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

(21) BR 102012033128-4 A2

(22) Data do Depósito: 21/12/2012

(43) Data da Publicação: 17/11/2015

(RPI 2341)

(54) Título: MÉTODO PARA GERAÇÃO DE CHAVES BASEADO EM ALGORITMOS GENÉTICOS

(51) Int. Cl.: H04L 9/08

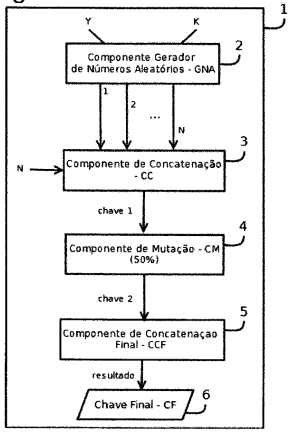
(52) CPC: H04L 9/0861; H04L 9/0869

(73) Titular(es): UNIVERSIDADE ESTADUAL DE CAMPINAS - UNICAMP, UNIVERSIDADE ESTADUAL DO OESTE DO PARANÁ - UNIOESTE

(72) Inventor(es): WU FENG CHUNG, CLÁUDIO SADDY RODRIGUES COY, HUEI DIANA LEE, MARIA DE LOURDES SETSUKO AYRIZONO, RAQUEL FRANCO LEAL, JOÃO JOSÉ FAGUNDES, RENATO BOBSIN MACHADO, JOYLAN NUNES MACIEL, EVERTON ALVARES CHERMAN, RICHARDSON FLORIANI VOLTOLINI, ANDRÉ GUSTAVO MALETZKE

(74) Procurador(es): OTACÍLIO MACHADO RIBEIRO

(57) Resumo: MÉTODO PARA GERAÇÃO DE CHAVES BASEADO EM ALGORITMOS GENÉTICOS. Refere-se o presente pedido de patente de invenção a um novo método computacional sistêmico para a geração de chaves secretas, inspirado na Teoria da Evolução das Espécies, especialmente na genética e seleção natural. Esse método permite que sejam definidos parâmetros importantes, como limite inferior e superior para geração de números aleatórios, assim como quantidade de números que irão contribuir para compor a chave e ainda índice de mutação que será aplicado no algoritmo. Desse modo o método proposto pode ser aplicado para distintas finalidades, tais como para a aplicação como chaves de algoritmos de criptografia, para geração de senhas, para a proteção de arquivos, para publicação de streamings de áudio e vídeo, entre outros. As principais vantagens do método proposto consistem em não necessitar nenhum hardware específico para ser executado, utiliza operações matemáticas simples e sem alto custo de execução, é configurável para trabalhar as variáveis e definir o grau de segurança desejado, e foi concebido com conceitos de algoritmos genéticos dificultando tentativas(...)



MÉTODO PARA GERAÇÃO DE CHAVES BASEADO EM ALGORITMOS GENÉTICOS

Campo da invenção

O presente pedido de patente de invenção se refere a um novo método computacional, baseado em *software,* para a geração de chaves secretas que podem ser utilizadas por diferentes aplicações. O método consiste em um algoritmo computacional, inspirado em conceitos da Teoria da Evolução das Espécies, para a geração de chaves secretas, as quais podem ser empregadas na área da criptografia e em sistemas que manipulam dados digitais para aumentar do nível de segurança no acesso as informações, sejam estas compostas por dados, imagens, fluxos de áudio e de vídeo, etc. Essas chaves também podem ser aplicadas para outras finalidades, tais como para geração de senhas, identificação de *streamings*, proteção de arquivos, entre outras.

Fundamentos da invenção

A evolução tecnológica tem estimulado o aumento do uso de recursos computacionais em diversas as áreas do conhecimento. Cada vez mais aplicativos baseados em *softwares* estão sendo utilizados em dispositivos eletrônicos, tais como *tablets*, celulares, relógios, câmeras, equipamentos da área médica, veículos, entre outros. Uma das preocupações que surgem a partir desse cenário é a proteção e segurança de informações e de procedimentos. Associado a essa questão, verifica-se um aumento das violações cibernéticas, envolvendo acesso à informações digitais por meio de interceptações indevidas, permitindo o acesso, a leitura e a cópia não autorizada de dados.

O problema supracitado é mais grave quando os sistemas manipulam informações com caráter sigiloso, as quais têm sido crescentemente transformadas e digitalizadas para o universo computacional. Nesse contexto, uma das áreas que endereçam tal problema é a Segurança da Informação, especificamente em relação a confidencialidade, que consiste em uma

propriedade que limita o acesso a informação para somente aquelas entidades legitimamente autorizadas pelo proprietário da informação (Tanenbaum, 2011).

Desse modo, é importante o delineamento de métodos computacionais que possam contribuir para aumentar o nível de segurança no acesso a essas informações confidenciais. Um dos objetivos da Criptografia é a de garantir confidencialidade e, nesse sentido, diversos modelos de segurança que protegem e aumentam a confidencialidade das informações foram criados. Tais modelos são conhecidos como métodos criptográficos e trabalham com a geração e/ou utilização de chaves criptográficas (ou chaves-secretas) para garantir o acesso as informações protegidas.

Alguns métodos criptográficos oferecem maior nível de segurança e, desse modo, também exigem maior capacidade de processamento para cifrar e/ou decifrar dados por meio da utilização de chaves-secretas. Sendo assim, existem métodos que não podem ser utilizados em qualquer dispositivo eletrônico, com restrições de desempenho e *hardware*, ou seja, principalmente aqueles com menor capacidade de processamento.

