República Federativa do Brasil
Ministério do Desenvolvimento, Indústria e do Comércio Exterior
Instituto Nacional da Propriedade Industrial

(21) PI 0719636-9 A2

* B R P I 0 7 1 9 6 3 6 A 2 *

(22) Data de Depósito: 26/12/2007
(43) Data da Publicação: 17/12/2013
(RPI 2241)

(51) Int.Cl.:
G11C 29/12

(54) Título: DISPOSITIVO PROCESSADOR DE INFORMÁTICA, MÉTODO PROCESSADOR DE INFORMAÇÃO E PROPAGANDA DE COMPUTADOR.

(57) Resumo:

(30) Prioridade Unionista: 28/12/2006 JP 2006-356594

(73) Titular(es): N - CRYPT, INC

(72) Inventor(es): TAKATOSHI NAKAMURA

(74) Procurador(es): Veirano e Advogados Associados

(86) Pedido Internacional: PCT JP2007075376 de 26/12/2007

(87) Publicação Internacional: WO 2008/081975de 10/07/2008

Relatório Descritivo da Patente de Invenção para: "**DISPOSITIVO DE PROCESSAMENTO DE INFORMAÇÕES, MÉTODO DE PROCESSAMENTO DE INFORMAÇÕES E PROGRAMA COMPUTADORIZADO**"

CAMPO DA INVENÇÃO

A presente invenção refere-se a uma técnica para a redução do risco de perda de dados.

FUNDAMENTOS DA INVENÇÃO

As demandas sobre segurança estão crescendo a cada dia.

Os dados são perdidos de diversas maneiras. Por exemplo, os dados são perdidos de um computador conectado a um ambiente de rede por acesso não autorizado ou por uma interrupção para uma via de comunicação. Quando os dados são gravados em um meio de gravação incluído em um computador ou em um meio de gravação portátil, a perda de dados ocorre a partir de um computador roubado ou de um meio de gravação portátil.

Especificamente, os dados ficam constantemente expostos ao risco de perda por todo o tempo de sua existência.

Em vista de tal risco, prefere-se que os dados sejam excluídos imediatamente após serem utilizados ou assim que não forem mais necessários. Entretanto, é incômodo para os usuários passar por tal esforço extra. Além disso, a exclusão de dados executada em um computador por um processamento geral apenas exclui dados em uma área de gerenciamento de arquivos. Como o conteúdo dos dados (mais precisamente de um arquivo) permanece, na maioria dos casos no disco rígido, fica difícil a exclusão completa dos dados. É certo que existe software para escrita de dados "0" ou "1" em uma seqüência de dados existentes para excluir completamente os dados existentes, a fim de excluí-los completamente em um disco rígido (mais precisamente, os dados existentes são transformados em dados completamente não significativos ou, de certa forma, em

dados "inúteis"). Entretanto, como tal processamento leva um tempo extremamente longo, fica difícil para os usuários executar o processamento rotineiramente.

O(s) inventor(es) da presente invenção realizaram estudos sobre o problema de segurança, como descrito acima, para descobrir o seguinte ponto. O ponto está relacionado a uma técnica de criptografia que o(s) inventor(es) tem(têm) estudado diariamente.

Os dados criptografados obtidos pela criptografia de dados de textos simples apropriados (mencionados como "dados a serem processados" por toda esta especificação) são completamente não significativos, a não ser que os dados criptografados sejam descriptografados. Sob esse aspecto, os dados criptografados têm uma forte semelhança com os dados "inúteis" sobrescritos com os dados "0" ou "1" descritos acima. Ampliando a idéia, os dados criptografados são transformados em dados completamente insignificantes, "dados inúteis", logo que a descriptografia dos dados criptografados se torna impossível.

O avanço posterior da idéia descrita acima levou o(s) inventor(es) da presente invenção ao seguinte. Para os dados criptografados, em particular os dados criptografados que contêm informações necessárias para a descriptografia como parte disso, a destruição da parte que contém as informações necessárias para a descriptografia torna a descriptografia dos dados criptografados impossível. Como resultado, os dados criptografados podem ser transformados em dados "inúteis" mesmo sem ser excluídos. Tal método de destruição de dados (essa "destruição" produz substancialmente o mesmo efeito que o da "exclusão") toma um tempo muito menor do que a sobrescrita de todos os dados com dados "0" ou "1". Portanto, o método de destruição de dados é adequado para o uso diário do usuário.

A presente invenção foi planejada com base na idéia descrita acima e apresenta uma técnica para evitar que os dados criptografados gerados pela

criptografia dos dados a serem processados sejam descriptografados, a fim de produzir o mesmo efeito que o da exclusão completa dos dados a serem processados.

DESCRIÇÃO DA INVENÇÃO

A fim de solucionar o problema descrito acima, o(s) inventor(es) da presente invenção propõe(m) as invenções a seguir. As invenções desta especificação podem ser classificadas em uma invenção básica e nas invenções primeira à terceira baseadas na invenção básica.

A invenção básica é a seguinte.

A invenção básica se refere a um aparelho de processamento de informações para processamento de dados criptografados obtidos pela criptografia de dados de textos simples a serem processados, os dados criptografados contendo informações de especificação para a descriptografia dos dados criptografados, inclusive meios de gravação para a gravação dos dados criptografados, meios de detecção para a detecção das informações de especificação dos dados criptografados e meios de processamento para causar uma alteração irreversível nas informações de especificação detectadas pelos meios de detecção nos dados criptografados gravados nos meios de gravação quando uma condição predeterminada é satisfeita.

Os dados criptografados utilizados no aparelho de processamento de informações contêm as informações de especificação para a descriptografia dos dados criptografados. Na descriptografia dos dados criptografados, as informações de especificação são necessárias. Especificamente, se uma alteração irreversível for causada nas informações de especificação, os dados criptografados não podem mais ser descriptografados. Os dados criptografados que não podem mais ser descriptografados, como descrito acima, podem ser mencionados como dados "inúteis". A prevenção da descriptografia dos dados criptografados desta maneira produz o mesmo efeito que o da exclusão completa dos dados a serem processados.

O mesmo efeito que o da invenção básica também pode ser obtido pelo método a seguir.

O método consiste em um método de processamento de informações para o processamento de dados criptografados obtidos pela criptografia de dados de textos simples a serem processados, os dados criptografados contendo informações de especificação para a descriptografia dos dados criptografados, inclusive meios de gravação e processamento, e o método incluindo as etapas, que são executadas pelos meios de processamento, de gravação dos dados criptografados nos meios de gravação, de detecção das informações de especificação dos dados criptografados e de provocação de uma alteração irreversível nas informações de especificação detectadas no processo de detecção nos dados criptografados gravados nos meios de gravação quando uma condição predeterminada é satisfeita.

O efeito obtido pelo aparelho de processamento de informações descrito acima também pode ser obtido, por exemplo, pelo programa computadorizado a seguir. Utilizando o programa computadorizado a seguir, o mesmo efeito que o da invenção descrita acima pode ser obtido com um computador comum.

O programa é um programa computadorizado para processamento de dados criptografados obtidos pela criptografia de dados de textos simples a serem processados, os dados criptografados contendo informações de especificação para a descriptografia dos dados criptografados, o programa computadorizado tem como objetivo fazer com que um computador contido em um aparelho de processamento de informações, incluindo meios de gravação e o computador conectado execute as etapas de gravação dos dados criptografados nos meios de gravação, detectando as informações de especificação dos dados criptografados, e causando uma alteração irreversível nas informações de especificação detectadas no processo de detecção nos dados criptografados gravados nos meios de gravação quando uma condição predeterminada é satisfeita.

Note que a condição predeterminada na invenção básica pode ser a

mesma que a de um disparador para o início do processo de processamento para causar a alteração irreversível na primeira até a terceira invenções (qualquer entrada de informações do disparador de destruição, a determinação de que o cronograma especificado pelas informações de especificação do cronograma chegou ou não e a entrada das informações do disparador de descriptografia).

A primeira invenção é um aparelho de processamento de informações para o processamento de dados criptografados que consiste em uma unidade de uma série de partes dos dados criptografados divisionais gerados pela criptografia de uma série de partes dos dados de textos simples divisionais utilizando uma série de chaves geradas pela divisão dos dados de textos simples a serem processados nos dados que são compostos por um número predeterminadode bits, pelo menos uma das chaves diferindo da(s) outra(s); os dados criptografados são novamente descriptografados nos dados a serem processados pela descriptografia dos dados criptografados divisionais em uma ordem predeterminada para conectar os dados descriptografados em uma unidade, cada um dos dados criptografados divisionais, exceto o último a ser descriptografado, contendo informações de especificação para a especificação de uma chave para a descriptografia do próximo dado criptografado divisional a ser descriptografado para permitir a descriptografia.

Além disso, o aparelho de processamento de informações inclui: meios de gravação para a gravação dos dados criptografados; meios de entrada do disparador de destruição para a entrada de informações do disparador de destruição para o início de um processamento a fim de evitar que os dados criptografados sejam descriptografados; meios de detecção para a detecção do primeiro dado criptografado divisional correspondente aos dados criptografados divisionais que é o primeiro a ser descriptografado em todos os dados criptografados divisionais dos dados criptografados; e meios de processamento para a recepção de uma entrada das informações do disparador de destruição na entrada do mesmo para fazer com que aconteça uma alteração irreversível no

primeiro dado criptografado divisional detectado pelos meios de detecção nos dados criptografados gravados nos meios de gravação.

Nos dados criptografados utilizados no aparelho de processamento de informações, cada um dos dados criptografados divisionais, exceto o último a ser descriptografado, contém as informações de especificação para a especificação da chave para a descriptografia do próximo dado criptografado divisional a ser descriptografado. Os dados criptografados são descriptografados em seqüência pela execução de um processo de descriptografia do primeiro dado criptografado divisional nos dados de textos simples divisionais, utilizando a chave especificada pelas informações de especificação extraídas dos dados de textos simples divisionais obtidos para descriptografar o segundo dado criptografado divisional nos dados de textos simples divisionais, utilizando a chave especificada pelas informações de especificação extraídas dos dados de textos simples divisionais obtidos para descriptografar o terceiro dado criptografado divisional nos dados de textos simples divisionais, e assim por diante. Portanto, se uma alteração irreversível for causada no dado criptografado divisional que deve ser o primeiro a ser descriptografado, todos os dados criptografados não podem mais ser descriptografados. Os dados criptografados que não podem mais ser descriptografados podem ser mencionados como dados "inúteis". A prevenção da descriptografia dos dados criptografados desta maneira produz o mesmo efeito que o da exclusão completa dos dados a serem processados.

O mesmo efeito que o da presente invenção também pode ser obtido, por exemplo, pelo método a seguir.

É fornecido um método de processamento de informações executado em um aparelho de processamento de informações, inclusive meios de gravação, meios de entrada do disparador de destruição e meios de processamento, para o processamento de dados criptografados, que consiste em uma unidade de uma série de partes dos dados criptografados divisionais gerados pela criptografia de uma série de partes dos dados de textos simples divisionais utilizando uma série

de chaves geradas pela divisão dos dados de textos simples a serem processados nos dados que são compostos por um número predeterminadode bits, pelo menos uma das chaves diferindo da(s) outra(s); os dados criptografados são novamente descriptografados nos dados a serem processados pela descriptografia dos dados criptografados divisionais em uma ordem predeterminada para conectar os dados descriptografados em uma unidade, cada um dos dados criptografados divisionais, exceto o último dado a ser descriptografado, contendo informações de especificação para a especificação de uma chave para a descriptografia do próximo dado criptografado divisional a ser descriptografado para permitir a descriptografia.

O método inclui as etapas, executadas pelos meios de processamento, de: gravação dos dados criptografados nos meios de gravação; recepção de informações do disparador de destruição para o início de um processamento a fim de evitar que os dados criptografados sejam descriptografados a partir dos meios de entrada do disparador de destruição; detecção do primeiro dado criptografado divisional que é o primeiro a ser descriptografado em todos os dados criptografados divisionais dos dados criptografados; e provocação de uma alteração irreversível no primeiro dado criptografado divisional detectado na etapa de detecção nos dados criptografados gravados nos meios de gravação quando as informações do disparador de destruição são recebidas.

O mesmo efeito que o da invenção descrita acima também pode ser obtido, por exemplo, pelo programa computadorizado a seguir. Utilizando o programa computadorizado a seguir, o mesmo efeito que o da invenção descrita acima pode ser obtido com um computador comum.

É fornecido um programa computadorizado para o processamento de dados criptografados que consiste em uma unidade de uma série de partes dos dados criptografados divisionais gerados pela criptografia de uma série de partes dos dados de textos simples divisionais utilizando uma série de chaves geradas pela divisão dos dados de textos simples a serem processados nos dados que

são compostos por um número predeterminadode bits, pelo menos uma das chaves diferindo da(s) outra(s); os dados criptografados são novamente descriptografados nos dados a serem processados pela descriptografia dos dados criptografados divisionais em uma ordem predeterminada para conectar os dados descriptografados em uma unidade, cada um dos dados criptografados divisionais, exceto o último a ser descriptografado, contendo informações de especificação para a especificação de uma chave para a descriptografia do próximo dado criptografado divisional a ser descriptografado para permitir a descriptografia, o programa computadorizado tem como objetivo fazer com que um computador contido em um aparelho de processamento de informações, incluindo meios de gravação, meios de entrada do disparador de destruição e o computador também conectado, execute as etapas a seguir.

As etapas são: gravação dos dados criptografados nos meios de gravação; recepção de informações do disparador de destruição para o início de um processamento a fim de evitar que os dados criptografados sejam descriptografados a partir dos meios de entrada do disparador de destruição; detecção do primeiro dado criptografado divisional que é o primeiro a ser descriptografado em todos os dados criptografados divisionais dos dados criptografados; e provocação de uma alteração irreversível no primeiro dado criptografado divisional detectado na etapa de detecção nos dados criptografados gravados nos meios de gravação quando as informações do disparador de destruição são recebidas.

Como descrito acima, nos dados criptografados utilizados no aparelho de processamento de informações, de acordo com a primeira invenção, cada um dos dados criptografados divisionais, exceto o último a ser descriptografado, contém as informações de especificação para a especificação da chave para a descriptografia do próximo dado criptografado divisional a ser descriptografado. Os dados criptografados utilizados no aparelho de processamento de informações, de acordo com a primeira invenção, podem conter primeiro as informações de

especificação para a especificação da chave para a descriptografia do dado criptografado divisional que é o primeiro a ser descriptografado.

Cada uma das chaves para a descriptografia dos dados criptografados divisionais, que são o segundo e o subseqüente a ser descriptografados, é especificada pelas informações de especificação extraídas dos dados de textos simples divisionais obtidos pela descriptografia dos dados criptografados divisionais que são descriptografados imediatamente antes. Para descriptografar o dado criptografado divisional que é o primeiro a ser descriptografado, entretanto, a primeira informação de especificação para a especificação da chave para a descriptografia dos dados criptografados divisionais de interesse é normalmente necessária. A primeira informação de especificação está incorporada nos dados criptografados em alguns casos e não está incorporada nos dados criptografados como regra específica compartilhada entre, por exemplo, um aparelho que criptografou os dados criptografados e outro aparelho que deve descriptografar os dados criptografados em outros casos. Quando a primeira informação de especificação estiver incorporada nos dados criptografados, a primeira invenção pode ser constituída da seguinte maneira.

A primeira invenção, neste caso, é um aparelho de processamento de informações para o processamento de dados criptografados que consiste em uma unidade de uma série de partes dos dados criptografados divisionais gerados pela criptografia de uma série de partes dos dados de textos simples divisionais utilizando uma série de chaves geradas pela divisão dos dados de textos simples a serem processados nos dados que são compostos por um número predeterminadode bits, pelo menos uma das chaves diferindo da(s) outra(s); os dados criptografados são novamente descriptografados nos dados a serem processados pela descriptografia dos dados criptografados divisionais em uma ordem predeterminada para conectar os dados descriptografados em uma unidade, cada um dos dados criptografados divisionais, exceto o último a ser descriptografado, contendo informações de especificação para a especificação de

uma chave para a descriptografia do próximo dado criptografado divisional a ser descriptografado para permitir a descriptografia, os dados criptografados contendo a primeira informação de especificação para a especificação da chave para a descriptografia do dado criptografado divisional a ser descriptografado primeiro.

Além disso, o aparelho de processamento de informações inclui: meios de gravação para a gravação dos dados criptografados; meios de entrada do disparador de destruição para a entrada de informações do disparador de destruição para o início de um processamento a fim de evitar que os dados criptografados sejam descriptografados; meios de detecção para a detecção da primeira informação de especificação contida nos dados criptografados ou do primeiro dado criptografado divisional correspondente ao dado criptografado divisional que é o primeiro a ser descriptografado dos dados criptografados; e meios de processamento para a recepção de uma entrada das informações do disparador de destruição na entrada do mesmo para fazer com que aconteça uma alteração irreversível na primeira informação de especificação ou no primeiro dado criptografado divisional detectado pelos meios de detecção nos dados criptografados gravados nos meios de gravação.

Especificamente, o aparelho de processamento de informações faz com que uma alteração irreversível no dado criptografado divisional que deve ser o primeiro a ser descriptografado, ou na primeira informação de especificação utilizada para a descriptografia do dado criptografado divisional que deve ser o primeiro a ser descriptografado em todos os dados criptografados divisionais. Com a execução de tal processo, os dados criptografados não podem mais ser descriptografados. Os dados criptografados que não podem mais ser descriptografados, como descrito acima, podem ser mencionados como dados "inúteis". A prevenção da descriptografia dos dados criptografados desta maneira produz o mesmo efeito que o da exclusão completa dos dados a serem processados.

O mesmo efeito que o da presente invenção também pode ser obtido, por exemplo, pelo método a seguir.

É fornecido um método de processamento de informações executado em um aparelho de processamento de informações, inclusive meios de gravação, meios de entrada do disparador de destruição e meios de processamento, para o processamento de dados criptografados, que consiste em uma unidade de uma série de partes dos dados criptografados divisionais gerados pela criptografia de uma série de partes dos dados de textos simples divisionais utilizando uma série de chaves geradas pela divisão dos dados de textos simples a serem processados nos dados que são compostos por um número predeterminadode bits, pelo menos uma das chaves diferindo da(s) outra(s); os dados criptografados são novamente descriptografados nos dados a serem processados pela descriptografia dos dados criptografados divisionais em uma ordem predeterminada para conectar os dados descriptografados em uma unidade, cada um dos dados criptografados divisionais, exceto o último dado a ser descriptografado, contendo informações de especificação para a especificação de uma chave para a descriptografia do próximo dado criptografado divisional a ser descriptografado para permitir a descriptografia, os dados criptografados contendo a primeira informação de especificação para a especificação da chave para a descriptografia do dado criptografado divisional que é o primeiro a ser descriptografado.

O método inclui as etapas, executadas pelos meios de processamento, de: gravação dos dados criptografados nos meios de gravação; recepção de informações do disparador de destruição para o início de um processamento a fim de evitar que os dados criptografados sejam descriptografados a partir dos meios de entrada do disparador de destruição; detecção da primeira informação de especificação contida nos dados criptografados ou do primeiro dado criptografado divisional que é o primeiro a ser descriptografado em todos os dados criptografados divisionais dos dados criptografados; e provocação de uma

alteração irreversível na primeira informação de especificação ou no primeiro dado criptografado divisional detectado na etapa de detecção nos dados criptografados gravados nos meios de gravação quando as informações do disparador de destruição são recebidas.

O mesmo efeito que o da invenção descrita acima também pode ser obtido, por exemplo, pelo programa computadorizado a seguir. Utilizando o programa computadorizado a seguir, o mesmo efeito que o da invenção descrita acima pode ser obtido com um computador comum.

É fornecido um programa computadorizado para o processamento de dados criptografados que consiste em uma unidade de uma série de partes dos dados criptografados divisionais gerados pela criptografia de uma série de partes dos dados de textos simples divisionais utilizando uma série de chaves geradas pela divisão dos dados de textos simples a serem processados nos dados que são compostos por um número predeterminadode bits, pelo menos uma das chaves diferindo da(s) outra(s); os dados criptografados são novamente descriptografados nos dados a serem processados pela descriptografia dos dados criptografados divisionais em uma ordem predeterminada para conectar os dados descriptografados em uma unidade, cada um dos dados criptografados divisionais, exceto o último a ser descriptografado, contendo informações de especificação para a especificação de uma chave para a descriptografia do próximo dado criptografado divisional a ser descriptografado para permitir a descriptografia, os dados criptografados contendo a primeira informação de especificação para a especificação da chave para a descriptografia do dado criptografado divisional que é o primeiro a ser descriptografado, o programa computadorizado tendo como objetivo fazer com que um computador contido em um aparelho de processamento de informações, incluindo meios de gravação, meios de entrada do disparador de destruição, e o computador conectado, execute as etapas a seguir.

As etapas são: gravação dos dados criptografados nos meios de

gravação; recepção de informações do disparador de destruição para o início de um processamento a fim de evitar que os dados criptografados sejam descriptografados a partir dos meios de entrada do disparador de destruição; detecção da primeira informação de especificação contida nos dados criptografados ou do primeiro dado criptografado divisional que é o primeiro a ser descriptografado em todos os dados criptografados divisionais dos dados criptografados; e provocação de uma alteração irreversível na primeira informação de especificação ou no primeiro dado criptografado divisional detectado na etapa de detecção nos dados criptografados gravados nos meios de gravação quando as informações do disparador de destruição são recebidas.

A segunda invenção é um aparelho de processamento de informações para o processamento de dados criptografados que consiste em uma unidade de uma série de partes dos dados criptografados divisionais gerados pela criptografia de uma série de partes dos dados de textos simples divisionais utilizando uma série de chaves geradas pela divisão dos dados de textos simples a serem processados nos dados que são compostos por um número predeterminadode bits, pelo menos uma das chaves diferindo da(s) outra(s); os dados criptografados são novamente descriptografados nos dados a serem processados pela descriptografia dos dados criptografados divisionais em uma ordem predeterminada para conectar os dados descriptografados em uma unidade, cada um dos dados criptografados divisionais, exceto o último a ser descriptografado, contendo informações de especificação para a especificação de uma chave para a descriptografia do próximo dado criptografado divisional a ser descriptografado para permitir a descriptografia, os dados criptografados contendo informações de especificação do cronograma para especificar o cronograma a fim de evitar que os dados criptografados sejam descriptografados.

Além disso, o aparelho de processamento de informações inclui: meios de gravação para a gravação dos dados criptografados; meios de leitura das informações de especificação do cronograma para a leitura das informações de

especificação do cronograma dos dados criptografados; meios de detecção para a detecção do primeiro dado criptografado divisional correspondente ao dado criptografado divisional a ser descriptografado primeiro em todos os dados criptografados divisionais dos dados criptografados; e meios de processamento para monitorar se o cronograma especificado pelas informações de especificação do cronograma lidas pelos meios de leitura das informações de especificação do cronograma chegou ou não, e causando uma alteração irreversível no primeiro dado criptografado divisional detectado pelos meios de detecção no caso de o cronograma ter chegado.

Os dados criptografados utilizados no aparelho de processamento de informações são aproximadamente os mesmos que na primeira invenção, mas ainda contêm as informações de especificação do cronograma para especificar o cronograma a fim de evitar que os dados criptografados sejam descriptografados. O aparelho de processamento de informações causa uma alteração irreversível no primeiro dado criptografado divisional para transformar os dados criptografados em uma espécie de dados "inúteis", como na primeira invenção. O cronograma para transformar os dados criptografados em dados "inúteis" é controlado pelas informações de especificação do cronograma. O aparelho de processamento de informações, por exemplo, monitora constantemente se o cronograma, a fim de evitar que os dados criptografados especificados pelas informações de especificação do cronograma sejam descriptografados, chegou ou não, e se chegou causa uma alteração irreversível no primeiro dado criptografado divisional imediatamente após o cronograma ou após o decorrer de um determinado período de tempo após o cronograma, como na primeira invenção. Como descrito na arte relacionada, sempre há risco de perda de dados, mesmo que os dados estejam criptografados. A execução automática do processamento descrito acima de transformação dos dados criptografados em uma espécie de dados "inúteis" pelo aparelho de processamento de informações é significativa em vista da prevenção da perda de dados a serem processados.

O mesmo efeito que o da presente invenção também pode ser obtido, por exemplo, pelo método a seguir.

É fornecido um método de processamento de informações executado em um aparelho de processamento de informações, inclusive meios de gravação e meios de processamento, para o processamento de dados criptografados, que consiste em uma unidade de uma série de partes dos dados criptografados divisionais gerados pela criptografia de uma série de partes dos dados de textos simples divisionais utilizando uma série de chaves geradas pela divisão dos dados de textos simples a serem processados nos dados que são compostos por um número predeterminadode bits, pelo menos uma das chaves diferindo da(s) outra(s); os dados criptografados são novamente descriptografados nos dados a serem processados pela descriptografia dos dados criptografados divisionais em uma ordem predeterminada para conectar os dados descriptografados em uma unidade, cada um dos dados criptografados divisionais, exceto o último dado a ser descriptografado, contendo informações de especificação para a especificação de uma chave para a descriptografia do próximo dado criptografado divisional a ser descriptografado para permitir a descriptografia, os dados criptografados contendo informações de especificação do cronograma para especificar o cronograma a fim de evitar que os dados criptografados sejam descriptografados.

