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

(21) PI 0719642-3 A2

* B R P I 0 7 1 9 6 4 2 A 2 *

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

(51) Int.Cl.:
H04L 9/14
H04L 9/26

(54) Título: DISPOSITIVO PROCESSADOR DE DESCODIFICAÇÃO, MÉTODO PROCESSADOR DE DADOS E PROGRAMA DE COMPUTADOR

(57) Resumo:

(30) Prioridade Unionista: 28/12/2006 JP 2006-356595

(73) Titular(es): N-Crypt, INC.

(72) Inventor(es): TAKATOSHI NAKAMURA

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

(86) Pedido Internacional: PCT JP2007075375 de 26/12/2007

(87) Publicação Internacional: WO 2008/081974de 10/07/2008

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

CAMPO DA INVENÇÃO

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

FUNDAMENTO 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 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 é relativo 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 "inúteis" não significativos assim 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 a fim de 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 primeira à terceira invenções.

A primeira invenção refere-se a um aparelho de processamento de descriptografia utilizado juntamente com um aparelho de processamento de criptografia para a criptografia de dados de textos simples a serem processados para obter dados criptografados, o aparelho de processamento de criptografia contém: meios de divisão para a divisão dos dados a serem processados em uma série de partes dos dados de textos simples divisionais, cada um sendo composto por um número predeterminado de bits; meios de geração de soluções para a geração contínua de soluções, cada uma sendo determinada exclusivamente com base em soluções anteriores, os meios de geração de soluções armazenando uma solução inicial utilizada para gerar uma primeira solução para a geração contínua das soluções; meios de criptografia para a criptografia dos dados de textos simples divisionais utilizando as soluções para converter os dados de textos simples divisionais em dados criptografados divisionais; e meios de conexão para a conexão dos dados criptografados divisionais para obter os dados criptografados.

Adicionalmente, o aparelho de processamento de descriptografia inclui uma unidade de descriptografia que contém: meios de divisão para a divisão dos dados criptografados em uma série de partes dos dados criptografados divisionais, cada um sendo composto por um número predeterminado de bits; meios de geração de soluções para a geração contínua de soluções, cada uma sendo determinada exclusivamente com base em soluções anteriores, as soluções sendo geradas como as mesmas soluções geradas no aparelho de processamento de criptografia, os meios de geração de soluções armazenando

uma solução inicial utilizada para gerar uma primeira solução para a geração contínua das soluções; meios de descriptografia para a descriptografia dos dados criptografados divisionais utilizando as soluções para converter os dados criptografados divisionais em dados de textos simples divisionais; e meios de conexão para a conexão dos dados de textos simples divisionais para obter os dados a serem processados; 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; e meios de processamento para a destruição de uma solução gerada antes das soluções utilizadas para a descriptografia dos dados criptografados de maneira irreversível quando as informações do disparador de destruição são inseridas, a solução anterior sendo necessária para a geração das soluções utilizadas para a descriptografia dos dados criptografados.

O aparelho de processamento de descriptografia, como descrito acima, é utilizado juntamente com um aparelho de processamento de criptografia para a criptografia de dados de textos simples a serem processados para obter dados criptografados, o aparelho de processamento de criptografia contém: meios de divisão para a divisão dos dados a serem processados em uma série de partes dos dados de textos simples divisionais, cada um sendo composto por um número predeterminado de bits; meios de geração de soluções para a geração contínua de soluções, cada uma sendo determinada exclusivamente com base em soluções anteriores, os meios de geração de soluções armazenando uma solução inicial utilizada para gerar uma primeira solução para a geração contínua das soluções; meios de criptografia para a criptografia dos dados de textos simples divisionais utilizando as soluções para converter os dados de textos simples divisionais em dados criptografados divisionais; e meios de conexão para a conexão dos dados criptografados divisionais para obter os dados criptografados.

No caso em que o aparelho de processamento de descriptografia descriptografa os dados criptografados obtidos pela criptografia dos dados a

serem processados no aparelho de processamento de criptografia, a mesma solução que é usada no aparelho de processamento de criptografia é indispensável (a quantidade de soluções necessárias para a descriptografia dos dados criptografados é uma em alguns casos e várias em outros casos). Na invenção, as soluções geradas no aparelho de processamento de descriptografia (e também as soluções geradas no aparelho de processamento de criptografia) são geradas continuamente utilizando-se as soluções anteriores. Portanto, quando o aparelho de processamento de descriptografia deve descriptografar uma parte dos dados criptografados, a parte dos dados criptografados não pode ser descriptografada se uma alteração irreversível for causada na solução gerada antes da solução necessária para a descriptografia da parte dos dados criptografados, que deve ser utilizada para a geração da solução necessária para a descriptografia da parte dos dados criptografados. O aparelho de processamento de descriptografia, de acordo com essa invenção, causa a alteração irreversível na solução, como descrito acima, na entrada das informações do disparador de destruição. 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.

A quantidade de soluções anteriores, nas quais a alteração irreversível é causada nesta invenção, pode ser uma ou várias. Além disso, a solução anterior, na qual a alteração irreversível é causada, pode ser uma solução inicial.

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

É fornecido um método de processamento de dados executado em um aparelho de processamento de descriptografia utilizado juntamente com um aparelho de processamento de criptografia para a criptografia de dados de textos simples a serem processados para obter dados criptografados, o aparelho de processamento de criptografia contém: meios de divisão para a divisão dos dados

a serem processados em uma série de partes dos dados de textos simples divisionais, cada um sendo composto por um número predeterminado de bits; meios de geração de soluções para a geração contínua de soluções, cada uma sendo determinada exclusivamente com base em soluções anteriores, os meios de geração de soluções armazenando uma solução inicial utilizada para gerar uma primeira solução para a geração contínua das soluções; meios de criptografia para a criptografia dos dados de textos simples divisionais utilizando as soluções para converter os dados de textos simples divisionais em dados criptografados divisionais; e meios de conexão para a conexão dos dados criptografados divisionais para obter os dados criptografados, o aparelho de processamento de descriptografia, incluindo uma unidade de descriptografia, contém: meios de divisão para a divisão dos dados criptografados em uma série de partes dos dados criptografados divisionais, cada um sendo composto por um número predeterminado de bits; meios de geração de soluções para a geração contínua de soluções, cada uma sendo determinada exclusivamente com base em soluções anteriores, as soluções sendo geradas como as mesmas soluções geradas no aparelho de processamento de criptografia, os meios de geração de soluções armazenando uma solução inicial utilizada para gerar uma primeira solução para a geração contínua das soluções; meios de descriptografia para a descriptografia dos dados criptografados divisionais utilizando as soluções para converter os dados criptografados divisionais em dados de textos simples divisionais; e meios de conexão para a conexão dos dados de textos simples divisionais para obter os dados a serem processados; meios de entrada do disparador de destruição; e meios de processamento.

O método contém as etapas, executadas pelos meios de processamento, de: 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; e provocação de uma alteração irreversível em uma solução gerada antes das

soluções utilizadas para a descriptografia dos dados criptografados, a solução anterior sendo necessária para a geração das soluções utilizadas para a descriptografia dos dados criptografados, 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 mesmo com um computador comum.

É fornecido um programa computadorizado para um computador como um aparelho de processamento de descriptografia utilizado juntamente com um aparelho de processamento de criptografia para a criptografia de dados de textos simples a serem processados para obter dados criptografados, o aparelho de processamento de criptografia contém: meios de divisão para a divisão dos dados a serem processados em uma série de partes dos dados de textos simples divisionais, cada um sendo composto por um número predeterminado de bits; meios de geração de soluções para a geração contínua de soluções, cada uma sendo determinada exclusivamente com base em soluções anteriores, os meios de geração de soluções armazenando uma solução inicial utilizada para gerar uma primeira solução para a geração contínua das soluções; meios de criptografia para a criptografia dos dados de textos simples divisionais utilizando as soluções para converter os dados de textos simples divisionais em dados criptografados divisionais; e meios de conexão para a conexão dos dados criptografados divisionais para obter os dados criptografados, o aparelho de processamento de descriptografia, incluindo uma unidade de descriptografia, contém: meios de divisão para a divisão dos dados criptografados em uma série de partes dos dados criptografados divisionais, cada um sendo composto por um número predeterminado de bits; meios de geração de soluções para a geração contínua de soluções, cada uma sendo determinada exclusivamente com base em soluções anteriores, as soluções sendo geradas como as mesmas soluções

geradas no aparelho de processamento de criptografia, os meios de geração de soluções armazenando uma solução inicial utilizada para gerar uma primeira solução para a geração contínua das soluções; meios de descriptografia para a descriptografia dos dados criptografados divisionais utilizando as soluções para converter os dados criptografados divisionais em dados de textos simples divisionais; e meios de conexão para a conexão dos dados de textos simples divisionais para obter os dados a serem processados; meios de entrada do disparador de destruição; e o computador também conectado.

O programa computadorizado faz com que o computador execute as etapas a seguir: 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; e provocação de uma alteração irreversível em uma solução gerada antes das soluções utilizadas para a descriptografia dos dados criptografados, a solução anterior sendo necessária para a geração das soluções utilizadas para a descriptografia dos dados criptografados, quando as informações do disparador de destruição são recebidas.

Como descrito acima, os dados criptografados utilizados no aparelho de processamento de descriptografia, de acordo com a primeira invenção, utilizam a solução para criptografar os dados a serem processados para a geração dos dados criptografados, bem como para descriptografar os dados criptografados. No caso descrito acima, a solução é gerada com base nas soluções anteriores. Entretanto, a solução pode ser gerada com base não apenas na solução anterior, mas também na solução e nas informações ambientais invariáveis contidas nos dados criptografados a serem gerados. Com a solução como descrita acima, quando o aparelho de processamento de descriptografia deve descriptografar uma parte dos dados criptografados, não apenas a alteração irreversível causada na solução gerada antes da solução necessária para a descriptografia da parte dos dados criptografados, que deve ser utilizada para a geração da solução

necessária para a descriptografia da parte dos dados criptografados, mas também a alteração irreversível causada nas informações ambientais pode evitar que a parte dos dados criptografados seja descriptografada. Os dados criptografados, que não podem mais ser descriptografados dessa maneira, são transformados em uma espécie de dados "inúteis", como no caso descrito acima. A prevenção da descriptografia dos dados criptografados desta maneira produz o mesmo efeito que o da exclusão completa dos dados a serem processados.

As informações ambientais nesta especificação são utilizadas para a geração das soluções. Em contraste com as soluções, as informações ambientais não são geradas continuamente (em outras palavras, expressas como "invariáveis") e podem ser informações apropriadas contidas nos dados criptografados. A quantidade de informações ambientais pode corresponder a várias. Nesta especificação, as informações ambientais podem ser, por exemplo, um nome de arquivo dos dados criptografados contendo as informações ambientais, informações da data e da hora da criação, informações da data e da hora da atualização, informações de um tipo ou formato de arquivo e semelhantes. Especificamente, as informações adicionadas aos dados criptografados, em outras palavras, que indicam algumas características próprias dos dados criptografados, podem ser utilizadas como informações ambientais nas invenções desta especificação.

Quando as informações ambientais são utilizadas para gerar a solução, a primeira invenção pode ser constituída da seguinte maneira.

A primeira invenção, neste caso, é um aparelho de processamento de descriptografia utilizado juntamente com um aparelho de processamento de criptografia para a criptografia de dados de textos simples a serem processados para obter dados criptografados, o aparelho de processamento de criptografia contém: meios de divisão para a divisão dos dados a serem processados em uma série de partes dos dados de textos simples divisionais, cada um sendo composto por um número predeterminado de bits; meios de geração de soluções para a

geração contínua de soluções, cada uma sendo determinada exclusivamente com base em soluções anteriores e informações ambientais invariáveis a serem contidas nos dados criptografados a serem gerados, os meios de geração de soluções armazenando uma solução inicial utilizada para gerar uma primeira solução para a geração contínua das soluções; meios de criptografia para a criptografia dos dados de textos simples divisionais utilizando as soluções para converter os dados de textos simples divisionais em dados criptografados divisionais; e meios de conexão para a conexão dos dados criptografados divisionais para obter os dados criptografados contendo as informações ambientais.

Adicionalmente, o aparelho de processamento de descriptografia inclui uma unidade de descriptografia que contém: meios de divisão para a divisão dos dados criptografados em uma série de partes dos dados criptografados divisionais, cada um sendo composto por um número predeterminado de bits; meios de geração de soluções para a geração contínua de soluções, cada uma sendo determinada exclusivamente com base em soluções anteriores e informações ambientais contidas e lidas dos dados criptografados, as soluções sendo geradas como as mesmas soluções geradas no aparelho de processamento de criptografia, os meios de geração de soluções armazenando uma solução inicial utilizada para gerar uma primeira solução para a geração contínua das soluções; meios de descriptografia para a descriptografia dos dados criptografados divisionais utilizando as soluções para converter os dados criptografados divisionais em dados de textos simples divisionais; e meios de conexão para a conexão dos dados de textos simples divisionais para obter os dados a serem processados; 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; e meios de processamento para a destruição das informações ambientais contidas nos dados criptografados de maneira irreversível quando as informações do disparador de

destruição são inseridas.

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

É fornecido um método de processamento de dados executado em um aparelho de processamento de descriptografia utilizado juntamente com um aparelho de processamento de criptografia para a criptografia de dados de textos simples a serem processados para obter dados criptografados, o aparelho de processamento de criptografia contém: meios de divisão para a divisão dos dados a serem processados em uma série de partes dos dados de textos simples divisionais, cada um sendo composto por um número predeterminado de bits; meios de geração de soluções para a geração contínua de soluções, cada uma sendo determinada exclusivamente com base em soluções anteriores e informações ambientais invariáveis a serem contidas nos dados criptografados a serem gerados, os meios de geração de soluções armazenando uma solução inicial utilizada para gerar uma primeira solução para a geração contínua das soluções; meios de criptografia para a criptografia dos dados de textos simples divisionais utilizando as soluções para converter os dados de textos simples divisionais em dados criptografados divisionais; e meios de conexão para a conexão dos dados criptografados divisionais para obter os dados criptografados contendo as informações ambientais, o aparelho de processamento de descriptografia, incluindo uma unidade de descriptografia, contém: meios de divisão para a divisão dos dados criptografados em uma série de partes dos dados criptografados divisionais, cada um sendo composto por um número predeterminado de bits; meios de geração de soluções para a geração contínua de soluções, cada uma sendo determinada exclusivamente com base em soluções anteriores e informações ambientais contidas e lidas dos dados criptografados, as soluções sendo geradas como as mesmas soluções geradas no aparelho de processamento de criptografia, os meios de geração de soluções armazenando uma solução inicial utilizada para gerar uma primeira solução para a

geração contínua das soluções; meios de descriptografia para a descriptografia dos dados criptografados divisionais utilizando as soluções para converter os dados criptografados divisionais em dados de textos simples divisionais; e meios de conexão para a conexão dos dados de textos simples divisionais para obter os dados a serem processados; meios de entrada do disparador de destruição; e meios de processamento.

O método contém as etapas, executadas pelos meios de processamento, de: 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; e provocação de uma alteração irreversível nas informações ambientais contidas nos dados criptografados 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 mesmo com um computador comum.

É fornecido um programa computadorizado para um computador como um aparelho de processamento de descriptografia utilizado juntamente com um aparelho de processamento de criptografia para a criptografia de dados de textos simples a serem processados para obter dados criptografados, o aparelho de processamento de criptografia contém: meios de divisão para a divisão dos dados a serem processados em uma série de partes dos dados de textos simples divisionais, cada um sendo composto por um número predeterminado de bits; meios de geração de soluções para a geração contínua de soluções, cada uma sendo determinada exclusivamente com base em soluções anteriores e informações ambientais invariáveis a serem contidas nos dados criptografados a serem gerados, os meios de geração de soluções armazenando uma solução inicial utilizada para gerar uma primeira solução para a geração contínua das

soluções; meios de criptografia para a criptografia dos dados de textos simples divisionais utilizando as soluções para converter os dados de textos simples divisionais em dados criptografados divisionais; e meios de conexão para a conexão dos dados criptografados divisionais para obter os dados criptografados contendo as informações ambientais, o aparelho de processamento de descriptografia, incluindo uma unidade de descriptografia, contém: meios de divisão para a divisão dos dados criptografados em uma série de partes dos dados criptografados divisionais, cada um sendo composto por um número predeterminado de bits; meios de geração de soluções para a geração contínua de soluções, cada uma sendo determinada exclusivamente com base em soluções anteriores e informações ambientais contidas e lidas dos dados criptografados, as soluções sendo geradas como as mesmas soluções geradas no aparelho de processamento de criptografia, os meios de geração de soluções armazenando uma solução inicial utilizada para gerar uma primeira solução para a geração contínua das soluções; meios de descriptografia para a descriptografia dos dados criptografados divisionais utilizando as soluções para converter os dados criptografados divisionais em dados de textos simples divisionais; e meios de conexão para a conexão dos dados de textos simples divisionais para obter os dados a serem processados; meios de entrada do disparador de destruição; e o computador também conectado.

O programa computadorizado faz com que o computador execute as etapas a seguir: 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; e provocação de uma alteração irreversível nas informações ambientais contidas nos dados criptografados quando as informações do disparador de destruição são recebidas.

A segunda invenção é um aparelho de processamento de descriptografia utilizado juntamente com um aparelho de processamento de criptografia para a

criptografia de dados de textos simples a serem processados para obter dados criptografados, o aparelho de processamento de criptografia contém: meios de divisão para a divisão dos dados a serem processados em uma série de partes dos dados de textos simples divisionais, cada um sendo composto por um número predeterminado de bits; meios de geração de soluções para a geração contínua de soluções, cada uma sendo determinada exclusivamente com base em soluções anteriores, os meios de geração de soluções armazenando uma solução inicial utilizada para gerar uma primeira solução para a geração contínua das soluções; meios de criptografia para a criptografia dos dados de textos simples divisionais utilizando as soluções para converter os dados de textos simples divisionais em dados criptografados divisionais; meios de geração de informações de especificação do cronograma para a geração de informações de especificação do cronograma para especificar o cronograma a fim de evitar que os dados criptografados contendo as informações de especificação do cronograma sejam descriptografados; e meios de conexão para a conexão dos dados criptografados divisionais para obter os dados criptografados contendo as informações de especificação do cronograma.