A partir da identificação do aumento de problemas relacionados a confidencialidade de informações, e considerando as invenções de métodos criptográficos e de geração de chaves-secretas, definiu-se, por meio desta invenção, um novo método computacional que consiste num algoritmo original para geração de chaves-secretas, de baixo custo de processamento, aplicável para ampliar a o nível de confidencialidade das informações em sistemas baseados em computador. Ao longo do texto os termos chave-secreta e chave serão utilizados com o mesmo significado.

O método proposto neste documento não está limitado a aplicações relacionadas à criptografia, podendo ser utilizada para qualquer tipo de aplicação que necessite uma chave ou identificação com alto grau de segurança. Dentro desse gama de possíveis aplicações pode-se citar a publicação de *streaming*, geração de senhas fortes, proteção de arquivos, geração de chaves para serem utilizadas por algoritmos criptográficos, entre outras.

Atualmente, no estado da técnica, existem diversos trabalhos que se valem do conceito de criptografia e geração de chaves-secretas para desenvolver tecnologias que aumentam a confidencialidade em sistemas computacionais. Neste pedido de patente apresenta-se um método computacional, de baixo custo operacional, que agrega características originais, descritas neste documento, para geração de chaves-secretas únicas e que podem ser aplicadas para distintas finalidades.

A título de se determinar o estado da técnica e fundamentar o presente pedido de patente de acordo com o item 15.1.2 do Ato normativo 127/97 do INPI, segue abaixo uma relação de patentes e pedidos de patentes e artigos que versam sobre a mesma área do conhecimento do presente pedido de patente.

A patente **US7406175-B2 (WO03/090185)** descreve um método que utiliza equipamentos (*hardware*) para a geração de chaves-secretas. A segurança da chave é assegurada prevenindo a utilização de circuitos projetados, ou mesmo de pessoas, que consigam ler e decifrar o valor da chave-secreta. Nessa invenção os circuitos geradores de números aleatórios criam números aleatórios de acordo com diferentes relógios (**CLK1**, **CLK2**, **CLK3**). Um circuito aritmético opera sobre os números aleatórios criados nos geradores para produzir um número aleatório de **N bits** como saída. Este número é adquirido por meio de um seletor de chaves e é armazenado em um registrador a partir de um sinal que habilita a aquisição. Tal processo é gerenciado por contadores de monitoramento de tempo, ou seja, distintos relógios do computador, sendo ao final produzida uma chave em *hardware* que é única e secreta. As chaves secretas geradas por esse invento podem ser aplicadas para criptografia (codificação) ou decodificação em aparelhos equipados com tal gerador e método de geração.

O invento existente aplica componentes arquiteturais e define um método de geração das chaves secretas, usando números aleatórios a partir de valores dados pelo relógio, sendo tais chave-secretas armazenadas em *hardware*. A invenção não realiza a geração das chaves secretas em *software*,

e é totalmente atrelada a utilização de equipamentos de *hardware*, diferenciando-se do presente pedido de patente. A invenção proposta neste documento não trabalha somente com componentes aleatórios, mas também aplica um componente de mutação inspirado na Teoria da Evolução das Espécies, permitindo maior dinamismo na geração de chaves secretas. Outra vantagem da tecnologia proposta consiste em sua implementação ser realizada por meio de *software*, pois, desse modo, a tecnologia pode ser aplicada em distintos dispositivos, de modo independente do *hardware* e de sistema operacional, ampliando sua aplicabilidade. Adicionalmente, a tecnologia proposta não utiliza recursos computacionais que exijam grande poder de processamento, podendo ser executada em qualquer computador atual, assim como em outros dispositivos móveis. Resumidamente, a patente US7406175-B2 trata-se de uma tecnologia distinta em relação ao presente pedido, tanto em seu material quanto ao método aplicado, bem como sua finalidade e aplicabilidade.

Na patente **US7739501-B2** é apresentado um produto que consiste em um programa de computador que realiza a geração de chaves criptográficas secretas, nela denominada rótulo, para uso na troca de informações entre membros de organizações em matrizes e filiais. O programa reside em um computador cujos dados armazenados podem ser lidos somente por dispositivos mecânicos. As instruções configuradas para o computador são: produzir uma chave de leitura-escrita usando ao menos um valor base; criar uma chave de escrita usando a chave de leitura e escrita produzida; combinar um primeiro identificador, unicamente associado com a primeira organização, e um segundo identificador, unicamente associado com o rótulo chave a ser produzido. Para a criptografia foi aplicada uma função *hash* de único sentido, a qual utiliza um gerador não determinístico de *bits* aleatórios, com o objetivo de produzir uma chave pura, associando-a com as chaves de leitura-escrita e de escrita para formar rótulo final (chave criptográfica final).

A invenção existente é aplicada especificamente para a área de criptografia. Assim como o processo de leitura da chave gerada, ela é realizada

por meio de dispositivos mecânicos (*hardware*), diferenciando-se da invenção proposta que trabalha com *software* tanto para a leitura quanto para a manipulação das chaves secretas. Nesse sentido, a tecnologia proposta pode ser aplicada em qualquer dispositivo de *hardware* computacional, tornando a invenção proposta independente e com maior gama de aplicabilidade. Em segundo lugar, o método para a geração das chaves secretas da patente **US7739501-B2** é distinto do proposto neste pedido, pois, o mesmo associa as chaves secretas aos nomes de domínios, que representam as organizações. Além disso, é utilizado um gerador não-determinístico de *bits* aleatórios, o que não ocorre no presente pedido no qual são aplicados conceitos de Seleção Natural e Genética. De modo resumido, o propósito da invenção, o método de geração de chaves secretas, que consiste em uma etapa da invenção, e os materiais empregados são distintos do presente pedido de patente.