O método inclui as etapas, executadas pelos meios de processamento, de: gravação dos dados criptografados nos meios de gravação; leitura das informações de especificação do cronograma dos dados criptografados; detecção do primeiro dado criptografado divisional que é o primeiro a ser descriptografado em todos os dados criptografados divisionais dos dados criptografados; e monitorar se o cronograma especificado pelas informações de especificação do cronograma lidas na etapa de leitura chegou, causando uma alteração irreversível no primeiro dado criptografado divisional detectado na etapa de detecção no caso de o cronograma ter chegado.

O mesmo efeito que o da invenção descrita acima também pode ser obtido, por exemplo, pelo programa computadorizado a seguir. Utilizando o programa computadorizado a seguir, o mesmo efeito que o da invenção descrita acima pode ser obtido com um computador comum.

É fornecido um programa computadorizado para o processamento de dados criptografados que consiste em uma unidade de uma série de partes dos dados criptografados divisionais gerados pela criptografia de uma série de partes dos dados de textos simples divisionais utilizando uma série de chaves geradas pela divisão dos dados de textos simples a serem processados nos dados que são compostos por um número predeterminadode bits, pelo menos uma das chaves diferindo da(s) outra(s); os dados criptografados são novamente descriptografados nos dados a serem processados pela descriptografia dos dados criptografados divisionais em uma ordem predeterminada para conectar os dados descriptografados em uma unidade, cada um dos dados criptografados divisionais, exceto o último a ser descriptografado, contendo informações de especificação para a especificação de uma chave para a descriptografia do próximo dado criptografado divisional a ser descriptografado para permitir a descriptografia, os dados criptografados contendo informações de especificação do cronograma para especificar o cronograma a fim de evitar que os dados criptografados sejam descriptografados, o programa computadorizado tem como objetivo fazer com que um computador contido em um aparelho de processamento de informações, incluindo o computador conectado aos meios de gravação, execute as etapas a seguir.

As etapas são: gravação dos dados criptografados nos meios de gravação; leitura das informações de especificação do cronograma dos dados criptografados; detecção do primeiro dado criptografado divisional que é o primeiro a ser descriptografado em todos os dados criptografados divisionais dos dados criptografados; e monitorar se o cronograma especificado pelas informações de especificação do cronograma lidas na etapa de leitura chegou,

causando uma alteração irreversível no primeiro dado criptografado divisional detectado na etapa de detecção no caso de o cronograma ter chegado.

Como descrito acima, nos dados criptografados utilizados no aparelho de processamento de informações, de acordo com a segunda invenção, cada um dos dados criptografados divisionais, exceto o último a ser descriptografado, contém as informações de especificação para a especificação da chave para a descriptografia do próximo dado criptografado divisional a ser descriptografado. Assim, os dados criptografados utilizados no aparelho de processamento de informações, de acordo com a segunda invenção, podem conter primeiro as informações de especificação para a especificação da chave para a descriptografia do dado criptografado divisional que é o primeiro a ser descriptografado.

Quando a primeira informação de especificação estiver incorporada nos dados criptografados, a segunda invenção pode ser constituída da seguinte maneira.

A segunda invenção, neste caso, é um aparelho de processamento de informações para o processamento de dados criptografados que consiste em uma unidade de uma série de partes dos dados criptografados divisionais gerados pela criptografia de uma série de partes dos dados de textos simples divisionais utilizando uma série de chaves geradas pela divisão dos dados de textos simples a serem processados nos dados que são compostos por um número predeterminadode bits, pelo menos uma das chaves diferindo da(s) outra(s); os dados criptografados são novamente descriptografados nos dados a serem processados pela descriptografia dos dados criptografados divisionais em uma ordem predeterminada para conectar os dados descriptografados em uma unidade, cada um dos dados criptografados divisionais, exceto o último a ser descriptografado, contendo informações de especificação para a especificação de uma chave para a descriptografia do próximo dado criptografado divisional a ser descriptografado para permitir a descriptografia, os dados criptografados

contendo a primeira informação de especificação para a especificação da chave para a descriptografia do dado criptografado divisional que é o primeiro a ser descriptografado e as informações de especificação do cronograma para especificar o cronograma a fim de evitar que os dados criptografados sejam descriptografados.

Além disso, o aparelho de processamento de informações inclui: meios de gravação para a gravação dos dados criptografados; meios de leitura das informações de especificação do cronograma para a leitura das informações de especificação do cronograma dos dados criptografados; meios de detecção para a detecção da primeira informação de especificação contida nos dados criptografados ou do primeiro dado criptografado divisional correspondente ao dado criptografado divisional que é o primeiro a ser descriptografado em todos os dados criptografados divisionais dos dados criptografados; e meios de processamento para monitorar se o cronograma especificado pelas informações de especificação do cronograma lidas pelos meios de leitura das informações de especificação do cronograma chegou ou não, causando uma alteração irreversível na primeira informação de especificação ou no primeiro dado criptografado divisional detectado pelos meios de detecção no caso de o cronograma ter chegado.

Especificamente, o aparelho de processamento de informações faz com que uma alteração irreversível no dado criptografado divisional que deve ser o primeiro a ser descriptografado ou na primeira informação de especificação utilizada para a descriptografia do dado criptografado divisional que deve ser o primeiro a ser descriptografado em todos os dados criptografados divisionais. Com a execução de tal processamento, os dados criptografados não podem mais ser descriptografados. Os dados criptografados que não podem mais ser descriptografados, como descrito acima, podem ser mencionados como dados "inúteis". A prevenção da descriptografia dos dados criptografados desta maneira produz o mesmo efeito que o da exclusão completa dos dados a serem

processados.

O mesmo efeito que o da presente invenção também pode ser obtido, por exemplo, pelo método a seguir.

É fornecido um método de processamento de informações executado em um aparelho de processamento de informações, inclusive meios de gravação e meios de processamento, para o processamento de dados criptografados, que consiste em uma unidade de uma série de partes dos dados criptografados divisionais gerados pela criptografia de uma série de partes dos dados de textos simples divisionais utilizando uma série de chaves geradas pela divisão dos dados de textos simples a serem processados nos dados que são compostos por um número predeterminadode bits, pelo menos uma das chaves diferindo da(s) outra(s); os dados criptografados são novamente descriptografados nos dados a serem processados pela descriptografia dos dados criptografados divisionais em uma ordem predeterminada para conectar os dados descriptografados em uma unidade, cada um dos dados criptografados divisionais, exceto o último dado a ser descriptografado, contendo informações de especificação para a especificação de uma chave para a descriptografia do próximo dado criptografado divisional a ser descriptografado para permitir a descriptografia, os dados criptografados contendo a primeira informação de especificação para a especificação da chave para a descriptografia do dado criptografado divisional que é o primeiro a ser descriptografado e as informações de especificação do cronograma para especificar o cronograma a fim de evitar que os dados criptografados sejam descriptografados.

O método inclui as etapas, executadas pelos meios de processamento, de: gravação dos dados criptografados nos meios de gravação; leitura das informações de especificação do cronograma dos dados criptografados; detecção da primeira informação de especificação contida nos dados criptografados ou do primeiro dado criptografado divisional que é o primeiro a ser descriptografado em todos os dados criptografados divisionais dos dados criptografados; e monitorar

se o cronograma especificado pelas informações de especificação do cronograma lidas na etapa de leitura chegou, causando uma alteração irreversível na primeira informação de especificação ou no primeiro dado criptografado divisional detectado na etapa de detecção no caso de o cronograma ter chegado.

O mesmo efeito que o da invenção descrita acima também pode ser obtido, por exemplo, pelo programa computadorizado a seguir. Utilizando o programa computadorizado a seguir, o mesmo efeito que o da invenção descrita acima pode ser obtido com um computador comum.

É fornecido um programa computadorizado para o processamento de dados criptografados que consiste em uma unidade de uma série de partes dos dados criptografados divisionais gerados pela criptografia de uma série de partes dos dados de textos simples divisionais utilizando uma série de chaves geradas pela divisão dos dados de textos simples a serem processados nos dados que são compostos por um número predeterminadode bits, pelo menos uma das chaves diferindo da(s) outra(s); os dados criptografados são novamente descriptografados nos dados a serem processados pela descriptografia dos dados criptografados divisionais em uma ordem predeterminada para conectar os dados descriptografados em uma unidade, cada um dos dados criptografados divisionais, exceto o último a ser descriptografado, contendo informações de especificação para a especificação de uma chave para a descriptografia do próximo dado criptografado divisional a ser descriptografado para permitir a descriptografia, os dados criptografados contendo a primeira informação de especificação para a especificação da chave para a descriptografia do dado criptografado divisional que é o primeiro a ser descriptografado e as informações de especificação do cronograma para especificar o cronograma a fim de evitar que os dados criptografados sejam descriptografados, o programa computadorizado tem como objetivo fazer com que um computador contido em um aparelho de processamento de informações, incluindo o computador conectado aos meios de gravação, execute as etapas a seguir.

As etapas são: gravação dos dados criptografados nos meios de gravação; leitura das informações de especificação do cronograma dos dados criptografados; detecção da primeira informação de especificação contida nos dados criptografados ou do primeiro dado criptografado divisional que é o primeiro a ser descriptografado em todos os dados criptografados divisionais dos dados criptografados; e monitorar se o cronograma especificado pelas informações de especificação do cronograma lidas na etapa de leitura chegou ou não, causando uma alteração irreversível na primeira informação de especificação ou no primeiro dado criptografado divisional detectado na etapa de detecção no caso de o cronograma ter chegado.

A terceira invenção é um aparelho de processamento de informações para o processamento de dados criptografados que consiste em uma unidade de uma série de partes dos dados criptografados divisionais gerados pela criptografia de uma série de partes dos dados de textos simples divisionais utilizando uma série de chaves geradas pela divisão dos dados de textos simples a serem processados nos dados que são compostos por um número predeterminadode bits, pelo menos uma das chaves diferindo da(s) outra(s); os dados criptografados são novamente descriptografados nos dados a serem processados pela descriptografia dos dados criptografados divisionais em uma ordem predeterminada para conectar os dados descriptografados em uma unidade, cada um dos dados criptografados divisionais, exceto o último a ser descriptografado, contendo informações de especificação para a especificação de uma chave para a descriptografia do próximo dado criptografado divisional a ser descriptografado para permitir a descriptografia, os dados criptografados contendo informações de especificação do cronograma para especificar o cronograma a fim de evitar que os dados criptografados sejam descriptografados.

Além disso, o aparelho de processamento de informações inclui: meios de gravação para a gravação dos dados criptografados; meios de descriptografia capazes de descriptografar os dados criptografados; meios de entrada do

disparador de descriptografia para a entrada de informações do disparador de descriptografia para o início da descriptografia dos dados criptografados; meios de leitura das informações de especificação do cronograma para a leitura das informações de especificação do cronograma dos dados criptografados quando as informações do disparador de descriptografia forem inseridas nos meios de entrada do disparador de descriptografia; meios de detecção para a detecção do primeiro dado criptografado divisional que é o primeiro a ser descriptografado em todos os dados criptografados divisionais dos dados criptografados; e meios de processamento para a recepção das informações de especificação do cronograma lidas pelos meios de leitura das informações de especificação do cronograma na entrada das informações do disparador de descriptografia para determinar se o cronograma especificado pelas informações de especificação do cronograma chegou e permitir que os meios de descriptografia descriptografem os dados criptografados se o cronograma ainda não chegou, causando uma alteração irreversível no primeiro dado criptografado divisional detectado pelos meios de detecção no caso de o cronograma ter chegado.

Os dados criptografados utilizados no aparelho de processamento de informações são os mesmos que na segunda invenção e contêm as informações de especificação do cronograma para especificar o cronograma a fim de evitar que os dados criptografados sejam descriptografados. Como na segunda invenção, o aparelho de processamento de informações controla o cronograma de causar uma alteração irreversível no primeiro dado criptografado divisional pelas informações de especificação do cronograma. Em contraste com a primeira e a segunda invenções, nas quais a descriptografia dos dados criptografados não é necessariamente possível, o aparelho de processamento de informações, de acordo com a terceira invenção, pode descriptografar os dados criptografados. Nessa base, quando as informações do disparador de descriptografia para solicitação da descriptografia dos dados criptografados são inseridas, o aparelho de processamento de informações, de acordo com a terceira invenção, recebe as

informações de especificação do cronograma lidas pelos meios de leitura das informações de especificação do cronograma para determinar se o cronograma especificado pelas informações de especificação do cronograma chegou e permite que os meios de descriptografia descriptografem os dados criptografados se o cronograma ainda não chegou, causando uma alteração irreversível no primeiro dado criptografados divisional detectado pelos meios de detecção no caso de o cronograma ter chegado. Como descrito acima, quando um usuário executar uma operação de descriptografia, o aparelho de processamento de informações, de acordo com a terceira invenção, descriptografa os dados criptografados que devem ser descriptografados pelo usuário ou transforma os dados criptografados em uma espécie de dados "inúteis". Isto também é eficaz ao evitar que os dados a serem processados sejam perdidos devido à perda de dados criptografados.

O mesmo efeito que o da presente invenção também pode ser obtido, por exemplo, pelo método a seguir.

É fornecido um método de processamento de informações executado em um aparelho de processamento de informações, inclusive meios de gravação, meios de entrada do disparador de descriptografia e meios de processamento, para o processamento de dados criptografados, que consiste em uma unidade de uma série de partes dos dados criptografados divisionais gerados pela criptografia de uma série de partes dos dados de textos simples divisionais utilizando uma série de chaves geradas pela divisão dos dados de textos simples a serem processados nos dados que são compostos por um número predeterminadode bits, pelo menos uma das chaves diferindo da(s) outra(s); os dados criptografados são novamente descriptografados nos dados a serem processados pela descriptografia dos dados criptografados divisionais em uma ordem predeterminada para conectar os dados descriptografados em uma unidade, cada um dos dados criptografados divisionais, exceto o último dado a ser descriptografado, contendo informações de especificação para a especificação de

uma chave para a descriptografia do próximo dado criptografado divisional a ser descriptografado para permitir a descriptografia, os dados criptografados contendo informações de especificação do cronograma para especificar o cronograma a fim de evitar que os dados criptografados sejam descriptografados.

O método inclui as etapas, executadas pelos meios de processamento, de: gravação dos dados criptografados nos meios de gravação; recepção de informações do disparador de descriptografia para o início da descriptografia dos dados criptografados dos meios de entrada do disparador de descriptografia; leitura das informações de especificação do cronograma dos dados criptografados quando a etapa de recepção ocorrer; detecção do primeiro dado criptografado divisional que é o primeiro a ser descriptografado em todos os dados criptografados divisionais dos dados criptografados; e recepção das informações de especificação do cronograma lidas na etapa de leitura quando a etapa de recepção ocorrer para determinar se o cronograma especificado pelas informações de especificação do cronograma chegou e descriptografar os dados criptografados se o cronograma ainda não chegou, causando uma alteração irreversível no primeiro dado criptografado divisional detectado na etapa de detecção no caso de o cronograma ter chegado.

O mesmo efeito que o da invenção descrita acima também pode ser obtido, por exemplo, pelo programa computadorizado a seguir. Utilizando o programa computadorizado a seguir, o mesmo efeito que o da invenção descrita acima pode ser obtido com um computador comum.

É fornecido um programa computadorizado para o processamento de dados criptografados que consiste em uma unidade de uma série de partes dos dados criptografados divisionais gerados pela criptografia de uma série de partes dos dados de textos simples divisionais utilizando uma série de chaves geradas pela divisão dos dados de textos simples a serem processados nos dados que são compostos por um número predeterminadode bits, pelo menos uma das chaves diferindo da(s) outra(s); os dados criptografados são novamente

descriptografados nos dados a serem processados pela descriptografia dos dados criptografados divisionais em uma ordem predeterminada para conectar os dados descriptografados em uma unidade, cada um dos dados criptografados divisionais, exceto o último a ser descriptografado, contendo informações de especificação para a especificação de uma chave para a descriptografia do próximo dado criptografado divisional a ser descriptografado para permitir a descriptografia, os dados criptografados contendo informações de especificação do cronograma para especificar o cronograma a fim de evitar que os dados criptografados sejam descriptografados, o programa computadorizado tem como objetivo fazer com que um computador contido em um aparelho de processamento de informações, incluindo meios de gravação, meios de entrada do disparador de descriptografia e o computador também conectado, execute as etapas a seguir.

As etapas são: gravação dos dados criptografados nos meios de gravação; recepção de informações do disparador de descriptografia para o início da descriptografia dos dados criptografados dos meios de entrada do disparador de descriptografia; leitura das informações de especificação do cronograma dos dados criptografados quando a etapa de recepção ocorrer; detecção do primeiro dado criptografado divisional que é o primeiro a ser descriptografado em todos os dados criptografados divisionais dos dados criptografados; e recepção das informações de especificação do cronograma lidas na etapa de leitura quando a etapa de recepção ocorrer para determinar se o cronograma especificado pelas informações de especificação do cronograma chegou e descriptografar os dados criptografados se o cronograma ainda não chegou, causando uma alteração irreversível no primeiro dado criptografado divisional detectado na etapa de detecção no caso de o cronograma ter chegado.

Como descrito acima, nos dados criptografados utilizados no aparelho de processamento de informações, de acordo com a terceira invenção, cada um dos dados criptografados divisionais, exceto o último a ser descriptografado, contém as informações de especificação para a especificação da chave para a

descriptografia do próximo dado criptografado divisional a ser descriptografado. Assim, os dados criptografados utilizados no aparelho de processamento de informações, de acordo com a terceira invenção, podem conter primeiro as informações de especificação para a especificação da chave para a descriptografia do dado criptografado divisional que é o primeiro a ser descriptografado.

Quando a primeira informação de especificação estiver incorporada nos dados criptografados, a terceira invenção pode ser constituída da seguinte maneira.

A terceira invenção, neste caso, é um aparelho de processamento de informações para o processamento de dados criptografados que consiste em uma unidade de uma série de partes dos dados criptografados divisionais gerados pela criptografia de uma série de partes dos dados de textos simples divisionais utilizando uma série de chaves geradas pela divisão dos dados de textos simples a serem processados nos dados que são compostos por um número predeterminadode bits, pelo menos uma das chaves diferindo da(s) outra(s); os dados criptografados são novamente descriptografados nos dados a serem processados pela descriptografia dos dados criptografados divisionais em uma ordem predeterminada para conectar os dados descriptografados em uma unidade, cada um dos dados criptografados divisionais, exceto o último a ser descriptografado, contendo informações de especificação para a especificação de uma chave para a descriptografia do próximo dado criptografado divisional a ser descriptografado para permitir a descriptografia, os dados criptografados contendo a primeira informação de especificação para a especificação da chave para a descriptografia do dado criptografado divisional que é o primeiro a ser descriptografado e as informações de especificação do cronograma para especificar o cronograma a fim de evitar que os dados criptografados sejam descriptografados.

Além disso, o aparelho de processamento de informações inclui: meios de

gravação para a gravação dos dados criptografados; meios de descriptografia capazes de descriptografar os dados criptografados; meios de entrada do disparador de descriptografia para a entrada de informações do disparador de descriptografia para o início da descriptografia dos dados criptografados; meios de leitura das informações de especificação do cronograma para a leitura das informações de especificação do cronograma dos dados criptografados quando as informações do disparador de descriptografia forem inseridas dos meios de entrada do disparador de descriptografia; meios de detecção para a detecção da primeira informação de especificação contida nos dados criptografados ou do primeiro dado criptografado divisional que é o primeiro a ser descriptografado em todos os dados criptografados divisionais; e meios de processamento para a recepção das informações de especificação do cronograma lidas pelos meios de leitura das informações de especificação do cronograma na entrada das informações do disparador de descriptografia para determinar se o cronograma especificado pelas informações de especificação do cronograma chegou ou não e permitir que os meios de descriptografia descriptografem os dados criptografados se o cronograma ainda não chegou, e causando uma alteração irreversível na primeira informação de especificação ou no primeiro dado criptografado divisional detectado pelos meios de detecção no caso de o cronograma ter chegado.

Especificamente, o aparelho de processamento de informações faz com que uma alteração irreversível no dado criptografado divisional que deve ser o primeiro a ser descriptografado ou na primeira informação de especificação utilizada para a descriptografia do dado criptografado divisional que deve ser o primeiro a ser descriptografado em todos os dados criptografados divisionais ocorra. Com a execução de tal processamento, os dados criptografados não podem mais ser descriptografados. Os dados criptografados que não podem mais ser descriptografados, como descrito acima, podem ser mencionados como dados "inúteis". A prevenção da descriptografia dos dados criptografados desta maneira produz o mesmo efeito que o da exclusão completa dos dados a serem

processados.

O mesmo efeito que o da presente invenção também pode ser obtido, por exemplo, pelo método a seguir.

É fornecido um método de processamento de informações executado em um aparelho de processamento de informações, inclusive meios de gravação, meios de entrada do disparador de descriptografia e meios de processamento, para o processamento de dados criptografados, que consiste em uma unidade de uma série de partes dos dados criptografados divisionais gerados pela criptografia de uma série de partes dos dados de textos simples divisionais utilizando uma série de chaves geradas pela divisão dos dados de textos simples a serem processados nos dados que são compostos por um número predeterminadode bits, pelo menos uma das chaves diferindo da(s) outra(s); os dados criptografados são novamente descriptografados nos dados a serem processados pela descriptografia dos dados criptografados divisionais em uma ordem predeterminada para conectar os dados descriptografados em uma unidade, cada um dos dados criptografados divisionais, exceto o último dado a ser descriptografado, contendo informações de especificação para a especificação de uma chave para a descriptografia do próximo dado criptografado divisional a ser descriptografado para permitir a descriptografia, os dados criptografados contendo a primeira informação de especificação para a especificação da chave para a descriptografia do dado criptografado divisional que é o primeiro a ser descriptografado e as informações de especificação do cronograma para especificar o cronograma a fim de evitar que os dados criptografados sejam descriptografados.

O método inclui as etapas, executadas pelos meios de processamento, de: gravação dos dados criptografados nos meios de gravação; recepção de informações do disparador de descriptografia para o início da descriptografia dos dados criptografados dos meios de entrada do disparador de descriptografia; leitura das informações de especificação do cronograma dos dados criptografados

quando a etapa de recepção ocorrer; detecção da primeira informação de especificação contida nos dados criptografados ou do primeiro dado criptografado divisional que é o primeiro a ser descriptografado em todos os dados criptografados divisionais dos dados criptografados; e recepção das informações de especificação do cronograma lidas na etapa de leitura quando a etapa de recepção ocorrer para determinar se o cronograma especificado pelas informações de especificação do cronograma chegou e descriptografar os dados criptografados se o cronograma ainda não chegou, causando uma alteração irreversível na primeira informação de especificação ou no primeiro dado criptografado divisional detectado na etapa de detecção no caso de o cronograma ter chegado.

O mesmo efeito que o da invenção descrita acima também pode ser obtido, por exemplo, pelo programa computadorizado a seguir. Utilizando o programa computadorizado a seguir, o mesmo efeito que o da invenção descrita acima pode ser obtido com um computador comum.

É fornecido um programa computadorizado para o processamento de dados criptografados que consiste em uma unidade de uma série de partes dos dados criptografados divisionais gerados pela criptografia de uma série de partes dos dados de textos simples divisionais utilizando uma série de chaves geradas pela divisão dos dados de textos simples a serem processados nos dados que são compostos por um número predeterminadode bits, pelo menos uma das chaves diferindo da(s) outra(s); os dados criptografados são novamente descriptografados nos dados a serem processados pela descriptografia dos dados criptografados divisionais em uma ordem predeterminada para conectar os dados descriptografados em uma unidade, cada um dos dados criptografados divisionais, exceto o último a ser descriptografado, contendo informações de especificação para a especificação de uma chave para a descriptografia do próximo dado criptografado divisional a ser descriptografado para permitir a descriptografia, os dados criptografados contendo a primeira informação de especificação para a

especificação da chave para a descriptografia do dado criptografado divisional que é o primeiro a ser descriptografado e as informações de especificação do cronograma para especificar o cronograma a fim de evitar que os dados criptografados sejam descriptografados, o programa computadorizado tendo como objetivo fazer com que um computador contido em um aparelho de processamento de informações, incluindo meios de gravação, meios de entrada do disparador de descriptografia e o computador também conectado, execute as etapas a seguir.