Adicionalmente, o aparelho de processamento de descriptografia inclui uma unidade de descriptografia que contém: meios de divisão para a divisão dos dados criptografados em uma série de partes dos dados criptografados divisionais, cada um sendo composto por um número predeterminado de bits; meios de geração de soluções para a geração contínua de soluções, cada uma sendo determinada exclusivamente com base em soluções anteriores, as soluções sendo geradas como as mesmas soluções geradas no aparelho de processamento de criptografia, os meios de geração de soluções armazenando uma solução inicial utilizada para gerar uma primeira solução para a geração contínua das soluções; meios de descriptografia para a descriptografia dos dados criptografados divisionais utilizando as soluções para converter os dados criptografados divisionais em dados de textos simples divisionais; e meios de

conexão para a conexão dos dados de textos simples divisionais para obter os dados a serem processados; meios de leitura das informações de especificação do cronograma para a leitura das informações de especificação do cronograma dos dados criptografados; e meios de processamento para a destruição de uma solução gerada antes das soluções utilizadas para a descriptografia dos dados criptografados, a solução anterior sendo necessária para a geração das soluções utilizadas para a descriptografia dos dados criptografados de maneira irreversível; os meios de processamento monitoram 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 destroem a solução no caso de o cronograma ter chegado.

Os dados criptografados utilizados no aparelho de processamento de descriptografia são aproximadamente os mesmos que na primeira invenção, mas contêm ainda as informações de especificação do cronograma para especificar o cronograma a fim de evitar que os dados criptografados sejam descriptografados. Como na primeira invenção, o aparelho de processamento de descriptografia causa a alteração irreversível na solução anterior, que é necessária para gerar a solução necessária para a descriptografia dos dados criptografados, para transformar os dados criptografados em uma espécie de dados "inúteis". O cronograma para transformar os dados criptografados em dados "inúteis" é controlado pelas informações de especificação do cronograma. O aparelho de processamento de descriptografia, por exemplo, monitora constantemente se o cronograma evita que os dados criptografados sejam descriptografados, que é especificado pelas informações de especificação do cronograma, chegou ou não e causando a alteração irreversível na solução anterior necessária para gerar a solução necessária para a descriptografia dos dados criptografados, como na primeira invenção, imediatamente após o cronograma ou após o decorrer de um período de tempo predeterminado após o cronograma no caso de o cronograma ter chegado. 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 descriptografia é significativa em vista da prevenção da perda dos dados a serem processados.

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

É fornecido um método de processamento de dados executado em um aparelho de processamento de descriptografia utilizado juntamente com um aparelho de processamento de criptografia para a criptografia de dados de textos simples a serem processados para obter dados criptografados, o aparelho de processamento de criptografia contém: meios de divisão para a divisão dos dados a serem processados em uma série de partes dos dados de textos simples divisionais, cada um sendo composto por um número predeterminado de bits; meios de geração de soluções para a geração contínua de soluções, cada uma sendo determinada exclusivamente com base em soluções anteriores, os meios de geração de soluções armazenando uma solução inicial utilizada para gerar uma primeira solução para a geração contínua das soluções; meios de criptografia para a criptografia dos dados de textos simples divisionais utilizando as soluções para converter os dados de textos simples divisionais em dados criptografados divisionais; meios de geração de informações de especificação do cronograma para a geração de informações de especificação do cronograma para especificar o cronograma a fim de evitar que os dados criptografados contendo as informações de especificação do cronograma sejam descriptografados; e meios de conexão para a conexão dos dados criptografados divisionais para obter os dados criptografados contendo as informações de especificação do cronograma, o aparelho de processamento de descriptografia, incluindo uma unidade de descriptografia, contém: meios de divisão para a divisão dos dados criptografados em uma série de partes dos dados criptografados divisionais, cada um sendo

composto por um número predeterminado de bits; meios de geração de soluções para a geração contínua de soluções, cada uma sendo determinada exclusivamente com base em soluções anteriores, as soluções sendo geradas como as mesmas soluções geradas no aparelho de processamento de criptografia, os meios de geração de soluções armazenando uma solução inicial utilizada para gerar uma primeira solução para a geração contínua das soluções; meios de descriptografia para a descriptografia dos dados criptografados divisionais utilizando as soluções para converter os dados criptografados divisionais em dados de textos simples divisionais; e meios de conexão para a conexão dos dados de textos simples divisionais para obter os dados a serem processados; e meios de processamento.

O método contém as etapas, executadas pelos meios de processamento, de: leitura das informações de especificação do cronograma dos dados criptografados; e monitorar se o cronograma especificado pelas informações de especificação do cronograma lidas na etapa de leitura das informações de especificação do cronograma chegou ou não e causando uma alteração irreversível em uma solução gerada antes das soluções utilizadas para a descriptografia dos dados criptografados, a solução anterior sendo necessária para a geração das soluções utilizadas para a descriptografia dos dados criptografados, 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 mesmo com um computador comum.

É fornecido um programa computadorizado para um computador como um aparelho de processamento de descriptografia utilizado juntamente com um aparelho de processamento de criptografia para a criptografia de dados de textos simples a serem processados para obter dados criptografados, o aparelho de processamento de criptografia contém: meios de divisão para a divisão dos dados

a serem processados em uma série de partes dos dados de textos simples divisionais, cada um sendo composto por um número predeterminado de bits; meios de geração de soluções para a geração contínua de soluções, cada uma sendo determinada exclusivamente com base em soluções anteriores, os meios de geração de soluções armazenando uma solução inicial utilizada para gerar uma primeira solução para a geração contínua das soluções; meios de criptografia para a criptografia dos dados de textos simples divisionais utilizando as soluções para converter os dados de textos simples divisionais em dados criptografados divisionais; meios de geração de informações de especificação do cronograma para a geração de informações de especificação do cronograma para especificar o cronograma a fim de evitar que os dados criptografados contendo as informações de especificação do cronograma sejam descriptografados; e meios de conexão para a conexão dos dados criptografados divisionais para obter os dados criptografados contendo as informações de especificação do cronograma, o aparelho de processamento de descriptografia, incluindo uma unidade de descriptografia, contém: meios de divisão para a divisão dos dados criptografados em uma série de partes dos dados criptografados divisionais, cada um sendo composto por um número predeterminado de bits; meios de geração de soluções para a geração contínua de soluções, cada uma sendo determinada exclusivamente com base em soluções anteriores, as soluções sendo geradas como as mesmas soluções geradas no aparelho de processamento de criptografia, os meios de geração de soluções armazenando uma solução inicial utilizada para gerar uma primeira solução para a geração contínua das soluções; meios de descriptografia para a descriptografia dos dados criptografados divisionais utilizando as soluções para converter os dados criptografados divisionais em dados de textos simples divisionais; e meios de conexão para a conexão dos dados de textos simples divisionais para obter os dados a serem processados; e o computador também conectado.

O programa computadorizado faz com que o computador execute as

etapas a seguir: leitura das informações de especificação do cronograma dos dados criptografados; e monitorar se o cronograma especificado pelas informações de especificação do cronograma lidas na etapa de leitura das informações de especificação do cronograma chegou ou não e causando uma alteração irreversível em uma solução gerada antes das soluções utilizadas para a descriptografia dos dados criptografados, a solução anterior sendo necessária para a geração das soluções utilizadas para a descriptografia dos dados criptografados, no caso de o cronograma ter chegado.

Mesmo na segunda invenção, as informações ambientais são, às vezes, utilizadas para gerar a solução, como na primeira invenção. Neste caso, a segunda invenção pode ser constituída da seguinte maneira.

A segunda invenção, neste caso, é um aparelho de processamento de descriptografia utilizado juntamente com um aparelho de processamento de criptografia para a criptografia de dados de textos simples a serem processados para obter dados criptografados, o aparelho de processamento de criptografia contém: meios de divisão para a divisão dos dados a serem processados em uma série de partes dos dados de textos simples divisionais, cada um sendo composto por um número predeterminado de bits; meios de geração de soluções para a geração contínua de soluções, cada uma sendo determinada exclusivamente com base em soluções anteriores e informações ambientais invariáveis a serem contidas nos dados criptografados a serem gerados, os meios de geração de soluções armazenando uma solução inicial utilizada para gerar uma primeira solução para a geração contínua das soluções; meios de criptografia para a criptografia dos dados de textos simples divisionais utilizando as soluções para converter os dados de textos simples divisionais em dados criptografados divisionais; meios de geração de informações de especificação do cronograma para a geração de informações de especificação do cronograma para especificar o cronograma a fim de evitar que os dados criptografados contendo as informações de especificação do cronograma sejam descriptografados; e meios

de conexão para a conexão dos dados criptografados divisionais para obter os dados criptografados contendo as informações ambientais e as informações de especificação do cronograma.

Além disso, o aparelho de processamento de descriptografia inclui uma unidade de descriptografia que contém: meios de divisão para a divisão dos dados criptografados em uma série de partes dos dados criptografados divisionais, cada um sendo composto por um número predeterminado de bits; meios de geração de soluções para a geração contínua de soluções, cada uma sendo determinada exclusivamente com base em soluções anteriores e informações ambientais contidas e lidas dos dados criptografados, as soluções sendo geradas como as mesmas soluções geradas no aparelho de processamento de criptografia, os meios de geração de soluções armazenando uma solução inicial utilizada para gerar uma primeira solução para a geração contínua das soluções; meios de descriptografia para a descriptografia dos dados criptografados divisionais utilizando as soluções para converter os dados criptografados divisionais em dados de textos simples divisionais; e meios de conexão para a conexão dos dados de textos simples divisionais para obter os dados a serem processados; meios de leitura das informações de especificação do cronograma para a leitura das informações de especificação do cronograma dos dados criptografados; e meios de processamento para a destruição das informações ambientais contidas nos dados criptografados de maneira irreversível, e os meios de processamento que monitoram 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 destroem a solução no caso de o cronograma ter chegado.

Mesmo com este aparelho de processamento de descriptografia, pode-se evitar que os dados criptografados sejam 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 desta invenção também pode ser obtido, por exemplo, pelo método a seguir.

É fornecido um método de processamento de dados executado em um aparelho de processamento de descriptografia utilizado juntamente com um aparelho de processamento de criptografia para a criptografia de dados de textos simples a serem processados para obter dados criptografados, o aparelho de processamento de criptografia contém: meios de divisão para a divisão dos dados a serem processados em uma série de partes dos dados de textos simples divisionais, cada um sendo composto por um número predeterminado de bits; meios de geração de soluções para a geração contínua de soluções, cada uma sendo determinada exclusivamente com base em soluções anteriores e informações ambientais invariáveis a serem contidas nos dados criptografados a serem gerados, os meios de geração de soluções armazenando uma solução inicial utilizada para gerar uma primeira solução para a geração contínua das soluções; meios de criptografia para a criptografia dos dados de textos simples divisionais utilizando as soluções para converter os dados de textos simples divisionais em dados criptografados divisionais; meios de geração de informações de especificação do cronograma para a geração de informações de especificação do cronograma para especificar o cronograma a fim de evitar que os dados criptografados contendo as informações de especificação do cronograma sejam descriptografados; e meios de conexão para a conexão dos dados criptografados divisionais para obter os dados criptografados contendo as informações ambientais e as informações de especificação do cronograma, o aparelho de processamento de descriptografia, incluindo uma unidade de descriptografia, contém: meios de divisão para a divisão dos dados criptografados em uma série de partes dos dados criptografados divisionais, cada um sendo composto por um número predeterminado de bits; meios de geração de soluções para a geração

contínua de soluções, cada uma sendo determinada exclusivamente com base em soluções anteriores e informações ambientais contidas e lidas dos dados criptografados, as soluções sendo geradas como as mesmas soluções geradas no aparelho de processamento de criptografia, os meios de geração de soluções armazenando uma solução inicial utilizada para gerar uma primeira solução para a geração contínua das soluções; meios de descriptografia para a descriptografia dos dados criptografados divisionais utilizando as soluções para converter os dados criptografados divisionais em dados de textos simples divisionais; e meios de conexão para a conexão dos dados de textos simples divisionais para obter os dados a serem processados; e meios de processamento.

O método contém as etapas, executadas pelos meios de processamento, de: leitura das informações de especificação do cronograma dos dados criptografados; e monitorar se o cronograma especificado pelas informações de especificação do cronograma lidas na etapa de leitura das informações de especificação do cronograma chegou ou não e causando uma alteração irreversível nas informações ambientais contidas nos dados criptografados 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 mesmo com um computador comum.

É fornecido um programa computadorizado para um computador como um aparelho de processamento de descriptografia utilizado juntamente com um aparelho de processamento de criptografia para a criptografia de dados de textos simples a serem processados para obter dados criptografados, o aparelho de processamento de criptografia contém: meios de divisão para a divisão dos dados a serem processados em uma série de partes dos dados de textos simples divisionais, cada um sendo composto por um número predeterminado de bits; meios de geração de soluções para a geração contínua de soluções, cada uma

sendo determinada exclusivamente com base em soluções anteriores e informações ambientais invariáveis a serem contidas nos dados criptografados a serem gerados, os meios de geração de soluções armazenando uma solução inicial utilizada para gerar uma primeira solução para a geração contínua das soluções; meios de criptografia para a criptografia dos dados de textos simples divisionais utilizando as soluções para converter os dados de textos simples divisionais em dados criptografados divisionais; meios de geração de informações de especificação do cronograma para a geração de informações de especificação do cronograma para especificar o cronograma a fim de evitar que os dados criptografados contendo as informações de especificação do cronograma sejam descriptografados; e meios de conexão para a conexão dos dados criptografados divisionais para obter os dados criptografados contendo as informações ambientais e as informações de especificação do cronograma, o aparelho de processamento de descriptografia, incluindo uma unidade de descriptografia, contendo: meios de divisão para a divisão dos dados criptografados em uma série de partes dos dados criptografados divisionais, cada um sendo composto por um número predeterminado de bits; meios de geração de soluções para a geração contínua de soluções, cada uma sendo determinada exclusivamente com base em soluções anteriores e informações ambientais contidas e lidas dos dados criptografados, as soluções sendo geradas como as mesmas soluções geradas no aparelho de processamento de criptografia, os meios de geração de soluções armazenando uma solução inicial utilizada para gerar uma primeira solução para a geração contínua das soluções; meios de descriptografia para a descriptografia dos dados criptografados divisionais utilizando as soluções para converter os dados criptografados divisionais em dados de textos simples divisionais; e meios de conexão para a conexão dos dados de textos simples divisionais para obter os dados a serem processados; e o computador também conectado.

O programa computadorizado faz com que o computador execute as etapas a seguir: leitura das informações de especificação do cronograma dos

dados criptografados; e monitorar se o cronograma especificado pelas informações de especificação do cronograma lidas na etapa de leitura das informações de especificação do cronograma chegou ou não e causando uma alteração irreversível nas informações ambientais contidas nos dados criptografados no caso de o cronograma ter chegado.

A terceira invenção é um aparelho de processamento de descriptografia utilizado juntamente com um aparelho de processamento de criptografia para a criptografia de dados de textos simples a serem processados para obter dados criptografados, o aparelho de processamento de criptografia contém: meios de divisão para a divisão dos dados a serem processados em uma série de partes dos dados de textos simples divisionais, cada um sendo composto por um número predeterminado de bits; meios de geração de soluções para a geração contínua de soluções, cada uma sendo determinada exclusivamente com base em soluções anteriores, os meios de geração de soluções armazenando uma solução inicial utilizada para gerar uma primeira solução para a geração contínua das soluções; meios de criptografia para a criptografia dos dados de textos simples divisionais utilizando as soluções para converter os dados de textos simples divisionais em dados criptografados divisionais; meios de geração de informações de especificação do cronograma para a geração de informações de especificação do cronograma para especificar o cronograma a fim de evitar que os dados criptografados contendo as informações de especificação do cronograma sejam descriptografados; e meios de conexão para a conexão dos dados criptografados divisionais para obter os dados criptografados contendo as informações de especificação do cronograma.

Além disso, o aparelho de processamento de descriptografia inclui uma unidade de descriptografia que contém: meios de divisão para a divisão dos dados criptografados em uma série de partes dos dados criptografados divisionais, cada um sendo composto por um número predeterminado de bits; meios de geração de soluções para a geração contínua de soluções, cada uma sendo

determinada exclusivamente com base em soluções anteriores, as soluções sendo geradas como as mesmas soluções geradas no aparelho de processamento de criptografia, os meios de geração de soluções armazenando uma solução inicial utilizada para gerar uma primeira solução para a geração contínua das soluções; meios de descriptografia para a descriptografia dos dados criptografados divisionais utilizando as soluções para converter os dados criptografados divisionais em dados de textos simples divisionais; e meios de conexão para a conexão dos dados de textos simples divisionais para obter os dados a serem processados; 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 são inseridas dos meios de entrada do disparador de descriptografia; e meios de processamento para a recepção das informações de especificação do cronograma lidas pelos meios de leitura das informações de especificação do cronograma quando as informações do disparador de descriptografia são inseridas para monitorar se o cronograma especificado pelas informações de especificação do cronograma chegou ou não e permitir que a unidade de descriptografia descriptografe os dados criptografados se o cronograma ainda não chegou, e causando uma alteração irreversível em uma solução gerada antes das soluções utilizadas para a descriptografia dos dados criptografados, a solução anterior sendo necessária para a geração das soluções utilizadas para a descriptografia dos dados criptografados, no caso de o cronograma ter chegado.

Os dados criptografados utilizados na terceira invenção 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. O aparelho de processamento de

descriptografia, de acordo com a terceira invenção, controla o cronograma para causar a alteração irreversível na solução gerada antes da solução necessária para a descriptografia dos dados criptografados, que é necessária para gerar a solução necessária para a descriptografia dos dados criptografados pelas informações de especificação do cronograma, como na segunda invenção. Quando as informações do disparador de descriptografia para solicitação da descriptografia dos dados criptografados são inseridas, o aparelho de processamento de descriptografia na 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 ou não e permitir que a unidade de descriptografia descriptografe os dados criptografados se o cronograma ainda não chegou, e causando a alteração irreversível na solução gerada antes da solução necessária para a descriptografia dos dados criptografados, que é necessária para gerar a solução necessária para a descriptografia dos dados criptografados, no caso de o cronograma ter chegado. Como descrito acima, o aparelho de processamento de descriptografia na terceira invenção descriptografa os dados criptografados que devem ser descriptografados pelo usuário ou transforma os dados criptografados em uma espécie de dados "inúteis" quando o usuário executa uma operação de descriptografia. Esta invenção também é eficaz ao evitar que os dados a serem processados sejam perdidos devido à perda dos dados criptografados.