A patente **US7372961-B2** refere-se a sistemas de criptografia de chave pública, mais particularmente, ao método geração de chaves dentro destes sistemas. A estrutura básica de um sistema de criptografia de chave pública é bem conhecida e se tornou ubíqua com a segurança em sistemas de comunicação de dados. Esses sistemas usam uma chave privada k e uma chave pública correspondente αk onde α é um gerador do grupo. Assim, um lado pode criptografar a mensagem m com a chave pública dos destinatários pretendidos e o destinatário pode solicitar sua chave privada para decifrar m.

Em termos gerais, a patente descrita provê uma técnica de geração de chaves em que qualquer desvio é eliminado durante a seleção da chave. Além disso, são descritos os principais elementos comuns aos cenários preferenciais, onde existe uma rede de comunicação e dois dispositivos eletrônicos (computadores, celulares, ou qualquer outro), os quais possuem segurança criptográfica baseadas em *hash*, tal como o *Secure Hash Algorithm* - SHA-1.

Na patente existente, **US007372961-B2,** foi desenvolvido um método para garantir a geração e o acesso a chaves secretas, e não o um

método para geração dessas chaves. No exemplo citado é utilizado o SHA-1, um conhecido método de criptografia.

De modo resumido, o objetivo e o método diferem do presente pedido de patente, pois o objetivo não consiste em gerar as chaves, mas sim, em garantir que novas chaves sejam geradas em casos de não conformidade com os parâmetros do sistema. O método proposto nesta invenção trata especificamente de um método para a geração de chaves secretas, de propósito geral, aplicando operadores aleatórios e de mutação, aplicando técnicas de algoritmos genéticos e seleção natural, para dar maior dinamismo a geração de chaves, assim como para permitir configurações específicas em função da aplicação a que a chave será destinada. Adicionalmente os processos realizados no método proposto são realizados totalmente por *software*, podendo ser aplicado em qualquer configuração de *hardware* e sistema operacional computacional. Desse modo o método proposto possui diversas características direcionas a ampliar o seu rol de aplicabilidades.

A patente **EP2120389-A1 (WO2008/113279)** apresenta a invenção de um método para geração de uma chave de sessão e dispositivos de comunicação. O método consiste na geração de uma chave pública e outra privada, de longo prazo, nas duas partes da comunicação. A parte *X* seleciona uma chave privada aleatoriamente, assim como a parte *Y* seleciona outra chave privada aleatoriamente. A parte *X* usa a chave secreta de longo prazo e sua chave secreta aleatória para calcular e enviar a mensagem para *Y*. Após isso, a parte *Y* usa sua chave secreta de longo prazo e sua chave secreta aleatória para calcular e enviar a mensagem *Y* para *X*. Desse modo, a parte *X* calcula a sua chave secreta de sessão *Kx* e a parte *Y* calcula sua chave secreta de sessão *Ky*.

A solução descrita possui um gerenciador de chaves central que cria e manipula as chaves utilizando algoritmos de mapeamento em conjunto com uma matriz de Fatores de Chaves Públicas e matrizes de Fatores de Chaves Públicas/Privadas. Além disso, na patente existente são apresentados diversos cenários de aplicação do método e os dispositivos de comunicação

empregados. Uma característica da patente **EP2120389-A1** é que as chaves de cada parte da comunicação são elaboradas de acordo com parâmetros do sistema de criptografia. Além disso, a chave de sessão gerada após a comunicação das partes é variável, evitando grande dependência do gerenciador de chaves central.

Os conceitos e procedimentos de geração da chave da patente existente são distintos do presente pedido de patente, pois utilizam matrizes de fatores e algoritmos de mapeamento. Além disso, são geradas diversas chaves dentre as quais uma é escolhida aleatoriamente para ser utilizada na criação da chave de sessão para a comunicação.

De modo resumido, a patente apresentada se distingue da invenção proposta em relação ao método de geração das chaves, aos dispositivos utilizados, e, principalmente em relação ao objetivo, que consiste em gerar uma chave de sessão para comunicação entre dois sistemas, e não a geração de chave secreta aplicável em qualquer cenário. Ambas as patentes podem ser utilizadas em conjunto, de forma de a patente **EP2120389-A1** pode aplicar em seus cenários de uso o método definido no presente pedido de invenção.

Outros diferenciais da tecnologia proposta consistem na aplicação não somente de fatores aleatórios para geração das chaves secretas, mas também de mutação. A invenção proposta pode ser aplicada para distintas finalidades, sendo que as características da chave a serem geradas podem ser configuradas em função das particularidades da aplicação. Outra particularidade da tecnologia proposta é que a mesma é implementada totalmente em *software* e aplicando operações de baixo custo de processamento.

Breve descrição da invenção

Refere-se o presente pedido de patente a um novo método computacional, por meio de *software*, cuja finalidade é a geração de chaves secretas que possam ser aplicadas de modo genérico para distintas

finalidades. Esse pedido de patente consiste em um **Método para Geração de Chaves Baseado em Algoritmos Genéticos.**

A chave gerada por meio do método proposto pode ser utilizada para qualquer fim que necessite uma identificação, denominada neste documento como **chave** ou **chave secreta**, que seja difícil de ser quebrada por invasores (*crackers*), principalmente aplicando-se métodos de força bruta.

Algumas possíveis aplicações do método incluem a sua utilização para a publicação de *streamings* de vídeo e/ou áudio por meio da Internet; para chaves de métodos criptográficos; como senhas de sistemas computacionais e redes; para a proteção de arquivos; entre outros.

O presente pedido de patente foi concebido baseado no conceito da Teoria da Evolução das Espécies aplicado a métodos computacionais.