As etapas são: gravação dos dados criptografados nos meios de gravação; recepção de informações do disparador de descriptografia para o início da descriptografia dos dados criptografados dos meios de entrada do disparador de descriptografia; leitura das informações de especificação do cronograma dos dados criptografados quando a etapa de recepção ocorrer; detecção da primeira informação de especificação contida nos dados criptografados ou do primeiro dado criptografado divisional que é o primeiro a ser descriptografado em todos os dados criptografados divisionais dos dados criptografados; e recepção das informações de especificação do cronograma lidas na etapa de leitura quando a etapa de recepção ocorrer para determinar se o cronograma especificado pelas informações de especificação do cronograma chegou e descriptografar os dados criptografados se o cronograma ainda não chegou, causando uma alteração irreversível na primeira informação de especificação ou no primeiro dado criptografado divisional detectado na etapa de detecção no caso de o cronograma ter chegado.

Os dados a seguir são comuns para a invenção básica e para a primeira à terceira invenções.

Os meios de processamento nas invenções da presente aplicação causam uma alteração irreversível no primeiro dado criptografado divisional (na primeira informação de especificação ou no primeiro dado criptografado divisional em alguns casos). A alteração irreversível pode ser causada, por exemplo, pela

escrita dos dados apropriados sobre o primeiro dado criptografado divisional (a primeira informação de especificação ou o primeiro dado criptografado divisional em alguns casos) ou pela conversão irreversível do primeiro dado criptografado divisional (a primeira informação de especificação ou o primeiro dado criptografado divisional em alguns casos). Para a conversão irreversível, por exemplo, após a execução de um processamento de corte de uma parte dos números decimais ou dos primeiros dígitos do resultado de um cálculo apropriado executado em uma seqüência de dados do primeiro dado criptografado divisional (a primeira informação de especificação ou o primeiro dado criptografado divisional em alguns casos), o primeiro dado criptografado divisional (a primeira informação de especificação ou o primeiro dado criptografado divisional em alguns casos) pode ser substituído pelo resultado do cálculo processado. Por outro lado, o primeiro dado criptografado divisional (a primeira informação de especificação ou o primeiro dado criptografado divisional em alguns casos) pode ficar sujeito a uma conversão JPEG.

BREVE DESCRIÇÃO DAS FIGURAS

A Figura 1 é uma ilustração da configuração completa de um sistema de criptografia conforme a primeira abordagem.

A Figura 2 é uma configuração de hardware de um aparelho de processamento de criptografia contido no sistema de criptografia ilustrado na Figura 1.

A Figura 3 é um diagrama de blocos ilustrando uma configuração de um dispositivo de criptografia contido no aparelho de processamento de criptografia ilustrado na Figura 2.

As Figuras 4 são diagramas ilustrando a estrutura de dados dos dados criptografados gerados no aparelho de processamento de criptografia ilustrado na Figura 2.

A Figura 5 é um diagrama ilustrando uma configuração de hardware de um aparelho de processamento de descriptografia contido no sistema de

criptografia ilustrado na Figura 1.

A Figura 6 é um diagrama de blocos ilustrando uma configuração de um dispositivo de descriptografia contido no aparelho de processamento de descriptografia ilustrado na Figura 5.

A Figura 7 é um diagrama de blocos funcionais ilustrando os blocos funcionais gerados no aparelho de processamento de descriptografia ilustrado na Figura 1.

A Figura 8 é um fluxograma ilustrando um fluxo de um processamento de criptografia executado no sistema de criptografia ilustrado na Figura 1.

A Figura 9 é um fluxograma ilustrando um fluxo de um processamento de descriptografia executado no sistema de criptografia ilustrado na Figura 1.

A Figura 10 é um diagrama de blocos ilustrando uma configuração de um dispositivo de criptografia contido em um aparelho de processamento de criptografia em uma variação.

A Figura 11 é um diagrama de blocos ilustrando uma configuração de um dispositivo de descriptografia contido em um aparelho de processamento de descriptografia na variação.

DESCRIÇÃO DETALHADA DA INVENÇÃO

Daqui em diante, uma abordagem preferida da presente invenção e uma variação dela serão descritas.

Na descrição da abordagem e da variação, o mesmo objeto é indicado pelo mesmo número de referência. Dependendo do caso, a descrição sobreposta é omitida.

Nesta abordagem, um sistema de criptografia contendo um aparelho de processamento de criptografia 1 e uma série de aparelhos de processamento de descriptografia 2, como ilustrado na Figura 1, é descrito como uma abordagem da presente invenção. O aparelho de processamento de descriptografia 2 corresponde a um aparelho de processamento de informações da presente invenção.

O aparelho de processamento de criptografia 1 e os aparelhos de processamento de descriptografia 2 são conectados entre si através de uma rede N como em uma rede local (LAN) ou semelhante para habilitar a transmissão de dados criptografados gerados pelo aparelho de processamento de criptografia 1 na maneira descrita a seguir para cada um dos aparelhos de processamento de descriptografia 2.

É certo que o aparelho de processamento de criptografia 1 e os aparelhos de processamento de descriptografia 2 não são necessariamente conectados entre si através da rede N. Entretanto, quando o aparelho de processamento de criptografia 1 e os aparelhos de processamento de descriptografia 2 não estiverem conectados entre si, é necessário que cada um dos aparelhos de processamento de descriptografia 2 seja capaz de receber os dados criptografados gerados pelo aparelho de processamento de criptografia 1 através, por exemplo, de um meio de gravação como um CD-ROM do aparelho de processamento de criptografia 1. A descrição de um escritor de dados para a gravação dos dados criptografados no meio de gravação ou de um leitor de dados para a leitura dos dados criptografados do meio de gravação, que são necessários para a recepção dos dados criptografados, é omitida porque geralmente são técnicas empregadas.

Pelo menos um aparelho de processamento de descriptografia 2 é suficiente. Em alguns casos, o aparelho de processamento de criptografia 1 também serve como o aparelho de processamento de descriptografia 2.

As configurações do aparelho de processamento de criptografia 1 e do aparelho de processamento de descriptografia 2 serão descritas. Em primeiro lugar, será descrita a configuração do aparelho de processamento de criptografia 1.

A Figura 2 ilustra uma configuração de hardware do aparelho de processamento de criptografia 1.

Nesta abordagem, o aparelho de processamento de criptografia 1 contém

uma unidade central de processamento (CPU) 21, uma memória somente de leitura (ROM) 22, uma unidade de disco rígido (HDD) 23, uma memória de acesso aleatório (RAM) 24, um dispositivo de entrada 25, um dispositivo de display 26, um dispositivo de criptografia 27, um dispositivo de comunicação 28 e um barramento 29. A CPU 21, a ROM 22, a HDD 23, a RAM 24, o dispositivo de entrada 25, o dispositivo de display 26, o dispositivo de criptografia 27 e o dispositivo de comunicação 28 podem trocar dados através do barramento 29.

Um programa predeterminado e os dados predeterminados (contendo dados a serem processados em alguns casos incluindo esta abordagem, e também contendo os dados necessários para a execução do programa) são gravados na ROM 22 ou na HDD 23. A CPU 21 controla todo o aparelho de processamento de criptografia 1 e executa um processamento descrito a seguir com base no programa ou nos dados gravados na ROM 22 ou na HDD 23. A RAM 24 é utilizada como uma área de memória de trabalho para a execução do processamento na CPU 21.

O dispositivo de entrada 25 contém um teclado e um mouse ou similar e é utilizado para comandos ou entrada de dados. O dispositivo de display 26 contém um display de cristal líquido (LCD) e um tubo de raios catódicos (CRT) ou similar e é utilizado para exibir o comando, os dados de entrada ou um estado do processamento descrito a seguir.

O dispositivo de criptografia 27 criptografa os dados a serem processados, como descrito a seguir.

O dispositivo de comunicação 28 executa a comunicação com os aparelhos de processamento de descriptografia 2 através da rede N. O dispositivo de comunicação 28 transmite os dados criptografados para um destino designado por um endereço MAC ou similar contido em um cabeçalho dos dados criptografados descrito a seguir.

A configuração do dispositivo de criptografia 27 será descrita a seguir. A Figura 3 é um diagrama de configuração de blocos do dispositivo de criptografia

27.

O dispositivo de criptografia 27 contém uma unidade de interface 271, uma unidade de pré-processamento 272, uma unidade de criptografia 273, uma unidade de geração de soluções 274, uma unidade de geração de algoritmos 275, uma unidade de geração de chaves 276, uma unidade de geração de informações de especificação 277, uma unidade de geração de informações de especificação do cronograma 278, uma unidade de geração de cabeçalhos 279 e uma unidade de conexão 280.

A unidade de interface 271 recebe e transmite dados entre o barramento 29 e o dispositivo de comunicação 28.

A unidade de interface 271 recebe os dados a serem processados da HDD 23 através do barramento 29 e transmite os dados recebidos a serem processados para a unidade de pré-processamento 272. Na recepção dos dados a serem processados, a unidade de interface 271 transmite os dados indicando a recepção dos dados a serem processados para a unidade de geração de soluções 274. A unidade de interface 271 também recebe uma entrada do dispositivo de entrada 25 para transmitir a entrada recebida para a unidade de geração de informações de especificação do cronograma 278.

Por outro lado, a unidade de interface 271 recebe os dados criptografados da unidade de conexão 280, como descrito a seguir, para transmitir os dados criptografados recebidos para o barramento 29. Os dados criptografados são transmitidos para o aparelho de processamento de descriptografia 2 através da rede N por meio do dispositivo de comunicação 28.

A unidade de pré-processamento 272 tem uma função de dividir os dados a serem processados, que são recebidos do barramento 29, através da unidade de interface 271, nos dados de textos simples divisionais, cada um sendo composto por um número predeterminadode bits e, depois, de transmitir os dados de textos simples divisionais obtidos para a unidade de criptografia 273. Como dividir os dados a serem processados será descrito a seguir. A unidade de

criptografia 273 criptografa os dados de textos simples divisionais na ordem das posições mais próximas do cabeçalho nos dados a serem processados nos dados criptografados divisionais. O primeiro dado criptografado divisional gerado corresponde ao primeiro dado criptografado divisional nesta especificação.

A unidade de criptografia 273 tem uma função de receber os dados de textos simples divisionais da unidade de pré-processamento 272 e de criptografar os dados de textos simples divisionais recebidos. A unidade de criptografia 273 tem uma outra função de receber informações de especificação descritas a seguir da unidade de geração de informações de especificação 277 para misturar as informações de especificação nos dados de textos simples divisionais antes da criptografia.

Os detalhes de um processamento de criptografia serão descritos a seguir.

A unidade de geração de soluções 274 gera soluções em seqüência. As soluções geradas pela unidade de geração de soluções 274 do aparelho de processamento de criptografia 1, que são geradas na mesma ordem, se tornam sempre as mesmas. Um dispositivo de descriptografia no aparelho de processamento de descriptografia 2 descrito a seguir também contém uma unidade de geração de soluções, que é a mesma que a unidade de geração de soluções 274 contida no aparelho de processamento de criptografia 1. Especificamente, pela comparação entre as soluções geradas na mesma ordem, a solução gerada pela unidade de geração de soluções 274 contida no aparelho de processamento de criptografia 1 e a gerada pela unidade de geração de soluções contida no aparelho de processamento de descriptografia 2 se tornam idênticas entre si. A solução nesta abordagem é um número pseudo-aleatório. A solução gerada é transmitida para a unidade de geração de algoritmos 275, para a unidade de geração de chaves 276 e para a unidade de geração de informações de especificação 277.

A unidade de geração de algoritmos 275 gera um algoritmo com base na

solução recebida da unidade de geração de soluções 274. O algoritmo é utilizado para executar o processamento de criptografia na unidade de criptografia 273.

A unidade de geração de chaves 276 gera uma chave com base na solução recebida da unidade de geração de soluções 274. A chave é utilizada para executar o processamento de criptografia na unidade de criptografia 273.

A unidade de geração de informações de especificação 277 gera informações de especificação com base nos dados recebidos, por exemplo, do dispositivo de entrada 25 operado por um usuário através da unidade de interface 271.

A unidade de geração de informações de especificação 277 gera as informações de especificação como informações indicando a ordem de geração da solução transmitida da unidade de geração de soluções 274. As informações de especificação geradas pela unidade de geração de informações de especificação 277 são utilizadas para a descriptografia de cada um dos dados criptografados divisionais descritos acima no aparelho de processamento de descriptografia 2. As informações de especificação especificam diretamente uma solução utilizada para a descriptografia de cada um dos dados criptografados divisionais e especificam indiretamente uma chave utilizada para a descriptografia de cada um dos dados criptografados divisionais.

As informações de especificação nesta abordagem são várias. É necessário que pelo menos uma das séries de informações de especificação seja diferente das outras informações de especificação. Nesta abordagem, as informações de especificação diferem entre si. Tendo em vista isso, cada parte das informações de especificação está associada a um dado criptografado divisional e especifica, indiretamente, uma chave utilizada para a descriptografia dos dados criptografados divisionais.

A unidade de geração de informações de especificação 277 transmite as informações de especificação para a unidade de criptografia 273.

Fundamentalmente, nesta abordagem, as informações de especificação indicam a ordem de geração da solução no aparelho de processamento de criptografia 1. A unidade de geração de informações de especificação 277 transmite as informações de especificação utilizadas para a descriptografia do dado criptografado divisional que é o primeiro a ser descriptografado (correspondente à primeira informação de especificação nesta especificação; nesta abordagem, a informação indicando a ordem de geração da primeira solução gerada para a criptografia dos dados criptografados no aparelho de processamento de criptografia 1 corresponde à primeira informação de especificação) não para unidade de criptografia 273, mas, excepcionalmente, para a unidade de geração de cabeçalhos 279.

A unidade de geração de informações de especificação do cronograma 278 gera informações de especificação do cronograma com base nos dados recebidos através da unidade de interface 271, por exemplo, do dispositivo de entrada 25 operado pelo usuário.

As informações de especificação do cronograma geradas pela unidade de geração de informações de especificação do cronograma 278 especificam o cronograma para evitar que os dados criptografados contendo as informações de especificação do cronograma sejam descriptografados. Para as informações de especificação do cronograma, uma designação simples de data e hora, por exemplo X (mês), X (dia), 200X (ano) ou X (hora), X (minuto), X (mês), X (dia), 200X (ano), é suficiente. As informações de especificação do cronograma podem ter o conteúdo para permitir ou inibir a descriptografia, como a inibição da descriptografia dos dados criptografados contendo as informações de especificação do cronograma após a data e a hora predeterminadas ou a permissão da descriptografia dos dados criptografados contendo as informações de especificação do cronograma antes da data e da hora predeterminadas.

A unidade de geração de informações de especificação do cronograma 278 transmite as informações de especificação do cronograma geradas para a

unidade de geração de cabeçalhos 279.

A unidade de geração de cabeçalhos 279 gera dados de cabeçalho que servem como cabeçalho dos dados criptografados com base nos dados recebidos através da unidade de interface 271, por exemplo, do dispositivo de entrada operado pelo usuário.

Os dados de cabeçalho contêm um endereço do aparelho de processamento de criptografia 1 correspondente a uma fonte de transmissão dos dados criptografados e um endereço do aparelho de processamento de descriptografia 2 correspondente a um destino dos dados criptografados. A unidade de geração de dados de cabeçalho 279 permite que os dados de cabeçalho contenham tanto a primeira informação de especificação recebida da unidade de geração de informações de especificação 277 como as informações de especificação do cronograma recebidas da unidade de geração de informações de especificação do cronograma 278.

A unidade de geração de cabeçalhos 279 transmite os dados de cabeçalho gerados para a unidade de conexão 280.

A unidade de conexão 280 tem uma função de conectar os dados criptografados divisionais gerados pela criptografia dos dados de textos simples divisionais na unidade de criptografia 273 para obter uma unidade de dados criptografados. A unidade de conexão 280 nesta abordagem conecta os dados de cabeçalho gerados pela unidade de geração de cabeçalhos 279, além dos dados criptografados divisionais recebidos da unidade de criptografia 273 para obter uma unidade de dados criptografados.

Uma estrutura de dados dos dados criptografados está exemplificada na Figura 4(A). Apesar de uma quantidade real dos dados criptografados divisionais 502 serem muito maior do que a ilustrada, a quantidade dos dados criptografados divisionais 502 ilustrados é pequena nas Figuras 4(A) e 4(B) por conveniência de ilustração.

Os dados criptografados contêm os dados de cabeçalho 501 descritos

acima em seu cabeçalho (uma extremidade esquerda nas Figuras 4(A) e 4(B) corresponde ao cabeçalho dos dados criptografados), como ilustrado na Figura 4(A). Os múltiplos dados criptografados divisionais 502 seguem os dados de cabeçalho 501. Os dados criptografados divisionais 502, que são descriptografados previamente na descriptografia dos dados criptografados, estão situados mais próximos do cabeçalho nos dados criptografados. Em outras palavras, para a descriptografia dos dados criptografados, os dados criptografados divisionais 502 são descriptografados na ordem de disposição dos dados criptografados divisionais 502 do primeiro dado criptografado divisional 502 para o último dado criptografado divisional 502.

Os dados criptografados gerados na unidade de conexão 280 são transmitidos para a unidade de interface 271 e, depois, para o dispositivo de comunicação 28 através do barramento 29 e são, posteriormente, transmitidos para o aparelho de processamento de descriptografia 2 através da rede N.

A seguir, será descrita a configuração do aparelho de processamento de descriptografia 2.

Na Figura 5, está ilustrada uma configuração de hardware do aparelho de processamento de descriptografia 2.

O aparelho de processamento de descriptografia 2 contém uma CPU 31, uma ROM 32, uma HDD 33, uma RAM 34, um dispositivo de entrada 35, um dispositivo de display 36, um dispositivo de descriptografia 37, um dispositivo de comunicação 38 e um barramento 39. A CPU 31, a ROM 32, a HDD 33, a RAM 34, o dispositivo de entrada 35, o dispositivo de display 36 e o barramento 39 no aparelho de processamento de descriptografia 2 estão configurados, respectivamente, para serem os mesmos que a CPU 21, a ROM 22, a HDD 23, a RAM 24, o dispositivo de entrada 25, o dispositivo de display 26 e o barramento 29 no aparelho de processamento de criptografia 1 e terem as mesmas funções. A HDD 33 no aparelho de processamento de descriptografia 2 armazena um endereço MAC do aparelho de processamento de descriptografia 2.

Note que o dispositivo de comunicação 38 no aparelho de processamento de descriptografia 2 pode receber os dados criptografados transmitidos do aparelho de processamento de criptografia 1 através da rede N.

O dispositivo de descriptografia 37 descriptografa os dados criptografados recebidos do aparelho de processamento de criptografia 1 e é configurado como ilustrado na Figura 6.

O dispositivo de descriptografia 37 contém uma unidade de interface 371, uma unidade de pré-processamento 372, uma unidade de descriptografia 373, uma unidade de geração de soluções 374, uma unidade de geração de algoritmos 375, uma unidade de geração de chaves 376, uma unidade de análise de informações de especificação 377 e uma unidade de conexão 379.

A unidade de interface 371 recebe os dados criptografados do dispositivo de comunicação 38 através do barramento 39 e transmite os dados criptografados recebidos para a unidade de pré-processamento 372.

Por outro lado, a unidade de interface 371 recebe os dados a serem processados da unidade de conexão 379, como descrito a seguir, para transmitir os dados recebidos a serem processados para o barramento 39.

Ao receber os dados criptografados do barramento 39 através da unidade de interface 371, a unidade de pré-processamento 372 executa o processamento a seguir.

A unidade de pré-processamento 372, que recebeu os dados criptografados, primeiro extrai os dados de cabeçalho dos dados criptografados recebidos e também extrai a primeira informação de especificação contida nos dados de cabeçalho a partir deste ponto para transmitir a primeira informação de especificação para a unidade de análise de informações de especificação 377.

A unidade de pré-processamento 372 também executa um processamento de divisão dos dados criptografados para obter os dados criptografados divisionais. A divisão se torna possível, por exemplo, através do acordo entre o aparelho de processamento de criptografia 1 e a série de

aparelhos de processamento de descriptografia 2 de mesmo tamanho dos dados criptografados divisionais ou com a escrita de um método de divisão dos dados criptografados para obter os dados criptografados divisionais nos dados de cabeçalho contidos nos dados criptografados para dividir, assim, os dados criptografados de acordo com as informações escritas na unidade de pré-processamento 372. Os dados criptografados são divididos seqüencialmente a partir do lado do cabeçalho para obter os dados criptografados divisionais.

A unidade de pré-processamento 372 transmite os dados criptografados divisionais obtidos pela divisão dos dados criptografados para a unidade de descriptografia 373.

A unidade de descriptografia 373 tem a função de descriptografar os dados criptografados divisionais recebidos da unidade de pré-processamento 372. Os detalhes da descriptografia serão descritos a seguir.

Cada dado criptografado divisional, exceto o último, contém as informações de especificação (mais precisamente, as informações de especificação estão contidas de forma criptografada para cada parte dos dados de textos simples divisionais). A unidade de descriptografia 373 possui uma outra função de transmitir as informações de especificação contidas nos dados descriptografados obtidos pela descriptografia dos dados criptografados divisionais para a unidade de análise de informações de especificação 377.

A unidade de análise de informações de especificação 377 analisa o conteúdo indicado pelas informações de especificação (a primeira informação de especificação recebida da unidade de pré-processamento 372 ou as outras informações de especificação recebidas da unidade de descriptografia 373). A unidade de análise de informações de especificação 377 transmite informações no conteúdo especificado pelas informações de especificação para a unidade de geração de soluções 374. Como as informações de especificação indicam a ordem de geração da solução no aparelho de processamento de criptografia 1 nesta abordagem, a unidade de análise de informações de especificação 377

transmite as informações de especificação para a unidade de geração de soluções 374.

A unidade de geração de soluções 374 gera as soluções em seqüência. A solução gerada pela unidade de geração de soluções 374 é a mesma gerada pela unidade de geração de soluções 274 no aparelho de processamento de criptografia 1 na mesma ordem. A ordem da solução a ser gerada pela unidade de geração de soluções 374 é especificada pelas informações transmitidas a partir da unidade de análise de informações de especificação 377. A solução gerada é transmitida para a unidade de geração de algoritmos 375 e a unidade de geração de chaves 376.

A unidade de geração de algoritmos 375 gera o algoritmo com base na solução recebida da unidade de geração de soluções 374. O algoritmo é utilizado para a execução do processamento de descriptografia na unidade de descriptografia 373. O algoritmo gerado pela unidade de geração de algoritmos 375 no aparelho de processamento de descriptografia 2 é o mesmo gerado pela unidade de geração de algoritmos 275 no aparelho de processamento de criptografia 1 na mesma ordem.

A unidade de geração de chaves 376 gera a chave com base na solução recebida da unidade de geração de soluções 374. A chave é utilizada para a execução do processamento de descriptografia na unidade de descriptografia 373. A chave gerada pela unidade de geração de chaves 376 no aparelho de processamento de descriptografia 2 é a mesma gerada pela unidade de geração de chaves 276 no aparelho de processamento de criptografia 1 na mesma ordem.

A função da unidade de conexão 379 no aparelho de processamento de descriptografia 2 é aproximadamente a mesma do aparelho de processamento de criptografia 1. A unidade de conexão 379 obtém os dados de textos simples divisionais gerados pela descriptografia dos dados criptografados divisionais na unidade de descriptografia 373 em uma unidade para geração dos dados a serem processados. Os dados a serem processados são os mesmos que os dados

originais a serem processados, que foram criptografados no aparelho de processamento de criptografia 1. Os dados a serem processados são transmitidos através do barramento 39 para o exterior do dispositivo de descriptografia 37 (por exemplo, para a HDD 33).

No aparelho de processamento de descriptografia 2, a CPU 31 executa o programa gravado na ROM 32 o na HDD 33 para formar blocos funcionais, como ilustrado na Figura 7. Os blocos funcionais ilustrados na Figura 7 podem ser formados somente pelo programa descrito acima gravado na ROM 32 ou na HDD 33, mas também podem ser formados pela cooperação entre o programa descrito acima e outro programa que é, por exemplo, um OS incluso no aparelho de processamento de descriptografia 2. Além disso, uma parte do dispositivo de descriptografia 37 descrito acima pode ser formada pelo programa descrito acima.

Os blocos funcionais no aparelho de processamento de descriptografia 2, que são formados pela CPU 31, contêm uma unidade de controle de entrada 410, uma unidade de controle 420 e uma unidade de controle de saída 430, como ilustrado na Figura 7.

A unidade de controle de entrada 410 possui uma função de receber uma entrada do dispositivo de entrada 35 através do barramento 39 e de analisar o conteúdo da entrada para transmitir o conteúdo analisado para a unidade de controle 420. O conteúdo da entrada do dispositivo de entrada 35, que é recebido pela unidade de controle de entrada 410, será descrito a seguir. A unidade de controle de entrada 410 possui uma outra função de receber os dados criptografados através do barramento 39, por exemplo, da HDD 33 para transmitir os dados criptografados recebidos para a unidade de controle 420.