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

É fornecido um método de processamento de dados executado em um aparelho de processamento de descriptografia utilizado juntamente com um aparelho de processamento de criptografia para a criptografia de dados de textos simples a serem processados para obter dados criptografados, o aparelho de processamento de criptografia contém: meios de divisão para a divisão dos dados

a serem processados em uma série de partes dos dados de textos simples divisionais, cada um sendo composto por um número predeterminado de bits; meios de geração de soluções para a geração contínua de soluções, cada uma sendo determinada exclusivamente com base em soluções anteriores, os meios de geração de soluções armazenando uma solução inicial utilizada para gerar uma primeira solução para a geração contínua das soluções; meios de criptografia para a criptografia dos dados de textos simples divisionais utilizando as soluções para converter os dados de textos simples divisionais em dados criptografados divisionais; meios de geração de informações de especificação do cronograma para a geração de informações de especificação do cronograma para especificar o cronograma a fim de evitar que os dados criptografados contendo as informações de especificação do cronograma sejam descriptografados; e meios de conexão para a conexão dos dados criptografados divisionais para obter os dados criptografados contendo as informações de especificação do cronograma, o aparelho de processamento de descriptografia, incluindo uma unidade de descriptografia, contém: meios de divisão para a divisão dos dados criptografados em uma série de partes dos dados criptografados divisionais, cada um sendo composto por um número predeterminado de bits; meios de geração de soluções para a geração contínua de soluções, cada uma sendo determinada exclusivamente com base em soluções anteriores, as soluções sendo geradas como as mesmas soluções geradas no aparelho de processamento de criptografia, os meios de geração de soluções armazenando uma solução inicial utilizada para gerar uma primeira solução para a geração contínua das soluções; meios de descriptografia para a descriptografia dos dados criptografados divisionais utilizando as soluções para converter os dados criptografados divisionais em dados de textos simples divisionais; e meios de conexão para a conexão dos dados de textos simples divisionais para obter os dados a serem processados; meios de entrada do disparador de descriptografia; e meios de processamento.

O método contém as etapas, executadas pelos meios de processamento, de: 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 as informações do disparador de descriptografia são inseridas dos meios de entrada do disparador de descriptografia; e recepção das informações de especificação do cronograma lidas na etapa de leitura das informações de especificação do cronograma quando as informações do disparador de descriptografia são inseridas para determinar se o cronograma especificado pelas informações de especificação do cronograma chegou ou não e permitir que a unidade de descriptografia descriptografe os dados criptografados se o cronograma ainda não chegou,e causando uma alteração irreversível em uma solução gerada antes das soluções utilizadas para a descriptografia dos dados criptografados, a solução anterior sendo necessária para a geração das soluções utilizadas para a descriptografia dos dados criptografados, 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 mesmo com um computador comum.

É fornecido um programa computadorizado para um computador como um aparelho de processamento de descriptografia utilizado juntamente com um aparelho de processamento de criptografia para a criptografia de dados de textos simples a serem processados para obter dados criptografados, o aparelho de processamento de criptografia contém: meios de divisão para a divisão dos dados a serem processados em uma série de partes dos dados de textos simples divisionais, cada um sendo composto por um número predeterminado de bits; meios de geração de soluções para a geração contínua de soluções, cada uma sendo determinada exclusivamente com base em soluções anteriores, os meios

de geração de soluções armazenando uma solução inicial utilizada para gerar uma primeira solução para a geração contínua das soluções; meios de criptografia para a criptografia dos dados de textos simples divisionais utilizando as soluções para converter os dados de textos simples divisionais em dados criptografados divisionais; meios de geração de informações de especificação do cronograma para a geração de informações de especificação do cronograma para especificar o cronograma a fim de evitar que os dados criptografados contendo as informações de especificação do cronograma sejam descriptografados; e meios de conexão para a conexão dos dados criptografados divisionais para obter os dados criptografados contendo as informações de especificação do cronograma, o aparelho de processamento de descriptografia, incluindo uma unidade de descriptografia, contém: meios de divisão para a divisão dos dados criptografados em uma série de partes dos dados criptografados divisionais, cada um sendo composto por um número predeterminado de bits; meios de geração de soluções para a geração contínua de soluções, cada uma sendo determinada exclusivamente com base em soluções anteriores, as soluções sendo geradas como as mesmas soluções geradas no aparelho de processamento de criptografia, os meios de geração de soluções armazenando uma solução inicial utilizada para gerar uma primeira solução para a geração contínua das soluções; meios de descriptografia para a descriptografia dos dados criptografados divisionais utilizando as soluções para converter os dados criptografados divisionais em dados de textos simples divisionais; e meios de conexão para a conexão dos dados de textos simples divisionais para obter os dados a serem processados; meios de entrada do disparador de descriptografia; e o computador também conectado.

O programa computadorizado faz com que o computador execute as etapas a seguir: 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 as informações do disparador de descriptografia são inseridas dos meios de entrada do disparador de descriptografia; e recepção das informações de especificação do cronograma lidas na etapa de leitura das informações de especificação do cronograma quando as informações do disparador de descriptografia são inseridas para determinar se o cronograma especificado pelas informações de especificação do cronograma chegou ou não e permitir que a unidade de descriptografia descriptografe os dados criptografados se o cronograma ainda não chegou,e causando uma alteração irreversível em uma solução gerada antes das soluções utilizadas para a descriptografia dos dados criptografados, a solução anterior sendo necessária para a geração das soluções utilizadas para a descriptografia dos dados criptografados, no caso de o cronograma ter chegado.

Mesmo na terceira invenção, as informações ambientais são, às vezes, utilizadas para gerar a solução, como na primeira e na segunda invenções. Neste caso, a terceira invenção pode ser constituída da seguinte maneira.

A terceira invenção, neste caso, é um aparelho de processamento de descriptografia utilizado juntamente com um aparelho de processamento de criptografia para a criptografia de dados de textos simples a serem processados para obter dados criptografados, o aparelho de processamento de criptografia contém: meios de divisão para a divisão dos dados a serem processados em uma série de partes dos dados de textos simples divisionais, cada um sendo composto por um número predeterminado de bits; meios de geração de soluções para a geração contínua de soluções, cada uma sendo determinada exclusivamente com base em soluções anteriores e informações ambientais invariáveis a serem contidas nos dados criptografados a serem gerados, os meios de geração de soluções armazenando uma solução inicial utilizada para gerar uma primeira solução para a geração contínua das soluções; meios de criptografia para a criptografia dos dados de textos simples divisionais utilizando as soluções para converter os dados de textos simples divisionais em dados criptografados

divisionais; meios de geração de informações de especificação do cronograma para a geração de informações de especificação do cronograma para especificar o cronograma a fim de evitar que os dados criptografados contendo as informações de especificação do cronograma sejam descriptografados; e meios de conexão para a conexão dos dados criptografados divisionais para obter os dados criptografados contendo as informações ambientais e as informações de especificação do cronograma.

Além disso, o aparelho de processamento de descriptografia inclui uma unidade de descriptografia que contém: meios de divisão para a divisão dos dados criptografados em uma série de partes dos dados criptografados divisionais, cada um sendo composto por um número predeterminado de bits; meios de geração de soluções para a geração contínua de soluções, cada uma sendo determinada exclusivamente com base em soluções anteriores e informações ambientais contidas e lidas dos dados criptografados, as soluções sendo geradas como as mesmas soluções geradas no aparelho de processamento de criptografia, os meios de geração de soluções armazenando uma solução inicial utilizada para gerar uma primeira solução para a geração contínua das soluções; meios de descriptografia para a descriptografia dos dados criptografados divisionais utilizando as soluções para converter os dados criptografados divisionais em dados de textos simples divisionais; e meios de conexão para a conexão dos dados de textos simples divisionais para obter os dados a serem processados; 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 são inseridas dos meios de entrada do disparador de descriptografia; e meios de processamento para a recepção das informações de especificação do cronograma lidas pelos meios de leitura das informações de especificação do

cronograma quando as informações do disparador de descriptografia são inseridas para determinar se o cronograma especificado pelas informações de especificação do cronograma chegou ou não e permitir que a unidade de descriptografia descriptografe os dados criptografados se o cronograma ainda não chegou, e causando uma alteração irreversível nas informações ambientais contidas nos dados criptografados no caso de o cronograma ter chegado.

Especificamente, mesmo com este aparelho de processamento de descriptografia, pode-se evitar que os dados criptografados sejam 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 desta invenção também pode ser obtido, por exemplo, pelo método a seguir.

É fornecido um método de processamento de dados executado em um aparelho de processamento de descriptografia utilizado juntamente com um aparelho de processamento de criptografia para a criptografia de dados de textos simples a serem processados para obter dados criptografados, o aparelho de processamento de criptografia contém: meios de divisão para a divisão dos dados a serem processados em uma série de partes dos dados de textos simples divisionais, cada um sendo composto por um número predeterminado de bits; meios de geração de soluções para a geração contínua de soluções, cada uma sendo determinada exclusivamente com base em soluções anteriores e informações ambientais invariáveis a serem contidas nos dados criptografados a serem gerados, os meios de geração de soluções armazenando uma solução inicial utilizada para gerar uma primeira solução para a geração contínua das soluções; meios de criptografia para a criptografia dos dados de textos simples divisionais utilizando as soluções para converter os dados de textos simples divisionais em dados criptografados divisionais; meios de geração de informações

de especificação do cronograma para a geração de informações de especificação do cronograma para especificar o cronograma a fim de evitar que os dados criptografados contendo as informações de especificação do cronograma sejam descriptografados; e meios de conexão para a conexão dos dados criptografados divisionais para obter os dados criptografados contendo as informações ambientais e as informações de especificação do cronograma, o aparelho de processamento de descriptografia, incluindo uma unidade de descriptografia, contém: meios de divisão para a divisão dos dados criptografados em uma série de partes dos dados criptografados divisionais, cada um sendo composto por um número predeterminado de bits; meios de geração de soluções para a geração contínua de soluções, cada uma sendo determinada exclusivamente com base em soluções anteriores e informações ambientais contidas e lidas dos dados criptografados, as soluções sendo geradas como as mesmas soluções geradas no aparelho de processamento de criptografia, os meios de geração de soluções armazenando uma solução inicial utilizada para gerar uma primeira solução para a geração contínua das soluções; meios de descriptografia para a descriptografia dos dados criptografados divisionais utilizando as soluções para converter os dados criptografados divisionais em dados de textos simples divisionais; e meios de conexão para a conexão dos dados de textos simples divisionais para obter os dados a serem processados; meios de entrada do disparador de descriptografia; e meios de processamento.

O método contém as etapas, executadas pelos meios de processamento, de: 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 as informações do disparador de descriptografia são inseridas dos meios de entrada do disparador de descriptografia; e recepção das informações de especificação do cronograma lidas na etapa de leitura das informações de especificação do cronograma quando as informações do

disparador de descriptografia são inseridas para determinar se o cronograma especificado pelas informações de especificação do cronograma chegou e permitir que a unidade de descriptografia descriptografe os dados criptografados se o cronograma ainda não chegou, causando uma alteração irreversível nas informações ambientais contidas nos dados criptografados 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 mesmo com um computador comum.

É fornecido um programa computadorizado para um computador como um aparelho de processamento de descriptografia utilizado juntamente com um aparelho de processamento de criptografia para a criptografia de dados de textos simples a serem processados para obter dados criptografados, o aparelho de processamento de criptografia contém: meios de divisão para a divisão dos dados a serem processados em uma série de partes dos dados de textos simples divisionais, cada um sendo composto por um número predeterminado de bits; meios de geração de soluções para a geração contínua de soluções, cada uma sendo determinada exclusivamente com base em soluções anteriores e informações ambientais invariáveis a serem contidas nos dados criptografados a serem gerados, os meios de geração de soluções armazenando uma solução inicial utilizada para gerar uma primeira solução para a geração contínua das soluções; meios de criptografia para a criptografia dos dados de textos simples divisionais utilizando as soluções para converter os dados de textos simples divisionais em dados criptografados divisionais; meios de geração de informações de especificação do cronograma para a geração de informações de especificação do cronograma para especificar o cronograma a fim de evitar que os dados criptografados contendo as informações de especificação do cronograma sejam descriptografados; e meios de conexão para a conexão dos dados criptografados

divisionais para obter os dados criptografados contendo as informações ambientais e as informações de especificação do cronograma, o aparelho de processamento de descriptografia, incluindo uma unidade de descriptografia, contém: meios de divisão para a divisão dos dados criptografados em uma série de partes dos dados criptografados divisionais, cada um sendo composto por um número predeterminado de bits; meios de geração de soluções para a geração contínua de soluções, cada uma sendo determinada exclusivamente com base em soluções anteriores e informações ambientais contidas e lidas dos dados criptografados, as soluções sendo geradas como as mesmas soluções geradas no aparelho de processamento de criptografia, os meios de geração de soluções armazenando uma solução inicial utilizada para gerar uma primeira solução para a geração contínua das soluções; meios de descriptografia para a descriptografia dos dados criptografados divisionais utilizando as soluções para converter os dados criptografados divisionais em dados de textos simples divisionais; e meios de conexão para a conexão dos dados de textos simples divisionais para obter os dados a serem processados; meios de entrada do disparador de descriptografia; e o computador também conectado.

O programa computadorizado faz com que o computador execute as etapas a seguir: 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 as informações do disparador de descriptografia são inseridas dos meios de entrada do disparador de descriptografia; e recepção das informações de especificação do cronograma lidas na etapa de leitura das informações de especificação do cronograma quando as informações do disparador de descriptografia são inseridas para determinar se o cronograma especificado pelas informações de especificação do cronograma chegou ou não e permitir que a unidade de descriptografia descriptografe os dados criptografados se o cronograma ainda não chegou, e causando uma

alteração irreversível nas informações ambientais contidas nos dados criptografados no caso de o cronograma ter chegado.

Os dados a seguir são comuns da primeira à terceira invenções.

Os meios de processamento nas invenções desta especificação causam a alteração irreversível na solução gerada antes da solução utilizada para a descriptografia dos dados criptografados, que é necessária para gerar a solução utilizada para a descriptografia dos dados criptografados, ou nas informações ambientais. O modo para causar a alteração irreversível na solução ou nas informações ambientais, nas quais a alteração irreversível deve ser causada, pode ser determinado de maneira apropriada. Por exemplo, a solução ou as informações ambientais, nas quais a alteração irreversível deve ser causada, são sobrescritas com dados apropriados ou convertidas de modo irreversível para causar a alteração irreversível na solução ou nas informações ambientais. Os dados apropriados a serem escritos sobre a solução ou as informações ambientais são, por exemplo, dados irrelevantes aos dados criptografados. Para a conversão irreversível, por exemplo, após um processamento de corte dos números decimais ou dos primeiros dígitos do resultado de um cálculo apropriado ser executado em uma seqüência de dados da solução ou das informações ambientais a serem convertidas de maneira irreversível, a seqüência de dados da solução original ou das informações ambientais originais pode ser substituída pelo resultado do cálculo assim processado. Por outro lado, a solução ou as informações ambientais podem ser sujeitas a uma conversão JPEG.

Os meios de geração de soluções no aparelho de processamento de criptografia podem gerar a solução em qualquer cronograma. Por exemplo, os meios de geração de soluções no aparelho de processamento de criptografia podem gerar a solução sempre que os meios de criptografia criptografarem os dados de textos simples divisionais. Os meios de geração de soluções no aparelho de processamento de descriptografia podem gerar a solução em qualquer cronograma, e os meios de geração de soluções no aparelho de

processamento de descriptografia podem gerar a solução sempre que os meios de descriptografia descriptografarem os dados criptografados divisionais se os meios de geração de soluções no aparelho de processamento de criptografia geram a solução sempre que os meios de criptografia criptografarem os dados de textos simples divisionais. Desta maneira, se uma série de soluções é utilizada para a criptografia de uma parte dos dados a serem processados para gerar uma parte dos dados criptografados ou para a descriptografia de uma parte dos dados criptografados para gerar uma parte dos dados a serem processados, a confidencialidade da criptografia dos dados criptografados é aprimorada. Além disso, a possibilidade de descriptografia dos dados criptografados que não podem mais ser descriptografados aproxima-se de zero.

Os meios de criptografia do aparelho de processamento de criptografia nas invenções desta especificação podem utilizar uma chave predeterminada e um algoritmo predeterminado para criptografar os dados de textos simples divisionais. Além disso, o aparelho de processamento de criptografia pode conter os meios de geração de pelo menos uma das chaves e um dos algoritmos utilizados para a criptografia com base na solução. Ainda, os meios de descriptografia do aparelho de processamento de descriptografia nas invenções desta especificação podem utilizar a chave e o algoritmo predeterminados para descriptografar os dados criptografados divisionais. Além disso, o aparelho de processamento de descriptografia pode conter os meios de geração de pelo menos uma das chaves e um dos algoritmos utilizados para a descriptografia com base na solução. Quando o aparelho de processamento de criptografia contém os meios de geração de pelo menos uma das chaves e um dos algoritmos utilizados para a criptografia com base na solução, o aparelho de processamento de descriptografia contém os meios de geração de pelo menos uma das chaves e um dos algoritmos utilizados para a descriptografia com base na solução. Se uma série de chaves ou algoritmos é utilizada para a criptografia de uma parte dos dados a serem processados para gerar uma parte dos dados criptografados

ou para a descriptografia de uma parte dos dados criptografados para gerar uma parte dos dados a serem processados e, posteriormente, as soluções são utilizadas para a geração das chaves ou dos algoritmos, a confidencialidade da criptografia dos dados criptografados é aprimorada.

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.

DESCRIÇÃO DETALHADA DA INVENÇÃO

Daqui em diante, uma abordagem preferida da presente invenção será descrita.

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 descriptografia 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 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 predeterminado de 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.

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 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 uma solução utilizada para a descriptografia de cada um dos dados criptografados divisionais.

As informações de especificação nesta abordagem são várias. 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 (daqui em diante, considerado como a "primeira informação de especificação" em alguns casos; 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 a unidade de especificação 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 25 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, um endereço do aparelho de processamento de descriptografia 2 correspondente a um destino dos dados criptografados, informações ambientais dos dados criptografados contendo o cabeçalho e semelhantes. 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.

As informações ambientais descritas acima são informações invariáveis predeterminadas, em outras palavras, informações predeterminadas que não variam nos dados de cabeçalho. As informações ambientais são geradas automaticamente com base na entrada de informações do dispositivo de entrada 25 pelo usuário ou pela função de um OS ou de outros programas instalados no dispositivo de criptografia 1. As informações ambientais podem, por exemplo, ser um nome de arquivo dos dados criptografados contendo as informações ambientais, informações da data e da hora da criação, informações da data e da hora da atualização (por exemplo, a data e a hora da última atualização), informações de um tipo ou formato de arquivo e semelhantes. Nesta abordagem, um nome de arquivo dos dados criptografados é utilizado como as informações

ambientais.

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). A quantidade real dos dados criptografados divisionais 502 é muito maior do que a ilustrada, mas a quantidade dos dados criptografados divisionais 502 ilustrados é bem 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 (extremidade esquerda nas Figuras 4(A) e 4(B) correspondentes ao cabeçalho dos dados criptografados), como ilustrado na Figura 4(A). As múltiplas partes dos 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. Note que 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 uma função de descriptografar os dados criptografados divisionais recebidos da unidade de pré-processamento 372.

Os detalhes da descriptografia serão descritos a seguir.