O **Método para Geração de Chaves Baseado em Algoritmos Genéticos** foi definido conforme o sistema descrito na Figura 1, sendo este composto pelos seguintes elementos:

1. **Componente Gerador de Números Aleatórios - GNA** (2): responsável pela geração de números aleatórios, aplicando o operador de aleatoriedade inspirado na Teoria de Evolução das Espécies;
2. **Componente de Concatenação - CC** (3): possui a função de receber **N** números aleatórios (com número de dígitos variável), converter para o formato texto e por fim retornar uma **chave** consistindo na concatenação desses **N** números aleatórios;
3. **Componente de Mutação - CM** (4): O CM é derivado dos princípios de mutação de algoritmos genéticos, inspirados na Teoria de Evolução das Espécies. No caso do presente método, o CM recebe uma **chave1** como entrada e aplica uma mutação de 50% gerando uma **chave2**;
4. **Componente de Concatenação Final - CCF** (5): O CCF recebe uma chave como entrada, no caso deste método foi aplicada especificamente a **chave2**, e são acrescentadas algumas características adicionais para dificultar a descoberta da chave por técnicas maliciosas;

5. **Chave Final - CF** (6): Consiste na **chave** gerada a partir de todas as etapas do método e que poderá ser aplicada para as mais diversas aplicabilidades, conforme apresentado inicialmente.

A partir das definições gerais e da apresentação dos componentes que são aplicados no método, a seguir detalha-se a sequencia de execução do método, representado por três fases:

Fase 1: Geração da primeira Chave (chave 1)

Nesta fase é gerada a **chave1** por meio da aplicação de componentes aleatórios. Para isso são executados os seguintes procedimentos:

1. Gera-se **N** números aleatórios utilizando o Componente Gerador de Números Aleatórios - GNA (2). Cada um desse números deve ficar dentro dos limites entre **Y** e **K**. Cada um desses valores numéricos pode conter uma quantidade de caracteres variando entre o número de dígitos de **Y** e o número de dígitos de **K**;

2. O resultado da Fase 1 (**chave 1**) consiste na concatenação dos caracteres gerados pelos **N** números aleatórios, convertidos para formato texto. Esse procedimento é realizado pelo Componente de Concatenação (3).

Fase 2: Geração da segunda Chave (chave 2)

Nesta fase gera-se a **chave2 por meio do Componente de Mutação (4)**, a qual utilizar o operador de mutação sobre 50% da **chave1**. A seguir apresenta-se este procedimento:

1. Todos os caracteres da **chave1** são percorridos, de modo que:

   i. Se a posição do caracter na **chave1** for par, esse caracter é adicionado a **chave2**;

   ii.Se a posição do caracter na **chave1** for impar, será adicionado na **chave2** um caracter ASCCII aleatório.

Fase 3: Geração da Chave Final

A **chave final** é gerada pelo Componente de Concatenação Final (5), sendo composta pelos seguintes elementos:

i. Hora, minutos, segundos e milissegundos da geração da chave;

ii. chave2.

Parâmetros de Configuração:

Esse método pode ser aplicado para distintos propósitos e por conseguinte os valores de **N**, **Y** e **K** podem ser personalizados conforme critério de segurança da aplicação. Neste caso, especificamente, foram adotados os valores **N=300**, **Y=0**, **k=9999999999** e operador de mutação de **50%**.

Características do Método Proposto

A tecnologia proposta por meio deste pedido de patente diferencia-se dos métodos existentes por não ser direcionado a uma aplicação específica, e de modo contrário, podendo ser aplicada para distintas finalidades para segurança de informações e de procedimentos. Como exemplos de possíveis aplicações da tecnologia pode-se citar a utilização dessas chaves secretas para métodos criptográficas, a aplicação das chaves geradas como identificador para publicação de *streamings*, a sua utilização para a geração de senhas, a sua aplicação para a proteção de arquivos, entro outros.

Outro diferencial da tecnologia proposta consiste na definição e na implementação do método totalmente por *software*, desse modo não sendo necessário atrelar a utilização da solução a existência de componentes específicos de *hardware*, além de ser independente de plataforma e de sistema operacional.

Associado a essas características de dinamicidade e portabilidade apresentadas, o método proposto no presente documento aplica conceitos provenientes da Teoria de Evolução das Espécies, tais como operadores de aleatoriedade, mutação e cruzamento; permitindo assim a geração de chaves

secretas com altos níveis de segurança e sem a utilização de operações matemáticas que exijam alto poder de processamento.

Em função do tipo de aplicação e do grau de segurança necessário, o método foi concebido para permitir configurações que irão influenciar no tamanho da chave, grau de aleatoriedade e índices de mutação. Desse modo, a tecnologia se torna ainda mais flexível para ser aplicada a propósitos diversificados.

Quanto ao tempo de utilização das chaves geradas pelo método, essas podem ser utilizadas tanto para curto quanto para longo prazo, pois o tempo para quebra da chave por meio de técnicas de força bruta, para a configuração padrão do método, é de no mínimo ria $\mathbf{10^{338}}$ anos.

Breve descrição das figuras

A Figura 1 demonstra um diagrama do método para a geração de chaves secretas baseada em algoritmos genéticos (1); composto por um Componente Gerador de Números Aleatórios (2), um Componente de Concatenação (3), um Componente de Mutação (4), um Componente de Concatenação Final (5) e pela Chave Final (6).

A Figura 2 demonstra o Componente Gerador de Números Aleatórios.

Na Figura 3 é apresentado o Componente de Concatenação.

A Figura 4 demonstra o Componente de Mutação.

Na Figura 5 apresenta-se o Componente de Concatenação Final.