A unidade de controle 420 possui uma função principal de transformar os dados criptografados em dados "inúteis", de acordo com a presente invenção. A unidade de controle 420 possui uma outra função de determinar se os dados criptografados devem ou não ser transformados em dados "inúteis", de acordo com a presente invenção, apesar de a unidade de controle 420 nem sempre

executar tal determinação para todos os dados criptografados.

A unidade de controle 420 contém uma seção de controle principal 421, uma seção de detecção 422, um temporizador 423 e uma seção de destruição 424.

A seção de controle principal 421 possui uma função de determinar se os dados criptografados devem ou não ser transformados em dados "inúteis", de acordo com a presente invenção. Há três casos, como descrito a seguir, nos quais o aparelho de processamento de descriptografia 2, nesta abordagem, transforma os dados criptografados em dados "inúteis", de acordo com a presente invenção. Em qualquer caso, a seção de destruição 424, que recebeu uma instrução de transformar os dados criptografados em dados "inúteis" com a seção de controle principal 421, transforma os dados criptografados em dados "inúteis" através de um método, conforme descrito a seguir. Quando a seção de controle principal 421 não transforma os dados criptografados na presente invenção em dados "inúteis" e, além disso, a condição a seguir é satisfeita, a seção de controle principal 421 gera uma notificação que permite que o dispositivo de descriptografia 37 descriptografe os dados criptografados.

Como descrito acima, a seção de destruição 424 possui a função de executar o processo de transformação dos dados criptografados em dados "inúteis". O processo é realizado convertendo, de maneira irreversível, uma parte dos dados criptografados ou escrevendo os dados apropriados sobre uma parte dos dados criptografados. Para a sobrescrita de uma parte dos dados criptografados, o conteúdo dos dados a serem sobrescritos pode ser qualquer conteúdo de dados, contanto que a sobrescrita cause uma alteração irreversível em uma parte dos dados criptografados e evite que os dados criptografados sejam descriptografados. Por exemplo, dados apropriados, tais como enumeração de dados como "0" ou "1" ou dados alternados "0" e "1", podem ser usados. A repetição da data de sobrescrita ou a repetição de informações de um tamanho de arquivo de um outro arquivo atualizado por último pode ser utilizada como o dado

para a sobrescrita. Os dados escritos sobre uma parte dos dados criptografados podem ser alterados em um cronograma adequado. Em qualquer caso em que uma parte dos dados criptografados é convertida de maneira irreversível e no caso em que uma parte dos dados criptografados é sobrescrita, é necessário especificar uma "parte" dos dados criptografados a ser convertida de maneira irreversível ou sobrescrita.

É a seção de detecção 422 que tem uma função de especificar a "parte". A seção de detecção 422 especifica a parte dos dados criptografados que deve ser convertida de maneira irreversível ou sobrescrita e transmite as informações da parte especificada para a seção de destruição 424. A parte dos dados criptografados que é especificada pela seção de detecção 422 é a parte cuja conversão irreversível ou sobrescrita evita que os dados criptografados sejam descriptografados. Nesta abordagem, a "parte" contém pelo menos uma das primeiras informações de especificação nos dados criptografados e o primeiro dado criptografado divisional nos dados criptografados. A primeira informação de especificação e o primeiro dado criptografado divisional podem ser convertidos ou sobrescritos. Em tal caso, a faixa que permite tanto que a primeira informação de especificação como o primeiro dado criptografado divisional sejam convertidos ou sobrescritos é especificada pela seção de detecção 422. Quando a primeira informação de especificação deve ser convertida ou sobrescrita, a "parte" dos dados criptografados que deve ser convertida ou sobrescrita não deve necessariamente ser a primeira informação de especificação e pode ser uma faixa adequada contendo a primeira informação de especificação, que não é tão grande. Quando o primeiro dado criptografado divisional deve ser convertido ou sobrescrito, a "parte" dos dados criptografados que deve ser convertida ou sobrescrita não deve necessariamente ser o primeiro dado criptografado divisional e pode ser uma faixa adequada contendo o primeiro dado criptografado divisional, que não é tão grande. Em qualquer caso, a seção de detecção 422 especifica a parte dos dados criptografados que deve ser convertida ou sobrescrita e notifica a

seção de destruição 424 da parte especificada. A seção de destruição 424, que recebe a notificação, sobrescreve ou converte a parte dos dados criptografados que é especificada pela seção de detecção 422. Nesta abordagem, a seção de detecção 422 especifica o cabeçalho dos dados criptografados contendo a primeira informação de especificação como a parte dos dados criptografados que deve ser convertida ou sobrescrita quando a primeira informação de especificação é convertida ou sobrescrita e especifica, por si só, o primeiro dado criptografado divisional quando o primeiro dado criptografado divisional é convertido ou sobrescrito.

O temporizador 423 especifica uma data e uma hora do cronograma de sobrescrita ou conversão da parte dos dados criptografados. Como um OS geral possui tal função, o temporizador 423 pode ser implementado emprestando a função de um OS.

A unidade de controle de saída 430 transmite uma saída da unidade de controle 420 para um local apropriado através do barramento 39. A unidade de controle 420 emite, por exemplo, os dados criptografados em alguns casos, os dados "inúteis" obtidos dos dados criptografados em alguns casos e a notificação descrita acima para permitir que o dispositivo de criptografia 37 descriptografe os dados criptografados em outros casos. Os casos em que essas saídas são executadas e o destino das saídas serão descritos a seguir.

A seguir, será descrito um fluxo de um processamento executado no sistema de criptografia.

O fluxo do processamento executado no sistema de criptografia é o seguinte.

Primeiramente, o aparelho de processamento de criptografia 1 criptografa os dados a serem processados para gerar os dados criptografados.

Em seguida, o aparelho de processamento de criptografia 1 transmite os dados criptografados para o aparelho de processamento de descriptografia 2.

Em seguida, o aparelho de processamento de descriptografia 2, que

recebeu os dados criptografados, descriptografa os dados criptografados, de acordo com um requisito do usuário do aparelho de processamento de descriptografia 2, para obter os dados a serem processados. O aparelho de processamento de descriptografia 2 também transforma os dados criptografados em dados "inúteis" de acordo com um requisito do usuário do aparelho de processamento de descriptografia 2 ou em um cronograma predeterminado.

Primeiramente, o processo descrito acima, no qual o aparelho de processamento de criptografia 1 criptografa os dados a serem processados para gerar os dados criptografados, será descrito em detalhes em relação à Figura 8.

Primeiro, os dados a serem processados são lidos (S1101). Os dados a serem processados podem ser quaisquer dados, contanto que seja necessário que sejam transmitidos do aparelho de processamento de criptografia 1 para o aparelho de processamento de descriptografia 2. Nesta abordagem, os dados a serem processados são gravados na HDD 23. Os dados a serem processados podem ser de um tipo de dados que sejam lidos a partir de outro meio de gravação, como um meio de gravação externo, no aparelho de processamento de criptografia 1.

Quando um comando de transmissão de dados a serem processados para o aparelho de processamento de descriptografia 2 é inserido a partir, por exemplo, do dispositivo de entrada 25, a CPU 21 lê os dados a serem processados a partir da HDD 23 para transmitir os dados lidos através do barramento 29 para o dispositivo de criptografia 27. Mais especificamente, os dados a serem processados são transmitidos do barramento 29 para a unidade de interface 271 no dispositivo de criptografia 27 e, depois, para a unidade de pré-processamento 272.

Quase ao mesmo tempo em que a leitura dos dados a serem processados, informações de destino indicando o aparelho de processamento de descriptografia 2 correspondente a um destino da transmissão dos dados criptografados obtidos pela criptografia dos dados a serem processados e

informações que servem para gerar as informações de especificação do cronograma são inseridas a partir do dispositivo de entrada 25 (S1102). As informações de destino e as informações que servem para gerar as informações de especificação do cronograma são transmitidas pela CPU 21 através do barramento 29 para o dispositivo de criptografia 27. Mais especificamente, as informações de destino são transmitidas através da unidade de interface 271 para a unidade de geração de cabeçalhos 279, considerando que as informações que servem para gerar as informações de especificação do cronograma são transmitidas através da unidade de interface 271 para a unidade de geração de informações de especificação do cronograma 278.

A unidade de geração de informações de especificação do cronograma 278 gera as informações de especificação do cronograma com base nas informações recebidas que servem para gerar as informações de especificação do cronograma. As informações de especificação do cronograma nesta abordagem são uma data e uma hora para a especificação de um instante de tempo predeterminado, por exemplo X (hora), X (minuto), X (mês), X (dia), 200X (ano).

A unidade de geração de informações de especificação do cronograma 278 transmite as informações de especificação do cronograma geradas para a unidade de geração de cabeçalhos 279.

A unidade de geração de soluções 274 gera a solução no método a seguir. A solução gerada é transmitida da unidade de geração de soluções 274 tanto para a unidade de geração de algoritmos 275 como para a unidade de geração de chaves 276. A unidade de geração de soluções 274 também transmite informações para especificar a ordem de geração da solução no aparelho de processamento de criptografia 1 para a unidade de geração de informações de especificação 277. A unidade de geração de informações de especificação 277 transmite as informações, como as informações de especificação, para a unidade de criptografia 273 ou a unidade de geração de cabeçalhos 279. Somente a

informação de especificação indicando a ordem de geração da primeira solução gerada para os dados criptografados no aparelho de processamento de criptografia 1 (a primeira informação de especificação) é transmitida para a unidade de geração de cabeçalhos 279.

As soluções utilizadas para a criptografia dos dados a serem processados no aparelho de processamento de criptografia 1 não são limitadas a uma série de soluções iniciando com a primeira solução gerada no aparelho de processamento de criptografia 1. O motivo é, por exemplo, o seguinte. Quando um outro dado a ser processado foi criptografado anteriormente no aparelho de processamento de criptografia 1 para gerar uma série de soluções contínuas, uma série de soluções após as soluções geradas na criptografia anterior é utilizada para a criptografia dos dados atuais a serem processados em alguns casos. Portanto, é necessária a informação de especificação que indica a ordem de geração da solução que é utilizada para a criptografia dos dados a serem processados na criptografia atual.

Como a unidade de geração de soluções 274 gera a solução será descrito a seguir.

Quando a unidade de interface 271 recebe os dados a serem processados do barramento 29, a unidade de geração de soluções 274 recebe as informações da recepção dos dados da unidade de interface 271.

Na recepção das informações, a unidade de geração de soluções 274 inicia a geração da solução. Nesta abordagem, a unidade de geração de soluções 274 gera uma solução sempre que os dados a serem processados forem recebidos pela unidade de interface 271. A solução nesta abordagem é uma matriz 8×8 (X), apesar de a solução não ser limitada também.

A unidade de geração de soluções 274 gera continuamente as soluções como soluções de transição não linear, apesar de não ser necessário. Como resultado, cada uma das soluções é um número pseudo-aleatório.

A fim de gerar continuamente as soluções em um modo de transição não

linear, por exemplo, (1) a inclusão de um cálculo ascendente da solução anterior no processo de geração das soluções, (2) a inclusão de uma multiplicação das duas ou mais soluções anteriores no processo de geração das soluções, ou a combinação de (1) e (2) são concebidas.

Nesta abordagem, a unidade de geração de soluções 274 tem uma primeira solução (X_{01}) predeterminada e uma segunda solução (X_{02}) predeterminada como uma matriz inicial correspondente às soluções iniciais (por exemplo, a primeira solução e a segunda solução são armazenadas em uma memória predeterminada, como a HDD 23 ou a ROM 22). A matriz inicial contida no aparelho de processamento de criptografia 1 é a mesma que está contida no aparelho de processamento de descriptografia 2, como descrito a seguir.

A unidade de geração de soluções 274 atribui a matriz inicial ao algoritmo para a geração de soluções armazenadas na unidade de geração de soluções 274 para gerar uma primeira solução (X_1) como a seguir.

Primeira solução (X_1) = $X_{02}X_{01} + \alpha$ (α = uma matriz 8×8)

Esta é a primeira solução gerada.

A seguir, quando a unidade de interface 271 recebe os dados a serem processados do barramento 29, a unidade de geração de soluções 274 gera uma segunda solução (X_2) como a seguir.

Segunda solução (X_2) = $X_1X_{02} + \alpha$

De maneira semelhante, sempre que a unidade de interface 271 recebe os dados a serem processados do barramento 29, a unidade de geração de soluções 274 gera uma terceira solução, uma quarta solução, uma enésima solução e assim por diante como a seguir.

Terceira solução (X_3) = $X_2X_1 + \alpha$

Quarta solução (X_4) = $X_3X_2 + \alpha$

Enésima solução (X_N) = $X_{N-1}X_{N-2}$ + (

As soluções geradas assim são transmitidas à unidade de geração de algoritmos 275 e à unidade de geração de chaves 276 e ficam armazenadas na

unidade de geração de soluções 274. Nesta abordagem, para a geração da enésima solução (XN), a enésima solução 1 (XN-1) e a enésima solução 2 (XN-2), em resumo, as duas soluções geradas anteriormente, são utilizadas. Portanto, para a geração de uma nova solução, a unidade de geração de soluções 274 deve armazenar as duas soluções anteriores que são geradas imediatamente antes da nova solução (ou uma unidade diferente da unidade de geração de soluções 274 deve armazenar as duas soluções).

As soluções geradas assim se tornam caóticas para o trânsito não linear e são, portanto, números pseudo-aleatórios.

Não é necessário utilizar a matriz (correspondente às informações ambientais para cada caso em que a solução é gerada. Por exemplo, (pode ser utilizada para a primeira solução (X1) = X02X01 + (e para o caso em que a primeira solução é utilizada. A segunda solução e as soluções subseqüentes podem ser obtidas através de uma fórmula geral: Enésima solução (XN) = XN-1XN-2.

Para causar a transição não linear, além de usar a fórmula descrita acima:

Enésima solução (XN) = XN-1XN-2 (+()

a fórmula a seguir também pode ser utilizada.

O parêntesis para α significa que α não é necessária para obter a segunda solução e as soluções subseqüentes, o que se aplica ao caso exemplificado a seguir.

Por exemplo,

(a) Enésima solução $(X_N) = (X_{N-1})^P$

(b) Enésima solução $(X_N) = (X_{N-1})^P(X_{N-2})^Q(X_{N-3})^R(X_{N-4})^S$

(c) Enésima solução $(X_N) = (X_{N-1})^P+(X_{N-2})^Q$

em que cada P, Q, R e S é uma constante predeterminada. A unidade de geração de soluções 274 possui uma matriz inicial quando a Fórmula (a) é utilizada, duas matrizes para a utilização da Fórmula (c) e quatro matrizes para a utilização da Fórmula (b).

Apesar de a α descrita acima ser uma constante, α também pode ser a informação ambiental de variação específica. As informações ambientais são informações espontaneamente geradas de forma seqüencial com o decorrer do tempo e podem ser comumente obtidas mesmo em um local distante. As informações ambientais são, por exemplo, informações determinadas com base no estado atmosférico em uma determinada área, informações determinadas com base no conteúdo de um programa de televisão transmitido em uma determinada hora de uma determinada estação de TV ou informações determinadas pelo resultado de um determinado esporte.

Se a α descrita acima for criada seqüencialmente a partir das informações ambientais descritas acima para gerar informações comuns, a confidencialidade da comunicação pode ser adicionalmente aprimorada.

É evidente que a α (que pode ser gerada a partir das informações ambientais) pode ser adicionada ao lado direito de cada uma das Fórmulas (a) a (c) descritas acima.

A unidade de geração de cabeçalhos 279, que recebeu as informações de destino, as informações de especificação do cronograma e a primeira informação de especificação, gera os dados de cabeçalho (S1103). Os dados de cabeçalho gerados contêm as informações de destino, as informações de especificação do cronograma e a primeira informação de especificação.

Apesar de as informações de especificação nesta abordagem indicarem a ordem de geração da solução de interesse, como descrito acima, a solução pode servir como a informação de especificação. Neste caso, a primeira informação de especificação que é a primeira solução gerada é transmitida para a unidade de geração de cabeçalhos 279, considerando que as outras informações específicas que são a segunda solução e as soluções subseqüentes geradas são transmitidas para a unidade de criptografia 273. As informações específicas também podem servir como a chave. Neste caso, a unidade de geração de soluções 274 não é necessária para transmitir a solução para a unidade de geração de informações

de especificação 277. Ao invés disso, a chave gerada pela unidade de geração de chaves 276 precisa ser transmitida para a unidade de geração de informações de especificação 277. Quando a informação de especificação for uma chave, a primeira informação de especificação, que é a primeira chave gerada, é transmitida para a unidade de geração de cabeçalhos 279, considerando que as outras informações de especificação, que são a segunda chave e as chaves subseqüentes geradas, são transmitidas para a unidade de criptografia 273, como no caso em que a informação de especificação é uma solução.

Os dados de cabeçalho são transmitidos da unidade de geração de cabeçalhos 279 para a unidade de conexão 280.

A unidade de pré-processamento 272 divide os dados a serem processados nos dados de textos simples divisionais, cada um composto por um número predeterminado de bits (S1104).

Apesar de poder haver uma série de métodos para a geração dos dados de textos simples divisionais dos dados a serem processados (especificamente, um comprimento de dados dos dados de textos simples divisionais pode diferir para cada parte dos dados de textos simples divisionais), os comprimentos de dados de todos os dados de textos simples divisionais são os mesmos (por exemplo, um comprimento de 8 bits) nesta abordagem. Os dados de textos simples divisionais gerados são transmitidos da unidade de pré-processamento 272 para a unidade de criptografia 273.

Em paralelo com a geração dos dados de textos simples divisionais, o algoritmo e a solução são gerados. O algoritmo e a solução são utilizados para a criptografia dos dados de textos simples divisionais para obter os dados criptografados divisionais.

O algoritmo é gerado pela unidade de geração de algoritmos 275.

A unidade de geração de algoritmos 275 nesta abordagem gera o algoritmo com base na solução.

A unidade de geração de algoritmos 275 nesta abordagem gera o

algoritmo com base na solução como a seguir.

O algoritmo nesta abordagem é definido como "sendo obtido pela elevação da matriz 8×8 X correspondente à solução à potência "a", girando a matriz no sentido horário em n×90° e depois multiplicando a matriz girada por Y quando os dados de textos simples divisionais de 8 bits forem uma matriz 1×8 Y".

Apesar de 'a' ser uma constante predeterminada em alguns casos, 'a' é um valor numérico que varia com base na solução nesta abordagem. Especificamente, o algoritmo nesta abordagem varia com base na solução. Por exemplo, 'a' pode ser definido como um lembrete obtido pela divisão do valor numérico obtido com a adição de todos os valores numéricos correspondentes aos elementos de matriz contidos na solução, que é a matriz 8×8, por 5 (entretanto, a = 1 quando o lembrete for 0).

O 'n' descrito acima é a chave e é um valor numérico predeterminado. Quando a chave é um valor constante, 'n' é fixo. Como descrito a seguir, a chave varia com base na solução. Especificamente nesta abordagem, 'n' também varia com base na solução.

É evidente que o algoritmo pode ser determinado de outra maneira. Além disso, o algoritmo pode ser fixo.

Nesta abordagem, a unidade de geração de algoritmos 275 gera o algoritmo para cada recepção da solução da unidade de geração de soluções 274 e transmite o algoritmo gerado para a unidade de criptografia 273.

Em paralelo com a geração dos dados de textos simples divisionais, a unidade de geração de chaves 276 gera a chave utilizada para a criptografia dos dados de textos simples divisionais.

A unidade de geração de chaves 276 gera a chave com base na solução.

Nesta abordagem, a unidade de geração de chaves 276 gera a chave como a seguir.

A chave nesta abordagem corresponde a um valor numérico obtido pela adição de todos os valores correspondentes aos elementos da matriz contida na

solução, que é a matriz 8×8. Portanto, a chave varia com base na solução nesta abordagem.

A chave também pode ser determinada de outra maneira.

Nesta abordagem, para cada recepção da solução da unidade de geração de soluções 274, a unidade de geração de chaves 276 gera a chave e transmite a chave gerada para a unidade de criptografia 273.

A unidade de criptografia 273 criptografa os dados de textos simples divisionais recebidos da unidade de pré-processamento 272 com base no algoritmo recebido da unidade de geração de algoritmos 275 e na chave recebida da unidade de geração de chaves 276 (S1105).

Como descrito acima, o algoritmo é definido como "sendo obtido pela elevação da matriz 8×8 X correspondente à solução para a potência 'a', girando a matriz no sentido horário em n×90° e depois multiplicando a matriz girada por Y quando os dados de textos simples divisionais de 8 bits forem uma matriz 1×8 Y" e o "n" correspondente à chave é um valor numérico, como descrito acima.

Por exemplo, quando 'a' for 3 e 'n' for 6, a matriz 8×8, que é obtida com a rotação de uma outra matriz 8×8 obtida pela elevação de X à terceira potência em 6×90° = 540° no sentido horário, é multiplicada pelos dados de textos simples divisionais para executar a criptografia.

Os dados gerados assim são os dados criptografados divisionais.

Para a criptografia do segundo e dos subseqüentes dados de textos simples divisionais, a unidade de criptografia 273 mistura a solução recebida da unidade de geração de soluções 274 nos dados de textos simples divisionais e depois criptografa os dados de textos simples divisionais para obter os dados criptografados divisionais.

Nesta abordagem, as etapas em S1104 e S1105 são repetidas até que todos os dados a serem processados sejam criptografados e se tornem dados criptografados divisionais.

Os dados criptografados divisionais são transmitidos para a unidade de

conexão 280. A unidade de conexão 280 conecta os dados de cabeçalho 501 e os dados criptografados divisionais 502 em uma unidade contendo a estrutura conforme ilustrada na Figura 4(A) e gera os dados criptografados (S1106). A ordem de disposição dos dados criptografados divisionais corresponde àquela dos dados de textos simples divisionais originais.

Como descrito acima, o processo no qual o aparelho de processamento de criptografia 1 criptografa os dados a serem processados para gerar os dados criptografados é encerrado primeiro.

Os dados criptografados gerados assim são transmitidos através do barramento 29 para o dispositivo de comunicação 28 no aparelho de processamento de criptografia 1.

O dispositivo de comunicação 28 transmite os dados criptografados para o aparelho de processamento de descriptografia 2 designado pelo endereço MAC contido nos dados de cabeçalho dos dados criptografados através da rede N.

Os dados criptografados transmitidos para o aparelho de processamento de descriptografia 2 são recebidos pelo dispositivo de comunicação 38 no aparelho de processamento de descriptografia 2. Os dados criptografados são transmitidos para a HDD 33 através do barramento 39 para serem gravados.

Um processamento de descriptografia dos dados criptografados, que pode ser executado no aparelho de processamento de descriptografia 2 que recebe os dados criptografados, será agora descrito.

Daqui em diante, para o processo de descriptografia, um processamento de descriptografia dos dados criptografados novamente nos dados a serem processados será descrito em detalhes em relação à Figura 9.

Quando o usuário opera o dispositivo de entrada 35 do aparelho de processamento de descriptografia 2 para inserir uma instrução de descriptografia dos dados criptografados (S1301), a instrução é transmitida para a CPU 31. Com base na instrução, a CPU 31 transmite os dados criptografados para o dispositivo de descriptografia 37.

Os dados criptografados são recebidos pela unidade de pré-processamento 372 no dispositivo de descriptografia 37 através da unidade de interface 371.

Então, a unidade de pré-processamento 372 extrai os dados de cabeçalho dos dados criptografados recebidos (S1302) e também extrai a primeira informação de especificação dos dados de cabeçalho para transmitir a primeira informação de especificação extraída para a unidade de análise de informações de especificação 377.

A unidade de análise de informações de especificação 377, que recebeu a primeira informação de especificação, especifica a ordem de geração da solução que deve ser utilizada para a descriptografia do primeiro dado criptografado divisional no aparelho de processamento de criptografia 1 (S1303). Então, a unidade de análise de informações de especificação 377 transmite as informações especificadas para a unidade de geração de soluções 374.

A unidade de geração de soluções 374 gera a solução para a descriptografia dos dados criptografados divisionais com base nas informações (S1304).

A solução é gerada na unidade de geração de soluções 374 no dispositivo de descriptografia 37 do aparelho de processamento de descriptografia 2 através do mesmo processo que é executado na unidade de geração de soluções 274 no aparelho de processamento de criptografia 1.

Como descrito acima, a unidade de geração de soluções 374 possui a mesma matriz inicial e o mesmo algoritmo para a geração das soluções como as armazenadas na unidade de geração de soluções 274 do aparelho de processamento de criptografia 1 associado ao dispositivo de descriptografia 37, incluindo a unidade de geração de soluções 374. Portanto, quando a solução gerada no dispositivo de descriptografia 37 do aparelho de processamento de descriptografia 2 é comparada com a solução gerada no dispositivo de criptografia 27 do aparelho de processamento de criptografia 1 na mesma ordem, as soluções

são as mesmas. A ordem da solução a ser gerada é determinada pelas informações de especificação.