Note que 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 dado de textos simples divisional). 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 de múltiplas partes dos dados criptografados divisionais na unidade de descriptografia 373 em uma unidade para a 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 ou 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 um 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" da seção de controle principal 421, transforma os dados criptografados em dados "inúteis" com

um método, conforme descrito a seguir. Note que 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 processamento de transformação dos dados criptografados em dados "inúteis". O processamento é realizado através da conversão irreversível de pelo menos uma das soluções geradas antes da solução necessária para a descriptografia dos dados criptografados, que é necessária para a geração da solução necessária para a descriptografia dos dados criptografados a serem transformados em dados "inúteis" e das informações ambientais contidas nos dados criptografados necessários para gerar a solução necessária para a descriptografia dos dados criptografados a serem transformados em dados "inúteis", ou através da escrita dos dados apropriados sobre pelo menos uma das soluções e informações ambientais mencionadas acima. Em resumo, se a alteração irreversível for causada na solução anterior ou nas informações ambientais, os dados criptografados podem ser transformados em dados "inúteis". Para a escrita dos dados apropriados sobre a solução anterior ou as informações ambientais, o conteúdo dos dados a serem sobrescritos pode ser qualquer conteúdo, contanto que a sobrescrita evite que os dados criptografados sejam descriptografados. Para a sobrescrita, uma parte dos dados criptografados, por exemplo dados apropriados, tais como enumeração de dados como "0" ou "1" ou dados alternados "0" e "1", pode ser utilizada como o conteúdo dos dados para sobrescrita. A repetição de uma data de sobrescrita ou a repetição de informações de um tamanho de arquivo de outro arquivo atualizado por último pode ser utilizada como o dado para a sobrescrita. Os dados a serem escritos sobre uma parte dos dados criptografados podem ser alterados em qualquer cronograma. Para a conversão irreversível de uma parte dos dados

criptografados, é efetuado um cálculo na parte dos dados. Daí em diante, realiza-se o corte dos primeiros dígitos ou dos últimos dígitos do resultado do cálculo, o corte dos números decimais do resultado do cálculo, uma conversão JPEG na parte dos dados ou uma operação semelhante. O método de conversão pode não pode ser fixo e pode ser alterado em qualquer cronograma. Para a alteração irreversível ou a sobrescrita das informações ambientais correspondentes a uma parte dos dados criptografados, há a necessidade de especificar a "parte" dos dados criptografados a ser convertida ou sobrescrita.

É a seção de detecção 422 que tem uma função de especificar a "parte" dos dados criptografados. 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 irreversivelmente convertida ou sobrescrita a fim de que não seja descriptografada e contém as informações ambientais. A "parte" pode consistir nas próprias informações ambientais ou em uma faixa apropriada, que não seja tão grande, contendo as informações ambientais, como os dados de cabeçalho. Nesta abordagem, a seção de detecção 422 detecta a parte correspondente às informações ambientais nos dados criptografados. A seção de detecção 422 especifica a parte nos dados criptografados que deve ser excluída ou sobrescrita e notifica a seção de destruição 424 da parte especificada. A seção de destruição 424, que recebeu a notificação, sobrescreve ou converte irreversivelmente a parte dos dados criptografados que corresponde às informações ambientais e é especificada pela seção de detecção 422.

O temporizador 423 especifica uma data e uma hora do cronograma de sobrescrita ou conversão. 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, os dados "inúteis" obtidos dos dados criptografados e a notificação descrita acima para permitir que o dispositivo de criptografia 37 descriptografe os dados criptografados, dependendo do caso. 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 de acordo com 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 para a transmissão dos 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. Nesta abordagem, as informações ambientais, que são o nome de arquivo dos dados criptografados, também são inseridas do dispositivo de entrada 25. As informações ambientais também são transmitidas pela CPU 21 através do barramento 29 para a unidade de geração de cabeçalhos 279 no dispositivo de criptografia 27.

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 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.

Note que as soluções utilizadas para a criptografia dos dados a serem processados no aparelho de processamento de criptografia 1 não são necessárias para uma série de soluções iniciando com a primeira solução gerada no aparelho de processamento de criptografia 1. O motivo é, portanto, o seguinte. Por exemplo, 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, são necessárias as informações de especificação que indicam 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. Note que 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, os seguintes métodos são concebíveis: (1) um método de inclusão de um cálculo ascendente da solução anterior no processo de geração das soluções; (2) um método de inclusão de uma multiplicação das duas ou mais soluções anteriores no processo de geração das soluções; e um método de combinação dos métodos (1) e (2).

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). Note que 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) = $X_{02}X_{01}$ + α (α = uma matriz 8×8)

Esta é a primeira solução a ser gerada.

Neste documento, α é a informação ambiental. A informação ambiental α é obtida, por exemplo, seqüencialmente, atribuindo uma seqüência de dados representada por "1" e "0", que é obtida de códigos de caracteres binários constituindo o nome de arquivo, para os elementos da matriz 8×8. Se a quantidade de dígitos na seqüência de dados representada por "1" e "0", que é obtida de códigos de caracteres binários constituindo o nome de arquivo, for menor do que 64, que corresponde à quantidade dos elementos da matriz 8×8, a seqüência de dados é utilizada repetidamente. Deve ser notado que a maneira de utilizar as informações ambientais pode ser determinada de maneira adequada. Por exemplo, quando caracteres do alfabeto constituem o nome de arquivo, "A" pode ser convertido para 1, "B" para 2, "C" para 3, ... e "Z" para 26. Então, um valor numérico obtido pela adição ou pela multiplicação de todos os valores numéricos obtidos pela conversão dos alfabetos pode ser atribuído aos elementos da matriz 8×8.

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} + α

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) = $X_{N-1}X_{N-2} + \alpha$

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 (X_N), a enésima solução 1 (X_{N-1}) e a enésima solução 2 (X_{N-2}), em resumo, as duas soluções que são geradas por último, a penúltima e a última, 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).

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

Não é necessário utilizar a matriz α correspondente às informações ambientais para cada caso em que a solução é gerada. Por exemplo, α pode ser utilizada para a primeira solução (X_1) = $X_{02}X_{01} + \alpha$ 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 (X_N) = $X_{N-1}X_{N-2}$.

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

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

a fórmula a seguir também pode ser utilizada.

Note que 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) = $(X_{N-1})^P$ ($+\alpha$)

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

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

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).

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.

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, a primeira informação de especificação e as informações ambientais.

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).

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 dado de textos simples divisional), mas, nesta abordagem, os comprimentos de dados de todos os dados de textos simples divisionais são os mesmos (por exemplo, um comprimento de 8 bits). 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 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.

Deve ser notado 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.

Note que 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, deste modo, 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.

Note que, na 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 de 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, com relação ao 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 pré-processamento 372 extrai os dados de cabeçalho dos dados criptografados recebidos e também extrai as informações ambientais dos dados de cabeçalho para transmitir as informações ambientais extraídas 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 de especificação e nas informações ambientais recebidas (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. Nesta abordagem, a solução é gerada utilizando-se a solução inicial, as informações ambientais e as informações de especificação.

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, no caso em que a matriz inicial, o algoritmo para a geração das soluções e as informações ambientais são utilizados, 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 8x8 X à potência 'a', girando a matriz obtida em nx90°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 8x8 X correspondente à solução à potência 'a', girando a matriz no sentido horário em nx90°e depois multiplicando a matriz girada por Y quando os dados de textos simples criptografados de 8 bits forem a matriz 1x8 Y") e executa o processamento de descriptografia ao realizar, com a chave, um cálculo de acordo com a definição descrita acima.

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 as de informações de especificação contidas nos dados de textos simples divisionais para transmitir as informações de especificação extraídas 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, geram o algoritmo e a chave, respectivamente, ao utilizar a solução recebida e transmitem o algoritmo ou a chave gerado 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 de 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.

Note que, no exemplo descrito acima, tanto o algoritmo como a chave, utilizados para a geração dos dados criptografados, são gerados na unidade de geração de algoritmos 375 e na unidade de geração de chaves 376, respectivamente. Entretanto, quando o acordo para fixar pelo menos um dos algoritmos e uma das chaves é feito entre o aparelho de processamento de criptografia 1 e o aparelho de processamento de descriptografia 2, apenas um dos algoritmos e uma das chaves, que não está fixado, pode ser gerado com base na solução. Em tal caso, uma vez fixados um dos algoritmos e uma das chaves, os mesmos são sempre utilizados.

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 exemplos 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 associados aos dados criptografados e solta o ícone sobre outro ícone associado a um programa para a 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 é a parte correspondente às informações ambientais dos dados de

cabeçalho contidos nos dados criptografados, a seção de detecção 422 especifica uma área correspondente às informações ambientais 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 arbitrários 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 a fim de 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.

No exemplo 1 descrito acima, uma parte dos dados criptografados é destruída a fim de evitar que os dados criptografados sejam descriptografados, mas também é possível evitar que os dados criptografados sejam descriptografados sem destruir os dados criptografados.

Tal caso será descrito a seguir.

Neste caso, o usuário insere um comando de transformação dos dados criptografados em dados "inúteis" do dispositivo de entrada 35. Quando a seção de controle principal 421, que recebeu o comando, determina transformar os dados criptografados no que é mencionado como "inútil" na presente invenção, o dispositivo de entrada 35 transmite uma instrução de causar uma alteração irreversível na solução gerada antes da solução necessária para a descriptografia

dos dados criptografados, que é necessária para a geração da solução necessária para a descriptografia dos dados criptografados, para o dispositivo de descriptografia 37. Nesta abordagem, a solução inicial é indispensável para gerar a solução, como descrito acima. Nesta abordagem, o dispositivo de descriptografia 37, que recebeu a instrução de causar a alteração irreversível na solução necessária para a geração da solução para a descriptografia dos dados criptografados da seção de controle principal 421, converte de maneira irreversível a solução inicial ou escreve os dados arbitrários sobre a solução inicial para causar a alteração irreversível na solução inicial. Como a solução inicial é armazenada na unidade de geração de soluções 374 nesta abordagem, a unidade de geração de soluções 374 causa a alteração irreversível na solução inicial nela armazenada. Dessa maneira, os dados criptografados não podem mais ser descriptografados.

Note que, para ilustrar o processamento de evitar que os dados criptografados sejam descriptografados, foram descritos dois casos de exemplo, isto é, o caso em que a alteração irreversível é causada em uma parte (informações ambientais) dos dados criptografados e o caso em que a alteração irreversível é causada na solução inicial. Cada um dos dois casos de exemplo tem uma vantagem e uma desvantagem.

No último caso, não é necessário causar qualquer alteração nos próprios dados criptografados. Portanto, o último caso tem a vantagem de que os dados criptografados não podem ser descriptografados mesmo quando os dados criptografados são escritos em um meio de gravação como um CD-ROM (no qual a sobrescrita não é permitida (apenas leitura)). Essa vantagem é significativa no sentido de que os dados criptografados gravados em um meio de gravação desse tipo podem ser transformados em dados "inúteis" sem causar qualquer alteração nos próprios dados criptografados. Entretanto, o último caso tem a seguinte desvantagem. No último caso, uma vez que a alteração irreversível é causada na solução inicial, o aparelho de processamento de criptografia 1 e o aparelho de

processamento de descriptografia 2 não podem mais gerar uma solução comum. Como resultado, após a alteração irreversível ser causada na solução inicial, há uma possibilidade de que os dados criptografados obtidos no aparelho de processamento de criptografia 1 não possam ser descriptografados no aparelho de processamento de descriptografia 2. Tal situação pode ser evitada da seguinte maneira, por exemplo. Uma parte das soluções iniciais que são comuns ao aparelho de processamento de criptografia 1 e ao aparelho de processamento de descriptografia 2 e diferentes entre si é preparada antecipadamente. Neste caso, quando a alteração irreversível é causada em uma das soluções iniciais no aparelho de processamento de descriptografia 2, o aparelho de processamento de descriptografia 2 notifica o aparelho de processamento de criptografia 1 sobre a alteração irreversível assim causada para permitir que o aparelho de processamento de criptografia 1 e o aparelho de processamento de descriptografia 2 sempre utilizem as mesmas soluções iniciais de maneira seqüencial. Por outro lado, quando a alteração irreversível é causada na solução inicial, o aparelho de processamento de criptografia 1 é notificado sobre uma nova solução inicial gerada no aparelho de processamento de descriptografia 2 ou o aparelho de processamento de descriptografia 2 é notificado sobre uma nova solução inicial gerada no aparelho de processamento de criptografia 1 que foi notificado sobre a alteração irreversível causada na solução inicial. Dessa maneira, o aparelho de processamento de criptografia 1 e o aparelho de processamento de descriptografia 2 podem armazenar a mesma solução inicial nova, evitando, assim, a situação descrita acima. Entretanto, o último caso é desvantajoso no sentido de que o método, conforme descrito acima, precisa ser preparado para a descriptografia, no aparelho de processamento de descriptografia 2, dos dados criptografados gerados no aparelho de processamento de criptografia 1, mesmo após a alteração irreversível ser causada na solução inicial.

O primeiro caso tem uma desvantagem e uma vantagem opostas às do

último caso.

As desvantagens e as vantagens - no caso em que a alteração irreversível é causada em uma parte (informações ambientais) dos dados criptografados e no caso em que a alteração irreversível é causada na solução inicial no processamento a fim de evitar que os dados criptografados sejam descriptografados - são as mesmas que nos casos 2 e 3.

Note que o caso 1 pode ser executado mesmo se os dados criptografados não contiverem 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. Note que 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. Mais especificamente, o processamento de evitar que os dados criptografados sejam descriptografados é executado no aparelho de processamento de descriptografia 2. O processamento é executado, causando a alteração irreversível em uma parte (informações ambientais) dos dados criptografados ou causando a alteração irreversível na solução inicial.

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, 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 Caso 1 após a determinação como descrita acima. Mais especificamente, o processamento de evitar que os dados criptografados sejam descriptografados é executado no aparelho de processamento de descriptografia 2. O processamento é executado causando a alteração irreversível em uma parte (informações ambientais) dos dados criptografados ou causando a alteração irreversível na solução inicial.

REIVINDICAÇÕES

1. Um aparelho de processamento de descriptografia utilizado juntamente com um aparelho de processamento de criptografia para a criptografia de dados de textos simples a serem processados para obter dados criptografados, o aparelho de processamento de criptografia compreende:

meios de divisão para a divisão dos dados a serem processados em uma série de partes dos dados de textos simples divisionais, cada um sendo composto por um número predeterminado de bits;

meios de geração de soluções para a geração contínua de soluções, cada uma sendo determinada exclusivamente com base em soluções anteriores, os meios de geração de soluções armazenando uma solução inicial utilizada para gerar uma primeira solução para a geração contínua das soluções;

meios de criptografia para a criptografia dos dados de textos simples divisionais utilizando as soluções para converter os dados de textos simples divisionais em dados criptografados divisionais; e

meios de conexão para a conexão dos dados criptografados divisionais para obter os dados criptografados;

o aparelho de processamento de descriptografia compreende:

uma unidade de descriptografia contendo:

meios de divisão para a divisão dos dados criptografados em uma série de partes dos dados criptografados divisionais, cada um sendo composto por um número predeterminado de bits;

meios de geração de soluções para a geração contínua de soluções, cada uma sendo determinada exclusivamente com base em soluções anteriores, as soluções sendo geradas como as mesmas soluções geradas no aparelho de processamento de criptografia, os meios de geração de soluções armazenando uma solução inicial utilizada para gerar uma primeira solução para a geração contínua das soluções;

meios de descriptografia para a descriptografia dos dados criptografados divisionais utilizando as soluções para converter os dados criptografados divisionais em dados de textos simples divisionais; e

meios de conexão para a conexão dos dados de textos simples divisionais para obter os dados a serem processados;

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; e

meios de processamento para a destruição de uma solução gerada antes das soluções utilizadas para a descriptografia dos dados criptografados de maneira irreversível quando as informações do disparador de destruição são inseridas, a solução anterior sendo necessária para a geração das soluções utilizadas para a descriptografia dos dados criptografados.

2. Um aparelho de processamento de descriptografia utilizado juntamente com um aparelho de processamento de criptografia para a criptografia de dados de textos simples a serem processados para obter dados criptografados, o aparelho de processamento de criptografia compreende:

meios de divisão para a divisão dos dados a serem processados em uma série de partes dos dados de textos simples divisionais, cada um sendo composto por um número predeterminado de bits;

meios de geração de soluções para a geração contínua de soluções, cada uma sendo determinada exclusivamente com base em soluções anteriores e informações ambientais invariáveis a serem contidas nos dados criptografados a serem gerados, os meios de geração de soluções armazenando uma solução inicial utilizada para gerar uma primeira solução para a geração contínua das soluções;

meios de criptografia para a criptografia dos dados de textos simples divisionais utilizando as soluções para converter os dados de textos simples divisionais em dados criptografados divisionais; e

meios de conexão para a conexão dos dados criptografados divisionais para obter os dados criptografados contendo as informações ambientais,

o aparelho de processamento de descriptografia compreende:

uma unidade de descriptografia contendo:

meios de divisão para a divisão dos dados criptografados em uma série de partes dos dados criptografados divisionais, cada um sendo composto por um número predeterminado de bits;

meios de geração de soluções para a geração contínua de soluções, cada uma sendo determinada exclusivamente com base em soluções anteriores e informações ambientais contidas e lidas dos dados criptografados, as soluções sendo geradas como as mesmas soluções geradas no aparelho de processamento de criptografia, os meios de geração de soluções armazenando uma solução inicial utilizada para gerar uma primeira solução para a geração contínua das soluções;

meios de descriptografia para a descriptografia dos dados criptografados divisionais utilizando as soluções para converter os dados criptografados divisionais em dados de textos simples divisionais; e

meios de conexão para a conexão dos dados de textos simples divisionais para obter os dados a serem processados;

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; e

meios de processamento para a destruição das informações ambientais contidas nos dados criptografados de maneira irreversível quando as informações do disparador de destruição são inseridas, a solução anterior sendo necessária para a geração das soluções utilizadas para a descriptografia dos dados criptografados.