Descrição detalhada da invenção

Para alcançar os objetivos descritos na breve descrição da invenção definiu-se o **Método para Geração de Chaves Baseado em Algoritmos Genéticos,** o qual consiste na utilização de conceitos relacionados a algoritmos genéticos (Teoria da Evolução das Espécies) e recursos computacionais para a geração de chaves secretas que sejam difíceis de serem quebradas por meio das técnicas computacionais atuais, principalmente por meio de métodos de força bruta.

O presente pedido de patente foi concebido baseado no conceito da Teoria da Evolução das Espécies aplicado a métodos computacionais, os quais originaram diversos subgrupos como os Algoritmos Genéticos e a Programação Genética. A principal característica desses métodos é a aplicação dos conceitos de Seleção Natural e Genética para a busca por soluções de problemas complexos, utilizando para tanto conceitos como indivíduo, gene, lócus, alelo, genótipo, fenótipo, cromossomo e genoma. Essa busca pela solução é dada, de modo geral, pela evolução da população (conjunto de indivíduos) por meio da aplicação de operadores genéticos, como *crossover*, mutação e cruzamento, bem como de componente aleatório para a manutenção da diversidade da população.

O **Método para Geração de Chaves Baseado em Algoritmos Genéticos** foi delineado contemplando métodos e recursos computacionais e conceitos de Algoritmos Genéticos. Os componentes que fazem parte da invenção são apresentados na Figura 1, a partir da qual serão descritos os detalhes de seus elementos constituintes e dos métodos aplicados. Embora seja apresentada uma configuração específica, o método pode ser executado de modos diversos em face de personalizações que venham a ser aplicadas. Para isso podem-se personalizar alguns parâmetros, tais como quantidade de números aleatórios, valor mínimo e máximo permitidos para a geração de números aleatórios e o percentual de mutação da chave intermediária (denominada **chave1** neste documento).

O primeiro elemento constituinte do modelo é o Componente Gerador de Números Aleatórios - GNA (2), o qual possui a função de utilizar o operador de aleatoriedade e criar números aleatórios dentro do conjunto de números compreendidos entre um limite inferior e um limite superior. Esses limites, inferior e superior, podem ser definidos em função do objetivo de aplicação do método, sendo parâmetros configuráveis. Esses limites são representados na Figura 1 pelas variáveis de entrada **Y** e **K** respectivamente. Desse modo, cada vez que o GNA executa, pode gerar um número que além de variar o valor, também pode variar o número de dígitos. Cada número

gerado possuirá o número de dígitos variando entre a quantidade de dígitos de **Y** e a quantidade de dígitos de **K**. O GNA foi inspirado nos operadores de aleatoriedade dos Algoritmos Genéticos.

O Componente de Concatenação - CC (3) por sua vez é responsável pelo recebimento de **N** números aleatórios e pela geração de uma chave (denominada neste documento de chave1). O procedimento realizado pelo CC (3) consiste em solicitar um conjunto de **N** números aleatórios ao GNA (2). Posteriormente o CC (3) recebe esses **N** números aleatórios, os converte unitariamente para o formato texto e por fim concatena todos esses números em modo texto. O produto gerado pelo CC (3) foi denominado **chave1**. O valor de **N** também é parametrizado e pode ser definido em função das necessidades específicas de tamanho de chave e segurança que a aplicação necessite.

Após a geração da **chave1** utiliza-se outro elemento constituinte, denominado Componente de Mutação - CM (4). O CM (4) também foi inspirado nas operações genéticas aplicadas para a busca da evolução da população, especificamente pelos operadores de mutação. O CM (4) recebe uma chave como entrada, tendo sido aplicado neste método especificamente a **chave1** gerada pelo CC (3) e GNA (2), e gera uma chave de saída aplicando um conjunto de mutações sobre a chave de entrada. O percentual de mutação pode ser variável, tendo-se aplicado neste método específico um fator de aleatoriedade de 50%, o que significa de a metade dos caracteres presentes na chave de entrada sofrem modificações para gerar a chave de saída. Neste documento especificamente nomeou-se a chave gerada pelo CM (4) como **chave2**.

O Componente de Concatenação Final - CCF (5) recebe uma chave como entrada e agrega algumas características, também aplicando operadores evolutivos e de mutação. Especificamente neste trabalho o CCF (5) recebe como entrada a chave2 e gera uma chave final composta pela data, hora, minuto, segundo e milissegundo que a chave foi gerada. Posteriormente

o CCF (5) concatena a **chave2** a chave final e essa é o produto final do método.

Ainda na Figura 1 apresenta-se Chave Final - CF (6) que consiste no produto final gerado pelo método e que será aplicado para as mais distintas finalidades, entre as quais para a publicação de *streamings* de vídeo e/ou áudio por meio da Internet; para chaves de métodos criptográficos; como senhas de sistemas computacionais e redes; para a proteção de arquivos; como chave em sistemas de autenticação, entre outros.

A partir da descrição detalhada dos componentes do método expostos na Figura 1, a seguir apresenta-se o método computacional concebido para a implementação do modelo. O método pode ser representado por três fases:

Fase 1: Geração da primeira Chave (chave 1)

Nesta fase é gerada a **chave1** por meio da aplicação de componentes aleatórios. Para isso são executados os seguintes procedimentos:

1. Gera-se **N** números aleatórios utilizando o Componente Gerador de Números Aleatórios - GNA (2). Cada um desses números deve ficar dentro dos limites entre **Y** e **K**. Cada um desses valores numéricos pode conter uma quantidade de caracteres variando entre o número de dígitos de **Y** e o número de dígitos de **K**;

2. O resultado da Fase 1 (**chave 1**) consiste na concatenação dos caracteres gerados pelos **N** números aleatórios, convertidos para formato texto. Esse procedimento é realizado pelo Componente de Concatenação (3).