A solução gerada é transmitida da unidade de geração de soluções 374 para a unidade de geração de algoritmos 375 e para a unidade de geração de chaves 376.

A unidade de geração de algoritmos 375 e a unidade de geração de chaves 376, respectivamente, geram o algoritmo e a chave para a descriptografia dos dados criptografados divisionais (S1305).

A unidade de geração de algoritmos 375 gera o algoritmo com base nas informações recebidas. O processo no qual a unidade de geração de algoritmos 375 do aparelho de processamento de descriptografia 2 gera o algoritmo é o mesmo processo no qual a unidade de geração de algoritmos 275 do aparelho de processamento de criptografia 1 gera o algoritmo. O algoritmo gerado pela unidade de geração de algoritmos 375, com base na mesma solução, é sempre o mesmo que o gerado na unidade de geração de algoritmos 275 do aparelho de processamento de criptografia 1.

Por outro lado, a unidade de geração de chaves 376 gera a chave com base nas informações recebidas. O processo no qual a unidade de geração de chaves 376 do aparelho de processamento de descriptografia 2 gera a chave é o mesmo processo no qual a unidade de geração de chaves 276 do aparelho de processamento de criptografia 1 gera a chave. A chave gerada pela unidade de geração de chaves 376, com base na mesma solução, é sempre a mesma que a gerada pela unidade de geração de chaves 276 do aparelho de processamento de criptografia 1.

O aparelho de processamento de descriptografia 2 gera a mesma solução gerada no aparelho de processamento de criptografia 1, com base nas informações que indicam a ordem da geração da solução utilizada para a criptografia das informações de especificação no aparelho de processamento de criptografia 1, e, então, gera o algoritmo e a chave com base na solução gerada.

Portanto, o aparelho de processamento de descriptografia 2 pode gerar o mesmo algoritmo e a mesma chave que são utilizados para a criptografia das informações de especificação no aparelho de processamento de criptografia 1.

O algoritmo gerado é transmitido da unidade de geração de algoritmos 375 para a unidade de descriptografia 373. A chave gerada é transmitida da unidade de geração de chaves 376 para a unidade de descriptografia 373.

A seguir, utilizando o algoritmo e a chave recebidos da unidade de geração de algoritmos 375 e da unidade de geração de chaves 376, respectivamente, a unidade de descriptografia 373 descriptografa os dados criptografados divisionais (S1306).

Mais especificamente, a unidade de descriptografia 373 gera o algoritmo para a execução do processamento de descriptografia (a definição "quando os dados criptografados divisionais são considerados como uma matriz 1×8 Z, os dados de textos simples divisionais são obtidos pela elevação da matriz 8×8 X à potência 'a', girando a matriz obtida em n×90° no sentido horário e depois multiplicando uma matriz inversa da matriz girada por Z") com base no algoritmo recebido da unidade de geração de algoritmos 375 (a definição "os dados criptografados divisionais são obtidos pela elevação da matriz 8×8 X correspondente à solução à potência 'a', girando a matriz no sentido horário em n×90° e depois multiplicando a matriz girada por Y quando os dados de textos simples criptografados de 8 bits forem a matriz 1×8 Y") e usa a chave para executar um cálculo de acordo com a definição descrita acima para executar o processamento de descriptografia.

Da maneira descrita acima, a unidade de descriptografia 373 descriptografa os dados criptografados divisionais transmitidos da unidade de pré-processamento 372 para gerar os dados de textos simples divisionais.

A unidade de descriptografia 373 transmite os dados de textos simples divisionais descriptografados para a unidade de conexão 379.

A unidade de descriptografia 373 também extrai os dados de informações

de especificação contidos nos dados de textos simples divisionais para transmitir os dados de informações de especificação extraídos para a unidade de análise de informações de especificação 377. A unidade de análise de informações de especificação 377 transmite o conteúdo das informações de especificação para a unidade de geração de soluções 374. A unidade de geração de soluções 374 gera a solução com base nas informações transmitidas para transmitir a solução gerada para a unidade de geração de algoritmos 375 e a unidade de geração de chaves 376. A unidade de geração de algoritmos 375 e a unidade de geração de chaves 376, que receberam a solução, transmitem a solução para a unidade de descriptografia 373. Então, a unidade de descriptografia 373 descriptografa o segundo dado criptografado divisional para gerar o segundo dado de textos simples divisional. Especificamente, o dispositivo de descriptografia 37 repete as etapas descritas acima em S1303 a S1306 até que todos os dados criptografados divisionais sejam descriptografados.

Como descrito acima, o aparelho de processamento de descriptografia 2 nesta abordagem utiliza as informações de especificação, que são extraídas pela descriptografia dos dados criptografados divisionais, para descriptografar os dados criptografados divisionais subseqüentes. A Figura 4(B) ilustra esquematicamente um estado da descriptografia. A Figura 4(B) ilustra os dados de textos simples divisionais indicados pelo número de referência 503 e as informações de especificação em uma forma de chave indicadas por K.

A seguir, os dados de textos simples divisionais descriptografados são transmitidos para a unidade de conexão 379. A unidade de conexão 379 conecta os dados de textos simples divisionais recebidos em uma unidade para obter os dados a serem processados (S1307).

Dessa maneira, o aparelho de processamento de descriptografia 2 pode descriptografar novamente os dados criptografados nos dados a serem processados.

Os dados gerados a serem processados são transmitidos da unidade de

conexão 379 para a unidade de interface 371 e, depois, através do barramento 39, para, por exemplo, a HDD 33. Os dados a serem processados são utilizados de maneira apropriada no aparelho de processamento de descriptografia 2.

No exemplo descrito acima, as informações de especificação indicam a ordem de geração da solução que é utilizada para a criptografia dos dados criptografados divisionais no aparelho de processamento de criptografia 1. Entretanto, as informações de especificação não são limitadas também.

Por exemplo, as informações de especificação podem ser a própria solução. Neste caso, o dispositivo de descriptografia 37 não precisa da unidade de geração de soluções 374. Neste caso, é suficiente que a unidade de análise de informações de especificação 377 do dispositivo de descriptografia 37 transmita a solução especificada pela unidade de análise de informações de especificação 377 para a unidade de geração de algoritmos 375 e a unidade de geração de chaves 376.

Por outro lado, as informações de especificação podem ser a própria chave. Neste caso, o dispositivo de descriptografia 37 não precisa da unidade de geração de soluções 374 ou da unidade de geração de chaves 376. Neste caso, é suficiente que a unidade de análise de informações de especificação 377 do dispositivo de descriptografia 37 transmita a chave especificada pela unidade de análise de informações de especificação 377 para a unidade de descriptografia 373. Neste caso, o algoritmo utilizado para a criptografia ou a descriptografia é fixado entre o aparelho de processamento de criptografia 1 e o aparelho de processamento de descriptografia 2.

A seguir, um processamento de transformação dos dados criptografados em dados "inúteis", que é executado no aparelho de processamento de descriptografia 2, será descrito.

Os dados criptografados são transformados em dados "inúteis" no aparelho de processamento de descriptografia 2 nos três casos a seguir.

EXEMPLOS

Exemplo 1: os dados criptografados são transformados em dados "inúteis" com base na intenção do usuário.

Quando o usuário introduz um comando de transformação dos dados criptografados em dados "inúteis" através do dispositivo de entrada 35 (por exemplo, o usuário arrasta um ícone associado aos dados criptografados e solta o ícone sobre um outro ícone associado a um programa de transformação dos dados criptografados em dados "inúteis"), os dados criptografados são transformados em dados "inúteis".

Na entrada do comando, o conteúdo do comando é transmitido através do barramento 39 para a unidade de controle de entrada 410. A unidade de controle de entrada 410 analisa e transmite o conteúdo para a seção de controle principal 421 da unidade de controle 420.

A seção de controle principal 421, que recebeu o conteúdo, determina transformar os dados criptografados em "inúteis", de acordo com a presente invenção, para ler os dados criptografados especificados pelo comando, por exemplo, da HDD 33. Os dados criptografados são lidos através do barramento 39 e da unidade de controle de entrada 410. A seção de controle principal 421 também transmite uma instrução de execução do processamento de transformação dos dados criptografados em "inúteis", de acordo com a presente invenção, para a seção de destruição 424. Por outro lado, a seção de controle principal 421 transmite uma instrução de especificação de uma parte a ser destruída nos dados criptografados para a seção de detecção 422.

A seção de detecção 422 especifica a parte a ser destruída nos dados criptografados. Como a parte a ser destruída nos dados criptografados nesta abordagem corresponde aos dados de cabeçalho ou ao primeiro dado criptografado divisional nos dados criptografados, a seção de detecção 422 especifica uma área dos dados de cabeçalho ou o primeiro dado criptografado divisional nos dados criptografados.

A seção de detecção 422 notifica a seção de destruição 424 da área detectada.

A seção de destruição 424, que recebeu a instrução descrita acima da seção de controle principal 421 e a notificação descrita acima da seção de detecção 422, executa o processamento de transformação dos dados criptografados em dados "inúteis". O processamento é executado pela conversão irreversível da área especificada pela seção de detecção 422 ou pela escrita dos dados apropriados irrelevantes para os dados criptografados sobre a área especificada. Os dados criptografados que estão sujeitos a tal processamento não podem mais ser descriptografados.

A seção de controle principal 421 transmite os dados criptografados, que estão sujeitos ao processamento descrito acima para evitar que sejam descriptografados, para um local apropriado onde os dados criptografados devem ser gravados, por exemplo para a HDD 33, através da unidade de controle de saída 430 e do barramento 39. Os dados criptografados que não podem mais ser descriptografados são gravados na HDD 33.

Note que o exemplo 1 pode ser executado mesmo que os dados criptografados não contenham as informações de especificação do cronograma.

Exemplo 2: os dados criptografados são automaticamente transformados em dados "inúteis" no cronograma predeterminado.

Como descrito acima, os dados criptografados nesta abordagem contêm as informações de especificação do cronograma. A seção de controle principal 421, que executa o exemplo 2, tem uma função de monitorar constantemente se os dados criptografados estão presentes ou não no aparelho de processamento de descriptografia 2 e de ler as informações de especificação do cronograma contidas nos dados criptografados quando os dados criptografados estiverem presentes. Para executar a função, a seção de controle principal 421 pesquisa, constante ou periodicamente, o aparelho de processamento de descriptografia 2 para monitorar a presença dos dados criptografados.

Na detecção dos dados criptografados contendo as informações de especificação do cronograma no aparelho de processamento de descriptografia 2, a seção de controle principal 421, como descrito acima, por exemplo, monitora constantemente se o cronograma especificado pelas informações de especificação do cronograma chegou ou não. O monitoramento pode ser executado para cada um dos dados criptografados quando uma série de dados criptografados estiver presente no aparelho de processamento de descriptografia 2. Para executar tal monitoramento, a seção de controle principal 421 obtém constantemente as informações sobre a data e a hora atuais do temporizador 423.

Quando a seção de controle principal 421 detecta que o cronograma especificado pelas informações de especificação do cronograma contidas em uma parte dos dados criptografados chegou, a seção de controle principal 421 determina a transformação dos dados criptografados contendo as informações de especificação do cronograma em dados "inúteis".

O conteúdo do processamento executado após tal determinação da seção de controle principal 421 é o mesmo que no exemplo 1 executado após a determinação como descrita acima.

Exemplo 3: corresponde a um caso intermediário entre o exemplo 1 e o exemplo 2.

Como descrito acima, os dados criptografados nesta abordagem contêm as informações de especificação do cronograma.

O exemplo 3 é executado quando o usuário insere um comando para a descriptografia dos dados criptografados para o dispositivo de entrada 35 e a condição a seguir é satisfeita.

Quando o usuário insere o comando para a descriptografia dos dados criptografados, a entrada é transmitida através da unidade de controle de entrada 410 para a seção de controle principal 421.

A seção de controle principal 421, que recebeu a entrada, tem a função de ler as informações de especificação do cronograma contidas nos dados

criptografados especificados pelo comando. A seção de controle principal 421 determina se o cronograma especificado pelas informações de especificação do cronograma contidas nos dados criptografados chegou ou não, com base na comparação com a data e a hora atuais lidas do temporizador 423.

Se o cronograma especificado pelas informações de especificação do cronograma contidas nos dados criptografados ainda não chegou, a seção de controle principal 421 permite que o dispositivo de descriptografia 37 descriptografe os dados criptografados. Com tal permissão, o dispositivo de descriptografia 37 executa o processamento, como descrito acima, para descriptografar os dados criptografados.

Se o cronograma especificado pelas informações de especificação do cronograma contidas nos dados criptografados chegou, a seção de controle principal 421 determina a transformação dos dados criptografados em dados "inúteis".

O conteúdo do processamento executado após tal determinação da seção de controle principal 421 é o mesmo que no exemplo 1 após a determinação como descrita acima.

VARIAÇÃO

Uma variação do sistema de criptografia na primeira abordagem será descrita.

Uma configuração básica do sistema de criptografia na variação é fundamentalmente a mesma que a do sistema de criptografia na primeira abordagem. O sistema de criptografia, de acordo com a variação, difere do sistema de criptografia descrito acima em uma parte da configuração do dispositivo de criptografia 27 no aparelho de processamento de criptografia 1 e em uma parte da configuração do dispositivo de descriptografia 37 no aparelho de processamento de descriptografia 2.

O dispositivo de criptografia 27 no aparelho de processamento de criptografia 1, de acordo com a variação, é configurado como ilustrado na Figura

10.

O dispositivo de criptografia 27 contido no aparelho de processamento de criptografia 1 na variação difere daquele da primeira abordagem no sentido de que a unidade de geração de algoritmos 275 e a unidade de geração de chaves 276 são substituídas por uma unidade de armazenamento de algoritmos 281 e uma unidade de armazenamento de chaves 282, como ilustrado na Figura 10.

A unidade de armazenamento de algoritmos 281 armazena uma série de algoritmos, enquanto que a unidade de armazenamento de chaves 282 armazena uma série de chaves. O algoritmo é utilizado para a criptografia dos dados de textos simples divisionais na unidade de criptografia 273, enquanto que a chave é utilizada para a criptografia dos dados de textos simples divisionais na unidade de criptografia 273.

Na primeira abordagem, os algoritmos e as chaves são gerados continuamente a partir da unidade de geração de algoritmos 275 e da unidade de geração de chaves 276, com base nas soluções geradas pela unidade de geração de soluções 274. Nesta variação, entretanto, a série de algoritmos e a série de chaves são preparadas e armazenadas na unidade de armazenamento de algoritmos 281 e na unidade de armazenamento de chaves 282 como o algoritmo e a chave utilizados para a criptografia dos dados de textos simples divisionais, respectivamente. Especificamente nesta variação, a série de algoritmos ou chaves é preparada com antecedência. Como resultado, as séries de algoritmos e chaves são utilizadas para a criptografia dos dados de textos simples divisionais sem a geração de novos algoritmos ou chaves.

Para cada criptografia dos dados criptografados divisionais, o algoritmo e a chave apropriados são selecionados da série de algoritmos gravados na unidade de armazenamento de algoritmos 281 e da série de chaves gravadas na unidade de armazenamento de chaves 282. A seleção do algoritmo e da chave da série de algoritmos e chaves, que são utilizados para a criptografia de cada um dos dados criptografados divisionais, pode ser determinada de maneira

apropriada.

Nesta variação, o algoritmo e a chave são selecionados utilizando-se a solução da seguinte maneira.

Nesta variação, sempre que a unidade de criptografia 273 criptografar os dados de textos simples divisionais para obter os dados criptografados divisionais, a solução gerada como um número pseudo-aleatório é transmitida da unidade de geração de soluções 274 para a unidade de criptografia 273 antes da criptografia. A unidade de criptografia 273 utiliza a solução transmitida para selecionar um algoritmo da série de algoritmos gravados na unidade de armazenamento de algoritmos 281 e também uma chave da série de chaves gravadas na unidade de armazenamento de chaves 282 para, assim, criptografar os dados de textos simples divisionais utilizando o algoritmo e a chave selecionados. O algoritmo e a chave são selecionados utilizando-se a solução, por exemplo, da seguinte maneira.

Nesta variação, cada uma das séries de algoritmos gravados na unidade de armazenamento de algoritmos 281 possui um identificador de algoritmos que é um número contínuo. Semelhantemente, cada uma das séries de chaves gravadas na unidade de armazenamento de chaves 282 possui um identificador de chaves que é um número contínuo. Por exemplo, quando três algoritmos são armazenados na unidade de armazenamento de algoritmos 281, os identificadores de algoritmos 0, 1 e 2 são compartilhados com os algoritmos um a um. Semelhantemente, quando três chaves são gravadas na unidade de armazenamento de chaves 282, os identificadores de chaves 0, 1 e 2 são compartilhados com as chaves um a um. Nesta abordagem, a soma de todos os elementos (valores numéricos) da solução gerada como a matriz 8×8, como na primeira abordagem, é dividida por 3. A unidade de criptografia 273 seleciona o algoritmo e a chave associados ao identificador de algoritmos ou ao identificador de chaves que seja idêntico ao lembrete da divisão.

Nesta variação, a unidade de criptografia 273 transmite o identificador de

algoritmos compartilhado com o algoritmo ou o identificador de chaves compartilhado com a chave utilizado para a criptografia dos dados criptografados para a unidade de geração de informações de especificação 277, a qual utiliza o identificador transmitido como a informação de especificação. Como na primeira abordagem, a unidade de geração de informações de especificação 277 transmite a primeira informação de especificação para a unidade de geração de cabeçalhos 279 e as outras informações de especificação para a unidade de criptografia 273.

O dispositivo de descriptografia 37 no aparelho de processamento de descriptografia 2, de acordo com a variação, é configurado como ilustrado na Figura 11.

O dispositivo de descriptografia 37 é aproximadamente o mesmo que na primeira abordagem, mas difere do dispositivo de descriptografia 37 na primeira abordagem no sentido de que a unidade de geração de algoritmos 375 e a unidade de geração de chaves 376 são substituídas por uma unidade de armazenamento de algoritmos 381 e uma unidade de armazenamento de chaves 382. Esta alteração corresponde à alteração descrita acima no dispositivo de criptografia 27.

Como não há necessidade de gerar a solução no dispositivo de descriptografia 37 nesta variação, como descrito a seguir, a unidade de geração de soluções 374 é omitida, ao contrário da primeira abordagem.

A unidade de armazenamento de algoritmos 381 e a unidade de armazenamento de chaves 382, incluindo o conteúdo dos algoritmos e das chaves armazenados, são as mesmas que a unidade de armazenamento de algoritmos 281 e a unidade de armazenamento de chaves 282 no dispositivo de criptografia 27. A unidade de armazenamento de algoritmos 381 armazena uma série de algoritmos, enquanto que a unidade de armazenamento de chaves 382 armazena uma série de chaves. Os múltiplos algoritmos gravados na unidade de armazenamento de algoritmos 381 são compartilhados com os identificadores de algoritmos, que são números contínuos, respectivamente. Semelhantemente, as

múltiplas chaves gravadas na unidade de armazenamento de chaves 382 são compartilhadas com os identificadores de chaves, que são números contínuos, respectivamente.

O algoritmo é utilizado para a descriptografia dos dados criptografados divisionais na unidade de descriptografia 373, enquanto que a chave é utilizada para a descriptografia dos dados criptografados divisionais na unidade de descriptografia 373.

Em contraste com a primeira abordagem, os algoritmos e as chaves não são gerados continuamente nesta variação. Ao invés disso, a série de algoritmos gravados na unidade de armazenamento de algoritmos 381 e a série de chaves gravadas na unidade de armazenamento de chaves 382 são utilizadas para a descriptografia.

Na variação, na recepção da primeira informação de especificação lida a partir dos dados de cabeçalho da unidade de pré-processamento 372, a unidade de análise de informações de especificação 377 contida no dispositivo de descriptografia 37 transmite o identificador de algoritmos e o identificador de chaves indicados pela primeira informação de identificação para a unidade de descriptografia 373. A unidade de descriptografia 373, que recebeu o identificador de algoritmos e o identificador de chaves, lê o algoritmo associado ao identificador de algoritmos recebido e a chave associada ao identificador de chaves recebido da unidade de armazenamento de algoritmos 381 e da unidade de armazenamento de chaves 382, respectivamente, para descriptografar os dados criptografados divisionais utilizando o algoritmo e a chave lidos. Desta maneira, o algoritmo e a chave lidos, respectivamente, da unidade de armazenamento de algoritmos 381 e da unidade de armazenamento de chaves 382 são os mesmos que os utilizados para a criptografia dos dados criptografados divisionais no aparelho de processamento de criptografia 1.

Como na primeira abordagem, as informações de especificação contidas nos dados criptografados divisionais são transmitidas da unidade de

descriptografia 373 para a unidade de análise de informações de especificação 377 quando os dados criptografados divisionais são descriptografados, e o conteúdo das informações de especificação é transmitido da unidade de análise de informações de especificação 377 para a unidade de descriptografia 373 para ser utilizado para a descriptografia subseqüente dos dados criptografados divisionais.

REIVINDICAÇÕES

1. Um aparelho de processamento de informações para o processamento de dados criptografados que consiste em uma unidade de uma série de partes dos dados criptografados divisionais gerados pela criptografia de uma série de partes dos dados de textos simples divisionais utilizando uma série de chaves geradas pela divisão dos dados de textos simples a serem processados nos dados que são compostos por um número predeterminado de bits, pelo menos uma das chaves diferindo da(s) outra(s); os dados criptografados são novamente descriptografados nos dados a serem processados pela descriptografia dos dados criptografados divisionais em uma ordem predeterminada para conectar os dados descriptografados em uma unidade, cada parte dos dados criptografados divisionais, exceto o último dado criptografado divisional a ser descriptografado, contendo informações de especificação para a especificação de uma chave para a descriptografia do próximo dado criptografado divisional a ser descriptografado para permitir a descriptografia, o aparelho de processamento de informações compreende:

meios de gravação para a gravação dos dados criptografados;

meios de entrada do disparador de destruição para a entrada de informações do disparador de destruição para o início de um processamento a fim de evitar que os dados criptografados sejam descriptografados;

meios de detecção para a detecção do primeiro dado criptografado divisional correspondente ao dado criptografado divisional que é o primeiro a ser descriptografado em todos os dados criptografados divisionais dos dados criptografados; e

meios de processamento para a recepção de uma entrada das informações do disparador de destruição na entrada para fazer com que ocorra uma alteração irreversível no primeiro dado criptografado divisional detectado pelos meios de detecção nos dados criptografados gravados nos meios de

gravação.

2. Um aparelho de processamento de informações para o processamento de dados criptografados que consiste em uma unidade de uma série de partes dos dados criptografados divisionais gerados pela criptografia de uma série de partes dos dados de textos simples divisionais utilizando uma série de chaves geradas pela divisão dos dados de textos simples a serem processados nos dados que são compostos por um número predeterminado de bits, pelo menos uma das chaves diferindo da(s) outra(s); os dados criptografados são novamente descriptografados nos dados a serem processados pela descriptografia dos dados criptografados divisionais em uma ordem predeterminada para conectar os dados descriptografados em uma unidade, cada parte dos dados criptografados divisionais, exceto o último dado criptografado divisional a ser descriptografado, contendo informações de especificação para a especificação de uma chave para a descriptografia do próximo dado criptografado divisional a ser descriptografado para permitir a descriptografia, os dados criptografados contendo a primeira informação de especificação para a especificação da chave para a descriptografia do dado criptografado divisional a ser primeiro descriptografado, o aparelho de processamento de informações compreende:

meios de gravação para a gravação dos dados criptografados;

meios de entrada do disparador de destruição para a entrada de informações do disparador de destruição para o início de um processamento a fim evitar que os dados criptografados sejam descriptografados;

meios de detecção para a detecção da primeira informação de especificação contida nos dados criptografados ou do primeiro dado criptografado divisional correspondente ao dado criptografado divisional que é o primeiro a ser descriptografado dos dados criptografados; e

meios de processamento para a recepção de uma entrada das informações do disparador de destruição na entrada para fazer com que ocorra uma alteração irreversível na primeira informação de especificação ou no primeiro

dado criptografado divisional detectado pelos meios de detecção nos dados criptografados gravados nos meios de gravação.

