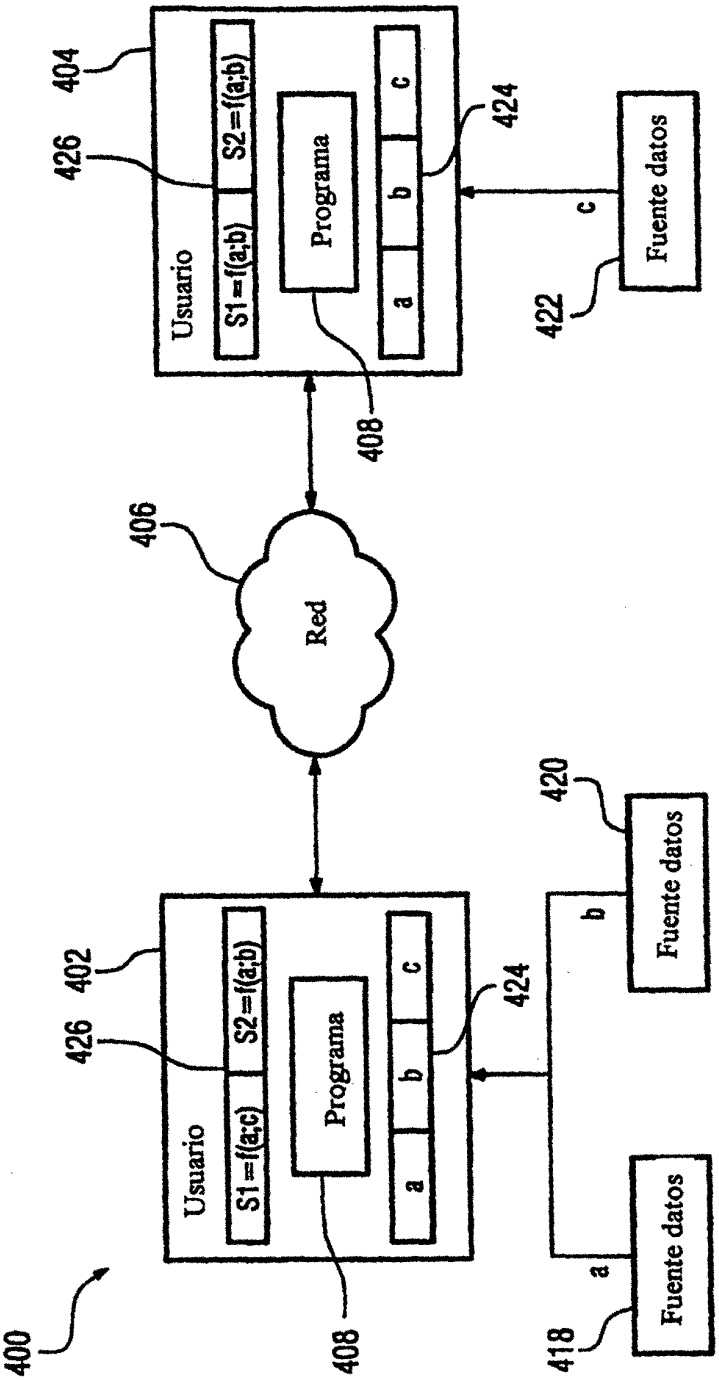

Valor de medición
MSB
LSB
300

FIG 4


400
402
404
406
408
418
420
422
424
426
Usuario
S1=f(a;c)
S2=f(a;b)
Programa
a
b
c
Red
Fuente datos
Fuente datos
Fuente datos
Usuario
S1=f(a;b)
S2=f(a;b)
Programa
a
b
c

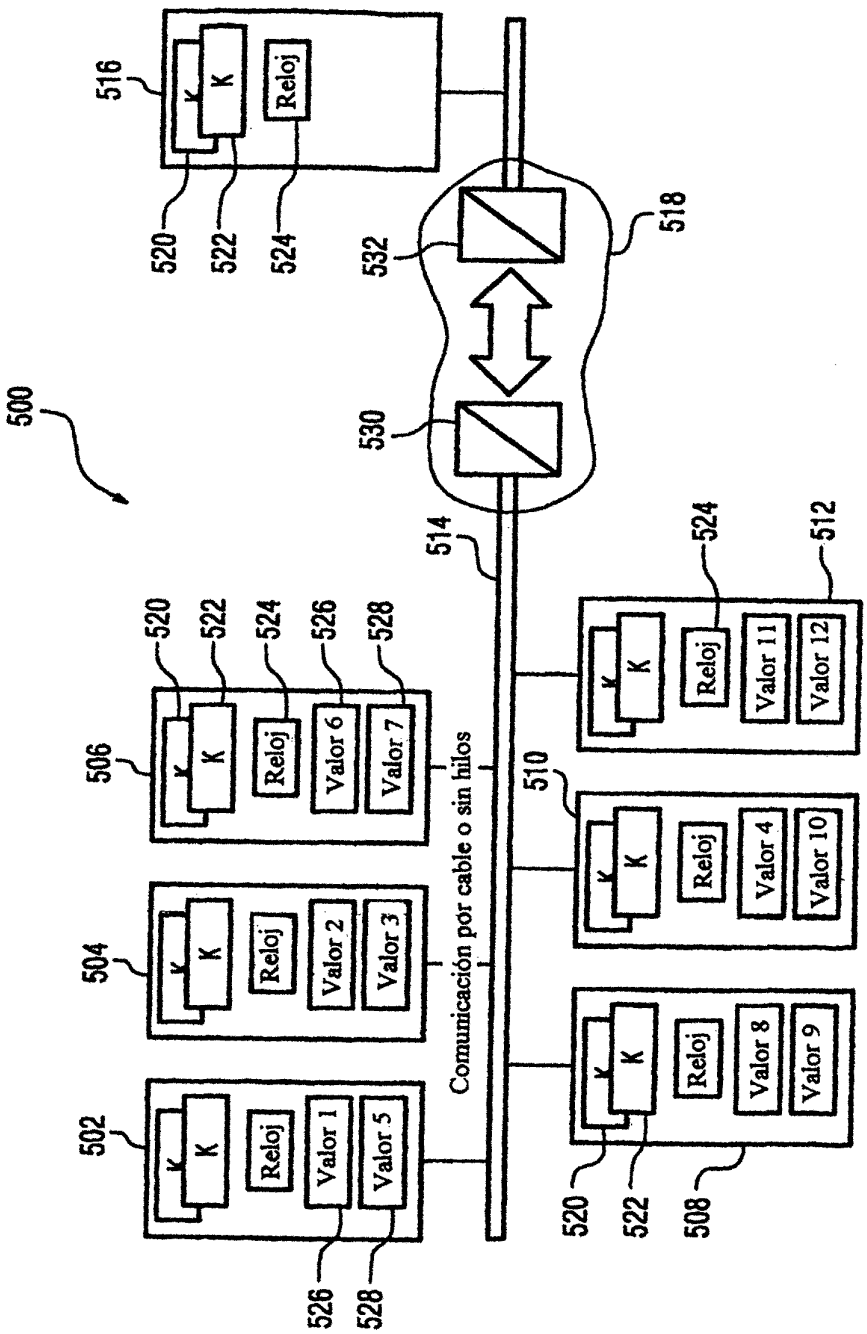

500
502
504
506
508
510
512
514
516
518
520
522
524
526
528
530
532
K
Reloj
Valor 1
Valor 2
Valor 3
Valor 4
Valor 5
Valor 6
Valor 7
Valor 8
Valor 9
Valor 10
Valor 11
Valor 12
Comunicación por cable o sin hilos

FIG. 5