3. Um aparelho de processamento de descriptografia utilizado juntamente com um aparelho de processamento de criptografia para a criptografia de dados

de textos simples a serem processados para obter dados criptografados, o aparelho de processamento de criptografia compreende:

meios de divisão para a divisão dos dados a serem processados em uma série de partes dos dados de textos simples divisionais, cada um sendo composto por um número predeterminado de bits;

meios de geração de soluções para a geração contínua de soluções, cada uma sendo determinada exclusivamente com base em soluções anteriores, os meios de geração de soluções armazenando uma solução inicial utilizada para gerar uma primeira solução para a geração contínua das soluções;

meios de criptografia para a criptografia dos dados de textos simples divisionais utilizando as soluções para converter os dados de textos simples divisionais em dados criptografados divisionais;

meios de geração de informações de especificação do cronograma para a geração de informações de especificação do cronograma para especificar o cronograma a fim de evitar que os dados criptografados contendo as informações de especificação do cronograma sejam descriptografados; e

meios de conexão para a conexão dos dados criptografados divisionais para obter os dados criptografados contendo as informações de especificação do cronograma,

o aparelho de processamento de descriptografia compreende:

uma unidade de descriptografia contendo:

meios de divisão para a divisão dos dados criptografados em uma série de partes dos dados criptografados divisionais, cada um sendo composto por um número predeterminado de bits;

meios de geração de soluções para a geração contínua de soluções, cada uma sendo determinada exclusivamente com base em soluções anteriores, as soluções sendo geradas como as mesmas soluções geradas no aparelho de processamento de criptografia, os meios de geração de soluções armazenando uma solução inicial utilizada para gerar uma primeira solução para a

geração contínua das soluções;

meios de descriptografia para a descriptografia dos dados criptografados divisionais utilizando as soluções para converter os dados criptografados divisionais em dados de textos simples divisionais; e

meios de conexão para a conexão dos dados de textos simples divisionais para obter os dados a serem processados;

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

meios de processamento para a destruição de uma solução gerada antes das soluções utilizadas para a descriptografia dos dados criptografados de maneira irreversível, a solução anterior sendo necessária para a geração das soluções utilizadas para a descriptografia dos dados criptografados; os meios de processamento monitoram 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 destroem a solução no caso de o cronograma ter chegado.

4. Um aparelho de processamento de descriptografia utilizado juntamente com um aparelho de processamento de criptografia para a criptografia de dados de textos simples a serem processados para obter dados criptografados, o aparelho de processamento de criptografia compreende:

meios de divisão para a divisão dos dados a serem processados em uma série de partes dos dados de textos simples divisionais, cada um sendo composto por um número predeterminado de bits;

meios de geração de soluções para a geração contínua de soluções, cada uma sendo determinada exclusivamente com base em soluções anteriores e informações ambientais invariáveis a serem contidas nos dados criptografados a serem gerados, os meios de geração de soluções armazenando uma solução inicial utilizada para gerar uma primeira solução para a geração contínua das

soluções;

meios de criptografia para a criptografia dos dados de textos simples divisionais utilizando as soluções para converter os dados de textos simples divisionais em dados criptografados divisionais;

meios de geração de informações de especificação do cronograma para a geração de informações de especificação do cronograma para especificar o cronograma a fim de evitar que os dados criptografados contendo as informações de especificação do cronograma sejam descriptografados; e

meios de conexão para a conexão dos dados criptografados divisionais para obter os dados criptografados contendo as informações ambientais e as informações de especificação do cronograma,

o aparelho de processamento de descriptografia compreende:

uma unidade de descriptografia contendo:

meios de divisão para a divisão dos dados criptografados em uma série de partes dos dados criptografados divisionais, cada um sendo composto por um número predeterminado de bits;

meios de geração de soluções para a geração contínua de soluções, cada uma sendo determinada exclusivamente com base em soluções anteriores e informações ambientais contidas e lidas dos dados criptografados, as soluções sendo geradas como as mesmas soluções geradas no aparelho de processamento de criptografia, os meios de geração de soluções armazenando uma solução inicial utilizada para gerar uma primeira solução para a geração contínua das soluções;

meios de descriptografia para a descriptografia dos dados criptografados divisionais utilizando as soluções para converter os dados criptografados divisionais em dados de textos simples divisionais; e

meios de conexão para a conexão dos dados de textos simples divisionais para obter os dados a serem processados;

meios de leitura das informações de especificação do cronograma para a

leitura das informações de especificação do cronograma dos dados criptografados; e

meios de processamento para a destruição das informações ambientais contidas nos dados criptografados de maneira irreversível; os meios de processamento monitoram 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 destroem a solução no caso de o cronograma ter chegado.

5. Um aparelho de processamento de descriptografia utilizado juntamente com um aparelho de processamento de criptografia para a criptografia de dados de textos simples a serem processados para obter dados criptografados, o aparelho de processamento de criptografia compreende:

meios de divisão para a divisão dos dados a serem processados em uma série de partes dos dados de textos simples divisionais, cada um sendo composto por um número predeterminado de bits;

meios de geração de soluções para a geração contínua de soluções, cada uma sendo determinada exclusivamente com base em soluções anteriores, os meios de geração de soluções armazenando uma solução inicial utilizada para gerar uma primeira solução para a geração contínua das soluções;

meios de criptografia para a criptografia dos dados de textos simples divisionais utilizando as soluções para converter os dados de textos simples divisionais em dados criptografados divisionais;

meios de geração de informações de especificação do cronograma para a geração de informações de especificação do cronograma para especificar o cronograma a fim de evitar que os dados criptografados contendo as informações de especificação do cronograma sejam descriptografados; e

meios de conexão para a conexão dos dados criptografados divisionais para obter os dados criptografados contendo as informações de especificação do cronograma,

o aparelho de processamento de descriptografia compreende:

uma unidade de descriptografia contendo:

meios de divisão para a divisão dos dados criptografados em uma série de partes dos dados criptografados divisionais, cada um sendo composto por um número predeterminado de bits;

meios de geração de soluções para a geração contínua de soluções, cada uma sendo determinada exclusivamente com base em soluções anteriores, as soluções sendo geradas como as mesmas soluções geradas no aparelho de processamento de criptografia, os meios de geração de soluções armazenando uma solução inicial utilizada para gerar uma primeira solução para a geração contínua das soluções;

meios de descriptografia para a descriptografia dos dados criptografados divisionais utilizando as soluções para converter os dados criptografados divisionais em dados de textos simples divisionais; e

meios de conexão para a conexão dos dados de textos simples divisionais para obter os dados a serem processados;

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 são inseridas dos meios de entrada do disparador de descriptografia; e

meios de processamento para a recepção das informações de especificação do cronograma lidas pelos meios de leitura das informações de especificação do cronograma quando as informações do disparador de descriptografia são inseridas para monitorar se o cronograma especificado pelas informações de especificação do cronograma chegou e permitir que a unidade de descriptografia descriptografe os dados criptografados se o cronograma ainda não

chegou, causando uma alteração irreversível em uma solução gerada antes das soluções utilizadas para a descriptografia dos dados criptografados, a solução anterior sendo necessária para a geração das soluções utilizadas para a descriptografia dos dados criptografados, no caso de o cronograma ter chegado.

6. Um aparelho de processamento de descriptografia utilizado juntamente com um aparelho de processamento de criptografia para a criptografia de dados de textos simples a serem processados para obter dados criptografados, o aparelho de processamento de criptografia compreende:

meios de divisão para a divisão dos dados a serem processados em uma série de partes dos dados de textos simples divisionais, cada um sendo composto por um número predeterminado de bits;

meios de geração de soluções para a geração contínua de soluções, cada uma sendo determinada exclusivamente com base em soluções anteriores e informações ambientais invariáveis a serem contidas nos dados criptografados a serem gerados, os meios de geração de soluções armazenando uma solução inicial utilizada para gerar uma primeira solução para a geração contínua das soluções;

meios de criptografia para a criptografia dos dados de textos simples divisionais utilizando as soluções para converter os dados de textos simples divisionais em dados criptografados divisionais;

meios de geração de informações de especificação do cronograma para a geração de informações de especificação do cronograma para especificar o cronograma a fim de evitar que os dados criptografados contendo as informações de especificação do cronograma sejam descriptografados; e

meios de conexão para a conexão dos dados criptografados divisionais para obter os dados criptografados contendo as informações ambientais e as informações de especificação do cronograma,

o aparelho de processamento de descriptografia compreende:

uma unidade de descriptografia contendo:

meios de divisão para a divisão dos dados criptografados em uma série de partes dos dados criptografados divisionais, cada um sendo composto por um número predeterminado de bits;

meios de geração de soluções para a geração contínua de soluções, cada uma sendo determinada exclusivamente com base em soluções anteriores e informações ambientais contidas e lidas dos dados criptografados, as soluções sendo geradas como as mesmas soluções geradas no aparelho de processamento de criptografia, os meios de geração de soluções armazenando uma solução inicial utilizada para gerar uma primeira solução para a geração contínua das soluções;

meios de descriptografia para a descriptografia dos dados criptografados divisionais utilizando as soluções para converter os dados criptografados divisionais em dados de textos simples divisionais; e

meios de conexão para a conexão dos dados de textos simples divisionais para obter os dados a serem processados;

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 são inseridas dos meios de entrada do disparador de descriptografia; e

meios de processamento para a recepção das informações de especificação do cronograma lidas pelos meios de leitura das informações de especificação do cronograma quando as informações do disparador de descriptografia são inseridas para determinar se o cronograma especificado pelas informações de especificação do cronograma chegou e permitir que a unidade de descriptografia descriptografe os dados criptografados se o cronograma ainda não chegou, causando uma alteração irreversível nas informações ambientais

contidas nos dados criptografados no caso de o cronograma ter chegado.

7. Um aparelho de processamento de descriptografia, de acordo com a reivindicação 1, 3 ou 5, caracterizado pelo fato de que os meios de processamento causam a alteração irreversível na solução gerada antes das soluções utilizadas para a descriptografia dos dados criptografados, a solução anterior sendo necessária para a geração das soluções utilizadas para a descriptografia dos dados criptografados, por meio da escrita dos dados apropriados sobre a solução anterior ou da conversão irreversível da solução anterior.

8. Um aparelho de processamento de descriptografia, de acordo com a reivindicação 2, 4 ou 6, caracterizado pelo fato de que os meios de processamento causam a alteração irreversível nas informações ambientais por meio da escrita dos dados apropriados sobre as informações ambientais ou da conversão irreversível das informações ambientais.

9. Um aparelho de processamento de descriptografia, de acordo com uma das reivindicações 1 a 6, caracterizado por:

os meios de geração de soluções no aparelho de processamento de criptografia geram as soluções sempre que os meios de criptografia criptografam os dados de textos simples divisionais; e

os meios de geração de soluções no aparelho de processamento de descriptografia geram as soluções sempre que os meios de descriptografia descriptografam os dados criptografados divisionais.

10. Um aparelho de processamento de descriptografia, de acordo com uma das reivindicações 1 a 6, caracterizado por:

os meios de criptografia no aparelho de processamento de criptografia utilizam uma chave predeterminada e um algoritmo predeterminado para criptografar os dados de textos simples divisionais, o aparelho de processamento de criptografia contendo meios de geração de pelo menos uma das chaves predeterminadas e um dos algoritmos predeterminados utilizados para a

criptografia com base nas soluções; e

os meios de descriptografia no aparelho de processamento de descriptografia utilizam uma chave predeterminada e um algoritmo predeterminado para descriptografar os dados criptografados divisionais, o aparelho de processamento de descriptografia contendo meios de geração de pelo menos uma das chaves predeterminadas e um dos algoritmos predeterminados utilizados para a descriptografia com base nas soluções.

11. Um método de processamento de dados executado em um aparelho de processamento de descriptografia utilizado juntamente com um aparelho de processamento de criptografia para a criptografia de dados de textos simples a serem processados para obter dados criptografados, o aparelho de processamento de criptografia compreende:

meios de divisão para a divisão dos dados a serem processados em uma série de partes dos dados de textos simples divisionais, cada um sendo composto por um número predeterminado de bits;

meios de geração de soluções para a geração contínua de soluções, cada uma sendo determinada exclusivamente com base em soluções anteriores, os meios de geração de soluções armazenando uma solução inicial utilizada para gerar uma primeira solução para a geração contínua das soluções;

meios de criptografia para a criptografia dos dados de textos simples divisionais utilizando as soluções para converter os dados de textos simples divisionais em dados criptografados divisionais; e

meios de conexão para a conexão dos dados criptografados divisionais para obter os dados criptografados,

o aparelho de processamento de descriptografia compreende:

uma unidade de descriptografia contendo:

meios de divisão para a divisão dos dados criptografados em uma série de partes dos dados criptografados divisionais, cada um sendo composto por um número predeterminado de bits;

meios de geração de soluções para a geração contínua de soluções, cada uma sendo determinada exclusivamente com base em soluções anteriores, as soluções sendo geradas como as mesmas soluções geradas no aparelho de processamento de criptografia, os meios de geração de soluções armazenando uma solução inicial utilizada para gerar uma primeira solução para a geração contínua das soluções;

meios de descriptografia para a descriptografia dos dados criptografados divisionais utilizando as soluções para converter os dados criptografados divisionais em dados de textos simples divisionais; e

meios de conexão para a conexão dos dados de textos simples divisionais para obter os dados a serem processados;

meios de entrada do disparador de destruição; e

meios de processamento,

o método de processamento de dados compreende as etapas, executadas pelos meios de processamento, de:

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; e

provocação de uma alteração irreversível em uma solução gerada antes das soluções utilizadas para a descriptografia dos dados criptografados, a solução anterior sendo necessária para a geração das soluções utilizadas para a descriptografia dos dados criptografados, quando as informações do disparador de destruição são recebidas.

12. Um método de processamento de dados executado em um aparelho de processamento de descriptografia utilizado juntamente com um aparelho de processamento de criptografia para a criptografia de dados de textos simples a serem processados para obter dados criptografados, o aparelho de processamento de criptografia compreende:

meios de divisão para a divisão dos dados a serem processados em uma

série de partes dos dados de textos simples divisionais, cada um sendo composto por um número predeterminado de bits;

meios de geração de soluções para a geração contínua de soluções, cada uma sendo determinada exclusivamente com base em soluções anteriores e informações ambientais invariáveis a serem contidas nos dados criptografados a serem gerados, os meios de geração de soluções armazenando uma solução inicial utilizada para gerar uma primeira solução para a geração contínua das soluções;

meios de criptografia para a criptografia dos dados de textos simples divisionais utilizando as soluções para converter os dados de textos simples divisionais em dados criptografados divisionais; e

meios de conexão para a conexão dos dados criptografados divisionais para obter os dados criptografados contendo as informações ambientais,

o aparelho de processamento de descriptografia compreende:

uma unidade de descriptografia contendo:

meios de divisão para a divisão dos dados criptografados em uma série de partes dos dados criptografados divisionais, cada um sendo composto por um número predeterminado de bits;

meios de geração de soluções para a geração contínua de soluções, cada uma sendo determinada exclusivamente com base em soluções anteriores e informações ambientais contidas e lidas dos dados criptografados, as soluções sendo geradas como as mesmas soluções geradas no aparelho de processamento de criptografia, os meios de geração de soluções armazenando uma solução inicial utilizada para gerar uma primeira solução para a geração contínua das soluções;

meios de descriptografia para a descriptografia dos dados criptografados divisionais utilizando as soluções para converter os dados criptografados divisionais em dados de textos simples divisionais; e

meios de conexão para a conexão dos dados de textos simples

divisionais para obter os dados a serem processados;

meios de entrada do disparador de destruição; e

meios de processamento,

o método de processamento de dados compreende as etapas, executadas pelos meios de processamento, de:

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; e

provocação de uma alteração irreversível nas informações ambientais contidas nos dados criptografados quando as informações do disparador de destruição são recebidas.

13. Um método de processamento de dados executado em um aparelho de processamento de descriptografia utilizado juntamente com um aparelho de processamento de criptografia para a criptografia de dados de textos simples a serem processados para obter dados criptografados, o aparelho de processamento de criptografia compreende:

meios de divisão para a divisão dos dados a serem processados em uma série de partes dos dados de textos simples divisionais, cada um sendo composto por um número predeterminado de bits;

meios de geração de soluções para a geração contínua de soluções, cada uma sendo determinada exclusivamente com base em soluções anteriores, os meios de geração de soluções armazenando uma solução inicial utilizada para gerar uma primeira solução para a geração contínua das soluções;

meios de criptografia para a criptografia dos dados de textos simples divisionais utilizando as soluções para converter os dados de textos simples divisionais em dados criptografados divisionais;

meios de geração de informações de especificação do cronograma para a geração de informações de especificação do cronograma para especificar o cronograma a fim de evitar que os dados criptografados contendo as informações

de especificação do cronograma sejam descriptografados; e

meios de conexão para a conexão dos dados criptografados divisionais para obter os dados criptografados contendo as informações de especificação do cronograma,

o aparelho de processamento de descriptografia compreende:

uma unidade de descriptografia contendo:

meios de divisão para a divisão dos dados criptografados em uma série de partes dos dados criptografados divisionais, cada um sendo composto por um número predeterminado de bits;

meios de geração de soluções para a geração contínua de soluções, cada uma sendo determinada exclusivamente com base em soluções anteriores, as soluções sendo geradas como as mesmas soluções geradas no aparelho de processamento de criptografia, os meios de geração de soluções armazenando uma solução inicial utilizada para gerar uma primeira solução para a geração contínua das soluções;

meios de descriptografia para a descriptografia dos dados criptografados divisionais utilizando as soluções para converter os dados criptografados divisionais em dados de textos simples divisionais; e

meios de conexão para a conexão dos dados de textos simples divisionais para obter os dados a serem processados; e

meios de processamento,

o método de processamento de dados compreende as etapas, executadas pelos meios de processamento, de:

leitura das informações de especificação do cronograma dos dados criptografados; e

monitorar se o cronograma especificado pelas informações de especificação do cronograma lidas na etapa de leitura das informações de especificação do cronograma chegou, causando uma alteração irreversível em uma solução gerada antes das soluções utilizadas para a descriptografia dos

dados criptografados, a solução anterior sendo necessária para a geração das soluções utilizadas para a descriptografia dos dados criptografados, no caso de o cronograma ter chegado.