3. Um aparelho de processamento de informações para o processamento de dados criptografados que consiste em uma unidade de uma série de partes dos dados criptografados divisionais gerados pela criptografia de uma série de partes dos dados de textos simples divisionais utilizando uma série de chaves geradas pela divisão dos dados de textos simples a serem processados nos dados que são compostos por um número predeterminado de bits, pelo menos uma das chaves diferindo da(s) outra(s); os dados criptografados são novamente descriptografados nos dados a serem processados pela descriptografia dos dados criptografados divisionais em uma ordem predeterminada para conectar os dados descriptografados em uma unidade, cada parte dos dados criptografados divisionais, exceto o último dado criptografado divisional a ser descriptografado, contendo informações de especificação para a especificação de uma chave para a descriptografia do próximo dado criptografado divisional a ser descriptografado para permitir a descriptografia, os dados criptografados contendo informações de especificação do cronograma para especificar o cronograma a fim de evitar que os dados criptografados sejam descriptografados, o aparelho de processamento de informações compreende:

meios de gravação para a gravação dos dados criptografados;

meios de leitura das informações de especificação do cronograma para a leitura das informações de especificação do cronograma dos dados criptografados;

meios de detecção para a detecção do primeiro dado criptografado divisional correspondente ao dado criptografado divisional que é o primeiro a ser descriptografado em todos os dados criptografados divisionais dos dados criptografados; e

meios de processamento para monitorar se o cronograma especificado pelas informações de especificação do cronograma lidas pelos meios de leitura

das informações de especificação do cronograma chegou ou não e causando uma alteração irreversível no primeiro dado criptografado divisional detectado pelos meios de detecção no caso de o cronograma ter chegado.

4. Um aparelho de processamento de informações para o processamento de dados criptografados que consiste em uma unidade de uma série de partes dos dados criptografados divisionais gerados pela criptografia de uma série de partes dos dados de textos simples divisionais utilizando uma série de chaves geradas pela divisão dos dados de textos simples a serem processados nos dados que são compostos por um número predeterminado de bits, pelo menos uma das chaves diferindo da(s) outra(s); os dados criptografados são novamente descriptografados nos dados a serem processados pela descriptografia dos dados criptografados divisionais em uma ordem predeterminada para conectar os dados descriptografados em uma unidade, cada parte dos dados criptografados divisionais, exceto o último dado criptografado divisional a ser descriptografado, contendo informações de especificação para a especificação de uma chave para a descriptografia do próximo dado criptografado divisional a ser descriptografado para permitir a descriptografia, os dados criptografados contendo a primeira informação de especificação para a especificação da chave para a descriptografia do dado criptografado divisional a ser primeiro descriptografado e as informações de especificação do cronograma para especificar o cronograma a fim de evitar que os dados criptografados sejam descriptografados, o aparelho de processamento de informações compreende:

meios de gravação para a gravação dos dados criptografados;

meios de leitura das informações de especificação do cronograma para a leitura das informações de especificação do cronograma dos dados criptografados;

meios de detecção para a detecção da primeira informação de especificação contida nos dados criptografados ou do primeiro dado criptografado divisional correspondente ao dado criptografado divisional que é o primeiro a ser

descriptografado em todos os dados criptografados divisionais dos dados criptografados; e

meios de processamento para monitorar se o cronograma especificado pelas informações de especificação do cronograma lidas pelos meios de leitura das informações de especificação do cronograma chegou ou não e causando uma alteração irreversível na primeira informação de especificação ou no primeiro dado criptografado divisional detectado pelos meios de detecção no caso de o cronograma ter chegado.

5. Um aparelho de processamento de informações para o processamento de dados criptografados que consiste em uma unidade de uma série de partes dos dados criptografados divisionais gerados pela criptografia de uma série de partes dos dados de textos simples divisionais utilizando uma série de chaves geradas pela divisão dos dados de textos simples a serem processados nos dados que são compostos por um número predeterminado de bits, pelo menos uma das chaves diferindo da(s) outra(s); os dados criptografados são novamente descriptografados nos dados a serem processados pela descriptografia dos dados criptografados divisionais em uma ordem predeterminada para conectar os dados descriptografados em uma unidade, cada parte dos dados criptografados divisionais, exceto o último dado criptografado divisional a ser descriptografado, contendo informações de especificação para a especificação de uma chave para a descriptografia do próximo dado criptografado divisional a ser descriptografado para permitir a descriptografia, os dados criptografados contendo informações de especificação do cronograma para especificar o cronograma a fim de evitar que os dados criptografados sejam descriptografados, o aparelho de processamento de informações compreende:

meios de gravação para a gravação dos dados criptografados;

meios de descriptografia capazes de descriptografar os dados criptografados;

meios de entrada do disparador de descriptografia para a entrada de

informações do disparador de descriptografia para o início da descriptografia dos dados criptografados;

meios de leitura das informações de especificação do cronograma para a leitura das informações de especificação do cronograma dos dados criptografados quando as informações do disparador de descriptografia forem inseridas dos meios de entrada do disparador de descriptografia;

meios de detecção para a detecção do primeiro dado criptografado divisional que é o primeiro dado criptografado divisional a ser descriptografado em todos os dados criptografados divisionais dos dados criptografados; e

meios de processamento para a recepção das informações de especificação do cronograma lidas pelos meios de leitura das informações de especificação do cronograma na entrada das informações do disparador de descriptografia para determinar se o cronograma especificado pelas informações de especificação do cronograma chegou ou não e permitir que os meios de descriptografia descriptografem os dados criptografados se o cronograma ainda não chegou e causando uma alteração irreversível no primeiro dado criptografado divisional detectado pelos meios de detecção no caso de o cronograma ter chegado.

6. Um aparelho de processamento de informações para o processamento de dados criptografados que consiste em uma unidade de uma série de partes dos dados criptografados divisionais gerados pela criptografia de uma série de partes dos dados de textos simples divisionais utilizando uma série de chaves geradas pela divisão dos dados de textos simples a serem processados nos dados que são compostos por um número predeterminado de bits, pelo menos uma das chaves diferindo da(s) outra(s); os dados criptografados são novamente descriptografados nos dados a serem processados pela descriptografia dos dados criptografados divisionais em uma ordem predeterminada para conectar os dados descriptografados em uma unidade, cada parte dos dados criptografados divisionais, exceto o último dado criptografado divisional a ser descriptografado,

contendo informações de especificação para a especificação de uma chave para a descriptografia do próximo dado criptografado divisional a ser descriptografado para permitir a descriptografia, os dados criptografados contendo a primeira informação de especificação para a especificação da chave para a descriptografia do dado criptografado divisional a ser primeiro descriptografado e as informações de especificação do cronograma para especificar o cronograma a fim de evitar que os dados criptografados sejam descriptografados, o aparelho de processamento de informações compreende:

meios de gravação para a gravação dos dados criptografados;

meios de descriptografia capazes de descriptografar os dados criptografados;

meios de entrada do disparador de descriptografia para a entrada de informações do disparador de descriptografia para o início da descriptografia dos dados criptografados;

meios de leitura das informações de especificação do cronograma para a leitura das informações de especificação do cronograma dos dados criptografados quando as informações do disparador de descriptografia forem inseridas dos meios de entrada do disparador de descriptografia;

meios de detecção para a detecção da primeira informação de especificação contida nos dados criptografados ou do primeiro dado criptografado divisional que é o primeiro a ser descriptografado em todos os dados criptografados divisionais; e

meios de processamento para a recepção das informações de especificação do cronograma lidas pelos meios de leitura das informações de especificação do cronograma na entrada das informações do disparador de descriptografia para determinar se o cronograma especificado pelas informações de especificação do cronograma chegou ou não e permitir que os meios de descriptografia descriptografem os dados criptografados se o cronograma ainda não chegou e causando uma alteração irreversível na primeira informação de

especificação ou no primeiro dado criptografado divisional detectado pelos meios de detecção no caso de o cronograma ter chegado.

7. Um aparelho de processamento de informações, de acordo com qualquer uma das reivindicações 1 a 6, caracterizado pelo fato de que os meios de processamento escrevem os dados apropriados sobre a primeira informação de especificação ou o primeiro dado criptografado divisional para causar a alteração irreversível na primeira informação de especificação ou no primeiro dado criptografado divisional.

8. Um aparelho de processamento de informações, de acordo com qualquer uma das Reivindicações 1 a 6, caracterizado pelo fato de que os meios de processamento convertem de maneira irreversível a primeira informação de especificação e o primeiro dado criptografado divisional para causar a alteração irreversível na primeira informação de especificação ou no primeiro dado criptografado divisional.

9. Um método de processamento de informações executado em um aparelho de processamento de informações, composto por meios de gravação, meios de entrada do disparador de destruição e meios de processamento, para o processamento de dados criptografados, que consiste em uma unidade de uma série de partes dos dados criptografados divisionais gerados pela criptografia de uma série de partes dos dados de textos simples divisionais utilizando uma série de chaves geradas pela divisão dos dados de textos simples a serem processados nos dados que são compostos por um número predeterminado de bits, pelo menos uma das chaves diferindo da(s) outra(s); os dados criptografados são novamente descriptografados nos dados a serem processados pela descriptografia dos dados criptografados divisionais em uma ordem predeterminada para conectar os dados descriptografados em uma unidade, cada parte dos dados criptografados divisionais, exceto o último dado criptografado divisional a ser descriptografado, contendo informações de especificação para a especificação de uma chave para a descriptografia do próximo dado criptografado

divisional a ser descriptografado para permitir a descriptografia, o método de processamento de informações compreende as etapas, executadas pelos meios de processamento, de:

gravação dos dados criptografados nos meios de gravação;

recepção de informações do disparador de destruição para o início de um processamento a fim evitar que os dados criptografados sejam descriptografados dos meios de entrada do disparador de destruição;

detecção do primeiro dado criptografado divisional que é o primeiro dado criptografado divisional a ser descriptografado em todos os dados criptografados divisionais dos dados criptografados; e

provocação de uma alteração irreversível no primeiro dado criptografado divisional detectado na etapa de detecção nos dados criptografados gravados nos meios de gravação quando as informações do disparador de destruição são recebidas.

10. Um método de processamento de informações executado em um aparelho de processamento de informações, composto por meios de gravação, meios de entrada do disparador de destruição e meios de processamento, para o processamento de dados criptografados, que consiste em uma unidade de uma série de partes dos dados criptografados divisionais gerados pela criptografia de uma série de partes dos dados de textos simples divisionais utilizando uma série de chaves geradas pela divisão dos dados de textos simples a serem processados nos dados que são compostos por um número predeterminado de bits, pelo menos uma das chaves diferindo da(s) outra(s); os dados criptografados são novamente descriptografados nos dados a serem processados pela descriptografia dos dados criptografados divisionais em uma ordem predeterminada para conectar os dados descriptografados em uma unidade, cada dado criptografado divisional, exceto o último dado criptografado divisional a ser descriptografado, contendo informações de especificação para a especificação de uma chave para a descriptografia do próximo dado criptografado divisional a ser

descriptografado para permitir a descriptografia, os dados criptografados contendo a primeira informação de especificação para a especificação da chave para a descriptografia do dado criptografado divisional a ser primeiro descriptografado, o método de processamento de informações compreende as etapas, executadas pelos meios de processamento, de:

gravação dos dados criptografados nos meios de gravação;

recepção de informações do disparador de destruição para o início de um processamento a fim de evitar que os dados criptografados sejam descriptografados dos meios de entrada do disparador de destruição;

detecção da primeira informação de especificação contida nos dados criptografados ou do primeiro dado criptografado divisional que é o primeiro a ser descriptografado em todos os dados criptografados divisionais dos dados criptografados; e

provocação de uma alteração irreversível na primeira informação de especificação ou no primeiro dado criptografado divisional detectado na etapa de detecção nos dados criptografados gravados nos meios de gravação quando as informações do disparador de destruição são recebidas.

11. Um método de processamento de informações executado em um aparelho de processamento de informações, composto por meios de gravação e meios de processamento, para o processamento de dados criptografados, que consiste em uma unidade de uma série de partes dos dados criptografados divisionais gerados pela criptografia de uma série de partes dos dados de textos simples divisionais utilizando uma série de chaves geradas pela divisão dos dados de textos simples a serem processados nos dados que são compostos por um número predeterminado de bits, pelo menos uma das chaves diferindo da(s) outra(s); os dados criptografados são novamente descriptografados nos dados a serem processados pela descriptografia dos dados criptografados divisionais em uma ordem predeterminada para conectar os dados descriptografados em uma unidade, cada parte dos dados criptografados divisionais, exceto o último dado

criptografado divisional a ser descriptografado, contendo informações de especificação para a especificação de uma chave para a descriptografia do próximo dado criptografado divisional a ser descriptografado para permitir a descriptografia, os dados criptografados contendo informações de especificação do cronograma para especificar o cronograma a fim de evitar que os dados criptografados sejam descriptografados, o método de processamento de informações compreende as etapas, executadas pelos meios de processamento, de:

gravação dos dados criptografados nos meios de gravação;

leitura das informações de especificação do cronograma dos dados criptografados;

detecção do primeiro dado criptografado divisional que é o primeiro dado criptografado divisional a ser descriptografado em todos os dados criptografados divisionais dos dados criptografados; e

monitorar se o cronograma especificado pelas informações de especificação do cronograma lidas na etapa de leitura chegou ou não e causando uma alteração irreversível no primeiro dado criptografado divisional detectado na etapa de detecção no caso de o cronograma ter chegado.

12. Um método de processamento de informações executado em um aparelho de processamento de informações, composto por meios de gravação e meios de processamento, para o processamento de dados criptografados, que consiste em uma unidade de uma série de partes dos dados criptografados divisionais gerados pela criptografia de uma série de partes dos dados de textos simples divisionais utilizando uma série de chaves geradas pela divisão dos dados de textos simples a serem processados nos dados que são compostos por um número predeterminado de bits, pelo menos uma das chaves diferindo da(s) outra(s); os dados criptografados são novamente descriptografados nos dados a serem processados pela descriptografia dos dados criptografados divisionais em uma ordem predeterminada para conectar os dados descriptografados em uma

unidade, cada parte dos dados criptografados divisionais, exceto o último dado criptografado divisional a ser descriptografado, contendo informações de especificação para a especificação de uma chave para a descriptografia do próximo dado criptografado divisional a ser descriptografado para permitir a descriptografia, os dados criptografados contendo a primeira informação de especificação para a especificação da chave para a descriptografia do dado criptografado divisional a ser primeiro descriptografado e as informações de especificação do cronograma para especificar o cronograma a fim de evitar que os dados criptografados sejam descriptografados, o método de processamento de informações compreende as etapas, executadas pelos meios de processamento, de:

gravação dos dados criptografados nos meios de gravação;

leitura das informações de especificação do cronograma dos dados criptografados;

detecção da primeira informação de especificação contida nos dados criptografados ou do primeiro dado criptografado divisional que é o primeiro a ser descriptografado em todos os dados criptografados divisionais dos dados criptografados; e

monitorar se o cronograma especificado pelas informações de especificação do cronograma lidas na etapa de leitura chegou ou não e causando uma alteração irreversível na primeira informação de especificação ou no primeiro dado criptografado divisional detectado na etapa de detecção no caso de o cronograma ter chegado.

13. Um método de processamento de informações executado em um aparelho de processamento de informações, composto por meios de gravação, meios de entrada do disparador de descriptografia e meios de processamento, para o processamento de dados criptografados, que consiste em uma unidade de uma série de partes dos dados criptografados divisionais gerados pela criptografia de uma série de partes dos dados de textos simples divisionais utilizando uma

série de chaves geradas pela divisão dos dados de textos simples a serem processados nos dados que são compostos por um número predeterminado de bits, pelo menos uma das chaves diferindo da(s) outra(s); os dados criptografados são novamente descriptografados nos dados a serem processados pela descriptografia dos dados criptografados divisionais em uma ordem predeterminada para conectar os dados descriptografados em uma unidade, cada parte dos dados criptografados divisionais, exceto o último dado criptografado divisional a ser descriptografado, contendo informações de especificação para a especificação de uma chave para a descriptografia do próximo dado criptografado divisional a ser descriptografado para permitir a descriptografia, os dados criptografados contendo informações de especificação do cronograma para especificar o cronograma a fim de evitar que os dados criptografados sejam descriptografados, o método de processamento de informações compreende as etapas, executadas pelos meios de processamento, de:

gravação dos dados criptografados nos meios de gravação;

recepção de informações do disparador de descriptografia para o início da descriptografia dos dados criptografados dos meios de entrada do disparador de descriptografia;

leitura das informações de especificação do cronograma dos dados criptografados quando ocorrer a etapa de recepção;

detecção do primeiro dado criptografado divisional que é o primeiro dado criptografado divisional a ser descriptografado em todos os dados criptografados divisionais dos dados criptografados; e

recepção das informações de especificação do cronograma lidas na etapa de leitura quando ocorrer a etapa de recepção para determinar se o cronograma especificado pelas informações de especificação do cronograma chegou ou não e descriptografar os dados criptografados se o cronograma ainda não chegou e causando uma alteração irreversível no primeiro dado criptografado divisional detectado na etapa de detecção no caso de o cronograma ter chegado.

14. Um método de processamento de informações executado em um aparelho de processamento de informações, composto por meios de gravação, meios de entrada do disparador de descriptografia e meios de processamento, para o processamento de dados criptografados, que consiste em uma unidade de uma série de partes dos dados criptografados divisionais gerados pela criptografia de uma série de partes dos dados de textos simples divisionais utilizando uma série de chaves geradas pela divisão dos dados de textos simples a serem processados nos dados que são compostos por um número predeterminado de bits, pelo menos uma das chaves diferindo da(s) outra(s); os dados criptografados são novamente descriptografados nos dados a serem processados pela descriptografia dos dados criptografados divisionais em uma ordem predeterminada para conectar os dados descriptografados em uma unidade, cada parte dos dados criptografados divisionais, exceto o último dado criptografado divisional a ser descriptografado, contendo informações de especificação para a especificação de uma chave para a descriptografia do próximo dado criptografado divisional a ser descriptografado para permitir a descriptografia, os dados criptografados contendo a primeira informação de especificação para a especificação da chave para a descriptografia do dado criptografado divisional a ser primeiro descriptografado e as informações de especificação do cronograma para especificar o cronograma a fim de evitar que os dados criptografados sejam descriptografados, o método de processamento de informações compreende as etapas, executadas pelos meios de processamento, de:

gravação dos dados criptografados nos meios de gravação;

recepção de informações do disparador de descriptografia para o início da descriptografia dos dados criptografados dos meios de entrada do disparador de descriptografia;

leitura das informações de especificação do cronograma dos dados criptografados quando ocorrer a etapa de recepção;

detecção da primeira informação de especificação contida nos dados

criptografados ou do primeiro dado criptografado divisional que é o primeiro a ser descriptografado em todos os dados criptografados divisionais dos dados criptografados; e

recepção das informações de especificação do cronograma lidas na etapa de leitura quando ocorrer a etapa de recepção para determinar se o cronograma especificado pelas informações de especificação do cronograma chegou ou não e descriptografar os dados criptografados se o cronograma ainda não chegou e causando uma alteração irreversível na primeira informação de especificação ou no primeiro dado criptografado divisional detectado na etapa de detecção no caso de o cronograma ter chegado.

15. Um programa computadorizado para o processamento de dados criptografados que consiste em uma unidade de uma série de partes dos dados criptografados divisionais gerados pela criptografia de uma série de partes dos dados de textos simples divisionais utilizando uma série de chaves geradas pela divisão dos dados de textos simples a serem processados nos dados que são compostos por um número predeterminado de bits, pelo menos uma das chaves diferindo da(s) outra(s); os dados criptografados são novamente descriptografados nos dados a serem processados pela descriptografia dos dados criptografados divisionais em uma ordem predeterminada para conectar os dados descriptografados em uma unidade, cada parte dos dados criptografados divisionais, exceto o último dado criptografado divisional a ser descriptografado, contendo informações de especificação para a especificação de uma chave para a descriptografia do próximo dado criptografado divisional a ser descriptografado para permitir a descriptografia, o programa computadorizado é caracterizado por fazer com que um computador contido em um aparelho de processamento de informações, composto por meios de gravação, meios de entrada do disparador de destruição e o computador também conectado, execute as etapas de:

gravação dos dados criptografados nos meios de gravação;

recepção de informações do disparador de destruição para o início de um

processamento a fim de evitar que os dados criptografados sejam descriptografados dos meios de entrada do disparador de destruição;

detecção do primeiro dado criptografado divisional que é o primeiro dado criptografado divisional a ser descriptografado em todos os dados criptografados divisionais dos dados criptografados; e

provocação de uma alteração irreversível no primeiro dado criptografado divisional detectado na etapa de detecção nos dados criptografados gravados nos meios de gravação quando as informações do disparador de destruição são recebidas.

16. Um programa computadorizado para o processamento de dados criptografados que consiste em uma unidade de uma série de partes dos dados criptografados divisionais gerados pela criptografia de uma série de partes dos dados de textos simples divisionais utilizando uma série de chaves geradas pela divisão dos dados de textos simples a serem processados nos dados que são compostos por um número predeterminado de bits, pelo menos uma das chaves diferindo da(s) outra(s); os dados criptografados são novamente descriptografados nos dados a serem processados pela descriptografia dos dados criptografados divisionais em uma ordem predeterminada para conectar os dados descriptografados em uma unidade, cada parte dos dados criptografados divisionais, exceto o último dado criptografado divisional a ser descriptografado, contendo informações de especificação para a especificação de uma chave para a descriptografia do próximo dado criptografado divisional a ser descriptografado para permitir a descriptografia, os dados criptografados contendo a primeira informação de especificação para a especificação da chave para a descriptografia do dado criptografado divisional a ser primeiro descriptografado, o programa computadorizado é caracterizado por fazer com que um computador contido em um aparelho de processamento de informações, composto por meios de gravação, meios de entrada do disparador de destruição e o computador também conectado, execute as etapas de:

gravação dos dados criptografados nos meios de gravação;

recepção de informações do disparador de destruição para o início de um processamento a fim de evitar que os dados criptografados sejam descriptografados dos meios de entrada do disparador de destruição;

detecção da primeira informação de especificação contida nos dados criptografados ou do primeiro dado criptografado divisional que é o primeiro a ser descriptografado em todos os dados criptografados divisionais dos dados criptografados; e

provocação de uma alteração irreversível na primeira informação de especificação ou no primeiro dado criptografado divisional detectado na etapa de detecção nos dados criptografados gravados nos meios de gravação quando as informações do disparador de destruição são recebidas.

17. Um programa computadorizado para o processamento de dados criptografados que consiste em uma unidade de uma série de partes dos dados criptografados divisionais gerados pela criptografia de uma série de partes dos dados de textos simples divisionais utilizando uma série de chaves geradas pela divisão dos dados de textos simples a serem processados nos dados que são compostos por um número predeterminado de bits, pelo menos uma das chaves diferindo da(s) outra(s); os dados criptografados são novamente descriptografados nos dados a serem processados pela descriptografia dos dados criptografados divisionais em uma ordem predeterminada para conectar os dados descriptografados em uma unidade, cada parte dos dados criptografados divisionais, exceto o último dado criptografado divisional a ser descriptografado, contendo informações de especificação para a especificação de uma chave para a descriptografia do próximo dado criptografado divisional a ser descriptografado para permitir a descriptografia, os dados criptografados contendo informações de especificação do cronograma para especificar o cronograma a fim de evitar que os dados criptografados sejam descriptografados, o programa computadorizado é caracterizado por fazer com que um computador contido em um aparelho de

processamento de informações, composto pelo computador conectado aos meios de gravação, execute as etapas de:

gravação dos dados criptografados nos meios de gravação;

leitura das informações de especificação do cronograma dos dados criptografados;

detecção do primeiro dado criptografado divisional que é o primeiro dado criptografado divisional a ser descriptografado em todos os dados criptografados divisionais dos dados criptografados; e

monitorar se o cronograma especificado pelas informações de especificação do cronograma lidas na etapa de leitura chegou ou não e causando uma alteração irreversível no primeiro dado criptografado divisional detectado na etapa de detecção no caso de o cronograma ter chegado.

18. Um programa computadorizado para o processamento de dados criptografados que consiste em uma unidade de uma série de partes dos dados criptografados divisionais gerados pela criptografia de uma série de partes dos dados de textos simples divisionais utilizando uma série de chaves geradas pela divisão dos dados de textos simples a serem processados nos dados que são compostos por um número predeterminado de bits, pelo menos uma das chaves diferindo da(s) outra(s); os dados criptografados são novamente descriptografados nos dados a serem processados pela descriptografia dos dados criptografados divisionais em uma ordem predeterminada para conectar os dados descriptografados em uma unidade, cada parte dos dados criptografados divisionais, exceto o último dado criptografado divisional a ser descriptografado, contendo informações de especificação para a especificação de uma chave para a descriptografia do próximo dado criptografado divisional a ser descriptografado para permitir a descriptografia, os dados criptografados contendo a primeira informação de especificação para a especificação da chave para a descriptografia do dado criptografado divisional a ser primeiro descriptografado e as informações de especificação do cronograma para especificar o cronograma a fim de evitar

que os dados criptografados sejam descriptografados, o programa computadorizado é caracterizado por fazer com que um computador contido em um aparelho de processamento de informações, composto pelo computador conectado aos meios de gravação, execute as etapas de:

gravação dos dados criptografados nos meios de gravação;

leitura das informações de especificação do cronograma dos dados criptografados;

detecção da primeira informação de especificação contida nos dados criptografados ou do primeiro dado criptografado divisional que é o primeiro a ser descriptografado em todos os dados criptografados divisionais dos dados criptografados; e

monitorar se o cronograma especificado pelas informações de especificação do cronograma lidas na etapa de leitura chegou ou não e causando uma alteração irreversível na primeira informação de especificação ou no primeiro dado criptografado divisional detectado na etapa de detecção no caso de o cronograma ter chegado.