Fase 2: Geração da segunda Chave (chave 2)

Nesta fase gera-se a **chave2 por meio do Componente de Mutação (4)**, a qual utilizar o operador de mutação sobre 50% da **chave1**. A seguir apresenta-se este procedimento:

1. Todos os caracteres da **chave1** são percorridos, de modo que:

i. Se a posição do caracter na **chave1** for par, esse caracter é adicionado a **chave2**;

ii.Se a posição do caracter na **chave1** for impar, será adicionado na **chave2** um caracter ASCCII aleatório.

Fase 3: Geração da Chave Final

A **chave final** é gerada pelo Componente de Concatenação Final (5), sendo composta pelos seguintes elementos:

i. Hora, minutos, segundos e milissegundos da geração da chave;

ii. chave2.

Parâmetros de Configuração:

Esse método pode ser aplicado para distintos propósitos e, por conseguinte, os valores de **N**, **Y** e **K** podem ser personalizados conforme critério de segurança da aplicação. Neste caso, especificamente, foram adotados os valores **N=300**, **Y=0**, **k=9999999999** e operador de mutação de **50%.**

Análise de Segurança do Método para Geração de Chaves Baseada em Algoritmos Genéticos

Um dos objetivos de sistemas maliciosos e de invasores (*crackers*) é quebrar a segurança do sistema computacional. Um modo de obter êxito neste propósito consiste em utilizar algoritmos e técnicas computacionais para a descoberta de senhas, chaves criptográficas, identificações de *streamings*, entre outros. O método mais utilizado para buscar quebrar qualquer mecanismo de segurança é a utilização de algoritmos de força bruta, onde o propósito do invasor é tentar todas as combinações possíveis até quebrar uma senha ou chave de segurança.

Em função desse contexto, os diferentes métodos criptográficos, assim como métodos para geração de chaves secretas são analisados sob o prisma do tempo necessário para a segurança ser quebrada aplicando técnicas

de força bruta. Desse modo, na sequencia, será apresentada uma análise dos níveis de segurança do **método para Geração de Chaves Baseado em Algoritmos Genéticos** proposto neste documento.

A tentativa de quebra de segurança do **método para Geração de Chaves Baseado em Algoritmos Genéticos** poderia ser realizada, por invasores, por meio da identificação do componente mais elaborado da **chave final**, ou seja, a **chave2**. Para demonstrar a segurança do presente método, a seguir são apresentados os cálculos do tempo necessário para a identificação e quebra da **chave2**. O melhor e o pior caso do algoritmo são considerados em função da abordagem de invasão "força-bruta", na qual todas as alternativas de nomes são testadas pelo suposto invasor.

Também é importante ressaltar que a análise será realizada considerando os valores de configuração adotados especificamente nesta descrição do método, que são **N=300**, **Y=0**, **k=9999999999** e **operador de mutação de 50%**.

A **chave1** é gerada utilizando a concatenação de **300** números aleatórios e, por isso, ela contém tamanho variável. O pior caso do algoritmo e o mais simples para o invasor é o caso em que todos os **300** números aleatórios da **chave1** sejam gerados contendo apenas um único dígito. Desse modo, a **chave1** seria composta por **300** caracteres. No melhor caso para o algoritmo e o caso de maior complexidade para o invasor é a situação em que todos os **300** números aleatórios da **chave1** sejam gerados com o número máximo de algarismos. Nesse caso, a **chave1** seria composta por um total de **3000** caracteres. Por fim, a **chave2** é gerada substituindo cada caracter decimal de posição ímpar da **chave1** (**mutação de 50%**) por um caracter ASCII aleatório dentre os **256** possíveis.

Desse modo, considerando inicialmente o caso mais simples para o invasor, são necessárias $\mathbf{256^{300} \approx 10^{722}}$ tentativas para cobrir todas as possibilidades da **chave2**. Para simplificar os cálculos, ressalta-se que cada tentativa de quebra do algoritmo pode ser realizada por uma operação de ponto flutuante do processador. Considerando um supercomputador com

processamento de **1000 TFlops**[1] (10^{15} operações de ponto flutuante por segundo), seriam necessários $\mathbf{10^{722-15} = 10^{707}}$segundos para que esse supercomputador realizasse tentativas sobre todas as possibilidades de geração da **chave2** no caso mais simples. Levando em conta que um ano contém aproximadamente $\mathbf{3.158 \times 10^7}$ segundos e arredondando por simplicidade para $\mathbf{10^8}$segundos, seriam necessários $\mathbf{10^{699}}$ anos para a quebra da **chave2** utilizando essa abordagem.

Para o caso em que a **chave1**, e consequentemente também a **chave2**, seja gerada com **3000** caracteres, seriam necessárias $\mathbf{256^{3000}} \approx \mathbf{10^{7224}}$ tentativas para cobrir todas as combinações possíveis. Nesse caso, seguindo os cálculos de maneira análoga ao caso mais simples, seriam necessários $\mathbf{10^{7201}}$ anos para efetuar todas as tentativas de quebra da segurança da **chave2**.