14. Um método de processamento de dados executado em um aparelho de processamento de descriptografia utilizado juntamente com um aparelho de processamento de criptografia para a criptografia de dados de textos simples a serem processados para obter dados criptografados, o aparelho de processamento de criptografia compreende:

meios de divisão para a divisão dos dados a serem processados em uma série de partes dos dados de textos simples divisionais, cada um sendo composto por um número predeterminado de bits;

meios de geração de soluções para a geração contínua de soluções, cada uma sendo determinada exclusivamente com base em soluções anteriores e informações ambientais invariáveis a serem contidas nos dados criptografados a serem gerados, os meios de geração de soluções armazenando uma solução inicial utilizada para gerar uma primeira solução para a geração contínua das soluções;

meios de criptografia para a criptografia dos dados de textos simples divisionais utilizando as soluções para converter os dados de textos simples divisionais em dados criptografados divisionais;

meios de geração de informações de especificação do cronograma para a geração de informações de especificação do cronograma para especificar o cronograma a fim de evitar que os dados criptografados contendo as informações de especificação do cronograma sejam descriptografados; e

meios de conexão para a conexão dos dados criptografados divisionais para obter os dados criptografados contendo as informações ambientais e as informações de especificação do cronograma,

o aparelho de processamento de descriptografia compreende:

uma unidade de descriptografia contendo:

meios de divisão para a divisão dos dados criptografados em uma série de partes dos dados criptografados divisionais, cada um sendo composto por um número predeterminado de bits;

meios de geração de soluções para a geração contínua de soluções, cada uma sendo determinada exclusivamente com base em soluções anteriores e informações ambientais contidas e lidas dos dados criptografados, as soluções sendo geradas como as mesmas soluções geradas no aparelho de processamento de criptografia, os meios de geração de soluções armazenando uma solução inicial utilizada para gerar uma primeira solução para a geração contínua das soluções;

meios de descriptografia para a descriptografia dos dados criptografados divisionais utilizando as soluções para converter os dados criptografados divisionais em dados de textos simples divisionais; e

meios de conexão para a conexão dos dados de textos simples divisionais para obter os dados a serem processados; e

meios de processamento,

o método de processamento de dados compreende as etapas, executadas pelos meios de processamento, de:

leitura das informações de especificação do cronograma dos dados criptografados; e

monitorar se o cronograma especificado pelas informações de especificação do cronograma lidas na etapa de leitura das informações de especificação do cronograma chegou, causando uma alteração irreversível nas informações ambientais contidas nos dados criptografados no caso de o cronograma ter chegado.

15. Um método de processamento de dados executado em um aparelho de processamento de descriptografia utilizado juntamente com um aparelho de processamento de criptografia para a criptografia de dados de textos simples a serem processados para obter dados criptografados, o aparelho de

processamento de criptografia compreende:

meios de divisão para a divisão dos dados a serem processados em uma série de partes dos dados de textos simples divisionais, cada um sendo composto por um número predeterminado de bits;

meios de geração de soluções para a geração contínua de soluções, cada uma sendo determinada exclusivamente com base em soluções anteriores, os meios de geração de soluções armazenando uma solução inicial utilizada para gerar uma primeira solução para a geração contínua das soluções;

meios de criptografia para a criptografia dos dados de textos simples divisionais utilizando as soluções para converter os dados de textos simples divisionais em dados criptografados divisionais;

meios de geração de informações de especificação do cronograma para a geração de informações de especificação do cronograma para especificar o cronograma a fim de evitar que os dados criptografados contendo as informações de especificação do cronograma sejam descriptografados; e

meios de conexão para a conexão dos dados criptografados divisionais para obter os dados criptografados contendo as informações de especificação do cronograma,

o aparelho de processamento de descriptografia compreende:

uma unidade de descriptografia contendo:

meios de divisão para a divisão dos dados criptografados em uma série de partes dos dados criptografados divisionais, cada um sendo composto por um número predeterminado de bits;

meios de geração de soluções para a geração contínua de soluções, cada uma sendo determinada exclusivamente com base em soluções anteriores, as soluções sendo geradas como as mesmas soluções geradas no aparelho de processamento de criptografia, os meios de geração de soluções armazenando uma solução inicial utilizada para gerar uma primeira solução para a geração contínua das soluções;

meios de descriptografia para a descriptografia dos dados criptografados divisionais utilizando as soluções para converter os dados criptografados divisionais em dados de textos simples divisionais; e

meios de conexão para a conexão dos dados de textos simples divisionais para obter os dados a serem processados;

meios de entrada do disparador de descriptografia; e

meios de processamento,

o método de processamento de dados compreende as etapas, executadas pelos meios de processamento, de:

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 as informações do disparador de descriptografia são inseridas dos meios de entrada do disparador de descriptografia; e

recepção das informações de especificação do cronograma lidas na etapa de leitura das informações de especificação do cronograma quando as informações do disparador de descriptografia são inseridas para determinar se o cronograma especificado pelas informações de especificação do cronograma chegou e permitir que a unidade de descriptografia descriptografe os dados criptografados se o cronograma ainda não chegou, causando uma alteração irreversível em uma solução gerada antes das soluções utilizadas para a descriptografia dos dados criptografados, a solução anterior sendo necessária para a geração das soluções utilizadas para a descriptografia dos dados criptografados, no caso de o cronograma ter chegado.

16. Um método de processamento de dados executado em um aparelho de processamento de descriptografia utilizado juntamente com um aparelho de processamento de criptografia para a criptografia de dados de textos simples a serem processados para obter dados criptografados, o aparelho de

processamento de criptografia compreende:

meios de divisão para a divisão dos dados a serem processados em uma série de partes dos dados de textos simples divisionais, cada um sendo composto por um número predeterminado de bits;

meios de geração de soluções para a geração contínua de soluções, cada uma sendo determinada exclusivamente com base em soluções anteriores e informações ambientais invariáveis a serem contidas nos dados criptografados a serem gerados, os meios de geração de soluções armazenando uma solução inicial utilizada para gerar uma primeira solução para a geração contínua das soluções;

meios de criptografia para a criptografia dos dados de textos simples divisionais utilizando as soluções para converter os dados de textos simples divisionais em dados criptografados divisionais;

meios de geração de informações de especificação do cronograma para a geração de informações de especificação do cronograma para especificar o cronograma a fim de evitar que os dados criptografados contendo as informações de especificação do cronograma sejam descriptografados; e

meios de conexão para a conexão dos dados criptografados divisionais para obter os dados criptografados contendo as informações ambientais e as informações de especificação do cronograma,

o aparelho de processamento de descriptografia compreende:

uma unidade de descriptografia contendo:

meios de divisão para a divisão dos dados criptografados em uma série de partes dos dados criptografados divisionais, cada um sendo composto por um número predeterminado de bits;

meios de geração de soluções para a geração contínua de soluções, cada uma sendo determinada exclusivamente com base em soluções anteriores e informações ambientais contidas e lidas dos dados criptografados, as soluções sendo geradas como as mesmas soluções geradas no aparelho de

processamento de criptografia, os meios de geração de soluções armazenando uma solução inicial utilizada para gerar uma primeira solução para a geração contínua das soluções;

meios de descriptografia para a descriptografia dos dados criptografados divisionais utilizando as soluções para converter os dados criptografados divisionais em dados de textos simples divisionais; e

meios de conexão para a conexão dos dados de textos simples divisionais para obter os dados a serem processados;

meios de entrada do disparador de descriptografia; e

meios de processamento,

o método de processamento de dados compreende as etapas, executadas pelos meios de processamento, de:

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 as informações do disparador de descriptografia são inseridas dos meios de entrada do disparador de descriptografia; e

recepção das informações de especificação do cronograma lidas na etapa de leitura das informações de especificação do cronograma quando as informações do disparador de descriptografia são inseridas para determinar se o cronograma especificado pelas informações de especificação do cronograma chegou e permitir que a unidade de descriptografia descriptografe os dados criptografados se o cronograma ainda não chegou, causando uma alteração irreversível nas informações ambientais contidas nos dados criptografados no caso de o cronograma ter chegado.

17. Um programa computadorizado para um computador como um aparelho de processamento de descriptografia utilizado juntamente com um aparelho de processamento de criptografia para a criptografia de dados de textos

simples a serem processados para obter dados criptografados, o aparelho de processamento de criptografia compreende:

meios de divisão para a divisão dos dados a serem processados em uma série de partes dos dados de textos simples divisionais, cada um sendo composto por um número predeterminado de bits;

meios de geração de soluções para a geração contínua de soluções, cada uma sendo determinada exclusivamente com base em soluções anteriores, os meios de geração de soluções armazenando uma solução inicial utilizada para gerar uma primeira solução para a geração contínua das soluções;

meios de criptografia para a criptografia dos dados de textos simples divisionais utilizando as soluções para converter os dados de textos simples divisionais em dados criptografados divisionais; e

meios de conexão para a conexão dos dados criptografados divisionais para obter os dados criptografados,

o aparelho de processamento de descriptografia compreende:

uma unidade de descriptografia contendo:

meios de divisão para a divisão dos dados criptografados em uma série de partes dos dados criptografados divisionais, cada um sendo composto por um número predeterminado de bits;

meios de geração de soluções para a geração contínua de soluções, cada uma sendo determinada exclusivamente com base em soluções anteriores, as soluções sendo geradas como as mesmas soluções geradas no aparelho de processamento de criptografia, os meios de geração de soluções armazenando uma solução inicial utilizada para gerar uma primeira solução para a geração contínua das soluções;

meios de descriptografia para a descriptografia dos dados criptografados divisionais utilizando as soluções para converter os dados criptografados divisionais em dados de textos simples divisionais; e

meios de conexão para a conexão dos dados de textos simples

divisionais para obter os dados a serem processados;

meios de entrada do disparador de destruição; e

o computador também conectado,

o programa computadorizado é caracterizado por fazer com que o computador execute as etapas de:

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; e

provocação de uma alteração irreversível em uma solução gerada antes das soluções utilizadas para a descriptografia dos dados criptografados, a solução anterior sendo necessária para a geração das soluções utilizadas para a descriptografia dos dados criptografados, quando as informações do disparador de destruição são recebidas.

18. Um programa computadorizado para um computador como um aparelho de processamento de descriptografia utilizado juntamente com um aparelho de processamento de criptografia para a criptografia de dados de textos simples a serem processados para obter dados criptografados, o aparelho de processamento de criptografia compreende:

meios de divisão para a divisão dos dados a serem processados em uma série de partes dos dados de textos simples divisionais, cada um sendo composto por um número predeterminado de bits;

meios de geração de soluções para a geração contínua de soluções, cada uma sendo determinada exclusivamente com base em soluções anteriores e informações ambientais invariáveis a serem contidas nos dados criptografados a serem gerados, os meios de geração de soluções armazenando uma solução inicial utilizada para gerar uma primeira solução para a geração contínua das soluções;

meios de criptografia para a criptografia dos dados de textos simples divisionais utilizando as soluções para converter os dados de textos simples

divisionais em dados criptografados divisionais; e

meios de conexão para a conexão dos dados criptografados divisionais para obter os dados criptografados contendo as informações ambientais,

o aparelho de processamento de descriptografia compreende:

uma unidade de descriptografia contendo:

meios de divisão para a divisão dos dados criptografados em uma série de partes dos dados criptografados divisionais, cada um sendo composto por um número predeterminado de bits;

meios de geração de soluções para a geração contínua de soluções, cada uma sendo determinada exclusivamente com base em soluções anteriores e informações ambientais contidas e lidas dos dados criptografados, as soluções sendo geradas como as mesmas soluções geradas no aparelho de processamento de criptografia, os meios de geração de soluções armazenando uma solução inicial utilizada para gerar uma primeira solução para a geração contínua das soluções;

meios de descriptografia para a descriptografia dos dados criptografados divisionais utilizando as soluções para converter os dados criptografados divisionais em dados de textos simples divisionais; e

meios de conexão para a conexão dos dados de textos simples divisionais para obter os dados a serem processados;

meios de entrada do disparador de destruição; e

o computador também conectado,

o programa computadorizado é caracterizado por fazer com que o computador execute as etapas de:

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; e

provocação de uma alteração irreversível nas informações ambientais contidas nos dados criptografados quando as informações do disparador de

destruição são recebidas.

19. Um programa computadorizado para um computador como um aparelho de processamento de descriptografia utilizado juntamente com um aparelho de processamento de criptografia para a criptografia de dados de textos simples a serem processados para obter dados criptografados, o aparelho de processamento de criptografia compreende:

meios de divisão para a divisão dos dados a serem processados em uma série de partes dos dados de textos simples divisionais, cada um sendo composto por um número predeterminado de bits;

meios de geração de soluções para a geração contínua de soluções, cada uma sendo determinada exclusivamente com base em soluções anteriores, os meios de geração de soluções armazenando uma solução inicial utilizada para gerar uma primeira solução para a geração contínua das soluções;

meios de criptografia para a criptografia dos dados de textos simples divisionais utilizando as soluções para converter os dados de textos simples divisionais em dados criptografados divisionais;

meios de geração de informações de especificação do cronograma para a geração de informações de especificação do cronograma para especificar o cronograma a fim de evitar que os dados criptografados contendo as informações de especificação do cronograma sejam descriptografados; e

meios de conexão para a conexão dos dados criptografados divisionais para obter os dados criptografados contendo as informações de especificação do cronograma,

o aparelho de processamento de descriptografia compreende:

uma unidade de descriptografia contendo:

meios de divisão para a divisão dos dados criptografados em uma série de partes dos dados criptografados divisionais, cada um sendo composto por um número predeterminado de bits;

meios de geração de soluções para a geração contínua de

soluções, cada uma sendo determinada exclusivamente com base em soluções anteriores, as soluções sendo geradas como as mesmas soluções geradas no aparelho de processamento de criptografia, os meios de geração de soluções armazenando uma solução inicial utilizada para gerar uma primeira solução para a geração contínua das soluções;

meios de descriptografia para a descriptografia dos dados criptografados divisionais utilizando as soluções para converter os dados criptografados divisionais em dados de textos simples divisionais; e

meios de conexão para a conexão dos dados de textos simples divisionais para obter os dados a serem processados; e

o computador também conectado,

o programa computadorizado é caracterizado por fazer com que o computador execute as etapas de:

leitura das informações de especificação do cronograma dos dados criptografados; e

monitorar se o cronograma especificado pelas informações de especificação do cronograma lidas na etapa de leitura das informações de especificação do cronograma chegou, causando uma alteração irreversível em uma solução gerada antes das soluções utilizadas para a descriptografia dos dados criptografados, a solução anterior sendo necessária para a geração das soluções utilizadas para a descriptografia dos dados criptografados, no caso de o cronograma ter chegado.

20. Um programa computadorizado para um computador como um aparelho de processamento de descriptografia utilizado juntamente com um aparelho de processamento de criptografia para a criptografia de dados de textos simples a serem processados para obter dados criptografados, o aparelho de processamento de criptografia compreende:

meios de divisão para a divisão dos dados a serem processados em uma série de partes dos dados de textos simples divisionais, cada um sendo composto

por um número predeterminado de bits;

meios de geração de soluções para a geração contínua de soluções, cada uma sendo determinada exclusivamente com base em soluções anteriores e informações ambientais invariáveis a serem contidas nos dados criptografados a serem gerados, os meios de geração de soluções armazenando uma solução inicial utilizada para gerar uma primeira solução para a geração contínua das soluções;

meios de criptografia para a criptografia dos dados de textos simples divisionais utilizando as soluções para converter os dados de textos simples divisionais em dados criptografados divisionais;

meios de geração de informações de especificação do cronograma para a geração de informações de especificação do cronograma para especificar o cronograma a fim de evitar que os dados criptografados contendo as informações de especificação do cronograma sejam descriptografados; e

meios de conexão para a conexão dos dados criptografados divisionais para obter os dados criptografados contendo as informações ambientais e as informações de especificação do cronograma,

o aparelho de processamento de descriptografia compreende:

uma unidade de descriptografia contendo:

meios de divisão para a divisão dos dados criptografados em uma série de partes dos dados criptografados divisionais, cada um sendo composto por um número predeterminado de bits;

meios de geração de soluções para a geração contínua de soluções, cada uma sendo determinada exclusivamente com base em soluções anteriores e informações ambientais contidas e lidas dos dados criptografados, as soluções sendo geradas como as mesmas soluções geradas no aparelho de processamento de criptografia, os meios de geração de soluções armazenando uma solução inicial utilizada para gerar uma primeira solução para a geração contínua das soluções;

meios de descriptografia para a descriptografia dos dados criptografados divisionais utilizando as soluções para converter os dados criptografados divisionais em dados de textos simples divisionais; e

meios de conexão para a conexão dos dados de textos simples divisionais para obter os dados a serem processados; e

o computador também conectado,

o programa computadorizado é caracterizado por fazer com que o computador execute as etapas de:

leitura das informações de especificação do cronograma dos dados criptografados; e

monitorar se o cronograma especificado pelas informações de especificação do cronograma lidas na etapa de leitura das informações de especificação do cronograma chegou, causando uma alteração irreversível nas informações ambientais contidas nos dados criptografados no caso de o cronograma ter chegado.

21. Um programa computadorizado para um computador como um aparelho de processamento de descriptografia utilizado juntamente com um aparelho de processamento de criptografia para a criptografia de dados de textos simples a serem processados para obter dados criptografados, o aparelho de processamento de criptografia compreende:

meios de divisão para a divisão dos dados a serem processados em uma série de partes dos dados de textos simples divisionais, cada um sendo composto por um número predeterminado de bits;

meios de geração de soluções para a geração contínua de soluções, cada uma sendo determinada exclusivamente com base em soluções anteriores, os meios de geração de soluções armazenando uma solução inicial utilizada para gerar uma primeira solução para a geração contínua das soluções;

meios de criptografia para a criptografia dos dados de textos simples divisionais utilizando as soluções para converter os dados de textos simples

divisionais em dados criptografados divisionais;

meios de geração de informações de especificação do cronograma para a geração de informações de especificação do cronograma para especificar o cronograma a fim de evitar que os dados criptografados contendo as informações de especificação do cronograma sejam descriptografados; e

meios de conexão para a conexão dos dados criptografados divisionais para obter os dados criptografados contendo as informações de especificação do cronograma,

o aparelho de processamento de descriptografia compreende:

uma unidade de descriptografia contendo:

meios de divisão para a divisão dos dados criptografados em uma série de partes dos dados criptografados divisionais, cada um sendo composto por um número predeterminado de bits;

meios de geração de soluções para a geração contínua de soluções, cada uma sendo determinada exclusivamente com base em soluções anteriores, as soluções sendo geradas como as mesmas soluções geradas no aparelho de processamento de criptografia, os meios de geração de soluções armazenando uma solução inicial utilizada para gerar uma primeira solução para a geração contínua das soluções;

meios de descriptografia para a descriptografia dos dados criptografados divisionais utilizando as soluções para converter os dados criptografados divisionais em dados de textos simples divisionais; e

meios de conexão para a conexão dos dados de textos simples divisionais para obter os dados a serem processados;

meios de entrada do disparador de descriptografia; e

o computador também conectado,

o programa computadorizado é caracterizado por fazer com que o computador execute as etapas de:

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 as informações do disparador de descriptografia são inseridas dos meios de entrada do disparador de descriptografia; e

recepção das informações de especificação do cronograma lidas na etapa de leitura das informações de especificação do cronograma quando as informações do disparador de descriptografia são inseridas para determinar se o cronograma especificado pelas informações de especificação do cronograma chegou e permitir que a unidade de descriptografia descriptografe os dados criptografados se o cronograma ainda não chegou, causando uma alteração irreversível em uma solução gerada antes das soluções utilizadas para a descriptografia dos dados criptografados, a solução anterior sendo necessária para a geração das soluções utilizadas para a descriptografia dos dados criptografados, no caso de o cronograma ter chegado.