19. Um programa computadorizado para o processamento de dados criptografados que consiste em uma unidade de uma série de partes dos dados criptografados divisionais gerados pela criptografia de uma série de partes dos dados de textos simples divisionais utilizando uma série de chaves geradas pela divisão dos dados de textos simples a serem processados nos dados que são compostos por um número predeterminado de bits, pelo menos uma das chaves diferindo da(s) outra(s); os dados criptografados são novamente descriptografados nos dados a serem processados pela descriptografia dos dados criptografados divisionais em uma ordem predeterminada para conectar os dados descriptografados em uma unidade, cada parte dos dados criptografados divisionais, exceto o último dado criptografado divisional a ser descriptografado, contendo informações de especificação para a especificação de uma chave para a descriptografia do próximo dado criptografado divisional a ser descriptografado

para permitir a descriptografia, os dados criptografados contendo informações de especificação do cronograma para especificar o cronograma a fim de evitar que os dados criptografados sejam descriptografados, o programa computadorizado é caracterizado por fazer com que um computador contido em um aparelho de processamento de informações, composto por meios de gravação, meios de entrada do disparador de descriptografia e o computador também conectado, execute as etapas de:

gravação dos dados criptografados nos meios de gravação;

recepção de informações do disparador de descriptografia para o início da descriptografia dos dados criptografados dos meios de entrada do disparador de descriptografia;

leitura das informações de especificação do cronograma dos dados criptografados quando ocorrer a etapa de recepção;

detecção do primeiro dado criptografado divisional que é o primeiro dado criptografado divisional a ser descriptografado em todos os dados criptografados divisionais dos dados criptografados; e

recepção das informações de especificação do cronograma lidas na etapa de leitura quando ocorrer a etapa de recepção para determinar se o cronograma especificado pelas informações de especificação do cronograma chegou ou não e descriptografar os dados criptografados se o cronograma ainda não chegou e causando uma alteração irreversível no primeiro dado criptografado divisional detectado na etapa de detecção no caso de o cronograma ter chegado.

20. Um programa computadorizado para o processamento de dados criptografados que consiste em uma unidade de uma série de partes dos dados criptografados divisionais gerados pela criptografia de uma série de partes dos dados de textos simples divisionais utilizando uma série de chaves geradas pela divisão dos dados de textos simples a serem processados nos dados que são compostos por um numero predeterminado de bits, pelo menos uma das chaves diferindo da(s) outra(s); os dados criptografados são novamente

descriptografados nos dados a serem processados pela descriptografia dos dados criptografados divisionais em uma ordem predeterminada para conectar os dados descriptografados em uma unidade, cada parte dos dados criptografados divisionais, exceto o último dado criptografado divisional a ser descriptografado, contendo informações de especificação para a especificação de uma chave para a descriptografia do próximo dado criptografado divisional a ser descriptografado para permitir a descriptografia, os dados criptografados contendo a primeira informação de especificação para a especificação da chave para a descriptografia do dado criptografado divisional a ser primeiro descriptografado e as informações de especificação do cronograma para especificar o cronograma a fim de evitar que os dados criptografados sejam descriptografados, o programa computadorizado é caracterizado por fazer com que um computador contido em um aparelho de processamento de informações, composto por meios de gravação, meios de entrada do disparador de descriptografia e o computador também conectado, execute as etapas de:

gravação dos dados criptografados nos meios de gravação;

recepção de informações do disparador de descriptografia para o início da descriptografia dos dados criptografados dos meios de entrada do disparador de descriptografia;

leitura das informações de especificação do cronograma dos dados criptografados quando ocorrer a etapa de recepção;

detecção da primeira informação de especificação contida nos dados criptografados ou do primeiro dado criptografado divisional que é o primeiro a ser descriptografado em todos os dados criptografados divisionais dos dados criptografados; e

recepção das informações de especificação do cronograma lidas na etapa de leitura quando ocorrer a etapa de recepção para determinar se o cronograma especificado pelas informações de especificação do cronograma chegou ou não e descriptografar os dados criptografados se o cronograma ainda não chegou e

causando uma alteração irreversível na primeira informação de especificação ou no primeiro dado criptografado divisional detectado na etapa de detecção no caso de o cronograma ter chegado.

21. Um aparelho de processamento de informações para o processamento de dados criptografados obtidos pela criptografia dos dados de textos simples a serem processados, os dados criptografados contendo informações de especificação para a descriptografia dos dados criptografados, compreendendo:

meios de gravação para a gravação dos dados criptografados;

meios de detecção para a detecção das informações de especificação dos dados criptografados; e

meios de processamento para causar uma alteração irreversível nas informações de especificação detectadas pelos meios de detecção nos dados criptografados gravados nos meios de gravação quando uma condição predeterminada é satisfeita.

22. Um método de processamento de informações para o processamento de dados criptografados obtidos pela criptografia dos dados de textos simples a serem processados, os dados criptografados contendo informações de especificação para a descriptografia dos dados criptografados, o método de processamento de informações sendo executado em um aparelho de processamento de informações composto pelos meios de gravação e pelos meios de processamento, o método de processamento de informações compreende as etapas, executadas pelos meios de processamento, de:

gravação dos dados criptografados nos meios de gravação;

detecção das informações de especificação dos dados criptografados; e

provocação de uma alteração irreversível nas informações de especificação detectadas na etapa de detecção nos dados criptografados gravados nos meios de gravação quando uma condição predeterminada é satisfeita.

23. Um programa computadorizado para o processamento de dados criptografados obtidos pela criptografia dos dados de textos simples a serem processados, os dados criptografados contendo informações de especificação para a descriptografia dos dados criptografados, o programa computadorizado é caracterizado por fazer com que um computador contido em um aparelho de processamento de informações, composto por meios de gravação e o computador também conectado, execute as etapas de:

gravação dos dados criptografados nos meios de gravação;

detecção das informações de especificação dos dados criptografados; e

provocação de uma alteração irreversível nas informações de especificação detectadas na etapa de detecção nos dados criptografados gravados nos meios de gravação quando uma condição predeterminada é satisfeita.

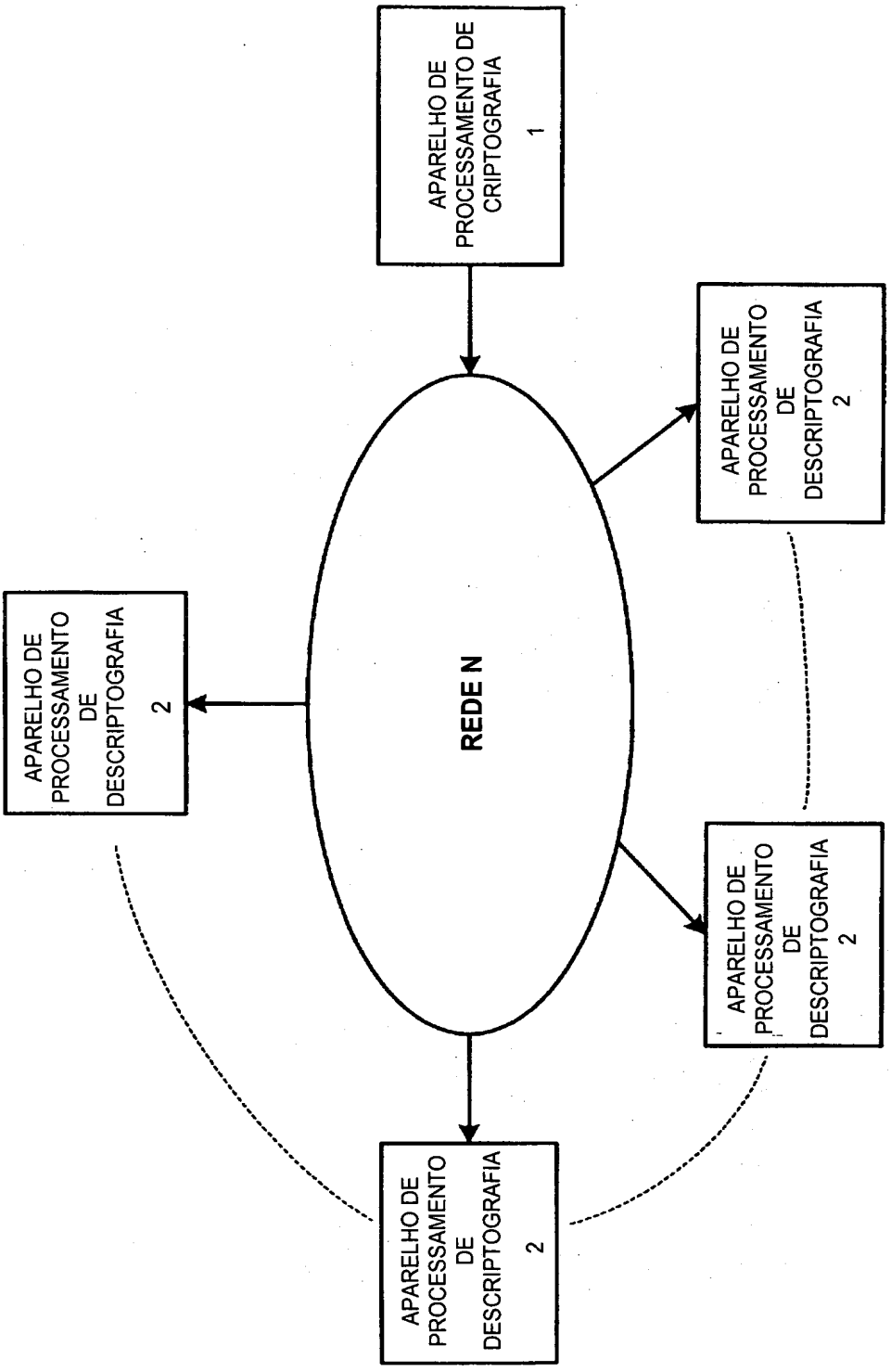
APARELHO DE PROCESSAMENTO DE CRIPTOGRAFIA 1
APARELHO DE PROCESSAMENTO DE DESCRIPTOGRAFIA 2
APARELHO DE PROCESSAMENTO DE DESCRIPTOGRAFIA 2
REDE N
APARELHO DE PROCESSAMENTO DE DESCRIPTOGRAFIA 2
APARELHO DE PROCESSAMENTO DE DESCRIPTOGRAFIA 2

FIG. 1

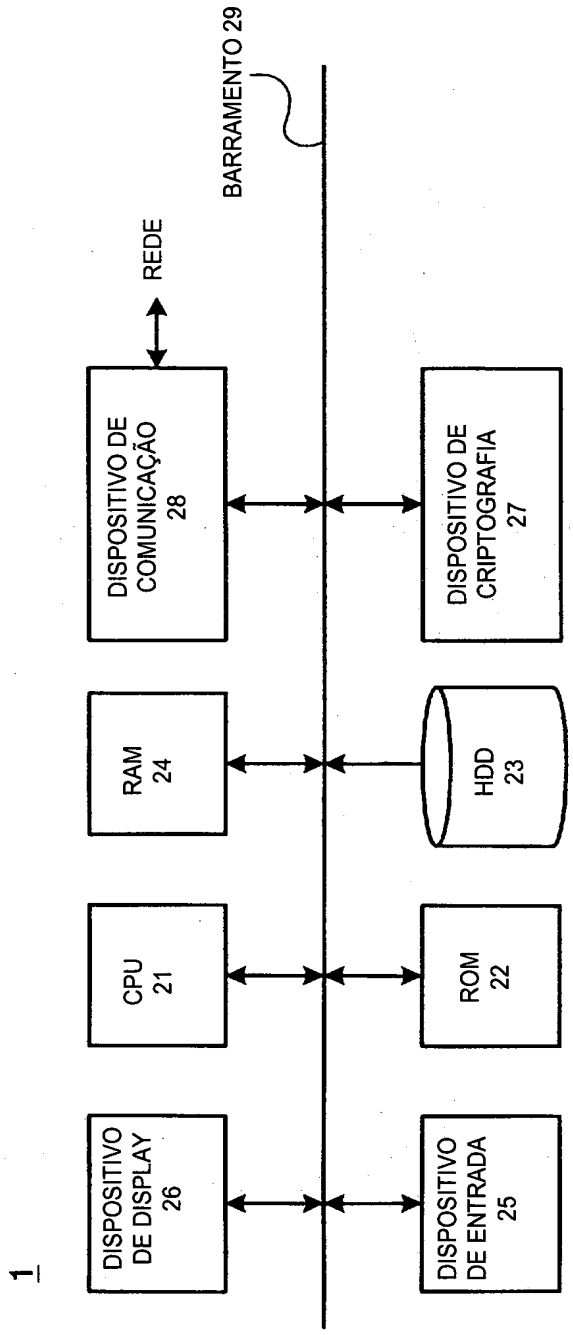
1
DISPOSITIVO DE DISPLAY 26
CPU 21
RAM 24
DISPOSITIVO DE COMUNICAÇÃO 28
REDE
BARRAMENTO 29
DISPOSITIVO DE ENTRADA 25
ROM 22
HDD 23
DISPOSITIVO DE CRIPTOGRAFIA 27

FIG. 2

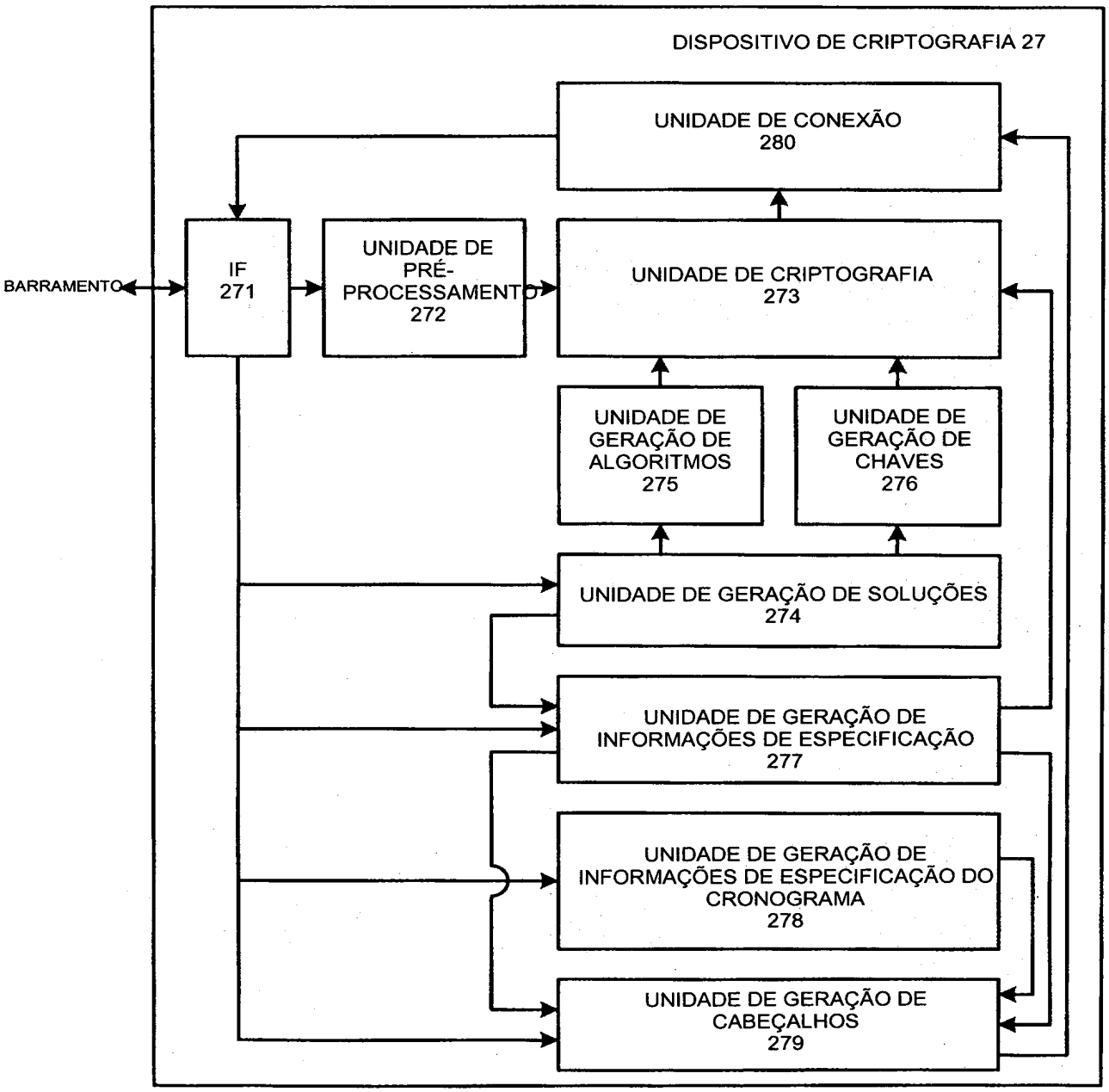
DISPOSITIVO DE CRIPTOGRAFIA 27
UNIDADE DE CONEXÃO
280
BARRAMENTO
IF
271
UNIDADE DE
PRÉ-
PROCESSAMENTO
272
UNIDADE DE CRIPTOGRAFIA
273
UNIDADE DE
GERAÇÃO DE
ALGORITMOS
275
UNIDADE DE
GERAÇÃO DE
CHAVES
276
UNIDADE DE GERAÇÃO DE SOLUÇÕES
274
UNIDADE DE GERAÇÃO DE
INFORMAÇÕES DE ESPECIFICAÇÃO
277
UNIDADE DE GERAÇÃO DE
INFORMAÇÕES DE ESPECIFICAÇÃO DO
CRONOGRAMA
278
UNIDADE DE GERAÇÃO DE
CABEÇALHOS
279

FIG. 3

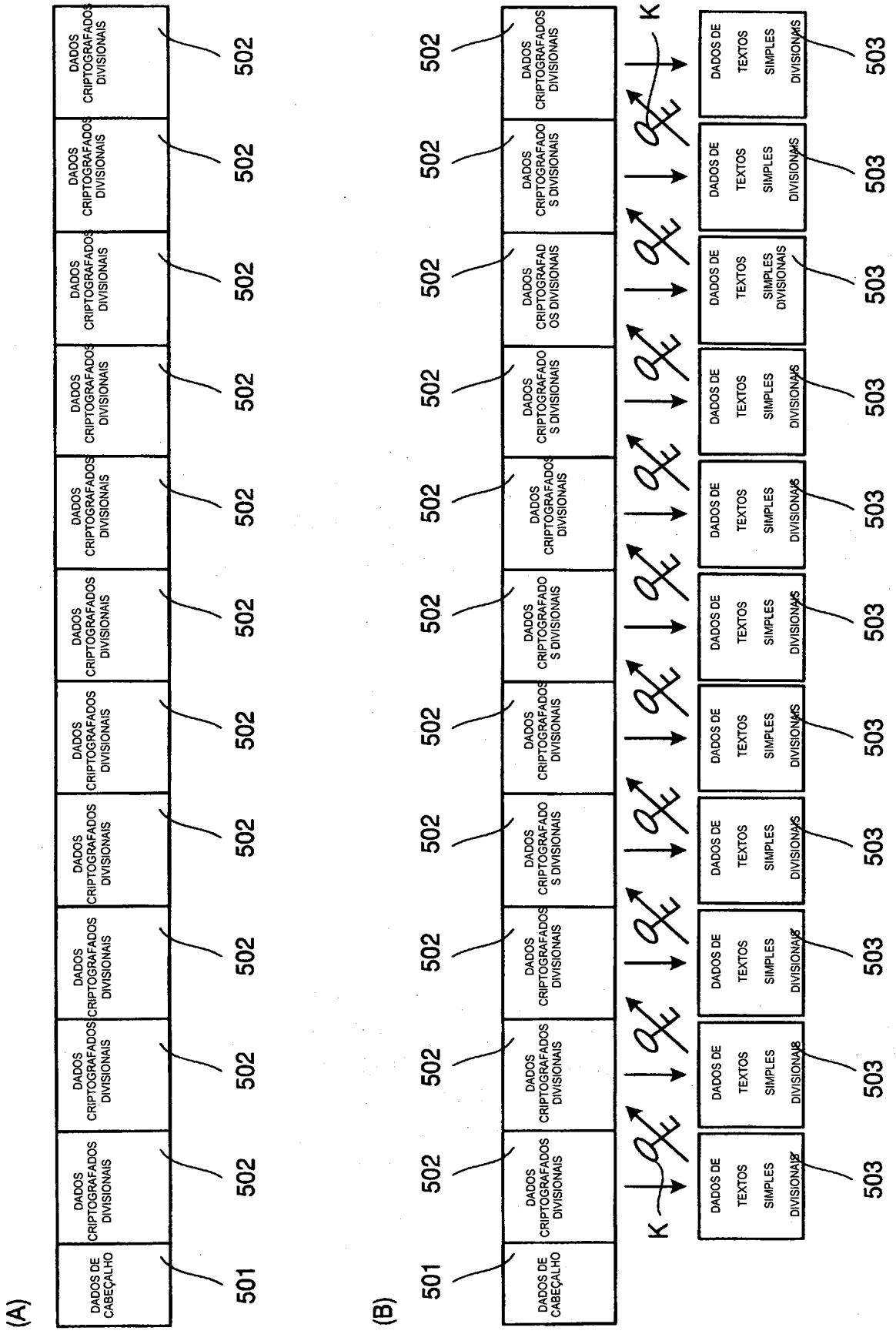
(A)
DADOS DE CABEÇALHO
DADOS CRIPTOGRAFADOS DIVISIONAIS
501
502
(B)
K
DADOS DE TEXTOS SIMPLES DIVISIONAIS
503

FIG. 4

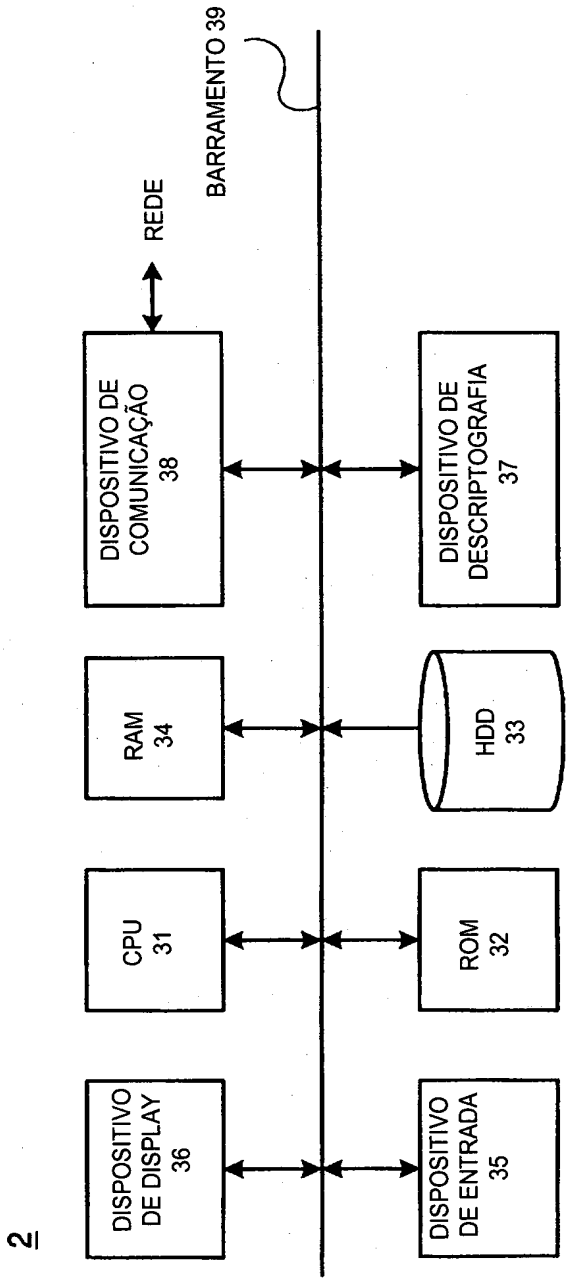
2
DISPOSITIVO DE DISPLAY 36
CPU 31
RAM 34
DISPOSITIVO DE COMUNICAÇÃO 38
REDE
BARRAMENTO 39
DISPOSITIVO DE ENTRADA 35
ROM 32
HDD 33
DISPOSITIVO DE DESCRIPTOGRAFIA 37