Além das duas situações anteriormente mencionadas, também se considerou a situação hipotética de que o invasor conheça de antemão a **chave1** e também o mecanismo de geração da **chave2**, *i.e.*, o invasor sabe que precisa descobrir apenas os dígitos ímpares da **chave2**, gerados aleatoriamente com caracteres ASCII. Desse modo, cai pela metade a quantidade de caracteres a serem descobertos, tanto no caso mais simples quanto do caso mais complexo. Assim, no caso mais simples seriam necessárias $\mathbf{256^{150}} \approx \mathbf{10^{361}}$ tentativas para cobrir todas as possibilidades, o que, também de maneira análoga aos cálculos anteriores, gastaria $\mathbf{10^{338}}$ anos para ser realizada. Para o caso mais complexo seriam gastos $\mathbf{10^{3589}}$ anos para quebrar a **chave2**.

Para se ter uma ideia da ordem de grandeza desses números, ressalta-se que $\mathbf{10^9}$ anos é igual a um bilhão de anos, o que demonstra a segurança do sistema e a necessidade de estratégias muito mais complexas por parte do invasor.

---

[1] Um supercomputador com essa capacidade de processamento estaria entre os 10 computadores mais rápidos do mundo segundo o ranking disponibilizado em http://www.top500.org/list/2012/06/100 em Junho de 2012.

Além dos dados analisados em relação a **chave1** e a **chave2**, a **chave final** ainda inclui outras importantes características que dificultam a ação de possíveis invasores, como a inclusão da **data**, **hora**, **minuto**, **segundo** e **milissegundo** que a chave foi gerada.

Outro fator que dificulta a ação dos invasores é que cada chave gerada possuir um número variável de caracteres, sendo necessário por força bruta, testar todas as combinações para cada configuração possível. No caso em análise cada chave gerada pode ter um número de caracteres variando entre 300 e 3000, o que dificulta muito a ação dos invasores.

Desse modo verifica-se que o método proposto, por meio deste pedido de invenção, possui as seguintes características principais: não necessidade nenhum *hardware* especial, o algoritmo não aplica operações matemáticas complexas e tempo elevado de processamento, além de possuir alto índice de confiabilidade em relação a segurança.

REIVINDICAÇÕES

1. Método para geração de chaves baseado em algoritmos genéticos **caracterizado por** compreender basicamente três fases, sendo elas:

   Fase 1: Geração da primeira Chave (chave 1)

   Nesta fase é gerada a chave1 por meio da aplicação de componentes aleatórios;

   Fase 2: Geração da segunda Chave (chave 2)

   Nesta fase gera-se a chave2 por meio do Componente de Mutação (4), a qual utilizar o operador de mutação sobre 50% da chave1;

   Fase 3: Geração da Chave Final

   A chave final é gerada pelo Componente de Concatenação Final (5).

2. Método para geração de chaves baseado em algoritmos genéticos, de acordo com a reivindicação 1, **caracterizado por** na fase 1 serem executados os seguintes procedimentos:

   a. Gera-se **N** números aleatórios utilizando o Componente Gerador de Números Aleatórios - GNA (2), cada um desse números deve ficar dentro dos limites entre **Y** e **K**, cada um desses valores numéricos pode conter uma quantidade de caracteres variando entre o número de dígitos de **Y** e o número de dígitos de **K**;

   b. O resultado da Fase 1 (chave 1) consiste na concatenação dos caracteres gerados pelos **N** números aleatórios, convertidos para formato texto, esse procedimento é realizado pelo Componente de Concatenação (3).

3. Método para geração de chaves baseado em algoritmos genéticos, de acordo com a reivindicação 1, **caracterizado por** na fase 2 ser executado o seguinte procedimento:

a. Todos os caracteres da chave1 são percorridos, de modo que:
    i. Se a posição do caracter na chave1 for par, esse caracter é adicionado a chave2;
    ii. Se a posição do caracter na chave1 for impar, será adicionado na chave2 um caracter ASCCII aleatório.

4. Método para geração de chaves baseado em algoritmos genéticos, de acordo com a reivindicação 1, **caracterizado por** na fase 3, Componente de Concatenação Final (5) é composto pelos seguintes elementos:
    a. Hora, minutos, segundos e milissegundos da geração da chave;
    b. chave2.
5. Método para geração de chaves baseado em algoritmos genéticos, de acordo com a reivindicação 2, **caracterizado por N**, **Y** e **K** poderem ter seus valores personalizados conforme critério de segurança da aplicação.
6. Sistema para geração de chaves **caracterizado por** compreender os seguintes elementos:
    a. Componente Gerador de Números Aleatórios - GNA (2);
    b. Componente de Concatenação - CC (3);
    c. Componente de Mutação - CM (4);
    d. Componente de Concatenação Final - CCF (5);
    e. Chave Final - CF (6).
7. Sistema para geração de chaves, de acordo com a reivindicação 6, **caracterizado por** a etapa "a" ser responsável pela geração de números aleatórios, aplicando o operador de aleatoriedade inspirado na Teoria de Evolução das Espécies.
8. Sistema para geração de chaves, de acordo com a reivindicação 6, **caracterizado por** a etapa "b" possuir a função de receber **N** números aleatórios (com número de dígitos variável), converter para o formato

texto e por fim retornar uma chave consistindo na concatenação desses **N** números aleatórios.

9. Sistema para geração de chaves, de acordo com a reivindicação 6, **caracterizado por** a etapa "c" ser derivada dos princípios de mutação de algoritmos genéticos, receber uma chave1 como entrada e aplicar uma mutação de 50% gerando uma chave2.
10. Sistema para geração de chaves, de acordo com a reivindicação 6, **caracterizado por** a etapa "d" receber a chave2 como entrada e serem acrescentadas algumas características adicionais para dificultar a descoberta da chave por técnicas maliciosas.
11. Uso do método descrito nas reivindicações de 1 a 5 **caracterizado por** ser na geração de chaves que podem ser utilizadas para distintas finalidades, tais como para a publicação de *streamings* áudio e vídeo, para algoritmos de criptografia, para geração de senhas, para proteção de arquivos, entre outros.