22. Um programa computadorizado para um computador como um aparelho de processamento de descriptografia utilizado juntamente com um aparelho de processamento de criptografia para a criptografia de dados de textos simples a serem processados para obter dados criptografados, o aparelho de processamento de criptografia compreende:

meios de divisão para a divisão dos dados a serem processados em uma série de partes dos dados de textos simples divisionais, cada um sendo composto por um número predeterminado de bits;

meios de geração de soluções para a geração contínua de soluções, cada uma sendo determinada exclusivamente com base em soluções anteriores e informações ambientais invariáveis a serem contidas nos dados criptografados a serem gerados, os meios de geração de soluções armazenando uma solução inicial utilizada para gerar uma primeira solução para a geração contínua das soluções;

meios de criptografia para a criptografia dos dados de textos simples divisionais utilizando as soluções para converter os dados de textos simples divisionais em dados criptografados divisionais;

meios de geração de informações de especificação do cronograma para a geração de informações de especificação do cronograma para especificar o cronograma a fim de evitar que os dados criptografados contendo as informações de especificação do cronograma sejam descriptografados; e

meios de conexão para a conexão dos dados criptografados divisionais para obter os dados criptografados contendo as informações ambientais e as informações de especificação do cronograma,

o aparelho de processamento de descriptografia compreende:

uma unidade de descriptografia contendo:

meios de divisão para a divisão dos dados criptografados em uma série de partes dos dados criptografados divisionais, cada um sendo composto por um número predeterminado de bits;

meios de geração de soluções para a geração contínua de soluções, cada uma sendo determinada exclusivamente com base em soluções anteriores e informações ambientais contidas e lidas dos dados criptografados, as soluções sendo geradas como as mesmas soluções geradas no aparelho de processamento de criptografia, os meios de geração de soluções armazenando uma solução inicial utilizada para gerar uma primeira solução para a geração contínua das soluções;

meios de descriptografia para a descriptografia dos dados criptografados divisionais utilizando as soluções para converter os dados criptografados divisionais em dados de textos simples divisionais; e

meios de conexão para a conexão dos dados de textos simples divisionais para obter os dados a serem processados;

meios de entrada do disparador de descriptografia; e

o computador também conectado,

o programa computadorizado é caracterizado por fazer com que o computador execute as etapas de:

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 as informações do disparador de descriptografia são inseridas dos meios de entrada do disparador de descriptografia; e

recepção das informações de especificação do cronograma lidas na etapa de leitura das informações de especificação do cronograma quando as informações do disparador de descriptografia são inseridas para determinar se o cronograma especificado pelas informações de especificação do cronograma chegou e permitir que a unidade de descriptografia descriptografe os dados criptografados se o cronograma ainda não chegou, causando uma alteração irreversível nas informações ambientais contidas nos dados criptografados no caso de o cronograma ter chegado.

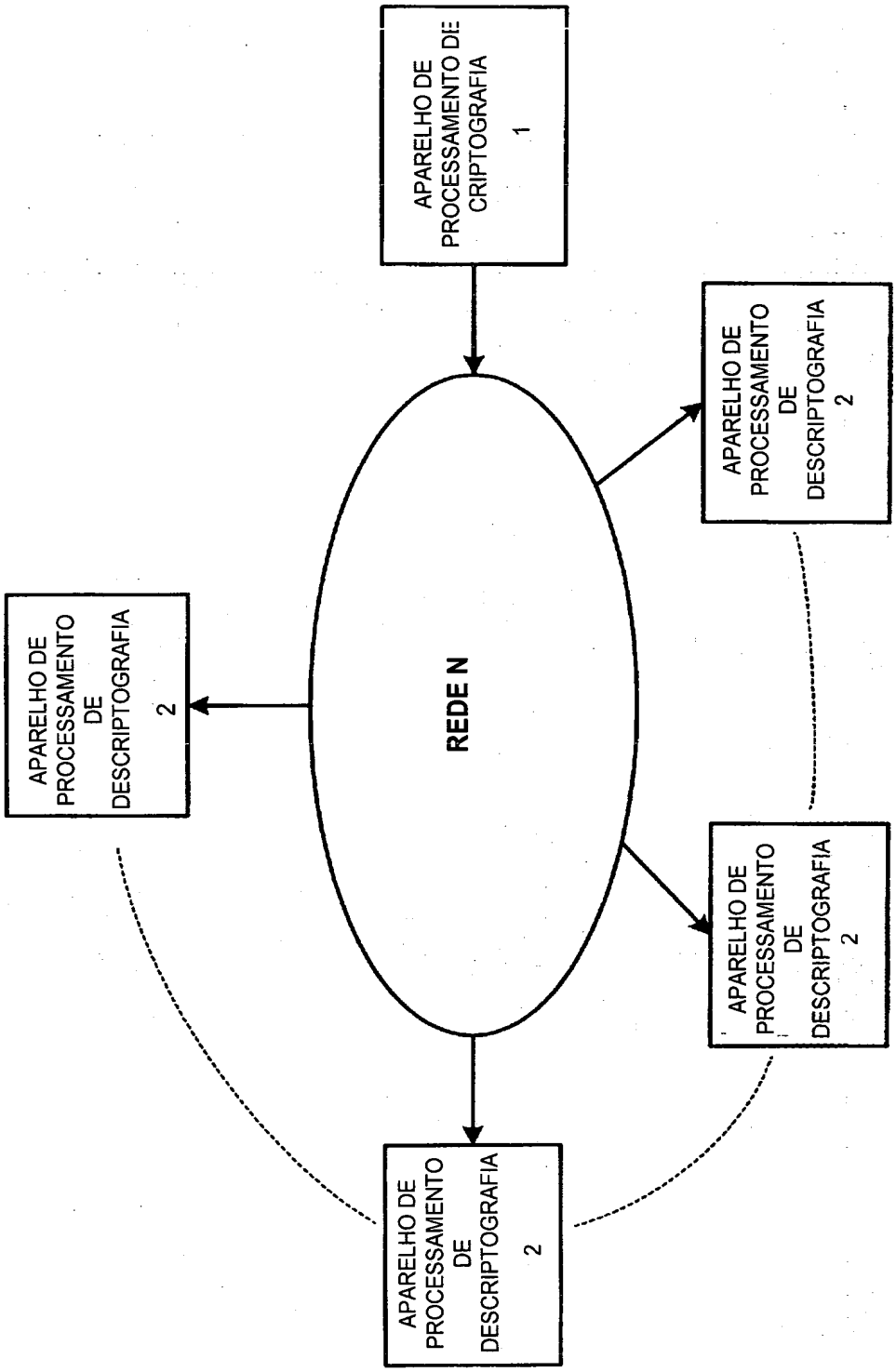

APARELHO DE PROCESSAMENTO DE CRIPTOGRAFIA 1
APARELHO DE PROCESSAMENTO DE DESCRIPTOGRAFIA 2
APARELHO DE PROCESSAMENTO DE DESCRIPTOGRAFIA 2
REDE N
APARELHO DE PROCESSAMENTO DE DESCRIPTOGRAFIA 2
APARELHO DE PROCESSAMENTO DE DESCRIPTOGRAFIA 2

FIG. 1

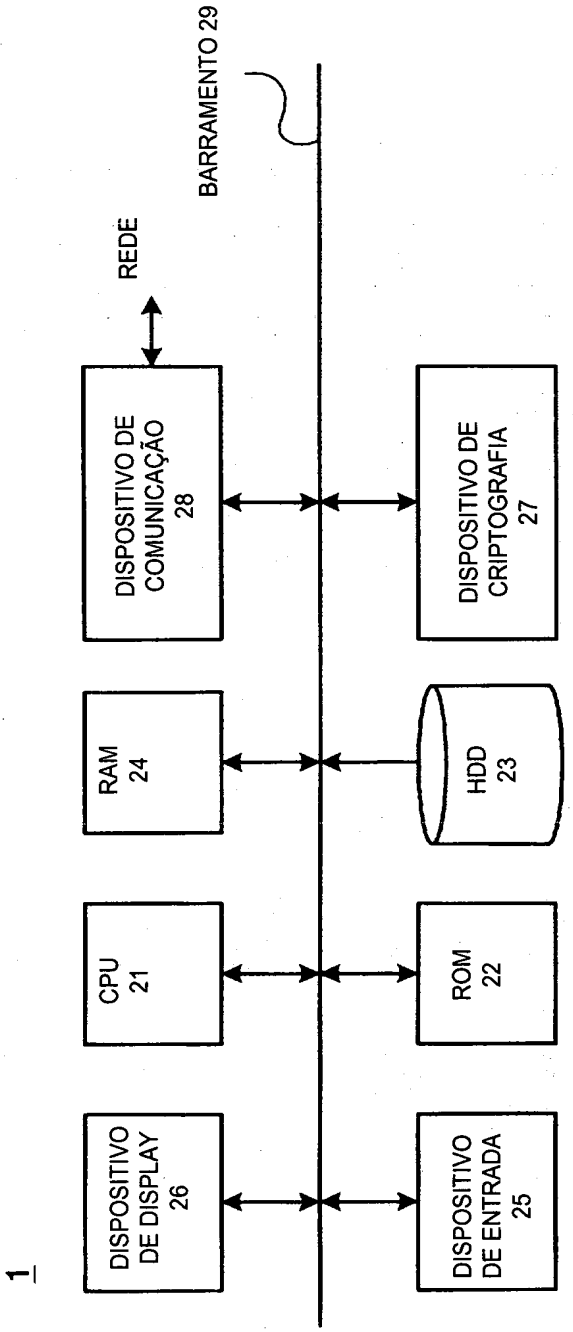

1
DISPOSITIVO DE DISPLAY 26
CPU 21
RAM 24
DISPOSITIVO DE COMUNICAÇÃO 28
REDE
BARRAMENTO 29
DISPOSITIVO DE ENTRADA 25
ROM 22
HDD 23
DISPOSITIVO DE CRIPTOGRAFIA 27

FIG. 2

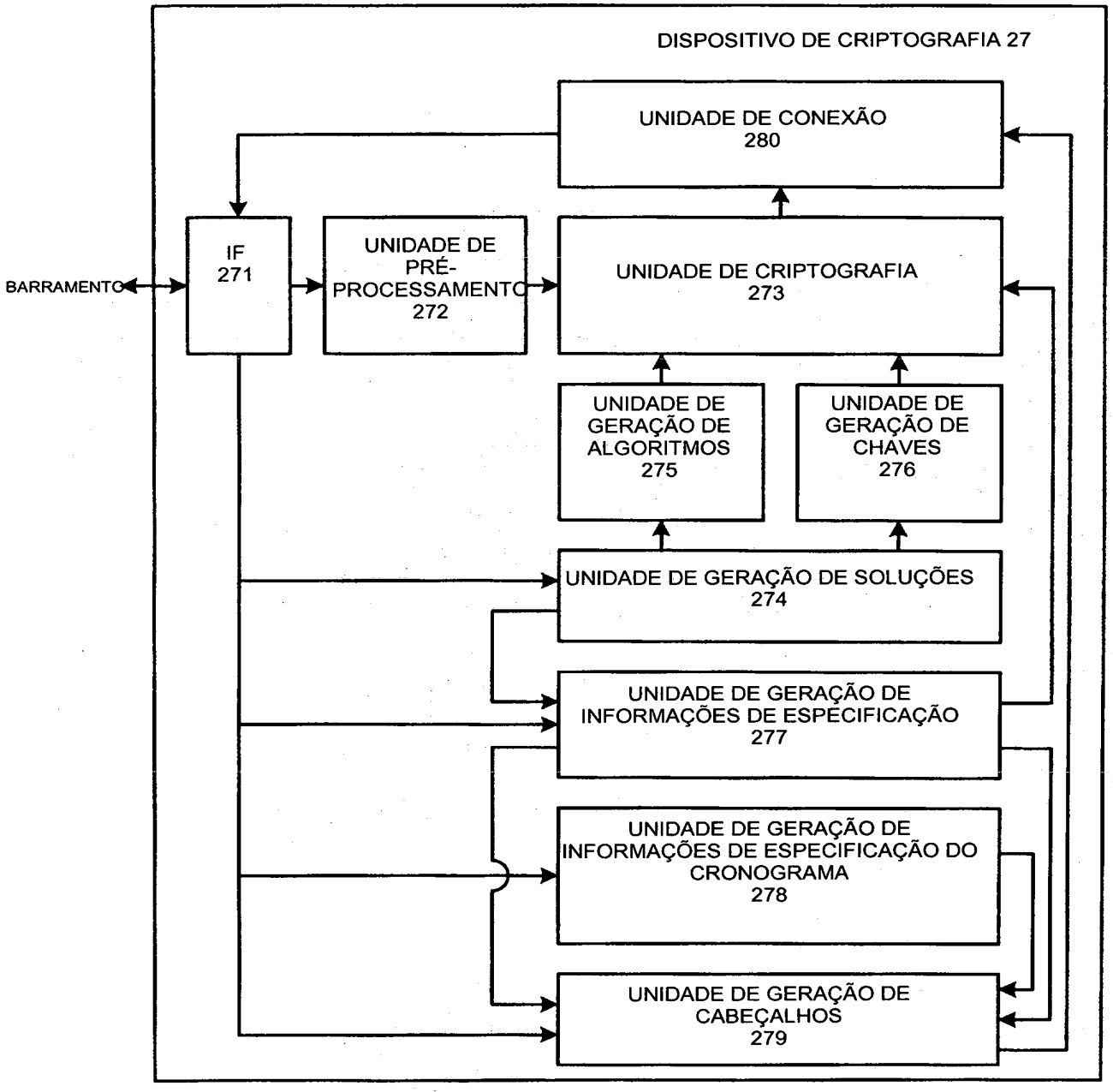
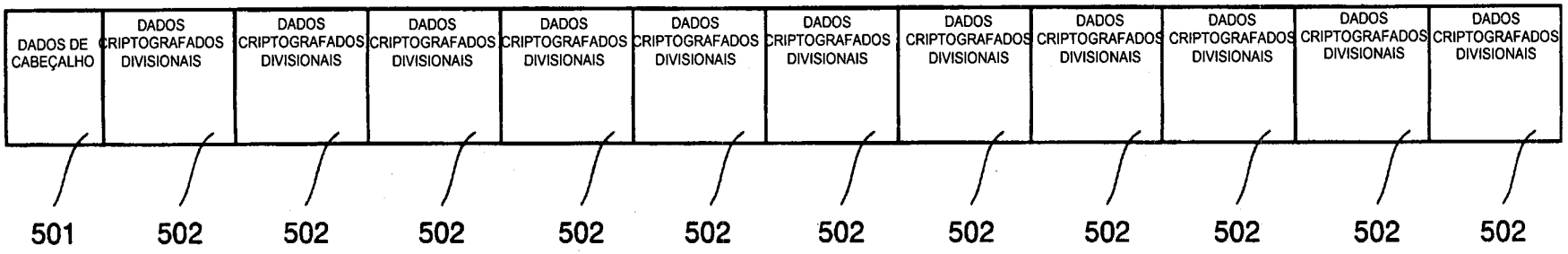

DISPOSITIVO DE CRIPTOGRAFIA 27
UNIDADE DE CONEXÃO
280
BARRAMENTO
IF
271
UNIDADE DE
PRÉ-
PROCESSAMENTO
272
UNIDADE DE CRIPTOGRAFIA
273
UNIDADE DE
GERAÇÃO DE
ALGORITMOS
275
UNIDADE DE
GERAÇÃO DE
CHAVES
276
UNIDADE DE GERAÇÃO DE SOLUÇÕES
274
UNIDADE DE GERAÇÃO DE
INFORMAÇÕES DE ESPECIFICAÇÃO
277
UNIDADE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

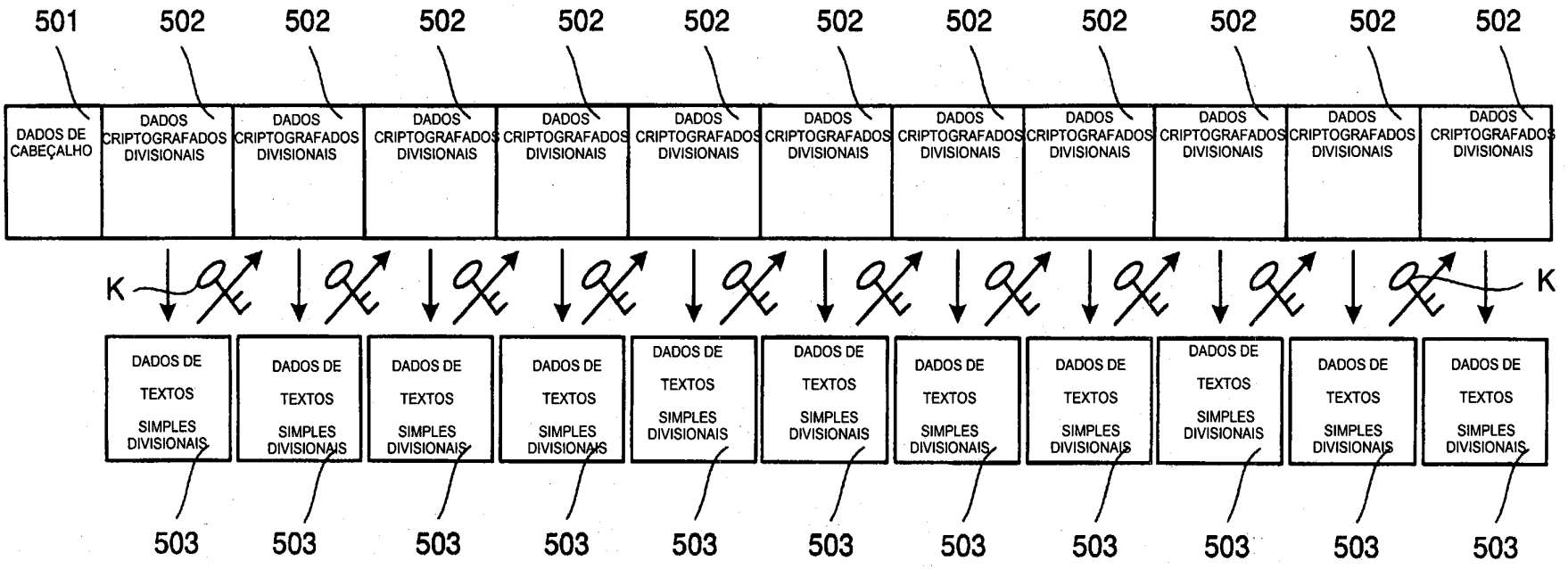

DADOS DE CABEÇALHO
DADOS CRIPTOGRAFADOS DIVISIONAIS
K
DADOS DE TEXTOS SIMPLES DIVISIONAIS
501
502
503

FIG. 4

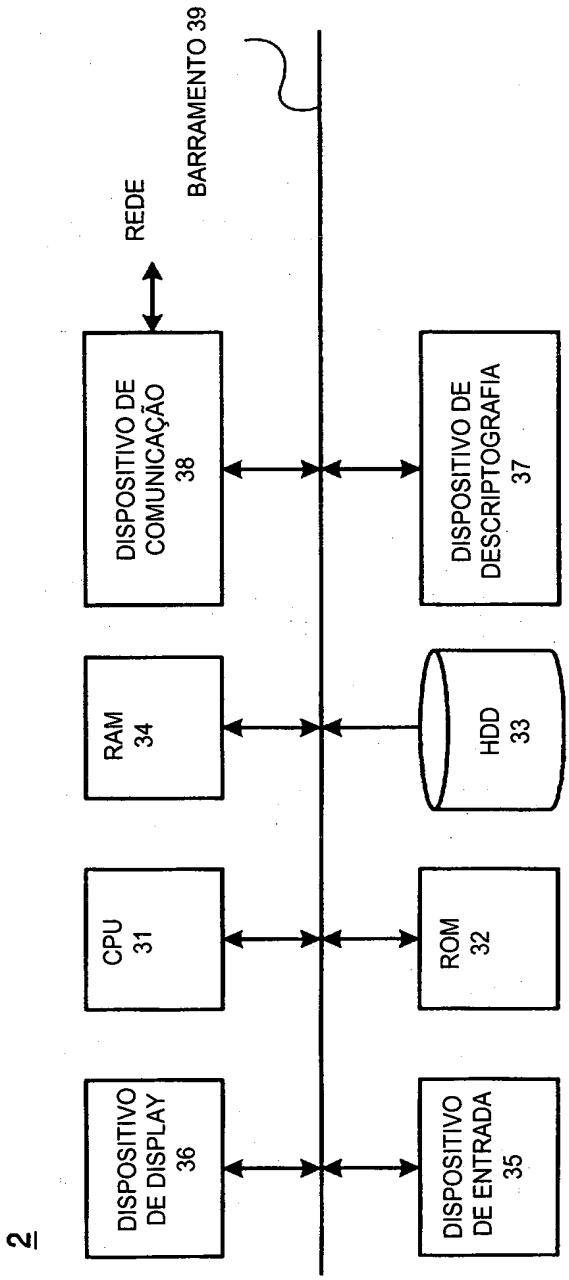

2
DISPOSITIVO DE DISPLAY 36
CPU 31
RAM 34
DISPOSITIVO DE COMUNICAÇÃO 38
REDE
BARRAMENTO 39
DISPOSITIVO DE ENTRADA 35
ROM 32
HDD 33
DISPOSITIVO DE DESCRIPTOGRAFIA 37