FIG. 5

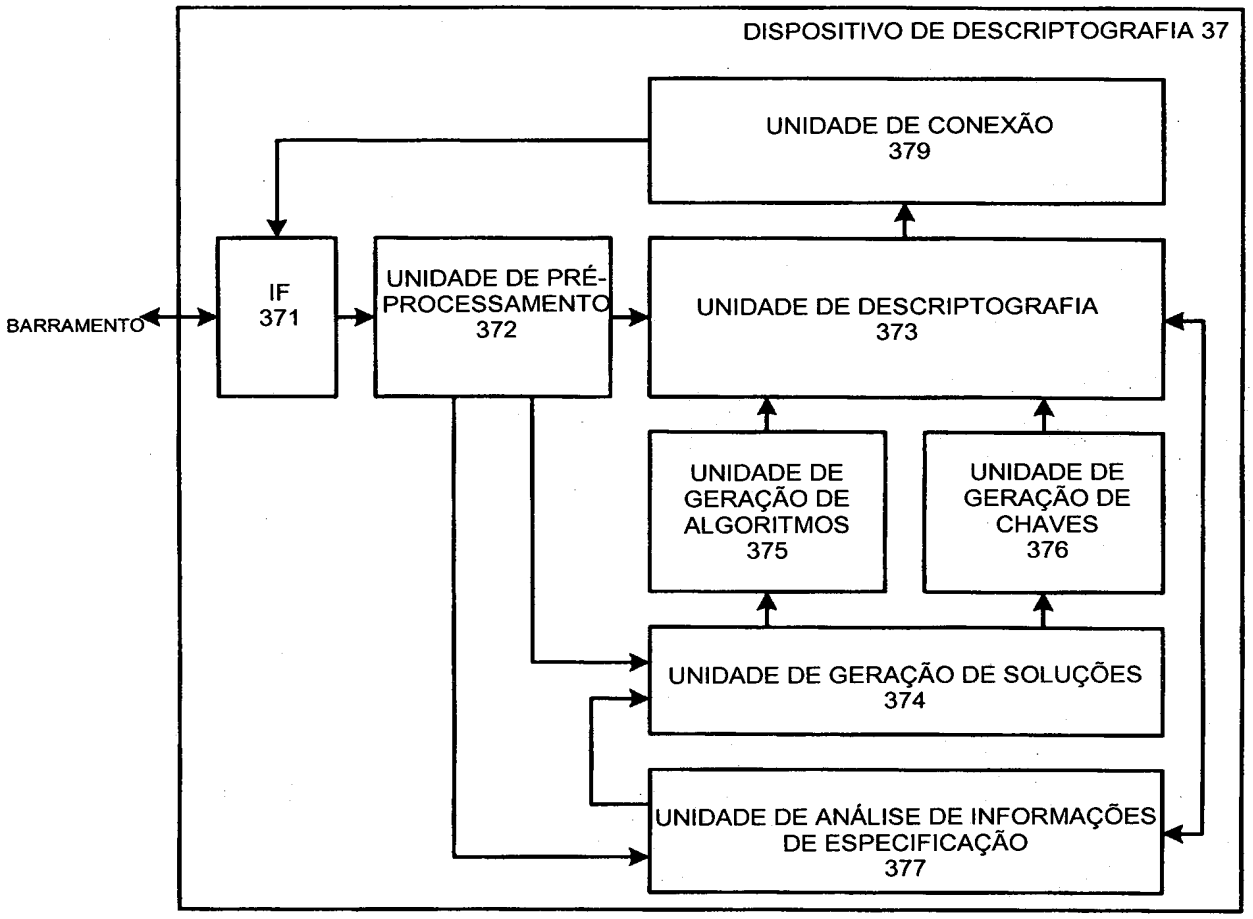
DISPOSITIVO DE DESCRIPTOGRAFIA 37
UNIDADE DE CONEXÃO
379
BARRAMENTO
IF
371
UNIDADE DE PRÉ-PROCESSAMENTO
372
UNIDADE DE DESCRIPTOGRAFIA
373
UNIDADE DE GERAÇÃO DE ALGORITMOS
375
UNIDADE DE GERAÇÃO DE CHAVES
376
UNIDADE DE GERAÇÃO DE SOLUÇÕES
374
UNIDADE DE ANÁLISE DE INFORMAÇÕES DE ESPECIFICAÇÃO
377

FIG. 6

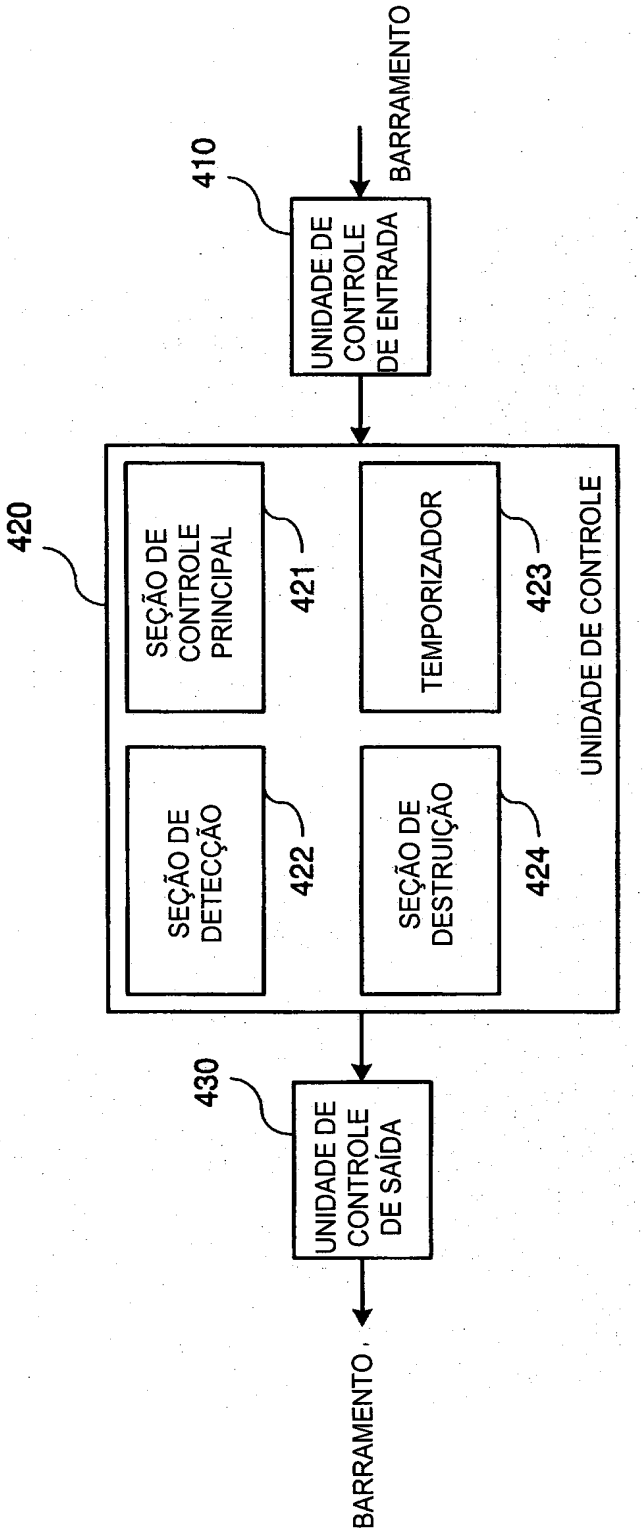
BARRAMENTO
410
UNIDADE DE CONTROLE DE ENTRADA
420
SEÇÃO DE CONTROLE PRINCIPAL
421
TEMPORIZADOR
423
SEÇÃO DE DETECÇÃO
422
SEÇÃO DE DESTRUIÇÃO
424
UNIDADE DE CONTROLE
430
UNIDADE DE CONTROLE DE SAÍDA
BARRAMENTO

FIG. 7

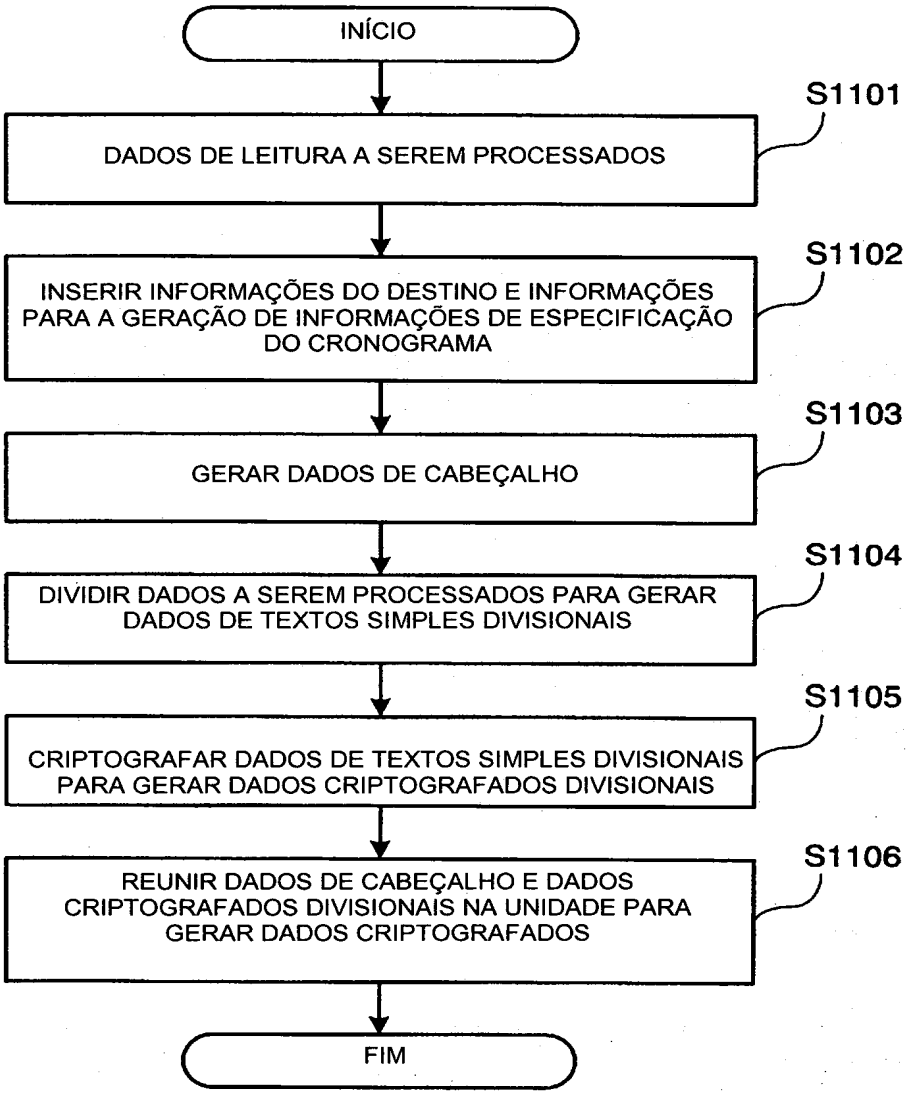
INÍCIO
S1101
DADOS DE LEITURA A SEREM PROCESSADOS
S1102
INSERIR INFORMAÇÕES DO DESTINO E INFORMAÇÕES PARA A GERAÇÃO DE INFORMAÇÕES DE ESPECIFICAÇÃO DO CRONOGRAMA
S1103
GERAR DADOS DE CABEÇALHO
S1104
DIVIDIR DADOS A SEREM PROCESSADOS PARA GERAR DADOS DE TEXTOS SIMPLES DIVISIONAIS
S1105
CRIPTOGRAFAR DADOS DE TEXTOS SIMPLES DIVISIONAIS PARA GERAR DADOS CRIPTOGRAFADOS DIVISIONAIS
S1106
REUNIR DADOS DE CABEÇALHO E DADOS CRIPTOGRAFADOS DIVISIONAIS NA UNIDADE PARA GERAR DADOS CRIPTOGRAFADOS
FIM

FIG. 8

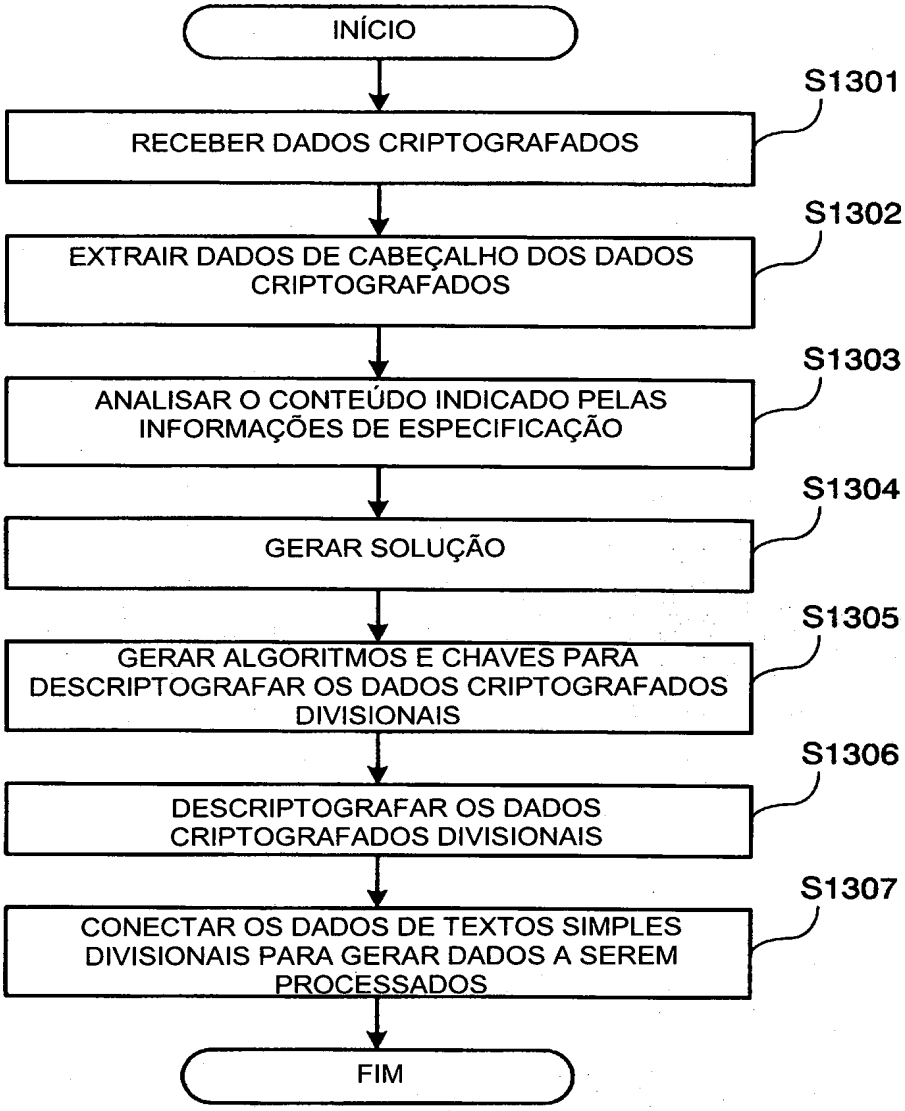
INÍCIO
S1301
RECEBER DADOS CRIPTOGRAFADOS
S1302
EXTRAIR DADOS DE CABEÇALHO DOS DADOS CRIPTOGRAFADOS
S1303
ANALISAR O CONTEÚDO INDICADO PELAS INFORMAÇÕES DE ESPECIFICAÇÃO
S1304
GERAR SOLUÇÃO
S1305
GERAR ALGORITMOS E CHAVES PARA DESCRIPTOGRAFAR OS DADOS CRIPTOGRAFADOS DIVISIONAIS
S1306
DESCRIPTOGRAFAR OS DADOS CRIPTOGRAFADOS DIVISIONAIS
S1307
CONECTAR OS DADOS DE TEXTOS SIMPLES DIVISIONAIS PARA GERAR DADOS A SEREM PROCESSADOS
FIM

FIG. 9

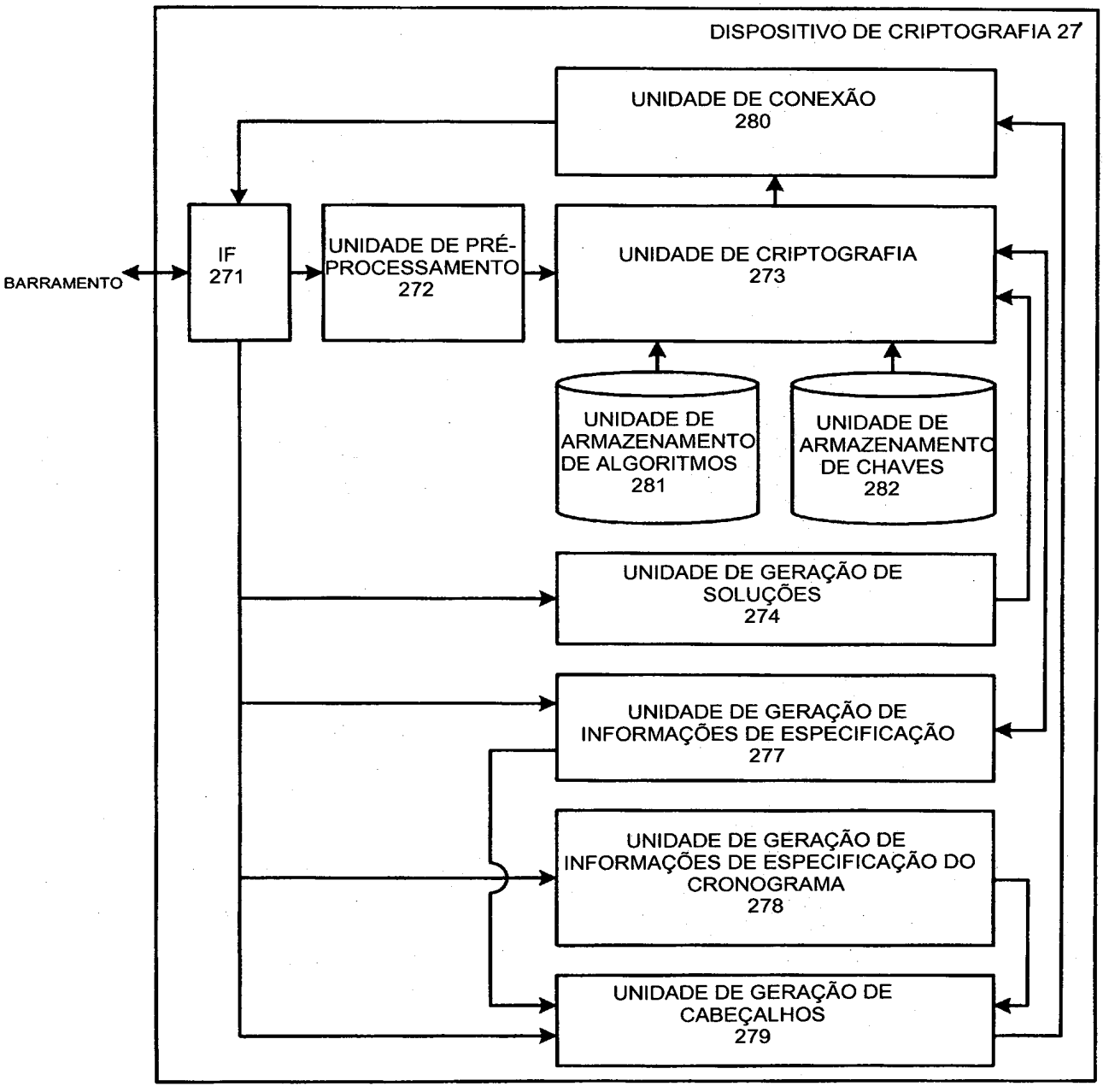
DISPOSITIVO DE CRIPTOGRAFIA 27
UNIDADE DE CONEXÃO
280
BARRAMENTO
IF
271
UNIDADE DE PRÉ-PROCESSAMENTO
272
UNIDADE DE CRIPTOGRAFIA
273
UNIDADE DE ARMAZENAMENTO DE ALGORITMOS
281
UNIDADE DE ARMAZENAMENTO DE CHAVES
282
UNIDADE DE GERAÇÃO DE SOLUÇÕES
274
UNIDADE DE GERAÇÃO DE INFORMAÇÕES DE ESPECIFICAÇÃO
277
UNIDADE DE GERAÇÃO DE INFORMAÇÕES DE ESPECIFICAÇÃO DO CRONOGRAMA
278
UNIDADE DE GERAÇÃO DE CABEÇALHOS
279

FIG. 10

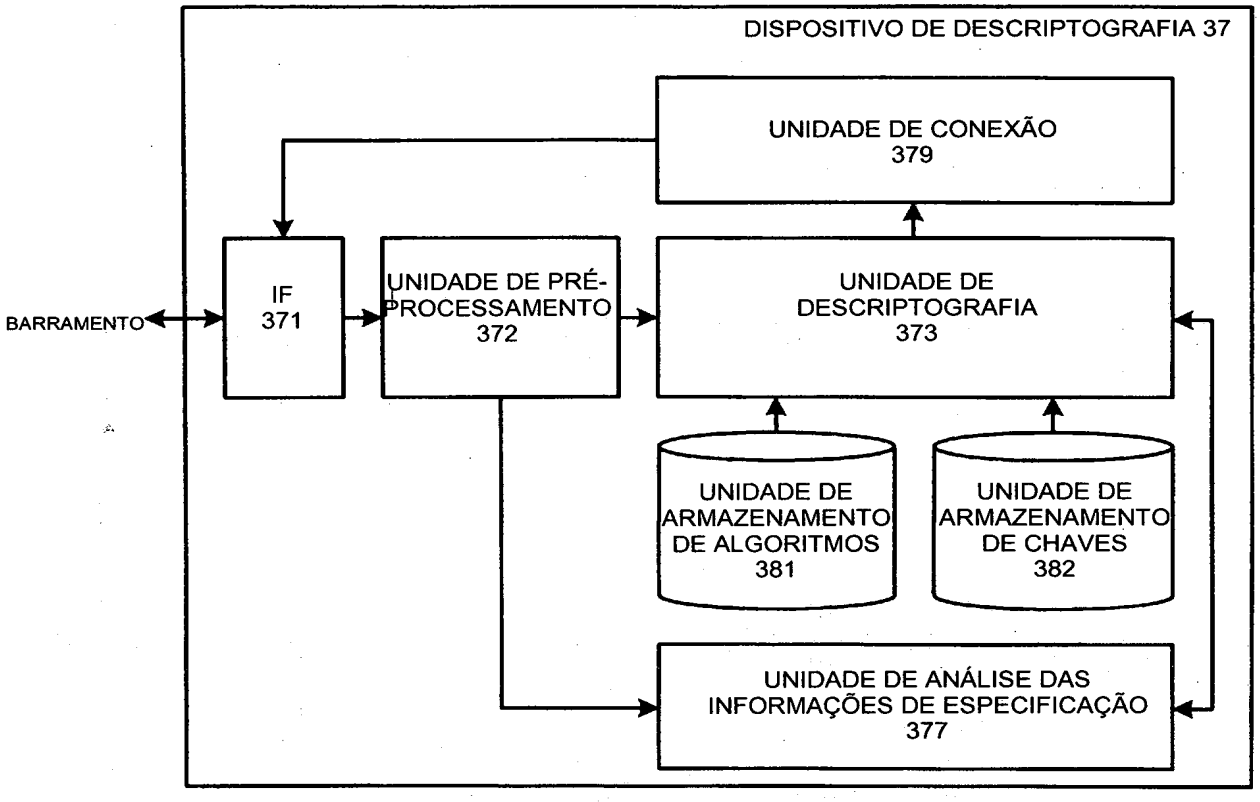
DISPOSITIVO DE DESCRIPTOGRAFIA 37
UNIDADE DE CONEXÃO
379
BARRAMENTO
IF
371
UNIDADE DE PRÉ-PROCESSAMENTO
372
UNIDADE DE DESCRIPTOGRAFIA
373
UNIDADE DE ARMAZENAMENTO DE ALGORITMOS
381
UNIDADE DE ARMAZENAMENTO DE CHAVES
382
UNIDADE DE ANÁLISE DAS INFORMAÇÕES DE ESPECIFICAÇÃO
377

FIG. 11

Resumo da Patente de Invenção para: **"DISPOSITIVO DE PROCESSAMENTO DE INFORMAÇÕES, MÉTODO DE PROCESSAMENTO DE INFORMAÇÕES E PROGRAMA COMPUTADORIZADO"**

Os dados criptografados são impedidos de ser descriptografados para evitar a perda de dados. Os dados criptografados obtidos pela criptografia dos dados a serem processados correspondem a uma relação de dados de cabeçalho (501) e múltiplos dados criptografados divisionais (502). Cada um dos dados criptografados divisionais (502), exceto o último, contém informações indispensáveis para a descriptografia do próximo dado criptografado divisional (502). Na presente invenção, o primeiro dado criptografado divisional (502) é destruído no cronograma apropriado para evitar que os dados criptografados sejam descriptografados.