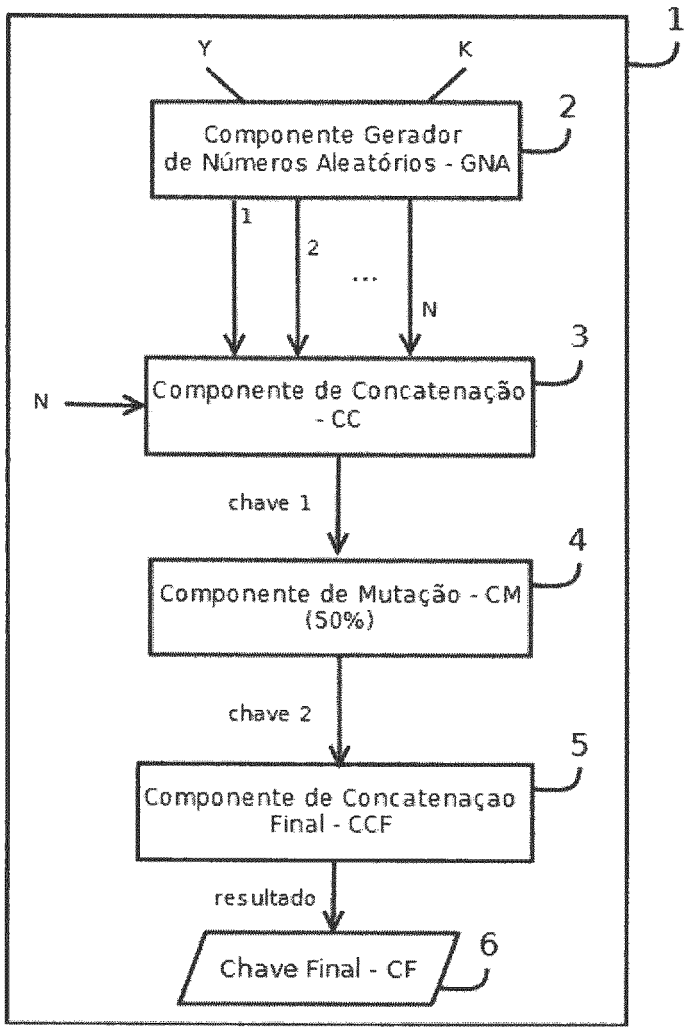


Figura 1

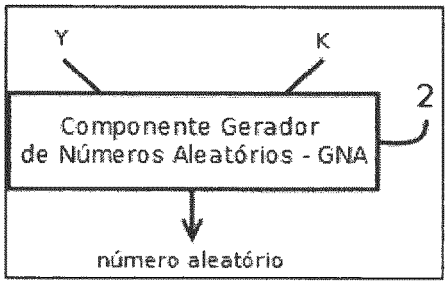


Figura 2

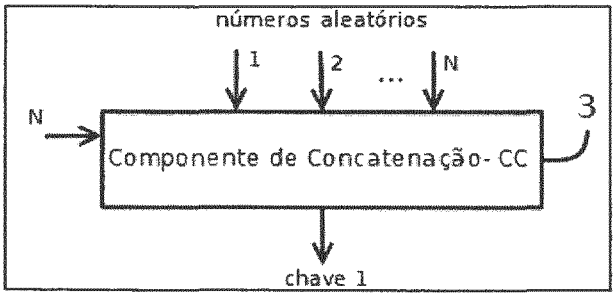


Figura 3

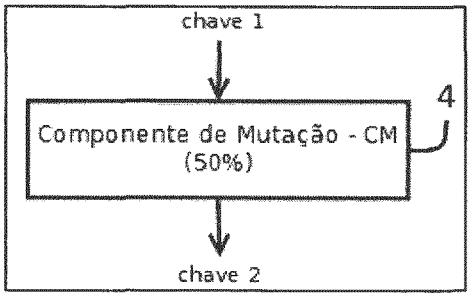


Figura 4

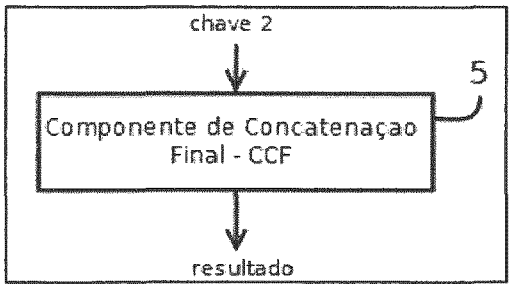


Figura 5

RESUMO

MÉTODO PARA GERAÇÃO DE CHAVES BASEADA EM ALGORITMOS GENÉTICOS

Refere-se o presente pedido de patente de invenção a um novo método computacional sistêmico para a geração de chaves secretas, inspirado na Teoria da Evolução das Espécies, especialmente na genética e seleção natural. Esse método permite que sejam definidos parâmetros importantes, como limite inferior e superior para geração de números aleatórios, assim como quantidade de números que irão contribuir para compor a chave e ainda índice de mutação que será aplicado no algoritmo.

Desse modo o método proposto pode ser aplicado para distintas finalidades, tais como para a aplicação como chaves de algoritmos de criptografia, para geração de senhas, para a proteção de arquivos, para publicação de *streamings* de áudio e vídeo, entre outros.

As principais vantagens do método proposto consistem em não necessitar nenhum *hardware* específico para ser executado, utiliza operações matemáticas simples e sem alto custo de execução, é configurável para trabalhar as variáveis e definir o grau de segurança desejado, e foi concebido com conceitos de algoritmos genéticos dificultando tentativas de invasão.