FIG. 5

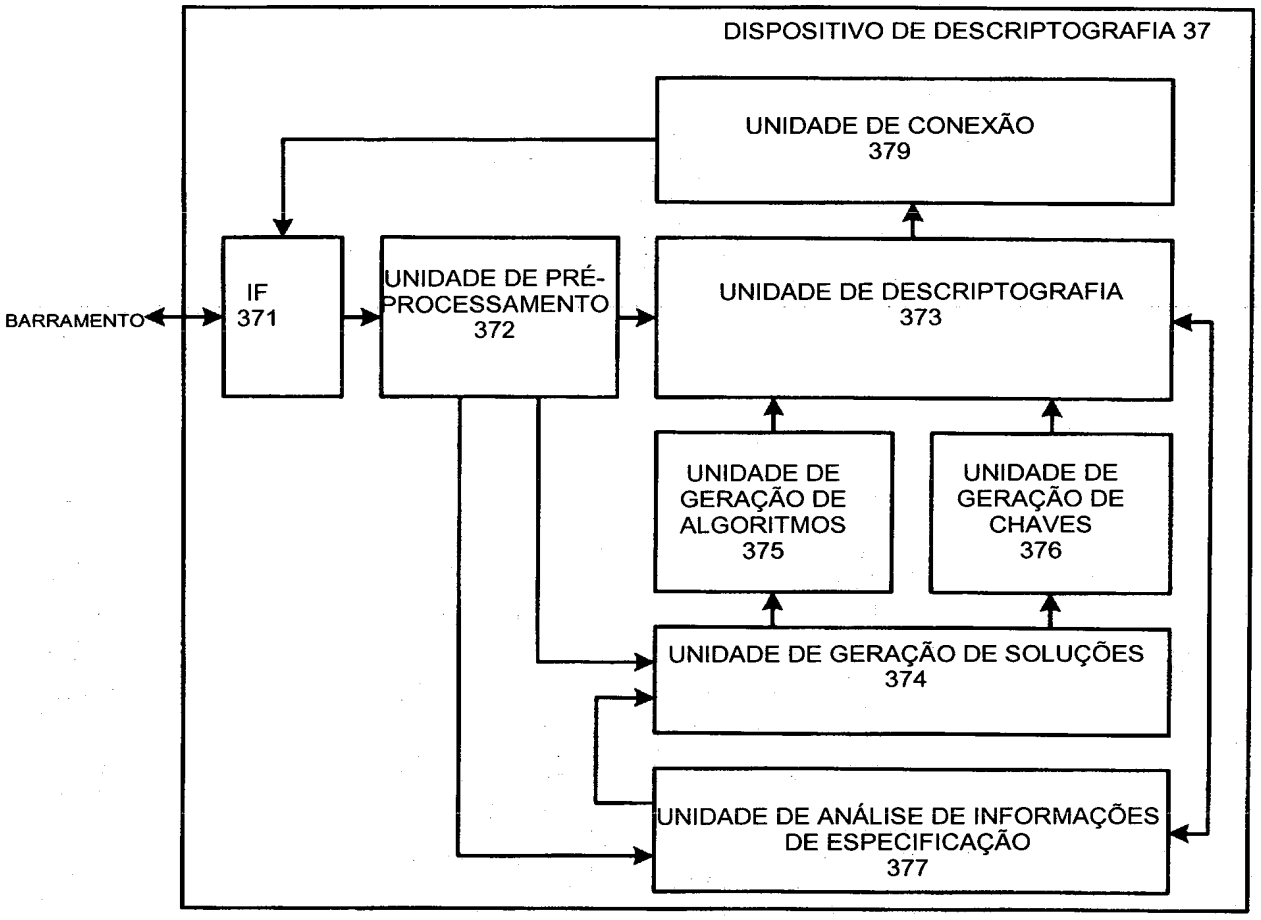

DISPOSITIVO DE DESCRIPTOGRAFIA 37
UNIDADE DE CONEXÃO
379
BARRAMENTO
IF
371
UNIDADE DE PRÉ-PROCESSAMENTO
372
UNIDADE DE DESCRIPTOGRAFIA
373
UNIDADE DE GERAÇÃO DE ALGORITMOS
375
UNIDADE DE GERAÇÃO DE CHAVES
376
UNIDADE DE GERAÇÃO DE SOLUÇÕES
374
UNIDADE DE ANÁLISE DE INFORMAÇÕES DE ESPECIFICAÇÃO
377

FIG. 6

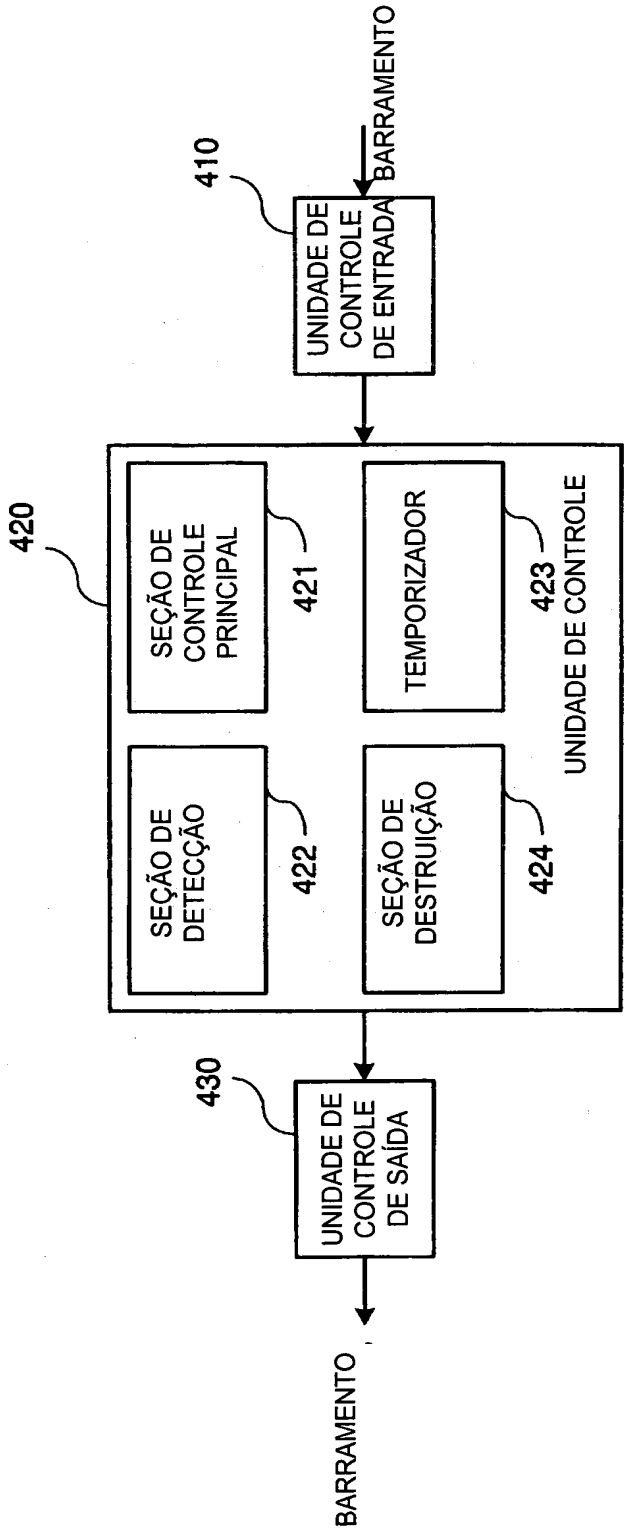

BARRAMENTO
410
UNIDADE DE CONTROLE DE ENTRADA
420
SEÇÃO DE CONTROLE PRINCIPAL
421
TEMPORIZADOR
423
UNIDADE DE CONTROLE
SEÇÃO DE DETECÇÃO
422
SEÇÃO DE DESTRUIÇÃO
424
430
UNIDADE DE CONTROLE DE SAÍDA
BARRAMENTO

FIG. 7

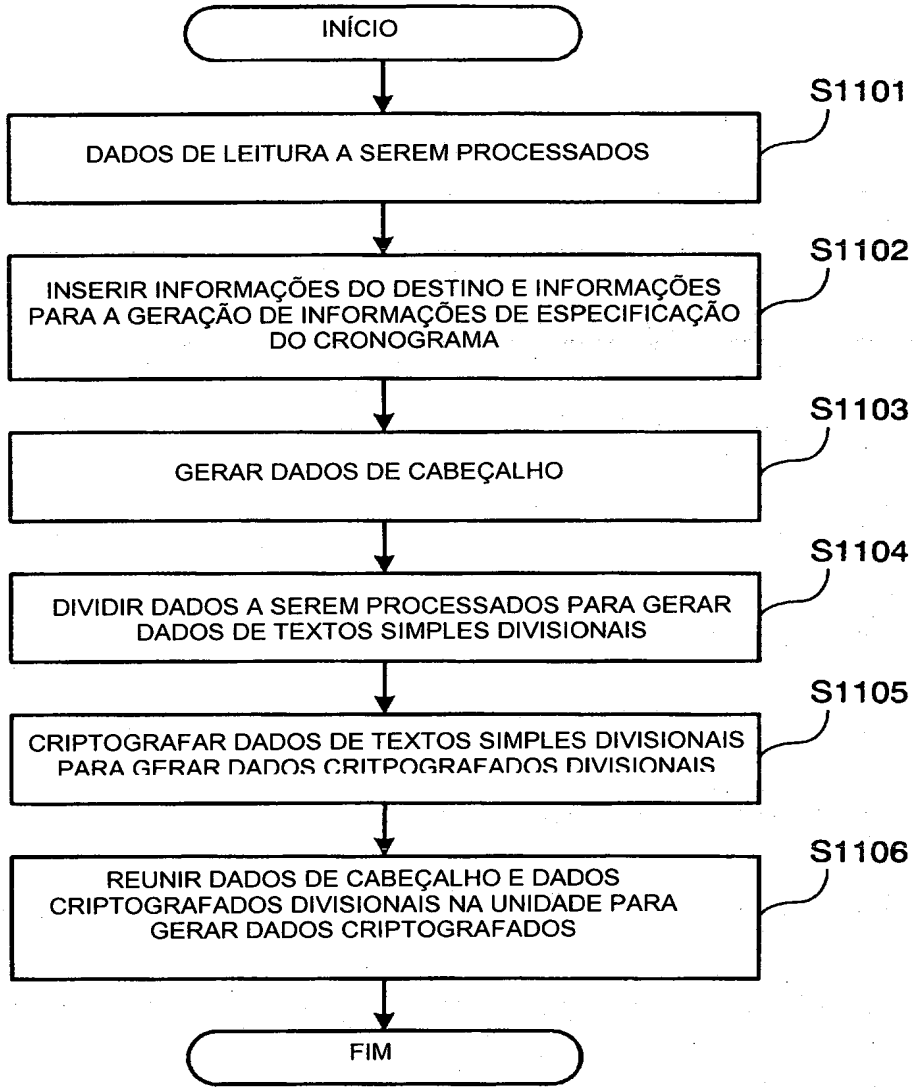

INÍCIO
S1101
DADOS DE LEITURA A SEREM PROCESSADOS
S1102
INSERIR INFORMAÇÕES DO DESTINO E INFORMAÇÕES PARA A GERAÇÃO DE INFORMAÇÕES DE ESPECIFICAÇÃO DO CRONOGRAMA
S1103
GERAR DADOS DE CABEÇALHO
S1104
DIVIDIR DADOS A SEREM PROCESSADOS PARA GERAR DADOS DE TEXTOS SIMPLES DIVISIONAIS
S1105
CRIPTOGRAFAR DADOS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

FIG. 8

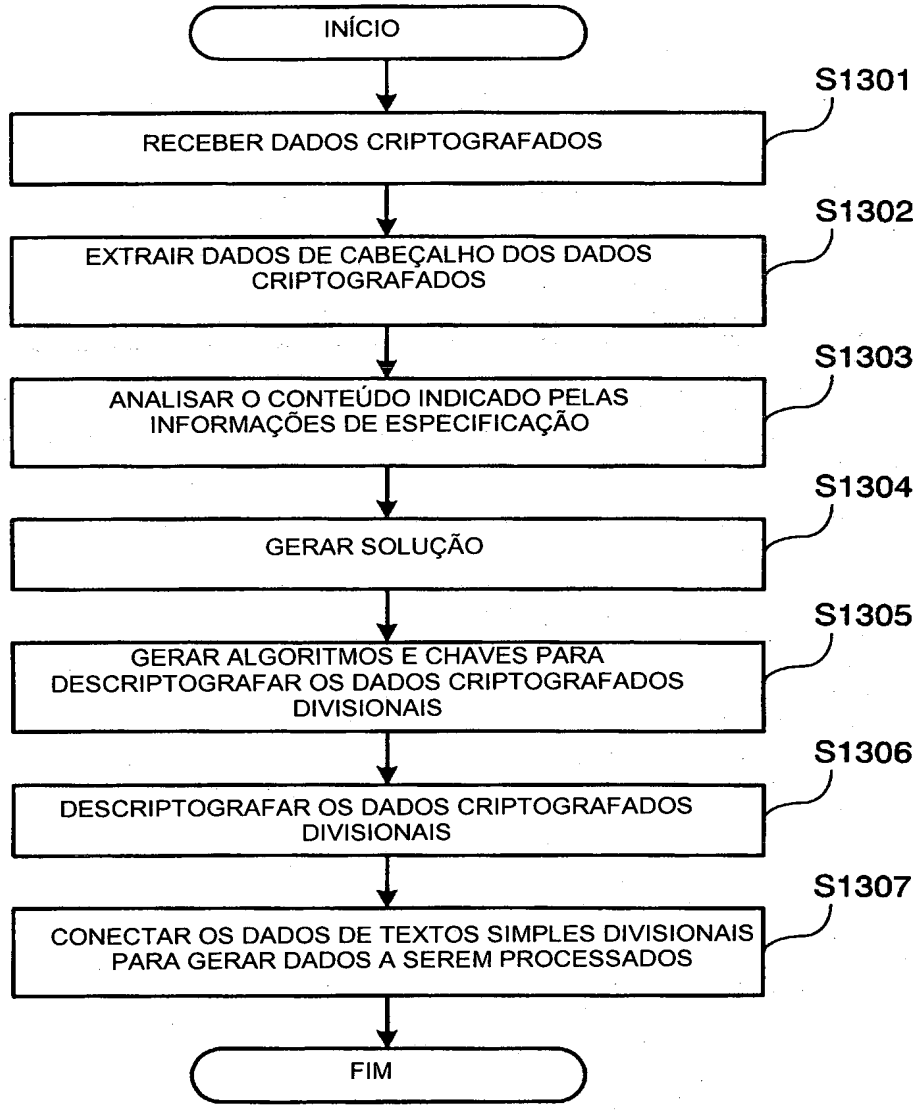

INÍCIO
S1301
RECEBER DADOS CRIPTOGRAFADOS
S1302
EXTRAIR DADOS DE CABEÇALHO DOS DADOS CRIPTOGRAFADOS
S1303
ANALISAR O CONTEÚDO INDICADO PELAS INFORMAÇÕES DE ESPECIFICAÇÃO
S1304
GERAR SOLUÇÃO
S1305
GERAR ALGORITMOS E CHAVES PARA DESCRIPTOGRAFAR OS DADOS CRIPTOGRAFADOS DIVISIONAIS
S1306
DESCRIPTOGRAFAR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

FIG. 9

Resumo da Patente de Invenção para: "**DISPOSITIVO DE PROCESSAMENTO DE DECODIFICAÇÃO, MÉTODO DE PROCESSAMENTO DE DADOS 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 múltiplas partes dos dados criptografados divisionais (502). Um aparelho de processamento de descriptografia descriptografa os dados criptografados obtidos em um aparelho de processamento de criptografia. Para a descriptografia, o aparelho de processamento de descriptografia utiliza uma solução utilizada para a criptografia dos dados para obter os dados criptografados no aparelho de processamento de criptografia e um nome de arquivo dos dados criptografados. Na presente invenção, uma área nos dados de cabeçalho (501) correspondente a um nome de arquivo, na qual o nome de arquivo dos dados criptografados é gravado, é excluída ou sobrescrita no cronograma apropriado para ser destruída, evitando, assim, que os dados criptografados sejam descriptografados.